Jak chronić się przed cyberatakami?

Praktyczne wskazówki dla parlamentarzystów i nie tylko.

GOV.pl CYFRYZACJA

PORADNIK

Więcej informacji
gov.pl/cyfryzacja

SPIS TREŚCI

WSTĘP

Internet zagościł w naszym życiu na dobre. Coraz więcej spraw załatwiamy online, zarówno prywatnych, jak i służbowych. Pandemia dodatkowo nasiliła ruch w sieci, gdzie przeniosło się wiele aspektów naszego dotychczasowego życia, jak praca, nauka, zakupy, wydarzenia kulturalne czy sprawy urzędowe.

W 2020 r. dostęp do internetu posiadało 90,4% gospodarstw domowych w Polsce[1], z serwisów społecznościowych korzystało 65,9% internautów w wieku 16-74 lat, zakupy w sieci robiło 60,9% internautów, zaś wiadomości i różnego rodzaju internetowe czasopisma czytało aż 78,6% osób z tej grupy wiekowej.

Rosnąca liczba dostępnych w internecie usług, jak i internautów przyciąga również cyberprzestępców - jednym nieopatrznym kliknięciem można stracić nie tylko pieniądze, ale również ważne dane, czy nadszarpnąć wizerunek, co jest szczególnie istotne dla osób publicznych.

W naszym poradniku przedstawiamy podstawowe informacje, które mają na celu podniesienie świadomości z zakresu cyberbezpieczeństwa – składają się de facto na tzw. cyberhigienę. Krok po kroku omawiamy także co zrobić w przypadku podejrzenia możliwości ataku ze strony cyberprzestępców.

Mamy nadzieję, że nasz poradnik okaże się przydatny. Stosowanie opisanych w nim zasad skutecznie wpłynie na podniesienie codziennego cyberbezpieczeństwa.

Dlatego zachęcamy nie tylko do lektury, ale przede wszystkim do stosowania naszych wskazówek w praktyce.

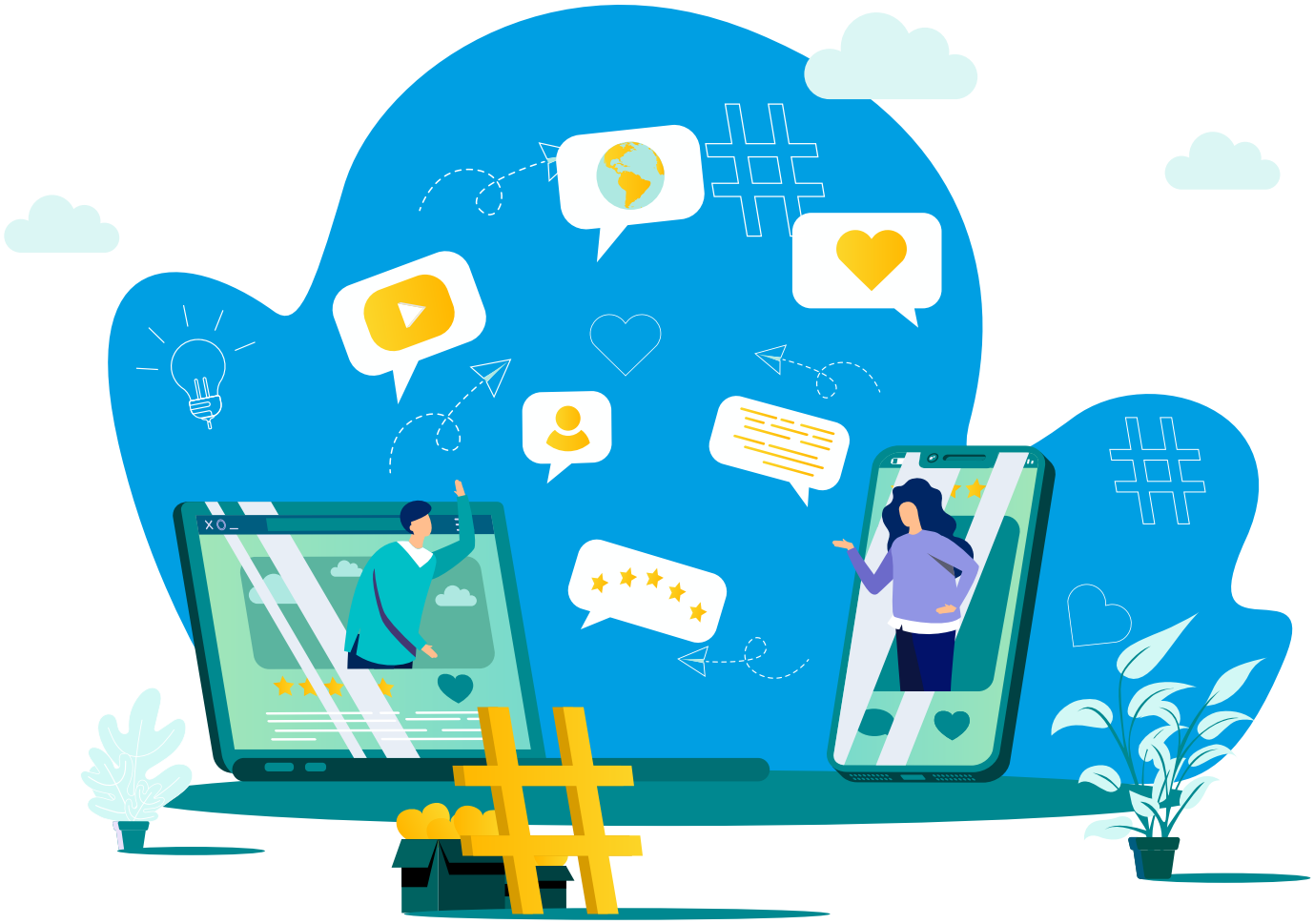
Uwaga! W poradniku opisujemy najpowszechniej stosowane narzędzia i usługi m.in. poczty elektronicznej i mediów społecznościowych. Na rynku istnieje wiele tego rodzaju rozwiązań. Ich wybór to zawsze indywidualna decyzja. Dlatego, nawet jeśli w poradniku pada nazwa konkretnego rozwiązania, nie oznacza to, że je oficjalnie rekomendujemy.

[1] Społeczeństwo informacyjne w Polsce w 2020 roku, Główny Urząd Statystyczny, Warszawa, 2020 r.

Co to jest cyberbezpieczeństwo i dlaczego jest takie ważne?

Cyberbezpieczeństwo to bezpieczeństwo w świecie cyfrowym (tzw. cyberprzestrzeni). To działania niezbędne do ochrony systemów informacyjnych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami. Cyberzagrożenia dotyczą przede wszystkim możliwości utraty poufności, dostępności i integralności danych oraz usług cyfrowych. Na rynku dostępne są różne narzędzia programowe i sprzętowe wspomagające cyberbezpieczeństwo. Żadne z nich nie będą skuteczne, jeśli nie będziemy przestrzegać podstawowych zasad korzystania z usług cyfrowych.

PAMIĘTAJ!
Żadne urządzenie nie zagwarantuje 100% bezpieczeństwa w sieci. Bezpieczeństwo w cyberprzestrzeni w dużej mierze zależy od nas samych i naszego postępowania. Ponad 90% współczesnych ataków bazuje na interakcji z użytkownikiem, którego najczęściej skłania się do np. otwarcia załącznika wiadomości poczty elektronicznej oraz kliknięcia w link (łącze) znajdujące się w treści wiadomości. Ponadto, niestety coraz częściej sami udostępniamy zbyt wiele informacji i danych, które powinniśmy chronić, a których poznanie pozwala cyberprzestępcom łatwiej przygotować i przeprowadzić atak.



Jak być bezpiecznym online? Podstawa to CYBERHIGIENA!

W wielu obszarach naszego życia konieczne jest podejmowanie odpowiednich działań, które mogą zabezpieczyć nas przed niebezpieczeństwem. Dotyczy to m.in. naszych bliskich, naszego zdrowia, dbania o samochód, czy dom. Taka profilaktyka powinna dotyczyć także aktywności w świecie cyfrowym. Tak jak regularne mycie rąk ma nas chronić przed infekcjami, a przeglądy techniczne samochodu przed groźnymi awariami, tak samo **aktualizowanie oprogramowania i zmiana haseł dostępu do kont i profili w usługach cyfrowych, powinny stać się naszymi zdrowymi i regularnymi nawykami w cyberprzestrzeni.**

Cyberprzestępcy stosują coraz bardziej wyrafinowane sposoby na to, aby zdobyć nasze dane czy pieniądze. Co więcej, wbrew niektórym opiniom, nie korzystają wcale z zaawansowanych środków technicznych do prowadzenia masowych ataków – dużo tańsze jest stosowanie prostych metod powtarzanych wielokrotnie. Tak, aby trafić na ten właściwy moment naszej osłabionej uwagi.

Czy wiesz, na co tak naprawdę jesteśmy narażeni ze strony cyberprzestępców?

Oto tylko kilka przykładów:

UTRATA WRAŻLIWYCH DANYCH

STRATY FINANSOWE W WYNIKU KRADZIEŻY

DUŻE KOSZTY ZWIĄZANE Z ODZYSKANIEM SKRADZIONYCH DANYCH

UTRATA DOBREJ REPUTACJI

Jak zatem należy dbać o cyberhigienę? W dalszej części poradnika zamieściliśmy wskazówki, jak w prosty sposób ograniczyć ryzyko znalezienia się w gronie ofiar cyberprzestępstw, bo samej liczby ataków nie jesteśmy w stanie ograniczyć tylko poprzez indywidualne działania.

Jak ograniczyć ryzyko cyberataków? – krok po kroku

1

Zainstaluj oprogramowanie antywirusowe

Obowiązkowo - powinno się znaleźć na każdym komputerze, a także smartfonie i innych urządzeniach podłączonych do internetu, w których możliwe jest instalowanie aplikacji. Współczesne oprogramowanie antywirusowe, stale aktualizowane, zapewnia ponad 95% ochronę przed złośliwym oprogramowaniem – dołączanym do treści wiadomości lub umieszczanym w witrynach internetowych, często specjalnie preparowanych przez cyberprzestępców. Codziennie trwa wyścig pomiędzy twórcami złośliwego oprogramowania a metodami jego wykrywania, ostatnio wspomaganymi tzw. sztuczną inteligencją. Dlatego tak ważne są regularne aktualizacje.

2

Aktualizuj oprogramowanie

Tak jak wspominaliśmy - w świecie technologii cyfrowych trwa nieustanny wyścig pomiędzy producentami sprzętu i oprogramowania, a przestępcami. Ci drudzy cały czas szukają luk i błędów, które mogliby wykorzystać do swoich celów, a firmy po ich wykryciu podejmują działania związane z wprowadzeniem poprawek i dodatkowych zabezpieczeń. Dlatego też **regularna aktualizacja systemu operacyjnego, oprogramowania aplikacyjnego, w tym przeglądarek internetowych, komunikatorów oraz oprogramowania do odbierania i wysyłania poczty e-mail, jest bardzo ważna dla cyberhigieny.** Takie aktualizacje zawierają bowiem poprawki, które mają ochronić przed znalezionymi podatnościami i błędami. Ich pominięcie to wręcz otwarte zaproszenie dla cyberprzestępców.

3

Dbaj o prywatność

Anonimowość w internecie nie istnieje, każde działanie pozostawia po sobie cyfrowe ślady, które w jakiś sposób określają daną osobę. Warto zadbać o to, żeby informacje o sobie udostępniać w sposób rozsądny i tylko w takim zakresie, w jakim jest to konieczne. Przede wszystkim należy unikać podawania swoich danych personalnych czy kontaktowych w miejscach, w których nie ma takiej potrzeby.

4

Rozsądek przede wszystkim

Przestępcy do perfekcji mają opanowane najróżniejsze techniki psychologiczne i socjotechniczne, które mają na celu skłonić nieświadomych użytkowników do wykonania określonej czynności. Podszywają się pod znane osoby i firmy, obiecują nagrody czy wykorzystują ciekawość – a wszystko po to, żeby skłonić nas do kliknięcia w link czy otwarcia jakiegoś pliku. Łatwo się domyślić, co się dzieje potem - cyberprzestępcy przejmują kontrolę nad naszym środowiskiem cyfrowym i mogą wykorzystać je do swoich celów. Dlatego też przy korzystaniu z usług internetowych konieczne jest zachowanie odpowiedniej ostrożności.

PAMIĘTAJ!

Nie otwieraj nieznanych załączników, w szczególności pochodzących od nieznanych nadawców. Nie klikaj w podejrzane linki, choćby miały atrakcyjne brzmiące tytuły... Stosuj się do zasady ograniczonego zaufania.

Czym jest cyfrowy ślad?

Cyfrowy ślad generuje każda nasza czynność w internecie. Składają się na niego dwa rodzaje informacji:

Dane o użytkowniku na podstawie adresu sieciowego – tzw. adresu IP — który jest generowany dla każdego urządzenia łączącego się z siecią. Adres IP może pomóc w ustaleniu lokalizacji, w której znajduje się urządzenie. Ponadto, na jego podstawie można ustalić m.in. wersję wykorzystywanego systemu operacyjnego, zestaw zainstalowanych czcionek i ustawienia przeglądarek internetowych;

Dane dotyczące ruchu w sieci, czyli ile czasu w niej spędzamy. Cały ruch na naszych urządzeniach jest zapisany na serwerze dostawcy usług telekomunikacyjnych. Przeglądarki zapamiętują odwiedzane strony, zaś wyszukiwarki — pytania, które zadajemy. Dzięki tzw. ciasteczkom (pliki „cookies") serwery stron mogą śledzić naszą aktywność w sieci. Pamiętaj, że masz możliwość samodzielnego zarządzania (w tym usuwania i blokowania) „cookies". Umożliwiają to np. przeglądarki internetowe, z których korzystasz.

Phishing – cyberprzestępcy na łowach

Wiele cyberataków jest realizowanych przez phishing. Phishing to metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych do logowania, danych zawartych na karcie płatniczej, haseł, kodów PIN), zainfekowania komputera szkodliwym oprogramowaniem, czy też nakłonienia ofiary do określonych działań w celu wyłudzenia pożądanych danych – w szczególności danych do logowania (identyfikator i hasło).

Cyberprzestępcy mogą wysyłać na pozór autentycznie wyglądające wiadomości dotyczące np. konserwacji konta, konieczności zmiany hasła, pilne komunikaty o rzekomych problemach finansowych, żądania kontaktu, powiadomienia o zmianie w usługach lub łącza do dokumentów wymagających do ich otwarcia podania identyfikatora i hasła.

Nazwa phishing budzi dźwiękowe skojarzenia z angielskim słowem „fishing" – czyli łowieniem ryb. Przestępcy, podobnie jak wędkarze, stosują bowiem odpowiednio przygotowaną „przynętę". Do tego wykorzystują sfałszowane e-maile, SMS-y czy wiadomości. Coraz częściej oszuści działają także za pośrednictwem komunikatorów i portali społecznościowych.

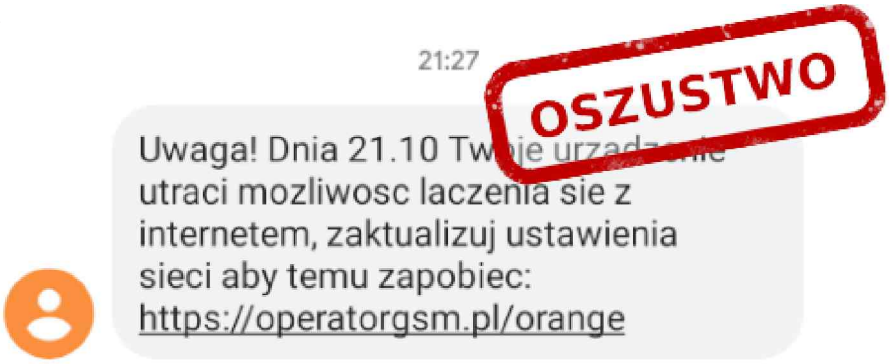
PAMIĘTAJ!

Zachowaj szczególną ostrożność w przypadku podejrzanych linków wysyłanych przez e-mail, SMS lub wiadomości z popularnych komunikatorów internetowych i mediów społecznościowych.

Jak działa phishing?

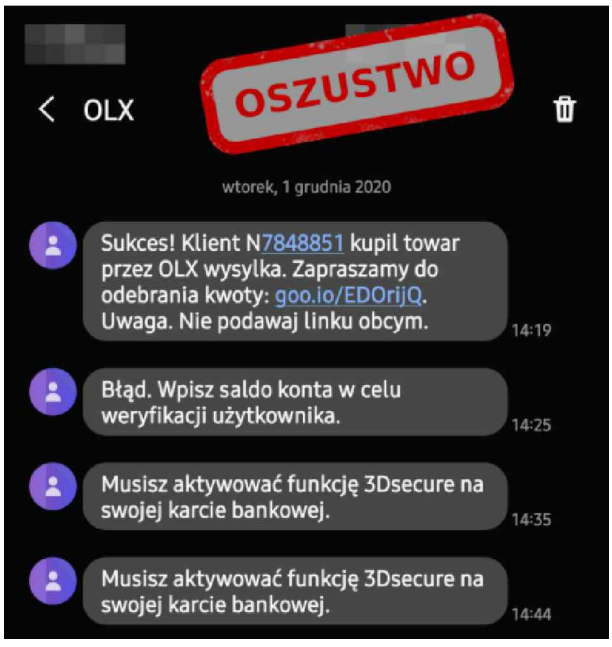
- Atakujący wykorzystują publicznie dostępne informacje na nasz temat. Aby ich wiadomości wydawały się bardziej przekonujące - wysyłają korespondencję z przejętych przez nich kont pierwotnie należących do znanych nam osób, firm lub instytucji.

- Techniki stosowane przez phisherów w wiadomościach e-mail mogą obejmować pilne lub autorytatywne nakazy. Chodzi o to, aby wywrzeć na nas presję – np. wymagając zalogowania w wyświetlonym dedykowanym oknie w ciągu 15 minut, pod rygorem zablokowania dostępu do konta.



- Wiele wiadomości phishingowych ma słabą gramatykę, interpunkcję i pisownię lub bazuje na trudności rozróżnienia na ekranie urządzeń mobilnych podobnie wyglądających znaków – np. wielka litera „I"(jak Irena) z małą literą „l" (jak lawina).

Dopóki nie masz pewności, że nadawca jest prawdziwy, **nie klikaj w żadne linki**, ani na nie nie odpowiadaj. W wiadomościach SMS lub e-mailach często wykorzystywane są tzw. tiny-URL, czyli skrócone adresy stron internetowych. Tak jak w poniższym przykładzie oszustwa – skrót do fałszywej strony „goo.io/EDOrijQ". Stąd też w ramach cyberhigieny należy zwracać szczególną uwagę na nazwy stron internetowych, które przesyłane są w podejrzanych mailach czy wiadomościach SMS.



Szczególnym rodzajem phishingu – zdecydowanie bardziej niebezpiecznym – jest tzw. **spearphishing**, czyli **atak ukierunkowany na KONKRETNEGO adresata**, mający na celu wywarcie określonego wpływu lub wymuszenie działania. Takim atakiem szczególnie zagrożone są osoby publiczne. Przestępcy mogą podszywać się pod znajomych z pracy, dziennikarzy, współpracowników, a wiadomość może być spersonalizowana, tzn. bezpośrednio odwoływać się do naszych relacji.

Jak dbać o bezpieczeństwo haseł?

Za pomocą haseł uzyskujemy dostęp do urządzeń, takich jak laptop lub smartfon, logujemy się do poczty elektronicznej, mediów społecznościowych czy bankowości elektronicznej oraz dokonujemy zakupów w sklepach internetowych. Można powiedzieć, że w wielu przypadkach hasła są niczym klucze do sejfu. W związku z tym, jeśli ktoś byłby w posiadaniu naszego hasła, mógłby dokonać przejęcia naszego konta w mediach społecznościowych, kradzieży naszej tożsamości, transferu pieniędzy lub uzyskać dostęp do naszych prywatnych danych.

PAMIĘTAJ!
Zadbaj o to, aby Twoje hasło było trudne do odgadnięcia!

Jakich haseł nie powinno się stosować?

- Nie stosuj najpopularniejszych haseł, jak: „**hasło", „123456**", „**qwerty**", „**piłka nożna**" itp.;
- Hasło nie powinno być takie samo jak nazwa użytkownika lub część tej nazwy;
- Hasło nie powinno być imieniem nikogo z naszego najbliższego otocznia (członka rodziny, znajomego ani zwierzaka);
- Nie powinno zawierać danych osobowych Twoich lub Twojej rodziny. Mowa tu o informacjach, które łatwo zdobyć, takie jak data urodzenia, numer telefonu, numer rejestracyjny samochodu, nazwa ulicy, numer mieszkania/domu itd.;
- Nie używaj sekwencji kolejnych liter, liczb lub innych znaków. Na przykład: **„abcde”**, „**12345**", „**QWERTY”**;
- Nie używaj pojedynczego wyrazu dowolnego języka pisanego normalnie lub wspak, ani tego wyrazu poprzedzonego lub/i zakończonego znakiem specjalnym lub cyfrą;
- Nie używaj więcej niż trzech kolejnych znaków na klawiaturze, takich jak „**abc**” lub „**123**";
- Nie używaj więcej niż dwóch kolejno powtarzających się ciągów znaków np. **”bbbb2bbb”**;
- Nie używaj oczywistych wyrażeń, takich jak np. „**wpuscmnie**".

Jak utworzyć silne hasło?

Hasło powinno zawierać co najmniej jeden znak z każdej z następujących grup:

MAŁE LITERY

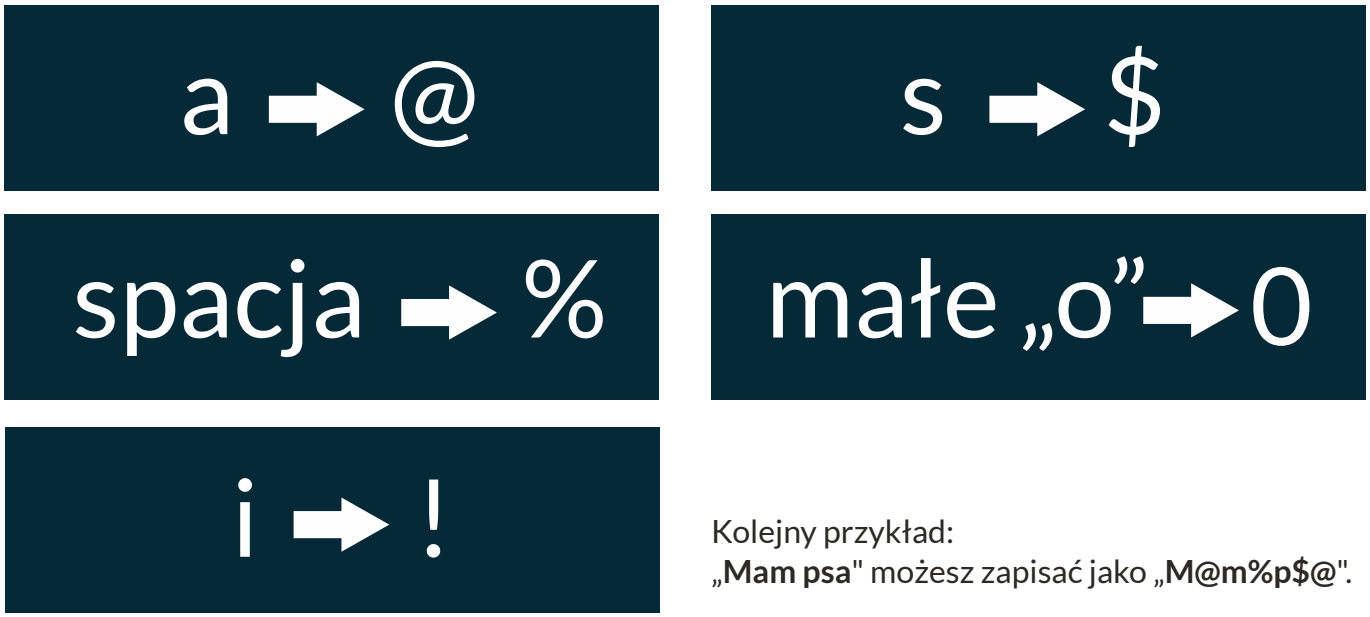
DUŻE LITERY

LICZBY

ZNAKI SPECJALNE

Użycie frazy - wybierz łatwy do zapamiętania cytat, piosenkę lub frazę i użyj pierwszej litery z każdego słowa. Używaj liter różnej wielkości. Pamiętaj, aby uwzględnić również liczby i symbole, zastępując nimi litery lub całe słowa.

Słowa „**Mam dwadzieścia lat**" można na przykład zapisać jako **M@m2dzie$ciAl4T**.
Możesz skorzystać z poniższych przykładów:



Kolejny przykład:
„**Mam psa**" możesz zapisać jako „**M@m%p$@**".

PAMIĘTAJ!
Używanie silnych haseł jest niezbędne, aby chronić swoją tożsamość i swoje informacje.

Co to jest podwójna weryfikacja (uwierzytelnienie) i jak ją stosować?

Hasła nie są już wystarczającym sposobem na ochronę naszych kont przez przejęciem przez przestępców. Hasła są podatne na podpatrzenie, wyłudzenie oraz skopiowanie. Większą ochronę dostępu do kont zapewnia stosowanie innych elementów zwiększających pewność poprawności identyfikacji użytkownika, czyli stosowanie dodatkowej weryfikacji (częściej stosowane fachowe określenie to - uwierzytelnienie wieloskładnikowe).

Uwierzytelnianie wieloskładnikowe (MFA - z ang. Multi-Factor Authentication), najczęściej stosowane jako dwuskładnikowe (często skracane do 2FA, z ang. two-factor authentication) zapewnia sposób podwójnej weryfikacji, że naprawdę jesteś osobą, za którą się podajesz, gdy korzystasz z usług online, mediów społecznościowych, bankowości lub poczty elektronicznej. **Nawet jeśli cyberprzestępca w jakiś sposób pozna Twój identyfikator/adres e-mail i hasło, nie będzie mógł uzyskać dostępu bez konieczności dodatkowej weryfikacji tożsamości.**

Na czym to polega? Podczas konfigurowania 2FA zostaniesz poproszony o **podanie „drugiego składnika weryfikującego"**, do którego masz dostęp tylko Ty. Może to być np.: kod wysyłany SMS-em na Twój numer telefonu (choć nie jest to już obecnie najbardziej bezpieczna metoda podwójnej weryfikacji) lub kod/jednorazowy numer utworzony przez aplikację zainstalowaną na Twoim urządzeniu mobilnym, a także wcześniej wygenerowana lista kodów, którą trzymasz w bezpiecznym miejscu.

Być może nie wszyscy o tym wiedzą, ale np. bankowość elektroniczna ma prawny obowiązek stosowania uwierzytelnienia dwuskładnikowego, aby zmniejszyć ryzyko nieuprawnionego dostępu do kont klientów.

Niektóre usługi online mają od razu włączone 2FA. Jeśli ta funkcja nie jest domyślnie aktywna, włącz ją samodzielnie, aby zapewnić dodatkową ochronę swoim kontom we wszystkich usługach takich jak poczta e-mail, media społecznościowe czy konto chmurowe.

Jeśli opcja włączenia 2FA jest dostępna, zwykle znajduje się ona w ustawieniach dotyczących bezpieczeństwa konta, gdzie może być nazwana „weryfikacją dwuetapową".

WAŻNE!
Sprawdź, w jaki sposób można włączyć funkcje 2FA w popularnych mediach społecznościowych, poznaj porady serwisów jeśli z nich korzystasz:

- Facebook – Zobacz jak ustawić uwierzytelnianie 2FA na Facebooku
- Instagram – Zobacz jak ustawić uwierzytelnianie 2FA na Instagramie
- LinkedIn – Zobacz jak ustawić uwierzytelnianie 2FA na LinkedIn
- Twitter – Zobacz jak ustawić uwierzytelnianie 2FA na Twitterze

PAMIĘTAJ!
Unikaj korzystania z usług, które nie dają możliwości wieloskładnikowego uwierzytelnienia (MFA/2FA). Zapytaj o nie usługodawcę i uruchom przed podjęciem decyzji o korzystaniu z danej usługi. Twoje dane są najcenniejsze!

Media społecznościowe – jak bezpiecznie z nich korzystać?

Popularne i szeroko wykorzystywane media społecznościowe pozwalają nie tylko na bieżący kontakt ze znajomymi, rodziną czy dostęp do najnowszych wiadomości, ale równie często są przez nas wykorzystywane do celów służbowych. Jest to również narzędzie o olbrzymim zasięgu oddziaływania dla mediów czy firm, które promują się w sieci, docierając często za naszym pośrednictwem do coraz to nowszych klientów.
Media społecznościowe to także narzędzie, które pozwala nam pozostać w kontakcie z ludźmi z całego świata. Platformy, takie jak Twitter czy Facebook, to narzędzia wykorzystywane przez nas na masową skalę w życiu prywatnym i zawodowym, a ich odziaływanie ma ogromną siłę. Jednak, wraz z rozwojem tego typu technologii, pojawiło się wiele niebezpieczeństw – takich jak: wycieki danych, kradzież tożsamości i utrata dostępu do danych.
Większość działań na platformach społecznościowych opiera się o nasze prywatne dane, począwszy od rejestracji, udostępniania zdjęć, postów, aktualności z życia, dołączanie do wydarzeń i różnego rodzaju grup. Dane te są bardzo atrakcyjne dla cyberprzestępców.

PAMIĘTAJ!
Co raz znajdzie się w sieci jest bardzo trudne do usunięcia.
Zanim coś opublikujesz, zastanów się, jakie reakcje mogą wywołać Twoje posty, co może stać się z Twoimi zdjęciami i filmami.

Niezwykle istotna jest wiedza o tym, jak zarządzać ustawieniami bezpieczeństwa i prywatności na swoich kontach, aby nasze dane osobowe były dostępne tylko dla nas.

Sprawdź, w jaki sposób można zadbać o swoją prywatność w popularnych mediach społecznościowych. Poznaj zalecenia serwisów, z których korzystasz:

- Facebook - Podstawowe ustawienia i narzędzia ochrony prywatności
- Twitter - Twitter – Jak chronić swoje Tweety
- Instagram - Ustawienia prywatności oraz informacje
- YouTube - Prywatność i Centrum bezpieczeństwa
- LinkedIn - Zarządzanie kontem i ustawieniami prywatności Informacje
- Snapchat - Snapchat Ustawienia prywatności

PAMIĘTAJ!
Korzystanie z mediów społecznościowych tylko pozornie jest bezpłatne – walutą tutaj są dane i reputacja użytkownika.

Najważniejsze zasady bezpieczeństwa w mediach społecznościowych

1

Utwórz silne hasło

Konto w serwisie społecznościowym zabezpiecz niepowtarzalnym i odpowiednio długim hasłem. Wielu użytkowników korzysta z tego samego hasła do wielu kont. Każde hasło powinno być nie tylko silne, ale też niepowtarzalne. Upewnij się, że nie korzystasz z żadnego ze swoich haseł na wielu kontach.

2

Ogranicz dostęp do konta

Uaktywnij dwuskładnikowe uwierzytelnianie na wszystkich swoich kontach. Z uwierzytelnienia dwuskładnikowego można korzystać w większości serwisów społecznościowych, a korzystanie z tej technologii nie jest uciążliwe.

3

Dodawaj do listy swoich znajomych wyłącznie osoby, które rzeczywiście znasz i którym ufasz.

Pamiętaj, że przyjmując nową osobę do grupy swoich znajomych najczęściej domyślnie udostępniasz jej swoje prywatne zdjęcia oraz informacje o sobie.

4

Nie ufaj udostępnianym w serwisach aplikacjom

Nigdy nie masz pewności, czy twórca programu jest uczciwy, czy nie jest to cyberprzestępca czyhający na Twoje dane.

5

Korzystaj tylko z oficjalnych aplikacji sieci społecznościowych

Aplikacje pobieraj wyłącznie z oficjalnych sklepów — np. Google Play dla Android, App Store dla iOS i Microsoft Store dla Windows.

6

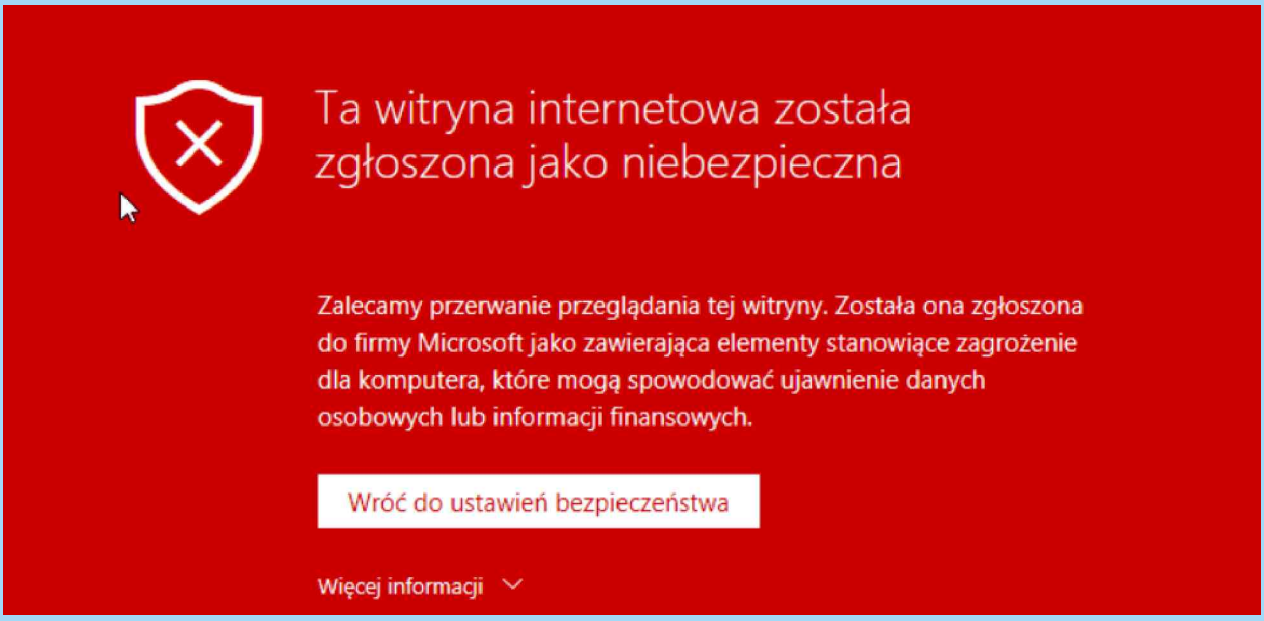
Dbaj o prywatność

Praktycznie wszystkie serwisy społecznościowe posiadają rozwiązania w zakresie zwiększania prywatności – aktywuj je!

7

Używaj programu antywirusowego i funkcji bezpieczeństwa w przeglądarkach internetowych

Dobry program antywirusowy ma zatrzymać złośliwe oprogramowanie, zanim jeszcze zostanie ono pobrane do systemu.
Najpopularniejsze przeglądarki internetowe ostrzegają o podejrzanych stronach internetowych –poważnie traktuj takie ostrzeżenia i nie odwiedzaj takich stron. Mogą zawierać złośliwe oprogramowanie, które umożliwi przestępcom przejęcie kontroli nad Twoim urządzeniem.



Jak chronić dane i prywatność w najpopularniejszych mediach społecznościowych?

Facebook

Facebook udostępnia narzędzia, które dają użytkownikom możliwość dostosowania sposobu korzystania z serwisu poprzez kontrolowanie tego, co widzą, z kim są połączeni oraz jakie informacje o nich widzą inne osoby, a także zgłaszania budzących wątpliwości treści.

Zabezpieczanie kont
Aby zapobiec włamaniu na konta, wykorzystaniu ich w niewłaściwy sposób lub posłużeniu się nimi bez zgody użytkownika, poświęć kilka chwil na przeprowadzenie kontroli bezpieczeństwa, aby sprawdzić, czy obecne ustawienia zabezpieczeń są właściwe.

- Upewnij się, że na wszystkich kontach włączono uwierzytelnianie dwuskładnikowe – to najłatwiejszy i bardzo skuteczny sposób ich ochrony.
- Rozważ włączenie zatwierdzania logowania i dodatkowych zabezpieczeń na swoich kontach.
- Podobne ustawienia można wprowadzić również do zabezpieczenia konta na Instagramie, usłudze także świadczonej przez firmę Facebook.

Zarządzanie stroną
Aby zapobiec pojawianiu się szkodliwych materiałów na Twojej stronie, możesz skorzystać z licznych narzędzi, które umożliwiają moderowanie i filtrowanie publikowanych tam treści.

Zgłaszanie i usuwanie treści
Na portalu Facebooku, obok każdej treści widnieje przycisk umożliwiający jej zgłoszenie. W przypadku stwierdzenia zagrożenia, oprócz usunięcia treści naruszających zasady - Facebook zawiadamiania także organy ścigania. Nad bezpieczeństwem czuwają Community Operations, czyli zespoły wspierające użytkowników Facebooka, dostępne 24 godziny na dobę, 7 dni w tygodniu. Obecnie nad bezpieczeństwem platformy czuwa 35 tys. osób na całym świecie.

PAMIĘTAJ!
Aby na Facebooku dokonać zgłoszenia naruszeń, skorzystaj z przycisku „Zgłoś". Wybierz odpowiednią kategorię problemu i postępuj zgodnie z instrukcjami.

Twitter

Twitter to wirtualne miejsce publiczne, gdzie poruszane są i dyskutowane wszelkiego rodzaju tematy. Dlatego też ten portal charakteryzuje się dużo większą otwartością i dużo mniejszą liczbą filtrów oraz barier w stosunku do innych sieci społecznościowych.

Wiele wiadomości na Twitterze zawiera skrócone linki. Czasami prowadzą one do niebezpiecznych miejsc, takich jak fałszywe formularze wyłudzające poufne dane lub zawierające wirusy, które są następnie pobierane przez naszą przeglądarkę. Klikanie w nieznane linki jest jedną z głównych przyczyn infekcji złośliwym oprogramowaniem za pośrednictwem portali społecznościowych, dlatego należy zachować ostrożność wobec wszelkich linków.

Najprostszym sposobem na sprawdzenie, co kryje się pod skróconym linkiem jest skorzystanie z rozszerzenia do przeglądarki, które zweryfikuje skrócony link. Do najpopularniejszych należą Unshorten.me (przeglądarka Chrome) i Unshorten.link (przeglądarka Firefox) lub z każdej wyszukiwarki unshorten.it

Jak uniemożliwić innym osobom zmianę hasła do swojego konta na Twitterze ?
Jeśli ktoś włamie się do Twojego konta, w pierwszej kolejności zapewne zmieni hasło. Aby temu zapobiec, skonfiguruj konto na Twitterze tak, aby żądało podania dodatkowych informacji (numeru telefonu lub adresu e-mail), gdy ktoś (w tym Ty) będzie próbował zmienić hasło.

Aby uniemożliwić cyberprzestępcom zmianę hasła, w sekcji Konto przejdź do pozycji Bezpieczeństwo i zaznacz pole Ochrona resetowania hasła. Pamiętaj, że to ustawienie nie pomoże, jeśli powiązany z Twoim kontem numer telefonu lub adres e-mail można znaleźć w internecie.

Usuń nieznane aplikacje ze swojego konta na Twitterze
Na Twitterze jest wiele dostępnych aplikacji (m.in. aplikacja informująca kto przestał śledzić profil, aplikacja do zdjęć, czy też aplikacja do czatowania). Coraz więcej takich programów wymaga dostępu do Twoich danych i niestety zbyt często pochopnie udzielamy zgody na ich uprawnienia. Skutkiem może być instalacja złośliwej aplikacji, która wślizgnie się między te autoryzowane. Wówczas Twoje dane znajdą się w poważnym niebezpieczeństwie.

Nie dziel się swoim kontem
Dzielenie się swoim kontem z innymi osobami może zdawać się wygodne, zwłaszcza dla osób publicznych. Nie dziel się nim jednak z osobami, o których nie możesz powiedzieć, że są absolutnie zaufane. Im więcej osób posiada dostęp do Twojego konta, tym bardziej zwiększa się ryzyko wycieku niepożądanych informacji.

Instagram

Instagram to fotograficzna sieć społecznościowa, która jest własnością Facebooka. Portal umożliwia dwa ustawienia dla konta:

- **konto publiczne** – wtedy Twoje zdjęcia, stories i inne materiały widzą wszyscy użytkownicy Instagrama;

- **konto prywatne** – Twoje zdjęcia, stories i materiały są dostępne tylko dla tych użytkowników, którym zezwolisz na obserwację. Zatwierdzasz każdą osobę pojedynczo. To znaczy, że rozsądne zatwierdzanie próśb o obserwację może być jedną z lepszych metod na zabezpieczenie swojej prywatności. Wystarczy, że zatwierdzać będziesz tylko te pochodzące od zaufanych i znajomych osób. Jest to jedyne i główne zabezpieczenie Twojej prywatności na Instagramie, oprócz blokowania poszczególnych użytkowników.

- Warto zadbać o odpowiednie zabezpieczenie każdego rodzaju konta na Instagramie, ustawienia prywatności wyglądają podobnie jak na Facebooku.

Komunikatory – jak bezpiecznie z nich korzystać?

Komunikator internetowy to program, który umożliwia szybkie przesyłanie wiadomości między użytkownikami. To najbardziej naturalna i popularna forma rozmowy w internecie. Obecnie - zamiast korzystania z tradycyjnych rozmów telefonicznych - coraz częściej wysyłamy wiadomości i rozmawiamy właśnie za pośrednictwem komunikatorów internetowych. Dlatego również tutaj nie można zapominać o podstawowych zasadach bezpieczeństwa.

PAMIĘTAJ!

Nigdy nie klikaj w linki w wiadomościach, które wydają Ci się podejrzane.

Zachowaj szczególną ostrożność, jeśli dostaniesz wiadomość od znajomego, która wydaje Ci się nietypowa i budzi Twoją wątpliwość (np. z prośbą o szybkie przesłanie kodu BLIK). Zadzwoń do znajomego i zapytaj, czy na pewno wysyłał/wysyłała Ci taką wiadomość.

Nie ujawniaj w wiadomościach żadnych poufnych danych (jak hasła, dane do logowania).

Nie odpowiadaj na podejrzane wiadomości, które otrzymujesz, szczególnie od nieznajomych osób.

Pamiętaj też, że nieszyfrowane wiadomości tekstowe (np. pisane za pośrednictwem popularnego komunikatora Messenger) mogą być przechwycone przez prawie każdego. Znacznie bezpieczniej jest używać narzędzi do przesyłania wiadomości, które wykorzystują szyfrowanie typu end-to-end (inaczej E2E), takich jak WhatsApp itp. Upewnij się jednak, że masz zainstalowaną prawdziwą aplikację, a nie fałszywą – np. sprytnie nazwaną „Aktualizuj WhatsApp Messenger", która oszukała ponad milion osób, które ją pobrały. W przypadku komunikatora WhatsApp duże kontrowersje budzi zapis w polityce umożliwiający wykorzystywanie danych przez Facebook.

PAMIĘTAJ!

Jeśli zależy Ci na prywatności - korzystaj z komunikatorów, które w minimalnym stopniu korzystają i zapisują Twoje dane. Warto zwracać uwagę, czy aplikacje mają otwarty kod, który umożliwia uczciwym zainteresowanym badanie ich bezpieczeństwa.

Komunikatory szyfrujące wykorzystują specjalną technologię, która w założeniu ma chronić informacje zawarte w przesłanych przez użytkowników wiadomościach. Gwarantują większe bezpieczeństwo prywatności i chronią dane przed przeglądaniem przez inne nieupoważnione osoby.
Na rynku jest coraz więcej tego typu rozwiązań. Obecnie, do najbardziej popularnych należą: Signal i WhatsApp.

UWAGA: przytoczone w poradniku przykłady komunikatorów odnoszą się do najpowszechniej stosowanych. Nie oznacza to, że rekomendujemy użycie tych konkretnych aplikacji, w szczególności do przekazywania jakichkolwiek kategorii informacji prawnie chronionych.

Jak stwierdzić, czy zabezpieczenia naszego konta w serwisie społecznościowym zostały złamane?

Jeśli nie stosujesz podstawowych zasad bezpieczeństwa - uzyskanie dostępu do Twoich kont w serwisach społecznościowych jest dla cyberprzestępców łatwiejsze niż się wydaje.

Co może świadczyć o włamaniu na konto?

- Otrzymujesz wiadomość e-mail z informacją o zmianie danych logowania, która nie została przez Ciebie zainicjowana.
- Masz problem z zalogowaniem się do swoich kont.
- Otrzymujesz mnóstwo reklam, które mają charakter spamu.
- Nagle zauważasz, że obserwujesz osoby, których nie znasz.
- Na Twoim koncie jest publikowana zawartość, która nie została przez Ciebie utworzona.
- Widzisz konto, które wykorzystuje Twoje imię i nazwisko i/lub Twoje zdjęcia.

Co robić, kiedy podejrzewamy, że konto zostało zaatakowane?

Postaraj się zalogować i sprawdzić dane dotyczące konta (adres e-mail i telefon), aby podjąć próbę sprawdzenia, kto ma dostęp do Twoich informacji

Gdy tylko zorientujesz się, że zabezpieczenia Twoich kanałów społecznościowych zostały złamane, sprawdź informacje dotyczące konta, aby przekonać się, czy żaden inny adres e-mail - poza Twoim adresem - nie ma dostępu do konta. Jeśli tak jest, natychmiast usuń ten adres.

Następnie sprawdź numer telefonu powiązany z Twoim kontem - jedynie Twój numer telefonu powinien być powiązany z kontem. Jeśli na koncie znajdują się jakiekolwiek nieznane numery, usuń je.
Często zdarza się, że po złamaniu zabezpieczeń konta atakujący dodaje do niego numer telefonu, którego może użyć w późniejszym czasie do zmiany hasła do konta.

Natychmiast zmień hasło na nowe - silne i niepowtarzalne - i włącz uwierzytelnianie dwuskładnikowe.

Sprawdź swoje konta w innych serwisach społecznościowych i poszukaj zaleceń dotyczących czynności w przypadku ataku.

W serwisach społecznościowych publikowane są zalecenia dotyczące działań, jakie należy podjąć, jeśli zabezpieczenia konta zostały złamane. Dzięki zawartym tam informacjom będziesz mieć pewność, że robisz wszystko, co możliwe, by zabezpieczać i chronić swoje konta.

Oto linki do wskazówek, co zrobić w przypadku ataków na konta w popularnych serwisach społecznościowych:

- Facebook - https://www.facebook.com/hacked
- Twitter - https://help.twitter.com/pl/rules-and-policies/twitter-report-violation
- Instagram - https://help.instagram.com/

LinkedIn - https://www.linkedin.com/help/linkedin?lang=pl

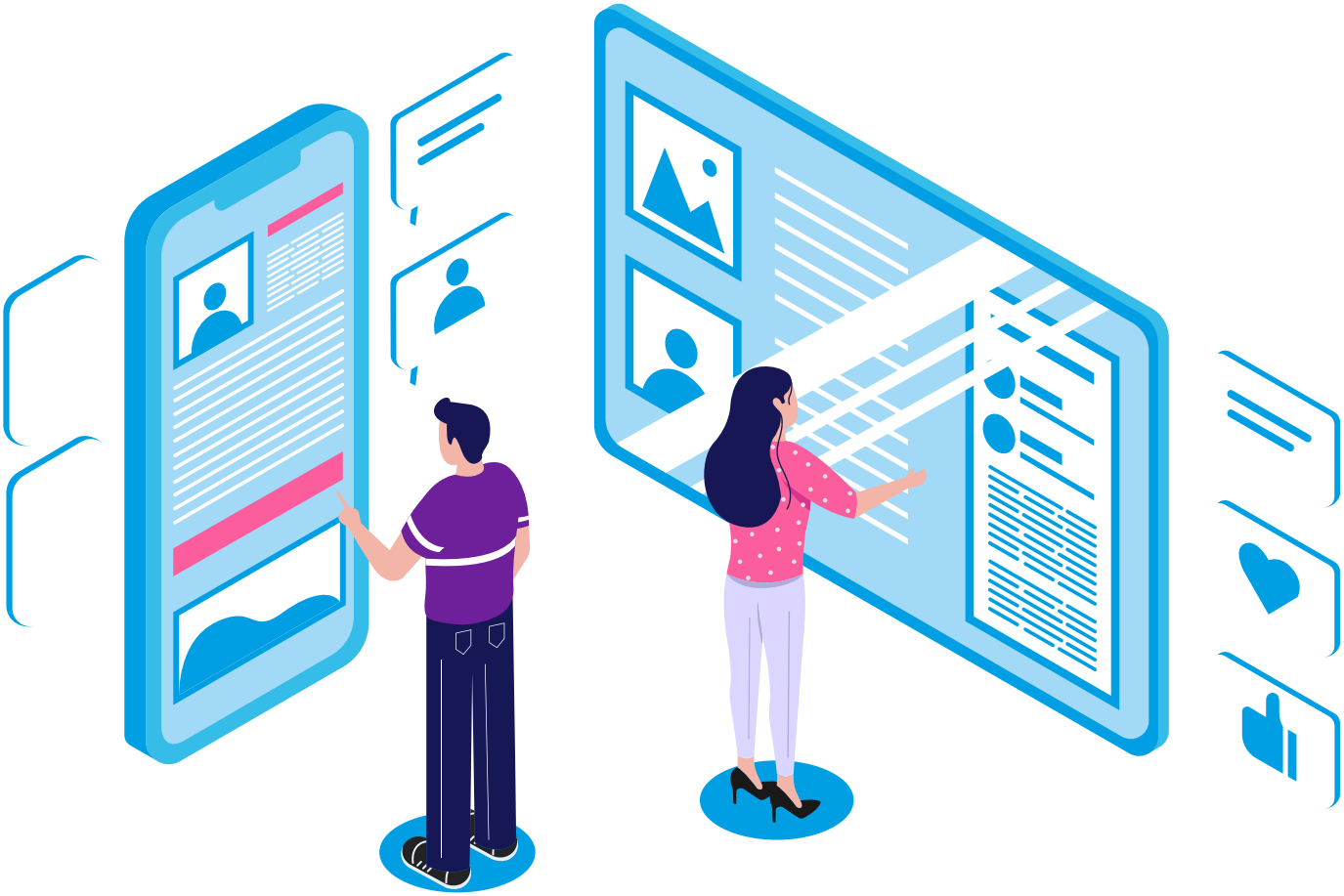
YouTube - https://support.google.com/youtube/?hl=en#topic=9257498

Snapchat - https://www.snap.com/pl-PL/safety/safety-center

Gdzie zgłaszać podejrzenia włamań na konta w mediach społecznościowych lub innych serwisach internetowych?

- Policja – Biuro do Walki z Cyberprzestępczością: cyber-kgp@policja.gov.pl
  Należy pamiętać, że w każdej wojewódzkiej komendzie Policji działa Wydział do Walki z Cyberprzestępczością.

- NASK (CSIRT NASK) cert@cert.pl oraz https://incydent.cert.pl/



Słownik pojęć

Adres IP *(z ang. Internet Protocol)* – to unikalny numer identyfikujący urządzenie w Internecie lub sieci lokalnej. Pozwala internetowi znaleźć konkretne urządzenie wśród miliardów innych podłączonych do niego urządzeń. Porównując do „normalnego" życia – to odpowiednik kodu pocztowego, ulicy i numeru domu.

Aplikacja mobilna – oprogramowanie działające na urządzeniach przenośnych, np. na smartfonie czy tablecie. Usługami, jakie oferują aplikacje mobilne są np. przelewy bankowe z dostępem do konta bankowego, zakupy internetowe, czytanie e-booków lub dostęp do poczty elektronicznej.

Awatar – inaczej zdjęcie profilowe lub grafika, która reprezentuje nas w sieci. Może nim być nasze własne zdjęcie, ale nie musi. Awatarów używa się zarówno w mediach społecznościowych, jak i w grach komputerowych.

Backup (kopia zapasowa) – metoda ochrony danych przed zniszczeniem i utratą. Polega na wykonywaniu ich kopii bezpieczeństwa. Innymi słowy backup to kopie informacji, które są przechowywane gdzie indziej niż ich oryginał. Kiedy stracisz ważne dane, można je odzyskać właśnie z kopii zapasowych. Dlatego warto regularnie robić kopie zapasowe!

Ban – zablokowanie użytkownika, gdy naruszy regulamin danej platformy (np. po publikacji nieodpowiednich, szkodliwych treści lub założeniu fałszywego konta na platformie). Zablokowany użytkownik nie może publikować postów i komentarzy na portalu.

Captcha *(z ang. Completely Automated Public Turing test to tell Computers and Humans Apart)* – rodzaj zabezpieczenia, którego zadaniem jest ochrona przed spamem oraz powstrzymanie automatów (zwanych botami) przed wprowadzaniem jakichkolwiek danych do serwisu internetowego. System polega na wyświetleniu prostego do wykonania testu, który ma za zadanie potwierdzić, że dane np. w formularzu zostały wprowadzone przez człowieka. Weryfikacja odbywa się zazwyczaj poprzez konieczność odczytania i przepisania zniekształconego tekstu z wyświetlonego obrazka.

CERT *(z ang. Computer Emergency Response Team)* – zespół reagowania na incydenty bezpieczeństwa. Jego zadaniem jest reagowanie na zdarzenia naruszające bezpieczeństwo sieci i systemów informacyjnych oraz prowadzenie działalności informacyjno-zapobiegawczej.

CSIRT *(z ang. Computer Security Incident Response Team)* – zespół reagowania na incydenty bezpieczeństwa komputerowego. Ustawa o krajowym systemie cyberbezpieczeństwa ustanowiła trzy Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego: CSIRT NASK, CSIRT GOV oraz CSIRT MON. Każdy z CSIRT odpowiedzialny jest za koordynację incydentów zgłaszanych przez przyporządkowane - zgodnie z ustawą - podmioty.

Chmura obliczeniowa *(z ang. cloud computing)* – to środowisko informatyczne dostarczające usługi chmurowe oraz infrastrukturę IT

za pośrednictwem internetu (tj. serwery, przestrzeń dyskowa, bazy danych, sieć, oprogramowanie, moc obliczeniowa, systemy backupu, systemy bezpieczeństwa itp.). Chmura obliczeniowa jest rozwiązaniem niewymagającym ponoszenia kosztów inwestycyjnych związanych z koniecznością wybudowania drogiej infrastruktury serwerowej. Cechuje ją wysoka wydajność, skalowalność zasobów oraz pełna dostępność dla każdego użytkownika w zależności od jego potrzeb. Opłaty ponoszone są za faktyczne użycie i tylko w okresie użytkowania.

DDoS *(z ang. distributed denial of service, co oznacza rozproszoną odmowę usługi)* – to rodzaj ataku np. na serwer lub stronę internetową, który generuje sztuczny ruch i może doprowadzić do niedostępności usług (np. sklepu internetowego, bankowości internetowej). Serwer, na którym znajduje się dana strona internetowa, dostaje w pewnym momencie tak dużą liczbę zapytań (prób otwarcia witryny), że następuje jego przeciążenie i przestaje radzić sobie z obsługą ruchu sieciowego. Kolejne osoby, które próbują połączyć się z serwerem, wchodząc na zaatakowaną stronę, otrzymują informację o czasowym braku dostępu do usługi

Domena – to unikalny adres internetowy, pod którym usługi, firmy, instytucje są dostępne w internecie. Nazwa domeny jest niepowtarzalna.

E-mail – inaczej poczta elektroniczna. To usługa internetowa, w nomenklaturze prawnej określana jako świadczenie usług drogą elektroniczną, służąca do przesyłania wiadomości tekstowych lub multimedialnych, tzw. listów elektronicznych.

Firewall – zapora sieciowa. To usługa, urządzenie lub program, który jest jednym z zabezpieczeń komputera przed włamaniem dokonywanym przez hakerów. Zadaniem zapory jest filtrowanie danych wychodzących i przychodzących do komputera poprzez sieć lub internet.

Haker – osoba, która korzysta z umiejętności komputerowych, aby uzyskać nieautoryzowany dostęp do danych, takich jak np.: karty kredytowe lub prywatne zdjęcia.

Hashtag – słowo lub połączenia słów oznaczone na początku symbolem kratki (#) i spełniające w ten sposób funkcję słów kluczowych lub wyszukiwanych pojęć. Hashtagi pozwalają użytkownikom serwisów łączyć swoje posty z danymi tematami. Dzięki temu inni użytkownicy mogą je znajdować.

Login – inne określenie na identyfikator użytkownika. Można powiedzieć, że jest to pseudonim używany internecie. Słowo login pochodzi od ang. log in, rozumianego jako polecenie wejścia do systemu komputerowego. Wyrażenie to ewoluowało do pojedynczego słowa login, rozumianego w uproszczeniu jako wymagany identyfikator, a nie czynność.

Malware – różnego rodzaju szkodliwe programy, które usiłują zainfekować komputer lub urządzenie mobilne.

Platforma internetowa – rozbudowane strony o określonych funkcjach, które umożliwiają interaktywny kontakt między użytkownikami i dostawcami usług.

Portal internetowy – złożonym ekosystemem, który użytkownik końcowy odbiera jako spójną całość. Portale od stron internetowych odróżnia ich wielkość i wielowarstwowość. Strona internetowa skupia się przede

wszystkim na udostępnianiu treści w konkretnym zakresie tematycznym, ma głównie charakter informacyjny. Natomiast portal oferuje szeroki zakres tematyczny informacji, skierowanych do różnych grup odbiorców. Często zawiera interaktywne elementy (takie jak kalkulatory czy formularze wniosków) i może wymagać zalogowania przed uzyskaniem dostępu do wszystkich funkcjonalności i treści.

Profil – część serwisu społecznościowego, zawierająca informacje o danym użytkowniku.

SCAM – oszustwo polegające na wzbudzeniu czyjegoś zaufania, a następnie wykorzystaniu tego zaufania do wyłudzenia pieniędzy lub innych składników majątku. Osoba wzbudzająca fałszywe zaufanie zwykle działa na jedną z ludzkich cech charakteru, zarówno negatywnych, jak i pozytywnych, takich jak: pycha i chciwość, ale też empatia i altruizm. Oszuści często działają na portalach społecznościowych, na których informacje bardzo szybko się rozchodzą, przez co zyskują duże zainteresowanie i zasięg.

SPAM – niechciane i potencjalnie szkodliwe wiadomości wysyłane masowo. Najbardziej rozpowszechniony jest spam wysyłany za pośrednictwem poczty elektronicznej, komunikatorów internetowych i wiadomości SMS.

Spearphishing – atak ukierunkowany na KONKRETNEGO adresata, mający na celu wywarcie określonego wpływu lub wymuszenia działania w stosunku do odbiorcy. Przestępcy mogą podszywać się pod naszych znajomych lub np. partnerów biznesowych. Wiadomość jest spersonalizowana, tzn. bezpośrednio odwołuje się do naszych relacji. Taki typ ataku jest często poprzedzony dokładnym rozpoznaniem przez atakującego np. naszego miejsca pracy, a także zebraniem i analizą informacji dostępnych o nas w mediach społecznościowych.

Vishing – metoda oszustwa, polegająca na wyłudzaniu danych w trakcie rozmowy telefonicznej. W tym przypadku definicja stanowi wariację słów „voice" (z ang. głos) i „fishing". Oszuści dzwonią do ofiary podając się za pracownika np. banku, kancelarii prawnej lub innej zaufanej instytucji. W trakcie rozmowy proszą o podanie loginu i hasła do bankowości internetowej i innych poufnych danych. Następnie - o podanie kodu SMS. Na podstawie tych danych oszust może m.in. zmienić w bankowości numer telefonu do autoryzacji transakcji. Od tej chwili kody SMS będą wysyłane na telefon przestępcy. W ten sposób złodziej może wyczyścić konto z pieniędzy.

VPN *(z ang. Virtual Private Network – Wirtualna Sieć Prywatna)* – technologia, która tworzy prywatny, szyfrowany tunel dla naszych działań online, czyniąc je o wiele trudniejszymi dla innych do obserwowania lub monitorowania tego co robimy w internecie. Ponadto VPN ukrywa lokalizację użytkownika, utrudniając zidentyfikowanie naszego położenie stronom internetowym, które odwiedzamy.

2FA – uwierzytelnianie dwuskładnikowe (ang. Two Factor Authenticaton, skracane do 2FA) zapewnia „podwójne sprawdzanie", że naprawdę jesteś osobą, za którą się podajesz, gdy korzystasz z usług online. Dostępny w większości powszechnych usług online, takich jak bankowość, poczta e-mail lub media społecznościowe. Podczas konfigurowania 2FA usługa poprosi Cię o podanie „drugiego składnika", do którego masz dostęp tylko Ty.

GOV.pl
CYFRYZACJA

Więcej informacji:
gov.pl/cyfryzacja