Nie daj się okraść – reaguj na włam

Kategoria: Styl życia
Opublikowano: środa, 03, kwiecień 2019 15:22
Artur Duda
Odsłony: 1443

Na swoim koncie masz transakcję, której na pewno nie dokonywałeś? A może znajomi nie są zachwyceni, bo wysyłasz sporo spamu? Hasło logowania nie działa, mimo że na 100% jest poprawne? Możesz być ofiarą hakera. Spokojnie, to nie koniec świata!

Masz zainstalowany program antywirusowy, nie wchodzisz na żadne „dziwne" strony, bardzo dbasz o swój komputer i jego zawartość? Doskonale. Mimo to możesz stać się ofiarą hakera. To trochę jak z jazdą samochodem – świetnie i ostrożnie prowadzisz, a mimo to ktoś może wjechać Ci w zderzak.

To dziwne…
Jak rozpoznać, że zawartość Twojego komputera nie należy tylko do Ciebie? Oto kilka wskazówek:

- Twój antywirus zgłasza alert infekcji.
  UWAGA! Upewnij się, że powiadomienie na pewno wysyła program antywirusowy. Zdarza się, że alert pochodzi z przeglądarki internetowej. To może być podstęp! Jeśli nie jesteś pewny skąd pochodzi powiadomienie, sprawdź to w swoim programie antywirusowym.
- Przeglądarka internetowa samoczynnie – bez Twojej woli – otwiera strony.
- Co chwilę wyskakują Ci dziwne okna aplikacji, a programy na Twoim sprzęcie często się zawieszają.
- Otrzymałeś informację o tym, że Twoje dane na komputerze zostały zaszyfrowane. Aby odzyskać do nich dostęp, powinieneś zapłacić wskazaną kwotę.
- Masz 100% pewności, że wpisujesz dobre hasło do systemu lub kont bankowych, a mimo to nie działa.
- Z Twojej karty kredytowej lub konta bankowego dokonano transakcji, o której nie masz zielonego pojęcia.
- Znajomi dają Ci znać, że ich spamujesz, a Ty nic o tym nie wiesz/ nie robisz tego.

Jeśli spotkała Cię któraś z tych sytuacji, możesz mieć problem. Spokojnie, pomożemy go rozwiązać.

Tempo!
– Jeśli podejrzewamy, że ktoś uzyskał nieautoryzowany dostęp do naszego komputera, nie ma co czekać. Najważniejsza jest szybka reakcja. Jeśli wiele wskazuje na to, że jesteśmy ofiarą cyberprzestępstwa, trzeba o tym poinformować odpowiednie służby. W przypadku mniej poważnych ataków – możemy zadziałać sami lub skorzystać z serwisu komputerowego – mówi Przemysław Jaroszewski z CERT Polska w NASK. – *Zmieńmy hasła do najważniejszych serwisów (w tym do poczty!), – koniecznie z innego, niezainfekowanego komputera! Postępujmy zgodnie z instrukcjami programu antywirusowego lub poszukajmy porady eksperta (np. znajomego czy pracownika serwisu). Niestety, może się okazać, że bez instalacji systemu od nowa się nie obędzie* – dodaje ekspert CERT.

Co jeszcze możemy zrobić sami?

- W przypadku problemów z kontem bankowym lub kartą kredytową – skontaktuj się ze swoim bankiem lub firmą, która obsługuje Twoją kartę. Numer telefonu znajdziesz na np. tylnej części karty, na wyciągu bankowym lub na stronie internetowej banku.
- Jeśli o problemie poinformował Cię program antywirusowy, wykonaj kroki, które doradza. Większość antywirusów udostępnia link do strony, gdzie znajdziesz informacje na temat wykrytego zagrożenia.
- Rób kopie zapasowe – to kluczowy krok, który pomoże Ci przygotować się na wypadek

włamania. Dlaczego? Dość często okazuje się, że po infekcji trzeba usunąć wszystkie dane z komputera i od nowa zainstalować system operacyjny. Możesz wybrać rozwiązanie, które automatycznie tworzy takie kopie (codziennie lub nawet co godzinę). Nieważne, na co się zdecydujesz – kopie muszą być robione regularnie i poprawnie. Warto raz na jakiś czas sprawdzić, czy dane rzeczywiście da się z nich odzyskać.

– *Jeśli uważasz, że padłeś ofiarą cyberprzestępców, zgłoś to nie tylko na policję, ale także na* https://incydent.cert.pl – mówi Przemysław Jaroszewski z CERT Polska w NASK. – *Rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo w sieci to jedno z naszych głównych zadań. Aktywnie reagujemy też m.in. w przypadkach bezpośrednich zagrożeń dla użytkowników* – dodaje ekspert.

Tylko w 2018 r. operatorzy z zespołu CERT Polska przyjęli 19 439 zgłoszeń, które zostały dokładnie przeanalizowane i odpowiednio zaklasyfikowane. W sumie odnotowano 3 739 incydentów bezpieczeństwa, czyli średnio ponad 10 dziennie.

Jeżeli widzisz w sieci, coś co Cię niepokoi – nie wahaj się. Reaguj, zgłaszaj! Gdzie?

- Incydenty naruszające bezpieczeństwo w sieci: https://incydent.cert.pl
- Nielegalne treści w Internecie: https://dyzurnet.pl

Źródło: www.gov.pl/web/cyfryzacja