Magiczny Kraków

Jak oszukują cyberprzestępcy?

2025-02-05

Jakich metod używają cyberprzestępcy? Jaki jest typowy scenariusz najczęstszego oszustwa? Jak się nie dać nabrać? Gdzie i po co zgłaszać próby oszustwa? Iwona Prószyńska, specjalistka od cyberbezpieczeństwa z NASK, mówiła o tym Tadeuszowi Mordarskiemu.

Odbieram telefon i słyszę: „Dzień dobry, panie (tu pada moje imię i nazwisko). Z tej strony bank XYZ. Właśnie wpłynął do nas wniosek o kredyt. Czy występował Pan o tę pożyczkę”? Co powinienem zrobić?

Iwona Prószyńska: Odłożyć słuchawkę i samodzielnie zatelefonować do tego banku, z którego rzekomo do nas dzwoniono. Każda sytuacja, gdy ktoś podaje się za policjanta, urzędnika, pracownika banku i próbuje uzyskać od nas informacje czy skłonić nas do działania, wywierając presję (poprzez stosowanie technik związanych z emocjami typu: „ktoś teraz bierze na pana kredyt” lub „dzieją się niepokojące rzeczy na pana koncie”) powinna być dla nas sygnałem, że możemy mieć do czynienia z oszustami. A najłatwiej to zweryfikować samemu, dzwoniąc do danej instytucji, by potwierdzić informację. Oszustwa oparte na socjotechnice to dominujący trend, jeśli spojrzymy na statystyki zgłoszeń wpływających do CERT Polska, bo to tzw. nisko wiszące owoce. Nie jest w nich wymagana żadna zaawansowana technologia. Nie potrzeba hakera włamującego się do systemu. To my sami pod wpływem emocji, dajemy oszustom to, czego od nas oczekują. W pośpiechu czytamy SMS-a, w którym ktoś grozi odłączeniem prądu lub platformy streamingowej, jeśli nie klikniemy w link i nie dopłacimy 90 groszy na podstawionej przez oszusta stronie. Odbieramy telefon od „konsultanta”, który mówi: coś złego dzieje się na pana koncie i musi pan natychmiast zareagować. No więc reagujemy. A skoro ta technika jest skuteczna, to oszuści często po nią sięgają.

Czy to oznacza, że jeżeli zostajemy w ten sposób oszukani, to możemy mieć pretensje wyłącznie do siebie?

Ostatecznie to my podajemy oszustom te dane, których od nas chcą. Ale nie jesteśmy przecież świadomi, że właśnie padamy ofiarą przestępców, dlatego CERT Polska, działający w instytucie NASK zespół reagowania na incydenty w sieci, podejmuje szereg działań mających za zadanie ochronić nas w sytuacji, w której nie wiemy, że komunikujemy się z oszustem. Jednym z takich działań jest Lista Ostrzeżeń, na którą trafiają strony jednoznacznie łączone przez naszych ekspertów z oszustwem. Jak to wygląda w praktyce? Dostajemy SMS z linkiem do strony, poprzez którą mamy rzekomo dopłacić kilka groszy za fakturę. Jeżeli prześlemy tego SMS-a do CERT Polska na bezpłatny numer 8080, analitycy ocenią, czy to strona wykorzystywana przez oszustów. Jeśli tak – dostęp do niej zostanie zablokowany. To oznacza, że kolejna osoba już nie będzie mogła tam wejść i podać oszustom swoich danych. Tylko w zeszłym roku zablokowaliśmy 75 milionów prób wejść na strony z tej listy! Czyli potencjalnie 75 mln razy ktoś mógłby dać się oszukać i stracić pieniądze, gdyby wcześniej ktoś inny nie zgłosił podejrzanej strony czy SMS-a. Analitycy CERT Polska także sami prowadzą działania, monitorują to, co się dzieje w internecie, i dopisują kolejne adresy na Listę Ostrzeżeń. Innym mechanizmem jest wzorzec SMS. Na podstawie zgłoszeń tworzymy wzorzec oszukańczego SMS-a,

następnie trafia on do operatorów, którzy blokują wszystkie SMS-y pasujące do wzorca, zanim dotrą one do użytkowników. To rozwiązanie działa od zeszłego roku i już udało się zablokować ponad 1,5 mln SMS-ów.

Mówi Pani o tak gigantycznej skali, że siłą statystyki ktoś da się oszukać.

Tak działają oszustwa masowe. Jeśli SMS np. dotyczący niedostarczonej paczki jest wysyłany jednocześnie do kilku tysięcy osób, to zawsze znajdzie się ktoś, kto właśnie czeka na przesyłkę.

Kolejna sytuacja. Siedzę w galerii handlowej, łączę się z ogólnodostępną siecią wi-fi i pracuję: loguję się na pocztę, robię przelewy…

Tu nie ma się czego obawiać. Mit związany z niebezpieczeństwami podczas korzystania z publicznych sieci wi-fi jest jednym z najczęściej powielanych. W ten sposób przestępcy mogli działać kilkanaście lat temu. Dziś cały ruch w sieci jest szyfrowany, a to zapewnia nam bezpieczeństwo. Możemy więc bezpiecznie korzystać z bankowości, logując się przez publiczną sieć. Od lat najpoważniejsze i najczęstsze oszustwa to te socjotechniczne. Ich scenariusz jest zawsze taki sam i warto go zapamiętać. Mamy podmiot (bank, instytucja itp.) cieszący się autorytetem, pod który podszywają się oszuści, mamy presję czasu i emocje (zrób coś natychmiast, bo inaczej grożą ci konsekwencje) i dzięki temu – jak po sznurku – idziemy do miejsca, do którego chcą nas zaprowadzić cyberprzestępcy (np. na stronę, na której podajemy swoje dane). Tego powinniśmy się wystrzegać.

Skąd powinniśmy czerpać wiedzę na temat cyberbezpieczeństwa?

Warto śledzić social media CERT Polska, bo tam na bieżąco i w czasie rzeczywistym publikowane są ostrzeżenia dotyczące różnych „kampanii” robionych przez oszustów. Możemy też włączyć powiadomienia push w aplikacji mObywatel w zakładce „Bezpiecznie w sieci”. Tam też można zgłaszać incydenty do CERT Polska i zapoznać się ze zbiorem krótkich materiałów edukacyjnych o najpopularniejszych oszustwach. Przydatne informacje oraz formularz zgłoszeń są także na stronie: **cert.pl**.

Iwona Prószyńska – ekspertka w Centrum Cyberbezpieczeństwa i Infrastruktury w instytucie badawczym NASK. Specjalistka ds. komunikacji w obszarze cyberbezpieczeństwa w CERT Polska.

CERT Polska działa w strukturach NASK – Państwowego Instytutu Badawczego, prowadzącego działalność naukową, krajowy rejestr domen.pl i dostarczającego zaawansowane usługi teleinformatyczne. CERT Polska to pierwszy powstały w naszym kraju zespół reagowania na incydenty związane z bezpieczeństwem w sieci.