OUCH! Listopad 2023

Biuletyn Bezpieczeństwa Komputerowego

Zaatakowali mnie hakerzy, co teraz?

Czy jestem ofiarą hakera?

Internet może być przytłaczający, a nowe technologie nieustannie się zmieniają. Bez względu na to, jak bardzo starasz się być bezpieczny, prędzej czy później możesz zostać zaatakowany przez hakerów. Im szybciej wykryjesz, że stało się coś złego i im szybciej zareagujesz, to konsekwencje ataku mogą być mniejsze. Poniżej przedstawiamy kilka wskazówek, które świadczą o tym że mogłeś zostać zhakowany i co możesz z tym zrobić.

Oznaki, że jedno z twoich kont internetowych mogło zostać zaatakowane

- Rodzina lub przyjaciele zwracają ci uwagę, że otrzymują od ciebie nietypowe wiadomości bądź zaproszenia, choć masz pewność, że ich nie wysyłałeś.
- Hasło do konta nie działa, nawet jeśli wiesz, że jest prawidłowe.
- Otrzymujesz powiadomienia o zalogowaniu na konto, chociaż wiesz, że tego nie robiłeś.
- Otrzymujesz wiadomości e-mail potwierdzające zmiany na koncie, których nie wprowadziłeś.

Oznaki, że komputer lub urządzenie mobilne zostało zaatakowane

- Program antywirusowy wysyła powiadomienia o zainfekowaniu systemu. Upewnij się, że powiadomienia generowane są przez program antywirusowy i nie są to przypadkowe wyskakujące okienka ze strony internetowej, nakłaniające do podjęcia działań takich jak zainstalowanie dodatkowego oprogramowania. Nie masz pewności? Uruchom program antywirusowy i sprawdź, czy komputer na pewno jest zainfekowany.
- Podczas przeglądania stron internetowych często następuje przekierowanie na inne strony, których nie chciałeś odwiedzić lub pojawiają się nowe, niechciane strony internetowe.
- Otrzymujesz powiadomienie, że pliki przechowywane na komputerze zostały zaszyfrowane i musisz zapłacić okup aby odzyskać do nich dostęp.

Oznaki, że Twoja karta kredytowa lub finanse zostały zaatakowane

- Zauważasz podejrzane, nieautoryzowane transakcje na karcie kredytowej lub koncie bankowym.

Co teraz? - Jak odzyskać kontrolę

Jeśli podejrzewasz, że zostałeś zaatakowany, zachowaj spokój. Dasz sobie z tym radę, najważniejsze jest nie wpadać w panikę. Jeśli problem wystąpił w miejscu pracy bądź na urządzeniu służbowym, nie próbuj naprawiać problemu na własną rękę. Zgłoś problem swojemu przełożonemu. Jeśli jest to urządzenie lub konto prywatne, wypróbuj kilka kroków, które możesz podjąć:

- **Odzyskanie konta online:** Jeśli nadal masz dostęp do swojego konta, zaloguj się z zaufanego komputera i zresetuj hasło. Użyj nowego, unikalnego i silnego hasła - im dłuższe, tym lepiej. Jeśli nie masz włączonego uwierzytelniania dwuskładnikowego (MFA), teraz jest dobry moment, aby je włączyć. Jeśli nie masz dostępu do konta, skontaktuj się z serwisem i poinformuj go, że Twoje konto zostało przejęte lub skorzystaj z formularza pomocy zawierającego wskazówki co w takiej sytuacji poczynić. Jeśli posiadasz inne konta, które mają to samo hasło, co twoje przejęte konto, natychmiast je zmień.
- **Odzyskiwanie urządzeń:** W sytuacji kiedy program antywirusowy nie był w stanie naprawić zainfekowanego komputera lub jeśli chcesz mieć pewność, że urządzenie jest wolne od wirusów, rozważ reinstalacje systemu operacyjnego. Zastanów się również czy urządzenie, które posiadasz przypadkiem nie jest przestarzałe. Czasami taniej będzie kupić nowy sprzęt.
- **Finanse:** W przypadku problemów z kartą kredytową lub kontem bankowym, należy niezwłocznie skontaktować się z bankiem lub firmą obsługującą kartę kredytową. Im szybciej do nich zadzwonisz, tym większe prawdopodobieństwo, że odzyskasz swoje pieniądze. Zadzwoń do nich używając zaufanego numeru telefonu, znajdującego się na odwrocie karty płatniczej, wydrukowanego na zestawieniu operacji lub widocznego na stronie internetowej. Monitoruj swoje transakcje regularnie, aby wczas zareagować na nieautoryzowane płatności. Jeśli to możliwe, włącz automatyczne powiadomienia o każdej płatności lub przelewie.

Co zrobić, aby wyprzedzić cyberprzestępców?

Biuletyn OUCH Security Awareness jest publikowany co miesiąc i porusza kwestie tego, jak skutecznie zabezpieczyć swoje cyfrowe życie. Poniższej wymieniliśmy najważniejsze biuletyny OUCH, które należy przeczytać, aby się chronić. Zasady te koncentrują się na trzech kluczowych krokach:

1. Aktualizuj wszystkie swoje systemy i urządzenia do najnowszej wersji.
2. Używaj silnych, unikalnych haseł dla każdego ze swoich kont, zarządzaj nimi za pomocą menedżera haseł i włącz uwierzytelnianie dwuskładnikowe (MFA).
3. Bądź sceptyczny - uważaj na taktyki socjotechniczne, takie jak wiadomości phishingowe.

Redaktor gościnny

Sarah Morales (@SarahManley) jest starszą specjalistką programu w zespole Google ds. prywatności, bezpieczeństwa i ochrony. Kieruje się zaangażowaniem, koncentrując się na budowaniu społeczności, współpracy i partnerstwach. Jest członkiem zarządu WiCyS i aktywnie angażuje się w działania DEI w społeczności cyberbezpieczeństwa.

Źródła

Menedżer haseł: https://www.sans.org/newsletters/ouch/password-managers/
Zabezpieczenie kont online: https://www.sans.org/newsletters/ouch/one-simple-step-to-securing-your-accounts/
Działania na emocjach - o tym jak cyberprzestępcy oszukują: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
Ataki phishingowe: https://www.sans.org/newsletters/ouch/phishing-attacks-getting-trickier/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz