10 zasad cyberbezpieczeństwa

Zdalny dostęp do własnych pieniędzy przez komputer lub telefon to z jednej strony wygoda, a z drugiej ryzyko, że padniemy ofiarą cyberprzestępców. W raporcie **Polska i Europa. Wyzwania i ograniczenia,** eksperci Związku Banków Polskich zauważają: *Codziennie, na całym świecie atakowanych jest 0,5 mln stron internetowych, a 76 procent stron internetowych ma słabe punkty, przez które można było je zaatakować.*

Czego nie robimy w sieci, a powinniśmy?

Niestety, jak wynika z analiz Komisji Europejskiej – jesteśmy najmniej ostrożnym narodem w UE, jeśli chodzi o zachowania w Internecie. Aż 57 proc. z nas nie instaluje oprogramowania antywirusowego, 72 proc. odwiedza strony internetowe mimo braku przekonania o ich bezpieczeństwie, 83 proc. Polaków używa tego samego hasła do różnych kont, 86 proc. nie zmienia regularnie haseł do posiadanych kont i 92 proc. nie zmienia ustawień dotyczących bezpieczeństwa w przeglądarkach internetowych.

Jeżeli więc chcemy być bezpieczni w sieci, to powinniśmy robić to, czego większość Polaków nie robi.

10 zasad cyberbezpieczeństwa

1. Instalujmy na swoim komputerze dobry program antywirusowy i regularnie go aktualizujmy.
2. Stosujmy się do ustalonych przez bank zasad bezpieczeństwa zamieszczonych na stronie. Jeśli coś odbiega od normy, to przerwijmy transakcję i skontaktujmy się z bankiem. Kupujmy tylko w takich sklepach internetowych, gdzie jest szyfrowane połączenie – widzimy kłódkę i odpowiedni certyfikat, najlepiej znanych nam już wcześniej.
3. Dokonujmy płatności tylko z własnego komputera lub telefonu. Nie korzystajmy z publicznej sieci np. na lotnisku, w kawiarence internetowej. Nie wchodźmy na stronę banku z linku w wyszukiwarce, lecz wpisujmy adres ręcznie. Tak samo postępujmy z numerem konta odbiorcy naszego przelewu.
4. Jeśli „bank" pyta Cię o hasła, czy też inne poufne dane, np. kod PIN do karty płatniczej, nie odpowiadaj! Na pewno nie jest to bank!
5. Nie oszczędzajmy, instalując na komputerze nielegalne oprogramowanie. Może ono zawierać przygotowane przez hakerów wirusy, które pomogą im w opanowaniu naszego komputera, wyłudzeniu danych, i w końcu pozwolą na okradzenie nas.
6. Nie otwierajmy wiadomości i dołączonych do nich załączników z nieznanych źródeł. W załącznikach może być ukryte złośliwe oprogramowanie.
7. Nie wchodźmy na podejrzane strony, np. strony z treścią pornograficzną. To także źródło wirusów.
8. Skanujmy od czasu do czasu nasz komputer, szczególnie przed zalogowaniem się na stronę banku.
9. Regularnie aktualizujmy oprogramowanie na komputerze, szczególnie oprogramowanie przeglądarek internetowych. Hakerzy szukają luk, a producenci cały czas „uszczelniają" wykryte luki w oprogramowaniu. Dzięki aktualizacjom mamy zawsze na komputerze najbardziej odporne na ataki hakerskie oprogramowanie.
10. Zmieniajmy regularnie hasła do swojego komputera, hasła dostępu do konta internetowego. Powinny to być hasła trudne i różne do każdej usługi internetowej.