OUCH! Czerwiec 2023

OUCH!

SANS SECURITY AWARENESS

Biuletyn Bezpieczeństwa Komputerowego

Bezpieczeństwo kont bankowych

Wstęp

Konta bankowe i ich zawartość są głównym celem cyberprzestępców. Najbardziej zależy im na Twoich pieniądzach. Oprócz kont bankowych, należy zwrócić uwagę na konta oszczędnościowe, inwestycyjne i płatności online. Na szczęście dzięki kilku prostym, podstawowym krokom możesz zadbać o ich bezpieczeństwo.

Jak przebiega atak?

Banki inwestują ogromne pieniądze w zabezpieczanie swoich systemów, co bardzo utrudnia cyberprzestępcom złamanie zabezpieczeń. Właśnie dlatego cyberprzestępcy atakują Ciebie zamiast bezpośrednio konta bankowe. Zdają sobie sprawę, że nie masz zespołu bezpieczeństwa, który będzie Cię chronił, więc o wiele łatwiej jest zaatakować Ciebie niż bank. Oto dwa najczęstsze sposoby ataków i kradzieży pieniędzy:

Hasła: Każde Twoje konto jest chronione hasłem. Jeśli cyberprzestępca może odgadnąć lub złamać którekolwiek z tych haseł, może zalogować się na konto, a następnie przelać pieniądze na kontrolowane przez siebie konta bankowe. Istnieje wiele sposobów przejmowania haseł. Jedną z najpopularniejszych metod jest infekowanie komputera szkodliwym oprogramowaniem. Gdy Twój komputer zostanie zainfekowany, atakujący mogą przechwycić dane logowania, które wprowadzasz na stronę banku. Inną popularną metodą jest wysyłanie e-maili phishingowych, które podszywają się pod różne banki. Klikając link w wiadomości e-mail, wydaje ci się, że logujesz się na stronie swojego banku, ale w rzeczywistości logujesz się na fałszywą stronę kontrolowaną przez przestępców. To pozwala im przejąć dane logowania do bankowości, które mogą zostać wykorzystane do nieautoryzowanego zalogowania się do bankowości.

Pytanie: Cyberprzestępcy mogą po prostu poprosić Cię o podanie hasła lub przekazanie im pieniędzy. Takie ataki często zaczynają się od nawiązania kontaktu telefonicznego. Cyberprzestępcy wiedzą, że kiedy wzbudzą zwątpienie lub strach w użytkowniku, łatwiej im będzie skłonić go do popełnienia błędu. Właśnie dlatego większość e-maili phishingowych, połączeń i reklam wywołują poczucie pilności i nakłaniają do szybkiego działania. Na przykład, gdy zadzwonisz pod numer telefonu podany przez oszustów, przestępcy wywierają ogromną presję, aby doprowadzić do przejęcia konta. Mogą powiedzieć, że są z pomocy technicznej lub urzędu, a komputer jest zainfekowany i jeśli nie podejmiesz działań, stracisz wszystkie swoje pieniądze.

Chroń siebie

Na szczęście zabezpieczenie kont bankowych jest prostsze niż myślisz. Oto niezbędne kroki aby się zabezpieczyć.

Bądź podejrzliwy: Pamiętaj to Ty jesteś dla siebie najlepszą ochroną. Jeśli otrzymasz wiadomość e-mail, wiadomość tekstową, lub pojawi się dziwne okienko, może to być próba ataku. Im większe poczucie pilności i im większa presja nadawcy, aby działać szybko, tym bardziej prawdopodobne jest, że jest to atak.

Używaj silnych haseł / uwierzytelnianie wieloskładnikowe: Chroń każde swoje kontro za pomocą długiego, unikalnego hasła. Nie możesz zapamiętać wszystkich haseł? Dobrym wyborem może okazać się menedżer haseł, który je zapamiętuje i przechowuje. Najlepszym sposobem ochrony każdego konta jest włączenie uwierzytelniania wieloskładnikowego (MFA) wszędzie tam, gdzie jest to możliwe.

Kontrola: Kontroluj swoje konta. Możesz ustawić automatyczne alerty, które będą wysyłane e-mailem lub SMS-em za każdym razem, gdy będzie jakikolwiek przepływ pieniędzy z konta, lub na nie. W ten sposób możesz szybko wykryć każdą nieautoryzowaną lub podejrzaną transakcję. Im szybciej wykryjesz nieprawidłowości i zgłosisz je do banku, tym większe prawdopodobieństwo odzyskania pieniędzy.

Redaktor gościnny

Lynn Dohm jest dyrektorą Women in CyberSecurity (WiCyS). Ma doświadczenie w edukacji w zakresie cyberbezpieczeństwa, aktywnie angażuje się w programy finansowane z grantów. Lynn propaguje świadomość na temat znaczenia cyberbezpieczeństwa.
Twitter: @lynn_dohm. Linkedin: https://www.linkedin.com/in/lynndohm/.

Źródła

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/
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/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz