CYBERBEZPIECZEŃSTWO

Źródło: materiały Państwowego Instytutu Badawczego NASK

Bezpieczeństwo w sieci

Zweryfikuj nazwę

- Linki, które prowadzą na podejrzane strony, mogą wyglądać na prawdziwe, ale zawierają drobne zmiany, np. literówki lub dodatkowe znaki.

Uważaj na skrócone linki

- Nie pokazują one pełnego adresu strony, dlatego oszuści z premedytacją wykorzystują je m.in. w wiadomościach SMS.

Sprawdź e-mail nadawcy

- Upewnij się, że brzmi on przekonująco, a część po znaku „@” nawiązuje do oficjalnej strony instytucji. Aby zobaczyć pełen adres, wystarczy, że klikniesz w pole nadawcy.

Bezpieczeństwo w sieci

Nie działaj pochopnie

- Często oszuści tworzą wrażenie, że konieczna jest Twoja szybka reakcja. Nie podejmuj decyzji pod wpływem emocji, ani też presji czasu.

Nie udostępniaj swoich danych

- Zwłaszcza takich jak PESEL, data urodzenia, numery kart płatniczych, loginy czy hasła do kont.

Zachowaj ostrożność

- Z ostrożnością podchodź do linków i załączników, które otrzymasz w wiadomości, jeśli nie wiesz, od kogo pochodzą i co się w nich znajduje.

Bezpieczeństwo w sieci

Nie trać czujności

- Nie loguj się do banku lub na inne konta za pośrednictwem linku otrzymanego w wiadomości e-mail lub SMS.

Zgłaszaj próby oszustwa

- Jeżeli coś budzi Twoje wątpliwości, poinformuj o tym CERT Polska! Takie zgłoszenie pomoże chronić innych!

Regularnie aktualizuj systemy i aplikacje

Twoje urządzenia i zainstalowane na nich programy przechowują tysiące danych - zarówno tych, które samodzielnie wprowadzisz, jak i tych, które są automatycznie zapisywane podczas codziennego korzystania z urządzenia, np. historia przeglądania, dane logowania, pliki, informacje o aktywności czy dane zapisane przez aplikacje. Te dane są pożądane przez oszustów, a dostęp do chronionych zasobów jest głównym celem każdego cyberprzestępcy. Dlatego każdego dnia hakerzy znajdują nowe podatności, a producenci oprogramowania publikują aktualizacje, które mają uszczelniać odkryte dziury.

Regularne aktualizowanie swoich systemów i programów to kluczowy element bezpieczeństwa. Warto korzystać z możliwości automatycznych aktualizacji, które oferują dostawcy urządzeń i dystrybutorzy aplikacji. Nie ignorujmy też przypomnień o aktualizacjach! Jeśli nawet pojawią się w nieodpowiedniej chwili, bo akurat aktywnie korzystamy z konkretnego narzędzia, poświęćmy chwilę, by zaplanować właściwy moment aktualizacji - po pracy, w nocy lub o dowolnej innej porze. Ważne, żeby stało się to jak najszybciej.

Oddziel pracę i prywatne urządzenia

Nie przechowuj dokumentów służbowych na prywatnym komputerze czy telefonie i nie przesyłaj ich na prywatne skrzynki e-mail. Firmowe zabezpieczenia chronią dane tylko wtedy, gdy korzystasz z zatwierdzonych urządzeń i narzędzi.

Na urządzeniach służbowych wykonuj wyłącznie zadania związane z pracą, a do prywatnych aktywności korzystaj z własnego sprzętu. Dzięki temu łatwiej chronić firmowe informacje i ograniczyć skutki ewentualnego cyberataku.

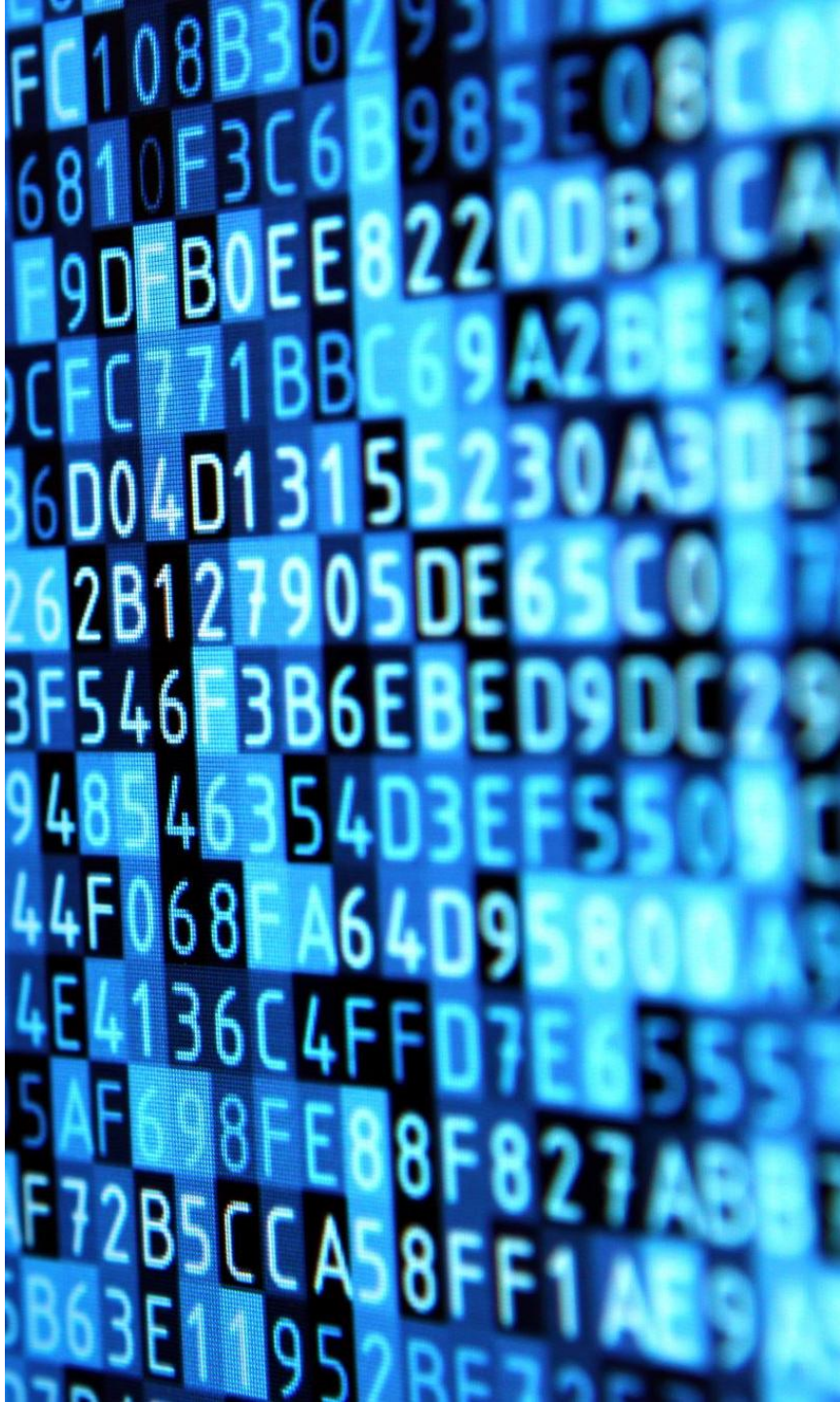
Włącz uwierzytelnianie dwuetapowe (2FA)

Samo hasło może nie wystarczyć – jeśli cyberprzestępca je zdobędzie, bezpieczeństwo Twoich kont pomoże zapewnić uwierzytelnianie dwuetapowe (2FA). Jest to potwierdzenie logowania za pomocą dodatkowego elementu, np. kodu z aplikacji uwierzytelniającej, powiadomienia na telefonie lub klucza bezpieczeństwa. Nawet jeśli hasło zostanie ujawnione, dodatkowe zabezpieczenie znacząco utrudni przejęcie konta.

W pierwszej kolejności uruchom dodatkowe zabezpieczenie dla poczty elektronicznej, bankowości, mediów społecznościowych i innych usług przechowujących ważne dane. To jeden z najprostszych i najskuteczniejszych sposobów wzmocnienia ochrony kont przed nieuprawnionym dostępem.

Używaj długich haseł i menedżera haseł

- Mocne hasła to jedna z podstawowych metod ochrony kont. Im są dłuższe i bardziej unikalne, tym trudniej je odgadnąć lub złamać. Dlatego zamiast krótkich kombinacji warto stosować hasła składające się z co najmniej 14 znaków.
- Żeby zapamiętać wszystkie hasła do różnych usług korzystaj z menedżera haseł, który bezpiecznie przechowuje dane logowania. Dzięki temu wystarczy pamiętać jedno silne hasło główne (najczęściej dodatkowo wspierane przez uwierzytelnianie dwuetapowe i/lub biometryczne). Aplikacja ułatwi też codzienne logowanie się na różnych stronach, a nawet zakładanie nowych kont, podpowiadając właściwe dane uwierzytelniające.
- Długie, niepowtarzalne hasła w połączeniu z menedżerem znacząco zwiększają poziom bezpieczeństwa i zmniejszają ryzyko utraty dostępu do ważnych kont oraz danych.



Nie używaj tych samych haseł w różnych miejscach

Nie używaj tego samego hasła w różnych serwisach. Jeśli hasło zostanie przejęte, cyberprzestępcy będą próbować wykorzystać te same dane logowania w innych usługach takich jak poczta elektroniczna, media społecznościowe czy bankowość internetowa.

Każde konto powinno mieć własne, unikalne hasło. Zapisuj je w menedżerze haseł, który bezpiecznie przechowuje dane logowania.

Weryfikuj zaskakujące informacje i prośby innymi kanałami

Jeśli znajomy pisze na komunikatorze, zadzwoń do niego na znany Ci numer telefonu. Dostałeś wiadomość SMS od Twojego dziecka? Napisz do niego na innym komunikatorze lub zadzwoń. Kilkadziesiąt sekund poświęconych na weryfikację może uchronić Cię przed utratą pieniędzy i danych. Podejrzane wiadomości zgłaszaj do zespołu CERT Polska na bezpłatny numer 8080. Twoje zgłoszenie pomaga chronić Ciebie i innych użytkowników.

Sygnałem ostrzegawczym powinna być każda nietypowa sytuacja: niespodziewany link, prośba o kod BLIK, pilny przelew lub wiadomość od osoby, z którą nie miałeś kontaktu od dłuższego czasu. W takiej sytuacji nie działaj pod wpływem emocji. Upewnij się najpierw, że wiadomość rzeczywiście pochodzi od osoby, za którą podaje się nadawca.

Nieoczekiwana wiadomość z linkiem od znajomego sprzed lat? Prośba od bliskiej osoby o szybki przelew lub kod BLIK? Informacja o wypadku kogoś z rodziny i pilnej potrzebie pieniędzy? A może znajomy przekonuje Cię do inwestycji, na której rzekomo szybko się wzbogacił?

Cyberprzestępcy często wykorzystują fakt, że ufamy osobom, które znamy. Mogą tworzyć fałszywe profile lub przejmować prawdziwe konta w mediach społecznościowych i komunikatorach. W efekcie wiadomość może wyglądać wiarygodnie, ponieważ jest wysłana z konta znajomego i podpisana jego nazwiskiem.

Sprawdzaj adres strony przed wpisaniem danych

Cyberprzestępcy tworzą strony do złudzenia przypominające serwisy banków, sklepów internetowych, bramek płatności czy mediów społecznościowych. Kopiują logo, zdjęcia, treści oraz układ witryny, dzięki czemu na pierwszy rzut oka trudno dostrzec jakiekolwiek różnice. Sam wygląd strony nie jest więc wiarygodnym potwierdzeniem jej autentyczności. Dlatego przed wpisaniem loginu, hasła, danych karty płatniczej lub innych informacji osobistych zawsze uważnie weryfikuj adres wyświetlany w pasku przeglądarki.

Oszuści rejestrują domeny bardzo podobne do prawdziwych adresów, licząc na pośpiech i nieuwagę użytkowników. Czasem zmieniają jedną literę, dodają myślnik lub dopisują dodatkowy wyraz, przez co fałszywy adres może wyglądać wiarygodnie. Spójrz:

- twojbank.pl
- twojbamk.pl
- twoj-bank.pl
- twojbank-logowanie.pl

Jeśli masz choćby cień wątpliwości, nie podawaj swoich danych! Zamiast tego zamknij stronę i samodzielnie znajdź oficjalny adres serwisu w wyszukiwarce lub skorzystaj z zapisanej wcześniej zakładki. Sprawdzenie adresu zajmuje zaledwie kilka sekund, a może uchronić Cię przed utratą danych i pieniędzy lub przejęciem konta.

Uważaj na „zbyt dobre” oferty inwestycyjne – to często oszustwo

Szybki i wysoki zysk przy niewielkim ryzyku to może być sygnał ostrzegawczy. Oszustwa inwestycyjne często zaczynają się od atrakcyjnej reklamy w mediach społecznościowych lub wyszukiwarce. Jeśli zostawimy tam swoje dane, skontaktuje się z nami rzekomy doradca inwestycyjny, który będzie zachęcał do szybkiej wpłaty pieniędzy. Wykorzysta w tym celu socjotechniki, czyli techniki manipulacji oparte na presji czasu, autorytecie, groźbie kary lub obietnicy dodatkowej nagrody.

Nie ufaj ofercie tylko dlatego, że zachęca do niej znana osoba. Oszuści coraz częściej wykorzystują nowoczesne technologie do tworzenia fałszywych materiałów, które mogą sprawiać wrażenie autentycznych rekomendacji.

Przestrzegaj prostej zasady: nie działaj pod presją czasu, nie wierz w gwarantowany zysk bez ryzyka i zawsze samodzielnie weryfikuj ofertę. W razie wątpliwości sprawdź ostrzeżenia publikowane przez Komisję Nadzoru Finansowego.

Przy podejrzanym telefonie (np. z banku) – rozłącz się i zadzwoń do swojego banku samodzielnie

Niepokojący telefon z banku? Ktoś informuje Cię o podejrzanej transakcji albo próbie włamania na Twoje konto i przekonuje, że trzeba działać natychmiast? Nie daj się ponieść emocjom. To jeden ze sposobów działania oszustów.

Nie działaj pochopnie. Presja czasu ma sprawić, że podejmiesz błędną decyzję, zanim zdążysz się zastanowić. Nie wykonuj przelewów ani innych operacji tylko dlatego, że rozmówca twierdzi, że sytuacja jest pilna.

Nie przekazuj danych i nie instaluj aplikacji. Nie podawaj haseł, danych logowania ani kodów SMS. Nie udostępniaj zdalnego dostępu do telefonu czy komputera na prośbę rozmówcy, nawet jeśli twierdzi, że to konieczne lub usprawni proces.

Rozłącz się i sprawdź. Jeśli coś wzbudza Twoją wątpliwość, zakończ rozmowę. Skontaktuj się z bankiem samodzielnie, korzystając z oficjalnego numeru infolinii albo sprawdź informacje w swojej aplikacji bankowej lub portalu bankowości elektronicznej.

Rób kopie zapasowe ważnych danych

Przygotowanie kopii zapasowych (backupu) to ostatnia, ale równie ważna zasada w naszym zbiorze. Odpowiednio zarządzane kopie chronią przed wypadkami natury losowej czy szkodliwym oprogramowaniem. Nieprzypadkowa jest też liczba mnoga - złota zasada przygotowaniu backupów to 3-2-1: trzy kopie, dwa różne typy nośników danych, przynajmniej jedna przechowywana w innym miejscu. To może wydawać się trudne, ale w rzeczywistości bardzo się przydaje.

Jeśli przechowujemy swoje dane w jakimś urządzeniu - na przykład komputerze - to chwilowy skok napięcia w sieci lub pechowo rozlana kawa mogą nas kosztować lata wspomnień, dokumentów biznesowych albo innych ważnych materiałów. Jeśli dodatkowo mamy ich kopię na zewnętrznym dysku leżącym w szafce, to łatwo je odzyskamy. Jednak w przypadku powodzi albo pożaru przepadną oba - trzecia kopia, na przykład w chmurze, pozwoli ochronić dane również przed tego typu zagrożeniem.

Warto korzystać z automatycznych rozwiązań do tworzenia kopii zapasowych - w aplikacji dostawcy usług chmurowych możemy wybrać, które pliki i foldery będą się automatycznie synchronizować. Co jakiś czas możemy też ręcznie podpiąć i zsynchronizować dysk zewnętrzny. Nie chodzi o to, żeby robić to po każdym wykonanym zadaniu, ale w razie wypadku lepiej stracić dane z ostatniego tygodnia niż z kilku lat.

Dodatkowym bonusem jest sytuacja, w której chcemy zmienić telefon, laptopa czy komputer. Mając odpowiednio przygotowaną kopię zapasową, odtworzenie swojego środowiska pracy na nowym urządzeniu jest proste, szybkie i wygodne.