ABC cyberbezpieczeństwa

Wi-Fi

nomofobia

użytkownik

trolling

uwierzytelnianie dwuskładnikowe

jailbreak

zakupy online

gray hat

phishing

vishing

aktualizacja

A–Z

oszustwa internetowe

cyberprzemoc

uzależnienie od gier komputerowych

malware

fake news

stalking

usługi bezpieczeństwa OSE

kradzież tożsamości

backup

www.it-szkola.edu.pl

Rzeczpospolita Polska

ose Ogólnopolska Sieć Edukacyjna

NASK

Spis treści

Wstęp

Szkodliwe treści, FOMO, child grooming, phishing, scam, hejt, oversharing – cyfrowych zagrożeń wciąż przybywa i coraz trudniej za nimi nadążyć. W Ogólnopolskiej Sieci Edukacyjnej (OSE) rozumiemy to doskonale! Warto poznać potencjalne niebezpieczeństwa i nauczyć się przed nimi chronić. Właśnie dlatego powstał poradnik „ABC cyberbezpieczeństwa": chcemy, by służył Wam jako koło ratunkowe i niezbędnik przybliżający szeroko pojęty świat internetu.

W publikacji znajdziecie ułożone alfabetycznie pigułki wiedzy, które dotyczą z jednej strony wirtualnych zagrożeń, a z drugiej – dobrych praktyk i cyfrowych nawyków. Czym jest malware, dlaczego warto zdecydować się na social media sabbatical, jak utworzyć silne hasło i kopię zapasową, gdzie zgłosić incydent bezpieczeństwa? Odpowiedzi na te i inne pytania znajdziecie w 157 hasłach opatrzonych obszerną bibliografią.

Nasz cyberbezpieczny alfabet od kwietnia do czerwca 2022 r. ukazywał się jako cykl aktualności na platformie e-learningowej OSE IT Szkoła. Teraz oddajemy w Wasze ręce hasła zebrane w publikacji „ABC cyberbezpieczeństwa" – w wersji odświeżonej i uzupełnione o nowe definicje.

Bezpieczeństwo w sieci to podstawa, więc dbajmy o nie razem. Życzymy owocnej lektury i… wszystkiego cyberbezpiecznego!

A

Administrator

Czy wiecie, kto nadzoruje działanie stron internetowych, baz danych i serwerów, odpowiada za konfigurację urządzeń i oprogramowania? Tą niezbędną do prawidłowego funkcjonowania lokalnych sieci internetowych osobą jest administrator.

Jego ważnym zadaniem jest również reagowanie na zgłoszenia użytkowników, dotyczące m.in. naruszeń prawa do prywatności i/lub bezpieczeństwa w sieci (np. hejtu w komentarzach na forach dyskusyjnych czy zamieszczanych na stronach szkodliwych treści). W takich przypadkach administratorzy mają możliwości i obowiązek usuwania niepożądanych materiałów czy blokowania cyberagresorów. Jeśli zauważycie w sieci coś, co Was zaniepokoi, skontaktujcie się z administratorem, np. za pomocą formularza kontaktowego.

W Ogólnopolskiej Sieci Edukacyjnej administratorami są Techniczni Reprezentanci Szkół (TRS), którzy pełnią rolę administratorów szkolnych sieci LAN, konfigurują urządzenia, instalują nowe wersje oprogramowania oraz na bieżąco współpracują z Centrum Kontaktu OSE (tel.: +48 22 182 55 55, e-mail: wsparcietechniczne_ose@nask.pl).

Adware

Pewnie nie raz podczas przeglądania internetu zdarzyło Wam się spotkać natarczywe reklamy, przede wszystkim w formie bannerów lub wyskakujących okien przeglądarki internetowej. Odpowiada za nie adware – niechciane oprogramowanie, które podszywa się pod pozornie bezpieczne aplikacje, aby skłonić użytkowników do zainstalowania ich na swoich urządzeniach (telefonach, komputerach, tabletach). Bywa, że takie programy występują w pakiecie z innym bezpłatnym oprogramowaniem.

Złośliwe oprogramowanie typu adware może być niebezpieczne – zdarza się, że automatycznie przekierowuje na określone strony internetowe, a także łączy się np. z programami szpiegującymi (spyware) czy umożliwiającymi włamania do systemów informatycznych (rootkit).

Jak chronić się przed adware? Przede wszystkim, chcąc pobrać jakąś aplikację czy program, korzystajcie tylko z wiarygodnych źródeł. Zastanówcie się dwa razy, czy faktycznie potrzebujecie nowego oprogramowania, zanim je pobierzecie! Korzystajcie też z antywirusa. Jeśli zauważycie coś niepokojącego, odinstalujcie nową aplikację, którą podejrzewacie o to, że jest powiązana z programem typu adware.

Aktualizacja

Systematyczne aktualizacje oprogramowania – czyli instalacje jego nowszych, poprawionych wersji – to podstawa! Pozwalają chronić urządzenia i dbać o Wasze bezpieczeństwo w sieci. Nowe wersje programów czy aplikacji zwykle naprawiają błędy, zawierają nowe funkcjonalności, wpływają również na wygodę użytkowania sprzętów.

Jak się pewnie domyślacie, dla cyberbezpieczeństwa ważne są zwłaszcza usprawnienia związane z prywatnością i ochroną. Producenci oprogramowania na bieżąco reagują na nowe zagrożenia pojawiające się w cyberprzestrzeni i dzięki aktualizacjom pomagają np. zwiększyć odporność aplikacji na ataki. Dzięki częstym aktualizacjom oprogramowania możecie czuć się bezpiecznie, korzystając z aplikacji bankowych czy innych programów przechowujących dane osobowe lub istotne informacje.

Jak być zawsze na bieżąco z kolejnymi aktualizacjami? Możecie np. włączyć automatyczne pobieranie aktualizacji (w ustawieniach telefonu czy komputera).

Więcej o aktualizacjach dowiecie się z aktualności na stronie ose.gov.pl: „Akcja-aktualizacja – zadbaj o swój sprzęt w wakacje!” i „E-wyprawka: sprawdź urządzenie, porozmawiaj z dzieckiem”.

Anonimowość w sieci

W internecie nic nie znika – znacie to powiedzenie? Korzystając z sieci, wszyscy pozostawiamy za sobą cyfrowe ślady – np. adres IP (*Internet Protocol*), wyszukiwania w przeglądarce, dane geolokalizacyjne i inne. Z kolei dzięki tzw. ciasteczkom (pliki cookies) serwery stron śledzą naszą aktywność w sieci. Wszystkie te informacje mogą trafić w niepowołane ręce i służyć m.in. do szpiegowania czy kradzieży tożsamości.

I tu z pomocą przychodzą narzędzia, które pozwalają zachować anonimowość w sieci oraz utrudniają cyberprzestępcom dotarcie do wrażliwych danych. Rozwiązaniem może być m.in.: łączenie się z internetem za pomocą VPN (*Virtual Private Network*) – tzw. sieci tunelowej, korzystanie z trybu incognito w przeglądarce i tymczasowych skrzynek poczty e-mail. Chcąc zachować anonimowość online, zwracajcie również uwagę na publikowane treści, m.in. w mediach społecznościowych (nigdy nie udostępniajcie tam np. skanów dokumentów lub innych wrażliwych informacji!).

A co, jeśli chcemy zniknąć z sieci? Umożliwia nam to prawo do bycia zapomnianym, wynikające z rozporządzenia unijnego RODO (Ogólnego rozporządzenia o ochronie danych). Dokument ten daje osobom fizycznym, a zatem nam wszystkim, prawo żądania od administratora niezwłocznego usunięcia swoich danych osobowych.

Jeśli chcecie dowiedzieć się więcej o anonimowości w internecie, koniecznie zajrzyjcie do e-kursu „Cyberprzemoc – anonimowość w sieci" dostępnego na platformie OSE IT Szkoła.

Aplikacja

Nawigacja, krokomierz, rozkład jazdy autobusów, serwisy streamingowe, komunikatory, bankowość mobilna, czytnik e-booków – z tych i innych aplikacji chętnie korzystamy na swoich urządzeniach przenośnych, takich jak smartfony czy tablety. Aplikacje ułatwiają nam wiele codziennych czynności: używanie poczty e-mail, kontakty z bliskimi, załatwianie formalności, zakupy czy oglądanie filmów lub seriali.

Na pewno znacie zalety aplikacji: należą do nich wygoda, powszechny dostęp, sprawne działanie, angażujące funkcje, możliwość personalizacji i zmiany ustawień.

Jeśli zależy Wam na bezpiecznym korzystaniu z aplikacji, musicie pamiętać o kilku zasadach. Przede wszystkim pobierajcie apki tylko z oficjalnych, bezpiecznych źródeł, czyli ze sklepów z aplikacjami przeznaczonymi dla odpowiednich systemów operacyjnych (najpopularniejsze to Google Play dla systemu Android i App Store dla systemu iOS). Pamiętajcie też o ograniczeniu uprawnień aplikacji – np. odmowie dostępu do danych lokalizacyjnych czy innych danych na urządzeniu i rozważnym dokonywaniu mikropłatności. Wreszcie – nie podawajcie swoich danych na nieznanych urządzeniach, logujcie się do nich tylko ze swojego smartfona czy tabletu.

Warto wiedzieć, że każda aplikacja może mieć luki, których efektem jest np. naruszenie prywatności. Z tego powodu regularnie przeglądajcie apki na swoim smartfonie i instalujcie aktualizacje zalecane przez producenta. Od jakiegoś czasu nie korzystacie z którejś aplikacji? Usuńcie ją!

Jeśli jesteście rodzicami – polecamy Wam naszą aplikację ochrony rodzicielskiej mOchrona, która skutecznie pomaga w kształtowaniu dobrych postaw oraz diagnozowaniu potencjalnych problemów i zagrożeń.

Porady dotyczące bezpiecznego korzystania z aplikacji znajdziecie w aktualności „Bezpieczni w sieci z OSE: aplikacje mobilne" na stronie ose.gov.pl.

B

Backdoor

To pojęcie możemy przetłumaczyć jako „tylne drzwi” lub „furtka”. Co ma wspólnego z bezpieczeństwem w sieci? Backdoor to nic innego jak umyślnie pozostawiona luka w zabezpieczeniach systemu komputerowego. Celem tego działania jest późniejsze wykorzystanie „szczeliny” w oprogramowaniu do bardzo niebezpiecznych działań, takich jak np. przejęcie kontroli nad zainfekowanym systemem. Backdoor może zostać pozostawiony przez złośliwe oprogramowanie (malware), cyberprzestępcę, ale też umyślnie stworzony przez autora danego programu.

Niestety „tylne drzwi” mogą być ogromnym zagrożeniem, dlatego zawsze powinniście pamiętać o zasadach bezpiecznego korzystania z urządzeń cyfrowych – w tym o aktualizacji oprogramowania i programu antywirusowego czy rozważnym instalowaniu aplikacji i innych narzędzi.

Backup

Urządzenia cyfrowe to dla wielu z nas prawdziwe kopalnie wspomnień – zdjęć, filmów i innych plików, mających wartość sentymentalną. Co w sytuacji, gdy utracicie Wasz sprzęt lub znajdujące się na nim pliki? Wtedy przyda się backup! To kopia zapasowa danych przechowywana w innych miejscach niż ich oryginalne wersje. Dzięki temu rozwiązaniu możecie zabezpieczyć ważne materiały przed utratą, np. na skutek usunięcia plików, kradzieży lub zainfekowania sprzętu złośliwym oprogramowaniem (malware). Najprościej mówiąc, backup to taki cyfrowy plan B, który pozwoli Wam szybko i bez zbędnego stresu odzyskać utracone cenne dane.

Jak przygotować się do stworzenia backupu? Wszystkiego dowiecie się z aktualności „Masz już swój plan B?”, którą znajdziecie na platformie OSE IT Szkoła.

Bańka informacyjna

Wiedzieliście, że w sieci łatwo można wpaść w tzw. bańkę informacyjną (filtrującą)? Co więcej – sami się w niej zamykamy!

Z bańką informacyjną możecie mieć do czynienia wtedy, gdy w internecie otrzymujecie wyselekcjonowane wiadomości, wybrane dla Was w wyniku działania określonych algorytmów. Jak to się dzieje? Algorytmy dobierają informacje podobne do tych, których wcześniej szukaliście – możliwie najbardziej atrakcyjne i odpowiadające Waszym potrzebom. Zwykle bazują też na wiedzy zgromadzonej o użytkowniku przez dany portal, np. na podstawie Waszej historii wyszukiwania.

Jakie mogą być skutki utknięcia w bańce filtrującej? Wśród nieprzyjemnych konsekwencji można wymienić m.in.: zamknięcie na nowe pomysły, tematy i ważne wiadomości, ograniczenie dostępu do innych punktów widzenia niż własny, jak również większą podatność na manipulację i propagandę.

Zobaczcie koniecznie konspekt zajęć „Fake newsy i dezinformacja – o tym warto porozmawiać w szkole" dostępny na platformie OSE IT Szkoła.

Baza danych

Czy wiecie, że każdego dnia korzystacie z różnych baz danych? Robicie to m.in. podczas używania wyszukiwarek internetowych, sprawdzania rozkładów jazdy pociągów lub autobusów, a nawet… wypłacania pieniędzy z bankomatu!

Większość systemów informatycznych wykorzystuje właśnie bazy danych – czym więc one są? Bazą danych nazywamy zbiór informacji zapisanych według ściśle określonych reguł. Celem gromadzenia danych jest późniejsze wykorzystanie, dlatego dzięki określonym zasadom możemy zachowywać porządek na etapie ich przechowywania, a także poprawnie je interpretować.

Więcej na temat baz danych oraz ich tworzenia dowiecie się z kursów e-learningowych zamieszczonych na platformie OSE IT Szkoła.

Bomba logiczna

To rodzaj złośliwego oprogramowania (malware), które aktywuje się po spełnieniu określonych warunków. Tykająca bomba eksplodująca w najmniej oczekiwanym momencie? Dosłownie! „Detonacja" może nastąpić np. w określonym dniu tygodnia lub o danej godzinie (bomba czasowa), po otwarciu przeglądarki, zalogowaniu się konkretnego użytkownika, otwarciu lub usunięciu pliku czy uruchomieniu programu.

Ten rodzaj cyfrowego ataku jest niebezpieczny, ponieważ po zainstalowaniu złośliwego oprogramowania na Waszym urządzeniu przez dłuższy czas możecie nie zauważać oznak zagrożenia. Problemy zaczną się w momencie aktywacji bomby logicznej, która wyrządza znaczne szkody. W wyniku jej działania możecie stracić swoje pliki, a nawet dane z dysku twardego. Zablokowanie dostępu do określonych programów lub aplikacji to również częste skutki uruchomienia szkodliwego kodu. Ponadto przestępcy mogą wykorzystać Wasz adres e-mail do przeprowadzenia kampanii spamowych (spam).

Jak się bronić przed tego typu atakiem? Jak zawsze korzystajcie z programów antywirusowych, dbajcie o regularne aktualizacje, pobierajcie oprogramowanie tylko ze sprawdzonych źródeł oraz uważajcie na ataki phishingowe.

Bot

To program mający na celu wykonywanie pewnych czynności za człowieka. Przykładów wykorzystania botów można wymienić wiele, a wraz z rozwojem nowych technologii na pewno będzie ich przybywać. Niezależnie, czy zdajecie sobie z tego sprawę, czy nie – programy te wykorzystywane są m.in. w automatycznych systemach obsługi klientów online (chatbot), do zbierania informacji (czyli tzw. indeksujące boty) czy obsługi inteligentnych domów. Warto pamiętać, że oprogramowanie typu bot może być wykorzystywane zarówno do pozytywnych, jak i negatywnych działań.

Wiadomości na temat botów znajdziecie w materiałach dostępnych na platformie OSE IT Szkoła: aktualności „Dzień Bota – dowiedz się więcej o sztucznej inteligencji!" oraz kursach e-learningowych o sztucznej inteligencji.

Botnet

Kolejnym zagrożeniem w sieci, które powinniście zapamiętać, jest botnet, czyli grupa komputerów-zombie zainfekowanych szkodliwym oprogramowaniem. Dlaczego to tak niebezpieczne? Ponieważ umożliwia cyberprzestępcy przejmowanie kontroli nad wieloma (a czasem nawet nad setkami lub tysiącami!) „zarażonymi" komputerami i wykorzystywanie ich np. do wykradania danych osobowych, rozsyłania spamu lub wirusów czy przeprowadzania ataków DDoS. Ponadto wszystkie te operacje dzieją się bez wiedzy i zgody właścicieli sprzętów, którzy są nieświadomi, do czego wykorzystuje się ich komputery.

Browser hijacker

Wyobraźcie sobie, że Wasze dziecko wbrew swojej woli trafia na witrynę ze szkodliwymi treściami albo w jego zakładkach z zaufanymi stronami pojawiają się nagle te nieodpowiednie dla młodych użytkowników sieci. Może to być wynik działania złośliwego oprogramowania (malware) – browser hijacker, którego nazwę można przetłumaczyć jako „porywacz przeglądarek".

Browser hijacker przejmuje kontrolę nad przeglądarką internetową, zarządzając nią bez udziału użytkownika. W efekcie może się nagle okazać, że Wasza strona główna została zmieniona lub otwierają się witryny, których nie zamierzaliście odwiedzać – najczęściej przeładowane reklamami czy nieodpowiednimi treściami. W ten sposób przestępcy czerpią zyski z liczby wejść na daną stronę. Co więcej, „porywacz przeglądarek" uniemożliwia dostanie się na platformy z oprogramowaniem antywirusowym czy antyszpiegowskim.

Takie działania znacznie utrudniają korzystanie z internetu, a nawet bywają bardzo niebezpieczne. Oprócz problemów z przeglądaniem sieci browser hijacker może bowiem zawierać oprogramowanie szpiegujące, np. keyloggery.

Jak dochodzi do zainfekowania sprzętu browser hijackerem? Najczęściej podczas pobierania plików i „przydatnych" dodatków z nieznanych źródeł. Złośliwe oprogramowanie ukrywa się też w załącznikach przesyłanych drogą mailową. Aby uniknąć tego typu zagrożenia, aktualizujcie system i przeglądarki, korzystajcie z programów antywirusowych oraz pobierajcie oprogramowanie tylko z legalnych stron. Nie klikajcie też w natarczywe reklamy – np. te w formie bannerów lub wyskakujących okien przeglądarki internetowej – mogą one uruchomić instalację „porywacza"!

Business Email Compromise (BEC)

Cyberprzestępcy stosują różne metody, by wyłudzić pieniądze lub poufne informacje. Ich ataki wymierzone są nie tylko w instytucje czy osoby prywatne, ale również w firmy – zarówno mniejsze, jak i te duże. Jedną z popularnych praktyk jest *Business Email Compromise* (BEC), czyli „oszustwo na dyrektora".

W tym przypadku przestępcy wykorzystują nieuwagę i uśpioną czujność pracowników. Jak działają? Dobrze przygotowują się do ataku: zbierają informacje o firmie, pracownikach – głównie wyższego szczebla – i kontrahentach. Następnie przygotowują fałszywe wiadomości e-mail, w których podszywają się pod prezesa danej firmy lub podają się za członków organizacji, z którymi firma współpracuje. W kolejnym kroku mailem wysyłają dyrektorom finansowym, głównym księgowym czy prawnikom – czyli osobom decyzyjnym – polecenie pilnego uregulowania zaległej płatności lub zmiany numeru rachunku, na który mają być przekazywane pieniądze. Niestety, często okazuje się, że prośby od rzekomego szefa lub partnera biznesowego zwykle spełniane są bez zbędnej zwłoki.

Jak więc bronić się przed BEC? Kierujcie się zasadą ograniczonego zaufania. Sprawdzajcie, czy adres e-mail, z którego otrzymaliście wiadomość, jest poprawny, zwróćcie też uwagę na domenę. Waszą czujność powinny wzbudzić błędy językowe, a także wymuszanie działania pod presją czasu. Pamiętajcie też, że przestępcy mogą uzyskać dostęp do poczty pracownika wyższego szczebla i maile od niego mogą wyglądać bardzo wiarygodnie. Jeśli więc cokolwiek wzbudzi Wasze podejrzenia, skontaktujcie się z daną osobą telefonicznie i potwierdźcie zasadność danego działania.

Cyberoszustwa zgłaszajcie na policję, a wszelkie incydenty zagrażające Waszemu bezpieczeństwu – do CERT Polska.

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)

Zakładacie konto na portalu lub forum dyskusyjnym, uzupełniacie formularz online, zmieniacie hasło do poczty e-mail – procedura już niemal zakończona, ale jeszcze… „Potwierdź, że nie jesteś robotem”. To tzw. CAPTCHA: rodzaj dodatkowego zabezpieczenia, znanego jako uwierzytelnianie typu wywołanie – reakcja. CAPTCHA polega na wyświetleniu prostego testu, który ma za zadanie sprawdzić, czy użytkownik próbujący się logować jest człowiekiem, a nie komputerem włamującym się na konto chronione hasłem.

Na pewno spotkaliście się z różnymi typami CAPTCHA: może to być np. prośba o wykonanie prostego działania matematycznego, przepisanie zniekształconego tekstu z obrazka, podanie odpowiedzi na wyświetlone pytanie, dopasowanie brakującego elementu układanki albo wskazanie określonych elementów na zdjęciu. Choć rozwiązanie to może wydawać się uciążliwe, to pozwala w znacznym stopniu zabezpieczyć nasze informacje, wrażliwe dane i ochronić przed nieuprawnionym dostępem do kont. Zastosowanie tego mechanizmu chroni m.in. przed tworzeniem sztucznych kont przez automaty (boty), dużą liczbą zapytań do serwera, spamem w formularzach kontaktowych czy reklamami w komentarzach na blogach.

CAPTCHA kojarzy Wam się pewnie z testem Turinga, który może pomóc odróżnić człowieka od komputera. I słusznie! Zabezpieczenie to od samego początku – po raz pierwszy w znanej dziś formie zostało użyte w 2000 r. – miało zapobiegać zautomatyzowaniu stron internetowych i działalności botów. W oryginalnym założeniu CAPTCHA to dowolne zadanie, z którym człowiek poradzi sobie łatwo, a komputer nie będzie w stanie go wykonać.

Chcecie dowiedzieć się więcej o teście Turinga i botach? Zajrzyjcie do kursów dotyczących sztucznej inteligencji na OSE IT Szkole!

CERT Polska

O tym, jak szkodliwe i nieprzyjemne w skutkach potrafią być incydenty w sieci, przekonało się już wielu użytkowników nowych technologii. Gdzie zgłosić niebezpieczną domenę wyłudzającą pieniądze, podejrzane SMS-y i e-maile, złośliwe oprogramowanie (malware) lub fałszywy sklep internetowy? Z pomocą przychodzi CERT Polska (Computer Emergency Response Team Polska) – czyli zespół reagowania na incydenty działający w strukturach NASK – Państwowego Instytutu Badawczego.

Do zadań CERT Polska należą: monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym, reagowanie na otrzymane zgłoszenia,

wydawanie komunikatów o zidentyfikowanych niebezpieczeństwach, współpraca z podobnymi jednostkami na całym świecie czy prowadzenie działań z zakresu budowania świadomości w obszarze cyberbezpieczeństwa. Od 2018 r. zespół CERT Polska realizuje część zadań CSIRT NASK.

Więcej o działaniach CERT Polska dowiecie się ze strony cert.pl.

Chmura

Choć nazwa ta pewnie przywołuje Wam na myśl głównie meteorologiczne skojarzenia, to w kontekście internetu i nowych technologii jako chmurę rozumiemy przestrzeń w sieci, w której dane są przechowywane i zarządzane przez dostawcę usługi. Taka wirtualna przestrzeń pozwala m.in. na tworzenie backupu, czyli kopii zapasowych cyfrowych zasobów.

Więcej o chmurze dowiecie się z biuletynu „OUCH! – Bezpieczne przechowywanie danych w chmurze" oraz aktualności na stronie ose.gov.pl „Bezpieczni w sieci z OSE: przechowywanie danych w chmurze".

Clickbait

Czy zdarzyło się Wam kiedyś kliknąć w artykuł tylko z powodu sensacyjnego tytułu lub miniaturki, która wyolbrzymiała faktyczną treść materiału bądź w ogóle do niej nie pasowała? Jeśli tak, to zetknęliście się z clickbaitem. Wyrażenie to powstało z połączenia angielskich słów *click* (kliknięcie) i *bait* (przynęta). Celem clickbaitów jest wyróżnienie się w morzu innych konkurencyjnych doniesień medialnych i skuteczne przyciągnięcie uwagi użytkownika, który – zachęcony zaskakującym przekazem – wejdzie w dany artykuł. Uwaga! Niektóre clickbaity mogą wpływać na szerzenie się dezinformacji w sieci!

Chcecie dowiedzieć się więcej o dezinformacji oraz ochronie przed manipulacją w internecie? Przeczytajcie koniecznie aktualności na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: fake newsy" oraz „Zanim uwierzysz, sprawdź!".

CRP (stopień alarmowy)

Spotkaliście się kiedyś w mediach lub internecie z określeniem „stopień CHARLIE-CRP" i zastanawialiście się, co to takiego? Śpieszymy z wyjaśnieniami. Termin ten jest związany z cyberbezpieczeństwem kraju. Stopnie alarmowe CRP zostały określone w ustawie o działaniach antyterrorystycznych i są wprowadzane w sytuacjach, gdy pojawia się wzmożone zagrożenie w cyberprzestrzeni. Wyróżniamy cztery stopnie alarmowe CRP: pierwszy (ALFA-CRP), drugi (BRAVO-CRP), trzeci (CHARLIE-CRP) i czwarty (DELTA-CRP).

Każdego dnia powinniście pamiętać o zachowaniu bezpieczeństwa w sieci, a w sytuacjach, gdy zostanie wprowadzony któryś stopień alarmowy CRP, swoją czujność warto jeszcze dodatkowo wzmocnić.

Więcej o stopniach alarmowych CRP dowiecie się z aktualności „Stopnie alarmowe i stopnie alarmowe CRP" dostępnej na stronie Ministerstwa Spraw Wewnętrznych i Administracji.

CSIRT

Czy wiecie, że o bezpieczeństwo naszego kraju dbają specjalnie utworzone zespoły CSIRT (*Computer Security Incident Response Team*), a dokładnie trzy Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego? Na mocy Ustawy o krajowym systemie cyberbezpieczeństwa rolę CSIRT poziomu krajowego przyjęły na siebie Agencja Bezpieczeństwa Wewnętrznego (CSIRT GOV), NASK – Państwowy Instytut Badawczy (CSIRT NASK) oraz resort obrony narodowej (CSIRT MON).

Koordynowanie oraz obsługa zgłoszonych incydentów, sprawne zarządzanie ryzykiem, a także skuteczne reagowanie na wszelkie niebezpieczne sytuacje zagrażające bezpieczeństwu sieci i systemów informatycznych – to główne zadania CSIRT.

Warto wspomnieć, że obowiązki CSIRT NASK zostały powierzone zespołowi CERT Polska i Dyżurnet.pl. Oprócz rejestrowania i obsługi zdarzeń naruszających bezpieczeństwo sieci, a także aktywnego reagowania na zagrożenia, CSIRT NASK prowadzi również działalność badawczą z zakresu metod wykrywania incydentów bezpieczeństwa. Ponadto realizuje też wiele projektów informacyjno-edukacyjnych, mających na celu poprawę świadomości użytkowników sieci w zakresie bezpieczeństwa teleinformatycznego. Zachęcamy do lektury raportów z działalności CERT Polska zawierających dane o popularnych cyberzagrożeniach, z którymi każdego roku stykają się polscy internauci.

Warto wiedzieć, że CSIRT NASK przyjmuje zgłoszenia od podmiotów publicznych, operatorów usług kluczowych, dostawców usług cyfrowych, ale też od wszystkich obywateli, którzy przekazując tego typu informacje, przyczyniają się do zwiększenia bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej.

Dowiedzcie się, jak zgłosić incydent bezpieczeństwa, i bądźcie bezpieczni w sieci!

Cyberprzemoc

Internet przynosi nam wiele korzyści, ale naraża też na niebezpieczeństwa. Jednym z nich jest cyberprzemoc, czyli agresywne zachowania lub działania w sieci. Zjawisko to inaczej określane jest jako cyberbulling, dręczenie, nękanie bądź prześladowanie w internecie. Cyberprzemoc może przybierać różne formy (np. agresji słownej, upubliczniania upokarzających zdjęć i filmów, wykluczenia z grona wirtualnych znajomych, szantażu). Rozprzestrzenia się szybko, a jej sprawcy niestety zwykle czują się anonimowi. Nie zapominajmy, że agresja w sieci jest tak samo szkodliwa jak ta w świecie realnym i może nieść za sobą przykre konsekwencje.

Chcecie dowiedzieć się więcej? Zapoznajcie się z aktualnością „Niebezpieczne zjawiska w internecie: cyberprzemoc w szkole", w której zebraliśmy pomocne materiały na temat cyberprzemocy. Znajdziecie ją na platformie OSE IT Szkoła.

Cyberstalking

To internetowa odmiana stalkingu, która polega na nękaniu drugiej osoby w sieci (np. przy wykorzystaniu serwisów społecznościowych czy komunikatorów). Ten rodzaj cyberprzemocy może mieć swoje źródło zarówno w świecie online, jak i offline.

Cyberstalkingiem określamy m.in. nękanie poprzez wielokrotne wysyłanie komuś w sieci lub przy użyciu urządzeń cyfrowych niechcianych materiałów i informacji, cyberdręczenie, kradzież tożsamości, nielegalny monitoring, śledzenie, rozsyłanie wiadomości w imieniu – ale wbrew woli – innej osoby. Działania stalkera wywołują u ofiary nieprzyjemne uczucia – strach, panikę, wstyd i poczucie winy.

Więcej informacji o cyberstalkingu oraz procedurach reagowania znajdziecie w poradniku „Bezpieczeństwo online w szkołach Ogólnopolskiej Sieci Edukacyjnej" – część 2 dostępnym na platformie OSE IT Szkoła.

Cyfrowy kidnapping

To zjawisko łączy się z sharentingiem, czyli regularnym – i niestety zwykle nierozsądnym – dzieleniem się w sieci zdjęciami swojego dziecka. Cyfrowy kidnapping to przestępstwo, w którym ktoś kradnie wizerunek dziecka. Po co to robi? Powodem może być m.in. oszustwo finansowe. Cyberprzestępcy tworzą w tym celu fałszywy profil rodzicielski, na którym będą zarabiać. Wykorzystują do tego skradzione, prawdziwe materiały (najczęściej zdjęcia), wokół których budują dziecku nową tożsamość – nadają mu fałszywe imię i nazwisko, opisują, co lubi, a czego nie, oraz przypisują fikcyjnych opiekunów.

Innym, jeszcze groźniejszym powodem cyfrowego kidnappingu jest kradzież wizerunku dziecka w celu realizacji różnych fantazji przestępcy i jego obserwatorów, w tym tych seksualnych lub przemocowych.

Aby chronić wizerunek, a często i bezpieczeństwo dziecka, rodzice zawsze powinni rozważnie udostępniać materiały z jego udziałem. Pamiętajcie, że nigdy nie mamy pewności, kto może być odbiorcą treści zamieszczanych przez nas w sieci!

Dowiedzcie się więcej o sharentingu, cyfrowym kidnappingu i ochronie wizerunku dziecka w sieci z materiałów dostępnych na platformie OSE IT Szkoła: poradnika dla rodziców „Sharenting i wizerunek dziecka w sieci" oraz kursu e-learningowego „Sharenting. Czy warto mieć rodzinny album w sieci?".

Zobaczcie też webinar „Rodzinny album z wakacji, czyli czego o dzieciach nie powinien wiedzieć internet” na Facebooku OSE – Ogólnopolska Sieć Edukacyjna.

Cyfrowy ślad

Wszyscy zostawiamy w internecie swój cyfrowy ślad – odciska go każda aktywność w sieci. Nasze dane (m.in. wpisywane w formularzach e-sklepów, wysyłane w wiadomościach czy przekazywane razem z komentarzami w mediach społecznościowych) trafiają do baz danych i chmur obliczeniowych, a tam… zaczynają żyć własnym życiem.

Swój cyfrowy ślad możemy zostawiać celowo – gdy wysyłamy e-maile, komentujemy posty w mediach społecznościowych, publikujemy zdjęcia czy filmy. Bierne ślady to m.in. informacja o systemie operacyjnym, adresie IP, używanej przeglądarce internetowej, ale też dane geolokalizacyjne czy godzina i data wykonania zdjęcia dodanego do posta w social mediach. Nawet jeśli wydaje nam się, że pozostajemy anonimowi, udostępniamy informacje o swoich kliknięciach, które mogą być analizowane, rejestrowane i przechowywane. Profilowane reklamy i bańki informacyjne to dopiero początek – dziś jeszcze nie do końca wiemy, jak nasze dane będą wykorzystywane w przyszłości!

Czy można zminimalizować swój cyfrowy ślad? Tak! Przede wszystkim bądźcie uważni w mediach społecznościowych – dostosujcie ustawienia prywatności i rozważnie dzielcie się treściami w internecie. Dodatkowo używajcie trybu prywatnego (incognito, In Private) w przeglądarkach, dzięki czemu uchronicie się przed zapisywaniem Waszej historii przeglądania, danych w formularzach czy tzw. ciasteczek. Pamiętajcie też o regularnych porządkach – pozbywajcie się nieużywanych kont czy adresów e-mail oraz sprawdźcie, czy aplikacje, z których korzystacie, nie mają dostępu do zbyt wielu Waszych danych.

Chcecie dowiedzieć się więcej o cyfrowym śladzie i ochronie swojego wizerunku online? Sięgniecie do aktualności na stronach ose.gov.pl i OSE IT Szkoła: „Letnia Akademia OSE 2022: wizerunek online i cyfrowy ślad” i „Bezpieczni w sieci z OSE na wakacje: wizerunek online i cyfrowy ślad” oraz publikacji Dyżurnet.pl „Cyfrowy ślad małego dziecka”.

Dane osobowe

Zgodnie z definicją Komisji Europejskiej dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania żyjącej osoby fizycznej. Skomplikowane, prawda? Mówiąc prościej, to m.in. imię i nazwisko, adres zamieszkania, adres e-mail – taki jak imię.nazwisko@firma.com, numer dowodu tożsamości czy dane geolokalizcyjne (np. ustawienia lokalizacji w telefonie komórkowym) i adres IP.

Naszymi danymi osobowymi, niestety, coraz częściej interesują się cyberprzestępcy. Dlatego trzeba je szczególnie chronić – zwłaszcza w internecie. Jak możecie to zrobić? Pierwsza i najlepsza rada: bądźcie czujni. Zwracajcie uwagę na otrzymywane SMS-y czy e-maile. Cyberprzestępcy wykorzystują takie wiadomości m.in. do ataku phishingowego, którego celem może być wyłudzenie nie tylko danych osobowych, ale i np. danych dostępowych do bankowości elektronicznej. Kradzież danych bywa dotkliwsza niż utrata rzeczy materialnych!

Więcej informacji o phishingu znajdziecie w aktualności „Bezpieczni w sieci z OSE: phishing" na stronie ose.gov.pl.

DDoS (Distributed Denial of Service)

Ataki typu DDoS (z ang. rozproszona odmowa usługi) to jedne z najczęstszych ataków na systemy komputerowe lub usługi sieciowe. Najprościej rzecz ujmując, ich celem jest zajęcie wszystkich dostępnych i wolnych zasobów komputera. Takie działanie cyberprzestępców ma uniemożliwić korzystanie z urządzenia i dostępnych na nim zasobów, a co za tym idzie – blokować funkcjonowanie usługi online (np. strony internetowej czy poczty e-mail znajdującej się na hostingu).

Ataki DDoS przeprowadzane są z wielu miejsc jednocześnie, czyli z wielu komputerów, nad którymi kontrolę przejęło specjalne oprogramowanie, takie jak boty czy trojany. Bywa, że właściciele tych komputerów nie wiedzą, że ich urządzenie podłączone do sieci jest wykorzystywane do przeprowadzenia ataku. Warto wiedzieć, że atak DDoS rozpoczyna się, gdy przejęte przez przestępców urządzenia jednocześnie atakują daną usługę lub system. Cel ataku jest wówczas zasypywany fałszywymi żądaniami – np. wywołania danej strony internetowej.

Zastanawiacie się, jak chronić się przed atakami tego typu? Najlepszą obroną jest regularne aktualizowanie programu antywirusowego. Można korzystać też ze specjalnego oprogramowania, które filtruje ruch sieciowy noszący znamiona ataku DDoS.

Deepfake

Dotychczas bywaliśmy nieufni wobec zdjęć, które w obecnych czasach łatwo przecież przerobić, a więc zmanipulować. Niestety to samo dotyczy też… filmów. Być może spotkaliście się już w sieci ze sfabrykowanymi nagraniami, stworzonymi przy użyciu prawdziwych próbek głosu, wideo i zdjęć. Film z udziałem znanego polityka lub celebryty zawierający nieprawdziwe, niewiarygodne informacje? Uwaga, to może być deepfake!

Sama nazwa tego zjawiska powstała z połączenia dwóch słów: *deep* (odnoszącego się do *deep learningu*, czyli systemów głębokiego uczenia maszynowego) oraz *fake* (czyli fałsz). Jest to technika obróbki obrazu, która korzysta z rozwiązań sztucznej inteligencji (SI): algorytm na podstawie realnych danych tworzy łudząco prawdopodobny, jednak zmanipulowany materiał. Co więcej, takie filmy działają zwykle na niekorzyść rzekomo występujących w nich osób, mogą być zatem wykorzystywane np. jako element walki politycznej.

Jak rozpoznać deepfake? Przede wszystkim spróbujcie ocenić, czy ruch warg bohatera filmiku jest zgodny ze słyszanymi słowami i czy postać nie wygląda dziwnie (może ma nienaturalny odcień skóry, nie mruga albo przyjmuje nietypowe pozy?). Zwróćcie też uwagę na jakość nagrania – w deepfake'ach mamy do czynienia zwykle ze słabszą ścieżką dźwiękową i innymi błędami, które świadczą o amatorskim poziomie produkcji, np. migotaniem twarzy czy przebijaniem się oryginalnego obrazu.

Szczegółowych informacji o zmanipulowanych filmach szukajcie w aktualności „Czy to nagranie może kłamać? Uwaga na deepfake!" na stronie ose.gov.pl.

Dezinformacja

Dezinformacji, podobnie jak fake newsom i propagandzie, przyświeca jeden cel: szerzenie nieprawdziwych i zmanipulowanych wiadomości. Dezinformacja to forma przekazu, bazująca na różnego rodzaju fałszywych dokumentach, które wprowadzają odbiorców w błąd, a dodatkowo skłaniają ich do podejmowania określonych działań.

Dezinformacja celowo destabilizuje sytuację w państwie, a także wywiera destrukcyjny wpływ na obywateli. Takie kroki mają wywołać niepewność lub wrogość oraz podsycać negatywne emocje, mimo że pozornie wydają się spontaniczne.

Pamiętajcie: dezinformacja karmi się naszymi lękami i uprzedzeniami. Ci, którzy rozprzestrzeniają fałszywe wiadomości, grają na emocjach, wiedzą, że uwagę odbiorców przykuwają szokujące nagłówki i złe informacje. Zależy im, żeby te treści jak najszybciej dotarły do jak największej liczby osób. Zastanówcie się więc dwa razy, zanim udostępnicie w sieci niesprawdzony news!

Jak rozpoznać dezinformację? Przede wszystkim nie wierzcie we wszystko, co przeczytacie w internecie, nawet jeśli szokujący news udostępnił Wam ktoś znajomy. Potwierdzajcie informacje w agencjach fact-checkingowych, sprawdzajcie profile #WłączWeryfikację prowadzone przez NASK, a przede wszystkim – korzystajcie z rzetelnych źródeł. Warto reagować, gdy widzicie fałszywe wiadomości w sieci, np. przesyłać je na adres: informacje@nask.pl.

Pomocne informacje znajdziecie w aktualności „Jak nie wpaść w pułapkę fake newsów" na stronie ose.gov.pl, w pakiecie materiałów dotyczących fałszywych wiadomości: ulotce „Fake newsy, bańki informacyjne, teorie spiskowe", konspekcie zajęć „Fake newsy i dezinformacja – o tym warto porozmawiać w szkole" i grafice „Jak rozpoznać fake newsa?" dostępnym na platformie OSE IT Szkoła oraz publikacji „Kodeks dobrych praktyk" opracowanej przez NASK razem z 11 innymi organizacjami i instytucjami.

Doomsurfing

Czy zwróciliście kiedyś uwagę, jakie treści śledzicie w internecie z największym zainteresowaniem? Okazuje się, że często poświęcamy nadmierną uwagę na przyswajanie negatywnych, niepokojących wiadomości z mediów, ciągłe scrollowanie serwisów internetowych czy mediów społecznościowych w poszukiwaniu katastroficznych informacji, teorii spiskowych, negatywnych relacji. To zjawisko to doomsurfing. Termin pochodzi od dwóch angielskich słów: *doom*, oznaczającego fatum, oraz *surfing*, czyli przeglądanie sieci.

Doomsurfing nasila się zwłaszcza podczas ważnych, krytycznych wydarzeń – mogliśmy zetknąć się z nim np. podczas pandemii, gdy na bieżąco śledziliśmy informacje o liczbach zachorowań i zgonów na COVID, czy po wybuchu wojny w Ukrainie, gdy większość z nas zaczynała dzień od sprawdzenia aktualnych doniesień. Niestety okazuje się, że nałogowe przeczesywanie sieci w poszukiwaniu najświeższych newsów nie przynosi ulgi i nie daje odpowiedzi na nurtujące nas pytania, a jedynie może wywołać poczucie lęku, bezradności czy nawet stany depresyjne.

Warto uświadomić sobie, że w tym przypadku mniej znaczy więcej. Spróbujcie wybrać jedno lub dwa rzetelne źródła wiadomości i kontrolujcie czas spędzany na scrollowaniu. W ograniczaniu liczby przyswajanych informacji niestety nie pomoże Wam technologia – algorytmy będą bowiem podsuwać kolejne podobne treści (bańka informacyjna), nierzadko niestety fałszywe lub sfabrykowane przez internetowych trolli. Przed powodzią złych wiadomości uchroni Was szukanie pozytywnych newsów, niezwiązanych z niepokojącym wydarzeniem, a także… odnalezienie alternatywnych sposobów spędzania czasu – najlepiej offline.

Więcej informacji o doomsurfingu znajdziecie w aktualności „Doomsurfing – jak wyrwać się z błędnego koła śledzenia złych informacji" na stronie ose.gov.pl.

Doxing

Niemal każdego dnia zostawiamy w sieci cyfrowy ślad: zamieszczając materiały w mediach społecznościowych, publikując komentarze na forach lub po prostu przeglądając konkretne strony. Ale czy wiecie, że z okruchów informacji porozrzucanych w sieci ktoś może stworzyć zbiór danych na Wasz temat, a następnie opublikować online wszystkie wiadomości – najczęściej te wpływające na bezpieczeństwo i wizerunek?

Takie działanie to doxing (znane też jako doxxing, doksing). Dokładnie oznacza śledzenie i gromadzenie informacji w sieci na temat określonej osoby lub organizacji w celu analizy zebranych danych, a następnie ich upublicznienia. Termin ten powstał z połączenia skrótu *dox (docs)*, utworzonego od angielskiego słowa *documents* (dokumenty), oraz *compiling/releasing* (przetwarzać, upubliczniać). Czy doxing może być niebezpieczny? W niektórych przypadkach nawet bardzo!

Doxer szuka wstydliwych zdjęć lub filmików, kontrowersyjnych wypowiedzi, danych osobowych i wrażliwych. W tym celu wciela się w cyfrowego detektywa, który legalnie uzyskuje informacje z sieci, ale też w cyberprzestępcę wykorzystującego oprogramowanie szpiegujące bądź socjotechnikę, by zmanipulować ofiarę i uzyskać interesujące go dane.

Przed doxingiem trzeba się bronić. Zanim wrzucicie coś do sieci – zastanówcie się, jak to wpłynie na Wasz wizerunek. Warto też zadbać o swoją prywatność w internecie: na portalach społecznościowych ustawiajcie profil prywatny zamiast publicznego, nie publikujcie zdjęć, z których można pozyskać istotne dane – biletów lotniczych, dokumentów tożsamości czy kart kredytowych (nawet ich fragmentów). Bądźcie wyczuleni na phishing i wszelkie próby wyłudzenia danych osobowych czy uwierzytelniających. Jeśli w sieci znajdują się dotyczące Was treści – nieaktualne, nieistotne lub takie, które naruszają Wasz wizerunek – skorzystajcie z prawa do bycia zapomnianym które wynika z rozporządzenia unijnego RODO.

Więcej przydatnych informacji znajdziecie na stronie ose.gov.pl w aktualności „Bezpieczni w sieci z OSE: doxing”.

Dyżurnet.pl

Internet otwiera nam okno na świat, w sieci możemy uczyć się, rozwijać, kontaktować z ludźmi z całego świata. Jednak co wtedy, gdy online spotka nas – lub nasze dzieci czy uczniów – coś nieprzyjemnego, np. natkniemy się na treści, których nie chcieliśmy zobaczyć? W takich przypadkach pomocą służy Dyżurnet.pl. To zespół ekspertów NASK działający jako punkt kontaktowy do zgłaszania nielegalnych treści w internecie, szczególnie związanych z seksualnym wykorzystywaniem dzieci.
Dyżurnet.pl m.in. obsługuje linię telefoniczną i serwis internetowy, umożliwiając

zgłaszanie i analizę przypadków dystrybucji, rozpowszechniania lub przesyłania materiałów przedstawiających seksualne wykorzystywanie dzieci, w skrócie CSAM (z ang. *child sexual abuse materials*), przez internet.

Zgłoszenia o potencjalnie nielegalnych treściach możecie przekazywać za pomocą formularza, na adres mailowy dyzurnet@dyzurnet.pl lub pod numerem telefonu 801 615 005. Jeśli zgłoszona treść dotyczy materiałów przestawiających seksualne wykorzystywanie dzieci, twardej pornografii, rasizmu i ksenofobii czy innych nielegalnych treści, zespół Dyżurnet.pl podejmuje odpowiednie działania (np. zgłasza sprawę na policję). Specjaliści reagują również na szkodliwe treści, zagrażające bezpieczeństwu dzieci. W takim przypadku najczęściej kontaktują się z administratorem, który moderuje np. wskazane posty na forach.

Szczegółowych informacji o zgłaszaniu nielegalnych treści i działaniach Zespołu Dyżurnet.pl szukajcie na stronie dyzurnet.pl.

Dzień Bezpiecznego Internetu (DBI)

Czy wiecie, które daty w corocznym kalendarzu są szczególnie ważne dla bezpieczeństwa w sieci? To na pewno październik będący Europejskim Miesiącem Cyberbezpieczeństwa (ECSM), ale też pierwsza połowa lutego, gdy obchodzimy Dzień Bezpiecznego Internetu. Celem tej akcji jest inicjowanie i propagowanie działań na rzecz bezpiecznego dostępu dzieci i nastolatków do sieci, zaznajomienie rodziców, nauczycieli i wychowawców z problematyką bezpieczeństwa online, a także promocja pozytywnego wykorzystywania internetu. Dzień Bezpiecznego Internetu obchodzimy od 2004 r. z inicjatywy Komisji Europejskiej. Od lat różnorodne wydarzenia z okazji DBI organizowane są nie tylko w Europie, ale na całym świecie.

Organizatorem DBI w naszym kraju jest Polskie Centrum Programu Safer Internet (PCPSI), które jako NASK – Państwowy Instytut Badawczy tworzymy z Fundacją Dajemy Dzieciom Siłę. Centralnym punktem naszych obchodów jest doroczna konferencja z udziałem ekspertów, ale i szkół, organizacji pozarządowych czy przedstawicieli biznesu, którzy angażują się w DBI.

Więcej informacji, w tym nagrania z wystąpień ekspertów podczas konferencji, znajdziecie na stronie internetowej DBI.

E-learning

Dostęp do nowych technologii ułatwia codzienność oraz umożliwia przeniesienie wielu aspektów naszego życia do sieci. Jednym z nich jest nauka. E-learning (lub e-nauka) to edukacja przy wykorzystaniu technologii informatycznych: internetu i urządzeń cyfrowych (np. smartfona, komputera). Dzięki niemu możecie uczyć się online bez konieczności wychodzenia z domu! E-learning pozwala także na zdalne przeprowadzenie szkoleń, konferencji czy wykładów.

Platform oferujących możliwość nauki online jest wiele – jedną z nich jest dobrze Wam znana OSE IT Szkoła. Nauczyciele, uczniowie i rodzice znajdą tutaj wiele pomocnych, bezpłatnych materiałów umożliwiających naukę w dowolnym miejscu i czasie (m.in. ponad 200 kursów e-learningowych, scenariusze zajęć, publikacje ekspertów czy infografiki).

Rozpocznijcie naukę z bezpłatną platformą OSE IT Szkoła!

E-mail

Chyba każdy internauta ma przynajmniej jeden adres e-mailowy. To właśnie on pozwala nam korzystać z wielu możliwości, jakie oferuje dostęp do sieci. E-mail to poczta elektroniczna (ang. *electronic mail*), dzięki której komunikujemy się przez internet. Określenie to stosujemy też do samej wiadomości elektronicznej.

Posiadając swój osobisty adres mailowy, możecie przesyłać wiadomości i otrzymywać je od innych, odbierać newslettery czy zakładać konta w różnych mediach społecznościowych oraz sklepach internetowych. Aby korzystać z poczty elektronicznej, wystarczy urządzenie (np. komputer, smartfon) z dostępem do internetu i skrzynka, którą można założyć bezpłatnie. Ważne, by zabezpieczyć ją silnym, unikalnym hasłem, a także skorzystać z uwierzytelniania dwuskładnikowego – pozwoli to skuteczniej chronić konto przed cyberprzestępcami.

Nie zapominajcie też o czujności! Wielu oszustów wykorzystuje wiadomości elektroniczne w swoich kampaniach phishingowych. Mogą w nich podszywać się pod Waszych znajomych, zaufane instytucje czy firmy, z których usług korzystacie. Otrzymując wiadomość na wirtualną skrzynkę, zawsze bądźcie ostrożni. Uważajcie na te oznaczone jako spam, nie klikajcie w żadne podejrzane linki zawarte w ich treści i nie pobierajcie załączników – najpierw upewnijcie się, że nadawca rzeczywiście jest tym, za kogo się podaje, i nie ma złych intencji.

Co powinno wzbudzić Waszą podejrzliwość? Wiadomość napisana niepoprawnym językiem lub nakłaniająca do nieprzemyślanego i szybkiego działania, np. udostępnienia wrażliwych danych, adres zawierający błędy czy ton wypowiedzi, w którym nadawca ostrzega Was, że wydarzy się coś złego, jeśli natychmiast nie wykonacie jego polecenia.

Chcecie dowiedzieć się więcej o poczcie elektronicznej? Zajrzyjcie do kursu e-learningowego „Techniki internetu” dostępnego na naszej platformie OSE IT Szkoła oraz aktualności „Bezpieczni w sieci z OSE: poczta e-mail”, którą znajdziecie na stronie ose.gov.pl.

Exploit

Uwaga! To kolejne niebezpieczeństwo, na jakie możecie być narażeni jako użytkownicy nowych technologii! Exploit to program wykorzystujący istniejące błędy w oprogramowaniu. Cyberprzestępca poprzez lukę przejmuje kontrolę nad urządzeniem lub zmusza je do wykonania żądanej przez niego operacji. Aby uchronić się przed konsekwencjami zainfekowania exploit, należy m.in. korzystać z legalnych programów i oprogramowania antywirusowego, warto też pamiętać, by nie klikać w podejrzane linki.

Emotikon

Z pewnością dobrze znacie emotikony (nazywane też emotkami) i chętnie wykorzystujecie je w internetowych konwersacjach. To znak, za pomocą którego możecie wyrażać w internecie swoje emocje, np. radość, złość, smutek, zdziwienie czy miłość. Najpopularniejszym emotikonem jest uśmiechnięta buźka „:)”. Netykieta – czyli zbiór zasad dotyczących dobrych zachowań w internecie – podpowiada, że buźki i inne sympatyczne emotikony powinny być jedynie ozdobnikami i dodatkami do naszych wiadomości, a nie ich głównym elementem. Pamiętajcie o tym podczas wirtualnych rozmów czy zamieszczania komentarzy w sieci.

Więcej na temat netykiety i emotikonów dowiecie się z czwartego modułu kursu e-learningowego „Przygody Profesora i N@tki, czyli jak mądrze korzystać z internetu”, który znajdziecie na platformie OSE IT Szkoła, oraz aktualności „Jak zrozumieć dziecko w sieci?” na ose.gov.pl.

Europejski Miesiąc Cyberbezpieczeństwa (ECSM)

To trwająca przez cały październik inicjatywa organizowana przez Europejską Agencję ds. Cyberbezpieczeństwa (ENISA) oraz Komisję Europejską. Głównym celem kampanii ECSM jest popularyzacja wiedzy, zwiększanie świadomości i wymiana dobrych praktyk w obszarze cyberbezpieczeństwa wśród szerokiej grupy użytkowników internetu, profesjonalistów czy osób zajmujących się edukacją oraz profilaktyką dzieci i młodzieży. Co roku w całej Europie organizowane są warsztaty, konferencje, kampanie i różne inicjatywy mające udowodnić, że „Cyberbezpieczeństwo to nasza wspólna odpowiedzialność”. W Polsce kampanię koordynuje NASK – Państwowy Instytut Badawczy. Pamiętajcie, że udział w różnych wydarzeniach może wziąć każdy, a także… sami możecie zorganizować własną inicjatywę.

Więcej o Europejskim Miesiącu Cyberbezpieczeństwa dowiecie się ze strony bezpiecznymiesiac.pl.

Fact-checking

To angielski termin, który oznacza proces weryfikacji faktów w celu dokładnego sprawdzenia wiarygodności informacji. Może nie wiecie, ale są osoby, które dbają o prawdziwość przekazywanych informacji. Fact-checkerzy docierają do danych, statystyk, dokumentów źródłowych, merytorycznych analiz, wypowiedzi specjalistów z określonej dziedziny, by zweryfikować treści pojawiające się w mediach i internecie. Wykorzystują też różne narzędzia, umożliwiające np. zbadanie autentyczności filmów czy zdjęć. Organizacje fact-checkingowe walczą z dezinformacją, szkodliwą narracją, budują świadomość społeczną. To szczególnie ważne zadanie w dobie rozwoju internetu i mediów społecznościowych, za pomocą których bardzo łatwo rozprzestrzeniane są fake newsy, czyli fałszywe informacje.

Fake news

Nie jest tajemnicą, że internet to skarbnica wiedzy, ale też źródło fałszywych wiadomości, często o sensacyjnym, szokującym charakterze. Popularne, a zarazem szkodliwe fake newsy przyciągają uwagę krzykliwymi nagłówkami i emocjonalnym językiem, co sprawia, że czytamy je chętnie i równie chętnie się nimi dzielimy – np. w mediach społecznościowych. Ale czy wiecie, że fałszywe wiadomości najczęściej mają za zadanie manipulować, dezinformować, wprowadzać odbiorców w błąd? Fake newsy niejednokrotnie są też narzędziem do przeprowadzenia ataków phishingowych. Zawarte w nich linki mogą Was przekierowywać do fałszywych witryn internetowych, których celem jest wyłudzenie Waszych danych lub kradzież środków finansowych.

Więcej wiadomości o fake newsach i dezinformacji znajdziecie na stronie ose.gov.pl w aktualności „Jak nie wpaść w pułapkę fake newsów?”.

Fałszywe domeny

Oszuści stosują różne metody, aby wyłudzić od internautów dane osobowe, dane uwierzytelniające do kont bankowych lub serwisów społecznościowych. Jedną z nich jest tworzenie stron internetowych podszywających się pod znane podmioty, firmy i instytucje. Co je odróżnia? Zazwyczaj niewiele – może to być błąd w nazwie strony, np. cyfra „0” zamiast litery „O”.

Bądźcie czujni, bardzo łatwo jest wpaść w sidła przestępców i przez nieuwagę zalogować się w oknie fałszywej strony banku, bramce płatności internetowej czy witrynie instytucji łudząco podobnej do tej prawdziwej. Dlatego zawsze zwracajcie szczególną uwagę na to, w co klikacie i gdzie wpisujecie swoje hasła i loginy!

Jeśli traficie na taką fałszywą stronę, warto to zgłosić do CERT Polska. Wystarczy wypełnić formularz dostępny na CERT.PL – zgłoś incydent.

Możecie też przesłać wiadomość SMS zawierającą potencjalnie groźny link. W tym celu skorzystajcie z funkcji „przekaż" albo „udostępnij" i wyślijcie wiadomość na numer 799 448 084. Eksperci NASK przyjmą i przeanalizują każde zgłoszenie, a podejrzaną domenę zamieszczą na liście ostrzeżeń przed niebezpiecznymi stronami.

Filtry kontroli rodzicielskiej

W budowaniu zdrowych nawyków cyfrowych dziecka ważna jest rozmowa na temat bezpieczeństwa w sieci. Wsparciem dla rodziców są też rozwiązania technologiczne, które pomagają minimalizować ryzyko kontaktu najmłodszych z niebezpiecznymi materiałami online. Filtry kontroli rodzicielskiej to właśnie oprogramowanie, które ogranicza dzieciom dostęp do szkodliwych lub nieodpowiednich do ich wieku treści.

Jednym z takich narzędzi jest stworzona w ramach Ogólnopolskiej Sieci Edukacyjnej (OSE) bezpłatna aplikacja ochrony rodzicielskiej – mOchrona. Ułatwia ona ustalenie zasad dotyczących korzystania z internetu i różnych aplikacji oraz daje rodzicom dostęp do informacji o aktywności dziecka na jego urządzeniu. Jeśli jeszcze nie korzystacie z tego narzędzia, koniecznie pobierzcie je bezpłatnie na urządzenia mobilne z oficjalnych sklepów z aplikacjami, a także w wersji dla systemu Windows.

Więcej informacji o naszej apce znajdziecie na stronie ose.gov.pl: w zakładce mOchrona i wywiadzie „5 pytań o... aplikację mOchrona".

Firewall

Inaczej zapora sieciowa (lub ogniowa). To bardzo ważne urządzenie lub oprogramowanie zabezpieczające sieć. Można powiedzieć, że jest to pierwsza linia obrony przed zagrożeniami płynącymi z internetu. Jak działa firewall? Filtruje zarówno dane sieciowe przychodzące, jak i wychodzące z urządzeń cyfrowych. W ten sposób zapora uniemożliwia intruzom nieautoryzowany dostęp do zasobów Waszego komputera.

Flaming

Byliście świadkiem żarliwej dyskusji na forach lub w mediach społecznościowych? Jeśli tak, prawdopodobnie mieliście okazję zaobserwować, jak działa flaming, czyli celowe „zaognianie" (od ang. *flame* – płomień) rozmowy w sieci. Flamerzy inicjują internetowe kłótnie, podczas których uszczypliwości szybko przeradzają się w konflikt przesycony wulgaryzmami, obelgami, a nawet groźbami. W takiej dyskusji merytoryczne argumenty schodzą na dalszy plan, a próba przedstawienia flamerowi faktów zazwyczaj kończy się niepowodzeniem.

Flaming to przykład łamania zasad netykiety. Internetowe kłótnie i wszelkie przejawy „wojny na obelgi" powinniście zgłaszać moderatorom – w celu ich usunięcia.

Więcej o zasadach netykiety przeczytacie w aktualności na portalu OSE IT Szkoła „Nie krzycz w internecie, czyli ściągawka z netykiety”.

Flooding

Zdarzyło Wam się dostać wiele niepotrzebnych, a może identycznych, pustych lub celowo zniekształconych wiadomości e-mail lub SMS w krótkim odstępie czasu? A może irytowały Was powtarzające się komentarze albo ciągi znaków na forach internetowych? To tzw. flooding (od ang. *flood* – powódź), czyli atak spamerski ukierunkowany na jednego odbiorcę.

Z floodingiem spotkacie się zazwyczaj w mediach społecznościowych, na czatach i w różnego rodzaju komunikatorach. Może on przybrać formę np. tej samej wiadomości publikowanej w ramach jednej dyskusji lub grupy na forum albo wielokrotnie pojawiającego się komentarza na YouTube z prośbą o subskrypcję danego kanału. Ten typ floodingu jest najczęściej wynikiem nieznajomości zasad netykiety albo niedbałego posługiwania się językiem.

Bardziej szkodliwy jest flooding stosowany celowo, prowadzący do zablokowania usługi, w obrębie której wielokrotnie wysyłane są pakiety identycznych danych. Hakerzy wykorzystują ten mechanizm w atakach typu DoS (ang. *Denial of Service*), uniemożliwiając działanie danego systemu lub usługi komputerowej.

Na flooding narażeni są również użytkownicy telefonów komórkowych i poczty elektronicznej. Skrzynki „zalewane” są wówczas dużą liczbą zbędnych wiadomości – mamy do czynienia z bombą pocztową (ang. *mail bobming*). Na szczęście tego typu ataki towarzyszą nam coraz rzadziej: zarówno komunikatory pocztowe, jak i smartfony wyposażane są obecnie w skuteczne filtry antyfloodowe, które blokują niechciane wiadomości.

Zastanawiacie się pewnie, czym flooding różni się od spamu. W przypadku floodingu mamy do czynienia z jednym odbiorcą niechcianych bądź niezamawianych wiadomości, z kolei spam polega na masowej wysyłce takich treści do wielu osób jednocześnie.

FOMO

Nie możecie wytrzymać nawet chwili bez smartfona? To może być objaw FOMO (od ang. *Fear of Missing Out*), czyli lęku przed odłączeniem, wypadnięciem z obiegu, kiedy akurat nie jesteście online.

Osoby doświadczające FOMO są rozdrażnione, skarżą się na poczucie pustki i nudę, a nawet wpadają w panikę czy reagują agresją, gdy nie mają dostępu do sieci i mediów społecznościowych. Ukojenie przynosi obecność smartfona oraz takie proste czynności jak odblokowywanie urządzenia czy bezwiedne scrollowanie postów. FOMO może dotknąć każdego, niezależnie od wieku, ale badania pokazują, że to nastolatki są na nie szczególnie narażone. Pamiętajcie,

że FOMO może doprowadzić do nadużywania nowych technologii i zwiększać ryzyko uzależnienia (ZUI).

Więcej informacji na temat FOMO znajdziecie na ose.gov.pl w aktualności „Temat lekcji: FOMO i problemowe używanie internetu wśród uczniów" oraz wywiadzie „5 pytań o... FOMO i problemowe używanie internetu". Skorzystajcie też z naszego bezpłatnego kursu e-learningowego „Zrozumieć FOMO" na platformie OSE IT Szkoła, adresowanego do nauczycieli i rodziców.

F

Fonoholizm

Telefon ułatwia życie – to pewne! Ale czy wiecie, że za jego sprawą niepostrzeżenie możecie wpaść w pułapkę uzależnienia? Wszystko przez to, że współczesne smartfony, oprócz możliwości wykonywania połączeń, oferują też szereg funkcjonalności, a przede wszystkim ułatwiają dostęp do sieci – o każdej porze i praktycznie z każdego miejsca.

Fonoholizm to nałogowe używanie telefonu komórkowego, które niesie za sobą wiele negatywnych konsekwencji dla zdrowia i funkcjonowania. Problemy ze snem i koncentracją, przemęczenie, izolowanie się od innych, a nawet depresja – to skutki braku kontroli nad czasem, jaki poświęcamy na korzystanie z urządzenia. Walka z uzależnieniem polega na podjęciu długofalowych działań.

Jeśli wpadliście w sidła fonoholizmu, koniecznie skorzystajcie z rad specjalisty, który pomoże Wam zmierzyć się z problemem i wskaże, jak mądrze wdrażać zdrowe cyfrowe nawyki.

Na stronie ose.gov.pl w aktualności „Niebieski Poniedziałek – zadbajmy o zdrowie psychiczne dzieci" przypominamy, gdzie znajdziecie wsparcie w przypadku wystąpienia sytuacji kryzysowej.

Gaming

Czyli najprościej rzecz ujmując: granie (w gry). To nie tylko sposób na nudę i spędzanie wolnego czasu, ale też rozrywka, która może przerodzić się w prawdziwą pasję – wiedzą o tym szczególnie młodzi amatorzy nowych technologii.

Gry komputerowe – strategiczne, fabularne, przygodowe, zręcznościowe, sportowe, symulacyjne, logiczne czy edukacyjne – niejednokrotnie wspomagają rozwój dziecka. Gra odpowiednio dobrana do wieku i możliwości uczy praktycznych umiejętności i działania w grupie, rozwija zainteresowania, wzmacnia kompetencje społeczne, a nawet pomaga zawierać przyjaźnie. Musicie jednak pamiętać o zagrożeniach wynikających z gamingu. Cyfrowa rozrywka potrafi angażować na długie godziny, co może prowadzić do nadużywania nowych technologii, a nawet uzależnienia od gier komputerowych.

Więcej informacji o pozytywnych i negatywnych skutkach gamingu znajdziecie w poradniku dla rodziców „Nastolatki i gry cyfrowe" dostępnym na platformie OSE IT Szkoła.

Generator hasła

Jeszcze do niedawna częstą praktyką tworzenia silnych i bezpiecznych haseł było stosowanie ciągu znaków niezwiązanych ze sobą znaczeniowo, ale na pierwszy rzut oka tworzących niemożliwy do złamania szyfr. Na takie hasło składały się małe i duże litery, a także cyfry oraz znaki specjalne, np. mx6t6Y8IsKWaYoo. Generatory hasła służą właśnie do tworzenia losowych kombinacji różnych znaków, co ma nam dać silne zabezpieczenie. I choć wiele portali stosuje jeszcze takie wymagania przy tworzeniu zabezpieczeń, to nowe rekomendacje CERT Polska w tym zakresie zwracają uwagę przede wszystkim na długość hasła.

Wasz szyfr powinien składać się z minimum 12 znaków. Ale to nie wszystko. Warto, by tworzyła go fraza łatwa do zapamiętania, ale trudna do złamania, czyli nie do końca oczywista. Sprawdzi się znany Wam cytat, ale po znacznych modyfikacjach, np. WlazlKostekNaMostekIStuka! Co ciekawe – administratorzy i projektanci systemów informatycznych, tworząc system uwierzytelniania użytkownika, nie powinni wymagać od Was dodatkowych kryteriów złożoności, np. znaków specjalnych, cyfr czy dużych liter. Czy zatem popularne generatory hasła przejdą do lamusa?

Aktualne rekomendacje dotyczące tworzenia silnych i bezpiecznych haseł znajdziecie na stronie ose.gov.pl w aktualności „Bezpieczni w sieci z OSE: bezpieczne logowanie".

Geolokalizacja

Czy wiecie, że wiele platform i aplikacji zbiera dane na temat Waszej aktualnej lokalizacji? Geolokalizacja to nic innego, jak określanie położenia geograficznego urządzenia podłączonego do sieci. W ustaleniu miejsca Waszego pobytu pomaga wiele narzędzi, choć nie zawsze zdajecie sobie sprawę z tego, że akurat w danym momencie jesteście „namierzani".

Położenie określane jest na podstawie włączonej funkcji udostępniania lokalizacji i adresu IP. Dzięki temu po wpisaniu w wyszukiwarkę zapytania o wyznaczenie trasy lub wskazanie interesującego Was obiektu otrzymacie precyzyjną informację, gdzie znajduje się najbliższa kawiarnia lub kino, a nawet jaka jest pogoda w danym miejscu!

Warto pamiętać, by nie wpaść w pułapkę zbyt łatwej dostępności serwisów społecznościowych, gier mobilnych czy aplikacji. Zanim zainstalujecie takie narzędzie na smartfonie, dokładnie przeczytajcie regulamin i politykę prywatności. Sprawdźcie, na co wyrażacie zgodę. Zastanówcie się, czy uzasadnione jest żądanie dostępu do aparatu, zdjęć, filmów, kontaktów, wiadomości, kamery lub właśnie geolokalizacji. Ulubiona gra lub apka może zbierać i przekazywać zbyt wiele wiadomości o Was, co ma wpływ na Wasze bezpieczeństwo.

Więcej o zasadach korzystania z aplikacji przeczytacie na ose.gov.pl w aktualności „Bezpieczni w sieci z OSE: aplikacje mobilne".

Gray hat

Kim jest osoba w szarym kapeluszu? Takim mianem określa się członka społeczności hakerskiej, czyli kogoś, kto odznacza się dużymi umiejętnościami informatycznymi. Gray hats działają jednak na krawędzi prawa, choć w przeciwieństwie do black hats (czarnych kapeluszy) – w dobrej wierze. Włamują się do systemów komputerowych lub sieci, by zlokalizować luki i błędy, a następnie pozyskane informacje zgłaszają zainteresowanym stronom. Dzięki temu możliwe jest zlikwidowanie potencjalnego zagrożenia.

Pomiędzy szarym i czarnym oczywiście jest jeszcze biały. White hats (białe kapelusze) to prawdziwi cyfrowi dżentelmeni. Zastanawiacie się pewnie, co ich odróżnia od gray hats? Białe kapelusze również tropią podatności oprogramowania na ataki i błędy w aplikacjach, ale robią to zgodnie z prawem. Potencjalne luki zgłaszają administratorom systemów, producentom oprogramowania czy zespołom reagowania na incydenty bezpieczeństwa – CSIRT oraz CERT. Ważna jest dla nich satysfakcja z możliwości uczestniczenia w procesie usuwania błędów, które mogą zagrażać bezpieczeństwu użytkowników.

Grooming (child grooming)

Pod tym pojęciem kryje się uwodzenie dziecka w internecie. W wielu przypadkach to długotrwały proces, podczas którego sprawca zaprzyjaźnia się

z osobą małoletnią, zdobywa jej zaufanie, buduje więź emocjonalną. Taka relacja zazwyczaj nie kończy się dobrze: zmierza do wykorzystania dziecka w świecie realnym lub produkcji nielegalnych treści z jego udziałem. Pamiętajcie, że child grooming jest przestępstwem, które należy zgłosić na policję! Dziecko, które doświadczyło uwodzenia w sieci, należy otoczyć szczególną opieką – stworzyć warunki do szczerej, wspierającej rozmowy. W wielu przypadkach wymagana jest pomoc specjalisty.

Nielegalne treści w sieci, szczególnie związane z seksualnym wykorzystywaniem dzieci, zgłaszajcie na policję lub do zespołu Dyżurnet.pl. Koniecznie porozmawiajcie też ze swoim dzieckiem o zagrożeniach związanych z zawieraniem nowych znajomości w internecie.

Rodziców i nauczycieli zachęcamy do skorzystania z materiałów z cyklu „Bądź z innej bajki" dostępnych na stronie gov.pl: animacji, podcastu oraz broszury omawiających zagadnienie groomingu. Pedagogom polecamy również powiązany tematycznie z animacją scenariusz lekcji „Złapani w sieć. Złota Rybka i niebezpieczne kontakty online", zamieszczony na platformie OSE IT Szkoła.

Haker

Zapewne na hasło haker myślicie – złodziej, przestępca. Nic dziwnego. W powszechnej opinii utarło się, że haker to cyberprzestępca, który wykorzystuje błędy, luki i złośliwe oprogramowanie (malware), by przeprowadzić atak. I choć jest to osoba wykazująca się bardzo dużymi umiejętnościami informatycznymi, dobrze znająca języki programowania i systemy operacyjne, przed którą internet nie ma żadnych tajemnic, nie oznacza to, że działa niezgodnie z prawem. Jeśli chcecie być precyzyjni, powinniście odróżnić hakera od crackera. Brzmi podobnie?

Członkowie społeczności hakerskiej, znani jako white hats (białe kapelusze), to grupa pasjonatów informatyki, programistów, wysoko wyspecjalizowanych ekspertów, którzy szukają podatności systemów komputerowych, ale robią to zgodnie z prawem – na wyraźne polecenie i za zgodą administratorów. Co więcej, hakerzy są poszukiwani szczególnie przez duże koncerny czy agencje rządowe, by chronić nas przed crackerami – black hats (czarnymi kapeluszami), którzy w przeciwieństwie do cyfrowych dżentelmenów swoje umiejętności wykorzystują do działań przestępczych.

Haktywista

Jeśli powiemy, że grupa Anonymous jest przykładem haktywistów, chyba nie będziecie mieli wątpliwości, co oznacza to pojęcie, które powstało z połączenia dwóch angielskich słów: *hacking* – hakowanie i *activism* – aktywizm.

Haktywiści, używając komputerów, sieci i swoich umiejętności, działają poza prawem, ale zawsze kierują się szlachetnymi pobudkami. Walka o wolność obywateli, prawdę, dostęp do informacji, sprzeciw wobec niesprawiedliwości, dyskryminacji, złych decyzji rządzących: to motywacje anonimowych specjalistów od łamania wszelkich zabezpieczeń. Atak na rządowe strony czy upublicznianie tajnych dokumentów – dla nich to nic trudnego. Haktywista to gray hat (szary kapelusz), czyli osoba, która potrafi działać w dobrej wierze, choć niekoniecznie zgodnie z obowiązującym prawem.

Happy slapping

Zapewne wielu z Was natknęło się w sieci na filmik, na którym przypadkowa ofiara została znienacka zaatakowana, a całe zajście nagrano, najczęściej smartfonem. Rozśmieszyć odbiorców i oczywiście zwiększyć statystyki „kliknięć” – taki cel mają twórcy „zabawnej przemocy”. Happy slapping nie ma jednak nic wspólnego z komedią, jeśli uświadomimy sobie, że to forma cyberprzemocy, której powinniśmy się stanowczo przeciwstawiać. Szczególnie że nagrania tego typu bardzo szybko rozprzestrzeniają się w sieci, a skutki agresji w internecie mogą być długofalowe i wiązać się z poważnymi problemami psychosomatycznymi, depresją, lękiem oraz obniżonym poczuciem wartości ofiary.

Chcecie wiedzieć, jak chronić dziecko przed cyberprzemocą oraz w jaki sposób reagować, gdy padnie ofiarą ataku w sieci? Zapraszamy do lektury aktualności „Temat lekcji: cyberprzemoc" dostępnej na stronie ose.gov.pl. Młodsze dzieci zachęcamy też do udziału w kursie e-learningowym na OSE IT Szkole „Owce w sieci – Zabawa w śnieżki", który przybliża problem happy slappingu.

Hasło

To nic innego jak szyfr, który chroni Wasz sprzęt przed atakiem cyberprzestępców. Silne, bezpieczne hasło to strażnik cyfrowych danych przechowywanych w różnych miejscach. Dostęp do portalu społecznościowego, bankowości elektronicznej czy skrzynki e-mail powinien być chroniony odpowiednim zabezpieczeniem. Czyli jakim?

Zasady tworzenia silnych haseł stale się zmieniają, bo też przestępcy doskonalą swoje metody działania. Ostatnie rekomendacje CERT Polska zwracają uwagę na długość hasła – minimum 12 znaków. Dobrze jest też stosować szyfry łatwe do zapamiętania, ale niemożliwe do odgadnięcia dla potencjalnych przestępców. Sprawdzi się wplatanie obcojęzycznych zwrotów we frazy, które tworzą długie hasło, np. DwaBialeLatajaceSophisticatedKroliki.

Zasady tworzenia silnych i bezpiecznych haseł znajdziecie na ose.gov.pl w aktualności „Bezpieczni w sieci z OSE: bezpieczne logowanie".

Hazard w internecie

Zapewne hazard kojarzy się Wam głównie z kasynem, ruletką, kartami i… grą na pieniądze. Powszechny dostęp do sieci sprawił, że dziś nie musimy nawet wychodzić z domu, by sprawdzić, czy Fortuna nam sprzyja. Niestety, niewinna zabawa może przerodzić się w uzależnienie. Z czym to się wiąże? Z wyczerpaniem fizycznym, emocjonalnym, a także kryzysem psychicznym.

Warto pamiętać, że hazard w sieci ma niejedno oblicze. Stykają się z nim już najmłodsi pasjonaci gier komputerowych (gaming), w które „zaszywane" są elementy hazardowe. Przykładem mogą być lootboxy (skrzynki z łupem), czyli artefakty oferujące losową zawartość, która może zwiększyć szansę na lepszy wynik, ale też wywołać dreszczyk emocji. Na zakupie jednej skrzynki zazwyczaj się nie kończy, a mikropłatności szybko potrafią wymknąć się graczowi spod kontroli.

Jak grać bezpiecznie? Odwiedźcie portal OSE IT Szkoła. Znajdziecie tam poradnik dla rodziców „Nastolatki i gry cyfrowe", broszurę „Zagrożenia w internecie. Zapobieganie – reagowanie. Hazard online wśród młodzieży" oraz aktualność „Letnia Akademia OSE 2022: hazard online".

Hejt

Określenie hejt (od ang. *hate* – nienawidzić) na stałe weszło do naszego słownika. Oznacza obrażanie, poniżanie, wyśmiewanie innych w sieci.

Negatywne, agresywne komentarze znajdziecie na forach, w mediach społecznościowych czy internetowych dyskusjach. Hejt jest jedną z form cyberprzemocy, a obiektem ataku może stać się każdy.

Poczucie anonimowości w sieci sprawia, że hejter – kierowany zazdrością lub chęcią odreagowania własnych niepowodzeń – bez większej refleksji stosuje mowę nienawiści. Sprawca przemocy nie widzi skutków swoich działań i krzywdy, którą wyrządza ofierze. Tymczasem dręczenie sprawia, że osoba napiętnowana w internecie musi się zmierzyć z obniżonym poczuciem własnej wartości, stresem, a nawet stanami depresyjnymi.Pamiętajcie – treści publikowane w sieci nie giną, dotyczy to również komentarzy!

Chcecie wiedzieć, jak reagować na hejt? Wskazówki znajdziecie w poradniku „Bezpieczeństwo online w szkołach Ogólnopolskiej Sieci edukacyjnej, cz. 2”. Zachęcamy też nauczycieli do skorzystania ze scenariusza lekcji „Nie wywołuj hejtu z lasu. Czerwony Kapturek i cyberprzemoc”. Materiały te dostępne są na naszej platformie e-learningowej OSE IT Szkoła.

H

Helpline

To inaczej linia pomocowa, czyli numer telefonu, pod którym możecie uzyskać poradę specjalisty, emocjonalne wsparcie w trudnej sytuacji lub po prostu zostać wysłuchanym. Osoby w kryzysie anonimowo mogą zgłaszać się do różnych służb oraz instytucji oferujących pomoc.

Pamiętajcie, że na zdrowie psychiczne dorosłych, ale też dzieci i młodzieży, ma wpływ wiele czynników, w tym problemowe użytkowanie sieci i urządzeń cyfrowych. Do internetu przenoszą się bowiem tradycyjne problemy, takie jak hejt, agresja, przemoc rówieśnicza, wykluczanie z grona „znajomych”. Nie należy lekceważyć żadnych przejawów cyberprzemocy, a jeśli wymaga tego sytuacja – kontaktować się ze specjalistami. Podpowiadamy, gdzie możecie uzyskać rzetelną pomoc, gdy tylko poczujecie, że znaleźliście się w sytuacji bez wyjścia.

- 116 111 (116111.pl) – Bezpłatny i anonimowy telefon zaufania dla dzieci
- 116 123 – Bezpłatny kryzysowy telefon zaufania dla dorosłych
- 800 100 100 (800100100.pl) – Bezpłatny i anonimowy telefon zaufania dla rodziców i nauczycieli
- 800 70 2222 (liniawsparcia.pl) – Centrum wsparcia dla osób w stanie kryzysu psychicznego
- 800 12 12 12 (brpd.gov.pl, e-mail: rpd@brpd.gov.pl) – Telefon zaufania Rzecznika Praw Dziecka

Hotline

Na pewno każdy z Was potrzebował kiedyś uzyskać informację w sprawie danego produktu, usługi czy wydarzenia albo zgłosić jakiś incydent. W takich sytuacjach z pomocą przychodzi „gorąca linia”, czyli infolinia, znana jako hotline.

Tak działa np. przynależny do Stowarzyszenia INHOPE (*The Association of Internet Hotline Providers*) Dyżurnet.pl. To zespół ekspertów NASK, który przyjmuje zgłoszenia nielegalnych treści w internecie, szczególnie związanych z seksualnym wykorzystywaniem dzieci. Możecie je przekazać za pomocą formularza, na adres e-mailowy (dyzurnet@dyzurnet.pl) lub dzwoniąc na infolinię: 801 615 005.

W ramach Ogólnopolskiej Sieci Edukacyjnej (OSE) również działa Centrum Kontaktu, które obsługuje szkoły podłączone do szybkiego i bezpiecznego internetu OSE. Nasi specjaliści odpowiadają na wszystkie pytania dyrektorów szkół i Technicznych Reprezentantów Szkół (TRS). Wystarczy zadzwonić na infolinię OSE: +48 22 182 55 55 czynną od poniedziałku do piątku w godzinach 7:30–16:00. Ponadto w każdą środę w godzinach 11:00–15:00 czeka na Was ekspert. Jak możecie się z nim skontaktować? Numer telefonu pozostaje bez zmian, ale dodatkowo należy wybrać cyfrę 6.

Zgłoszenia przyjmujemy także mailowo (wsparcietechniczne_ose@nask.pl) oraz przez portal Moje OSE i formularz dostępny na ose.gov.pl w zakładce Kontakt.

ID

Z tym hasłem możecie zetknąć się w sieci praktycznie każdego dnia. ID (ang. *user identifier*) to indywidualny identyfikator użytkownika zwany także loginem, dzięki któremu macie dostęp do Waszego konta (np. w bankowości internetowej, e-usługach czy grach online).

ID to określony, unikalny ciąg znaków. Co w tym przypadku oznacza unikalny? To, że np. logując się do bankowości elektronicznej jako Paweł8763XD, macie pewność, że nikt poza Wami nie korzysta z takiego samego ID. Inaczej: w danym systemie każdy użytkownik posiada swój własny indywidualny login, przypisany tylko do jego konta, i po zalogowaniu się (wpisaniu loginu i hasła) otrzymuje dostęp do określonych zasobów. Pamiętajcie, że ID często przydzielają administratorzy serwisów, natomiast hasło do konta powinno być tajne i zawsze znane jedynie jego właścicielowi!

Więcej na temat tworzenia bezpiecznych haseł dowiecie się z aktualności ose.gov.pl „Bezpieczni w sieci z OSE: bezpieczne logowanie".

Incydent bezpieczeństwa

Fałszywe strony logowania do bankowości internetowej lub mediów społecznościowych, szkodliwe treści czy podejrzane wiadomości SMS lub e-mail – te i inne niebezpieczne działania mogą doprowadzić do incydentu bezpieczeństwa komputerowego. To sytuacja, w której korzystając z internetu, możecie być narażeni na niebezpieczeństwo.

W sieci codziennie możemy stać się ofiarą różnych prób cyberataków, dlatego warto na bieżąco śledzić informacje na temat metod stosowanych przez oszustów (a tych ciągle przybywa!) oraz pamiętać o zgłaszaniu incydentów bezpieczeństwa. Jak to zrobić?

Z pomocą przychodzi CERT Polska, czyli zespół reagowania na incydenty. Aby zgłosić niebezpieczne zdarzenie, wypełnijcie formularz dostępny na stronie cert.pl, wyślijcie e-mail na adres: cert@cert.pl albo – w przypadku potencjalnie niebezpiecznej wiadomości SMS – przekażcie ją pod numer 799 448 084.

Zgłoszenia dotyczące nielegalnych treści w internecie, szczególnie związanych z seksualnym wykorzystywaniem dzieci, powinniście przesyłać do zespołu Dyżurnet.pl. W tym celu można skorzystać z formularza, wysłać wiadomość na e-mail (dyzurnet@dyzurnet.pl) lub zadzwonić na infolinię: 801 615 005. Pamiętajcie, że incydenty należy zgłaszać jak najszybciej – dzięki temu inni użytkownicy internetu będą mogli uchronić się przed zagrożeniami.

Inteligentne urządzenia

To urządzenia podłączone do globalnej sieci, posiadające często niestandardowe funkcje, które ułatwiają i usprawniają ich użytkowanie. Inteligentne urządzenia są częścią internetu rzeczy (*internet of things*, IoT).

Przykładów zastosowania inteligentnych urządzeń jest wiele. Wśród nich wymienić można dobrze Wam znane smartwatche, ale też… żarówki, lodówki, a nawet zamki w drzwiach! Pamiętajcie jednak, że każdy sprzęt podłączony do internetu wymaga odpowiedniej ochrony, np. przed zainfekowaniem malware (złośliwym oprogramowaniem). Jeśli w Waszym domu znajdują się inteligentne urządzenia, nie zapominajcie o kilku ważnych nawykach, m.in.: aktualizacjach oprogramowania, korzystaniu z bezpiecznego i silnego hasła czy podłączaniu do sieci jedynie tych urządzeń, których naprawdę potrzebujecie.

O inteligentnych urządzeniach i ich ochronie przeczytacie więcej w biuletynie „OUCH! – Inteligentne urządzenia w Twoim domu" – znajdziecie go na stronie CERT Polska.

Internet

Warto wiedzieć, że rok 1991 zapisał się szczególnie w historii internetu w Polsce. To właśnie wtedy podłączono nasz kraj do sieci, a NASK miał w tym swój znaczący udział. Z jej możliwości korzystamy dziś każdego dnia, ale czy wiemy, czym właściwie jest?

To ogólnoświatowa sieć komputerowa, która jest zbiorem wielu mniejszych sieci. W skład internetu wchodzą: serwery, routery, komputery użytkowników. Dzięki podłączeniu do sieci możecie – niezależnie od kraju i strefy czasowej – wymieniać się informacjami, komunikować, edukować na odległość (np. za pomocą e-learningu) czy korzystać z różnych e-usług. Wygodne, prawda?

Zobaczcie kurs e-learningowy „Techniki internetu" i dowiedzcie się więcej o internecie oraz możliwościach, jakie otwiera przed użytkownikami nowych technologii. Materiał znajdziecie na platformie OSE IT Szkoła.

Internet rzeczy (IoT)

Spotkaliście się kiedyś ze zwrotem internet rzeczy lub IoT (*internet of things*)? Jeśli tak, na pewno kojarzy się on Wam z nowymi technologiami. To koncepcja polegająca na tworzeniu sieci inteligentnych urządzeń wymieniających między sobą dane. Sieć łączy przewodowo lub bezprzewodowo sprzęty, które charakteryzują się autonomicznym, niewymagającym zaangażowania użytkownika działaniem, pozyskując, przetwarzając i udostępniając dane, a także pod ich wpływem wchodząc w interakcje z otoczeniem. Choć może to brzmieć trochę jak science fiction, to IoT jest coraz powszechniejszej wykorzystywany, a wśród przykładów jego zastosowania można wymienić: sprzęty medyczne, AGD i RTV, maszyny przemysłowe czy inteligentne domy.

Dowiedzcie się więcej o IoT i zorganizujcie zajęcia ze „Scenariuszem lekcji: Internet rzeczy jest wszędzie” przygotowanym w ramach programu „Przyszłość jest dziś”.

IP

Adres IP (ang. *IP address*) to unikatowy numer identyfikacyjny nadawany urządzeniom podłączonym do sieci (np. komputerom, tabletom). Jego rolę można porównać do tej, którą pełni adres na kopercie lub paczce wysyłanej tradycyjną drogą pocztową. Adres IP składa się z czterech części oddzielonych kropkami: dwie pierwsze oznaczają numer sieci, natomiast kolejne – numer komputera w tej sieci. Każdy Wasz sprzęt posiada unikalne IP, które może być przydzielone na stałe (adres statyczny) lub na określony czas (adres dynamiczny).

Więcej wiadomości na temat adresu IP znajdziecie na stronie ose.gov.pl w webinarze „Bezpieczni w sieci z OSE – Internet bez tajemnic”.

Jailbreak

Czy „ucieczka z więzienia” może mieć coś wspólnego z cyberbezpieczeństwem, w tym przypadku – bezpieczeństwem urządzenia mobilnego? Okazuje się, że tak! Jailbreak (z ang. *jail* – więzienie i *break* – złamać, ale też przerwa, luka) to bowiem usuwanie narzuconych przez producenta ograniczeń na urządzenia z danym systemem operacyjnym. Brzmi skomplikowanie? Chodzi tu o ustawienie urządzenia w trybie, który pozwala na instalację rozszerzeń do oprogramowania, modyfikowanie poszczególnych funkcji, wyglądu, a także instalację aplikacji niedostępnych dla danego systemu operacyjnego.

Niektórzy użytkownicy widzą zalety takiego działania. Trzeba jednak pamiętać, że każda ingerencja w system operacyjny wiąże się z wieloma zagrożeniami, przede wszystkim brakiem oficjalnej aktualizacji oprogramowania. Jailbreak wykorzystuje luki i może sprawić, że system Waszego urządzenia stanie się niestabilny, co zdecydowanie zwiększa ryzyko awarii i błędów w zakresie cyberbezpieczeństwa.

J

Jamming

Czy zastanawialiście się kiedyś, na czym polega łączność bezprzewodowa? Telefony komórkowe, routery Wi-Fi, nadajniki GPS, ale też radia, piloty zdalnego sterowania czy kontrolery dronów wysyłają i odbierają sygnały radiowe na różnych częstotliwościach (aby sobie wzajemnie „nie przeszkadzać”). Istnieją rozwiązania, które umożliwiają zagłuszanie tych sygnałów, a więc blokują komunikację urządzeń między nadajnikami/odbiornikami. To jamming (z ang. zagłuszanie).

Atak polega na zakłóceniu lub uniemożliwieniu odbioru transmisji. Używa się go do zablokowania pracy urządzeń sterowanych falami radiowymi, jak również do zahamowania przepływu informacji przekazywanych z wykorzystaniem tych fal. Zagłuszający emituje sygnały radiowe na tej samej częstotliwości i przy użyciu tej samej modulacji, co fala pierwotna. Najczęstszymi „zakłócaczami” są szum, pulsowanie dźwięku, muzyka lub inny program radiowy.

Co ciekawe, historia jammingu sięga już lat 20. XX w., kiedy to w Berlinie zagłuszano transmisje radiofoniczne w Radiu Komintern. Do kolejnych takich prób dochodziło podczas II wojny światowej i zimnej wojny.

JavaScript injection

JavaScript jest jedną z najpopularniejszych i najczęściej wykorzystywanych technologii tworzenia stron i aplikacji internetowych. Nadaje im interaktywności i umożliwia m.in. dynamiczne modyfikowanie zawartości czy tworzenie prostych funkcji, takich jak slidery, karuzele czy galerie zdjęć. Jak widać, JavaScript można wykorzystać do dobrych celów, jednak – niestety – także do szkodliwych działań. Jedynym z nich jest JavaScript injection. Jak działa?

To forma ataku na witrynę internetową, która polega na ulokowaniu (ang. *injection* – wstrzyknięciu) w jej treści kodu JavaScript uruchamianego po stronie użytkownika. Atakujący stronę oszust zyskuje dzięki temu wiele możliwości – jest w stanie modyfikować projekt witryny, uzyskiwać z niej informacje i manipulować parametrami (z wykorzystaniem plików cookie).

Efektem „wstrzyknięcia" kodu JavaScript może być np. wyciek poufnych informacji, istotna zmiana parametrów lub włamanie do kont użytkowników.

JOMO

Wielu z nas dotyka FOMO (ang. *Fear of Missing Out*), czyli wszechogarniający lęk przed odłączeniem, wypadnięciem z obiegu, strach przed tym, że coś może nas ominąć w sieci. Na drugim biegunie stoi JOMO (ang. *Joy of Missing Out*) – radość ze świadomego odłączenia się od internetu, ignorowania stale napływających komunikatów czy rezygnacji z ciągłego śledzenia znajomych online. JOMO pozwala cieszyć się z czasu spędzanego offline oraz nabrać dystansu do aktywności w sieci.

Jak jednak zmienić swoje cyfrowe nawyki i nauczyć się częściej odkładać smartfon na bok? Na początek przyda się na pewno metoda małych kroków. Znajdźcie ciekawą i atrakcyjną aktywność offline. Może to być nowe hobby lub coś, co już kiedyś sprawiało Wam przyjemność, np. jazda na rowerze, czytanie książek, puzzle czy podróże. Warto też nauczyć się spędzać przerwy (w pracy czy nauce) na aktywnościach innych niż przeglądanie stron internetowych oraz odciąć się od rozpraszaczy – wyłączyć dźwięki powiadomień, a nawet zainstalować specjalną aplikację, która poprzez małe nagrody zachęca do odkładania smartfona na bok.

Koniecznie spróbujcie też podjąć wyzwanie #offlinechallenge – przeżyjcie świadomie 48 godzin bez internetu. Trudne? Pewnie tak, ale gwarantujemy, że te dwa dni bez dostępu do sieci nauczą Was o sobie czegoś nowego!

Chcecie dowiedzieć się więcej o FOMO, JOMO i offline challenge? Sięgnijcie do naszych poradników „FOMO i problemowe używanie internetu", „FOMO i nadużywanie nowych technologii" i e-kursu „Zrozumieć FOMO" dostępnych na OSE IT Szkole oraz aktualności: „Urlop w wersji unplugged? Jesteśmy na tak!", „#offlinechallenge – czas na JOMO", „Majówka – cyfrowy detoks czy balans?", „W wakacje bez internetu? Podejmij wyzwanie!", „Letnia Akademia OSE 2022: offline challenge", „Bezpieczni w sieci z OSE na wakacje: offline challenge" na stronach ose.gov.pl i OSE IT Szkoła.

Keylogger

Znacie to uczucie, kiedy ktoś stoi za Waszymi plecami i podgląda, co robicie na komputerze? Szkodliwe oprogramowanie typu keylogger działa podobnie do podglądaczy – monitoruje Waszą aktywność na urządzeniu. Pojęcie to powstało z połączenia dwóch angielskich słów: *key* – klawisz oraz *logger* – rejestrator i oznacza oprogramowanie szpiegujące (spyware).

Jak dokładnie działa keylogger? Śledzi ruch ofiary na klawiaturze i przekazuje dane osobom trzecim. Choć to niejedyne zagrożenie – może też przechwytywać zrzuty ekranu, dźwięk z mikrofonu, a także rejestrować ruch kursora myszki. Tym sposobem w niepowołane ręce wpadają poufne informacje: dane logowania do bankowości elektronicznej, poczty e-mail czy serwisów społecznościowych.

Do zainfekowania może dojść poprzez otwarcie pliku z malware (złośliwym oprogramowaniem) lub w wyniku działania przestępców, którzy wykorzystują luki w zabezpieczeniach, by przeprowadzić atak. Spowolnione działanie sprzętu, zawieszanie się komputera czy pojawienie się na dysku folderu ze zrzutami ekranu, którego sami nie stworzyliście – te sygnały powinny Was zaniepokoić!

Aby uchronić się przed zainfekowaniem, pamiętajcie o aktualizacjach – także przeglądarki internetowej i oprogramowania antywirusowego. Podczas logowania stosujcie uwierzytelnianie dwuskładnikowe. Nie klikajcie w podejrzane linki, a jeśli to możliwe – korzystajcie z wirtualnej klawiatury. To aplikacja, która umożliwia wpisywanie loginów i haseł bez użycia fizycznej klawiatury.

Komunikatory internetowe

Zapewne korzystacie z nich bardzo chętnie! Nic dziwnego – narzędzia te łączą w sobie wiele funkcji. Dzięki nim możecie wysyłać wiadomości, prowadzić rozmowy – a nawet wideoczaty – przesyłać zdjęcia, linki czy lubiane przez wszystkich GIF-y.

Rosnąca popularność komunikatorów internetowych nie umknęła też uwadze cyberprzestępców. To właśnie tą drogą często rozsyłają niebezpieczne wiadomości. Mogą one trafić także do Was: z jednej strony od osoby nieznanej, co na pewno wzbudzi Wasze podejrzenia, a z drugiej – od potencjalnego znajomego. Dlaczego potencjalnego, skoro wyraźnie widać, że akurat pisze osoba, którą macie na liście kontaktów? Może się zdarzyć, że urządzenie znajomego zostało zainfekowane szkodliwym oprogramowaniem. Przejęcie kontroli nad cudzym kontem oznacza więc, że nadawca komunikatu wcale nie musi być tym, za kogo się podaje. Kliknięcie w przesłany przez oszusta link lub zalogowanie się w oknie fałszywej strony może się dla Was źle skończyć.

O czym warto pamiętać, korzystając z komunikatorów internetowych? Przede wszystkim bądźcie ostrożni i z rezerwą podchodźcie do dziwnie wyglądających wiadomości. Jeśli otrzymacie łańcuszki szczęścia, budzące wątpliwość linki czy prośby o dopłatę do paczki lub przesłanie kodu BLIK – nie reagujcie na takie komunikaty! Podejrzane wiadomości najlepiej skonsultować telefonicznie z nadawcą, jeśli to potencjalny znajomy, lub zgłosić incydent do CERT.

Pamiętajcie, jeśli zależy Wam na prywatności i bezpieczeństwie informacji, wybierajcie takie komunikatory, które nie gromadzą danych o użytkownikach oraz wykorzystują szyfrowanie typu end-to-end (inaczej E2E).

Więcej informacji znajdziecie na ose.gov.pl w aktualności „Bezpieczni w sieci z OSE: komunikatory internetowe".

Koń trojański (trojan)

To rodzaj szkodliwego oprogramowania, którego nazwa doskonale oddaje specyfikę jego działania. Konie trojańskie podszywają się pod przydatne aplikacje bądź programy, sprawiając wrażenie użytecznych. W rzeczywistości wykonują wiele szkodliwych działań: instalują backdoor czy oprogramowanie szpiegujące (spyware) lub szyfrujące dane na komputerze ofiary, tak by nie miała do nich dostępu (ransomware).

Jak możecie wpuścić trojana do systemu? Szkodliwe oprogramowanie ukrywa się najczęściej w darmowych aplikacjach pochodzących z nieznanych źródeł, grach, a nawet w cyfrowych kartkach z życzeniami. Konia trojańskiego możecie też pobrać wraz z kliknięciem w baner reklamowy lub z zainfekowanym załącznikiem, np. przesłanym w poczcie e-mail.

Pamiętajcie, przed szkodliwym oprogramowaniem ochroni Was przede wszystkim zdrowy rozsądek – nie otwierajcie e-maili od nieznanych osób, a już na pewno nie klikajcie w podejrzane linki. Ponadto pobierajcie aplikacje i pliki tylko z zaufanych źródeł. Warto też korzystać z zapory sieciowej firewall, która monitoruje przychodzące i wychodzące dane, a także z dobrego oprogramowania antywirusowego.

Kradzież danych

Taka kradzież – mimo że wirtualna – może mieć bardzo realne skutki. Cyberprzestępcy czyhają szczególnie na Wasze dane uwierzytelniające do bankowości elektronicznej, poczty e-mail, sklepów online, portali społecznościowych. Jeśli wejdą w ich posiadanie – stracicie nie tylko poczucie bezpieczeństwa, ale też posiadane środki na koncie.

Przestępcy stosują różne metody, by zdobyć poufne informacje. Rozsyłają e-maile (phishing), SMS-y (smishing) albo dzwonią (vishing), podszywając się pod znane instytucje: urzędy, banki, firmy kurierskie. Grożą np. utratą dostępu do internetowych usług, wymuszając na odbiorcy określone działanie – zazwyczaj

nalegają na podanie loginów i haseł. Cyberprzestępcy często też infekują komputer ofiary szkodliwym oprogramowaniem, by przejąć kontrolę nad cyfrowymi zasobami.

Chcecie wiedzieć, jak nie dać się oszukać? Przeczytajcie nasze aktualności na ose.gov.pl: „Bezpieczni w sieci z OSE: phishing" oraz „Uwaga, złodziej!".

Jeśli zauważyliście podejrzane domeny internetowe służące do wyłudzeń danych i środków finansowych, koniecznie zgłoście to do CERT Polska. Wystarczy wypełnić formularz online. A może przyszedł do Was dziwny SMS, np. informujący o konieczności dopłaty do paczki? Prześlijcie tę wiadomość dalej – do CSIRT NASK: 799 448 084. Każde zgłoszenie może pomóc innym ustrzec się przed kradzieżą danych!

Kradzież tożsamości

Wyobraźcie sobie, że dostajecie wezwanie do zapłaty za niezamawiane usługi, towary lub, co gorsza, monit o zaległych ratach kredytu, o którym nie mieliście pojęcia. Może się tak stać, jeśli Wasze dane osobowe – PESEL lub nr dowodu osobistego – wpadną w ręce cyberprzestępców.

Jak dochodzi do kradzieży tożsamości? Złodzieje mogą zainfekować Wasz komputer wirusami lub przesłać e-mail z próbą wyłudzenia poufnych informacji. Pamiętajcie, że oszuści niejednokrotnie też bacznie obserwują aktywność internautów w sieci. Źródłem cyberataku może być np. widoczny na opublikowanym przez Was zdjęciu dokument tożsamości czy fragment numeru karty kredytowej.

Jeśli padliście ofiarą kradzieży tożsamości, niezwłocznie powiadomcie o tym fakcie policję. Koniecznie poinformujcie też bank o podejrzanych transakcjach czy ewentualnych wnioskach kredytowych złożonych w Waszym imieniu.

Dowiedzcie się więcej o przeciwdziałaniu kradzieży tożsamości z biuletynu „OUCH! – Kradzież tożsamości – ochroń się przed nią".

Kruegerware (kruegerapps)

Znacie postać Freddy'ego Kruegera z filmu „Koszmar z ulicy Wiązów"? Do niej właśnie nawiązuje nazwa złośliwego oprogramowania – kruegerware (lub kruegerapps). Czym odróżnia się od innych wirusów komputerowych? Przede wszystkim trudno jest się go pozbyć, ponieważ może się odtworzyć nawet po usunięciu z komputera! Dzieje się tak np. przy wykorzystaniu mechanizmu odzyskiwania systemu Windows. Kruegerware zaliczany jest do niebezpiecznego oprogramowania typu malware (niszczącego zawartość komputera) i spyware (szpiegującego).

Jak się ustrzec przed tym zagrożeniem? Regularne aktualizacje systemu operacyjnego i programów na Waszym urządzeniu, a także korzystanie

z oprogramowania antywirusowego – to podstawa. Jak zawsze pamiętajcie też o zachowaniu ostrożności podczas korzystania z sieci i urządzeń cyfrowych. Zanim klikniecie w link przesłany w e-mailu lub pobierzecie pliki z sieci – zastanówcie się dwa razy. Lepiej zapobiegać niż leczyć!

LAN (Local Area Network)

Być może nie zawsze zdajemy sobie z tego sprawę, ale LAN towarzyszy nam na co dzień. Wiecie, czym jest? To lokalna sieć komputerowa – rodzaj połączenia, który umożliwia współpracę komputerów i urządzeń peryferyjnych (np. drukarek czy tablic multimedialnych) na danym obszarze, nie większym niż kilometr. Sieci o większym zasięgu noszą nazwę WAN (ang. *Wide Area Network*, rozległa sieć komputerowa).

Dobrym przykładem sieci LAN są chociażby sieci szkolne budowane w ramach Ogólnopolskiej Sieci Edukacyjnej. Taki typ połączenia stosują także bezprzewodowe drukarki, smartfony, laptopy czy inne urządzenia korzystające z jednej sieci. Można mówić o trzech typach sieci LAN: bezprzewodowej (WLAN), przewodowej i wirtualnej (VLAN). Najpopularniejszymi technologiami używanymi do budowy sieci LAN są Ethernet oraz Wi-Fi.

Aby możliwe było stworzenie sieci LAN (również w domu, gdy korzystamy z kilku urządzeń podłączonych do internetu), konieczny jest router bądź switch podłączony do gniazdka telefonicznego. Później wystarczy jedynie połączyć z nimi komputer, skonfigurować ustawienia i… gotowe!

Szczegółowe informacje o typach sieci oraz sposobach dbania o ich bezpieczeństwo znajdziecie w webinarze „Bezpieczni w sieci z OSE – Internet bez tajemnic”, w którym wzięli udział nasi eksperci techniczni. Zapraszamy do oglądania!

Likejacking

W świecie mediów społecznościowych często wiele zależy od „polubień” (ang. *like*). Lubimy zdjęcia i posty naszych znajomych, zostawiamy „lajki” też na fanpage’ach celebrytów, instytucji i miejsc. Wydawałoby się, że to po prostu miły gest, oznaka sympatii albo wyraz uznania. Okazuje się, że nie zawsze…

Bywa, że „polubienia” wykorzystywane są przez cyberoszustów, którzy chcą zwiększyć oglądalność wybranych profili, aby otrzymywać korzyści z umieszczonych tam reklam. Próbują w tym celu zainteresować jak największą liczbę internautów szokującą wiadomością lub bardzo atrakcyjnym materiałem. Ci, którzy połkną haczyk, zostają przekierowani na stronę, gdzie rzekomo znajdą szczegółowe informacje. Zobaczą jednak nie zawartość, której się spodziewają, ale spreparowaną stronę z niewidoczną ramką, aktywującą się razem z kliknięciem. Efektem jest zmiana ustawień konta użytkownika.

Co się stanie, gdy klikniecie w jakikolwiek przycisk lub obrazek na tej stronie? Wasz profil w mediach społecznościowych zostanie zainfekowany. Konto może stać się widoczne dla wszystkich (a więc dojdzie do zmiany ustawień prywatności), na tablicy pojawi się post o tym, że lubicie fałszywą stronę,

a do Waszych znajomych trafi spam. Co więcej – pechowe kliknięcie może uruchomić instalację aplikacji, która będzie próbować wyłudzać pieniądze, pobierać inne szkodliwe oprogramowanie i wciąż rozprzestrzeniać się wśród osób z Waszej listy znajomych.

Co zrobić, by nie paść ofiarą tego oszustwa, zwanego likejackingiem? Przede wszystkim nie możecie bezrefleksyjnie klikać we wszystkie linki, nawet jeśli pozornie wydają się ciekawe albo polecą je Wam znajomi. Uważajcie też na wszystkie sensacyjne informacje, które widzicie w swoich mediach społecznościowych. Czujność przede wszystkim!

Link

W świecie internetu pewnie nikomu nie trzeba przedstawiać linków – odnośników, dzięki którym, po kliknięciu, w ułamku sekundy przenosimy się pod dany adres w sieci. Linki, czyli inaczej mówiąc: hiperłącza, wykorzystują protokoły http lub https (w zależności od tego, czy strony są szyfrowane). Te internetowe odsyłacze albo występują w postaci adresu strony, albo mogą być ukryte pod innym tekstem (ang. *anchor text*).

Korzystanie z linków przyspiesza wymianę informacji oraz rozpowszechnianie wiadomości w internecie, a przede wszystkim ułatwia sprawny dostęp do zasobów online. Jednak czy wszystkie hiperłącza są bezpieczne? Niestety nie. Rozsyłanie linków, które pobierają złośliwe oprogramowanie i w efekcie prowadzą do zainfekowania urządzenia lub utraty danych osobowych czy pieniędzy, to częsta metoda stosowana przez cyberprzestępców. Uważajcie na wszystkie podejrzane linki: zawierające nietypowe kombinacje znaków czy literówki. Często możecie otrzymać je np. od rzekomej firmy kurierskiej żądającej dopłaty za paczkę. Jeśli link, który dostaniecie (nawet od znajomego!), prowadzi do systemu elektronicznych płatności – nie klikajcie w niego. To najskuteczniejsza obrona przed oszustwem!

Login

Gdy zakładacie internetowe konta – np. w mediach społecznościowych czy sklepach internetowych – pierwszą informacją, jaką musicie podać, jest Wasz login. To swoisty identyfikator użytkownika sieci lub systemu komputerowego. Swoją nazwę możecie wymyślić sami (np. dodając cyfry czy znaki do Waszego imienia lub pseudonimu), często jest nią np. adres e-mail lub jego początkowa część.

Login będziecie wpisywać za każdym razem podczas logowania do danego systemu, razem z hasłem. Sam kształt loginu nie wpływa na nasze bezpieczeństwo w sieci, warto jednak pamiętać, by nie zapisywać nigdzie loginów ani nie przekazywać ich nikomu. Znając login, cyberoszuści mogą spróbować włamać się do naszych kont, korzystając z funkcji „nie pamiętam hasła".

A skoro jesteśmy już przy hasłach, warto przypomnieć sobie zasady tworzenia silnych zabezpieczeń. Pisaliśmy o nich w aktualnościach „Silne hasło to podstawa!" na OSE IT Szkole i „Bezpieczni w sieci z OSE: bezpieczne logowanie" na ose.gov.pl. Zapoznajcie się też z nowymi rekomendacjami CERT Polska w zakresie tworzenia haseł i zabezpieczajcie wszystkie swoje konta!

Lootbox

Kto z nas nie męczył się długo z przejściem trudnego poziomu w grze i nie marzył o wsparciu wirtualnych mocy? Można próbować do skutku, można też skorzystać z dodatkowych skrzynek, zawierających losowo dobrane przedmioty czy inne pomoce ułatwiające rozgrywkę. To lootboxy (ang. *loot* – łup i *box* – skrzynka). Takie bonusy można kupić za monety zgromadzone w grze lub za realne pieniądze – za pomocą mikropłatności.

Lootboxy sprawiają, że gra staje się bardziej angażująca, a co za tym idzie: uzależniająca. Okazuje się bowiem, że działają tu te same mechanizmy co w przypadku hazardu i gier kasynowych. Choć mikropłatności wydają się pozornie niegroźne, niska z początku kwota zachęca do kupowania kolejnych skrzynek z bonusami. W efekcie może się nawet okazać, że za dodatkowe pomoce zapłacimy więcej niż za nową grę…

Więcej informacji o lootboxach oraz jasnych i ciemnych stronach gier komputerowych znajdziecie m.in. w poradniku dla rodziców „Nastolatki i gry cyfrowe" oraz w aktualnościach „Grać czy nie grać? Oto jest pytanie" i „Gra pod choinkę? Poradnik świętego Mikołaja" dostępnych na platformie OSE IT Szkoła.

Malware (złośliwe oprogramowanie)

To hasło z pewnością nie powinno kojarzyć się Wam pozytywnie – malware to złośliwe oprogramowanie, mogące przysporzyć nie lada kłopotów. Termin pochodzi od angielskich słów *malicious* (złośliwy) oraz *software* (oprogramowanie) i oznacza programy komputerowe, których celem jest wykonywanie szkodliwych działań, np. przejęcie kontroli nad urządzeniem ofiary czy kradzież danych, haseł bądź plików. Przykładami malware są m.in. wirusy, trojany, rootkit, oprogramowanie szyfrujące, robaki, keyloggery.

Złośliwe oprogramowanie może zaatakować niemal każde Wasze urządzenie – smartfony, komputery, kamery, pendrive, a nawet inteligentne urządzenia domowe, takie jak wideodomofony, sprzęt RTV – telewizory, a nawet AGD – lodówki, pralki. Niestety, im więcej sprzętów ofiary uda się cyberprzestępcom zainfekować, tym bardziej odczuje ona negatywne konsekwencje ich działania.

Aby chronić się przed malware, powinniście pamiętać o kilku ważnych zasadach, m.in. bieżącej aktualizacji oprogramowania i antywirusa, pobieraniu aplikacji i programów tylko z wiarygodnych źródeł, nieklikaniu w podejrzane linki i załączniki (np. otrzymane w e-mailu, SMS-ie), a także regularnym tworzeniu kopii zapasowych.

O malware oraz przeciwdziałaniu temu zagrożeniu dowiecie się więcej z kursu e-learningowego „Miękkie aspekty bezpieczeństwa w internecie" dostępnego na platformie OSE IT Szkoła. Zapoznajcie się też z biuletynem „OUCH! – Ochrona przed złośliwym oprogramowaniem".

Media społecznościowe

Kto z Was nie korzysta z mediów społecznościowych? W końcu to właśnie one są dla wielu internautów główną aktywnością online. Dzięki nim nawiązujemy i podtrzymujemy relacje, docieramy do informacji, dzielimy się swoimi opiniami lub wydarzeniami z życia.

Media społecznościowe (ang. *social media*, SM) to środki przekazu wykorzystujące technologie internetowe i mobilne, które pozwalają na komunikację na dowolną skalę. W odróżnieniu od tradycyjnych mediów (np. telewizji czy radia) social media nie tylko umożliwiają odbiór wiadomości, ale też dwukierunkową komunikację, np. w komentarzach. Dzięki nim nie musimy więc być już tylko biernymi odbiorcami, ale możemy też reagować na to, co publikują inni, oraz sami tworzyć przekazy.

Istnieje wiele rodzajów mediów społecznościowych, a tych – jak łatwo się domyślić – ciągle przybywa! Pamiętajcie jednak, że choć bardzo przyjemnie spędza się z nimi czas, to ich nadmierne użytkowanie może wiązać się z zagrożeniami, takimi jak: FOMO i nadużywanie nowych technologii, dezinformacja, przejęcie profilu czy kradzież tożsamości.

Jak bezpiecznie korzystać z mediów społecznościowych? Odpowiedzi znajdziecie w materiałach zamieszczonych na platformie OSE IT Szkoła: webinarze „Dzieci i młodzież a media społecznościowe” i poradniku „Media społecznościowe w szkole”. Przeczytajcie też koniecznie aktualności dostępne na ose.gov.pl: „Bezpieczne media społecznościowe”, „Bezpieczni w sieci z OSE: trolling w mediach społecznościowych” oraz ulotkę CERT Polska „Ważne zasady bezpiecznego użytkowania poczty elektronicznej i mediów społecznościowych”.

Menedżery haseł

Bezpieczne i unikalne hasła są ważne – to już na pewno wiecie – ale co zrobić, by spamiętać je wszystkie? Hasło do poczty, mediów społecznościowych, bankowości internetowej czy gier online: sami przyznajcie, że jest tego wiele. Pomocą w zapamiętaniu Waszych szyfrów mogą być właśnie menedżery haseł.

Na jakiej zasadzie działają? Takie aplikacje mają za zadanie przechowywać hasła w szyfrowanej bazie, dzięki czemu są one bezpieczne, a Wy nie musicie pamiętać ich wszystkich – wystarczy znać tylko jedno hasło, które umożliwia logowanie się do menedżera. Programy tego typu oferują również pomoc w wygenerowaniu hasła, a często umożliwiają też jego automatyczne wpisanie. Menedżery haseł mogą być wbudowane w przeglądarkę lub działać w chmurze.

Więcej informacji znajdziecie w biuletynie „OUCH! – Menedżer haseł” dostępnym na stronie CERT Polska. Zapoznajcie się też z aktualnością „Silne hasło to podstawa!” – znajdziecie ją na platformie OSE IT Szkoła.

mLegitymacja

Waszym uczniom lub dzieciom często zdarza się zapomnieć o zabraniu ze sobą legitymacji szkolnej? Może to być szczególnie kłopotliwe podczas kupowania biletu do kina lub na pociąg. Mamy na to proste rozwiązanie! mLegitymacja to legitymacja szkolna dostępna w smartfonie, dzięki czemu można mieć ją zawsze przy sobie. Z tego bezpłatnego, bezpiecznego i nowoczesnego narzędzia korzysta już wielu uczniów z całej Polski. mLegitymacja jest łatwa w obsłudze i uprawnia do tych samych ulg i zwolnień z opłat, co papierowa wersja dokumentu.

Co szkoła powinna zrobić, aby uczniowie mogli korzystać z elektronicznej legitymacji? Jeśli placówka została już podłączona do internetu OSE, wystarczy wypełnić dokumenty dostępne na portalu Moje OSE. Jeśli nie – na stronie ose.gov.pl należy wejść w zakładkę OSE poleca > mLegitymacja, a następnie postępować zgodnie z instrukcją. Do udziału w programie placówkę może zgłosić dyrekcja szkoły.

Elektroniczna legitymacja dla uczniów to jednak nie wszystko – swoją wirtualną wersję dokumentu mogą mieć również studenci! Na stronie ose.gov.pl sprawdźcie, co musi zrobić uczelnia, by dołączyć do projektu mLegitymacja studencka.

mLegitymacje szkolna i studencka są częścią aplikacji mObywatel, którą możecie pobrać na smartfon z systemem operacyjnym Android lub iOS.

Odwiedźcie stronę ose.gov.pl, gdzie znajdziecie więcej informacji o mLegitymacji szkolnej i studenckiej.

mOchrona

Coraz młodsi użytkownicy korzystają z internetu, gdzie mogą być narażeni na wiele cyberzagrożeń, m.in. zetknięcie ze szkodliwymi treściami czy nadużywanie nowych technologii. mOchrona to bezpłatna aplikacja kontroli rodzicielskiej stworzona w ramach Ogólnopolskiej Sieci Edukacyjnej. Pomaga rodzicom w zapewnianiu dzieciom bezpieczeństwa w sieci oraz diagnozowaniu potencjalnych problemów i zagrożeń, a co za tym idzie – szybszym reagowaniu na pojawiające się niebezpieczeństwa.

Aplikacja działa poprzez połączenie (sparowanie) urządzeń rodzica i dziecka, dzięki czemu ułatwia stałą opiekę nad najmłodszymi użytkownikami sieci. mOchrona wspiera ustalanie reguł dotyczących korzystania z urządzeń cyfrowych. Umożliwia wprowadzenie ustawień, które pomogą zminimalizować ryzyko kontaktu ze szkodliwymi treściami w internecie – rodzic może na sprzęcie dziecka m.in. blokować wybrane kategorie stron i aplikacji czy weryfikować czas, jaki spędza ono online.

Apka jest łatwa w obsłudze i zapewnia rodzicom dostęp do stale aktualizowanych treści edukacyjnych, dotyczących zasad bezpiecznego korzystania przez dzieci z internetu.

Więcej informacji na temat aplikacji mOchrona znajdziecie w na stronie ose.gov.pl: w zakładce „mOchrona” oraz wywiadzie „5 pytań o... aplikację mOchrona”.

Mowa nienawiści

Mowa nienawiści (ang. *hate speech*) to każda forma wypowiedzi, która znieważa, pomawia bądź rozbudza nienawiść wobec jakiejś osoby lub grupy. Takie negatywne i bolesne wypowiedzi wpływają na rozpowszechnianie się uprzedzeń i dyskryminacji ze względu na różne cechy, m.in.: rasę (rasizm), pochodzenie etniczne (ksenofobia), narodowość (szowinizm) czy wyznanie (antysemityzm, chrystianofobia, islamofobia).

Pamiętajcie, że według polskiego prawa treści propagujące rasizm i ksenofobię są nielegalne, a rozpowszechnianie ich w sieci jest karalne. W sytuacji, gdy zetkniecie się z takim materiałem w internecie, powinniście zgłosić ten fakt do zespołu Dyżurnet.pl. Możecie to zrobić za pomocą formularza, wysyłając wiadomość na adres e-mailowy: dyzurnet@dyzurnet.pl lub dzwoniąc pod numer 801 615 005.

Nadużywanie nowych technologii

Może dotknąć każdego – zarówno dorosłych, jak i dzieci, ale badacze wskazują, że nadużywanie nowych technologii najczęściej dotyczy nastolatków. Zbyt intensywne korzystanie z internetu i urządzeń cyfrowych może prowadzić do wielu problemów, takich jak: FOMO, nadużywanie telefonu (fonoholizm), a także zwiększać ryzyko uzależnienia – od gier czy hazardu online. Nadmierne zaangażowanie w świat online to również większe ryzyko podejmowania szkodliwych aktywności, np. oglądania pornografii w sieci.

Nadużywanie wiąże się występowaniem wewnętrznego przymusu bycia online, np. przeglądania mediów społecznościowych, grania w gry komputerowe czy posiadania urządzenia cyfrowego stale przy sobie. Zaniedbywanie przez dziecko nauki, przyjaciół spoza sieci, codziennych obowiązków, a także sięganie po urządzenie nawet w nocy, kosztem snu, smutek, rozdrażnienie, gdy w zasięgu ręki nie ma smartfona – te symptomy powinny Was zaniepokoić.

Co robić, aby internet i smartfon nie stały się problemem? Warto postawić na edukację i kształtowanie zdrowych nawyków cyfrowych. Dobre praktyki? Na początek zachęcamy do odkładania telefonu na czas posiłków, wyłączania powiadomień i nieużywania urządzenia godzinę przed snem. Z pomocą rodzicom przychodzi też bezpłatna aplikacja Ogólnopolskiej Sieci Edukacyjnej mOchrona. Ułatwia ona opiekę nad młodszymi dziećmi, które już surfują po internecie.

A co, gdy na profilaktykę jest już za późno? Jeśli korzystanie ze smartfona, komputera staje się dla Waszego dziecka przymusem, działajcie! Szczera rozmowa i wspólne ustalenie zasad korzystania z sieci – to pierwszy krok do zmian. Pamiętajcie, że częstym powodem nadużywania internetu jest nuda, dlatego należy postawić na ciekawe i angażujące dziecko aktywności offline.

Więcej informacji i praktycznych porad znajdziecie w publikacjach dostępnych na OSE IT Szkole: „FOMO i nadużywanie nowych technologii. Poradnik dla rodziców" i „FOMO i problemowe używanie internetu. Poradnik dla nauczycieli" oraz kursie e-learningowym „Zrozumieć FOMO". Dzieci zachęcamy do skorzystania z piątego modułu kursu e-learningowego „Przygody Profesora i N@tki, czyli jak mądrze korzystać z internetu", który pokazuje, czym jest równowaga pomiędzy światem online i offline.

Naruszenia prawa autorskiego

Twórcy, a więc autorowi dzieła – czy to muzycznego, literackiego, plastycznego, naukowego, czy fotograficznego – przysługuje prawo do wynagrodzenia i decydowania, w jaki sposób jego prace będą wykorzystywane. Niestety, w sieci bardzo często dochodzi do łamania praw autorskich. Dzieje się tak np. w przypadku, gdy ktoś pobiera z internetu utwory (najczęściej pliki muzyczne, filmy, aplikacje, zdjęcia, gry) i je rozpowszechnia. Takie działanie jest karalne!

Pamiętajcie też, że udostępnianie treści z internetu bez podania ich autora, źródła czy odnośnika do oryginalnego dzieła (łącza) również wiąże się z naruszeniem prawa autorskiego. Podobnie jest ze zdjęciami – jeśli już potrzebujecie obrazków z sieci, koniecznie wybierajcie te, które są udostępnione na licencji Creative Commons.

Więcej o naruszeniu prawa autorskiego znajdziecie na naszej platformie e-learningowej OSE IT Szkoła, np. w poradniku „Bezpieczeństwo online w szkołach Ogólnopolskiej Sieci Edukacyjnej – część 1". Zachęcamy też do skorzystania z kursów: „Własność intelektualna" oraz „Prawo autorskie – najważniejsze definicje", które w przystępny sposób przybliżają wiedzę na temat prawa autorskiego.

Naruszenia prywatności

Każdy z nas ma prawo do prywatności – również w internecie – a szczególnie do ochrony danych osobowych, takich jak: imię i nazwisko, data urodzenia, adres e-mail, numer PESEL, czy wrażliwych informacji, np. wyników badań.

Naruszenia prywatności to sytuacje, w których ktoś wykorzystuje cudzy wizerunek lub dane osobowe w celu wyrządzenia krzywdy osobistej bądź majątkowej. Przykładem takiego działania jest kradzież tożsamości, czyli przejęcie konta społecznościowego i podszywanie się pod jego właściciela. Uwaga: to przestępstwo!

Sieć nie sprzyja ochronie prywatności, szczególnie że sami często udostępniamy w niej więcej informacji o sobie, niż jest to konieczne. Nasze dane to też częsty cel cyberataków. Przestępcy wykorzystują złośliwe oprogramowanie (malware), by zainfekować cudzy sprzęt i wykraść cenne informacje. Ponadto stosują phishing, wyłudzając w ten sposób wartościowe dane (hasła logowania do serwisów społecznościowych czy bankowości elektronicznej).

Chrońcie swoją prywatność w internecie! Jeśli rejestrujecie się na nowej platformie lub w aplikacji, czytajcie politykę prywatności. Być może korzystanie z tych narzędzi będzie wymagać od Was zgody na udostępnienie zbyt wielu danych. Ponadto nie klikajcie w podejrzane linki, stosujcie silne i bezpieczne hasła, zmieńcie opcje prywatności w ustawieniach przeglądarki lub włączcie tryb incognito. Ograniczajcie też cyfrowy ślad. Pamiętacie, że cyberprzestępcy zdobywają wiedzę o Was, przeszukując różne platformy i serwisy – publikujcie więc w sieci jak najmniej informacji o sobie!

O naruszeniach prywatności przeczytacie na ose.gov.pl w aktualnościach: „Bezpieczni w sieci z OSE: ochrona danych osobowych" oraz „Bezpieczni w sieci z OSE: ochrona wizerunku i tożsamości w sieci". Sięgnijcie też po materiały dostępne na platformie OSE IT Szkoła: publikację „Bezpieczeństwo online w szkołach Ogólnopolskiej Sieci Edukacyjnej – część 1" oraz e-kurs dla dzieci „Przygody Profesora i N@tki, czyli jak mądrze korzystać z internetu". Pierwszy moduł „Pokaż siebie!" podejmuje właśnie temat ochrony prywatności online.

NASK

Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK-PIB) działa od 1991 r., a naszą misją jest cyfryzacja kraju oraz zapewnienie bezpieczeństwa w cyberprzestrzeni. Instytut prowadzi działalność naukową i badawczą (ThinkStat) oraz realizuje projekty edukacyjne (Akademia NASK, Safer Internet, ESA – Edukacyjna Sieć Antysmogowa), przekazując dzieciom i młodzieży wiedzę na temat zagrożeń w internecie. Promuje też koncepcję społeczeństwa informacyjnego otwartego na nowe technologie.

Ponadto, zgodnie z Ustawą o krajowym systemie cyberbezpieczeństwa, NASK pełni obowiązek jednego z Zespołów Reagowania na Incydenty Komputerowe – CSIRT (incydenty bezpieczeństwa i potencjalnie nielegalne treści można zgłaszać do CERT Polska i zespołu Dyżurnet.pl).

W ramach partnerstwa z Kancelarią Prezesa Rady Ministrów realizujemy też strategiczne projekty, takie jak: Ogólnopolska Sieć Edukacyjna (OSE), EZD RP – System Elektronicznego Zarządzania Dokumentami. Prowadzimy również Rejestr Domeny .pl oraz nowatorskie projekty w obszarze biometrii, usług Big Data czy sztucznej inteligencji.

Dowiedzcie się więcej o NASK-PIB – wejdźcie na stronę nask.pl.

„Nastolatki 3.0”

Od 2014 r. NASK prowadzi cykliczne badanie „Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów”, którego celem jest diagnoza zachowań polskich nastolatków w internecie. Od 2018 r. badaniem objęliśmy także rodziców, co umożliwia konfrontację opinii i wyobrażeń młodych z obserwacjami dorosłych. Regularność podejmowanych działań pozwala nam na uchwycenie dynamiki zmian związanych z aktywnością nastolatków online.

Do tej pory opublikowaliśmy cztery raporty, a ostatnie badanie zrealizowaliśmy w 2020 r. W kwestionariuszu znalazły się pytania dotyczące m.in.: czasu spędzanego w sieci, sposobu użytkowania internetu, świadomości zagrożeń, roli internetu i urządzeń mobilnych w edukacji czy doświadczenia cyberprzemocy oraz sposobów reagowania na niebezpieczne sytuacje w sieci.

Poznajcie interesujące wnioski płynące z najnowszego raportu „Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów”.

Netykieta

Czy wiecie, że dobre maniery obwiązują także w internecie? Netykieta to zbiór zasad dotyczących pozytywnych zachowań w sieci, a te wpływają też na nasze bezpieczeństwo. Kodeks online obejmuje wszystkich użytkowników wirtualnego świata. Złamanie dobrych obyczajów może wiązać się ze zgłoszeniem sprawy do administratora serwisu, a w konsekwencji – usunięciem członka z danej grupy, np. forum dyskusyjnego.

O jakich zasadach netykiety powinniście pamiętać? Przede wszystkim szanujcie innych użytkowników, nie bądźcie hejterami lub trollami! Przestrzegajcie regulaminu danego serwisu – nie zaśmiecajcie wirtualnej przestrzeni spamem, nie naruszajcie prawa autorskiego, nie rozpowszechniajcie fake newsów. Piszcie poprawnie, nie krzyczcie w internecie (wyłączcie CAPS LOCK), nie nadużywajcie emotikonów. Niebezpieczne i szkodliwe treści publikowane w sieci zgłaszajcie do odpowiednich instytucji, np. zespołu Dyżurnet.pl.

Przestrzeganie zasad netykiety na pewno sprawi, że cyfrowy świat będzie przyjaźniejszy i bezpieczniejszy dla jego wszystkich użytkowników.

Jak uczyć dziecko dobrych zachowań w internecie? Zachęcamy do skorzystania z naszych kursów e-learningowych na OSE IT Szkole: „Krasnoludki 2.0 – Mech w potrzebie" i „Relacje w środowisku medialnym".

Nielegalne treści

To szczególny rodzaj szkodliwych treści, które mogą wywołać negatywne emocje u odbiorcy i destrukcyjnie wpływać na rozwój dzieci i młodzieży. Nielegalne treści ponadto naruszają przepisy polskiego prawa (najczęściej przepisy Kodeksu karnego), a ich rozpowszechnianie jest karalne!

Do nielegalnych treści zaliczamy materiały przedstawiające m.in.: seksualne wykorzystywanie dziecka, propagujące rasizm i ksenofobię czy mogące ułatwić popełnienie przestępstwa o charakterze terrorystycznym.

Jeśli zetkniecie się w sieci z nielegalnymi treściami – reagujcie! O takiej sytuacji należy poinformować policję, a także działający w NASK zespół Dyżurnet.pl. Możecie to zrobić za pomocą formularza, wysyłając wiadomość e-mail na adres: dyzurnet@dyzurnet.pl lub dzwoniąc pod numer 801 615 005.

Więcej informacji o nielegalnych treściach znajdziecie na platformie OSE IT Szkoła w naszym poradniku „Szkodliwe treści w internecie". Zajrzyjcie też do aktualności „Niebezpieczne zjawiska w internecie: szkodliwe treści" – zebraliśmy w niej różne materiały na temat tego niebezpiecznego zjawiska.

Nomofobia

Tym terminem medycznym określa się jedną z chorób cywilizacyjnych. Nomofobia (z ang. *no mobile phone phobia*) oznacza paniczny strach przed brakiem dostępu do telefonu podłączonego do internetu. Osoby uzależnione od tego urządzenia oprócz lęku mogą odczuwać zawroty głowy, nudności czy ból w klatce piersiowej.

Chory dotknięty nomofobią dostaje ataku paniki na samą myśl, że może zgubić lub uszkodzić telefon. Frustracja pojawia się też w momencie, gdy traci go z zasięgu wzroku, zorientuje się, że bateria jest niemal wyczerpana lub telefon nie ma połączenia z siecią. Próby ograniczenia dostępu do urządzenia, brak

możliwości przeglądania mediów społecznościowych i reagowania na każde powiadomienie powodują nerwowość, poirytowanie, agresję.

Nomofobia to choroba, a więc osoby cierpiące z jej powodu powinny skorzystać z pomocy specjalisty. Warto jednak zawczasu podjąć działania profilaktyczne, by smartfon – ulubione urządzenie dzieci i młodzieży – nie stał się w przyszłości źródłem problemów.

Co zrobić, by nowe technologie były wsparciem w rozwoju młodych użytkowników? Zachęcamy do lektury aktualności „Cyfrowe nawyki u dzieci – to nasza wspólna sprawa" dostępnej na ose.gov.pl.

Niebezpieczne kontakty

Kontakty online mają wiele zalet – cenią je szczególnie osoby, dla których komunikacja przez internet bywa łatwiejsza od tej prowadzonej w realnym świecie. Warto jednak pamiętać, że niektóre znajomości bywają bardzo niebezpieczne. I choć z osobą o nieuczciwych intencjach może się w sieci zetknąć każdy, to skutki takiego kontaktu szczególnie dotkliwie odczują dzieci. Miły znajomy z internetu może się okazać niebezpiecznym przestępcą!

Na jakie zagrożenia narażeni są młodzi użytkownicy sieci podczas zawierania znajomości online? Jednym z nich jest child gromming, czyli uwodzenie nieletnich w internecie. To przestępstwo wiąże się też z nakłonieniem ofiary do produkcji intymnych materiałów (self generated content), a także z szantażem (sextortion), który sprawia, że generowane są kolejne zdjęcia lub filmy. Pamiętajcie, że relacja groomingowa bardzo często prowadzi do wykorzystania dziecka w świecie realnym!

Warto podjąć kroki zmierzające do ochrony dzieci i młodzieży przed nawiązywaniem niebezpiecznych kontaktów online. Postawcie na rozmowę i edukację w zakresie cyberzagrożeń. Budujcie relacje z dzieckiem oparte na zaufaniu. Wspierająca postawa rodziców i opiekunów sprawi, że chętniej zwróci się ono do Was po pomoc w przypadku doświadczenia trudnej sytuacji w internecie.

Jak bezpiecznie nawiązywać i podtrzymywać relacje w sieci? Wskazówek szukajcie w naszej aktualności na ose.gov.pl „Złote zasady internetowych znajomości".

Offline challenge

Zastanawialiście się kiedyś, ile razy w ciągu doby sięgacie po swój smartfon? Mamy odpowiedź: większość z nas robi to nawet kilkadziesiąt razy dziennie! Telefon towarzyszy nam w zasadzie wszędzie: podczas posiłków, w podróży, spotkań ze znajomymi. Zostawiamy lajki, scrollujemy media społecznościowe, wpadamy w pułapkę automatycznego odtwarzania filmików na YouTubie czy TikToku. Internet wciąga – to niezaprzeczalny fakt. Ale czy to znaczy, że nie mamy wpływu na nasze cyfrowe nawyki? Wręcz przeciwnie!

Warto zatrzymać się na chwilę i sprawdzić, jak dużo czasu spędzamy w sieci i na czym polegają nasze aktywności online. Z pomocą przychodzi akcja #offlinechallenge polegająca na odłączeniu się od internetu na 48 godzin. Czy dwie doby bez dostępu do sieci to dużo? I tak, i nie. W tym czasie na pewno nie zmienicie diametralnie swojego życia i przyzwyczajeń, nie będzie to detoks, po którym wyjdziecie odmienieni. Jednak 48 godzin offline na pewno pozwoli dokładniej przyjrzeć się temu, jak funkcjonujecie, gdy nie rozpraszają Was powiadomienia, gdy w różnych sytuacjach musicie sobie radzić bez kilku kliknięć na ekranie smartfona.

Możliwe, że dwie doby bez dostępu do sieci skłonią Was do ograniczenia czasu przeznaczanego np. na media społecznościowe. Zauważycie pewnie, że zamiast przeglądać zdjęcia i filmiki na Facebooku czy Instagramie, możecie w tym czasie zająć się swoimi pasjami, wyjść na spacer czy spotkać się ze znajomymi. A może to nietypowe wyzwanie będzie początkiem większych zmian, które wprowadzicie w swoim codziennym życiu? Spróbujcie i sami się przekonajcie – warto!

Szczegółowe informacje o wyzwaniu znajdziecie na stronie offlinechallenge.pl, a wskazówki dotyczące budowania zdrowych nawyków cyfrowych – w naszych aktualnościach na stronie ose.gov.pl: „5 pytań o… offlinechallenge”, „Majówka – cyfrowy detoks czy balans?”, „Bezpieczni w sieci z OSE na wakacje: offline challenge”, „W wakacje bez internetu? Podejmij wyzwanie!” i „Cyfrowe nawyki u dzieci – to nasza wspólna sprawa”.

Ogólnopolska Sieć Edukacyjna (OSE)

Trudno mówić o bezpieczeństwie w sieci bez przypomnienia, czym jest… Ogólnopolska Sieć Edukacyjna!

OSE to program publicznej sieci telekomunikacyjnej, dający szkołom w całej Polsce możliwość podłączenia szybkiego, bezpiecznego i bezpłatnego internetu. Realizujemy go my, czyli NASK Państwowy Instytut Badawczy, pod nadzorem Kancelarii Prezesa Rady Ministrów. W ramach programu OSE prowadzimy także działania edukacyjno-informacyjne, promujące zasady bezpiecznego korzystania z technologii cyfrowych. Ogólnopolska Sieć

Edukacyjna jest bowiem odpowiedzią na wyzwania współczesnej edukacji – kształtującej kompetencje cyfrowe i otwartej na nowoczesne technologie.

W ramach OSE razem z internetem dostarczamy profesjonalne usługi bezpieczeństwa: „Bezpieczny internet OSE", „Bezpieczeństwo użytkownika OSE", „Ochrona przed szkodliwym oprogramowaniem". Nasze usługi strzegą bezpieczeństwa szkolnych sieci, chronią przed różnego rodzaju niebezpieczeństwami online i atakami sieciowymi, a także monitorują, wykrywają i blokują zagrożenia związane ze złośliwym oprogramowaniem (malware) oraz nielegalnymi, szkodliwymi treściami. Codziennie dbamy o to, aby korzystający z internetu OSE byli bezpieczni online!

Usługi bezpieczeństwa to jednak nie wszystko. Sercem naszego programu są działania edukacyjne, które wspierają uczniów w bezpiecznym korzystaniu z sieci. Podpowiadamy nauczycielom, dyrektorom szkół i rodzicom, jak być przewodnikami dzieci w cyfrowym świecie. Z pomocą przychodzą nasi eksperci i tworzone przez nich materiały edukacyjne: poradniki, scenariusze zajęć i kursy e-learningowe, dotyczące m.in. rozważnych zachowań w sieci czy zagrożeń, z którymi mogą zetknąć się online dzieci i młodzież.

Nasze treści edukacyjne znajdziecie na bezpłatnej platformie e-learningowej OSE IT Szkoła, która powstała z myślą o dostarczeniu nauczycielom i uczniom wartościowych kursów w wielu kategoriach, takich jak cyberbezpieczeństwo, sztuczna inteligencja czy programowanie. Mogą oni skorzystać z ponad 200 materiałów, w tym najnowszych kursów „Przygody Profesora i N@tki, czyli jak mądrze korzystać z internetu" czy „Zrozumieć FOMO". Zapoznajcie się z całą ofertą edukacyjną OSE już dziś!

W ramach projektu OSEhero wspólnie tworzymy też grupę zaangażowanych nauczycieli, którzy we współpracy z ekspertami OSE przekazują wiedzę o bezpieczeństwie w internecie uczniom, pedagogom oraz rodzicom. Wiemy, że bezpieczeństwo cyfrowe to nasza wspólna sprawa i każdy może sprawić, by internet stał się dla dzieci i młodzieży bezpieczną przystanią.

Oprogramowanie antywirusowe

Bardzo często naszym pierwszym skojarzeniem z cyberbezpieczeństwem jest program antywirusowy. Co to takiego? Główną funkcją antywirusa – zawartą już w nazwie – jest skanowanie, wykrywanie, rozpoznawanie oraz usuwanie złośliwego oprogramowania (malware) z komputera lub innego urządzenia, na którym zostało zainstalowane. Można powiedzieć, że program antywirusowy to swego rodzaju szczepionka: jeśli na bieżąco go aktualizujemy, ryzyko cyfrowej infekcji się zmniejsza.

Zapewnianie bezpiecznego przeglądania zasobów internetu polega na skanowaniu dostępnych na urządzeniu obiektów i porównywaniu z dostępną bazą, czyli sygnaturami wirusów. Odbywa się na dwa sposoby: poprzez skanowanie ręczne, gdy sami uruchamiamy program antywirusowy, lub w trakcie automatycznego poszukiwania intruzów na naszym urządzeniu.

Jeśli antywirus wykryje złośliwe oprogramowanie, natychmiast zareaguje i zaproponuje potrzebne działanie – usunięcie, zablokowanie lub przeniesienie zainfekowanego pliku do kwarantanny.

Jak ważne jest regularne aktualizowanie oprogramowania, w tym antywirusa? Dowiecie się tego z naszych aktualności: „Akcja-aktualizacja – zadbaj o swój sprzęt w wakacje!" i „Czas na wiosenne – cyfrowe – porządki!".

Oprogramowanie szyfrujące

Silne hasła, uwierzytelnianie dwuskładnikowe, biometria – kolejne sposoby zabezpieczeń naszych kont i cennych informacji pojawiają się wraz z nowymi działaniami cyberprzestępców. Do niemałego arsenału środków ochrony warto dołączyć też oprogramowanie szyfrujące, które uniemożliwia osobom niepowołanym dostęp do naszych plików lub danych.

Prywatne materiały, tajne projekty, wrażliwe dane: wszystkie tego typu pliki warto zamykać w symbolicznym sejfie zabezpieczonym dobrze strzeżonym kluczem. Oprogramowanie szyfrujące jest przydatne zwłaszcza teraz – w czasach, gdy bardzo chętnie korzystamy z usług chmur umożliwiających przechowywanie informacji na wirtualnych serwerach. Pamiętajcie jednak, że takie rozwiązania, mimo że niewątpliwie wygodne i pomocne, wiążą się z ryzykiem kradzieży danych, a nawet kradzieży tożsamości.

Jak działa oprogramowanie szyfrujące? Po zainstalowaniu odpowiedniego programu nasze pliki są przetwarzane przez algorytm szyfrowania, który następnie konwertuje je i sprawia, że są nieczytelne. Gdy zamierzony odbiorca (my lub ktoś, komu udostępniamy dany dokument) uzyskuje dostęp do pliku, zawarte w nim informacje tłumaczone są na powrót do swojej pierwotnej postaci. Aby odszyfrować wiadomość, należy użyć klucza szyfrującego – zbioru algorytmów, które szyfrują i odszyfrowują dane do czytelnego formatu.

O szyfrowaniu powinniście pamiętać nie tylko przechowując poufne dokumenty, ale też wysyłając je za pośrednictwem poczty elektronicznej!

Oszustwa internetowe

Zapewne nie raz spotkaliście się z ostrzeżeniami przed oszustwami w wirtualnym świecie, może nawet śledzicie komunikaty publikowane przez CERT Polska. To dobrze! Warto trzymać rękę na pulsie, bo wraz z szerokim dostępem do internetu pojawiają się kolejne sposoby oszukiwania ofiar w sieci.

Mamy tutaj na myśli różnego rodzaju ataki przeprowadzane online – bezpośrednio w internecie lub przy użyciu oprogramowania z dostępem do sieci. Mają one wspólny mianownik, mianowicie przestępcy wykorzystują niewiedzę, nieświadomość, a nawet samotność i naiwność użytkowników, by okraść ich lub zdobyć cenne informacje.

Na co trzeba uważać? Na wszelkie podejrzane próby kontaktu w internecie: za pośrednictwem osobistych bądź służbowych kont e-mail, serwisów społecznościowych, a nawet aplikacji randkowych. Niech nie zwiedzie Was obietnica szybkiej wygranej, informacja o dużym spadku czy zbyt atrakcyjnej ofercie pracy! Uważajcie również na fałszywe sklepy internetowe, w których „płacimy tylko za dostawę", i na nieautoryzowane oferty sprzedaży biletów na popularne koncerty czy wydarzenia.

W internecie możemy wiele stracić, ufając jedynie emocjom. Jeśli otrzymacie e-mail, w którym wymusza się na Was natychmiastowe działanie, wpłacenie okupu za odzyskanie utraconych plików czy podanie danych osobowych, np. danych do logowania w bankowości elektronicznej – zignorujcie tę wiadomość! Zastanówcie się też dwa razy, gdy o dużą pożyczkę poprosi Was ktoś, kogo znacie jedynie z internetu.

Szczegółowe informacje znajdziecie w naszych aktualnościach: „Bezpieczni w sieci z OSE: phishing" i „Złote zasady internetowych znajomości" oraz w biuletynie OUCH! „Najpopularniejsze oszustwa w serwisach społecznościowych".

OUCH!

Źródeł informacji o bezpiecznym korzystaniu z internetu jest bardzo wiele. Oprócz materiałów tworzonych w ramach Ogólnopolskiej Sieci Edukacyjnej (poradników, webinarów, kursów e-learningowych czy aktualności) należy wspomnieć jeszcze o co najmniej jednym – serii biuletynów OUCH!. Dlaczego warto po nie sięgać?

OUCH! to zestawy porad w zakresie cyberbezpieczeństwa, wydawane w 22 językach na całym świecie. Polska wersja ukazuje się co miesiąc od kwietnia 2011 r. w ramach współpracy CERT Polska i SANS Institute. Każdy z biuletynów przybliża wybrane zagadnienie z obszaru bezpieczeństwa komputerowego. Co ważne – nie brakuje tutaj listy wskazówek, jak chronić się przed zagrożeniami w internecie.

Szukacie porad dotyczących bezpieczeństwa w sieci? Sięgnijcie np. do biuletynów OUCH! dotyczących oszustw w serwisach społecznościowych, wykrywania deepfake, kariery w cyberbezpieczeństwie i ataków w wiadomościach tekstowych. Wszystkie archiwalne wydania znajdziecie na stronie CERT Polska, koniecznie do nich zaglądajcie!

Oversharing

Zdjęcie śniadania, selfie w windzie i podczas treningu, fotka ze śpiącym kotem czy dzieckiem umorusanym marchewkową zupką. Wszyscy to znamy – dzielenie się w sieci szczegółami ze swojego życia to już codzienność. Chętnie dokumentujemy swoje dni i jeszcze chętniej pokazujemy prywatne pamiątki światu. Jednak czy zawsze słusznie…?

Zjawisko oversharingu (ang. *over* – ponad i *sharing* – udostępnianie), czyli nadmierna wylewność online, jednym może przysporzyć internetowych fanów, a drugim – kłopotów. Gdy zamieszczamy w mediach społecznościowych wiele swoich zdjęć i postów z informacjami o tym, gdzie teraz jesteśmy, czy co robimy, narażamy się na niebezpieczeństwo związane np. z kradzieżą (złodziej będzie przecież doskonale wiedział, że skoro właśnie opalamy się nad morzem, to nasz dom stoi pusty). A gdy przez nieuwagę na udostępnionym w sieci zdjęciu znajdzie się fragment dokumentu tożsamości czy numer PESEL, ułatwiamy cyberprzestępcom np. zaciągnięcie kredytu na nasze konto.

Dorosłych oversharing naraża często na śmieszność i zniecierpliwienie znajomych, którzy oglądają np. dziesiątki zdjęć zwierząt domowych w różnych pozach. Co jednak ze zdjęciami dzieci udostępnianymi przez rodziców? Warto pamiętać, że nadmierne publikowanie w sieci zdjęć najmłodszych (sharenting) również może nieść za sobą spore ryzyko. Przestępcy, obserwując kolejne dodawane posty, uzyskają o Waszym dziecku wiele ważnych informacji – w którym przedszkolu spędza czas do południa, jaka jest jego ulubiona maskotka i jakie bajki najbardziej lubi oglądać. Czy takie dane nie wystarczą, żeby wzbudzić zaufanie dziecka i przy nadarzającej się okazji spróbować je wykorzystać…?

Uważajcie na to, co udostępniacie w sieci. Tutaj także sprawdza się znana reguła: mniej znaczy więcej!

Patotreści

Czy zawsze wiecie, co Wasze dzieci lub uczniowie oglądają online i jak wpływa to na ich rozwój? Patotreści to materiały – filmy, transmisje na żywo – które prezentują zachowania uznawane za szkodliwe i destrukcyjne. Patostreamy pokazują np. upijanie się, bijatyki, sceny wulgarnego wyzywania i obrażania, przemoc domową i seksualną, okrucieństwo wobec zwierząt, zażywanie narkotyków lub innych substancji psychoaktywnych. Są szczególnie niebezpieczne dla dzieci i nastolatków, którzy zwykle nie zdają sobie sprawy z ich destrukcyjnego wpływu.

Kontakt z patotreściami może mieć negatywny wpływ na kształtującą się psychikę uczniów, ich zachowanie. Takie materiały mogą wywoływać lęk, skutkować obniżeniem nastroju, a niekiedy znieczuleniem i obojętnością wobec patologicznych zachowań. Powodów, dla których młodzi decydują się na oglądanie szkodliwych streamów (lub ich skrótów, tzw. shotów), jest wiele: ekscytacja, ciekawość, nuda, przypadek, chęć zapewnienia sobie rozrywki lub po prostu namowa znajomego, który podeśle im taki materiał. Co niepokojące, prawie co piąty nastolatek oglądający patostreamy przyznaje, że ich twórcy mu imponują (Wójcik, Wojtasik, 2019).

Więcej informacji na temat patotreści znajdziecie na platformie OSE IT Szkoła: w poradniku „Szkodliwe treści w internecie", scenariuszu lekcji „Co oglądamy w rozbitym lustrze? Królowa Śniegu i patostreamy". Przeczytajcie też na ose.gov.pl naszą aktualność „Bezpieczni w sieci z OSE: patostreamy". Pomocą dla rodziców w ochronie dzieci przed szkodliwymi treściami w internecie będzie również aplikacja Ogólnopolskiej Sieci Edukacyjnej mOchrona – sprawdźcie koniecznie, jak działa!

Pan European Game Information (PEGI)

PEGI to ogólnoeuropejski system klasyfikowania gier. Dlaczego warto się nim kierować, wybierając grę? Dzięki tym oznaczeniom możecie mieć pewność, że dostarczycie Waszemu dziecku rozrywki, która będzie nie tylko ciekawa, ale też bezpieczna i dostosowana do jego wieku.

Oznaczenia PEGI znajdziecie w sklepach z aplikacjami wśród podstawowych informacji o grze, jak również na opakowaniach gier. Podawane są na dwa sposoby: pierwszy dotyczy minimalnego wieku gracza (wyróżniamy pięć kategorii: PEGI 3, PEGI 7, PEGI 12, PEGI 16, PEGI 18), drugi to deskryptory treści w systemie PEGI, czyli oznaczenia informujące o rodzaju treści, jakie występują w danej grze. To właśnie one podpowiedzą Wam, czy dana propozycja zawiera np. wulgaryzmy, treści erotyczne czy sceny przemocy. Wyróżniamy osiem deskryptorów treści w systemie PEGI: Przemoc (*Violence*), Wulgaryzmy (*Bad language*), Strach/Groza (*Fear*), Elementy hazardu (*Gambling*), Odwołania do seksu (*Sex*), Narkotyki/używki (*Drugs*), Dyskryminacja (*Discrimination*) i Mikropłatności w grze (*In-game purchases*).

Szczegółowe wyjaśnienie oznaczeń oraz wiadomości na temat bezpiecznego grania znajdziecie na platformie OSE IT Szkoła w poradniku „Nastolatki i gry cyfrowe”. Przeczytajcie też koniecznie aktualność „Pomysł na Dzień Pac-Mana? Dowiedz się więcej na temat grania!”, w której polecamy ciekawe materiały o gamingu.

Password spraying

Używacie przewidywalnych, łatwych do odgadnięcia haseł? Uwaga, możecie być narażeni na password spraying!

To atak polegający na wykorzystaniu przez cyberprzestępców popularnych haseł w celu uzyskania dostępu do Waszych kont e-mailowych, założonych w bankowości elektronicznej czy sklepach online. Password spraying to dość częsty sposób działania oszustów, ponieważ – niestety – wiele osób zapomina o zasadach tworzenia silnych i bezpiecznych haseł. Łatwo się więc domyślić, czym grozi zastosowanie haseł typu 1234, admin1, hasło1 – i to na kilku lub wszystkich kontach. Cyberprzestępcy bez trudu mogą uzyskać do nich dostęp!

Koniecznie podejmijcie działania, które zminimalizują ryzyko ataku. Przede wszystkim zadbajcie o odpowiednie zabezpieczenie cyfrowych danych. Ostatnie rekomendacje CERT Polska w zakresie tworzenia silnych haseł zawierają np. zalecenie, by szyfry miały minimum 12 znaków i były łatwe do zapamiętania dla nas, ale trudne do odgadnięcia przez potencjalnych przestępców.

Pamiętajcie też o stosowaniu uwierzytelniania dwuskładnikowego (ang. *Two Factor Authenticaton, 2FA*). Dodatkowy kod przesłany SMS-em czy za pośrednictwem aplikacji lub zabezpieczenie biometryczne sprawią, że Wasze dane będą bardzo trudne do przejęcia przez cyberprzestępców.

Więcej praktycznych porad znajdziecie na ose.gov.pl w aktualnościach „Bezpieczni w sieci z OSE: bezpieczne logowanie” i „Bezpieczni w sieci z OSE: uwierzytelnianie dwuskładnikowe”. Sprawdźcie też nowe rekomendacjami CERT Polska dotyczące tworzenia silnych i bezpiecznych haseł.

Pełnomocnik Rządu ds. Cyberbezpieczeństwa

To osoba, która koordynuje działania i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa w kraju.

Do jego zadań należy m.in. analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa (KSC), nadzór nad procesem zarządzania ryzykiem KSC czy upowszechnianie nowych rozwiązań i inicjowanie działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym.

Więcej informacji na temat funkcji i zadań Pełnomocnika Rządu ds. Cyberbezpieczeństwa znajdziecie w Ustawie o krajowym systemie cyberbezpieczństwa.

Pharming

Jeśli kiedykolwiek zdarzyło Wam się zalogować do swojego banku online i stwierdzić, że Wasze dane zostały wykradzione, a pieniądze z konta zniknęły, najprawdopodobniej padliście ofiarą pharmingu. To podobna, lecz groźniejsza od phishingu forma oszustwa polegająca na tworzeniu fałszywych stron internetowych, które podszywają się pod znane, bezpieczne witryny, i gromadzeniu w ten sposób poufnych danych.

Na czym dokładnie polega pharming? Użytkownicy korzystający ze stron bankowości elektronicznej są przekierowywani na łudząco podobne, podszywające się pod nie strony, które instalują na urządzeniach złośliwe oprogramowanie wykradające dane osobowe, takie jak dane kont bankowych czy hasła. Bywa też, że cyberoszuści infekują od razu cały serwer DNS, a więc wszyscy, którzy chcą zalogować się do banku, trafiają na podrobioną wersję strony.

Czerwoną lampkę powinien zapalić nie tylko nieoczekiwany brak środków na koncie lub dziwna historia transakcji, ale też pojawienie się na komputerze aplikacji czy programów, których nie instalowaliście. Szkodliwe oprogramowanie może trafić do nas np. za pośrednictwem linków przesyłanych w e-mailach, zatem pod żadnym pozorem nie klikajcie w odnośniki w niechcianych wiadomościach!

Ustrzec się przed pharmingiem pomoże Wam stosowanie dobrze znanych zasad cyberhigieny: instalowanie i bieżące aktualizowanie programu antywirusowego, zwracanie uwagi na adres strony internetowej (sprawdzanie, czy nie ma w nim błędów, czy połączenie jest szyfrowane), a także nieotwieranie podejrzanych e-maili. Warto również włączyć uwierzytelnianie dwuskładnikowe oraz autoryzację transakcji w aplikacji banku.

Pamiętajcie, że wszelkie oszustwa internetowe, w tym wyłudzenia danych i środków finansowych, możecie zgłaszać do zespołu CERT Polska za pośrednictwem specjalnego formularza.

Phishing

Nazwa wydaje się Wam znajoma? I słusznie – termin phishing budzi dźwiękowe skojarzenie z angielskim słowem *fishing* oznaczającym łowienie ryb. Na tym jednak podobieństwo się nie kończy… Cyberprzestępcy podobnie do wędkarzy przygotowują odpowiednią przynętę, na którą usiłują złapać swoje potencjalne ofiary. Celem takich działań jest wyłudzenie poufnych danych – najczęściej logowania do serwisów społecznościowych lub bankowości elektronicznej.

Podczas wirtualnego ataku oszust stara się wprowadzić nas w błąd i przekonać do wykonania określonej czynności: otwarcia zainfekowanego załącznika, kliknięcia w złośliwy link lub zalogowania się w oknie fałszywej strony (np. bramki do płatności elektronicznych). Aby osiągnąć swój cel, próbuje

skontaktować się z ofiarą, wykorzystując sfabrykowane e-maile, SMS-y (vishing), wiadomości na komunikatorach i portalach społecznościowych. Do oszustwa może też dojść za pośrednictwem rozmowy telefonicznej (spoofing), podczas której przestępca podszywa się pod pracowników instytucji zaufania publicznego lub innego użytkownika. Jeśli podążycie za instrukcją przestępcy, szybko możecie przekonać się, że straciliście środki z konta bankowego, ważne dane lub informacje.

Jak nie połknąć haczyka? Najważniejsze są ostrożność i rozsądne podejście do otrzymywanych wiadomości. Pamiętajcie, że oszuści mogą podszywać się pod Waszych znajomych, zaufane instytucje czy firmy, z których usług korzystacie na co dzień. Waszą podejrzliwość powinna wzbudzić m.in. treść nakłaniająca do szybkiego i nieprzemyślanego działania lub udostępnienia wrażliwych danych, gdyż w przeciwnym wypadku wydarzy się coś złego (np. konto zostanie zablokowane) lub stracicie niepowtarzalną okazję.

Więcej na temat ochrony przed phishingiem dowiecie się z biuletynu „OUCH! – Powstrzymać phishing" oraz aktualności na stronie ose.gov.pl „Bezpieczni w sieci z OSE: phishing". Na młodszych uczniów czeka zaś na platformie OSE IT Szkoła kurs e-learningowy „Krasnoludki 2.0 – Phishing, czyli kłopoty to nasza specjalność".

Phubbing

Jak często prosicie dziecko lub ucznia o odłożenie telefonu i skupienie się na rozmowie czy lekcji? A może sami macie problem z rozstaniem się ze smartfonem nawet podczas rozmowy lub to właśnie Wy zostaliście zignorowani przez kogoś, kto nie może oderwać wzroku od ekranu urządzenia? Takie zachowanie to phubbing.

Termin ten powstał z połączenia angielskich słów *phone* (telefon) i *snubbing* (lekceważenie, odtrącenie). Odnosi się do sytuacji, w której ktoś jest tak pochłonięty i skoncentrowany na swoim smartfonie, że podczas spotkania z innymi osobami po prostu je lekceważy. W takich przypadkach potrzeba korzystania ze smartfona jest niestety silniejsza od przestrzegania zasad dobrego wychowania, a czasem nawet… własnego bezpieczeństwa!

Phubbing najczęściej dotyczy osób z wysokim FOMO, które nie potrafią rozstać się ze swoim telefonem. Dlatego już od najmłodszych lat powinniśmy dbać o przekazywanie uczniom wiedzy, jak zdrowo i rozsądnie korzystać z możliwości nowych technologii.

Więcej wiadomości na temat phubbingu dostarczy Wam aktualność „*Tylko zerknę*. Sprawdź, czy Twoje dziecko doświadcza phubbingu" – znajdziecie ją na stronie ose.gov.pl.

Polskie Centrum Programu Safer Internet (PCPSI)

W NASK aktywnie działamy na rzecz bezpieczeństwa dzieci i młodzieży korzystających z internetu i nowych technologii, m.in. jesteśmy koordynatorem projektu Polskie Centrum Programu Safer Internet. PCPSI zostało powołane w 2005 r. w ramach programu Komisji Europejskiej Safer Internet, a obecnie funkcjonuje jako element programu Digital Europe. Tworzymy je razem z Fundacją Dajemy Dzieciom Siłę.

Na działania PCPSI składają się trzy projekty:

1. **Saferinternet.pl**: projekt, w którym zwiększamy społeczną świadomość na temat zagrożeń w cyberprzestrzeni. Publikacje powstające w ramach projektu oraz organizowane konferencje kształtują kompetencje – dzieci, rodziców i profesjonalistów – w zakresie bezpiecznego korzystania z sieci. Z naszymi działaniami docieramy zarówno do młodszych (np. Sieciaki, Necio, Plik i Folder, Digital Youth), jak i starszych użytkowników internetu (np. Dzień Bezpiecznego Internetu, Międzynarodowa Konferencja „Bezpieczeństwo dzieci i młodzieży w internecie").
2. **Pomoc telefoniczna i online**: realizujemy ją poprzez Telefon zaufania dla dzieci i młodzieży (116 111) oraz Telefon dla rodziców i nauczycieli w sprawach bezpieczeństwa dzieci (800 100 100). Eksperci Fundacji Dajemy Dzieciom Siłę za ich pośrednictwem reagują w przypadkach zagrożeń związanych z korzystaniem z internetu.
3. **Dyżurnet.pl**: to punkt kontaktowy, który prowadzimy w NASK. Możecie do niego anonimowo zgłaszać przypadki występowania w internecie nielegalnych treści, w tym materiałów przedstawiających seksualne wykorzystanie dzieci (formularz zgłoszeniowy, tel.: 801 615 005, e-mail: dyzurnet@dyzurnet.pl).

Więcej informacji o działaniach w ramach PCPSI znajdziecie na stronie saferinternet.pl.

Propaganda

W internecie każdego dnia spotykamy się z różnymi przekazami, które mogą mieć na celu szerzenie propagandy i wpływanie na nasze poglądy. Propaganda to bowiem zaplanowane działanie, które ma za zadanie oddziaływać na zbiorowość i jednostki, zjednywać zwolenników i sojuszników określonych idei, poglądów, działań, wpajać konkretne przekonania oraz wywoływać określone zachowania.

Celem propagandy może być np. narzucanie odbiorcom danych poglądów lub postaw – wykorzystywane są do tego środki perswazji intelektualnej i emocjonalnej (m.in. słowa, gesty, obrazy) oraz metody manipulacji, takie jak np. dezinformacja.

Choć propaganda, fake newsy i dezinformacja nie są tym samym zjawiskiem, to mogą być wykorzystywane w tym samym celu – szerzenia nieprawdziwych

wiadomości. Jak nie wpaść w sidła manipulacji? Podpowiedzi znajdziecie w materiałach dostępnych na platformie OSE IT Szkoła: ulotce „Fake newsy, bańki informacyjne, teorie spiskowe", konspekcie zajęć „Fake newsy i dezinformacja – o tym warto porozmawiać w szkole" oraz infografice „Jak rozpoznać fake newsa". Zapoznajcie się też z aktualnościami na ose.gov.pl: „Zanim uwierzysz, sprawdź!" i „Jak nie wpaść w pułapkę fake newsów?".

Prywatność w sieci

Myśląc o bezpieczeństwie online, zwykle instalujemy program antywirusowy czy stosujemy silne hasła, ale czy równie często pamiętamy o ochronie prywatności? Czy wiecie, że każde nasze działanie w internecie – w tym komentowanie, dodawanie zdjęć, korzystanie z wyszukiwarki – pozostawia cyfrowy ślad, który dla naszego bezpieczeństwa powinniśmy tworzyć rozsądnie?

Warto pamiętać, że podczas różnych aktywności w sieci łatwo może dojść do kradzieży danych, a stąd już tylko krok od niemałych problemów. Ukradzione dane mogą posłużyć m.in. do wyłudzenia pożyczki, przeprowadzenia fałszywych transakcji bankowych czy podszywania się pod Was w korespondencji.

Jak oszuści uzyskują dostęp do poufnych informacji? Może się to wydarzyć na skutek ataku phishingowego czy w wyniku wycieku danych np. z e-sklepów. Najczęściej jednak sami dajemy cyberprzestępcom dostęp do prywatnych informacji – swobodnie dzieląc się nimi m.in. w serwisach społecznościowych. Pamiętajcie więc o konieczności zadbania o swoje bezpieczeństwo i prywatność w sieci – rozważnie publikujcie wiadomości o sobie, uważnie czytajcie politykę prywatności i regulaminy serwisów, wirtualnych sklepów oraz platform, na jakich się rejestrujecie. Udostępniajcie tylko te dane, które są niezbędne do skorzystania z usługi. Stosujcie też silne i unikalne hasła, a także nie klikajcie w podejrzane linki i załączniki.

Więcej praktycznych wskazówek, jak dbać o swoją prywatność w sieci, znajdziecie na platformie OSE IT Szkoła w poradniku „Bezpieczeństwo online w szkołach Ogólnopolskiej Sieci Edukacyjnej – część 1" oraz aktualności na stronie ose.gov.pl „Bezpieczni w sieci z OSE: ochrona danych osobowych".

Quishing

Wraz z usprawnianiem metod przeciwdziałania różnym atakom, cyberprzestępcy doskonalą swoje metody wyłudzania naszych danych osobowych oraz środków finansowych. Jedną z nich jest quishing. To forma phishingu, która wykorzystuje już nie linki przesyłane w e-mailach, ale odpowiednio spreparowane kody QR (ang. *Quick Response*, czyli szybka odpowiedź). Znacie na pewno czarno-białe kwadratowe kody graficzne, które po zeskanowaniu przenoszą na zaszyte pod nimi strony, prawda?

W przypadku quishingu po zeskanowaniu takiego kodu, rzekomo prowadzącego do e-płatności lub odbioru nagrody, pobieramy zainfekowany plik lub trafiamy na fałszywą stronę banku czy innej instytucji. Uwaga! Z takimi kodami możecie mieć do czynienia nie tylko w e-mailach czy na stronach internetowych, ale też np. na przystankach komunikacji miejskiej, w klubach, restauracjach czy nawet na ubraniach!

Tak jak w przypadku innych internetowych oszustw, przed quishingiem ochroni nas przede wszystkim zasada ograniczonego zaufania. Gdy po zeskanowaniu kodu cokolwiek wzbudzi Wasze wątpliwości – natychmiast zamknijcie stronę! Jeśli decydujecie się na korzystanie z kodów QR, za każdym razem sprawdzajcie adres strony, na którą zostaniecie przekierowani, i nie podawajcie tam żadnych swoich danych, loginów czy haseł. A jak mieć 100% pewności, że za czarno-białym kodem nie kryje się potencjalnie groźna strona? Jedyną skuteczną metodą jest po prostu… nieskanowanie kodów QR, co do których nie mamy pewności, że są bezpieczne.

Q

Ransomware

To rodzaj złośliwego oprogramowania wykorzystywanego przez przestępców, którego zadaniem jest zaszyfrowanie danych na komputerze ofiary, tak by nie miała do nich dostępu. Atak ma najczęściej na celu wyłudzenie pieniędzy w zamian za odblokowanie systemu – stąd nazwa ransomware, która powstała z połączenia angielskich słów *ransom* (okup) i *software* (oprogramowanie).

Coraz częściej pojawiają się przypadki, kiedy to atakujący nie tylko szyfrują dane, ale także wykradają je, by następnie szantażować ofiarę, grożąc ich ujawnieniem lub poinformowaniem innych o ataku, np. partnerów biznesowych, instytucji współpracujących czy opinii publicznej w przypadku niezapłacenia okupu.

Na tego typu niebezpieczeństwo narażone są przede wszystkim duże firmy i instytucje publiczne, które przechowują dane wrażliwe klientów lub dostarczają kluczowe usługi. Oczywiście ransomware może też przeniknąć do systemu indywidualnego użytkownika – wystarczy, że otworzycie zainfekowany załącznik w e-mailu, zainstalujecie aplikację lub program pochodzący z nieznanego źródła czy klikniecie w natarczywą reklamę.

Jak zabezpieczyć się przed atakiem? Niezawodne rady: na bieżąco aktualizujcie system operacyjny, aplikacje i oprogramowanie – w tym antywirusy. Stosujcie silne, bezpieczne hasła, a najlepiej uwierzytelnianie dwuskładnikowe. Twórzcie też kopie zapasowe (backup), co pomoże Wam odzyskać dane bez potrzeby „negocjacji" z przestępcami. I co najważniejsze – nie dajcie się złapać na haczyk oszustów wykorzystujących akcje phishingowe!

Pamiętajcie, że każde niebezpieczne zdarzenie zawsze możecie zgłosić do zespołu CSIRT NASK. Wystarczy wypełnić formularz na stronie incydent.cert.pl albo wysłać e-mail: cert@cert.pl. Bardziej zaawansowanym użytkownikom nowych technologii polecamy też stronę nomoreransom.org. Za jej pośrednictwem sprawdzicie, czy Wasze urządzenie nie zostało zainfekowane jednym z wariantów oprogramowania ransomware, dla którego udostępniane są bezpłatnie narzędzia do deszyfrowania.

Więcej praktycznych porad, jak postępować w przypadku zainfekowania sprzętu ransomware, znajdziecie na ose.gov.pl w aktualności: „Bezpieczni w sieci z OSE: ransomware".

Regulamin

Najprościej mówiąc, regulamin to zbiór przepisów i rozporządzeń opisujących sposób postępowania w danej sprawie. Z regulaminami spotkacie się praktycznie wszędzie: w bibliotece, na basenie, w pracy, szkole i… w internecie. I choć wszyscy wiemy, że takie dokumenty są, to niestety zbyt rzadko je czytamy.

R

Obowiązki, zakazy, nakazy, paragrafy nie zachęcają do lektury – a niesłusznie. Znajomość regulaminu bardzo pomaga – również w sieci.

Warto znać reguły panujące w wirtualnym świecie i pamiętać, że internauci oprócz obowiązków mają także swoje prawa. Jakie praktyczne wiadomości znajdziecie w regulaminach online? M.in. dokładne dane firmy świadczącej usługi drogą elektroniczną, zasady bezpiecznego korzystania z danego portalu, rejestracji, składania zamówień, reklamacji, zwrotów, dodawania komentarzy, informacje o ochronie danych osobowych…

Zanim jednak zaakceptujecie regulamin – przeczytajcie go! Dlaczego to takie ważne? Zdarza się, że czasem pochopnie zatwierdzicie coś, na co prawdopodobnie nie wyrazilibyście zgody, gdybyście wiedzieli, co kryje dany zapis. W regulaminach np. gier online może być zawarta informacja o dodatkowych opłatach. A jeśli bez zastanowienia zgodzicie się na warunki korzystania z jakiejś aplikacji, Wasze dane lub zdjęcia mogą zostać przekazane innym i dowolnie wykorzystane.

Warto uczulać dzieci, by nie wyrażały zgody na coś, z czym się nie zapoznały lub czego nie rozumieją. Regulaminy często pisane są skomplikowanym językiem, dlatego młodzi internauci przed ich akceptacją powinni zwrócić się o pomoc do rodziców lub opiekunów.

Rootkit

To rodzaj złośliwego oprogramowania (malware). Rootkit daje cyberprzestępcom dostęp do Waszego urządzenia – zarówno do programów, jak i poszczególnych elementów systemu. Jest trudny do zlokalizowania, ponieważ potrafi wyłączać działające zabezpieczenia, niełatwo też jest się go pozbyć. Jeśli już uda się Wam go namierzyć, czasem jedyną deską ratunku jest ponowna instalacja systemu operacyjnego.

Rootkit ma niejedno oblicze. Może zawierać w sobie wiele niebezpiecznych programów typu keylogger, spyware czy moduły przechwytujące hasła. Może też zagnieżdżać się w różnych miejscach systemu czy oprogramowania i niepostrzeżenie wyrządzać szkody.

W przypadku tego typu zagrożenia warto postawić na działania prewencyjne, które sprawdzą się w przypadku każdego ataku typu malware. Nie zapominajcie o aktualizacjach, a przede wszystkim o zasadzie ograniczonego zaufania – z dużą ostrożnością podchodźcie do podejrzanych linków, nietypowych wiadomości, aplikacji i programów pochodzących z nieoficjalnych źródeł!

Rozporządzenie o ochronie danych osobowych (RODO)

Obowiązuje od 2018 r. i określa ramy prawne przetwarzania danych osobowych w Europie. Wymogi RODO (także w internecie!) musi spełniać każda organizacja, która dysponuje naszymi danymi osobowymi, czyli wszelkimi informacjami umożliwiającymi identyfikację, takimi jak: imię i nazwisko, adres

zamieszkania, e-mail czy numer PESEL. Według tego rozporządzenia ochronie podlegają też dane wrażliwe, dotyczące np. zdrowia czy poglądów.

Prawo do ochrony swoich danych osobowych przysługuje wszystkim. Co to oznacza w praktyce? RODO dba, by Wasze dane nie dostawały się w niepowołane ręce i były wykorzystywane w konkretnym celu – o czym powinniście zostać poinformowani. Unijne rozporządzenie mówi też, że w każdej chwili możecie skorzystać z prawa do sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia Waszych danych.

Co ważne – RODO gwarantuje Wam również prawo do bycia zapomnianym. Oznacza to, że możecie zgłosić się do administratora danych (np. Google'a) z prośbą o usunięcie odnośników do stron z treściami na Wasz temat: nieaktualnymi, nieistotnymi lub takimi, które naruszają Wasz wizerunek.

Więcej informacji o RODO znajdziecie w podręczniku Generalnego Inspektora Ochrony Danych Osobowych „Gotowi na RODO".

Równowaga online–offline

Nietrudno zauważyć, że smartfon to nasz najwierniejszy towarzysz, a wpatrywanie się w ekrany urządzeń cyfrowych stanowi nieodłączną część naszego codziennego funkcjonowania. Internet i nowe technologie zawładnęły sercami i umysłami nie tylko dorosłych, ale też dzieci. Potwierdzają to badania – z raportu NASK „Nastolatki 3.0" wynika, że młodzi spędzają online średnio aż 4 godziny i 50 minut dziennie, w weekendy czas ten wydłuża się do ponad 6 godzin na dobę.

Niestety, ciągłe przebywanie w wirtualnym świecie nie służy zdrowiu dziecka, szczególnie jeśli zauważycie, że trudno jest mu funkcjonować bez stałego kontaktu z urządzeniem. Nadużywanie sieci może prowadzić do FOMO (ang. *Fear of Missing Out*), czyli lęku przed odłączeniem. Przymus bycia na bieżąco z newsami, e-mailami, komentarzami i informacjami publikowanymi w mediach społecznościowych, reagowanie na dźwięk każdego powiadomienia – to elementy, które skutecznie odciągają od codziennych obowiązków, dekoncentrują, zaburzają sen i potrzebę dbania o dobre samopoczucie. Stąd tak ważne jest zachowanie równowagi między światem online i offline. Jak to zrobić?

Na początek sprawdźcie, czy problem nadużywania smartfona, komputera, serwisów społecznościowych czy czy gier dotyka Was samych albo Waszego dziecka. Określcie, co sprawia, że tak wiele czasu spędzacie z urządzeniem w ręce – być może w taki sposób radzicie sobie z nudą lub tylko w sieci potraficie się dobrze bawić. Powodów może być wiele. Po diagnozie możecie działać. Ale pamiętajcie: radykalne odłączenie internetu rzadko kiedy przyniesie pożądany efekt. Jeśli na co dzień nie potraficie odłożyć smartfona nawet na chwilę, spędzacie godziny zanurzeni w grze, to trudno Wam będzie z tego

zrezygnować bez przygotowania. Najlepiej stosować metodę małych kroków, przyzwyczajając się stopniowo do bycia offline.

Próbujcie różnych rozwiązań: starannie planujcie czas poza siecią, postawcie na ciekawe aktywności, które wiążą się z odpoczynkiem od cyfrowego przemęczenia. Organizujcie rodzinne wyzwania (offline challenge), wyznaczcie w domu strefy bez urządzeń, odkładajcie telefony przed snem. W budowaniu zdrowych nawyków starajcie się działać zespołowo: z przyjaciółmi, rodzicami, rodzeństwem – w grupie raźniej!

Więcej ciekawych porad znajdziecie na ose.gov.pl w wywiadzie „5 pytań o… równowagę cyfrową”. Zachęcamy też do skorzystania z naszego bezpłatnego kursu e-learningowego dla dorosłych „Zrozumieć FOMO” oraz innych materiałów edukacyjnych dostępnych na platformie OSE IT Szkoła – informacje o nich znajdziecie w tekście „Niebezpieczne zjawiska w internecie: FOMO”.

Scam

Internetowi oszuści stają się coraz bardziej przebiegli. Zdarza się, że skutecznie działają na naszą wyobraźnię, oferując wartościową nagrodę lub wysokie zarobki, chcąc skłonić nas do powierzenia im swoich danych osobowych, a nawet środków finansowych. Takie formy oszustwa nazywamy scamem.

Najczęstszą formą scamu jest masowa korespondencja elektroniczna (spam), jednak cyberprzestępcy grają na naszych emocjach również podczas kontaktów telefonicznych (spoofing, vishing). Ofiara jest przekonana, że odbiera telefon od policjanta, urzędnika czy też pracownika banku, dlatego bez oporów wykonuje wszelkie polecenia, np. podaje swoje dane osobowe lub dane do logowania. Scamerzy korzystają też z formularzy i fałszywych stron internetowych do złudzenia przypominających prawdziwe witryny banku czy urzędu. Bywa, że wysyłają e-maile, w których nakłaniają do kliknięcia linków prowadzących do takich stron.

Oferty produktów w niskich cenach, nagrody bez udziału w konkursach, obietnica spadku po dalekim krewnym – to tylko niektóre przykłady scamu. Jak się przed nim chronić? Zachowujcie czujność i pamiętajcie o zasadzie ograniczonego zaufania. Nie klikajcie w podejrzane linki, weryfikujcie wszystkie „okazje" w sieci, a przede wszystkim… nie wierzcie, że wszystko, co widzicie w internecie, jest prawdziwe.

Self generated sexual content

To pojęcie wiąże się z ryzykownymi działaniami podejmowanymi przez dzieci i nastolatki. Self generated sexual content (z ang. treści wytwarzane samodzielnie) to zdjęcia, filmy czy pokazy (np. udostępniane na serwisach streamingowych) o charakterze erotycznym lub pornograficznym, wykonywane samodzielnie, choć nie zawsze dobrowolnie, przez osoby poniżej 18. roku życia. Takie materiały są szczególnym rodzajem szkodliwych treści – to treści nielegalne.

Self generated sexual content prezentują dziecko np. częściowo rozebrane, w bieliźnie lub nago, przyjmujące erotyczne pozy, czasami podejmujące różne czynności seksualne czy też naśladujące je. Dlaczego dzieci i nastolatki wytwarzają takie materiały? Powody są różne – może to być m.in. skutek uwodzenia dziecka przez internet (child grooming) czy sextortion.

Polskie prawo chroni osoby nieletnie przed produkowaniem lub utrwalaniem treści pornograficznych z ich udziałem. Zabrania także rozpowszechniania, utrwalania, sprowadzania, przechowywania, posiadania i uzyskiwania dostępu do takich materiałów.

Jeżeli natkniecie się w sieci na materiały self generated sexual content lub ofiarą stanie się Wasze dziecko albo uczeń – niezwłocznie reagujcie!

Poinformujcie o tym fakcie działający w NASK zespół Dyżurnet.pl, czyli punkt kontaktowy do zgłaszania nielegalnych treści w internecie, szczególnie związanych z seksualnym wykorzystywaniem dzieci. Możecie to zrobić: wypełniając formularz, wysyłając e-mail na adres dyzurnet@dyzurnet.pl lub dzwoniąc pod numer 801 615 005. O takim niebezpiecznym zdarzeniu powinniście też szybko poinformować policję.

Więcej wiadomości na temat self generated sexual content oraz porady, jak reagować na zagrożenia związane z sextingiem, znajdziecie w materiałach na naszych stronach OSE IT Szkoła i ose.gov.pl: poradniku „Sexting i nagie zdjęcia w sieci", webinarze „Sexting i nagie zdjęcia w sieci – profilaktyka i reagowanie" oraz aktualnościach „Niebezpieczne zjawiska w internecie: self-generated sexual content" i „5 pytań o… sexting".

Sexting

Zapewne zdajecie sobie sprawę, że w ostatnich latach, w związku z ułatwionym dostępem do internetu i urządzeń cyfrowych, problem wytwarzania i udostępniania przez uczniów intymnych materiałów staje się coraz powszechniejszy. Jednym z nasilających się zagrożeń jest sexting – ryzykowne zachowanie polegające na przesyłaniu innym osobom intymnych wiadomości tekstowych i erotycznych plików multimedialnych.

Na początku sexting dotyczył przede wszystkim tych, którzy pozostawali w związkach lub w bliskiej relacji. Wraz z rozwojem nowoczesnych technologii zaczął przyjmować nieco inną formę. Nie są to już tylko wiadomości tekstowe, ale przede wszystkim zdjęcia czy filmy, które przedstawiają ich twórców w intymnej, erotycznej sytuacji.

Sexting dla wielu młodych ludzi jest formą flirtu lub żartu. Z jednej strony pozwala na wyrażenie zainteresowania drugą osobą, bywa też sposobem na przeżywanie pierwszych doświadczeń i fascynacji seksualnych, a z drugiej – może prowadzić do niebezpiecznych sytuacji oraz utraty kontroli nad własnym wizerunkiem online.

Zdarza się, że dzieci i nastolatki, których intymne fotografie lub filmy zostały udostępnione, doświadczają przemocy zarówno online, jak i w świecie realnym, np. ze strony rówieśników. Ofiarom sextingu mogą towarzyszyć trudne emocje związane ze wstydem, lękiem, ośmieszeniem.

Badania wskazują, że 42% młodych ludzi w wieku 15–18 lat otrzymało od kogoś nagie zdjęcie lub film, a 13% wysłało takie materiały innej osobie (Makaruk, Włodarczyk, Michalski, 2017).

W niektórych przypadkach sexting może nosić znamiona przestępstwa związanego z produkcją materiałów pornograficznych z udziałem osoby niepełnoletniej (art. 202 § 3 Kodeksu karnego). Warto wiedzieć, że polskie prawo chroni osoby poniżej 18. roku życia przed produkowaniem lub utrwalaniem treści pornograficznych z ich udziałem. Zabrania też rozpowszechniania,

utrwalania, sprowadzania, przechowywania, posiadania czy nawet uzyskiwania dostępu do takich materiałów.

Więcej na temat sextingu dowiecie się z poradnika dla nauczycieli „Sexting i nagie zdjęcia w sieci". Zachęcamy także do zapoznania się z infografikami, eksperckim webinarem, scenariuszem zajęć „Decyzja" dostępnymi na platformie OSE IT Szkoła oraz aktualnościami: „Temat lekcji: sexting" i „5 pytań o... sexting" na stronie ose.gov.pl.

Sextortion

Z sextingiem wiąże się inne niebezpieczne zjawisko – sextortion, czyli pozyskanie od ofiary materiałów o charakterze seksualnym i późniejsze wymuszenie okupu (pieniędzy albo kolejnych treści pod groźbą ich opublikowania lub dalszego rozpowszechniania). Ofiarą takiego szantażu może paść każdy – dzieci, młodzież i dorośli, bez względu na płeć czy miejsce zamieszkania.

Sprawcy sextortion próbują coraz nowszych i skuteczniejszych metod pozyskania zdjęć lub filmów od potencjalnej ofiary. Szukają osób, które łatwo zmanipulować, które chętnie nawiązują kontakty z nieznajomymi i są gotowe do dzielenia się treściami o charakterze seksualnym. Zdarza się też, że sextortion jest jedną z konsekwencji sextingu.

Pamiętajcie: sextortion to nie tylko zagrożenie internetowe, ale przede wszystkim przestępstwo, które należy zgłosić (art. 190 oraz 191a Kodeksu karnego) na policję.

Sharenting

Dokumentowanie życia dziecka w internecie stało się co najmniej powszechnym zjawiskiem, o ile nie normą społeczną wśród współczesnych rodziców. Z sharentingiem (od ang. *share* – dzielić się oraz *parenting* – rodzicielstwo) mamy do czynienia na portalach społecznościowych, blogach, forach dyskusyjnych, czyli wszędzie tam, gdzie szczegółowe informacje, zdjęcia i filmy z życia dzieci znajdą szerokie grono odbiorców. Jednak czy mamy świadomość, że fotka naszego dziecka niespodziewanie może obiec interent, stać się memem, trafić w niepowołane ręce lub przyczynić się do cyberprzemocy?

Wielość materiałów zamieszczanych przez rodziców w sieci przyprawia o zawrót głowy. Wielu z nich dokumentuje każdy moment codziennego życia swoich pociech (publikują nawet zdjęcia USG nienarodzonych jeszcze dzieci), a często także śmieszne lub wzruszające scenki z ich udziałem. Zdarza się, że takie treści zdradzają więcej niż powinny: opiekunowie opatrują je komentarzami zawierającymi wiele szczegółów z życia dziecka, np. imię, wiek, datę urodzin, nazwę szkoły lub przedszkola, do którego chodzi. Takie informacje, mimo że podane w dobrej wierze, mogą realnie zagrozić bezpieczeństwu dziecka!

Jak bezpiecznie dzielić się zdjęciami swoich dzieci w internecie? Przede wszystkim róbcie to z głową – pamiętajcie, że mniej znaczy więcej i że Wasze działania dzisiaj kształtują wizerunek dziecka w przyszłości, także ten online. Zanim wrzucicie coś do sieci, zastanówcie się, czy materiał może narazić dziecko na śmieszność, upokorzenie bądź krytykę, czy nie prezentuje intymnych treści. Ograniczajcie widoczność zdjęć czy filmików i przede wszystkim – pytajcie dziecko o zgodę przed ich publikacją!

Więcej porad dotyczących udostępniania zdjęć swoich dzieci online znajdziecie w naszym poradniku dla rodziców „Sharenting i wizerunek dziecka w sieci" i kursie e-learningowym „Sharenting. Czy warto mieć rodzinny album w sieci?" na platformie OSE IT Szkoła, webinarze eksperckim „Rodzinny album z wakacji, czyli czego o dzieciach nie powinien wiedzieć internet" oraz w aktualnościach „Dzielisz się zdjęciem dziecka w sieci? Rób to z głową!" i „Zdjęcia dziecka w sieci? Zastanów się, zanim opublikujesz" na stronie ose.gov.pl.

Skimming

Wypłacając gotówkę w bankomacie, zwłaszcza położonym na uboczu lub w obcym miejscu, musimy mieć oczy i uszy szeroko otwarte – w przeciwnym razie możemy paść ofiarą przestępstwa zwanego skimmingiem. Jest to oszustwo polegające na kopiowaniu przez złodzieja zawartości paska magnetycznego lub chipa z karty płatniczej, prowadzące do obciążenia rachunku bankowego okradanej osoby.

Sprawcy przy pomocy tzw. skimmera – specjalnego urządzenia kopiującego umieszczanego w bankomacie – przechwytują informacje zawarte na karcie. Towarzysząca urządzeniu kopiującemu mikrokamera lub specjalna nakładka na klawiaturę pozwalają ponadto rejestrować wpisywany przez użytkownika PIN. Jak się ustrzec przed utratą gotówki? Korzystajcie z bankomatów położonych w uczęszczanych i dobrze oświetlonych miejscach, rezygnujcie z wypłat, gdy cokolwiek wzbudzi Wasze podejrzenia. Jak oka w głowie strzeżcie też swojej karty i numeru PIN – nie przekazujcie karty innym osobom i nie zapisujcie numeru PIN na karteczce noszonej w portfelu ani na samej karcie płatniczej.

Więcej o skimmingu dowiecie się z poradnika „Bezpieczeństwo online w szkołach OSE" (cz. 2) dostępnego na platformie OSE IT Szkoła i aktualności „Skimming, czyli co się może kryć w bankomacie" na ose.gov.pl.

Smishing

Wiecie już, czym jest phishing – to metoda oszustwa, w której przestępca podszywa się pod inną osobę bądź zaufaną instytucję, by wyłudzić od ofiary poufne informacje, nakłonić ją do określonych działań czy zainfekować jej urządzenie szkodliwym oprogramowaniem. Jednym z rodzajów phishingu jest smishing, w którym drogą ataku są wiadomości tekstowe lub SMS.

Wiadomość z żądaniem niewielkiej dopłaty do przesyłki od firmy kurierskiej czy do ostatniego rachunku za prąd od dostawcy energii, SMS z banku o blokadzie

naszego konta wraz z linkiem do jego odblokowania albo przypomnienie o rozliczeniu podatku – to tylko niektóre przykłady smishingowych wiadomości. Oszuści stają się coraz bardziej wyrafinowani i do swoich ataków wykorzystują często aktualne wydarzenia.

Dlaczego SMS-y, a nie e-maile, jak podczas tradycyjnych oszustw phishingowych? Oszuści wysyłają wiadomości na przypadkowe numery (mają do dyspozycji dużą, ale przecież ograniczoną pulę dziewięciocyfrowych numerów) – wiedzą, że część z nich trafi do realnych odbiorców, którzy odpowiedzą na SMS.

Antidotum na smishing po raz kolejny okazują się zdrowy rozsądek i podejrzliwość. Chcecie dowiedzieć się więcej? Sięgnijcie do biuletynu „OUCH! – Powstrzymać phishing" oraz naszej aktualności „Bezpieczni w sieci z OSE: phishing".

Smombie

Smartfonowy zombie, czyli smombie („smartfon" + „zombie"), zapewne nie raz był Waszym towarzyszem podróży, mogliście go spotkać też w kinie, teatrze, kościele czy nawet na pasach. To osoba, która godzinami wpatruje się w ekran swojego urządzenia, nie zauważa innych ludzi i rzeczy dookoła siebie. Nierzadko swoim zachowaniem stwarza realne zagrożenie, np. nie zwracając uwagi na przejeżdżające pojazdy.

Dla smombie przymus sięgnięcia po telefon jest silniejszy od czegokolwiek innego. Tak, ten stan jest jednym ze skutków FOMO, czyli lęku przed odłączeniem od sieci. W ten sposób objawiają się zaburzenie równowagi online–offline i pilna konieczność zadbania o cyfrową higienę.

Jak wrócić do realnego świata? Małymi krokami. Warto zacząć od poszukiwania alternatywy dla smartfona oraz ograniczenia kontaktu z ekranem urządzenia, np. podczas posiłków czy spotkań z bliskimi. Pomoże też wyznaczenie stref offline, gdzie wszyscy domownicy będą odkładać i ładować swoje urządzenia. A może #offlinechallenge?

Jeśli chcecie dowiedzieć się więcej na temat smombie, zajrzyjcie na ose.gov.pl do naszej aktualności „Smombie są wśród nas".

Social media sabbatical

Media społecznościowe umożliwiają podtrzymywanie kontaktów, dla wielu są też odskocznią od codziennych obowiązków. To ważny element wirtualnego, a jednocześnie bardzo realnego życia – szczególnie dla młodych użytkowników sieci. Badania potwierdzają, że ich aktywności online najczęściej dotyczą właśnie social mediów. Z naszego raportu „Nastolatki 3.0" wynika, że młodzież powszechnie korzysta m.in. z komunikatorów i serwisów społecznościowych – tylko 0,7% respondentów wskazało, że ich nie używa.

Tymczasem zbytnie przywiązanie do sieci i urządzeń cyfrowych może powodować przemęczenie nadmiernym obciążeniem informacjami, prowadzić do FOMO (ang. *Fear of Missing Out*), czyli lęku przed odłączeniem, a nawet uzależnienia. Jest na to rada – czasem warto po prostu pozostać offline chwilę dłużej i skupić się na aktywnościach poza siecią. Jak to zrobić?

Social media sabbatical oznacza właśnie świadomą, zaplanowaną, dłuższą przerwę od portali społecznościowych, by odzyskać równowagę online–offline. Zanim jednak postanowicie odłączyć się do sieci, warto się do tego dobrze przygotować. Ustalcie datę i poinformujcie znajomych o zniknięciu z internetu. Dokładnie zaplanujcie też czas offline – zróbcie coś, o czym dawno myśleliście, ale nie mieliście na to czasu. Ciekawy kurs, sport lub czytanie zaległych książek – brzmi świetnie, prawda? Podczas odłączenia od social mediów przyglądajcie się sobie. Być może odkryjecie, że odcięcie od wirtualnego świata przyniosło same dobre doświadczenia. Albo wręcz przeciwnie – bez mediów społecznościowych czuliście przygnębienie, obawy, irytację.

Po powrocie do popularnych serwisów społecznościowych starajcie się kontrolować czas spędzany w sieci. Uważajcie też, by stale napływające z internetu informacje, posty, komentarze znajomych i powiadomienia z komunikatorów nie pochłonęły Was zbyt mocno.

Więcej przydatnych informacji znajdziecie na ose.gov.pl w aktualności „Czas na social media sabbatical?”.

Spam

Najprościej mówiąc, spam to niechciane wiadomości przesyłane drogą e-mailową, SMS-ową lub za pośrednictwem serwisów społecznościowych. Termin pochodzi od… mielonki (oszukanego, mało wartościowego mięsa), co raczej nie budzi dobrych skojarzeń.

Czym charakteryzuje się spam? Wysyłany jest do wielu nadawców, przez co nie jest spersonalizowany. Zazwyczaj zawiera informacje marketingowe, ale też propagandowe. Spam to również narzędzie popularne wśród cyberprzestępców! Za jego pomocą oszuści stosują np. phishing, czyli wysyłają wiadomości, które zawierają m.in. zainfekowane załączniki lub linki kierujące do niebezpiecznych witryn internetowych. Celem ataku jest wyłudzenie poufnych danych – loginów i haseł do bankowości internetowej lub serwisów społecznościowych – a nawet zainfekowanie urządzenia ofiary złośliwym oprogramowaniem (malware) i przejęcie nad nim kontroli.

Specjalnie przygotowany spam potrafi wyglądać bardzo wiarygodnie, ponieważ oszuści często podszywają się pod znane firmy i instytucje. Spreparowana wiadomość ma skłonić ofiarę do działania – nagminne jest straszenie, że wydarzy się coś złego, jeśli nie podąży za otrzymaną instrukcją. Niestety, spełnienie próśb nadawcy kończy się źle dla odbiorcy – najczęściej utratą środków na koncie.

Sposób na niechciane wiadomości? Korzystajcie ze skrzynek pocztowych wyposażonych w filtr antyspamowy. Podczas rejestracji na portale czy do sklepów internetowych korzystajcie z adresu e-mail stworzonego specjalnie do tego celu. Na bieżąco usuwajcie wiadomości, które zaśmiecają Waszą skrzynkę.

I pamiętajcie – podejrzane e-maile lub SMS-y możecie zgłaszać do CERT Polska. Wystarczy, że otrzymaną na telefon wiadomość wyślecie na numer 799 448 084, używając funkcji „przekaż" albo „udostępnij". Natomiast informację o stronach internetowych służących do wyłudzania danych osobowych i uwierzytelniających możecie przesłać za pomocą formularza.

Spoofing

To rodzaj popularnego oszustwa polegający na podszywaniu się pod konkretną osobę lub podmiot (np. instytucję, firmę) w celu pozyskania istotnych informacji lub wyłudzenia pieniędzy. Termin powstał od ang. słowa *spoof* – naciąganie, szachrajstwo – i odnosi się do różnych typów ataków. Wyróżniamy np. spoofing telefoniczny, e-mail, IP i DNS.

W ostatnim czasie popularną formą oszustwa stał się spoofing telefoniczny. Przestępcy przejmują wybrany numer telefonu i dzwonią do ofiary, podając się np. za pracownika banku, przedstawiciela znanej instytucji czy osobę publiczną. Żądają przykładowo zainstalowania wskazanej aplikacji, która ma nas rzekomo uchronić przed utratą pieniędzy. Bezrefleksyjne spełnienie prośby to prosty krok do przekazania cyberprzestępcom zdalnego dostępu do urządzenia użytkownika, a co za tym idzie – utraty danych lub środków na koncie.

Spoofing e-mail również nie traci na popularności. Waszą czujność powinna wzbudzić każda podejrzana wiadomość, w której nadawca – na pierwszy rzut oka wiarygodny – prosi o podanie poufnych danych czy loginów i haseł do bankowości internetowej.

Najtrudniej jest rozpoznać spoofing IP lub DNS. Metoda ta polega na przekierowaniu internauty na fałszywą stronę, która do złudzenia przypomina tę oryginalną. Nietrudno się domyślić, że korzystanie z platformy przygotowanej przez przestępców naraża sprzęt ofiary na zainfekowanie złośliwym oprogramowaniem, a w konsekwencji na poważne straty.

Jak chronić się przed spoofingiem? Włączcie zasadę ograniczonego zaufania. Nie odpowiadajcie na żadne próby wyłudzenia poufnych informacji, sprawdzajcie dokładnie, czy na pewno logujecie się w oknie prawdziwej strony, omijajcie szerokim łukiem te platformy, które po prostu wydają się Wam dziwne. Podejrzane witryny zgłaszajcie do CERT Polska za pośrednictwem formularza na stronie incydent.cert.pl. A jeśli macie podejrzenie, że doszło do kontaktu telefonicznego z potencjalnym oszustem, rozłączcie się i sprawdźcie (np. dzwoniąc do banku), czy taka rozmowa w ogóle powinna mieć miejsce.

Więcej informacji o spoofingu telefonicznym znajdziecie na ose.gov.pl w aktualności „Uwaga na spoofing!".

Spyware (oprogramowanie szpiegujące)

W internecie nic nie ginie i nie do końca możemy pozostać anonimowi – to prawda stara jak (przynajmniej ten cyfrowy) świat. Niestety zdarza się, że nasze poczynania w sieci są bacznie śledzone, a dzieje się to za pomocą złośliwego oprogramowania szpiegującego (ang. *spyware*).

Oprogramowanie to zaraża komputer, telefon lub inne urządzenie, aby gromadzić nasze dane oraz ważne informacje, np. o sposobach korzystania z internetu. Złośliwe działania tych programów obejmują przechwytywanie naciśnięć klawiszy (keylogger), zrzutów ekranu, poświadczeń uwierzytelniających, danych z formularzy internetowych i innych danych osobowych, w tym numerów kart kredytowych.

Oprogramowanie szpiegujące rozprzestrzenia się w formie trojanów, wirusów i innych złośliwych programów. Uważajmy też na pozornie przydatne narzędzia czy aplikacje, darmowe oprogramowanie, a nade wszystko – linki i załączniki w podejrzanych e-mailach.

Zła wiadomość jest taka, że programy szpiegujące są wyjątkowo podstępne: zwykle instalują się na urządzeniach bez naszej wiedzy i zgody, a następnie działają w tle, zbierając informacje i wywołując szkodliwe skutki. Nawet gdy wykryjemy obecność szpiega w systemie operacyjnym, nie będzie łatwo go odinstalować!

Na szczęście jest światełko w tunelu. Aby chronić się przed oprogramowaniem szpiegującym, nadrzędne jest zachowanie zasady ograniczonego zaufania – nie otwierajcie wiadomości od nieznanych nadawców, nie klikajcie w podejrzane linki i nie pobierajcie załączników (chyba że pochodzą z pewnego źródła). Zawczasu zaopatrzcie się też w program antywirusowy, który zapewnia ochronę w czasie rzeczywistym i zablokuje potencjalnego szpiega, zanim ten zdąży uruchomić się na komputerze.

Stalking

To uporczywe nękanie, prześladowanie drugiej osoby, które powoduje u ofiary napięcie, stres, strach i poczucie utraty bezpieczeństwa nosi znamiona stalkingu. Działania stalkera mogą doprowadzić do dużych strat emocjonalnych, a nawet materialnych, gdy osoba pokrzywdzona będzie zmuszona np. do ciągłej zmiany numeru telefonu lub rezygnacji z pracy. Stalking – tak jak większość działań przemocowych – przeniósł się też do sieci.

Cyberstalking jest formą nękania drugiej osoby w internecie, co oczywiście ma wpływ na jej codzienne funkcjonowanie i powoduje znaczne szkody psychiczne. Zarówno stalking, jak i cyberstalking jest przestępstwem – wszelkie przejawy uporczywego nękania zgłaszajcie na policję!

Zapoznajcie się z publikacją „Bezpieczeństwo online w szkołach Ogólnopolskiej Sieci Edukacyjnej, cz. 2” dostępną na portalu OSE IT Szkoła i poznajcie procedurę reagowania na prześladowanie ucznia w internecie.

Stealware

Zapewne wiecie, że istnieje wiele szkodliwych programów, które potrafią działać niepostrzeżenie, a jednocześnie wyrządzać duże szkody. Jednym z nich jest oprogramowanie szpiegujące stealware, które zbiera informacje o użytkowniku, by następnie przekazać pozyskane dane osobom trzecim.

Oprogramowanie tego typu oczywiście instalowane jest bez wiedzy ofiary. Przedostaje się do systemu za pomocą odpowiednio przegotowanych robaków i wirusów oraz dzięki wykorzystaniu luk czy błędów w przeglądarkach internetowych. Stealware potrafi np. śledzić aktywność użytkownika na platformach z płatnością elektroniczną, by w odpowiednim momencie podmienić numer konta, przez co jego środki trafią do zupełnie innego odbiorcy niż zamierzał.

Jak chronić się przed stealware? Przede wszystkim unikajcie pobierania „przydatnych”, darmowych narzędzi z nieznanych źródeł. Ponadto dbajcie o swoje urządzenia – aktualizujcie system, programy, antywirusy. Nie klikajcie w podejrzane linki i reklamy. Bądźcie czujni!

Szkodliwe treści

W internecie znajdziemy z jednej strony pozytywne i inspirujące materiały, a z drugiej – takie, które mogą zaniepokoić, budzić złość, szokować. Szkodliwe treści wpływają negatywnie szczególnie na młodych internautów. Zaliczamy do nich m.in. materiały przedstawiające przemoc, pokazujące zachowania niebezpieczne dla zdrowia i życia (samookaleczenia, restrykcyjne diety, zażywanie szkodliwych substancji, samobójstwa, ryzykowne wyzwania), pornografię, treści szerzące mowę nienawiści, fake newsy czy patostreamy, czyli relacje online na żywo prezentujące zachowania określane i postrzegane jako patologiczne.

O ile sporadyczny kontakt dziecka z nieodpowiednimi materiałami może oddziaływać na jego samopoczucie, o tyle ich regularne oglądanie ma już destrukcyjny wpływ na rozwój, psychikę, postrzeganie świata. Szkodliwe treści narażają też młodych internautów na niebezpieczeństwa. Przykładowo popularne internetowe wyzwania – challenge, podczas których dziecko ma wykonać jakieś niebezpieczne zadanie, mogą prowadzić do negatywnych skutków zdrowotnych, a nawet zagrażać życiu.

Jak zapobiegać kontaktowi ze szkodliwymi treściami? Na pewno nie jesteście w stanie kontrolować każdego kroku dziecka w sieci, szczególnie jeśli już samodzielnie korzysta z internetu. Postawcie więc na profilaktykę: odpowiednie zabezpieczenie urządzenia dziecka, aby minimalizować kontakt

z nieodpowiednimi treściami, oraz naukę właściwego reagowania na niebezpieczne sytuacje w sieci.

W domu towarzyszcie dziecku w wirtualnym świecie, interesujcie się tym, co ogląda, jakie strony odwiedza. Wspólnie ustalcie też zasady korzystania z internetu. W przypadku starszych dzieci podstawą jest rozmowa i edukacja na temat cyberzagrożeń, u młodszych sprawdzi się np. aplikacja ochrony rodzicielskiej – mOchrona. Pamiętajcie też o wyborze odpowiednich dla wieku dziecka gier komputerowych – kierujcie się przy tym ogólnoeuropejskim systemem klasyfikowania gier (PEGI), który określa, jaka rozrywka będzie dla niego bezpieczna. W szkole rozmawiajcie o bezpieczeństwie w sieci już z najmłodszymi dziećmi, uczcie krytycznego podchodzenia do informacji znalezionych online, promujcie pozytywne treści.

Jeśli doszło do kontaktu dziecka ze szkodliwymi materiałami – reagujcie, zarówno w domu, jak i w szkole. Otoczcie dziecko opieką, wysłuchajcie, okażcie wsparcie. Niektóre szkodliwe treści mogą bardzo ciekawić dzieci, wywoływać ekscytację (np. kontakt z pornografią czy patostreamami) – nie oceniajcie, tylko starajcie się zrozumieć, dlaczego dziecko się nimi interesuje, wyjaśniajcie też różnicę między prezentowanymi treściami a tym, jak wygląda prawdziwe życie. Z pomocą zawsze przyjdą specjaliści – korzystajcie z telefonów zaufania (helpline).

Pamiętajcie też, że szkodliwe treści nie zawsze naruszają prawo, ale są wyjątki. Rozpowszechnianie materiałów m.in. związanych z seksualnym wykorzystywaniem dzieci jest karalne! Takie przypadki bezwzględnie zgłaszajcie na policję, możecie również skorzystać z pomocy zespołu Dyżurnet.pl.

Chcecie uzyskać więcej informacji na temat tego zagrożenia? Skorzystajcie z naszych materiałów dostępnych na platformie OSE IT Szkoła. Nauczycielom polecamy poradnik: „Szkodliwe treści w internecie”, scenariusz zajęć „Ryzykowne zachowania w internecie: szkodliwe treści” oraz webinar „Szkodliwe treści w internecie. Profilaktyka i reagowanie”. Rodzicom natomiast – poradnik „Szkodliwe treści w internecie. Nie akceptuję, reaguję!”.

Tabnabbing

To rodzaj phishingu polegający na podmianie zawartości strony internetowej. Jego celem jest wyłudzenie danych, do którego dochodzi po zalogowaniu się na fałszywej stronie, spreparowanej przez cyberprzestepcę.

Tabnabbing wykorzystuje Waszą nieuwagę i… nawyk korzystania z wielu kart w przeglądarce. W jaki sposób? Przestępca monitoruje ruch na złośliwej stronie i gdy zauważy, że przeglądacie inną zakładkę, przystępuje do ataku. Podmienia zawartość nieużywanej strony na swoją – fałszywą (która udaje np. popularny serwis społecznościowy, pocztę e-mail, a nawet stronę bankowości internetowej) i próbuje wyłudzić od Was dane logowania – np. zmuszając do ponownego zalogowania się do konta, z którego pozornie zostaliście wylogowani.

Ponieważ oszuści zwykle wykorzystują w tabnabbingu falsyfikaty popularnych stron – które często mamy stale otwarte w kartach przeglądarek – to zauważenie potencjalnego niebezpieczeństwa może być bardzo trudne.

Więcej o ochronie przed phishingiem dowiecie się z biuletynu „OUCH! – Powstrzymać phishing" oraz aktualności ose.gov.pl „Bezpieczni w sieci z OSE: phishing". Młodsi uczniowie mogą zaś poszerzyć swoją wiedzę z kursem e-learningowym „Krasnoludki 2.0 – Phishing, czyli kłopoty to nasza specjalność" dostępnym na platformie OSE IT Szkoła.

Techniczny Reprezentant Szkoły (TRS)

To hasło zapewne wielu z Was jest bardzo dobrze znane – w końcu Techniczni Reprezentanci Szkół codziennie wspierają proces dostarczania i utrzymania infrastruktury Ogólnopolskiej Sieci Edukacyjnej (OSE) w szkołach.

TRS to osoba lub podmiot, który został upoważniony przez dyrektora szkoły do kontaktów z operatorem OSE w sprawach technicznych. Jego zadania to m.in.: administrowanie szkolnymi sieciami LAN, konfiguracja urządzeń czy bieżąca współpraca z Centrum Kontaktu OSE. Dzięki pracy TRS-ów nauczyciele i uczniowie mogą cieszyć się możliwościami szybkiego i bezpiecznego internetu OSE w swoich szkołach.

Teorie spiskowe

Internet to potężna baza informacji, opinii, różnego rodzaju przekazów – nie zawsze wiarygodnych, a niekiedy wręcz szkodliwych dla odbiorców. Obok fake newsów i dezinformacji w sieci możecie się natknąć też na teorie spiskowe. Czym są i co powinniście o nich wiedzieć? To hipotezy próbujące wyjaśnić zjawiska lub sytuacje we własny, zwykle kontrowersyjny sposób, rozbieżny z powszechnie uznaną wersją wydarzeń i faktów. Teorie te zakładają istnienie intryg i spisków dotyczących pewnej grupy wpływowych ludzi, którzy działając

świadomie i w ukryciu, współpracują ze sobą celem osiągnięcia jakichś korzyści – często szkodliwych dla reszty społeczeństwa.

Teorie spiskowe upraszczają świat, zwykle tłumacząc różne zjawiska w kontekście walki o władzę i wpływy. Mogą nawiązywać np. do historii, nauki czy polityki, zniekształcać fakty lub manipulować nimi tak, aby pasowały do stawianych przez ich twórców hipotez. Często pojawiają się jako logiczne wyjaśnienie trudno zrozumiałych wydarzeń lub sytuacji, co może dać fałszywe poczucie kontroli i sprawczości. Pamiętajcie jednak, że te sensacyjne teorie nie mają wiarygodnego potwierdzenia!

Jakie są wspólne cechy teorii spiskowych? To m.in. wiara w domniemany tajny spisek i aktywną grupę spiskowców, dzielenie ludzi na dobrych i złych, wzmacnianie w odbiorcach przekonania, że należą do grupy „wybranych", którzy poznali niedostępną innym prawdę, czy prezentowanie „dowodów" rzekomo mających potwierdzać wymyśloną teorię.

Więcej na temat teorii spiskowych, fake newsów i dezinformacji dowiecie się z materiałów dostępnych na platformie OSE IT Szkoła: konspektu zajęć „Fake newsy i dezinformacja – o tym warto porozmawiać w szkole" oraz ulotki „Fake newsy, bańki informacyjne, teorie spiskowe". Zapoznajcie się też z raportem NASK „Zjawisko dezinformacji w dobie rewolucji cyfrowej".

Troll parenting

To ściśle związane z sharentingiem pojęcie odnosi się do zachowania rodziców, które polega na dzieleniu się w internecie (np. w mediach społecznościowych) materiałami ośmieszającymi ich dzieci lub ukazującymi je w sytuacjach trudnych, wstydliwych, a nawet upokarzających. Takimi treściami mogą być zdjęcia lub filmiki wideo prezentujące dzieci np. przebrane w dziwne kostiumy, płaczące, ubrudzone, włożone „dla żartu" do garnka lub piekarnika czy ubrane w spodnie z mokrą plamą, opatrzone pseudozabawnym podpisem.

Dlaczego rodzice podejmują takie bezmyślne działania? Powodem może być m.in. spontaniczna potrzeba podzielenia się z innymi pozornie śmieszną sytuacją z życia dziecka, a nawet zaplanowane działanie. Należy pamiętać, że troll parenting, tak jak sharenting, może być dla dziecka źródłem wielu nieprzyjemności. Udostępnione zdjęcie lub film może stać się np. memem, narażać dziecko na agresję w sieci (cyberprzemoc) i hejt. A ponieważ w internecie nic nie ginie, taka historia zostanie z dzieckiem na długo i będzie mu towarzyszyć nawet w dorosłym życiu. Dbajcie więc o rozważne dzielenie się materiałami w sieci.

Wskazówki dotyczące udostępniania zdjęć dzieci w internecie znajdziecie na platformie OSE IT Szkoła w poradniku „Sharenting i wizerunek dziecka w sieci", e-kursie „Sharenting. Czy warto mieć rodzinny album w sieci?", publikacji „Bezpieczeństwo dzieci i młodzieży online" oraz na ose.gov.pl w aktualności „Dzielisz się zdjęciem dziecka w sieci? Rób to z głową!".

Trolling w sieci

Czy zdarzyło Wam się kiedyś zetknąć w sieci – np. na forach, w mediach społecznościowych – z internautą, który celowo publikował kontrowersyjne lub prowokacyjne treści, tylko po to, by doprowadzić do kłótni lub wprowadzić innego użytkownika w błąd? Jeśli tak, prawdopodobnie spotkaliście internetowego trolla. To osoba lub program, który wykorzystuje narzędzia komunikacji cyfrowej do osiągania celów określanych jako antyspołeczne.

Trolling zaczerpnął swoją nazwę od angielskiego określenia *trolling for fish*, czyli łowienia ryb na rzucającą się w oczy przynętę. W tym przypadku haczykiem – na który wabi się użytkowników sieci – są zaczepne, często agresywne i wrogie komentarze lub prowokujące odpowiedzi. Katalog trollerskich zachowań jest szeroki i znajdziemy w nim zarówno pozornie nieszkodliwe memy, łańcuszki lub żartobliwe wyzwania (tzw. challenge), jak i zaplanowane, zorganizowane groźne akcje dezinformujące odbiorców.

Z przykładami trollingu możemy się zetknąć w sieci niemal na każdym kroku – np. w komentarzach lub postach w social mediach, artykułach, na blogach czy forach dyskusyjnych. Celem złośliwych internautów jest utrudnianie komunikacji, skłócenie stron zaangażowanych w dyskusję, sianie dezinformacji, kreowanie nieprawdziwego obrazu rzeczywistości, a nawet… szerzenie propagandy!

Nie dajcie się złapać na haczyk internetowych trolli! Jeśli zetkniecie się z nimi w sieci, najlepszym działaniem jest niepodejmowanie dyskusji. Każda Wasza reakcja – łapka w dół, komentarz czy udostępnienie – będzie skutkować zwiększeniem zasięgów przekazu trolla, co przełoży się na dotarcie do jeszcze większej liczby użytkowników.

Zapoznajcie się też z aktualnością ose.gov.pl „Bezpieczni w sieci z OSE: trolling w mediach społecznościowych” oraz raportem NASK „Trolling w mediach społecznościowych”.

User experience (UX)

Na co dzień korzystamy ze stron internetowych i aplikacji, jednak nie wszystkie lubimy w tym samym stopniu. Od czego to zależy? Przede wszystkim od user experience (UX), czyli doświadczenia użytkownika, a więc wrażeń i odczuć, które budzi w nas cyfrowy (w tym przypadku) produkt.

Strony i aplikacje zaprojektowane z uwzględnieniem UX w centrum stawiają człowieka i jego komfort. Liczą się zatem intuicyjność, przejrzystość nawigacji, jasny przekaz informacji i maksimum funkcjonalności. Nie bez znaczenia jest też atrakcyjny projekt interfejsu, a także ogólny wygląd strony. Im lepiej dana witryna jest przygotowana pod kątem user experience, tym większe szanse na to, że użytkownicy wrócą, polecą ją znajomym, zrobią zakupy – będą często z niej korzystać. Za projektem UX stoją specjaliści z zakresu IT, którym nieobce są zagadnienia związane z wzornictwem przemysłowym, dostępnością cyfrową, a nawet… psychologią i socjologią.

Czy UX może mieć coś wspólnego z cyberbezpieczeństwem? Okazuje się, że tak. Badania (Rybak, Dudczyk, 2019) wykazują, że osoby, które korzystają z portali społecznościowych, nie zawsze mają pełną świadomość zagrożeń związanych z udostępnianiem tam swoich danych osobowych. Dzielą się w sieci prywatnymi informacjami, kierując się… pozytywnymi wrażeniami wywoływanymi przez dany serwis. Pamiętajcie – zasada ograniczonego zaufania przede wszystkim!

Usługi bezpieczeństwa OSE

W ramach Ogólnopolskiej Sieci Edukacyjnej (OSE) oferujemy szkołom w całej Polsce dostęp do bezpłatnego, szybkiego, szerokopasmowego internetu o prędkości 100/100 Mb/s. Na tym nie koniec – nasi użytkownicy mogą liczyć także na profesjonalne, bezpłatne usługi bezpieczeństwa: „Bezpieczny internet OSE", „Bezpieczeństwo użytkownika OSE" i „Ochrona przed szkodliwym oprogramowaniem". Zapewniają one ochronę na poziomie sieciowym oraz strzegą bezpieczeństwa uczniów, broniąc ich przed nielegalnymi i szkodliwymi treściami.

Szczegółowych informacji na temat naszych usług bezpieczeństwa szukajcie w zakładkach FAQ i Internetowe usługi OSE na stronie ose.gov.pl oraz w aktualności „5 pytań o… usługi bezpieczeństwa OSE". Nie znaleźliście tam odpowiedzi na swoje pytanie? Wyślijcie e-mail na adres: wsparcietechniczne_ose@nask.pl lub zadzwońcie na infolinię OSE (+48 22 182 55 55), czynną od poniedziałku do piątku w godzinach 7:30–16:00.

Ustawa o krajowym systemie cyberbezpieczeństwa

Kto jest odpowiedzialny za cyberbezpieczeństwo w Polsce? Jakie są główne cele zapewniania bezpieczeństwa cyfrowego na poziomie kraju? Czym są

incydenty bezpieczeństwa i kto na nie reaguje? Odpowiedzi na te i inne pytania znajdziecie w Ustawie o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 5), która włącza do polskiego porządku prawnego dyrektywę Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa 2016/1148), tzw. Dyrektywa NIS.

Ustawa ta definiuje organizację krajowego systemu cyberbezpieczeństwa, zadania i obowiązki podmiotów wchodzących w skład tego systemu, sposób sprawowania nadzoru i kontroli w zakresie jej stosowania oraz opisuje Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

Uwierzytelnianie dwuskładnikowe

O tym, jak cenne są nasze dane, w tym dane osobowe czy dane do logowania, dowiadujemy się najczęściej w przypadku… ich utraty. Jak się przed tym zabezpieczyć? Przede wszystkim postawcie na silne hasła, które będą strzegły dostępu do Waszych kont w serwisach pocztowych, społecznościowych czy bankowości elektronicznej. Dobre hasło składa się z minimum 12 znaków i jest zmodyfikowaną frazą – łatwą do zapamiętania, ale trudną do odgadnięcia, np. ze względu na obcojęzyczny wtręt (DwaBialeLatajace**Sophisticated**Kroliki) lub sprytne zmiany (Wlazł**Kostek**Na**Mostek**I**Stuka**). Jeśli nie znacie jeszcze nowych wytycznych CERT Polska dotyczących zasad tworzenia silnych haseł, koniecznie się z nimi zapoznajcie i sprawdźcie, czy Wasze zabezpieczenia są wystarczające!

W dzisiejszych czasach silne hasło to niestety nie wszystko. Warto pomyśleć o włączeniu dodatkowej weryfikacji, tzw. uwierzytelniania dwuskładnikowego (ang. *Two Factor Authenticaton, 2FA*). Pomoże nam ono skutecznie chronić nie tylko nasze konta, ale również hasła do nich.

Decydując się na uwierzytelnienie dwuskładnikowe, mamy do wyboru kilka możliwości. To przede wszystkim jednorazowe kody generowane w aplikacji lub wysyłane SMS-em („coś, co znasz"), ale też klucz sprzętowy („coś, co posiadasz") – małe urządzenie, które pozwala potwierdzić, że to właśnie my próbujemy zalogować się do komputera, serwisu czy aplikacji. Drugim składnikiem może być też „coś, czym jesteś", a więc zabezpieczenie biometryczne w postaci odcisku palca, skanu twarzy czy obrazu tęczówki.

Po skonfigurowaniu 2FA podczas logowania – za każdym razem – oprócz hasła będziemy wprowadzać także np. specjalny kod. Ten dodatkowy składnik jest znany tylko nam, więc nawet jeśli hasło wycieknie lub stracimy je w inny sposób, cyberprzestępca nie włamie się na nasze konto.

Więcej porad dotyczących zabezpieczania swoich kont znajdziecie w aktualnościach na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: bezpieczne logowanie" i „Bezpieczni w sieci z OSE: uwierzytelnianie dwuskładnikowe".

Uzależnienie od gier komputerowych

W dobie powszechnego dostępu do internetu i urządzeń cyfrowych coraz łatwiej wpaść nam w pułapkę różnego rodzaju uzależnień behawioralnych, związanych z nowymi technologiami. Należą do nich m.in. uzależnienie od telefonu (fonoholizm) i gier komputerowych (gaming). Łączą je wspólne cechy, takie jak wewnętrzny przymus wykonywania określonych czynności (np. grania w grę, sięgnięcia po telefon), uporczywe powtarzanie tych czynności, nawet jeśli są szkodliwe (np. prowadzą do zaniedbania innych sfer życia) oraz zakończone niepowodzeniem próby kontrolowania lub zakończenia tych czynności.

Powodów, dla których dzieci i młodzież (bo to ich najczęściej dotyka uzależnienie od gier komputerowych) nadmiernie angażują się w aktywności online, może być bardzo wiele. Często to potrzeba wrażeń, nuda czy chęć sprawdzenia się. Gry umożliwiają dzieciom i nastolatkom ucieczkę od realnego świata w stworzoną przez siebie rzeczywistość, którą w pełni kontrolują i do której dorośli nie mają dostępu.

Oczywiście nie każdy, kto poświęca dużo czasu grom komputerowym, jest od nich uzależniony. O problemie mówimy, gdy ten czas wymyka się spod kontroli lub na korzyść gier zaniedbujemy codzienne sprawy. Jak rozpoznacie, czy Wasze dziecko jest uzależnione od gier? Obserwujcie je i zwracajcie uwagę na to, czy młody człowiek nie wycofuje się z kontaktów społecznych, czy rezygnuje z innych aktywności poza graniem, czy przestaje się martwić swoimi obowiązkami. Jeśli zauważycie u niego powyższe symptomy, a także zaburzenia pamięci i koncentracji, częste zmiany nastroju i objawy abstynencyjne po zaprzestaniu grania – zareagujcie!

Wskazówki dotyczące rozpoznawania uzależnienia od gier oraz ustalania z dzieckiem reguł korzystania z urządzeń cyfrowych znajdziecie w poradnikach „Nastolatki i gry cyfrowe” oraz „FOMO i nadużywanie nowych technologii” dostępnych na platformie OSE IT Szkoła. Sięgnijcie też do naszych aktualności, w których mówimy o jasnych i ciemnych stronach grania: „Cyfrowe gry a rozwój dziecka”, „Gaming – uzależnienie od gier komputerowych” i „Grać czy nie grać? Oto jest pytanie!”.

Użytkownik

Nie ma przesady w stwierdzeniu, że wszyscy jesteśmy użytkownikami – korzystamy przecież ze smartfonów i innych urządzeń cyfrowych, z internetu, aplikacji. Czy jednak zawsze posługujemy się tymi narzędziami w bezpieczny sposób?

Lista wskazówek, o których powinniście pamiętać, chcąc zadbać o swoje bezpieczeństwo w sieci, może nie jest zbyt krótka, mimo to warto upewnić się, że odhaczacie wszystkie ważne punkty. Bezpieczny użytkownik to ten, który mądrze i świadomie korzysta z zasobów oraz dobrodziejstw internetu – warto zatem poświęcić chwilę na wdrożenie zasad!

Zacznijcie od zabezpieczeń: to silne hasła, uwierzytelnianie dwuskładnikowe, ale też regularne aktualizacje, które chronią Was przed różnymi atakami sieciowymi i działaniem złośliwego oprogramowania (malware). A skoro mowa o szkodnikach – uważajcie również na oszustów, którzy w podstępny sposób rozsyłają niebezpieczne maile (phishing) lub próbują zagrozić Wam podczas rozmowy telefonicznej (vishing), a także za pośrednictwem niebezpiecznych SMS-ów (smishing). Świadomy użytkownik internetu unika też korzystania z publicznych sieci Wi-Fi, nie otwiera podejrzanych załączników i nie klika w linki pochodzące z nieznanych źródeł. W dzisiejszych czasach z dużą ostrożnością podchodzi też do informacji, które znajduje w sieci: uważa na fake newsy, deepfake i dezinformację. A przede wszystkim kieruje się zasadą ograniczonego zaufania!

W aktualnościach (na platformie OSE IT Szkoła, ale też na stronie ose.gov.pl) na bieżąco podpowiadamy Wam, jak zadbać o siebie w internecie. Najnowsze wskazówki znajdziecie np. w artykule „10 rad, jak dbać o bezpieczeństwo w sieci”.

Virtual Private Network (VPN)

Wirtualna sieć prywatna to technologia, która tworzy zaszyfrowany prywatny tunel podczas łączenia z internetem. Dzięki temu aktywności w sieci są trudniejsze do monitorowania i obserwowania przez innych. VPN ukrywa również lokalizację, co utrudnia odwiedzanym przez użytkownika stronom internetowym zidentyfikowanie jego położenia – także kraju, w jakim aktualnie przebywa.

Jak działa VPN? Gdy z niego korzystamy, nasze aktywności sieciowe przechodzą przez zaszyfrowany, wspomniany już tunel i następnie przesyłane są do zamierzonego celu. Co ważne, dzięki VPN-owi ruch jest odpowiednio zabezpieczony, prywatność chroniona, a korzystanie z internetu – bezpieczniejsze. Mechanizm tej technologii opiera się głównie na ukryciu rzeczywistego adresu IP urządzenia oraz szyfrowaniu danych, które przesyłane są w trakcie połączenia internetowego. Sieci VPN bazują na architekturze klient–serwer.

Do niedawna z VPN-ów korzystały głównie korporacje oraz banki, obecnie na taką usługę decyduje się również coraz więcej prywatnych użytkowników. Dlaczego? Przede wszystkim dla bezpieczeństwa. Dzięki wirtualnym sieciom prywatnym możecie bezpieczniej korzystać z publicznych sieci Wi-Fi (np. w hotelu podczas wakacji, restauracji czy na lotnisku), nie mając obaw, że ktoś obserwuje bądź rejestruje Wasze aktywności w sieci.

Chcecie wybrać dostawcę wirtualnej sieci prywatnej? Upewnijcie się, że jest on godny zaufania. W tym celu warto pamiętać m.in. o szukaniu usługi, która nie zapisuje logów i skupia się na zachowaniu prywatności użytkowników. Sprawdźcie też koniecznie, gdzie znajduje się siedziba przedsiębiorstwa (czy w tym kraju gwarantowane jest prawo do prywatności?) oraz wystrzegajcie się darmowych programów.

Więcej przydatnych informacji o VPN-ach oraz szczegółowe podpowiedzi, jak wybrać odpowiedniego dostawcę, znajdziecie w biuletynie „OUCH! – Wirtualne Sieci Prywatne (VPN)". Zajrzyjcie też na platformę OSE IT Szkoła, gdzie mamy dla Was kurs e-learningowy „VPN – bezpieczne przeglądanie internetu".

Vishing

To hasło na pierwszy rzut oka może kojarzyć się Wam z phishingiem – nie bez powodu, gdyż jest to odmiana tego ataku. Słowo vishing powstało z połączenia słów *voice* (głos) oraz *phishing* i odnosi się do wyłudzania poufnych danych lub pieniędzy podczas rozmowy telefonicznej. Ofiarami mogą się stać zarówno pracownicy instytucji rządowych czy prywatnych firm (próba wyłudzenia danych lub środków przedsiębiorstwa), jak i osoby prywatne.

Cyberprzestępcy dzwonią do ofiar, podszywają się np. pod pracownika banku, urząd skarbowy bądź inną znaną instytucję i próbują zmanipulować ofiarę,

wyłudzić od niej informacje, pieniądze, a nawet dostęp do komputera – instalując na nim oprogramowanie pozwalające na zdalną kontrolę nad urządzeniem.

Czy bez obaw możecie odbierać telefon, gdy na ekranie pojawia się znany, zapisany numer? Niestety – nawet wtedy możecie paść ofiarą vishingu! Cyberprzestępcy wykorzystują w tym ataku także spoofing, w którym przejmują wybrany numer telefonu i dzwonią do ofiary, podając się np. za przedstawiciela znanej instytucji, banku, a nawet osobę publiczną.

Aby chronić się przed vishingiem, musicie pamiętać o tych samych zasadach, które pozwolą Wam uniknąć pułapek phishingu czy spoofingu. Najważniejsza jest więc ostrożność, spora dawka podejrzliwości oraz niepodejmowanie pochopnych działań – tym bardziej, gdy rozmówca naciska na Was, straszy lub oczekuje bardzo szybkiej reakcji. Pamiętajcie też, że jeśli odbieracie telefon od rzekomego przedstawiciela zaufanej instytucji (np. banku), który prosi o podanie danych osobowych lub danych logowania, powinna zapalić się Wam czerwona lampka. W takiej sytuacji najlepiej samodzielnie skontaktować się z instytucją – np. wybierając się do oddziału lub dzwoniąc na infolinię podaną na oficjalnej stronie. Pamiętajcie jednak, by nie oddzwaniać na numer zapisany w rejestrze połączeń w telefonie, nawet jeśli wydaje się Wam prawdziwy, ponieważ może on należeć do przestępcy!

Wiadomości na temat ochrony przed phishingiem znajdziecie w biuletynie „OUCH! – Powstrzymać phishing” oraz aktualności ose.gov.pl „Bezpieczni w sieci z OSE: phishing”.

Wellbeing

Wiele aspektów codziennego życia przeniosło się w ostatnim czasie do sieci. E-maile, wideokonferencje, aplikacje, media społecznościowe – przed ekranami spędzamy długie godziny. Ciągłe powiadomienia, spływające zewsząd informacje, wiele zadań do wykonania przed komputerem i narastająca frustracja: znacie to uczucie? To prosta droga do cyfrowego stresu, na który pomóc może digital wellbeing.

Wellbeing najprościej można wyjaśnić jako komfort psychiczny. Dzięki dobremu samopoczuciu, pozytywnym emocjom oraz równowadze cyfrowej (digital wellbeing) możecie nie tylko uniknąć wypalenia, ale też ustrzec się przed FOMO i stresem cyfrowym. Zadbanie o równowagę online–offline pomoże Wam również wypracować korzystne nawyki na przyszłość.

Więcej wiadomości, jak zachować równowagę i pokonać cyfrowy stres, znajdziecie w naszych materiałach. Zajrzyjcie do aktualności na ose.gov.pl: „Stres cyfrowy – czym jest i jak go pokonać?", „#offlinechallenge – czas na JOMO", „5 pytań o… równowagę cyfrową", „Cyfrowe nawyki u dzieci – to nasza wspólna sprawa". Zapoznajcie się też z materiałami dostępnymi na platformie OSE IT Szkoła: kursem e-learningowym „Zrozumieć FOMO", poradnikiem dla nauczycieli „FOMO i problemowe używanie internetu" i scenariuszami zajęć profilaktycznych: „Otwórz oczy – internet to nie wszystko. Śpiąca Królewna i FOMO. Scenariusz zajęć lekcyjnych dla uczniów klas 5–6", „Jak się nie zaplątać w sieci? Ryzykowne zachowania w internecie: FOMO i problemowe używanie internetu".

Wideokonferencje

To wirtualna forma komunikacji przy wykorzystaniu urządzeń cyfrowych (np. laptopa, smartfona) i internetu. Wideokonferencje umożliwiają zdalne rozmowy w czasie rzeczywistym – niezależnie do odległości, jaka dzieli uczestników spotkania. Często wykorzystywane są w pracy, edukacji bądź przy organizacji różnych wydarzeń, np. ważnych uroczystości czy wykładów.

Wideokonferencje szczególnie doceniliśmy w trakcie pandemii – pozwoliły one na organizację zdalnych spotkań (zarówno zawodowych, szkolnych, jak i tych rodzinnych), które były bezpieczne dla zdrowia uczestników.

Mimo że wideokonferencje ułatwiają komunikację, korzystając z nich, musicie również zadbać o bezpieczeństwo i pamiętać o zasadach, które uchronią Was przed różnymi incydentami i nieprzyjemnościami. Ważne jest więc, aby pamiętać m.in. o aktualizacjach oprogramowania do wideokonferencji, odpowiedniej konfiguracji ustawień audio/wideo, zakrywaniu nieużywanej kamerki w laptopie lub innym urządzeniu czy niedzieleniu się swoimi zaproszeniami (linkami do spotkań) z innymi osobami – w takiej sytuacji najlepiej odesłać zainteresowanego do organizatora spotkania.

Więcej praktycznych informacji o bezpiecznych wideokonferencjach znajdziecie na ose gov.pl w aktualności „Bezpieczni w sieci z OSE: wideokonferencje”. Przeczytajcie też koniecznie biuletyn „OUCH! – Bezpieczeństwo wideokonferencji”.

Wi-Fi

To jedna z najpopularniejszych technologii wykorzystywanych przy budowie bezprzewodowych sieci, której szczególnym zastosowaniem jest tworzenie sieci lokalnych (LAN) opartych na komunikacji radiowej (WLAN). Brzmi skomplikowanie? Zatem prościej: dzięki Wi-Fi możemy bezprzewodowo łączyć się z internetem.

Wielu z Was używa tej technologii niemal każdego dnia – łącząc z domową siecią przenośne urządzenia cyfrowe (np. smartfony, tablety) czy inteligentne domowe sprzęty (np. telewizory, lodówki, roboty sprzątające), ale też korzystając z otwartych sieci publicznych.

Choć W-Fi jest dużym ułatwieniem, może też narażać Was na niebezpieczeństwa – szczególnie gdy korzystacie z sieci publicznych, np. w kawiarni lub hotelu. Takie sieci powinniście traktować jako niezaufane, gdyż nigdy nie możecie mieć pewności, kto jest do nich podłączony ani kto je Wam udostępnia. Decydując się na korzystnie z publicznego Wi-Fi, unikajcie logowania się do banku, mediów społecznościowych czy poczty elektronicznej i podawania haseł. Dbajcie też o aktualne oprogramowanie antywirusowe i systemowe Waszych urządzeń oraz rozważcie skorzystanie z VPN-ów.

Wasza domowa sieć również potrzebuje odpowiedniego zabezpieczenia przed wirtualnymi zagrożeniami. Jakiego? Odpowiedzi dostarczy biuletyn „OUCH! – Bezpieczna domowa sieć Wi-Fi”. Z kolei wiadomości na temat elementów sprzętowych służących do budowy domowej sieci przewodowej i bezprzewodowej szukajcie na platformie OSE IT Szkoła w kursie e-learningowym „Sieci komputerowe w powszechnym użyciu”.

Więcej podpowiedzi, jak bezpiecznie korzystać z publicznych sieci Wi-Fi, znajdziecie też na stronie ose.gov.pl w aktualności „Wi-Fi na wakacjach. Czy zawsze jest bezpieczne?”.

Wirus komputerowy

To rodzaj złośliwego oprogramowania (malware), które infekuje urządzenia (np. komputer, laptop, smartfon czy tablet). Podobnie do wirusa grypy także ten komputerowy ma zdolność powielania się i gdy przeniknie do Waszego sprzętu, może sprawić wiele problemów, modyfikując inne programy bądź pliki.

Najczęstsze skutki zainfekowania urządzenia wirusem to np. niszczenie lub zmienianie zawartości sprzętu czy utrudnienie korzystania z niego. Wirusy mogą być przenoszone m.in. poprzez pobierane pliki, załączniki otrzymane w wiadomości e-mailowej, urządzenia USB (np. dysk zewnętrzny, pendrive) lub komunikatory internetowe.

Nie lekceważcie wirusów – nawet te najprostsze mogą być niebezpieczne i szkodliwe! Jak więc chronić sprzęty przed zainfekowaniem? Przede wszystkim działajcie profilaktycznie – instalując i na bieżąco aktualizując program antywirusowy i używane oprogramowanie. Pamiętajcie też o niepodłączaniu do Waszych urządzeń USB niewiadomego pochodzenia i niepobieraniu załączników z podejrzanych e-maili czy plików z internetu (np. filmów, muzyki). Warto także zadbać o stworzenie kopii zapasowej (backup) swoich danych, która w razie niebezpieczeństwa pomoże odzyskać ważne pliki.

Informacji na temat wirusów komputerowych dostarczą Wam nasze kursy e-learningowe „Podstawy bezpieczeństwa sieciowego" oraz szósty moduł „Przygód Profesora i N@tki, czyli jak mądrze korzystać z internetu" – znajdziecie je na platformie OSEIT Szkoła. Wiele pomocnych wiadomości dostępnych jest też w biuletynie „OUCH! – Ochrona przed złośliwym oprogramowaniem".

Wizerunek online

Wizerunek jest zbiorem cech oraz informacji wpływających na to jak inni Was odbierają. Może dotyczyć zarówno konkretnej osoby, jak i przedsiębiorstwa lub produktu. Na wizerunek online składają się Wasze działania w sieci: udostępnienia (zdjęć, postów, filmów), komentarze, lajki, przynależność do grup lub wpisy w mediach społecznościowych czy dotyczące Was treści wrzucone do sieci przez innych użytkowników.

Nie zapominajcie, że wizerunek online często nie pozostaje jednak tylko w sferze wirtualnej i przenosi się na świat offline – dlatego działania w sieci zawsze warto podejmować rozważnie. Zanim więc udostępnicie materiały przedstawiające wizerunek Wasz lub innych osób – dobrze się zastanówcie, czy dane zdjęcie, film lub wpis będzie Wam się podobać również w przyszłości i czy będziecie zadowoleni, gdy ten materiał zobaczą np. rodzice, nauczyciel lub pracodawca. Pamiętajcie, że w internecie nic nie ginie!

Jak jeszcze dbać o swój wizerunek online? Warto m.in. korzystać z ustawień prywatności w mediach społecznościowych i przeglądarkach, nie publikować zdjęć dokumentów czy ustalić ze znajomymi zasady udostępniania materiałów przedstawiających Wasz wizerunek.

Więcej informacji na temat ochrony wizerunku w sieci znajdziecie na stronie ose.gov.pl w aktualnościach: „Bezpieczni w sieci z OSE: ochrona wizerunku i tożsamości w sieci", „Wizerunek online: pamiętaj o nim również w wakacje!". Pomocnej wiedzy dostarczą też kursy e-learningowe dostępne na platformie OSE IT Szkoła: „Wizerunek w sieci", „Cyberprzemoc – prześmiewcze serwisy internetowe", „Owce w sieci – Bekanie" oraz pierwszy moduł „Przygód Profesora i N@tki, czyli jak mądrze korzystać z internetu".

Wyzwanie (challenge)

Internetowe wyzwania, tzw. online challenge, to zabawa polegająca na zamieszczaniu w sieci materiałów (zdjęć lub filmów), na których wykonuje się

różne zadania – niekiedy dziwne, a nawet zagrażające życiu lub zdrowiu. Przykładami takich niebezpiecznych wyzwań są m.in.: Eraser challenge (w którym uczestnik ma energicznie pocierać skórę gumką i jednocześnie wykonywać zadanie, np. recytować alfabet), robienie sobie zdjęć w niebezpiecznych miejscach czy Bird Box Challenge (wykonywanie różnych czynności z zawiązanymi oczami).

Internetowe wyzwania to „rozrywka" szczególnie popularna wśród nastoletnich użytkowników nowych technologii, którzy nie tylko decydują się na podejmowanie kolejnych wyzwań, ale często prześcigają się w wymyślaniu ekstremalnych zadań dla swoich znajomych. Dlaczego wirtualne challenge przyciągają dzieci i młodzież? Przede wszystkim dlatego, że opierają się na rywalizacji oraz umożliwiają zdobycie popularności wśród rówieśników i w internecie.

Rodzice i nauczyciele niestety zwykle nie zdają sobie sprawy, że uczniowie angażują się w wyzwania, które nie tylko mogą zagrażać ich zdrowiu, ale też życiu. W ochronie dzieci przed podejmowaniem niebezpiecznych działań pomoże Wam profilaktyka i rozmowy na temat przykrych konsekwencji, jakie mogą wiązać się z tą szkodliwą „zabawą".

Więcej informacji na temat internetowych wyzwań oraz podpowiedzi, jak rozmawiać z dziećmi o szkodliwych treściach, znajdziecie na platformie OSE IT Szkoła: w poradniku dla nauczycieli „Szkodliwe treści w internecie" oraz aktualności „Niebezpieczne zjawiska w internecie: szkodliwe treści". Na naszym profilu na Facebooku OSE – Ogólnopolska Sieć Edukacyjna możecie też obejrzeć webinar „Szkodliwe treści w internecie".

Zabezpieczenia biometryczne

Wiemy doskonale, że podstawowym zabezpieczeniem naszych kont – a co za tym idzie: danych osobowych – są silne hasła. Coraz częściej ich funkcję pełnimy… my sami, np. odblokowując telefon odciskiem palca czy używając wizerunku twarzy do logowania się do banku. To przykłady zabezpieczeń biometrycznych, czyli takich, które wykorzystują nasze unikatowe cechy.

Jakie są najpopularniejsze obecnie techniki biometryczne? Poza odciskiem palca i geometrią twarzy wykorzystuje się także błyskawiczne selfie, rozpoznawanie głosu i tęczówki oka, geometrię dłoni i biometrię układu jej naczyń krwionośnych, a także biometrię siatkówki oka, kształtu ucha czy nawet identyfikację chodu.

Takie zabezpieczenia są przede wszystkim wygodne – zdecydowanie łatwiej jest przecież zgubić np. klucze czy kartę płatniczą niż własne oko lub palce. Wydaje się również, że biometryczne hasła są niemożliwe do podrobienia przez cyberprzestępców (jednak nie można ufać im bezgranicznie – wystarczy np. nagrać czyjś głos, by oszukać urządzenie, które go rozpoznaje). Przyzwyczajcie się do myśli, że biometria będzie wykorzystywana nie tylko w kryminologii (do badań daktyloskopijnych lub DNA), ale też na coraz szerszą skalę w naszym codziennym życiu. A może już teraz ustawiliście zabezpieczenie biometryczne jako dodatkowy element uwierzytelniania dwuskładnikowego?

Na koniec biometryczna ciekawostka: choć wydaje się, że tego typu zabezpieczenia są znakiem obecnych czasów, ich pierwszych śladów można szukać nawet w III/II tysiącleciu p.n.e. Istnieją bowiem dowody, że starożytni Babilończycy umieszczali odciski palców w formie podpisów na kontraktach!

Więcej informacji o silnych hasłach i sposobach zabezpieczania kont znajdziecie w aktualnościach na stronie ose.gov.pl: „Bezpieczni w sieci z OSE: bezpieczne logowanie" oraz „Bezpieczni w sieci z OSE: uwierzytelnianie dwuskładnikowe".

Zakupy online

Robicie zakupy w internecie – w sklepach online, serwisach aukcyjnych lub aplikacjach mobilnych? Zakupy online umożliwiają Wam zamawianie towarów bez wychodzenia z domu i czekania w często długich kolejkach do kasy. Dzięki nim możecie porównywać tysiące produktów w różnych sklepach i decydować się na najbardziej atrakcyjną dla Was ofertę, jak również łatwo zamawiać produkty z innych krajów.

Każdego dnia internauci na całym świecie kupują online. Taka forma transakcji ma wiele plusów, ale… może także narażać na niebezpieczeństwa. Aby ich uniknąć, zawsze powinniście być czujni i pamiętać o kilku zasadach.

Warto więc zadbać m.in. o weryfikację sprzedawcy – sprawdzić jego dane, opinie innych klientów – a także decydować się na zakupy w znanych i sprawdzonych sklepach. Upewnijcie się też, że na stronie e-sklepu jest regulamin (zawsze pamiętajcie, by go przeczytać!), informacje o sposobach dostawy, formach płatności czy wiadomości na temat zwrotu towaru. Z rezerwą podchodźcie też do promocyjnych wabików typu „oferta aktualna tylko dziś!".

Pomocne wiadomości na temat bezpiecznych zakupów online znajdziecie na stronie ose.gov.pl w aktualności „Bezpieczne zakupy w Black Friday" oraz platformie OSE IT Szkoła: w kursie e-learningowym „Bezpieczne zakupy w internecie" i poradniku „Jak się nie dać złapać w sieci nieuczciwych sprzedawców". Zapoznajcie się też z biuletynem „OUCH! – Bezpieczne zakupy online", raportem NASK „Nastolatki wobec zakupów w internecie" oraz poradnikiem CERT Polska „Jak się nie dać złapać w sieci nieuczciwych sprzedawców".

Zespół ds. nadużyć (zespół abuse)

O wspólne bezpieczeństwo w sieci powinniśmy dbać wszyscy – niezależnie od wieku. Staliście się ofiarą hejtu w internecie? Natknęliście się na szkodliwą treść, która nie powinna znaleźć się w serwisie? A może zauważyliście działanie naruszające bezpieczeństwo użytkowników danej witryny? W takich sytuacjach pomocy udzieli Wam zespół ds. nadużyć (zespół abuse).

To pracownicy danego serwisu lub witryny internetowej, którzy zajmują się bezpieczeństwem. Do zespołu abuse możecie zgłaszać przypadki naruszenia bezpieczeństwa technicznego (security), a także te związane z opublikowanymi treściami lub nieprawidłowymi zachowaniami innych użytkowników (safety).

Z inicjatywy CERT Polska powstało w 2005 r. forum polskich zespołów abuse – Abuse FORUM (AF), którego głównym celem jest zwiększenie skuteczności zapobiegania i reagowania na zagrożenia w internecie.

Zniesławienie

Ofiarą cyberprzemocy w sieci może stać się każdy, zarówno uczeń, nauczyciel, rodzic, jak i dowolny użytkownik internetu. Niektóre akty cyberprzemocy (np. zniesławienie) są nie tylko szkodliwe dla ofiary i niezgodne z netykietą, ale też stanowią naruszenie prawa i mogą być ścigane na wniosek osoby pokrzywdzonej lub jej rodzica bądź opiekuna (w przypadku dzieci poniżej 18. roku życia).

Zniesławienie to pomówienie innej osoby lub grupy, instytucji, osoby prawnej bądź jednostki organizacyjnej niemającej osobowości prawnej o postępowanie lub właściwości, jakie mogą ją poniżyć wśród opinii publicznej albo skutkować narażeniem zaufania dla danego stanowiska, zawodu lub rodzaju działalności (Polak i in., 2015). Zniesławienie w sieci może mieć bardzo szkodliwe skutki, niszczące wizerunek przez długie lata – nie ma pewności, że raz wrzucone do sieci materiały lub dodany komentarz kiedykolwiek znikną z internetu.

Jak reagować w przypadku zniesławienia? Przede wszystkim powinniście postarać się o usunięcie szkodliwej dla Was treści. W tym celu należy niezwłocznie zgłosić sprawę administratorowi danej witryny/serwisu za pomocą specjalnego formularza bądź wysyłając e-mail do ich zespołu abuse. Pamiętajcie też, że zniesławienie jest przestępstwem ściganym z oskarżenia prywatnego, dlatego powinniście zabezpieczyć wszelkie dowody i zgłosić sprawę na policję, do sądu lub prokuratury.

Więcej informacji na temat zniesławienia znajdziecie na platformie OSE IT Szkoła w poradniku „Zagrożenia internetowe. Wybrane zjawiska".

Zespół uzależnienia od internetu (ZUI)

Internet ułatwia kontakt, wyszukiwanie informacji, załatwianie spraw urzędowych czy oferuje wiele form rozrywki. Co jednak w sytuacji, gdy ten bardzo atrakcyjny wirtualny świat pochłonie Was za bardzo?

Zespół uzależnienia od internetu to inaczej uzależnienie od internetu, czyli wykonywania różnych czynności w sieci. Może on dotykać nie tylko dorosłych, ale też dzieci i nastolatków – szczególnie narażone są na niego osoby charakteryzujące się wysokim FOMO. Nałogowemu korzystaniu z sieci mogą też towarzyszyć inne zachowania problemowe, takie jak np. zakupoholizm czy hazard online. Nadużywanie internetu podobnie jak inne e-uzależnienia można zaliczyć do uzależnień behawioralnych, czyli uzależnień od czynności.

Jakie symptomy u dzieci powinny wzbudzić Wasz niepokój? M.in. ciągła i silna potrzeba bycia online, uczucie rozdrażnienia, złości lub obniżenie nastoju w sytuacji odłączenia, rezygnacja z dotychczasowych zainteresowań na rzecz wirtualnych aktywności czy nadmierne korzystanie z internetu pomimo pojawienia się negatywnych skutków dla zdrowia.

ZUI, podobnie do innych uzależnień, może wywoływać bardzo poważne skutki, dlatego ważna w ochronie młodych użytkowników internetu jest profilaktyka i nauka zdrowych cyfrowych nawyków. Wiedzy, jak rozmawiać o równowadze online–offline z dziećmi i młodzieżą, przeciwdziałać FOMO oraz nadużywaniu nowych technologii, dostarczą Wam materiały dostępne na platformie OSE IT Szkoła: poradnik „FOMO i problemowe używanie internetu", kurs e-learningowy „Zrozumieć FOMO" oraz scenariusze zajęć: „Jak się nie zaplątać w sieci? Ryzykowne zachowania w internecie: FOMO i problemowe używanie internetu" i „Otwórz oczy – internet to nie wszystko. Śpiąca Królewna i FOMO. Scenariusz zajęć lekcyjnych dla uczniów klas 5–6". Zapoznajcie się też z aktualnościami dostępnymi na stronie ose.gov.pl: „Cyfrowe nawyki u dzieci – to nasza wspólna sprawa", „5 pytań o… równowagę cyfrową".

Bibliografia

(dostęp do wszystkich treści online: 5.09.2022)

Artykuły – ose.gov.pl

a) **Z serii „5 pytań o…”**: „5 pytań o… aplikację mOchrona”; „5 pytań o… FOMO i problemowe używanie internetu”; „5 pytań o… offline challenge” ; „5 pytań o… równowagę cyfrową”; „5 pytań o… sexting”; „5 pytań o… usługi bezpieczeństwa OSE”.

b) **Z serii „Bezpieczni w sieci z OSE”**: „Bezpieczni w sieci z OSE: aplikacje mobilne”; „Bezpieczni w sieci z OSE: bezpieczne logowanie”; „Bezpieczni w sieci z OSE: doxing”; „Bezpieczni w sieci z OSE: fake newsy”; „Bezpieczni w sieci z OSE: ochrona danych osobowych”; „Bezpieczni w sieci z OSE: ochrona wizerunku i tożsamości w sieci”; „Bezpieczni w sieci z OSE: patostreamy”; „Bezpieczni w sieci z OSE: phishing”; „Bezpieczni w sieci z OSE: poczta e-mail”; „Bezpieczni w sieci z OSE: ransomware”; „Bezpieczni w sieci z OSE: trolling w mediach społecznościowych”; „Bezpieczni w sieci z OSE: uwierzytelnianie dwuskładnikowe”; „Bezpieczni w sieci z OSE: wideokonferencje”.

c) **Z serii „Bezpieczni w sieci z OSE na wakacje”**: „Akcja-aktualizacja – zadbaj o swój sprzęt w wakacje!”; „Bezpieczne media społecznościowe”; „Bezpieczni w sieci z OSE na wakacje: offline challenge”; „Wi-Fi na wakacjach. Czy zawsze jest bezpieczne?”.

d) **Inne**: „#offlinechallenge – czas na JOMO”; „10 rad, jak dbać o bezpieczeństwo w sieci”; „Cyfrowe gry a rozwój dziecka”; „Cyfrowe nawyki u dzieci – to nasza wspólna sprawa”; „Czas na social media sabbatical?”; „Czas na wiosenne – cyfrowe – porządki!”; „Czy to nagranie może kłamać? Uwaga na deepfake!”; „Doomsurfing – jak wyrwać się z błędnego koła śledzenia złych informacji”; „Dzielisz się zdjęciem dziecka w sieci? Rób to z głową!”; „E-wyprawka: sprawdź urządzenie, porozmawiaj z dzieckiem”; „Jak nie wpaść w pułapkę fake newsów?”; „Jak zrozumieć dziecko w sieci?”; „Majówka – cyfrowy detoks czy balans?”; „Niebezpieczne zjawiska w internecie: self-generated sexual content”; „Niebieski Poniedziałek – zadbajmy o zdrowie psychiczne dzieci”; „Skimming, czyli co się może kryć w bankomacie”; „Smombie są wśród nas”; „Stres cyfrowy – czym jest i jak go pokonać?”; „Temat lekcji: cyberprzemoc”; „Temat lekcji: FOMO i problemowe używanie internetu wśród uczniów”; „Temat lekcji: sexting”; „*Tylko zerknę*. Sprawdź, czy Twoje dziecko doświadcza phubbingu”; „Urlop w wersji unplugged? Jesteśmy na tak!”; „Uwaga na spoofing!”; „Uwaga, złodziej!”; „W wakacje bez internetu? Podejmij wyzwanie!”; „Wizerunek online: pamiętaj o nim również w wakacje!”; „Zanim uwierzysz, sprawdź!”; „Zdjęcia dziecka w sieci? Zastanów się, zanim opublikujesz”; „Złote zasady internetowych znajomości”.

Artykuły – OSE IT Szkoła (it-szkola.edu.pl)

„Bezpieczne zakupy w Black Friday”; „Dzień Bota – dowiedz się więcej o sztucznej inteligencji!”; „Gaming – uzależnienie od gier komputerowych”;

„Gra pod choinkę? Poradnik świętego Mikołaja”; „Grać czy nie grać? Oto jest pytanie!”; „Letnia Akademia OSE 2022: offline challenge”; „Masz już swój plan B?”; „Niebezpieczne zjawiska w internecie: cyberprzemoc w szkole”; „Niebezpieczne zjawiska w internecie: FOMO”; „Niebezpieczne zjawiska w internecie: szkodliwe treści”; „Nie krzycz w internecie, czyli ściągawka z netykiety”; „Pomysł na Dzień Pac-Mana? Dowiedz się więcej na temat grania!”; „Silne hasło to podstawa!”.

Artykuły – inne

Ministerstwo Spraw Wewnętrznych i Administracji, „Stopnie alarmowe i stopnie alarmowe CRP”.

Publikacje

Arseniuk R., (2021), „Co oglądamy w rozbitym lustrze? Królowa Śniegu i patostreamy. Scenariusz zajęć lekcyjnych dla uczniów klas 5–6”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Arseniuk R., (2021), „Nie wywołuj hejtu z lasu. Czerwony Kapturek i cyberprzemoc. Scenariusz zajęć lekcyjnych dla uczniów klas 5–6”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Arseniuk R., (2021), „Otwórz oczy – internet to nie wszystko. Śpiąca Królewna i FOMO. Scenariusz zajęć lekcyjnych dla uczniów klas 5–6”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Arseniuk R., (2021), „Złapani w sieć. Złota Rybka i niebezpieczne kontakty online. Scenariusz zajęć lekcyjnych dla uczniów klas 5–6”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Borkowska A., Karelus K., (2022), „Fake newsy i dezinformacja – o tym warto porozmawiać w szkole”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Borkowska A., Witkowska M., (2017), „Media społecznościowe w szkole”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Borkowska A., Witkowska M., (2020), „Sharenting i wizerunek dziecka w sieci. Poradnik dla rodziców”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Broszura „Zagrożenia w internecie. Zapobieganie – reagowanie. Hazard online wśród młodzieży”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Cherne L. (red.), (2020), „Bezpieczeństwo wideokonferencji”, tłum. Wnuk B., Węgrzynowicz A., „OUCH! Biuletyn Bezpieczeństwa Komputerowego”, nr 8 [online].

Cherne L. (red.), (2022), „Kariera w cyberbezpieczeństwie”, tłum. Wnuk B., Węgrzynowicz A., „Biuletyn Bezpieczeństwa Komputerowego OUCH!”, nr 2 [online].

Dudley T. (red.), (2018), „Powstrzymać phishing”, tłum. Kondraszuk S., Strzelczyk M., Sikorski J., „Biuletyn Bezpieczeństwa Komputerowego OUCH!”, nr 3 [online].

Elgee Ch. (red.), (2022), „Najpopularniejsze oszustwa w serwisach społecznościowych”, tłum. Wnuk B., Węgrzynowicz A., „Biuletyn Bezpieczeństwa Komputerowego OUCH!”, nr 4 [online].

Eubanks R. (red.), (2020), „Menedżer haseł”, tłum. Wnuk B., Purzycki K. „OUCH! Biuletyn Bezpieczeństwa Komputerowego”, nr 4 [online].

Fenik-Gaberle K., (2021a), „Decyzja. Ryzykowne zachowania w internecie: sexting. Scenariusz zajęć profilaktycznych dla uczniów w wieku 13–15 lat”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Fenik-Gaberle K., (2021), „Jak się nie zaplątać w sieci? Ryzykowne zachowania w internecie: FOMO i problemowe używanie internetu”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Fenik-Gaberle K., (2021b), „Czy wystarczy mi wyobraźnia? Ryzykowne zachowania w internecie: szkodliwe treści. Scenariusz zajęć profilaktycznych dla uczniów w wieku 13–15 lat”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

„Gotowi na RODO”, Generalny Inspektor Ochrony Danych Osobowych, Narodowy Instytut Wolności – Centrum Rozwoju Społeczeństwa Obywatelskiego [online].

Infografika „Jak rozpoznać fake newsa”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Infografiki „Sexting i nagie zdjęcia w sieci”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

„Jak się nie dać złapać w sieci nieuczciwych sprzedawców. Poradnik zespołu CERT Polska”, (2019), Warszawa: NASK – Państwowy Instytut Badawczy [online].

Johnsey P. (red.), (2019), „Wirtualne Sieci Prywatne (VPN)”, tłum. Wnuk B., Purzycki K., Urbanowicz J., „OUCH! Biuletyn Bezpieczeństwa Komputerowego”, nr 7 [online].

Kwaśnik A., (2021), „Sexting i nagie zdjęcia w sieci. Poradnik dla nauczycieli”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Lange R. (red.), (2021), „Nastolatki 3.0. Raport z ogólnopolskiego badania uczniów”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Lange R. (red.), (2020), „Trolling w mediach społecznościowych”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Lee R.M. (red.), (2018), „Inteligentne urządzenia w Twoim domu”, tłum. Kondraszuk S., Strzelczyk M., Sikorski J., „OUCH! Biuletyn Bezpieczeństwa Komputerowego”, nr 8 [online].

Lomas J. (red.), (2022), „Wykryj i zatrzymaj ataki w wiadomościach tekstowych”, tłum. Wnuk B., Węgrzynowicz A., „Biuletyn Bezpieczeństwa Komputerowego OUCH!”, nr 1 [online].

Makaruk K., Włodarczyk J., Michalski P., (2017), „Kontakt dzieci z pornografią. Raport z badań”, Warszawa: Fundacja Dajemy Dzieciom Siłę [online].

Maryl-Wojcik M., Puczko M., (2022), „Internet rzeczy jest wszędzie. Scenariusz przeznaczony dla uczniów szkół ponadpodstawowych”, Centrum Nauki Kopernik [online].

NASK i in., (2022), „Kodeks dobrych praktyk” [online].

Orlando M. (red.), (2021), „Bezpieczne zakupy online”, tłum. Wnuk B., Węgrzynowicz A., „OUCH! Biuletyn Bezpieczeństwa Komputerowego”, nr 11 [online].

Piechna J., (2019), „Szkodliwe treści w internecie. Nie akceptuję, reaguję! Poradnik dla rodziców”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Polak Z. (red.), (2021), „Cyfrowy ślad małego dziecka”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Polak Z., Różycka M., Marańda M., Szeląg M., (2015), „Zagrożenia internetowe. Wybrane zjawiska”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Reed T. (red.), (2021), „Bezpieczne przechowywanie danych w chmurze”, tłum. Wnuk B., Węgrzynowicz A., „OUCH! Biuletyn Bezpieczeństwa Komputerowego”, nr 8 [online].

Rybak Ł., Dudczyk J., (2019), „User experience w aspekcie zagrożenia dla bezpieczeństwa cyfrowego”, Journal of Modern Science, tom 2/41, s. 127–140 [online].

Rywczyńska A., Piechna J., (2021), „Szkodliwe treści w internecie. Poradnik dla nauczycieli”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Rywczyńska A., Wójcik S. (red.), (2018), „Bezpieczeństwo dzieci i młodzieży online. Kompendium dla rodziców i profesjonalistów”, Warszawa: NASK – Państwowy Instytut Badawczy i Fundacja Dajemy Dzieciom Siłę [online].

Sowala M., Wrońska A. (red.), (2020), „Bezpieczeństwo online w szkołach Ogólnopolskiej Sieci Edukacyjnej. Poradnik dla szkół Ogólnopolskiej Sieci Edukacyjnej, cz. 1”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Sowala M., Wrońska A. (red.), (2020), „Bezpieczeństwo online w szkołach Ogólnopolskiej Sieci Edukacyjnej. Poradnik dla szkół Ogólnopolskiej Sieci Edukacyjnej, cz. 2”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Tomlinson K., (2022), „Naucz się nowej umiejętności: wykrywanie Deepfake”, tłum. Wnuk B., Węgrzynowicz A., „Biuletyn Bezpieczeństwa Komputerowego OUCH!”, nr 3 [online].

Ulotka „Fake newsy, bańki informacyjne, teorie spiskowe”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Witkowska M., (2019), „FOMO i nadużywanie nowych technologii. Poradnik dla rodziców”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Witkowska M., (2021), „FOMO problemowe używanie internetu. Poradnik dla nauczycieli”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Witkowska M., (2021), „Nastolatki i gry cyfrowe. Poradnik dla rodziców”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Wójcik S., Wojtasik Ł. (red.), (2019), „Patotreści w internecie. Raport o problemie”, Warszawa: Fundacja Dajemy Dzieciom Siłę [online].

Wright J. (red.), (2021), „Bezpieczna domowa sieć Wi-Fi”, tłum. Wnuk B., Węgrzynowicz A., „OUCH! Biuletyn Bezpieczeństwa Komputerowego”, nr 1 [online].

Wrońska A. (red.), (2019), „Nastolatki wobec zakupów w internecie”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Wrzosek M., (2019), „Zjawisko dezinformacji w dobie rewolucji cyfrowej”, Warszawa: NASK – Państwowy Instytut Badawczy [online].

Zeltser L. (red.), (2021), „Kradzież tożsamości – ochroń się przed nią”, tłum. Wnuk B., Węgrzynowicz A., „OUCH! Biuletyn Bezpieczeństwa Komputerowego”, nr 3 [online].

Zelster L. (red.), (2018), „Ochrona przed złośliwym oprogramowaniem”, tłum. Kondraszuk S., Strzelczyk M., Sikorski J., „OUCH! Biuletyn Bezpieczeństwa Komputerowego”, nr 6 [online].

Kursy e-learningowe na platformie OSE IT Szkoła

„Bezpieczne zakupy w internecie”; „Cyberprzemoc – anonimowość w sieci”; „Cyberprzemoc – prześmiewcze serwisy internetowe”; „Krasnoludki 2.0 – Mech w potrzebie”; „Krasnoludki 2.0 – Phishing, czyli kłopoty to nasza specjalność”; „Miękkie aspekty bezpieczeństwa w internecie”; „Owce w sieci – Bekanie”; „Owce w sieci – Zabawa w śnieżki”; „Podstawy bezpieczeństwa sieciowego”; „Prawo autorskie – najważniejsze definicje”; „Przygody Profesora i N@tki, czyli jak mądrze korzystać z internetu”; „Relacje w środowisku medialnym”; „Sieci komputerowe w powszechnym użyciu”; „Sharenting. Czy warto mieć rodzinny album w sieci?”; „Techniki internetu”; „VPN – bezpieczne przeglądanie internetu”; „Wizerunek w sieci”; „Własność intelektualna”; „Zrozumieć FOMO. Kurs dla nauczycieli i wychowawców”.

Webinary z udziałem ekspertów OSE

„Bezpieczni w sieci z OSE – Internet bez tajemnic”; „Dzieci i młodzież a media społecznościowe”; „Rodzinny album z wakacji, czyli czego o dzieciach nie powinien wiedzieć internet”; „Sexting i nagie zdjęcia w sieci – profilaktyka i reagowanie”; „Szkodliwe treści w internecie. Profilaktyka i reagowanie”.

Inne materiały

Materiały CERT Polska: „Jak się nie dać złapać w sieci nieuczciwych sprzedawców”; „Kompleksowo o hasłach”; „Ważne zasady bezpiecznego użytkowania poczty elektronicznej i mediów społecznościowych”
Materiały z cyklu „Bądź z innej bajki”
„Raporty roczne” z działalności CERT Polska, zawierające zebrane dane o zagrożeniach dla polskich użytkowników internetu
Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018 poz. 1560)

Inne strony
Bezpłatny i anonimowy telefon zaufania dla dzieci: 116111.pl
Bezpłatny i anonimowy telefon zaufania dla rodziców i nauczycieli: 800100100.pl
Centrum wsparcia dla osób w stanie kryzysu psychicznego: liniawsparcia.pl
CERT Polska: cert.pl
CERT Polska – Zgłoś incydent: incydent.cert.pl
Dyżurnet.pl: dyzurnet.pl
Europejski Miesiąc Cyberbezpieczeństwa: bezpiecznymiesiac.pl
Krajowy Rejestr Domen: dns.pl
Moje OSE: moje.ose.gov.pl
NASK – Państwowy Instytut Badawczy: nask.pl
No More Ransom: nomoreransom.org
#offlinechallenge: offlinechallenge.pl
Telefon zaufania Rzecznika Praw Dziecka: brpd.gov.pl
#WłączWeryfikację: facebook.com/WeryfikacjaNASK

Autorki: Katarzyna Gańko, Diana Kania, Emilia Troszczyńska-Roszczyk

Opieka merytoryczna: Anna Borkowska, Joanna Dębek, Katarzyna Koletyńska, Anna Kwaśnik, Zuzanna Polak, Marta Witkowska

Opracowanie graficzne i skład: Aneta Witecka

© NASK – Państwowy Instytut Badawczy
Warszawa 2022

ISBN: 978-83-65448-49-1

NASK – Państwowy Instytut Badawczy
ul. Kolska 12
01-045 Warszawa