Biuletyn Bezpieczeństwa Komputerowego

Nie pozwól cyberprzestępcom ukraść swoich oszczędności

Oszustwo doskonałe i puste konto bankowe

Był pewien czwartkowy poranek. Ania spojrzała na telefon i zauważyła SMS-a z banku o treści: „Czy wykonałaś tę transakcję? Odpowiedz TAK lub NIE". SMS nie wzbudził u niej żadnych podejrzeń. Pomimo tego, że w dniu dzisiejszym nie dokonywała żadnych transakcji. Stwierdziła, że to prawdopodobnie błąd po stronie banku.

Odpowiedziała na SMS i w przeciągu kilku minut otrzymała telefon z banku. Dzwoniła kobieta podająca się za pracownika banku z działu ds. oszustw. Mówiąc spokojnym i stonowanym głosem powiedziała: „Wykryliśmy nietypową aktywność na Pani koncie. Aby to potwierdzić, musimy przeprowadzić weryfikację". Ania niczego nie podejrzewając zgodziła się. Kobieta przeprowadziła Anię przez szereg kroków, prosząc m.in. o podanie hasła do bankowości internetowej, a nawet prowadząc ją do zatwierdzenia powiadomienia na telefonie. „To zablokuje dostęp hakera" - zapewniła ją rozmówczyni. Ania zgadzała się na wszystko, nie zdając sobie sprawy, że właśnie rozmawia ze złodziejem.

Kilka godzin później telefon Ani zabrzęczał ponownie. Tym razem było to powiadomienie: "Z konta oszczędnościowego wypłacono 5000 zł". W panice usiłowała zalogować się do aplikacji bankowej, ale było już za późno. Hasło do aplikacji było niepoprawne. Atakujący zmienili hasło. Potem otrzymała kolejne powiadomienie o wypłacie środków.

Ania w jednej chwili zrozumiała, że padła ofiarą oszustwa. Wcześniejsza rozmowa z "pracownikiem działu ds. oszustw" była ukartowanym atakiem cyberprzestępcy, który zdobył pełną kontrolę nad jej kontem. Ania szybko zadzwoniła do banku, mając nadzieję, że uda jej się uratować zgromadzone środki finansowe.

Dlaczego należy chronić swoje konta finansowe?

Internetowe konta finansowe przechowują coś więcej niż tylko pieniądze. To najczęściej lata ciężkiej pracy, plany na przyszłość czy stabilność finansowa. Cyberprzestępcy nieustannie szukają okazji do szybkiego i łatwego zarobku, a jeden nasz błąd może doprowadzić do znacznych strat finansowych. Jeśli myślisz, że proste hasło powstrzyma tych przestępców to jesteś w błędzie.

Dzisiejsi cyberprzestępcy są sprytni, podstępni i nieustępliwi. Kluczowe jest proaktywne zabezpieczanie swoich kont finansowych. Nie tylko pomoże to zapobiec nieautoryzowanemu dostępowi, ale także zapewni ci spokój ducha, wiedząc, że twoje ciężko zarobione pieniądze są bezpieczne.

Pięć kroków do zatrzaśnięcia drzwi przed cyberprzestępcami

1. **Włącz uwierzytelnianie wieloskładnikowe (MFA):** Uwierzytelnianie wieloskładnikowe dodaje dodatkową warstwę zabezpieczeń do kont online, wymagając weryfikacji tożsamości za pomocą dwóch lub więcej metod: czegoś co znasz (hasło), czegoś co masz (smartfon lub token sprzętowy) lub czegoś czym jesteś (odcisk palca lub rozpoznawanie twarzy). Nawet jeśli cyberprzestępca uzyska dostęp do hasła, nadal będzie potrzebował drugiego czynnika, aby uzyskać dostęp do konta. Zawsze konfiguruj MFA gdy tylko jest dostępne, szczególnie w przypadku kont finansowych.

2. **Używaj silnych, unikalnych haseł:** Twórz silne, unikalne hasła dla każdego konta. Im dłuższe hasło i im więcej znaków zawiera, tym lepiej. Dobrym pomysłem jest użycie hasła, które składa się z wielu słów. Masz problem z zapamiętaniem haseł? Nie martw się, na to też jest rozwiązanie. Skorzystaj z menedżera haseł, który pomoże Ci wygenerować i pamiętać wszystkie te długie, unikalne hasła.

3. **Nie daj się nabrać na oszustwa:** Jednym z najłatwiejszych sposobów uzyskania dostępu do kont przez cyberprzestępców jest po prostu poproszenie o to użytkownika. Atakujący tworzą wiadomości e-mail, wiadomości tekstowe, które wyglądają jakby pochodziły z banku lub instytucji finansowej. Zawsze weryfikuj źródło przed kliknięciem w link, pobraniem załącznika lub odpowiedzią na wiadomości. Im większe poczucie pilności sprawia wiadomość, tym większe prawdopodobieństwo, że jest ona atakiem. Najlepszym sposobem ochrony jest bezpośrednie przejście na oficjalną stronę internetową banku poprzez wpisanie adresu w przeglądarce lub skontaktowanie się z bankiem przy użyciu zaufanego numeru telefonu.

4. **Monitoruj swoje konta:** Wyrób sobie nawyk systematycznego sprawdzania swoich kont finansowych pod kątem wszelkich nietypowych transakcji. Co więcej, większość instytucji finansowych oferuje automatyczne powiadomienia o dużych wypłatach lub podejrzanych działaniach. Skonfigurowanie automatycznych alertów może pomóc we wczesnym wykryciu nieuczciwych transakcji i podjęciu szybkich działań w celu zminimalizowania szkód. Jeśli coś nie wygląda dobrze, nie czekaj - podejmij natychmiastowe działania.

5. **Trzymaj swoje urządzenia pod kontrolą:** Telefon, laptop i tablet są jak sejfy do świata finansów. Zapewnij im bezpieczeństwo dzięki blokadzie ekranu, szyfrowaniu dysku i najnowszym aktualizacjom oprogramowania.

Redaktor gościnny

Elizabeth Rasnick jest adiunktem w Centrum Cyberbezpieczeństwa na University of West Florida. Posiada doświadczenie w programowaniu i pracy w zespole reagowania na incydenty. Pełni funkcję wiceprezesa WiCyS Florida Affiliate i posiada tytuł doktora w dziedzinie technologii informatycznych.

Źródła

Trzy najczęstsze sposoby ataków: https://www.sans.org/newsletters/ouch/top-ways-attackers-target-you/
Działania na emocjach - o tym jak cyberprzestępcy oszukują: https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/

Polski przekład CERT Polska: Aleksandra Węgrzynowicz, Bartłomiej Wnuk