Czy dbasz o swoje bezpieczeństwo w sieci? Sprawdź się.

ZACZNIJ TUTAJ

Czy do każdego serwisu, z którego korzystasz, masz inne hasło (poczta e-mail, bankowość etc.)?

Czy znasz konsekwencje korzystania z funkcji "Zapamiętaj hasło"?

Czy wiesz, że hasła należy regularnie zmieniać?

Czy pamiętasz o tym, że hasła powinny być trudno dostępne dla innych osób?

Czy przy instalowaniu aplikacji zwracasz uwagę na to, do jakich treści na urządzaniu ma ona dostęp?

Czy sprawdzasz opcje prywatności (np. widoczność swoich postów) na portalach społecznościowych?

Czy zwracasz uwagę na to, kto do Ciebie pisze i jakie treści wysyła?

Dostajesz od znajomego nietypową wiadomość, że ktoś zamieścił prześmiewcze informacje na Twój temat, a do wiadomości dołączony jest link. Czy weryfikujesz u źródła tę podejrzaną treść i czy dajesz znać, że konto tej osoby może być zhakowane lub zawirusowane?

Czy podczas logowania do bankowości internetowej lub wypełniania formularza z danymi sprawdzasz, czy strona ma certyfikat bezpieczeństwa?

Czy PIN do Twojego telefonu jest bardziej skomplikowany od 1111 lub 1234?

Czy używasz oprogramowania antywirusowego?

A TERAZ...

Czy na wszystkie pytania udało Ci się odpowiedzieć TAK? Gratulacje! Pamiętaj jednak, że nie wystarczy tylko wiedzieć, trzeba wcielać wiedzę w życie. A ciągłe aktualizowanie wiedzy i uważność w sieci to konieczność! Jeśli chociaż jedno pytanie zostało przez Ciebie zakreślone jako NIE, to koniecznie zadbaj o siebie i swoich bliskich. Przeczytaj też krótki poradnik z serią przydatnych wskazówek.

Podpowiadamy, na co zwrócić uwagę.

WARTO O TYM WIEDZIEĆ

HASŁA/PINY - kto nigdy nie wprowadził do hasła daty swoich urodzin, niech pierwszy rzuci telefonem! To bardzo częsty błąd! Podobnie z hasłami 1111, 1234, imionami dzieci czy zwierzaka. Nie zawsze warto korzystać z wielostopniowej weryfikacji, ale z pewnością warto regularnie zmieniać swoje hasła do telefonu, tabletu, komputera, skrzynki e-mail czy bankowości. Jeśli brakuje Ci pomysłów na hasła, skorzystaj z generatora. A jeśli boisz się, że nie zapamiętasz wszystkich haseł, przeczytaj o "bezpiecznych zdaniach" – to proste narzędzie oparte na mnemotechnikach, które znacząco wpłynie na Twoje bezpieczeństwo w sieci.

WIELOSTOPNIOWA WERYFIKACJA – to sposób zabezpieczenia sprzętu elektronicznego lub narzędzi (np. skrzynki e-mail), który choć nieco wydłuża dostanie się do jego zawartości, pomaga w zabezpieczeniu naszych danych i plików. Wielostopniowa weryfikacja wymusza na nas nie jedno, a kilka działań, które otwierają nam dostęp do urządzenia lub narzędzia – musimy zatem wpisać hasło i narysować szlaczek lub odpowiedzieć na pytanie. Gdzie warto stosować WW? W smartphonach (co ważne! Jeśli zajdzie potrzeba zadzwonienia na telefon alarmowy, dwustopniowa weryfikacja nie będzie potrzebna), w komputerach – zwłaszcza tych, na których trzymamy dokumenty, zdjęcia, pliki.

AKTUALIZACJE – tak, zawsze pojawiają się w złym momencie, kiedy właśnie mieliśmy zrobić coś turboważnego. Dlatego często kusi nas opcja “przypomnij mi jutro...” Ale jutro zwykle też są ważniejsze sprawy niż zaktualizowanie oprogramowania – musisz jednak pamiętać, że brak aktualizacji oprogramowania to otwarta furtka do Twojego urządzenia.

BACKUPY – podobno ludzie dzielą się na tych, którzy już je robią lub dopiero będą. O czym mowa? O kopiach bezpieczeństwa. Warto robić takie kopie nie tylko ze strachu przed cyberatakiem, ale także z uwagi na to, że urządzania, na których przechowujemy dane, nie są wieczne. Czasem może nas pokonać deszcz, który zmoczy naszego laptopa czy zbyt mocne szarpnięcie auta, na podłodze którego trzymamy torbę z tabletem. Jeśli chcemy chronić nasze dane, warto regularnie robić kopie bezpieczeństwa.

Sprawdź, czy Twoje hasło jest bezpieczne*:

https://howsecureismypassword.net/

* To narzędzie pozwoli Ci sprawdzić, ile czasu zajmie komputerowi włamanie się na Twoje konto.

Uwaga! Nie podawaj nigdy swojego prawdziwego hasła, a jedynie podobne, oparte o tę samą zasadę. np. jeśli Twoje prawdziwe hasło to Papierek67!, to na powyższej stronie wpisz Zeszycik?12.

Wynik wskazuje 7 miesięcy? 41 lat? 1200 lat? To nie jest dużo! Czemu? Pamiętaj, że to nie człowiek włamuje się na konto, lecz komputer, a moce obliczeniowe współczesnych komputerów są coraz większe!

Być może ciekawi Was fakt, że nie napisaliśmy nic na temat płacenia kartą w internecie. Dlatego chcielibyśmy Wam przypomnieć, że karty płatnicze posiadają mechanizm chargeback. Umożliwia on reklamowanie wszystkich płatności, które zostały wykonane bez naszej autoryzacji. Taką transakcję można cofnąć, a mamy na to zwykle około 90 dni.