Wskazówki i porady

Wyrób w sobie dobre nawyki bezpiecznego użytkowania internetu korzystając z poniższych wskazówek i porad. Niniejsza sekcja została opracowana we współpracy z Get Safe Online (UK) oraz Departamentem Bezpieczeństwa Krajowego (US)

- Chroń swój komputer osobisty (PC) i urządzenia przenośne
- Chroń swoje dane osobowe i tożsamość
- Chroń informacje handlowe poza miejscem pracy
- Zachowaj ostrożność łącząc się z internetem
- Rozsądnie korzystaj z internetu

Chroń swój komputer osobisty (PC) i urządzenia przenośne

PC

- Korzystaj z zapory sieciowej (firewalla): zapory sieciowe chronią Twoją sieć przed niektórymi wirusami i hakerami
- Zainstaluj oprogramowanie antywirusowe: oprogramowanie antywirusowe zapobiega rozprzestrzenianiu się wirusów w komputerze
- Zdobądź najnowsze aktualizacje systemu bezpieczeństwa: utrzymuj swoje aplikacje i system operacyjny w dobrym stanie i dbaj o ich aktualność
- Zwalczaj programy szpiegujące: unikaj podejrzanych e-maili i załączników, aby nieznajomi nie mogli uzyskać dostępu do Twojego komputera
- Regularnie twórz kopie zapasowe: chroń swoje dane przed utratą

Laptopy

- Wyłączaj połączenia bezprzewodowe, jeżeli nie są używane lub potrzebne
- Regularnie podłączaj swojego laptopa do zaufanej sieci w celu zaktualizowania mechanizmów bezpieczeństwa.
- Twórz kopie zapasowe informacji przechowywanych na laptopie
- Nie pozostawiaj swojego laptopa bez opieki

Napędy USB

- Korzystaj z pamięci USB z opcją szyfrowania
- Przestaw pamięć USB na tryb „tylko do odczytu” korzystając z przełącznika, aby uniknąć jej zainfekowania wirusem: niektóre pamięci USB są wyposażone w przełącznik umożliwiający przestawienie pamięci na tryb „tylko do odczytu”, co uniemożliwia komputerowi pełniącemu rolę hosta nadpisanie lub zmodyfikowanie danych umieszczonych na dysku

- Skanuj pamięć USB po skopiowaniu plików z nieznanego lub niezatwierdzonego urządzenia, aby uniknąć zainfekowania wirusem
- Przed połączeniem swojej pamięci USB do komputera należącego do innej osoby usuń wszystkie pliki, które nie są wymagane do przeprowadzenia danej operacji
- Twórz kopie zapasowe informacji na swoim dysku USB, aby móc je odzyskać w przypadku ich utraty
- Dołączaj pamięci USB do łańcuchów na klucze/smyczy, aby uniknąć ich zgubienia: niewielki rozmiar pamięci USB sprawia, że urządzenia tego rodzaju łatwiej jest zgubić lub ukraść Ponadto ich duża pojemność powoduje, że większa ilość danych może stać się przedmiotem nieuprawnionego dostępu. Pamięci USB z reguły umieszcza się w workach, plecakach, torbach na laptopy, kieszeniach marynarek i spodni lub też pozostawia się je na stanowiskach pracy. Ostatnio zaobserwować można wzrost liczby przypadków utraty, zgubienia, pożyczania bez pozwolenia lub kradzieży pamięci USB

Telefony komórkowe i komputery podręczne

Komputery podręczne, takie jak Windows Mobile, Palm, iPhone, Android i Blackberry, mogą zostać podłączone do internetu i być wykorzystywane do przechowywania ogromnej ilości informacji. Przy korzystaniu z takich urządzeń należy zachować szczególną ostrożność właśnie z uwagi na ich przenośność

- Wyłączaj połączenia bezprzewodowe (tj. Bluetooth i WLAN), jeżeli z nich nie korzystasz. Technologia Bluetooth pozwala urządzeniom elektronicznym na komunikowanie się między sobą przy pomocy łącza radiowego o krótkim zasięgu
- Nie zostawiaj swojego telefonu komórkowego i komputera podręcznego bez opieki. Może to doprowadzić do utraty danych
- Korzystaj z funkcji zabezpieczenia hasłem, aby udaremnić próby zdalnego włamania się do Twojego smartfona

Chroń swoje dane osobowe i tożsamość

- **Stosuj silne hasła:** Twoje hasło w internecie pełni tę samą rolę co zamek i klucz do Twojego domu. Hasła stanowią istotne narzędzie obrony przed atakami w sieci, dlatego wypracowanie dobrych praktyk związanych ze stosowaniem haseł pozwala lepiej chronić dane szczególnie chronione i tożsamość użytkownika. Znajomość hasła do Twojego komputera pozwala uzyskać dostęp do wszystkich przechowywanych w nim informacji – zarówno zawodowych, jak i osobistych – a także do kont internetowych. Korzystaj z silnego hasła, aby zapewnić ochronę swoich danych: stosuj złożony zestaw znaków; łącz litery (wielkie i małe), cyfry i symbole. Im większa różnorodność znaków, z których składa się hasła, tym trudniej będzie je odgadnąć. Nie wykorzystuj informacji osobistych – imienia, imienia dziecka, daty urodzin itp. – które osoba postronna może znać lub które może łatwo

uzyskać; staraj się unikać pospolitych słów: niektórzy hakerzy stosują programy pozwalające im wypróbować wszystkie słowa występujące w słowniku

- **Regularnie zmieniaj swoje hasło**: Jeżeli podejrzewasz, że ktoś włamał się do Twojego systemu, natychmiast zmień wszystkie hasła
- **Nie ujawniaj swojego hasła**: Twoje hasło jest unikalne i nie należy go nikomu ujawniać. O ile to możliwe, staraj się zapamiętywać wszystkie swoje hasła. Opracuj strategię zapamiętywania haseł. Jeżeli zapisujesz stosowane przez siebie hasła, przechowuj je w bezpiecznym miejscu. Nie zostawiaj listy haseł w miejscu, w którym nie pozostawiłbyś chronionych przez nie informacji
- **Inne konto, inne hasło:** stosuj różne hasła dla każdego konta internetowego, z którego korzystasz (lub przynajmniej kilka różnych haseł). Jeżeli stosujesz te same hasła w odniesieniu do szeregu kont, haker, który uzyska dostęp do jednego konta, będzie mógł uzyskać dostęp do wszystkich Twoich kont
- **Zabezpieczaj swoje konta:** wielu dostawców kont oferuje możliwość skorzystania z dodatkowych narzędzi uwierzytelniania, uruchamianych przed uzyskaniem dostępu do danej strony
- **Kontroluj swoją obecność w internecie:** w miarę możliwości dostosuj ustawienia prywatności i bezpieczeństwa na stronach internetowych do odpowiadającego Ci poziomu udostępniania informacji. Zaleca się ograniczenie liczby osób, z którymi wymienia się informacjami
- **Zachowaj ostrożność korzystając z portali społecznościowych:** miej świadomość, że korzystanie z portali społecznościowych wiąże się z wieloma zagrożeniami: nękanie online, ujawnianie informacji prywatnych, molestowanie za pośrednictwem Internetu (cyber-stalking), dostęp do treści niedostosowanych do wieku odbiorcy oraz, w najbardziej ekstremalnych przypadkach, uwodzenie dzieci przez Internet i wykorzystywanie dzieci

Chroń informacje handlowe poza miejscem pracy

- **Zapewnij bezpieczeństwo przechowywanych przez siebie danych szczególnie chronionych**: przebywając poza miejscem pracy upewnij się, że dane szczególnie chronione i wyposażenie znajdujące się w Twoim posiadaniu jest odpowiednio zabezpieczone, aby zapobiec jego kradzieży lub utracie. Zachowaj ostrożność przetwarzając informacje, w szczególności jeśli znajdujesz się w miejscu publicznym
- **Zachowaj poufność informacji handlowych**: miej świadomość, że osoba postronna może podsłuchać prowadzoną przez Ciebie rozmowę. Nie udostępniaj poufnych danych handlowych Twojego przedsiębiorstwa przypadkowym osobom
- **Uważaj na zjawisko „shoulder surfingu" (zaglądanie przez ramię przy korzystaniu z komputera)**: podróżując lub pracując zdalnie zabezpiecz się przed shoulder surfingiem
- **Rozsądnie korzystaj z konta poczty e-mail**: wykorzystywanie przeglądarki internetowej do przeglądania poczty wymaga zachowania takiej samej ostrożności, jak korzystanie ze służbowej poczty elektronicznej i wiąże się z kilkoma dodatkowymi zagrożeniami

Zachowaj ostrożność łącząc się z internetem

- **Wyłączaj połączenia bezprzewodowe, jeżeli nie są używane lub potrzebne**
- **Zwiększ swoją wiedzę na temat hotspotów (WLAN):** korzystając z hotspotów (WLAN), ograniczaj rodzaj wykonywanych czynności i zmieniaj ustawienia bezpieczeństwa na swoim urządzeniu przenośnym, aby ograniczyć liczbę osób mogących uzyskać dostęp do twojego komputera
- **Chroń swoje pieniądze**: korzystając z usług bankowych lub robiąc zakupy online upewnij się, że strony, z których korzystasz, są odpowiednio zabezpieczone. Zwracaj uwagę na adresy internetowe rozpoczynające się od https:// lub „shttp://" – oznacza to, że strona korzysta z dodatkowych narzędzi ułatwiających zabezpieczenie przekazywanych informacji. Format http:// nie jest bezpieczny
- **Blokuj niechcianą pocztę:** spam stanowi zagrożenie dla bezpieczeństwa. Nie otwieraj e-maili i załączników pochodzących od nieznanych nadawców
- **W razie wątpliwości usuwaj:** jeżeli linki w e-mailach, tweetach, postach i reklamach internetowych wydają ci się podejrzane, najlepiej jest je usunąć lub oznakować jako spam, nawet w przypadku, gdy znasz ich źródło
- **W stosownych przypadkach przesyłaj e-maile dalej.** Przed przekazaniem e-maila rozważ możliwość wyczyszczenia historii wiadomości
- **Zachowaj ostrożność korzystając z internetu**
- **Nie pobieraj dokumentów i materiałów z niesprawdzonych źródeł**
- **Zachowaj ostrożność korzystając z publicznych komputerów**: podłączaj się do publicznego komputera tylko jeśli dysponujesz szyfrowanym połączeniem (o istnieniu takiego połączenia świadczy ikona kłódki w prawym dolnym rogu okna przeglądarki oraz fraza „https://" na początku adresu strony internetowej)
- **Korzystaj z usług poczty e-mail dostarczanych przez dobrze znane i cieszące się zaufaniem firmy**

Rozsądnie korzystaj z internetu

- **Bądź na bieżąco:** szukaj informacji o nowych sposobach zapewnienia bezpieczeństwa w internecie: przeglądaj zaufane strony internetowe w celu zapoznania się z najnowszymi informacjami, dziel się swoją wiedzą z rodziną, przyjaciółmi i kolegami i zachęcaj ich do rozsądnego korzystania z internetu. Zwiększ bezpieczeństwo swojej przeglądarki internetowej
- **Pomyśl zanim coś zrobisz:** uważaj na komunikaty, które próbują nakłonić cię do natychmiastowego działania, oferują Ci coś, co wydaje się zbyt dobre, by mogło być prawdziwe, lub proszą Cię o podanie Twoich danych osobowych
- **Twórz kopie bezpieczeństwa:** chroń swoją pracę, muzykę, zdjęcia i inne informacje cyfrowe tworząc ich elektroniczne kopie i przechowując je w bezpiecznym miejscu