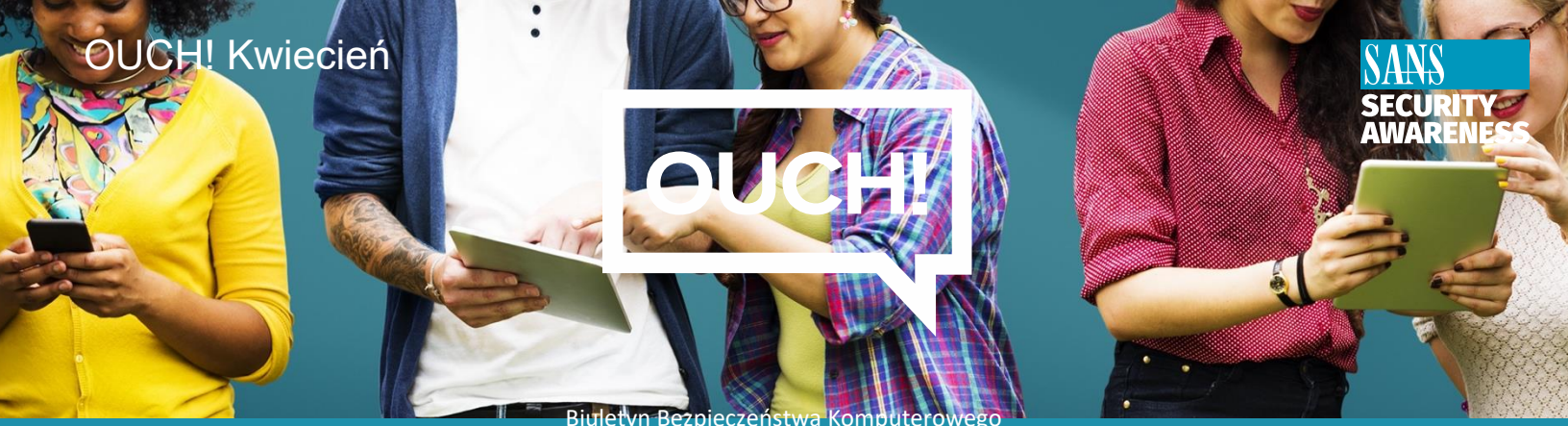

Biuletyn Bezpieczeństwa Komputerowego

Najpopularniejsze oszustwa w serwisach społecznościowych

Wstęp

Media społecznościowe to fantastyczny sposób na komunikowanie, dzielenie informacjami i zabawę z innymi, ale jest to również łatwy sposób na oszukiwanie i wykorzystywanie milionów ludzi przez cyberprzestępców. W tym wydaniu biuletynu bezpieczeństwa komputerowego opiszemy najpopularniejsze trzy sposoby oszustw, z którymi możemy sie spotkać za pośrednictwem serwisów mediów społecznościowych.

Oszustwa inwestycyjne

Czy kiedykolwiek widziałeś post o inwestycji, która obiecuje ogromny zysk w krótkim czasie i przy rzekomo niewielkim lub zerowym ryzyku? Zazwyczaj oferty takie nie istnieją, a obiecywanie szybkich i wysokich zysków bez ryzyka jest po prostu oszustwem inwestycyjnym. Tym sposobem oszuści próbują zachęcić do inwestycji, co w konsekwencji prowadzi do kradzieży zainwestowanych środków. Oszustwa te w celu uwiarygodnienia inwestycji i zwiększenia zainteresowania, często zawierają fałszywe reklamy lub historie sukcesów poprzednich klientów. Częstym motywem jest inwestowanie w kryptowaluty lub nieruchomości, a płatności możliwe są jedynie za pośrednictwem kryptowalut lub innych niestandardowych płatności. Pamiętaj że jeżeli oferta inwestycji wygląda zbyt dobrze, to najprawdopodobniej jest próbą oszustwa. Miej świadomość, że nie istnieje coś takiego jak gwarantowane inwestycje o wysokiej stopie zwrotu. Inwestuj swoje pieniądze tylko w zaufane, dobrze znane źródła inwestycyjne, a nie w poznanych w sieci nieznajomych, którzy wciskają Ci schemat szybkiego i łatwego wzbogacenia się.

Oszustwa matrymonialne

Oszustwo matrymonialne to sposób wyłudzenia pieniędzy od osób, które przez oszustów zostały uznane za samotne lub szukające miłości. Atakujący użyje wszelkich możliwych sposobów aby zbudować zaufanie u swojej ofiary. Przez pewien czas będzie korespondował ze swoją ofiarą, wysyłając jej drobne prezenty oraz fałszywe zdjęcia jego wizerunku. W pewnym momencie przedstawi tragiczną historię, która wymaga pożyczenia pieniędzy od poszkodowanej osoby, tj. na koszty leczenia w szpitalu, opłaty cła przesyłki itp. Aby unikać osobistego spotkania, atakujący zazwyczaj twierdzą, że pracują w branży, która im to uniemożliwia np. jest lekarzem lub pracuje w wojsku. Często proszą o przekazanie pieniędzy w formie przelewu lub karty podarunkowej, aby szybko zdobyć gotówkę i równocześnie zachować anonimowość.

Tego typu oszustwa są powszechne nie tylko w mediach społecznościowych, ale także w internetowych aplikacjach randkowych. Zachowaj ostrożność wobec osób poznanych w internecie. Nie spiesz się i nigdy nie wysyłaj pieniędzy osobie, której nigdy nie widziałeś.

Zainteresuj się osobami z Twojego otoczenia, które mogą być narażone na tego typu oszustwo a następnie ich ostrzeż. Osobie zaangażowanej w związek emocjonalny będzie ciężko uwierzyć, że to może być oszustwo.

Fałszywe sklepy i aukcje

Oszuści oferują przedmioty w wyjątkowo niskiej cenie, zachęcając tym samym potencjalne ofiary do złożenia zamówienia. Finalnie ofiara traci pieniędzy oraz nie otrzymuje towaru, za który zapłaciła. Interesujące reklamy w mediach społecznościowych będą promować niewiarygodnie niskie ceny i zawierać linki prowadzące do stron, które wydają się być prawdziwe i sprzedają przedmioty znanych marek. Zazwyczaj są to fałsze sklepy internetowe. Uważaj na sklepy, które nie zawierają informacji kontaktowych, nie mają regulaminu, mają niedziałający formularz kontaktowy, brak jest możliwości opłaty przedmiotu za pobraniem a przelew bankowy jest jedyną opcją płatności. Wpisz nazwę sklepu internetowego lub jego adres w wyszukiwarce, aby sprawdzić jakie są w internecie opinie o tym sklepie. Szukaj terminów takich jak "scam", "oszustwo", "nigdy więcej", "fake", "fałszywy". Bądź podejrzliwy w przypadku internetowych promocji lub ofert, które wydają się zbyt piękne, aby mogły być prawdziwe. Zamiast pozornej oszczędności, zakupy internetowe warto robić w zaufanych i sprawdzonych sklepach internetowych.

Pamiętaj, że to Ty jesteś dla siebie najlepszą ochroną. Wybierz sklep internetowy mądrze. Masz nad tym kontrolę. Wystarczy wiedzieć, że tego typu oszustwa często są dystrybuowane za pośrednictwem mediów społecznościowych. Bądź czujny i kupuj dopiero po upewnieniu się, że nie jest to oszustwo.

Redaktor gościnny

Chris Elgee (@chriselgee) pracuje jako pentester i tworzy wyzwania dla @CounterHackSec. Pracuje w Army National Guard oraz jest certyfikowanym instruktorem SANS. Lubi poznawać najdrobniejsze szczegóły techniczne, budować z nich coś większego i dzielić się tym z uczniami i klientami.

Źródła

Better Business Bureau Scam Tracker: https://www.bbb.org/ScamTracker
Ataki socjotechniczne: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Bezpieczne zakupy online: https://www.sans.org/newsletters/ouch/shopping-online-securely-nov-21/
Ataki i oszustwa telefoniczne: https://www.sans.org/newsletters/ouch/vishing/

Polski przekład CERT Polska: Bartłomiej Wnuk, Aleksandra Węgrzynowicz