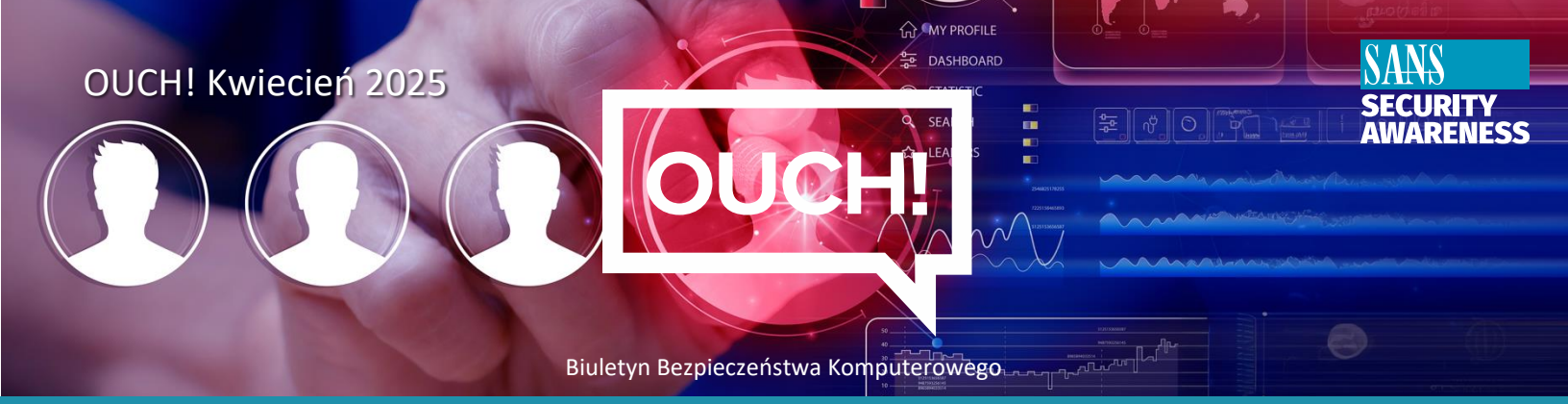

Przejęcia kont

Historia Emmy

Emma przeglądała Facebooka, kiedy zobaczyła post swojej kuzynki Sary. W poście zamieszczono druzgocącą wiadomość: ojciec Sary zamieszkał się do domu opieki i sprzedawał swoje rzeczy, aby pomóc w pokryciu kosztów pobytu. Dołączone były zdjęcia jego samochód, biżuterii i zabytkowych mebli w bardzo niskich cenach.

Chcąc pomóc, Emma po raz pierwszy od lat skontaktowała się z Sarą za pośrednictwem komunikatora. Sara ucieszyła się z wiadomości od kuzynki i poinformowała Emmę o stanie ojca. Sara naciskała na szybką finalizację zakupów i podkreślała, że oferowane przedmioty cieszą się dużą popularnością i mogą zostać szybko sprzedane. Emma przesłała pieniądze kuzynce, jednak szybko odkryła, że cały post był oszustwem.

Nigdy tak naprawdę nie rozmawiała ze swoją kuzynką. Konto Sary zostało przejęte przez oszusta. Po uzyskaniu dostępu do konta oszust opublikował fałszywe wiadomości o ojcu Sary, a następnie oszukał rodzinę i znajomych kobiety. Kiedy ludzie myśleli, że kupują przedmioty od Sary (i wspierają jej ojca), w rzeczywistości płacili oszustowi, który zniknął z pieniędzmi.

Jak to się stało?

Oszuści przejmują konta w mediach społecznościowych na platformach takich jak Facebook czy Instagram. Po uzyskaniu dostępu do konta, podszywają się pod właściciela i udostępniają posty, które wpływają na emocje odbiorców i mają nakłonić ludzi do działania. Oszustwa te często wykorzystują tematy takie jak: napad w mieście, porwanie dziecka, wypadek samochodowy lub poszukiwania osoby oskarżonej o czyn karalny.

Ofiary są manipulowane, wierząc, że post napisała osoba, którą znają i której ufają. Wysyłają pieniądze, często za pomocą BLIKa lub przelewu bankowego, by później dowiedzieć się, że tak naprawdę nie mieli do czynienia z nikim bliskim, a ich pieniądze zniknęły.

Co sprawia, że tego typu oszustwa są tak niebezpieczne?

- **Przejęte zaufanie**: Oszuści wykorzystują znajomych właściciela konta, które przejmują. Posty wydają się pochodzić od przyjaciela lub członka rodziny, co czyni je bardziej wiarygodnymi.
- **Manipulacja emocjonalna**: Oszuści wykorzystują tematy osobiste, które często stwarzają silne poczucie pilności i zmuszają do popełnienia błędu.
- **Szybkie rozprzestrzenianie się**: Gdy konto ofiary zostanie przejęte, oszust może szybko dotrzeć do setek, a nawet tysięcy osób. Ponadto wiele osób używa tego samego hasła do wielu serwisów, więc dane z jednego konta mogą zostać użyte do przejęcia innych kont ofiary.

Jak chronić siebie i innych

- **Bądź sceptyczny wobec postów wzbudzających silne emocje**: Jeśli post wydaje się niezwykle emocjonalny i wiąże się z wysłaniem komuś pieniędzy, zatrzymaj się i zweryfikuj, może to być oszustwo.

- **Sprawdź to bezpośrednio u danej osoby**: Skontaktuj się z tą osobą osobnym kanałem, aby potwierdzić informacje. Na przykład zadzwoń do niej przez telefon lub porozmawiaj z nią osobiście. Dość często ofiara nawet nie wie, że jej konto zostało przejęte ani o wpisach oszusta na jej koncie.

- **Zweryfikuj czerwone flagi** : Oszuści często proszą o płatność za pomocą takich metod jak BLIK lub zapłata przez kryptowaluty. Kolejną czerwoną flagą jest sytuacja, gdy proszą Cię o skorzystanie z innej platformy w celu kontynuowania komunikacji (np. przejście z Facebook Messenger do WhatsApp).

- **Ochrona konta:** Jeśli Twoje konto zostanie przejęte, pierwszą rzeczą, jaką często robią cyberprzestępcy, jest zmiana hasła. Gdy tak się stanie, odzyskanie konta może okazać się bardzo trudne. Zacznij od ochrony każdego konta za pomocą długiego i unikalnego hasła. Następnie włącz uwierzytelnianie wieloskładnikowe dla każdego konta. Te dwa proste kroki sprawią, że konta będą znacznie bezpieczniejsze, a oszuści Cię za to znienawidzą!

Bądź o krok do przodu

Jeśli chodzi o oszustwa polegające na przejęciu konta, jesteś swoją najlepszą ochroną. Jeśli podejrzewasz, że spotkałeś się z tym oszustwem, zgłoś podejrzane konto i natychmiast powiadom administratora platformy.

Redaktor gościnny

Amie Dsouza jest specjalistką ds. cyberbezpieczeństwa współpracującym z dużą amerykańską linią lotniczą. Pracowała w sześciu krajach i jest członkiem zarządu Women in Cybersecurity (WiCys). Amie aktywnie opowiada się za edukacją wszystkich na temat bezpieczeństwa danych osobowych w Internecie.

Źródła

Jak przestępcy kradną nasze danehttps://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/
Jak cyberprzestępcy kradną Twoje hasła:https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords
Moc haseł:https://www.sans.org/newsletters/ouch/power-passphrase/
Zostałem zhakowany. Co teraz?:https://www.sans.org/newsletters/ouch/im-hacked-now-what/

Polski przekład CERT Polska: Aleksandra Węgrzynowicz, Bartłomiej Wnuk