

Jedno hasło, jedno konto – to jedna z zasad, o której warto pamiętać korzystając z sieci. Stosujecie? Jest jeszcze czas, by to naprawić.

Wszyscy znamy się na Internecie, bo przecież wszyscy z niego korzystamy. Naprawdę? A kiedy ostatnio skanowaliście pendrive'a przed otwarciem plików? Wyłączacie transmisję Wi-Fi i Bluetooth, kiedy z nich nie korzystacie? No właśnie, dlatego przypominamy dobre praktyki korzystania z Internetu. Przeczytajcie i... stosujcie.

Pamiętaj, żeby nie zapomnieć

- Informacja – to jej najczęściej szukamy w Internecie, ale i to ją powinniśmy szczególnie chronić korzystając z sieci. Pamiętajmy, aby zabezpieczać dostęp do naszych danych – mówi Sebastian Kondraszuk z CERT Polska w NASK – Jak to zrobić? Po pierwsze – mocne hasło, po drugie – dwuskładnikowe uwierzytelnienie – dodaje ekspert.

Większość z nas logując się do konta e-mail, portali społecznościowych, czy nawet bankowości elektronicznej wpisuje jedynie nazwę użytkownika i hasło. Mało.

Rozbuduj ten proces - aktywuj weryfikację tożsamości opartą o dodatkowy składnik, np. kod SMS, token czy klucz sprzętowy.

Klucz do sukcesu? Dobre hasło. Jak je stworzyć? To przynajmniej 12 znaków. Nie wybieraj prostych kombinacji, takich jak imię i rok urodzenia. Jeśli chcesz je zapamiętać, tworząc hasło skup się na pozytywnych zdaniach lub zwrotach, o których lubisz myśleć. W takim przypadku jest szansa, że szybko go nie zapomnisz. Nie idź na skróty. Im dłuższe hasło, tym trudniej będzie je odgadnąć, czy złamać.

WAŻNE! Zadbaj o silne hasło do najistotniejszych serwisów (bankowość, poczta elektroniczna, portale społecznościowe).

Utrudniaj życie przestępcom. Dla każdego konta wymyśl (i zapamiętaj) oddzielne hasło. Absolutne minimum to rozdzielenie kont służbowych i prywatnych.

Jeśli masz problemy z pamięcią (kto nie ma?), korzystaj z menadżera haseł. To aplikacja, którą stworzono, by ułatwić nam życie. Dzięki niej bezpiecznie przechowasz swoje dane dostępowe. Nie zapisuj haseł na kartce, a jeśli już to zrobisz, nie naklejaj jej na komputerze. Opcja minimum – umieść kartkę w bezpiecznym miejscu, z dala od komputera. Nie zapomnij, gdzie ją schowałeś ;-)

Skanuj i chroń

- Kolejna dobra rada: dbajmy o aktualizacje i bezpieczeństwo urządzeń, z których korzystamy. I nie chodzi jedynie o komputer, przecież najczęściej korzystamy z telefonów. Regularne aktualizacje systemu operacyjnego, programu antywirusowego, czy przeglądarki internetowej pomogą ustrzec nas przed znanymi już błędami, które mogłyby zostać wykorzystane przez atakującego – mówi Sebastian Kondraszuk, ekspert zespołu CERT Polska.

Jak to zrobić? Włącz automatyczne aktualizacje. Wiele aplikacji daje taką możliwość. Skorzystaj z tego rozwiązania wszędzie tam, gdzie się da.

Podbijasz Internet? Rób to z głową

Kategoria: Styl życia

Opublikowano: wtorek, 26, marzec 2019 15:01

Artur Duda

Odsłony: 1274

Chroń WSZYSTKIE urządzenia podłączane do sieci. Uwaga, to nie tylko komputery. To także smartfony, czy tablety. One także potrzebują ochrony przed wirusami i złośliwym oprogramowaniem.

I jeszcze jedno: nie podłączaj do swoich sprzętów nośników (pendrive'y, dyski zewnętrzne), których nie znasz lub nie wiesz skąd je masz. Mogą być niebezpieczne (zainfekowane przez szkodliwe oprogramowanie). Zanim otworzysz ich zawartość, skorzystaj ze skanera antywirusowego.

Nie daj się złapać

Korzystaj z Internetu. Rozważnie. Otwarta, publiczna sieć Wi-Fi kusi, ale to żadna oszczędność. Ogranicz aktywność w takich sieciach. Jeśli chcesz – poza domem – korzystać z najważniejszych dla siebie serwisów (poczta e-mail, bankowość internetowa, portale społecznościowe), używaj własnego modemu LTE lub połączenia VPN. Będzie dużo bezpieczniej.

WAŻNE! Wyłączaj transmisje Wi-Fi i Bluetooth, kiedy z nich nie korzystasz.

A jeżeli widzisz w sieci, coś co Cię niepokoi - nie wahaj się. Reaguj, zgłaszaj! Gdzie?

- Incydenty naruszające bezpieczeństwo w sieci: <https://incydent.cert.pl>
- Nielegalne treści w Internecie: <https://dyzurnet.pl>

Pozostajemy w kontakcie!

Źródło: www.gov.pl/web/cyfryzacja