www.citihandlowy.pl
Bank Handlowy w Warszawie S.A.

150 lat postępu

citi handlowy®

Zabezpieczanie swojej sieci domowej

Obecnie sieć domowa może obejmować różne urządzenia bezprzewodowe, od komputerów i telefonów po kamery internetowe, inteligentne telewizory i inne podłączone urządzenia.

Przeczytaj instrukcje użytkownika otrzymane od producentów swoich routerów i komputerów i rozważ przedstawione poniżej podstawowe działania, by lepiej zabezpieczyć swoją sieć domową. Pomoże ci to lepiej chronić swoje urządzenia – i informacje – przed przechwyceniem:

1.
Zastąp domyślne hasło administratora (lub „admina") swojego domowego routera wi-fi na mocne hasło złożone z co najmniej 8 znaków i zawierające cyfry, wielkie i małe litery oraz znaki niealfanumeryczne.

2.
Wyłącz ustawienie umożliwiające zdalny dostęp i administrowanie twoim routerem wi-fi z internetu, jeżeli twój router takie ma.

3.
Sprawdź, czy wybrałeś WPA2 lub WPA3 dla ochrony twojego routera wi-fi.

4.
Zmień wszelkie domyślne kody dostępowe do twojej sieci wi-fi tak, aby miały podobną siłę i długość, jak opisano powyżej.

5.
Wyłącz funkcję WPS.

6.
Wyłącz udostępnianie PP2P na swoim routerze.

7.
Jeśli przyjmujesz w domu gości i chcesz udostępnić im swój internet, większość routerów wi-fi ma funkcję tworzenia sieci dla gości. Dzięki temu goście uzyskają dostęp do internetu, lecz ich komputery, telefony, tablety itp. nie będą mieć dostępu do twojej osobistej sieci i urządzeń.

8.
Włącz wbudowane zapory (firewall) na swoim routerze albo – jeśli używasz komputerów z systemem Windows lub Mac – upewnij się, że wbudowana bezpłatna zapora systemowa jest włączona.

9.
Dopilnuj, by program antywirusowy był zawsze włączony, aktualizował się automatycznie i rutynowo przeprowadzał skanowanie. Jeśli nie masz programu antywirusowego, możesz skorzystać z wielu różnych darmowych opcji, takich jak Windows Defender, który jest częścią systemu operacyjnego Windows.

Przypominamy, że klienci Citi Handlowy są odpowiedzialni za ochronę swoich komputerów i innych urządzeń, a także danych używanych do logowania, by przez cały czas zapewnić sobie bezpieczeństwo. Niniejsza informacja nie stanowi potwierdzenia zamiaru ani zobowiązania Citi Handlowy do przejęcia obowiązków twojej organizacji w tym zakresie.

Poniżej podano dodatkowe informacje dotyczące szyfrowania, konfiguracji sieci i ochrony urządzeń mobilnych.

Zasady działania sieci bezprzewodowych

Stosowanie łączności bezprzewodowej wymaga podłączenia internetowego „punktu dostępowego" – np. modemu przewodowego lub DSL – do routera bezprzewodowego, który wysyła sygnał drogą radiową, czasem nawet na odległość kilkuset metrów. Każde urządzenie w tym zasięgu może odebrać sygnał radiowy i uzyskać dostęp do internetu.

Jeżeli nie zastosujesz pewnych zabezpieczeń, każda osoba w pobliżu będzie mogła korzystać z twojej sieci. Oznacza to, że twoi sąsiedzi – albo hakerzy – mogą wykorzystać twoją sieć lub zyskać dostęp do informacji znajdujących się na twoim urządzeniu. Jeżeli osoba nieupoważniona wykorzysta twoją sieć do popełnienia przestępstwa lub wysyłki spamu, taką aktywność będzie można prześledzić wstecz aż do Twojego konta.

Stosuj szyfrowanie w swojej sieci bezprzewodowej

Gdy zaczniesz korzystać z sieci bezprzewodowej, szyfruj informacje wysyłane przez sieć, by cyberprzestępcy znajdujący się w pobliżu nie mogli podsłuchać tej komunikacji. Szyfrowanie przekształca przesyłane informacje do postaci kodu niedostępnego dla innych. Szyfrowanie jest najskuteczniejszym sposobem zabezpieczania swojej sieci przed intruzami.

W tym celu dostępne są dwa rodzaje szyfrowania: Wi-Fi Protected Access (WPA) oraz Wired Equivalent Privacy (WEP). Twój komputer, router i inne urządzenia muszą stosować to samo szyfrowanie. Najmocniejsze szyfrowanie to WPA2 – stosuj je, jeśli możesz. Niektóre starsze routery stosują tylko szyfrowanie WEP, które raczej nie obroni cię przed niektórymi powszechnie stosowanymi programami hakerskimi. Rozważ zakup nowego routera z szyfrowaniem WPA2.

Routery bezprzewodowe są często dostarczane z wyłączonym szyfrowaniem. Musisz je włączyć, jeśli chcesz korzystać z jakiegokolwiek zabezpieczenia przed hakerami. Instrukcja dołączona do routera wyjaśni ci, jak to zrobić. Jeśli nie, zajrzyj na stronę internetową producenta.

Ogranicz dostęp do swojej sieci

Ustaw swoją sieć bezprzewodową tak, by dostęp do niej miały tylko wskazane urządzenia. Każde urządzenie, które może komunikować się z siecią, ma przypisany niepowtarzalny adres Media Access Control (MAC). Routery bezprzewodowe zwykle mają mechanizm, który umożliwia dostęp do sieci tylko urządzeniom z określonymi adresami MAC. Niektórzy hakerzy podszywają się pod adresy MAC, więc nie polegaj tylko na tym zabezpieczeniu.

Zabezpiecz swój router

Równie ważne jest chronienie swojej sieci przed atakami przez internet poprzez zabezpieczenie swojego routera. Twój router kieruje ruchem między twoją siecią lokalną a internetem. Dlatego stanowi twoją pierwszą linię obrony przed takimi atakami. Jeśli nie zabezpieczysz routera, obcy mogą zyskać dostęp do wrażliwych informacji osobistych lub finansowych znajdujących się na twoim urządzeniu. Mogą również przejąć kontrolę nad twoim routerem, by kierować cię na fałszywe strony internetowe.

Zmień domyślną nazwę swojego routera. Prawdopodobnie nazwa twojego routera (często określana jak *service set identifier*, czyli SSID) to standardowy domyślny identyfikator przypisany przez producenta. Zmień ją na coś wyjątkowego, znanego tylko tobie.

Zmień fabryczne hasło (hasła) do routera. Producent twojego routera bezprzewodowego prawdopodobnie ustawił standardowe domyślne hasło, które umożliwia ci konfigurowanie i korzystanie z routera jako jego „administrator". Hakerzy znają te domyślne hasła, dlatego zmień je na coś, co będzie znane tylko tobie. To samo dotyczy wszystkich domyślnych haseł „użytkownika". Stosuj długie i skomplikowane hasła, najlepiej o długości co najmniej 12 znaków, zawierające cyfry, symbole oraz małe i wielkie litery. Wejdź na firmową stronę internetową i dowiedz się, jak zmienić hasło.

Wyłącz wszystkie funkcje „zdalnego zarządzania". Niektóre routery mają opcję umożliwiającą zdalny dostęp do mechanizmów sterowania, np. po to, by umożliwić producentowi realizację wsparcia technicznego. Nigdy nie zostawiaj tej funkcji włączonej. Hakerzy mogą ją wykorzystać, by dostać się do twojej sieci domowej.

Wyloguj się jako administrator. Gdy już skonfigurujesz swój router, wyloguj się jako administrator, by zmniejszyć ryzyko, że ktoś inny mógłby wykorzystać twoją sesję do przejęcia kontroli nad twoim urządzeniem.

Aktualizuj swój router. Żeby oprogramowanie, które otrzymujesz wraz z routerem, było bezpieczne i wydajne, trzeba je co jakiś czas aktualizować. Zanim skonfigurujesz nowy router, wejdź na stronę internetową producenta i sprawdź, czy udostępnił on do pobrania nową wersję oprogramowania, a potem rób to w miarę systematycznie. Aby nie przegapić najnowszej wersji, zarejestruj swój router u producenta i zapisz się na aktualizacje.

A gdy już zabezpieczysz swój router, nie zapomnij też o zabezpieczeniu komputera. Stosuj te same „najlepsze praktyki", których przestrzegasz dla każdego komputera podłączonego do Internetu. Przykładowo: stosuj zabezpieczania typu antywirus, anti-spyware czy zapora (firewall) – i pilnuj, by zawsze były one zaktualizowane.

Chroń swoją sieć w trakcie korzystania ze zdalnego dostępu

Obecnie aplikacje umożliwiają ci dostęp do twojej sieci domowej z urządzeń mobilnych. Zanim zaczniesz z tego korzystać, upewnij się, że chronią cię jakieś funkcje zabezpieczające.

Stosuj mocne hasło w każdej aplikacji, która ma dostęp do twojej sieci. Wyloguj się z aplikacji, gdy jej nie używasz. W ten sposób znacznie zmniejszasz prawdopodobieństwo, że ktoś inny uzyska dostęp do aplikacji, jeżeli zgubisz telefon albo ktoś ci go ukradnie.

Zabezpiecz telefon lub urządzenie mobilne hasłem. Nawet jeśli twoja aplikacja ma mocne hasło, najlepiej będzie, gdy zabezpieczysz hasłem także swoje urządzenie.