**Cyberochrona w czasach home office**

Wielu z nas, w ciągu ostatnich dwóch lat zmieniło tryb swojej pracy ze stacjonarnej na hybrydową lub całkowicie zdalną – „pracuję na home office”, zapewne jest to już znane nam zdanie.

Niestety, pracując w zaciszu swojego domu, często ignorujemy bardzo ważny aspekt pracy przy komputerze – cyberbezpieczeństwo. Jak więc zadbać o siebie i swoje urządzenia, kiedy nie mamy obok siebie ogromnego działu IT?

**Podstawowe zasady bezpieczeństwa**

Najprostszy sposób na ochronę? Zasada ograniczonego zaufania.

Nigdy nie wiemy kto (lub co!) znajduje się po drugiej stronie monitora, dlatego nie podajemy nikomu swoich danych poufnych, ani haseł do kont. Hasła to bardzo ciekawy temat, zapewne duża ilość z nas używa tego samego hasła do wielu kont, bo „nie zapamiętam więcej”. To oczywiście karygodny błąd! Posiadanie tego samego hasła do wszystkich usług w sieci sprawia, że stajemy się łatwym celem dla hakerów internetowych. Warto korzystać z menadżera haseł, jeśli nie mamy wystarczająco miejsca w głowie na kolejne skomplikowane wyrazy.

**Phishing**

Phishing to metoda cyberataku, która polega na przesyłaniu fałszywych e-maili od legalnych organizacji (np. bank, urząd, firma kurierska) lub przekierowywaniu na fałszywe strony WWW. Hakerzy grzecznie proszą o potwierdzenie czegoś, czasem sugerują jakiś problem, np. niedopłatę do paczki – po kliknięciu w link zostajemy przekierowani na fałszywą witrynę i nakłonieni do podania swoich danych prywatnych, najczęściej również numeru konta.

Dla nas to tylko jedno niewinne kliknięcie, a dane, które przesyłamy wtedy do hakerów, pozwalają im np. na wyczyszczenie naszego konta bankowego.

Nie reagujemy na podejrzane linki na Facebooku, a do niechcianych e-maili podchodzimy z dozą ostrożności. Sprawdzamy adresy URL stron – w przypadku oszustw, adresy wyglądają poprawnie, ale mogą mieć literówki czy inne domeny (rząd.com zamiast rząd.gov).

**VPN, czyli bezszelestne surfowanie**

Warto zainwestować w oprogramowanie VPN, które pozwala na zachowanie prywatności w sieci – to w swojej ofercie ma np. [G DATA](https://gdata.pl/vpn). Korzystanie z *Virtual Private Network* uniemożliwia śledzenie naszych działań, bo są one... wymazane. To bardzo fajna sprawa, gdy korzystamy z publicznego Wi-Fi, np. w hotelu czy w transporcie publicznym. W codziennym surfowaniu po Internecie to oprogramowanie również jest bardzo przydatne! A przy okazji umożliwia nam połączenie się z serwerem wybranego kraju – jeżeli chciałeś obejrzeć na Netflixie serial, który jest niedostępny w naszym kraju, to z oprogramowaniem VPN możesz to zrobić i spokojnie przysiąść przy swojej ulubionej produkcji!

**Korzyści płynące z VPN**

Szyfrowanie przesyłanych danych, czyli zabezpieczanie niechronionych połączeń, zarówno w domu, jak i korzystając z publicznych sieci WLAN, rygorystyczna polityka "No Logging" w usłudze G DATA VPN. Do tego nieograniczony dostęp do treści - omijanie ograniczeń związanych z dostępem do mediów i witryn internetowych obowiązujących w danym kraju.

Anonimowa aktywność w sieci jest możliwa dzięki prawie 2 000 serwerów VPN w ponad 75 lokalizacjach na całym świecie!