**Jak nie stać się okazją… dla oszustów**

**Przed nami Black Friday – ważny dzień dla całej branży związanej ze sprzedażą, zarówno stacjonarną, jak i online. Na żniwa liczą niestety nie tylko uczciwi sprzedawcy, ale także… oszuści coraz bardziej wyspecjalizowani w przekrętach w internecie.**

**Liczby robią wrażenie**

Internetowi oszuści mają się świetnie, polują nie tylko na starsze osoby, ale również na młodszych użytkowników, którzy w pędzie życia klikają często… zbyt szybko. Na szczęście coraz więcej internautów ma czujne oko i zgłasza podejrzane strony czy próby wyłudzenia danych.

Zespół CERT Polska, który zajmuje się monitorowaniem polskiej cyberprzestrzeni, odebrał w 2022 r. ponad **322 tysiące zgłoszeń dotyczących podejrzanych zjawisk** w sieci. W przypadku OLX jedynie od stycznia tego roku sam serwis zgłosił do zablokowania prawie 7000 fałszywych stron, z czego blisko 5000 użytkownicy zgłaszali sami. Warto również zauważyć, że ostrzeżenie phishingowe na blog.olx.pl, które opracował zespół OLX, ma średnio dziennie(od stycznia 2023 r.) ponad 1700 wyświetleń.

– *Każdy z uczestników platformy widzi nasze ostrzeżenia za każdym razem, gdy wchodzi do aplikacji i chce podać swoje dane na czacie. Jest uczulany na to, by w sposób ostrożny udostępniać swoje dane. Bannery z ostrzeżeniami phishingowymi były od stycznia 2023 r. wyświetlone prawie* ***550 mln razy****, to ponad pół miliarda!* – zauważa Piotr Chochłow, service content manager w OLX.

**Atlas (nieprzyjemnych) zdarzeń, czyli na co uważać w Black Friday?**

Oszuści posługują się różnymi sztuczkami. Spoofing, czyli podszywanie się pod numer telefonu znanej firmy czy instytucji i prowadzenie rozmowy w taki sposób, by rozmówca dał się nabrać, oraz fałszywe telefony z banków pod pretekstem próby włamania na konto to w ostatnich latach bardzo często stosowane metody. Wszystkie tricki dążą z reguły do wyłudzenia pieniędzy lub poufnych danych.

A jakie są najpopularniejsze chwyty internetowych cyberoszustów? Fałszywe smsy czy e-maile z prośbą o uregulowanie zaległej faktury. W przypadku braku wpłaty odcięty będzie prąd / internet / gaz. Czasem to tylko kwestia dopłaty kilku złotych, a jednak taki błąd może kosztować znacznie więcej. Wystarczy sprawdzić historię przelewów i przyjrzeć się dokładnie treści wiadomości czy nazwie nadawcy. Jedna mała literówka powinna wzbudzić naszą czujność, a błędnie zapisany np. NĘTFLIX od razu wygląda jakoś inaczej, gdy mu się bliżej przyjrzeć.

Na platformach zakupowych szczególnie trzeba uważać na zbyt mało prawdopodobne okazje, czyli naprawdę niewiarygodnie niskie ceny, oraz próby przeniesienia konwersacji poza serwis. Przykładowo Pan Maciej chciałby w okazyjnej cenie kupić dobry, ale używany rower dla syna. Znajduje interesujący go egzemplarz i nawiązuje kontakt ze sprzedawcą. Osoba sprzedająca prosi go o numer telefonu, pod pretekstem przyspieszenia transakcji, i kontakt za pośrednictwem aplikacji WhatsApp. Co się może wydarzyć? Sprzedający może wysłać fałszywe linki, w które nigdy pod żadnych pozorem nie należy klikać.

Wyłudzenie danych może przybierać różne formy. Stają się wiadomościami z fałszywymi regulaminami, pomocą techniczną, instrukcją odebrania paczki… A czasem wystarczy zdrowy rozsądek i chwila namysłu, czy treść nie wygląda jakoś podejrzanie.

**Kilka porad dla kupujących:**

* sprawdzaj wiarygodność stron, z których korzystasz (np. poprzez link checker)
* bądź świadomy możliwości zabezpieczeń kupna, np. przez Przesyłki OLX
* zdaj się na swoje oko – jeżeli strona wygląda nieprofesjonalnie, brakuje polskich znaków, a opisy brzmią nieskładnie, zachowaj czujność, może to być fałszywka
* nie klikaj w żadne linki pochodzące spoza danej platformy zakupowej, np. o zaległej płatności, instrukcji odbioru przesyłki w paczkomacie, pomocy technicznej
* kiedy trafisz na oszusta – zgłoś do CERT nielegalne działanie! W ten sposób inni nie dadzą się oszukać. Przykładem może być OLX, który dzięki aktywnemu udziałowi użytkowników skutecznie zmniejsza liczbę oszustw. Każde podejrzane ogłoszenie w OLX można oznaczyć przyciskiem Zgłoś i wybrać rodzaj naruszenia
* poświęć czas na edukację – posłuchaj np. podcastu FRAUDycja realizowanego przez OLX i CERT:

<https://www.youtube.com/watch?v=F_-YbVp8t1c&list=PLdYnmYhMUr5fqC8KEFuN_jZnYQRihHLIE&t=168>

**Czasy się zmieniły, oszuści się profesjonalizują**

Im szybciej postępuje rozwój technologii, tym większe jest zagrożenie ze strony oszustów coraz bardziej profesjonalizujących swoją działalność.

– *Rozwój sztucznej inteligencji niestety pomaga też oszustom, a cybeprzestępczość staje się coraz bardziej wyrafinowana. Jej ofiarami są coraz młodsze osoby, już nie tylko seniorzy. Coraz częściej młode pokolenia dają się złapać przez nadmierne poczucie pewności siebie. Skoro część ich życia związana jest z obecnością w sferze online, wydaje im się, że nie tak łatwo ich nabrać. Rzeczywistość okazuje się inna* – dodaje Piotr Chochłow.

Banki, Ministerstwo Cyfryzacji, instytucje, platformy sprzedażowe i wiele innych – przed phishingiem ostrzegają bardzo często. A my, kupujący, i tak się nabieramy. Może dla odmiany w tym roku nie dajmy się zrobić w bambuko, nie tylko na promocjach.

**OLX**

*Serwis OLX każdego dnia ułatwia dokonywanie dobrych wyborów milionom Polaków. We wrześniu 2023 roku OLX odwiedziło prawie 11 mln użytkowników (Badanie Mediapanel prowadzone przez Gemius Polska sp. z o.o., wrzesień 2023).*

**Kontakt dla mediów:**

Paulina Musielak-Rezmer

PR Lead

tel. +48 696 890 340