

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. Instalujemy na swoim komputerze dobry program antywirusowy i regularnie go aktualizujemy.
2. Stosujemy się do ustalonych przez bank zasad bezpieczeństwa zamieszczonych na stronie. Jeśli coś odbiega od normy, to przerwijmy transakcję i skontaktujmy się z bankiem. Kupujemy tylko w takich sklepach internetowych, gdzie jest szyfrowane połączenie – widzimy kłódkę i odpowiedni certyfikat, najlepiej znanych nam już wcześniej.
3. Dokonujemy płatności tylko z własnego komputera lub telefonu. Nie korzystamy z publicznej sieci np. na lotnisku, w kawiarence internetowej. Nie wchodzimy na stronę banku z linku w wyszukiwarce, lecz wpisujemy adres ręcznie. Tak samo postępujemy 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 nieznanymi źródłami. W załącznikach może być ukryte złośliwe oprogramowanie.
7. Nie wchodzimy na podejrzane strony, np. strony z treścią pornograficzną. To także źródło wirusów.
8. Skanujemy od czasu do czasu nasz komputer, szczególnie przed zalogowaniem się na stronę banku.

9. Regularnie aktualizujemy 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. Zmieniamy regularnie hasła do swojego komputera, hasła dostępu do konta internetowego. Powinny to być hasła trudne i różne do każdej usługi internetowej.



Program sektorowy „Bankowcy dla Edukacji” to jeden z największych programów edukacji finansowej w Europie. Jest on realizowany od 2016 r. z inicjatywy Związku Banków Polskich przez Warszawski Instytut Bankowości. Jego celem jest edukowanie uczniów, studentów i seniorów w zakresie podstaw praktycznej wiedzy dotyczącej ekonomii, finansów, bankowości, przedsiębiorczości, cyberbezpieczeństwa i obrotu bezgotówkowego.

Dowiedz się więcej na www.bde.wib.org.pl