

# Jak zabezpieczać dane (prywatne, firmowe) w internecie?

Objętość danych przechowywanych oraz przetwarzanych współcześnie w internecie jest praktycznie niemożliwa do określenia (a także do wyobrażenia). Według szacunków tygodnika Newsweek (dane z marca 2018 roku), każdy użytkownik sieci tworzy około 12 gigabajtów danych... dziennie! Spora część z nich to tzw. dane poufne, czyli np. adresy, hasła do kont bankowych i portali internetowych, dane osobiste, dane dotyczące stanu zdrowia itp. Korzystanie z dobrodziejstw i potencjału [internetu](#) narzuca w sposób oczywisty konieczność – szczególnie dla firm oraz instytucji dysponujących bardzo dużymi ilościami poufnych danych swoich klientów - troski o ochronę owych informacji. Jak zatem to robić?

## Ochrona podstawowa

Bez względu na to w jakim celu i przy użyciu jakiego rodzaju sprzętu korzysta się z sieci, ważne jest, aby pamiętać o pewnych uniwersalnych zasadach znacząco poprawiających stopień bezpieczeństwa zamieszczanych na stronach internetowych informacji.

**Zasada pierwsza** to dobre hasło, składające się z min. 8 znaków (choć dobrze, gdyby liczyło nawet kilkanaście), w tym dużych i wielkich liter oraz cyfr. Warto przy tym pamiętać, aby hasło nie kojarzyło się zbyt blisko z osobą użytkownika, będąc np. jego datą urodzin, imieniem dziecka, czy też nawiązywało do jego hobby. Jednak czasami samo hasło może okazać się zbyt słabe; dobrze więc skorzystać z tzw. uwierzytelniania dwuskładnikowego, kiedy to po wpisaniu hasła za konkretnej stronie www, otrzymamy mailem lub sms – dodatkowy kod, którego wpisanie umożliwi wejście na tę stronę.

**Zasada druga** nakazuje częste i regularne skanowanie komputera w celu wykrycia i usunięcia potencjalnie niebezpiecznych plików (robaki, malware, spyware, rootkit, adware, wabbit, keylogger), które mogą spowodować utratę poufnych danych a nawet ułatwić atak hakerski.

**Zasada trzecia** doradza zapewnienie sobie skutecznej zapory sieciowej (firewall), czyli oprogramowania blokującego niepowołany dostęp do komputera który ma chronić. Jej głównym zadaniem jest obrona sprzętu oraz sieci LAN przed niechcianą ingerencją z zewnątrz (czyli sieci publicznych). Sprawny firewall jest w stanie zabezpieczyć sprzęt przed próbami przechwycenia poufnych informacji przez niepowołane podmioty.

**Zasada czwarta** doradza archiwizację danych, najlepiej na dyskach zewnętrznych. Takie działanie ma niepodważalną zaletę: jeżeli twardy dysk ulega zniszczeniu lub uszkodzeniu, zostaje skradziony, cze też [komputer](#) pada ofiarą cyberataku skutkującego utratą zapisanych na nim danych, owe dane nie przepadają bezpowrotnie, ponieważ istnieją zapisane na innym nośniku. W przypadku szczególnie istotnych informacji, dobrze jest zapisać je na co najmniej dwóch dyskach zewnętrznych.

**Zasada piąta:** szyfrowanie. Współczesne programy szyfrujące są na tyle skuteczne, że w znaczącym stopniu utrudniają potencjalne ataki hakerskie, umożliwiając dostęp i korzystanie z konkretnych plików tylko i wyłącznie ich właścicielom.

za: infor.pl