KURIER SPECJALNY

W INTERNECIE BĄDŹ BEZPIECZNY

ISSUE NO. ONE AND ONLY | 8 LUTEGO 2022 R.

ŚWIAT TO ZA MAŁO – OSZUŚCI WOLĄ CYBERPRZESTRZEŃ

Paulina Rezmer

„Dzisiaj już nie ma szpiegów. Ta niepiękna profesja przestała się opłacać, odkąd zastąpiła ją prasa". O taką teorię pokusił się swego czasu Oskar Wilde. W rzeczy samej – mało dziś szpiegów nawet w literaturze i filmie. Za to wielu jest dziennikarzy, którzy na co dzień podążają tropem oszustów i oszukanych w wirtualnym świecie.

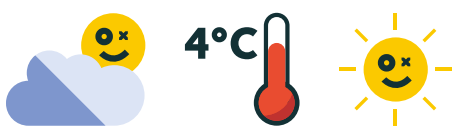
Jeśli już ktoś podejmuje ten trop, to pewnie trafniej byłoby nazywać go dziennikarzem-detektywem. Czasem w tej roli można mieć przygody tak zabawne, jak miewał Sherlock Holmes. Proszę sobie wyobrazić tropienie i opisywanie działań kogoś, kto wygenerował już fałszywą etykietę do przesyłki i namawia ofiarę do potwierdzenia płatności za... dom z ogłoszenia. Albo inną sytuację, gdy listy do redakcji pisze zakochany po uszy jegomość i prosi o poradę w sprawie złamanego serca, bo kontakt z hinduską księżniczką, która obiecywała złote góry i wieczne szczęście, nagle się urwał. Dziwnym zbiegiem okoliczności nastąpiło to akurat wtedy, kiedy nasz Romeo odmówił opłacenia jej biletu lotniczego.

Nigdy jednak nie jest zabawnie, gdy internauta padnie ofiarą oszustwa, tracąc przy tym oszczędności życia albo na życie. Każde, nawet najmniejsze pieniądze znikające z konta i każde, nawet z pozoru najmniej istotne dane osobowe użyte bez wiedzy i zgody osoby, której są częścią lub własnością, to nadużycie albo przestępstwo. Oszukany często ignoruje to, co wprawnemu śledczemu od razu rzuci się w oczy. Bagatelizuje znaki dymne i rozsypane przez oszustów okruszki. Doświadczony detektyw od razu rozpozna sygnały alarmowe i w porę powie: „stop, ręce do góry". Mniej ważne jest to, czy na to hasło oszust faktycznie zareaguje. Ważne, aby ręce podniósł (oby niedoszły!) poszkodowany. Podniósł i oderwał je od klawiatury komputera czy ekranu smartfona, unikając tym samym kliknięcia w nieodpowiedni link, nawiązania zgubnej znajomości lub udostępnienia danych.

Na kolejnych stronach zapraszamy do świata, w którym detektywi, złoczyńcy i poszkodowani spotykają się w jednej, wirtualnej przestrzeni. Co z tego wyniknie? Oby wiedza i mądre wnioski na przyszłość.

W internecie wszyscy musimy być ekspertami – Adam Haertle ..... str. 4

POGODA



BEZPIECZEŃSTWO NA KAŻDYM KLIKU

Paulina Rezmer

Niemal każdemu z dni w roku przypisano powód do świętowania albo zwracania uwagi na jakieś zjawisko lub problem. Chyba wszyscy wiemy, kiedy przypadają Dzień Dziecka czy walentynki. Ale czy wiedzą Państwo, że na początek lutego przypada uroczo nazwany Światowy Dzień Obszarów Wodno-Błotnych obchodzony od ponad 50 lat? Albo że 9 lutego miłośnicy pizzy mają pretekst, by ustawiać się w długich kolejkach po swój ulubiony przysmak? My w OLX szczególnie lubimy święto ruchome, przypadające w drugi wtorek lutego. To Dzień Bezpiecznego Internetu.

Wydarzenie obchodzone jest z inicjatywy Komisji Europejskiej od 2004 r. W tym roku przypada 8 lutego. Początkowo świętowały je jedynie państwa europejskie, ale już od lat w działania angażują się kraje z całego świata. Pierwotnie celem DBI było zwrócenie uwagi na kwestię bezpiecznego dostępu dzieci i młodzieży do zasobów internetowych. Obecnie kontekst jest znacznie szerszy i dotyczy zagrożeń czyhających na wszystkich użytkowników sieci.

Większość z nas nie wyobraża sobie dziś życia bez internetu. Choć trudno w to uwierzyć, w 2025 r. do trzydziestki dobije pokolenie Z, dla którego cyfrowy świat i nowoczesne technologie istnieją od zawsze. Wybuch pandemii koronawirusa przyspieszył rozwój wirtualnych narzędzi i naszą globalną przeprowadzkę do świata online. W sieci już nie tylko robimy zakupy i oglądamy seriale – możemy też skończyć szkołę, studia, znaleźć i wykonywać nową pracę bez wychodzenia z domu, porozmawiać z lekarzem i załatwić urzędową albo bankową sprawę.

Ale to nie wszystko. Wystarczy kilka kliknięć, by z poziomu własnej, wygodnej kanapy przenieść się do największego muzeum na świecie, paryskiego Luwru. Tak, można być w dresie, a dodatkowym udogodnieniem są puste korytarze i brak kolejek do Mona Lisy. Dzięki internetowej kamerze przez 24 godziny na dobę można też podglądać, co dzieje się np. na słynnej Bourbon Street w Nowym Orleanie albo na Times Square w Nowym Jorku. W chwili, kiedy pisaliśmy ten tekst, przez tę pierwszą lokalizację przejeżdżał wóz nocnego patrolu policji. Czy mundurowi jedli pączki i popijali gorącą kawę? Tego nie możemy stwierdzić na pewno. Po części przez przyciemnione szyby w samochodzie, po części dzięki prawu do ochrony prywatności i wizerunku, o które przecież wszyscy tak dbamy.

Niektórych cały ten wirtualny świat napawa niepokojem. Inni w cyberprzestrzeni czują się jak ryby w wodzie. Ocean możliwości, jakie daje internet, z powodzeniem wykorzystują też oszuści. Podobnie jak w realnym świecie, również tutaj czyhają na chwilę naszej nieuwagi, ale przede wszystkim liczą na brak wiedzy. Konsekwencje mogą być różne. Od kilku minut straconych na dialog z podejrzanym kupującym, poprzez wyciek danych z profilu w mediach społecznościowych, aż do utraty majątku, tożsamości, a nawet zdrowia.

Im szerszy płynie do nas strumień danych z internetu, tym szybciej musimy je przetwarzać. Im więcej używamy narzędzi i nowych technologii, tym więcej musimy się nauczyć i zapamiętać. Im większa liczba okazji do wydawania pieniędzy w sieci, tym uważniej powinniśmy trzymać się za portfel. Dzień Bezpiecznego Internetu to okazja, by mówić, czytać i edukować na temat bezpieczeństwa w sieci, tak abyśmy w miejscu, które dla wielu z nas stało się nowym domem, czuli się jak u siebie.

Sieć nask.pl od lat gromadzi informacje na temat inicjatyw podjętych w ramach DBI. Każdy może zadbać o edukację i bezpieczeństwo sieci w swojej lokalnej (a dzięki internetowi także globalnej!) społeczności.

Liczba zgłaszanych inicjatyw rośnie z roku na rok, a to pokazuje, że obchody Dnia Bezpiecznego Internetu zataczają coraz większe kręgi. W 2019 r. do projektu zgłoszono 3977 inicjatyw, w 2020 r. – 4600 inicjatyw, a rok temu już 4960 inicjatyw. Być może w tym roku padnie kolejny rekord, a Państwo pomogą go pobić?

SZANOWNI PAŃSTWO! WSZYSTKO W WASZYCH RĘKACH

Paulina Rezmer

Głównym zadaniem mediów jest informowanie o bieżących wydarzeniach. Państwo jako dziennikarze wiedzą to przecież doskonale, ale być może nie wiedzą Państwo, z jakim rozmachem i częstotliwością informują odbiorców swoich treści o zagrożeniach w sieci opartych tylko na jednym z patentów – „na OLX".

Przyznam się szczerze – kolekcjonuję oryginalne tytuły artykułów, w których piszą Państwo o (nie)bezpieczeństwie w sieci. Moje top trzy z poprzedniego roku to:

- *Gorzowianka chciała sprzedać buty. Padła ofiarą oszustwa „na OLX" i straciła 50 tys. zł* autorstwa Anny Kluwak z portalu gorzowianin.com (23.02.2021),
- *Na zastrzyk, na parawan, czy na okazję w sieci. Oto najnowsze metody złodziei* Andrzeja Zwolińskiego z „Gazety Wrocławskiej" (22.07.2021),
- wreszcie absolutny zwycięzca, redaktor Marcin Długosz z Inn:Poland, autor tekstu *Polka straciła pół miliona złotych. Myślała, że płaci na leczenie Clinta Eastwooda* (4.02.2021).

To trzy subiektywnie wybrane, abstrakcyjne nagłówki spośród ponad trzech tysięcy tekstów, jakie w ubiegłym roku napisali Państwo, by ostrzec swoich odbiorców przed działaniami cyberprzestępców, a w których pojawił się wątek OLX-a. Byłyby one nawet zabawne, gdyby nie prawdziwe historie i los poszkodowanych bohaterów, którzy się za nimi kryją.

Pisanie o oszustwach w sieci jest jak pisanie o grypie w sezonie jesiennym albo o kleszczach w sezonie letnim. Nigdy się nie kończy. Z tą różnicą, że grypa i kleszcze są dużo starsze niż phishing.

Tylko w okresie od początku kwietnia do końca września 2021 r. opublikowali Państwo dokładnie 1651 informacji, artykułów, wzmianek i notek o phishingu i innych przekrętach „na OLX". Media, na łamach których najczęściej gościły historie osób poszkodowanych przez cyberoszustów, to media lokalne. To całkowicie zrozumiałe, biorąc pod uwagę fakt, że są one najbliżej codziennych problemów swoich czytelników, słuchaczy, widzów.

Według szacunków firmy Press Service Monitoring Mediów te 1651 tekstów dotarło do 33 mln odbiorców. Proszę sobie wyobrazić, jaką mieliby Państwo siłę sprawczą, gdyby każdy z konsumentów tych treści wziął sobie do serca i wcielił w życie tak skrupulatnie spisywane przez Państwa rady i przestrogi.

O JEDEN KLIK ZA DALEKO. JAK NIE DAĆ SIĘ WPLĄTAĆ W SIEĆ OSZUSTW

Aleksandra Wróbel

„Witam. Ogłoszenie nadal aktualne? Mogę zapłacić dzisiaj w tedy jutro kurier przyjedzie jutro?" (pisownia oryginalna). Oczywiście chwilę później pojawia się link, a cała korespondencja odbywa się na WhatsAppie. Tak oszuści próbują wyłudzić dane, a następnie wykorzystać je do kolejnych przestępstw.

Phishing to oszustwo polegające na podszywaniu się pod osoby, firmy czy instytucje – zwłaszcza te cieszące się zaufaniem publicznym – w celu wyłudzenia danych, np. loginu i hasła do konta bankowego, numeru karty płatniczej, numeru CVV karty, numeru dowodu osobistego, numeru PESEL. Wszystkie te informacje mogą być wykorzystane w oszustwach i służyć do kradzieży tożsamości oraz pieniędzy.

Jak działa phishing?

Oszuści mogą podszywać się np. pod firmy kurierskie, banki, urzędy, operatorów płatności czy pod strony serwisów ogłoszeniowych, jak OLX. Robią to w celu wyłudzenia poufnych informacji. Komunikaty mogą dotyczyć przesyłki, pomocy technicznej, rzekomego zdezaktywowania konta i konieczności jego reaktywowania przez link znajdujący się w e-mailu albo są przekierowaniem do fałszywej strony. W momencie, w którym po kliknięciu w link wpiszemy dane na fałszywej stronie, nieświadomie udostępniamy je oszustom. Dzięki temu mogą oni dostać się do konta i np. ukraść pieniądze albo zdobyć więcej poufnych informacji i zaciągnąć kredyt. Wiadomości i strony, które tworzą oszuści, często są bardzo podobne do tych prawdziwych, dlatego tak ważne jest zwracanie uwagi na to, w co klikamy.

Rodzaje phishingu

Oszuści, podszywając się pod firmy czy instytucje, korzystają z różnych kanałów dotarcia do swoich potencjalnych ofiar. Wysyłają wiadomości e-mailowe z fałszywymi linkami, w których nakłaniają do kliknięcia w celu np. uregulowania zaległości, śledzenia zamówionej przesyłki czy dokonania opłaty za zamówiony przedmiot. Kontaktują się również za pośrednictwem komunikatorów, takich jak WhatsApp czy Messenger. Udając zainteresowanie kupnem przedmiotu, wysyłają linki z fałszywymi instrukcjami dotyczącymi przesyłki czy płatności. Wszystko po to, by nieświadoma osoba wpisała swoje dane, które następnie przestępcy mogliby ukraść i wykorzystać. Inną próbą wyłudzenia danych jest podszywanie się pod firmy czy instytucje w rozmowie telefonicznej. Dzwoniący oszust nakłania do podania naszych danych, numeru karty płatniczej czy danych do logowania.

OLX przestrzega przed oszustami

By podstępnie uzyskać dane z karty bankowej, oszuści będą przekonywać, że już zapłacili za przedmiot, proszą jedynie o wpisanie danych w formularzu, do którego wyślą link. Przesyłki OLX tak nie działają – OLX nie generuje takich linków. Osoba sprzedająca w serwisie nie musi nigdzie dodatkowo podawać danych karty bankowej do odebrania płatności za sprzedany przedmiot. Wystarczą dane, które podała na swoim koncie OLX. Podczas akceptacji pierwszej oferty kupna przez Przesyłki OLX serwis prosi o podanie numeru konta bankowego – na ten właśnie rachunek przelewane są pieniądze po odbiorze przesyłki przez kupującego.

Kilka wskazówek od serwisu, jak nie dać się nabrać na fałszywe wiadomości:

1. Dla pewności warto skopiować otrzymany link i wkleić go w sprawdzaczu linków (ang. *link checker*), który znajduje się na stronie OLX w zakładce Centrum pomocy. Jeśli link podświetli się na czerwono – oznacza to, że jest fałszywy.
2. Oszuści tworzą wiele instrukcji – zarówno w formie obrazków, jak i filmów wideo. Jedyne prawdziwe instrukcje na ten temat znajdują się na stronie przesylki.olx.pl oraz w Centrum pomocy OLX.
3. Wyłudzacze zawsze dążą do przeniesienia wymiany wiadomości poza OLX – najczęściej przez komunikator WhatsApp. Osoba sprzedająca w serwisie i korzystająca z opcji Przesyłki OLX powinna używać do kontaktu jedynie strony lub aplikacji OLX. Jeśli w ogłoszeniu nie ma podanego numeru telefonu, oszuści próbują kontaktować się, wysyłając e-maile z fałszywym komunikatem, np. o błędzie technicznym na OLX.
4. Oszuści próbują również podszywać się pod OLX poprzez fałszywe e-maile (niekoniecznie związane z Przesyłkami OLX, mogą to być też informacje np. o tymczasowym zawieszeniu konta czy nagrodach od administracji OLX) i SMS-y. Taka wiadomość może na pierwszy rzut oka wyglądać, jakby faktycznie została wysłana przez OLX. Należy pamiętać, że wszelkie SMS-y o rzekomej rezerwacji przedmiotu na OLX czy z linkiem do odebrania środków są nieprawdziwe. OLX nigdy nie wysyła wiadomości przez WhatsApp!
5. Przestępcy próbują też innych metod – takich jak telefoniczne podszywanie się pod pracowników banków lub OLX. Proszą wówczas o zainstalowanie aktualizacji do aplikacji OLX. Aktualizację aplikacji można pobrać jedynie z Google Play oraz Apple App Store.
6. OLX przestrzega również przed fałszywymi wiadomościami SMS, w których oszuści podszywają się pod partnerów, np. InPost, firmy kurierskie, banki czy inne serwisy sprzedażowe.

Jak chronić się przed phishingiem?

Zawsze należy sprawdzić, od kogo pochodzi wiadomość – nazwę nadawcy zarówno w przypadku wiadomości e-mail, jak i wiadomości SMS lub wysyłanych w komunikatorach można dowolnie zmodyfikować (i w ten sposób podszyć się pod prawdziwą firmę czy instytucję). Czytając wiadomość, warto zastanowić się, czy jest to standardowa forma komunikacji danej firmy i czy zwykle kontaktuje się ona właśnie tą drogą. Przykładowo, jeśli nasz dostawca prądu zawsze wysyła nam papierowe faktury, czy jest możliwe, by skontaktował się z nami za pośrednictwem SMS-a?

Jeśli wiadomość nie jest napisana poprawną polszczyzną, zawiera literówki czy inne błędy, najprawdopodobniej nie jest autentyczna. Jeżeli komunikat sprawia wrażenie wywierania presji, nakłaniania do kliknięcia w podany link, bo inaczej oferta przepadnie albo nasze konto zostanie zablokowane – należy się spokojnie zastanowić i w razie wątpliwości zaprzestać działań na stronie.

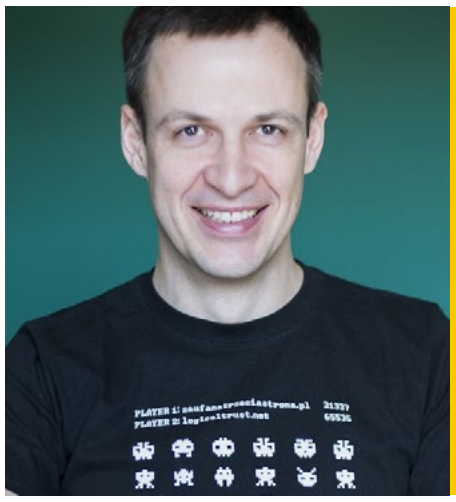
W serwisie OLX rozmowy należy prowadzić wyłącznie w ramach czatu na OLX – nigdy nie zgadzając się na przeniesienie negocjacji na e-mail, SMS czy zewnętrzne komunikatory. Warto pamiętać, że OLX nie generuje linków do opłacenia zakupu. Każda tego typu wiadomość poza serwisem, np. na WhatsAppie – to na pewno oszustwo!

Każdą próbę wyłudzenia danych lub nieprawidłowego zachowania należy zgłosić do OLX za pośrednictwem formularza kontaktowego.

W NUMERZE:

W INTERNECIE WSZYSCY MUSIMY BYĆ EKSPERTAMI

Internetowi naciągacze wymyślają wciąż nowe formy oszustw, ale jedno jest niezmienne. Ciągle liczą na to, że to my damy się nabrać. Adam Haertle, redaktor prowadzący i właściciel serwisu Zaufana-TrzeciaStrona.pl, wyjaśnia, jak wpadamy w pułapki oszustów.



Adam Haertle – ekspert bezpieczeństwa z 20-letnim doświadczeniem, a także prelegent, trener i wykładowca. Co roku prowadzi ponad 150 prelekcji dla grup otwartych i zamkniętych w całej Polsce poświęconych kwestiom: bezpieczeństwa w sieci, zagrożeń związanych z korzystaniem z bankowości elektronicznej, prywatności oraz ochrony informacji w przedsiębiorstwie. W swoich prezentacjach przystępnym językiem i na prawdziwych przykładach opisuje realne zagrożenia czyhające na firmy i użytkowników. Z sukcesem szkolił zarówno zarządy największych polskich przedsiębiorstw, jak i pracowników setek firm i instytucji w całym kraju.

Dlaczego wciąż dajemy się złapać na haczyk?

Nabieramy się wtedy, kiedy w coś wierzymy, kiedy chcemy, by było prawdziwe, np. kiedy wystawiamy przedmiot na sprzedaż, powiedzmy rowerek, z którego wyrosło nasze dziecko, i okazuje się, że już po 5 minutach mamy chętnego. Jaka jest nasza pierwsza reakcja?

Radość.

Dokładnie tak. W końcu celem naszego działania było wzbudzenie zainteresowania kupującego! Jeśli na dokładkę ten kupujący nie negocjuje ceny, nie zadaje dodatkowych pytań, np. o to, czy rowerek ma jakieś uszkodzenia, w dodatku od ręki deklaruje gotowość do płatności z wykorzystaniem jakiegoś mechanizmu wysyłki lub wręcz utwierdza nas w przekonaniu, że on już zrobił przelew…

Jak to zrobił przelew? Gdzie?

Ano właśnie! I tu zaczyna się problem, bo my, sprzedając rzeczony rowerek, uradowani faktem, że lada moment uda nam się pozbyć z domu zbędnego już przedmiotu, właśnie w tym miejscu słyszymy czy też czytamy w wiadomości od kupującego, że wystarczy kliknąć w wysłany link, podać dane karty płatniczej i po chwili przepisać kod z SMS-a od banku, a środki trafią na nasze konto.

I co? Rowerek sprzedany?

Rowerek ciągle zalega w garażu, ale za to z konta znikają nasze pieniądze. Użytkownik, który nie wie, jak działają mechanizmy zakupów online czy bankowości, właśnie powiązał swoją kartę i konto z elektronicznym portfelem złodzieja. A ten zaczyna ochoczo wydawać pieniądze bez zgody i wiedzy prawowitego posiadacza konta czy karty.

Czyli mamy kolejnego nabranego, okradzionego internautę, który dał się złapać, bo…

…bo przestępcy doskonale wiedzą, że się spieszymy. Przecież chodzi „tylko" o rowerek. Więc rzucamy szybko okiem, czy strona jest podobna do tej, którą znamy, czy kwota się zgadza. To naszemu mózgowi wystarczy, by zgodzić się na podanie danych do logowania. Na pierwszy rzut oka wszystko gra.

Po czym się zorientować, że nie jesteśmy na właściwej stronie? Przecież te linki wyglądają bardzo autentycznie.

Same linki nie. Jeżeli tak naprawdę dobrze przyjrzymy się takiemu linkowi, zobaczymy, że wygląda on zupełnie inaczej niż ten prawdziwy. Prawdziwy, np. jeśli chodzi o serwis OLX, będzie OLX.PL. I tyle. A fałszywe to np. olx-pl.club albo olx-pl.info, albo 0lx-id-035789.com. Takie domeny były używane przez przestępców. Zmieniają się one nawet kilka razy dziennie. Te adresy są jedynie nieco podobne do prawdziwego, więc gdybyśmy poświęcili chwilę na sprawdzenie, na jaką stronę prowadzi ten link i gdzie za nim „idziemy", można by było uniknąć wielu przykrych sytuacji.

W takim razie jak szybko stać się ekspertem?

Najprostszym i najtańszym sposobem jest czytanie informacji, które przesyłają nam banki i serwisy poświęcone bezpieczeństwu, a także aplikacje, z których korzystamy. Przykładowo w aplikacjach bankowych albo na stronach widnieje sekcja „Aktualne ostrzeżenia". Wchodząc na stronę banku, mamy cel, najczęściej wykonać przelew. Ale warto poświęcić minutę, dwie na zaktualizowanie naszej bazy wiedzy. Dodatkowo – uważnie przejrzeć to, co pojawia się w pasku adresu. Jeśli chcemy być na stronie swojego banku, sprawdźmy, czy w pasku adresu pojawia się nazwa naszego banku i nic więcej.

Czyli starsi, sprzed epoki internetu, muszą się uczyć… A co z młodszymi?

Co ciekawe, są statystyki mówiące o tym, że osoby 60+ są mniej podatne na oszustwa komputerowe. Być może po części wynika to z faktu, że rzadziej korzystają z urządzeń elektronicznych, np. do transakcji bankowych. Ale tak naprawdę to osoby, których życie trochę zwalnia, mają więc więcej czasu i mogą dołożyć większych starań do tego, co robią. Chcą zobaczyć, przeczytać, jak coś działa na spokojnie. To pozwala im przyjrzeć się detalom i często zrobić krok wstecz w sytuacji, w której coś ich zaniepokoi. A młodzi czują się w internecie pewnie. Może czasem zbyt pewnie. To dobrze, że biegle posługują się internetowymi narzędziami, ale czasem, robiąc coś odruchowo, w pośpiechu, narażają się na potknięcia.

Czyli wniosek z tego taki, że musimy się uczyć i zachować zimną krew.

Tak. Każdy, kto chce korzystać z internetu, powinien zdawać sobie sprawę z tego, jakie są dwa, trzy bieżące, najbardziej aktualne zagrożenia. Warto tę wiedzę aktualizować, powiedzmy raz na miesiąc. To powinno wystarczyć.

Rozmowę przeprowadziła Anna Stachowska, zredagowała Paulina Rezmer

Rozmowę przeprowadzono w ramach cyklu podcastów FRAUDycja. Cykl powstał we współpracy z Radiem Złote Przeboje. Pozostałej części rozmowy oraz innych odcinków z cyklu można posłuchać pod linkiem z kodu QR.

„BABCIU? TO JA, NIE POZNAJESZ?!"

PATENT NA WNUCZKA NIE PRZEJDZIE

Jolanta Kikiewicz

Według danych Komendy Głównej Policji w 2020 r. seniorzy padli ofiarą wyłudzeń opiewających na łączną kwotę prawie 86 mln zł*. Już w samym pierwszym półroczu 2021 r. wyłudzono 63 mln zł. Oszuści tworzą coraz bardziej skuteczne techniki kradzieży i grają na emocjach ofiary. W jaki sposób uchronić się przed ich atakiem?

Kogo udaje oszust? Najczęściej podszywa się pod:

- Wnuczka – lub inną bliską osobę z rodziny. Oszust zadaje skołowanej osobie pytanie: „Jak to, babciu, nie pamiętasz mnie?" lub: „Dziadku! Zgadnij, kto dzwoni?". Ofiara już na początku zdradza imię bliskiej osoby, a naciągacz wykorzystuje to do dalszego wyłudzania informacji. Twierdzi, że sam padł ofiarą oszustwa i potrzebuje pieniędzy.
- Policjanta lub funkcjonariusza CBŚ – status funkcjonariusza państwowego budzi respekt, który wykorzystują oszuści. Twierdzi, że pieniądze są niezbędne do ukończenia postępowania, a senior został wybrany do włączenia się w śledztwo i może bohatersko pomóc służbom państwowym.
- Instytucję zaufania publicznego – w okresie pandemii oszuści podszywają się pod sanepid lub Ministerstwo Zdrowia. Próbują wyłudzić pieniądze za szczepienia. Trzeba pamiętać, że przyjęcie szczepionki nie wymaga uiszczania dodatkowych opłat. Polska Policja ostrzega*, że oszuści mogą podszywać się pod pracowników NFZ lub Ministerstwa Zdrowia, żądając dodatkowej opłaty za dopuszczenie do szczepienia lub organizację szczepienia w domu.
- Pracownika banku – oszuści hakują numer telefoniczny banku (spoofing) i podają się za jego przedstawiciela. Informują seniora o próbie włamania na konto lub o konieczności zwiększenia ochrony konta klienta. Wymuszają ściągnięcie specjalnej aplikacji lub kliknięcie w link, który pozwala oszustom na instalację złośliwego oprogramowania.

Są seniorzy, którzy nie dają się nabrać naciągaczom. I warto wziąć z nich przykład! W grudniu 2021 r. dziennikarz Grzegorz Pilecki z Kalisza opublikował nagranie rozmowy z oszustami, którzy chcieli wyłudzić telefonicznie aż 50 tys. zł. Oszustka podawała się za wnuczkę Pileckiego i prosiła o wypłatę pieniędzy, aby mieć poręczenie majątkowe. Twierdziła, że potrąciła na pasach kobietę i grozi jej aresztowanie. Po „wnuczce" do rozmowy wtrącił się „policjant", który potwierdził jej słowa. Oszuści nie wiedzieli jednak, że trafili na dziennikarza – nie spodziewali się, że Pilecki będzie doskonale znał detale dotyczące Kalisza i nagra rozmowę ku przestrodze innych seniorów oraz jako dowód we własnej sprawie, którą następnie zgłosił służbom. Nagranie można odsłuchać na YouTubie.

Metoda na wnuczka – nie tylko przez telefon i internet

Według raportu aż 80 proc. osób powyżej 65. roku życia korzystających z internetu deklaruje, że używa wirtualnych lub telefonicznych narzędzi do zarządzania finansami. Manipulatorzy mają tego świadomość i żądają wykonania przelewu lub podania danych przez telefon, twierdząc, że na spotkaniu nie mogą pojawić się osobiście.

O czym trzeba pamiętać, by ochronić się przed naciągaczami? Oto kilka zasad, które warto przypomnieć seniorom:

- **Zasada ograniczonego zaufania** – nie należy ufać rozmówcy tylko dlatego, że przedstawia się jako wnuk czy inna bliska osoba. Warto skonsultować podejrzaną rozmowę z innymi członkami rodziny, np. rozłączyć się i oddzwonić na numer prawdziwego wnuka, bądź skontaktować się z policją.
- **Zasady funkcjonowania instytucji państwowych** – policja nigdy nie prosi osób cywilnych o wsparcie finansowe w poszukiwaniu przestępców ani nie udziela szczegółowych informacji o prowadzonych śledztwach.
- **Zasada nieulegania manipulacji** – fałszerze stosują różne techniki manipulacji. Najczęściej odwracają role, podając się za ofiarę, która potrzebuje pieniędzy. Policja zaleca, aby zachować wzmożoną czujność.
- **Zwracanie uwagi na treść SMS-ów i e-maili** – oszuści często wysyłają wiadomości z fałszywymi linkami. Wyglądają one nieco inaczej niż autentyczny adres strony, np. litera „o" jest zastąpiona przez zero.

Jeżeli senior padł już ofiarą oszustwa „na wnuczka" lub ktoś próbował go oszukać w taki sposób, należy zgłosić zdarzenie policji pod numerem 997 lub numerem alarmowym 112.

*Raport ZBP „Infosenior 2020".

ZARAZ BĘDZIESZ BOGATY

Zuzanna Pawłowska

Inwestorzy, uchodźcy polityczni, urzędnicy, dzielni żołnierze, zamożne wdowy z USA... wszyscy pragną obdarzyć nas niezwykłym majątkiem. O ile jednak w latach 90. XX w. e-maile cyberoszustów brzmiały topornie i bez sensu, o tyle dzisiaj nigeryjski przekręt potrafi przybrać przekonującą formę.

„Nazywam się Pani Theresa Gross ze Stanów Zjednoczonych Ameryki. Jestem żonaty z panem Anthonym Grossem, który kiedyś pracował w naszej ambasadzie w Niemczech w 2002 roku, a także pracował przez 16 lat w ambasadzie w Londynie, zanim zmarł. Byliśmy małżeństwem przez 25 lat bez dziecka. Od jego śmierci postanowiłem nie wychodzić za mąż z powodu moich przekonań religijnych. Kiedy mój zmarły mąż żył, zdeponował sumę 10.500.000.00 dolarów (dziesięć milionów pięćset tysięcy dolarów amerykańskich) w banku tutaj w Ameryce. [...] Chcę, żebyście wykorzystali te pieniądze na kościoły, organizacje charytatywne, sierocińce, wdowy i inne osoby w potrzebie. Podjąłem tę decyzję, bo nie mam dziecka, które odziedziczy te pieniądze. Co więcej, krewni mojego męża nie są ze mną blisko, ponieważ zachorowałam na raka, a ich życzeniem było widzieć mnie martwą, aby odziedziczyć jego majątek, ponieważ nie mamy Dziecka. Ci ludzie nie są godni tego dziedzictwa. Dlatego podejmuję decyzję o skontaktowaniu się z Wami i przekazaniu Wam tego funduszu na cele charytatywne [...]".

Zaczyna się niewinnie

Media obiegają zwykle spektakularne historie. Głośno było np. o e-mailach z prośbą o pomoc w uratowaniu pierwszego nigeryjskiego astronauty, który utknął na radzieckiej stacji kosmicznej. Doktor Bakare Tunde z National Space Research and Development Agency wtajemniczał w zawiłą i dramatyczną historię, tłumacząc, dlaczego to od naszego finansowego wsparcia zależą losy Nigeryjczyka. W zamian za pomoc obiecany był pokaźny procent z kilkunastomilionowego wynagrodzenia astronauty.

Myśląc o internetowych oszustwach, spodziewamy się albo równie absurdalnej historii, albo przynajmniej wiadomości pisanych bardzo pokraczną, momentami niezrozumiałą polszczyzną. Problem w tym, że obecnie często kontaktują się z nami oszuści pokroju pani Theresy – piszą całkiem składnie, interpunkcji pozazdrościć by mógł im niejeden Polak, a i cała ich opowieść raczej wzruszy, niż rozśmieszy.

Uwaga, to nigeryjski przekręt

Polega na wyłudzeniu pieniędzy od przypadkowej lub celowo wybranej osoby. Proceder różni się jednak od zwykłej kradzieży całą oprawą. Oszust nawiązuje z ofiarą kontakt e-mailowy albo rozpoczyna rozmowę na serwisach ogłoszeniowych i wciąga ją w fikcyjną, czasem niezwykle zawiłą historię. W latach 90. XX w. oszuści pisali najczęściej z kafejek internetowych w Nigerii, ale dziś kontaktują się z nami z różnych krajów (także z Polski).

W klasycznym nigeryjskim przekręcie pada obietnica przesłania ofierze pokaźnej kwoty – nawet kilkunastu milionów dolarów – w zamian za drobną, finansową pomoc. Przykładowo zaczyna się od prośby o przelanie pieniędzy, aby nasz „dobroczyńca" mógł wyrobić odpowiednie certyfikaty niezbędne do przekazania nam obiecanych milionów lub opłacić usługi prawne. Prośby są oczywiście uzasadniane (np. „to standardowa procedura"), a jeśli oszust widzi w nas potencjał, to na jednej nigdy się nie kończy. Kiedy przelejemy zadowalającą go kwotę, znika bez śladu razem z całym niesłychanym bogactwem, które już z uśmiechem trwoniliśmy w myślach.

> **Nabieramy się tak przynajmniej od... 500 lat**

Obietnicą nie zawsze musi być przekaz milionów. Niekiedy to kusząca oferta sprzedaży egzotycznych zwierząt, elektroniki, samochodów, czasami niezwykła okazja wynajmu mieszkania. Punktami wspólnymi nigeryjskich oszustw są przekonanie ofiary wymyśloną historią (bywa, że dość prawdopodobną) i sprowokowanie jej, aby z własnej woli przekazywała przestępcy pieniądze.

50 twarzy oszusta

Jego wyobraźnia nie zna granic. Bywa uchodźcą politycznym lub dziedzicem fortuny zgromadzonej przez przywódcę któregoś z państw afrykańskich obalonego w trakcie przewrotu politycznego – mamy wtedy mu pomóc w odzyskaniu majątku w zamian za pokaźny procent. Czasem jest młodym, wykształconym prawnikiem, którego ojciec chciałby korzystnie zainwestować swój ogromny majątek. Czasem udaje pracownika banku – informuje ofiarę, że jeden z klientów zmarł i zostawił po sobie konto z wielką sumą pieniędzy, ale nie ma rodziny i nie wskazał wcześniej spadkobierców. Bank szuka więc teraz osoby, która przejąłby majątek przed rychłą likwidacją konta.

Powszechnym scenariuszem są historie spadkowe. Oszust przekonuje, że jesteśmy jedynymi krewnymi pewnej bogatej osoby, która mieszkała za granicą i zginęła w tragicznym wypadku. Ogromny spadek trafi w nasze ręce, jak tylko uiścimy konieczne opłaty.

Równie często na nasze skrzynki e-mailowe trafiają wiadomości o wygranych w loteriach. Otrzymujemy sfałszowane certyfikaty i dokumenty poświadczające istnienie danego konkursu. Przelew za moment trafi na nasze konto, ale przed nami jeszcze kilka „niezbędnych, standardowych formalności": opłata za wystawienie wewnętrznych dokumentów banku, częściowe pokrycie kosztów usług prawnych, uregulowanie podatku od wzbogacenia...

Wszystkie te historie łączy jedno – są tak nieprawdopodobne, że po prostu nie mogą być prawdziwe. Dlaczego więc wciąż wpadamy w nigeryjskie pułapki?

(Nie)wyrafinowany szwindel – na co uważać?

Cyberoszuści wykorzystują naszą ufność, chęć pomocy, ale też próżność i pragnienie szybkiego zarobku. Jeśli dodatkowo dotknęła nas trudna sytuacja życiowa, a emocje zaczynają brać górę, stajemy się idealnym celem. Kiedy zachować czujność?

1. Korespondujemy ze sprzedawcą na serwisie ogłoszeniowym, a on proponuje przenieść kontakt poza portal (sugeruje komunikatory typu WhatsApp lub wymianę e-mailową).
2. Otrzymane wiadomości brzmią podejrzanie – pisane są łamaną polszczyzną, jakby z translatora, i rozpoczynają się w nietypowy sposób, np.: „Uwaga", „Witaj mój ukochany", "Witam, aukcja działa idealnie?".
3. Odbiorcami e-maila są „undisclosed-recipients", a adres rzekomych instytucji państwowych czy finansowych nie ma domeny firmowej, tylko np. Gmail lub Yahoo.
4. Nieznajomy nadawca przekonuje nas, że braliśmy udział w wydarzeniach, o których nie mamy pojęcia (aukcje, loterie), lub mamy krewnych, których istnienia nie podejrzewaliśmy.
5. Akurat nas wybrano do pomocy uchodźcom politycznym, do współpracy z zamożnymi inwestorami czy do przejęcia majątku po nieznajomym zmarłym...
6. Warunkiem kupna towaru lub otrzymania nagrody/spadku/udziału jest dokonanie dodatkowych opłat manipulacyjnych.
7. Otrzymujemy dokumenty potwierdzające historię naszego rozmówcy. Pamiętajmy, że ważne certyfikaty są zabezpieczane tak jak dokumenty identyfikacyjne, papiery wartościowe czy banknoty (np. hologramami, recto-verso, mikrodrukiem). Te wszystkie zabezpieczenia tracą swoje właściwości podczas digitalizacji obrazu, a zatem przesłane w formie cyfrowej nie mają żadnej wagi prawnej!

Nabieramy się tak przynajmniej od... 500 lat

Sama idea nigeryjskiego przekrętu nie jest nowa. Znamy historie sięgające XVI w., kiedy to okradano zamożnych metodą na „hiszpańskiego więźnia". Ofiarę zachęcano w listownej korespondencji do wydania pewnej sumy pieniędzy, aby otrzymać kuszącą nagrodę. Metoda oszustów uderzała w czułe punkty (zawsze chodziło o pomoc niesprawiedliwie osądzonemu, szlachetnemu człowiekowi), uwodziła rozmachem i romantyzmem. W dowód wdzięczności za pożyczkę „więzień" często obiecywał bowiem rękę swojej pięknej córki.

Stare schematy operują jedynie coraz nowszymi narzędziami. Dzięki internetowi i botom nigeryjskie przekręty rozwijają się na niespotykaną dotąd skalę, a przestępcy są właściwie nie do zidentyfikowania. W obliczu takich oszustw najpewniejszą ochroną pozostaje nasza czujność.

OFERTY ZBYT PIĘKNE, ABY BYŁY PRAWDZIWE

Aleksandra Wróbel

Cyberprzestępcy są coraz sprytniejsi, ale użytkownicy także mają coraz większą wiedzę na temat tego, jak poruszać się w sieci – kiedy nie klikać, z kim nie rozmawiać, jak bezpiecznie robić zakupy. Dobrych wskazówek nigdy jednak dość, ponieważ bezczelność oszustów nie zna granic: potrafią klientom sprzedawać laptopy, a wysyłać... cegły.

Przestępcy próbują swoich tricków na różnych stronach, m.in. na OLX, a częściej na stronach udających OLX. Serwis ogłoszeniowy, mając na uwadze bezpieczeństwo swoich użytkowników, przygotował wskazówki, które pomogą uchronić się przed oszustwem.

Poradnik bezpieczeństwa OLX

1. Bądź ostrożny w przypadku ofert, które są podejrzanie atrakcyjne, np. gdy ktoś oferuje do sprzedaży nowy telefon za 200 zł.
2. Prowadź rozmowy w ramach czatu OLX.
3. Nie klikaj w żadne zewnętrzne linki umożliwiające płatność.
4. Gdy to możliwe, korzystaj z wysyłki za pobraniem lub Przesyłek OLX. W razie odbioru osobistego zachowaj odpowiednie środki ostrożności.
5. Używaj przycisku „Kup z Przesyłką" tylko na stronie ogłoszenia umieszczonego na olx.pl.
6. Jeśli to możliwe, sprawdź stan produktu przy odbiorze.

Na co zwrócić szczególną uwagę?

Fałszywe potwierdzenia

Zachowaj ostrożność, gdy kupujący nalega na natychmiastową wysyłkę i dla uwiarygodnienia przelewu przesyła potwierdzenie. Najlepiej poczekaj, aż przelew pojawi się na twoim koncie.

Przesyłki za granicę

Prośby o wysyłkę przedmiotu za granicę pojawiają się najczęściej w wiadomościach tłumaczonych przez internetowy translator. Nie odpisuj na takie wiadomości.

Przelewy weryfikacyjne

Prośba o niewielki przelew, który ma zweryfikować twoją tożsamość, to najczęściej oszustwo. Zgłoś nam takie sytuacje.

Kiedy zachowanie sprzedającego może budzić wątpliwości?

Sprzedający poprosił o wpłatę z góry. Wpłata pieniędzy z góry poza płatnościami podczas korzytania z Przesyłek OLX zawsze obarczona jest sporym ryzykiem. Może się tak zdarzyć nie tylko przy kupnie przedmiotu, lecz także przy opłacie za usługi oraz gdy osoba sprzedająca prosi o zapłatę za przesyłkę darmowego przedmiotu. Jeśli już decydujesz się na przelew poza płatnościami OLX, sprawdź w internecie, czy podany numer konta bankowego nie był wykorzystywany w nieuczciwych celach. Nigdy nie wysyłaj pieniędzy za granicę! Bądź czujny, kiedy sprzedający poprosi o przelew ekspresowy lub dokonanie płatności z użyciem BLIK-a.

Sprzedający poprosił o wpłatę zaliczki. Prośba o zaliczkę za przedmiot lub usługę również niesie za sobą duże ryzyko utraty pieniędzy. Ponadto zdarza się, że sprzedający chce po prostu dokonać zakupów na twój koszt. Jak to działa? Sprzedający przekazuje dane do przelewu, które służą do zapłaty za przedmiot kupiony przez niego, np. w sklepie internetowym. Należy zwrócić uwagę na tytuł przelewu oraz numer konta bankowego, jakie przesłała osoba sprzedająca.

Sprzedający wysłał podejrzany skan nadania przesyłki. Kiedy sprzedający zapewnia, że wysłał już przedmiot i po krótkim czasie otrzymujesz skan potwierdzenia nadania paczki – uważaj! Przyjrzyj się dokładnie otrzymanemu dokumentowi. Twoją uwagę powinny zwrócić wszelkie zmiany na dokumencie: poprawianie pisma, aby było czytelne, wypełnienie potwierdzenia ołówkiem, ślady po wymazywaniu, zasłanianie części danych (więcej o takich praktykach piszemy na stronie 7).

Sprzedający pisze łamaną polszczyzną, z błędami (szczegółowo piszemy o tym na stronie 14). W takich sytuacjach zwróć uwagę na staż ogłoszeniodawcy w OLX – najczęściej jest to nowe konto, sprzedawane przedmioty są wycenione poniżej wartości rynkowej, a zdjęcia w ofercie pochodzą z internetu. Często takim ogłoszeniodawcom zależy na przeniesieniu kontaktu poza serwis OLX z uwagi na większą swobodę komunikacji i możliwość ominięcia mechanizmów zabezpieczających w serwisie.

Na co zwrócić szczególną uwagę?

Superokazja

Zachowaj czujność, jeśli ktoś sprzedaje przedmiot o dużej wartości w wyjątkowo niskiej cenie. Zwłaszcza jeśli sprzedający sugeruje, by najpierw przelać pieniądze na jego konto.

Zdjęcia z internetu

Oferty ze zdjęciami z internetu (np. z oficjalnych stron producenta) mogą wprowadzać w błąd. Takie fotografie często nie oddają faktycznego stanu przedmiotu, a zdarza się, że sprzedający nawet go nie posiada.

Phishing

Nie klikaj w linki (np. dotyczące płatności, przesyłki czy zamówienia kuriera), które wyśle ci sprzedający poza czatem OLX, np. przez komunikator WhatsApp. Może być to oszust próbujący uzyskać twoje dane i hasło do konta bankowego!

Kiedy zachowanie kupującego może budzić wątpliwości?

Kupujący prosi o niezwłoczne dostarczenie towaru i przesyła potwierdzenie przelewu. Czujność powinna wzbudzić sytuacja, w której kupujący naciska na natychmiastową przesyłkę, tłumacząc to tym, że bardzo zależy mu na czasie. Bardzo często załączone wówczas potwierdzenie przelewu jest sfałszowane. Warto czekać z wysyłką, aż przelew dotrze na twoje konto.

Kupujący pisze łamaną polszczyzną i prosi o wysyłkę za granicę. Wiadomość napisana niepoprawnie, z błędami, może wiązać się z próbą wyłudzenia przedmiotu. Kupujący stara się przekierować komunikację poza serwis OLX (np. rozpoczyna rozmowę przez SMS-y lub na WhatsAppie), a następnie proponuje zakup w bardzo korzystnej cenie, by nakłonić sprzedającego do wysyłki przedmiotu za granicę. Często przedstawia później sfałszowany dowód zapłaty, oczekując szybkiej przesyłki towaru.

Kupujący prosi o uwiarygodnienie przez dokonanie przelewu. Może to być oszustwo na tzw. słupa. Mechanizm jest następujący: kupujący prosi, aby sprzedający uwiarygodnił się przelewem na drobną kwotę, np. 50 gr na wskazane konto bankowe. W ten sposób sprzedający nieświadomie potwierdza swoje dane na koncie używanym przez osobę, która poprosiła o przelew. Takie konta najczęściej używane są w nieuczciwych celach. Przelewy weryfikacyjne na mniejsze kwoty także z reguły są oszustwem — mogą potwierdzać dane przy zakładaniu konta bankowego przez internet lub przy braniu pożyczek.

10 PRZYKAZAŃ BEZPIECZNEGO INTERNAUTY

1. Stosuj silne hasła dostępu do kont bankowych, poczty: użyj kombinacji dużych i małych liter, cyfr i znaków specjalnych, o długości powyżej 8 znaków. Hasłem nie powinny być twoje dane, takie jak: imię, nazwisko, pseudonim, data urodzenia dzieci.
2. Nie udostępniaj „sąsiadom" swojego Wi-Fi.
3. Nie loguj się do banku, poczty, aplikacji, gdy korzystasz z publicznego Wi-Fi.
4. Jeżeli strona logowania do banku czy innej instytucji finansowej, na której logowanie jest koniecznie, nie zawiera w adresie strony protokołu HTTPS (tzw. kłódeczki), zgłoś to do banku, a przede wszystkim nie podawaj żadnych danych.
5. Aktualizuj na komputerze oprogramowanie antywirusowe kupione z legalnego źródła.
6. Nie otwieraj załączników i nie klikaj linków od nieznanych lub budzących wątpliwość nadawców.
7. Nie przesyłaj e-mailem danych osobistych.
8. Nie podawaj swoich danych do logowania osobom trzecim.
9. Robiąc zakupy w internecie, uważaj na wyjątkowe okazje i promocje oraz sprawdzaj opinie o sprzedawcy.
10. Nigdy nie działaj w sieci pospiesznie, pod presją czasu.

WIEMY, JAK OSZUKUJĄ – POZNAJ ICH PATENTY

Alicja Chwieduk

Padamy ofiarą nadużyć nie dlatego, że jesteśmy wyjątkowo naiwni. Wprawni złodzieje wykorzystują codzienne, zautomatyzowane nawyki. Żerują więc na tym wszystkim, co czyni nas po prostu „bardziej ludzkimi" – na podstawowym zaufaniu do innych i braku obsesyjnej samokontroli. Aby zdemaskować oszusta, trzeba najpierw nauczyć się jego języka. Jak się zachowuje? W którym momencie zaczyna kombinować? Co robi, aby szybko osiągnąć swój cel?

Zaczyna się banalnie – nawiązanie kontaktu, wypytanie o szczegóły, wielkie zainteresowanie naszą ofertą. Złodzieje wyspecjalizowani w phishingu podszywają się zarówno pod sprzedających, jak i kupujących, i zawsze sprawiają wrażenie przeciętnego użytkownika. W trakcie rozmowy dążą jednak do tego, aby przekierować nas na fałszywe strony internetowe (instytucji finansowych, pośredników lub nawet łudząco podobne do serwisu OLX). Samo kliknięcie w link nie musi jeszcze doprowadzić do tragedii. Jeśli jednak podamy na takiej stronie dane naszej karty, oszust natychmiast zyskuje dostęp do konta bankowego, a kontakt z nim nagle się urywa. Sztuka polega więc na zakończeniu rozmowy w odpowiednim momencie. Tylko kiedy zwyczajna wymiana zdań powinna wzbudzić czujność? Przyjrzyjmy się najpierw sprzedawcom-oszustom.

Unika spotkania i utrudnia odbiór przesyłki

Odbiór osobisty, przesyłka za pobraniem lub Przesyłka OLX to obecnie najpewniejsze sposoby finalizowania transakcji. Ostatnie rozwiązanie jest bezpieczne i wygodne dla obu stron. Sprzedający otrzymuje przelew na konto bankowe w ciągu trzech dni roboczych od momentu potwierdzenia przez kupującego, że zamówienie jest w porządku. Z kolei kupujący ma 24 godziny od odbioru paczki na potwierdzenie zgodności zamówienia. Dopiero po potwierdzeniu lub upływie tego czasu pieniądze trafią do sprzedającego.

Jeżeli sprzedający nie daje możliwości skorzystania z tych opcji, powinno nas to zastanowić. Trudności w odbiorze zwykle idą w parze z obszernymi wymówkami, nierzadko pełnymi osobistych dramatów czy nagłych wypadków. Oszuści wysyłają też fałszywe instrukcje, uzasadniając to tym, że właśnie takie wytyczne otrzymali z działu obsługi użytkownika. Ponadto możemy spotkać się z próbą oszustwa w następujący sposób:

- Zła lokalizacja – produkt wystawiono w jednej miejscowości, ale okazuje się, że jest do odbioru na drugim końcu kraju. Sprzedawca utrzymuje, że „to OLX źle ustawił lokalizację" lub sam niespodziewanie musiał wyjechać i zabrać przedmiot ze sobą. Proponuje nam więc płatność z góry, przelanie zaliczki pod pretekstem rezerwacji przedmiotu lub przyspieszenia jego wysyłki.
- Odbiór osobisty możliwy... ale nie do końca – sprzedawca ciągle nas zwodzi: jest dostępny tylko bardzo późno w nocy, przekłada terminy ze względu na pracę czy problemy rodzinne. W zamian szlachetnie proponuje jednak wysyłkę – oczywiście pod warunkiem, że zapłacimy z góry.

Wywiera presję

„Kto pierwszy, ten lepszy!", „Jest ogromne zainteresowanie!", „Ktoś już ma zrobić przelew!" – te i podobne sformułowania mają jeden cel – skusić nas atrakcyjną ofertą i sprawić, że zaczniemy działać w pośpiechu, a więc mniej uważnie. Trudno oprzeć się starej, dobrej regule niedostępności (zwłaszcza jeśli na czymś faktycznie nam zależy), ale każdy taki nacisk ze strony sprzedającego jest podejrzany.

Naleganie na dokonanie ekspresowej wpłaty także powinno nas zaniepokoić. Oszuści uwielbiają przelewy typu BLIK, paysafecard czy Elixir. Dwa pierwsze są dla nich wyjątkowo wygodne, ponieważ nie wymagają podania numeru konta. Złodzieje znikają naprawdę bez śladu. Za każdym razem, kiedy usłyszymy: „Po prostu potrzebuję pieniędzy na weekend, a zwykły przelew już nie dojdzie" – weźmy głęboki wdech i zastanówmy się, na ile ufamy tej osobie.

Usypia naszą czujność

Zachowuje się tak, jakby niczego nie miał do ukrycia. Wysyła nawet zdjęcie/skan „swojego" dowodu osobistego lub prawa jazdy i to z widocznymi wszystkimi danymi wrażliwymi. Problem w tym, że ta przesadna szczerość jest podejrzana (kto pokazuje obcej, przypadkowej osobie tak ważne dokumenty?). Najczęściej są one zresztą skradzione lub sfałszowane.

Oszust w rozmowie manipuluje i próbuje udowodnić, że nasze podejrzenia są absurdalne. „Przecież masz wszystkie moje dane. A zresztą nikt dla takich kwot nie robiłby sobie kłopotów. Jak kraść, to miliony". Nikt z nas nie chce wyjść na obsesyjnie podejrzliwego i mało bystrego klienta, więc po kilku – na pozór racjonalnych – uwagach często odpuszczamy. Nie dajmy się jednak tak szybko zbić z tropu. Sprawdzenie w internecie numeru rachunku, na który oszust chce otrzymać przelew (np. na stronach jakitobank.pl czy numerkonta.com), zajmuje tylko chwilę.

Podaje nietypowe dane do przelewu

Rozmowa ze sprzedającym nie wzbudziła naszej czujności, zgodziliśmy się na płatność z góry. Otrzymujemy jednak prośbę, aby przelew zrobić na konto operatora płatności, np. PayU czy DotPay, i to mimo że dobijamy targu z osobą prywatną. Lepiej powstrzymajmy się przed taką transakcją. Bądźmy też szczególnie ostrożni, jeśli w tytule przelewu mamy wpisać dość przypadkowy ciąg znaków, niezwiązany z naszym zamówieniem, a nazwą odbiorcy przelewu nie są imię i nazwisko. Oszust w ten sposób chce wyłudzić dane, które następnie wykorzystałby do innych przekrętów.

Jak oszukuje kupujący?

Nieuczciwy nabywca próbuje udowodnić nam, że dokonał wpłaty, po czym wymusza szybką przesyłkę. Niby widzimy na własne oczy, że żaden przelew nie dotarł, a jednak zakładamy, że druga strona ma rację i przekazujemy zamówienie. Jak to możliwe? Oszuści okłamują nas na kilka sposobów:

- wysyłają zrzut ekranu ze strony banku, ale bez widocznej daty zrealizowania przelewu – nie jest to potwierdzenie, to tylko dyspozycja, którą oszust anulował zaraz po zrobieniu zdjęcia,
- podrabiają potwierdzenie przelewu – sprawdźmy, czy plik nie ma błędów ortograficznych i/lub gramatycznych, czy dane wyglądają na wklejone (odbiorca, nadawca, kwota i data),
- podstawiają kurierów (gdy to kupujący zamawia kuriera, a ten okazuje się fałszywy),
- podrabiają etykiety – piszą do sprzedających, że chcą kupić oferowany przedmiot z wysyłką paczkomatem za pobraniem, ale żeby nie robić kłopotu sprzedającemu, deklarują, że sami na stronie InPostu wygenerują etykietę i ją opłacą. Owszem generują etykietę, ale zwykłą, a nie pobraniową. Następnie etykietę przerabiają tak, żeby wyglądała na pobraniową i wysyłają sprzedającemu. Sprzedający wysyła przedmiot, będąc przekonanym, że to przesyłka pobraniowa i dostanie pieniądze na konto. Niestety tak się nie dzieje – oszust po prostu otwiera paczkomat i zabiera przesyłkę za darmo. Zanim sprzedający się zorientuje, mija kilka dni.

Jeśli mamy jakiekolwiek wątpliwości co do intencji kupującego, zawsze lepiej po prostu poczekać, aż przelew spłynie na nasze konto, lub zapytać bank, czy dana wpłata miała miejsce.

Nerwy ze stali?

Nie przewidzimy wszystkich ruchów złodzieja, ponieważ nie myślimy jak on. Dlatego w sieci lepiej nie mierzyć innych naszą miarą i mieć w pamięci podstawowe schematy zachowań oszustów. Nawet przy drobnych zakupach zachowajmy czujność i spokój – obserwujmy zachowanie rozmówcy, sprawdzajmy wiarygodność informacji, a przede wszystkim nie bójmy się wycofać! Niech myślą, co chcą – bezpieczeństwo jest najważniejsze.

> **Bądźmy też szczególnie ostrożni, jeśli w tytule przelewu mamy wpisać dość przypadkowy ciąg znaków, niezwiązany z naszym zamówieniem, a nazwą odbiorcy przelewu nie są imię i nazwisko.**

JAK MANIPULUJĄ NAMI PRZESTĘPCY?

ROZMOWA O SOCJOTECHNIKACH W SIECI

„Wygrałeś 1000 zł w Loterii Narodowego Programu Szczepień. Aby odebrać nagrodę, kliknij w link i potwierdź swoje dane". Oprócz ekscytacji, którą możemy poczuć, czytając takiego SMS-a, zaufanie budzi odniesienie do loterii, o której wcześniej słyszeliśmy w mediach, więc uznajemy, że komunikat jest wiarygodny. Dodatkowy 1000 zł zawsze się przyda. Nosimy też w sobie przekonanie o własnej wyjątkowości i niepowtarzalności, więc lampka alarmowa nie zapali się. Nic dziwnego, że spośród milionów wybrano właśnie mnie – wyjaśnia psycholog, Zofia Libera.

Zofia Libera – psycholog, absolwentka Uniwersytetu SWPS, specjalizuje się w psychologii pracy i organizacji. Z fascynacją odkrywa nowe kierunki rozwoju psychologii i interdyscyplinarne badania naukowe. W przyszłości chce łączyć pracę w organizacji z działalnością akademicką.

Jak działają oszuści?

Efektywność ataków w sieci jest tak wysoka ze względu na wykorzystanie metod inżynierii społecznej podczas projektowania wiadomości czy stron internetowych. Socjotechniki oparte są na znajomości psychologicznych mechanizmów funkcjonowania człowieka. Oszuści polegają na wiedzy o sposobie naszego myślenia i odczuwania, mają świadomość, na jakich informacjach opieramy się, konstruując nasze sądy, i jak podejmujemy decyzje. A znając schematy ludzkiego postępowania, są w stanie tworzyć komunikaty mające za zadanie nakłonić nas do działania zgodnego z ich zamierzeniami.

Co sprawia, że dajemy się nabrać?

Wirtualna rzeczywistość staje się tą, w której spędzamy coraz więcej czasu. Niewątpliwie brak naszego technicznego przygotowania, szybkość zmian i konieczność nadążania za nimi wpływają na to, że jesteśmy w znacznym stopniu narażeni na przestępstwa internetowe. A ataki, których możemy stać się celem, są różne – e-maile z fałszywymi linkami, oszustwa z wykorzystaniem SMS-ów, telefony od pseudokonsultantów bankowych czy przedstawicieli instytucji publicznych i wiele innych, bardziej wyrafinowanych praktyk cyberprzestępczego świata. Zasoby naszej uwagi i pamięci są bardzo ograniczone. W znacznym stopniu ogranicza nas również czas. Natomiast funkcjonowanie z nieustannie wzmożoną czujnością doprowadziłoby nas do wyczerpania. Co więcej, w łatwy sposób ulegamy emocjom. Pobudzenie emocjonalne, odczuwanie radości, zaskoczenia czy ekscytacji na skutek otrzymanej wiadomości o wygranej w loterii, pozytywnie rozpatrzonej kandydaturze czy możliwości wzięcia udziału w promocji mają za zadanie skłonić nas do podjęcia natychmiastowych działań. Podobnie zadziałają wiadomości niosące poczucie zagrożenia, strach, groźbę utraty czegoś. Chcąc chronić samych siebie i zabezpieczyć nasze podstawowe potrzeby, automatycznie klikamy w nadesłany link, by uregulować np. rachunek za prąd i tym samym – tak nam się wydaje – zapewnić sobie bezpieczeństwo i spokój.

> **Socjotechniki oparte są na znajomości psychologicznych mechanizmów funkcjonowania człowieka. Oszuści polegają na wiedzy o sposobie naszego myślenia i odczuwania, mają świadomość, na jakich informacjach opieramy się, konstruując nasze sądy, i jak podejmujemy decyzje.**

Może Pani podać przykłady działań oszustów w sieci, bazujących np. na poczuciu zagrożenia?

„Zauważyliśmy, że przeoczyłeś płatność za ostatnią fakturę. Aby uniknąć dodatkowych opłat, prosimy o uregulowanie należności teraz". Nie lubimy być narażeni na dodatkowe koszty. Co więcej w natłoku obowiązków zdarzają nam się niedopatrzenia. Otrzymując taką wiadomość, możemy poczuć się winni i chcąc szybko naprawić błąd, nie pozostawiamy sobie czasu na bardziej wnikliwe przeanalizowanie sytuacji. Phishingowe wiadomości bardzo często będą wywoływały w nas poczucie pilności. To technika perswazji, która ma nas zmotywować do podjęcia działań: po 24 godzinach utracisz dostęp do swojego konta; twoje hasło traci ważność, kliknij, by odnowić dostęp. Innym przykładem może być e-mail typu: „Jesteś w pracy? Potrzebuję, żebyś wysłał mi załącznik z ostatnim podsumowaniem...". Wiadomość sugeruje, że znamy jej nadawcę, który zwraca się do nas z prośbą o pomoc. Z dużo większą łatwością przychodzi nam pomaganie ludziom, z którymi coś nas łączy, a przecież jesteśmy pracownikami tej samej organizacji. Lubimy osoby podobne do nas samych i takim chętniej pomagamy.

Jak możemy się uchronić przed cyberprzestępcami?

Ważne jest śledzenie doniesień medialnych i internetowych na temat nowych metod stosowanych przez oszustów. Wiedząc, że możemy się spodziewać fałszywego SMS-a dotyczącego potwierdzenia wysłania paczki, możemy zwiększyć czujność. Łatwiej nam będzie powstrzymać się przed kliknięciem, gdy otrzymamy taką wiadomość. Warto planować dzień w taki sposób, by na wiadomości odpowiadać bez dodatkowej presji i czujności. Takiego stanu nie utrzymamy, gdy spieszymy się, a nasze myśli są na niebawem rozpoczynającym się spotkaniu, w ostatnich godzinach dnia pracy czy w piątkowe popołudnie, kiedy zwyczajnie jesteśmy zmęczeni. Ze względu na to, że część technik opiera się na próbie wywołania w nas intensywnych emocji, należy za każdym razem, gdy uda nam się zidentyfikować taką próbę, zostawić sprawę do momentu opadnięcia emocji. Dopiero kiedy wejdzie nam w nawyk weryfikowanie danych, ostrożność przy pobieraniu załączników i otwieraniu linków, będziemy w stanie efektywniej bronić się przed atakami.

Rozmowę przeprowadziła Aleksandra Wróbel

Więcej informacji na temat dokonywanych przez nas uproszczeń myślowych oraz technik wpływu społecznego, którym ulegamy, można znaleźć w książkach, np. „Pułapki myślenia. O myśleniu szybkim i wolnym" (D. Kahneman) oraz „Wywieranie wpływu na ludzi. Teoria i praktyka" (R.B. Cialdini).

ON NIE PLANOWAŁ NOCLEGU POD CHMURKĄ!

Cezary Kolasa

Stare polskie przysłowie brzmi: nie wynajmuj z głową w chmurach, bo skończysz pod gołym niebem. No dobra, nie ma takiego przysłowia, ale na potrzeby tego tekstu możemy je stworzyć. Choć wynajmowanie mieszkań lub kwater noclegowych przez internet jest bardzo popularnym, wygodnym i na ogół bezpiecznym rozwiązaniem, zdarzają się takie osoby, które czyhają w sieci na naszą nieuwagę, aby ją wykorzystać.

Piękna zima, sypie śnieg, na termometrach minusowe temperatury – idealny czas na wyjazd w góry. Dla Tomka, pracownika administracji spod Warszawy, to dobry moment na zabranie rodziny na zimowe ferie i kilkudniowy odpoczynek. Tomek ze względu na inne obowiązki zaczyna szukać noclegu na ostatnią chwilę. Najlepiej w dobrej cenie, bo po co przepłacać. Znajduje superatrakcyjną ofertę z załączonymi eleganckimi zdjęciami luksusowego wnętrza. W centrum Zakopanego, blisko stoku, z przestronną łazienką i osobnym pokojem dla każdego. Wystarczy tylko z góry wpłacić zaliczkę, a najlepiej kwotę za cały pobyt...

Nie ma na co czekać, więc Tomek chwyta za telefon. Pech chce, że właściciel obiektu nie może akurat rozmawiać, ale zaraz wyśle mu mailem lub na czacie numer konta i poprosi o szybki przelew. „Chyba przyzna pan, że 500 zł za wypasiony apartament to niezbyt wygórowana cena, a mam już kilku chętnych na ten termin" – czyta Tomek w wiadomości, więc bez zwłoki zleca transfer środków.

Tydzień później nasz wczasowicz wybiera się z rodziną we wskazane miejsce. Ku swojemu zaskoczeniu zamiast kwatery widzi łąkę i żadnych zabudowań. Skuszony wizją niebywale atrakcyjnego noclegu Tomek dał się wpuścić w maliny, został bez noclegu i bez pieniędzy, za to z rozczarowaną, żeby nie powiedzieć nieźle wkurzoną rodziną. Jak nie podzielić losu Tomka?

O ile przedpłata dla właściciela obiektu nie powinna wzbudzać czujności, bo tak działa branża turystyczna, a prośba o jej uiszczenie jest zgodna z prawem, o tyle w historii naszego wczasowicza jest kilka sygnałów ostrzegawczych. Zanim więc wpłacisz zaliczkę, sprawdź, z kim masz do czynienia.

Sygnały ostrzegawcze

Każdy chciałby spędzić luksusowe wakacje, płacąc przy tym jak najmniej. Ale oferty, które wydają się zbyt piękne, by były prawdziwe, zazwyczaj po prostu prawdziwe nie są. W pierwszej kolejności sprawdź więc, czy znaleziony przez ciebie bajkowy ośrodek w ogóle istnieje. Nie? No właśnie...

Nie poddajesz się? Jeśli nie znalazłeś informacji kontaktowych w ogłoszeniu, poproś właściciela o podanie pełnej nazwy i adresu ośrodka, apartamentu czy hostelu. Sprawdź w wyszukiwarce Google opinie innych turystów na temat danego miejsca. Możesz też zweryfikować numer telefonu. Jeśli wcześniej wzbudził czyjeś podejrzenia, w internecie bez trudu znajdziesz informacje na ten temat. Podany numer konta bankowego możesz sprawdzić np. na stronie jakitobank.pl. Może ktoś już dał się nabrać i napisał negatywny komentarz.

CZTERY KĄTY, PRZEKRĘT PIĄTY?

Cezary Kolasa

Pandemia COVID-19 mocno wpłynęła na rynek nieruchomości. Według danych serwisów OLX i Otodom w lutym 2021 r. było dostępnych o 26 proc. więcej mieszkań na wynajem niż rok wcześniej. I choć liczba studentów chętnych na wynajem spada, to w obiegu nadal funkcjonuje sprawdzony patent na wyłudzenie sporych sumek od potencjalnych lokatorów.

Świetna oferta, znakomita cena najmu, wolne od zaraz. Wszystko pięknie, mieszkanie może być twoje, jeśli chcesz i jesteś gotowy zapłacić za rezerwację. To nic, że jeszcze go nie widziałeś. Rozmówca zapewni, że „wpłata jest na poczet kosztów dojazdu" albo że „to prowizja, którą bierze, będąc tylko reprezentantem właściciela mieszkania". A „z oferty warto skorzystać, bo jest już sporo chętnych"... Z tak nawiniętym na uszy makaronem decydujesz się na wpłatę i zostajesz z niczym, bo o ile przedpłata w turystyce to powszechna praktyka, o tyle zaliczka za rezerwację mieszkania albo terminu na jego obejrzenie może być ogromnym błędem.

Mieszkanie w Łodzi, zdjęcia z Kalisza

Podejrzenia może wzbudzić fakt, że w ofercie nie podano numeru telefonu albo to, że numer jest podany w treści ogłoszenia w bardzo nietypowy sposób, np. 500///120\\\567 lub 505%^&123%^&222. Dodatkowo ciąg cyfr wpisz w wyszukiwarkę. Poza tym jeśli konto na OLX, z którego wystawiono ofertę, istnieje kilka dni, również warto wzmóc uwagę. Sprawdź też, czy zdjęcia mieszkania są dostępne w innych ogłoszeniach lub w wyszukiwarce. Możesz to zrobić, klikając prawym przyciskiem na zdjęcie i wybierając opcję „szukaj w Google". Jeśli znalazłeś zdjęcia również w innych ofertach, upewnij się, czy dotyczą tego samego lokum, bo czasem może się okazać, że zdjęcia mieszkania w Łodzi to zdjęcia mieszkania w Kaliszu.

Każda próba przekierowania konwersacji na drogę e-mailową czy za pośrednictwem aplikacji mobilnych – bo „mam problem z kontem" – powinna być sygnałem ostrzegawczym. Nawet zachęta do kontaktu poza OLX dodana już w treści ogłoszenia, np. w formie „zapraszam do kontaktu na WhatsApp" z dodanym numerem telefonu, powinna wzbudzić nasze podejrzenia.

Bądźmy czujni. Jeśli mamy uzasadnione wątpliwości, możemy to zgłosić – pod każdą ofertą na OLX jest przycisk „Zgłoś". Po wybraniu konkretnego rodzaju naruszenia należy opisać dokładnie, dlaczego uważamy, że ogłoszenie jest oszustwem. Szczegółowe wyjaśnienie pozwoli na szybkie działanie. Nawet jeśli nie zostaliśmy oszukani, bo w porę poczuliśmy, że coś wzbudza nasze podejrzenia, poinformujmy o tym OLX, aby portal zweryfikował ogłoszenie. Możemy pomóc innym przed dokonaniem złego wyboru.

10 000 ZŁ NA RĘKĘ OD ZARAZ! DADZĄ PRACĘ, JAK DASZ IM SWÓJ DOWÓD

Zuzanna Pawłowska

Dobrze płacą, zatrudniają od zaraz, nawet nie potrzeba doświadczenia. W dodatku rekruter szybko odpowiada i jest nami na serio zainteresowany! Właśnie trafiła nam się taka oferta pracy, że z emocji przestajemy racjonalnie patrzeć na całą sytuację. Chwila nieuwagi i z potencjalnego pracownika stajemy się ofiarą przestępstwa.

Fałszywe oferty pracy, w przeciwieństwie do wielu wiadomości od cyberprzestępców, są napisane poprawną polszczyzną. Samo ogłoszenie jeszcze nie musi wzbudzać podejrzeń, a nasza odpowiedź niekoniecznie doprowadza do tragedii. Trzeba jednak szczególnie uważać na kolejnych etapach.

Robi się podejrzanie...

Gdy „pracodawca" – na etapie rekrutacji – prosi o przesłanie zaświadczeń o niepełnosprawności, niekaralności, o skany dokumentów osobistych (prawa jazdy, dowodu czy paszportu) możemy mieć pewność, że niestety nie bierzemy udziału w naborze do pracy marzeń. Przekonuje nas, że przy rekrutacji na kuriera lub kierowcę skan prawa jazdy potwierdzającego kompetencje kandydata to standardowa procedura? Nic z tych rzeczy.

Jeśli pada prośba o wpłacenie jakiejkolwiek zaliczki (np. na materiały szkoleniowe, zakup niezbędnego sprzętu do naszej pracy, opłatę za pośrednictwo) również od razu zakończmy rozmowę. Każda taka kwota trafi na konto oszusta, a żądanie jej jest niezgodne z prawem. Na OLX-ie ogłoszenia od osób, które wymagają od nas poufnych dokumentów (jeszcze przed podpisaniem umowy) lub jakichkolwiek opłat, polecamy oznaczyć, klikając „zgłoś naruszenie". W przypadku innych serwisów również warto zgłosić to administracji za pośrednictwem dostępnych narzędzi.

Rekrutacja zgodna z prawem, czyli jaka?

Informacje, których może od nas zażądać pracodawca na etapie rekrutacji, są ściśle określone przez art. 221 Kodeksu pracy. Należą do nich wyłącznie:

- imię (imiona) i nazwisko,
- data urodzenia,
- dane kontaktowe wskazane przez kandydata,
- wykształcenie,
- kwalifikacje zawodowe,
- przebieg dotychczasowego zatrudnienia.

Przy czym danych dotyczących wykształcenia, kwalifikacji zawodowych oraz przebiegu dotychczasowego zatrudnienia rekruter może żądać, tylko jeśli jest to niezbędne do wykonywania pracy na określonym stanowisku. Oznacza to, że przed podpisaniem umowy nie są potrzebne rekruterowi żadne inne informacje (nawet PESEL i nr konta bankowego) ani tym bardziej dokumenty czy ich skany.

Sztuka czytania (między wierszami)

Wiele znaków ostrzegawczych znajduje się już w samym ogłoszeniu. Na co zwracać uwagę przy czytaniu oferty?

1. Bardzo wysokie zarobki – jeśli oferta dotyczy sporych kwot za dość proste czynności administracyjne, możemy mieć pewność, że kryje się za tym coś podejrzanego.
2. Nazwa firmy – już sam jej brak jest podejrzany. Ogólniki w stylu „polska, legalna firma" również nie budzą zaufania. Jeśli jednak nazwa się pojawia, warto sprawdzić, czy instytucja figuruje w publicznych rejestrach przedsiębiorstw.
3. Opis stanowiska – im bardziej zawiły, tym gorzej. Podejrzanie brzmią też oferty pracy „dla każdego, od zaraz i bez rekrutacji".
4. Potrzebujesz tylko... konta bankowego – to jeden z wymogów? Czyli trwa rekrutacja na tzw. słupa w zwykłym przestępstwie, np. praniu brudnych pieniędzy. Założone przez ciebie konto będzie służyło przestępcy do wykonywania wpłat i wypłat. Z obiecanej wielkiej prowizji pozostaną ci jedynie sprawa w sądzie i ciężkie zarzuty współudziału w kradzieży.
5. Ogłoszenie-widmo – ogłoszenia dużych korporacji zazwyczaj są zamieszczane także na oficjalnych, firmowych stronach, a nie jedynie na portalach.
6. Kontakt z kandydatem przez komunikatory – żadna poważna firma nie proponuje tego kanału komunikacji.

Co nas uratuje przed tragedią? Spojrzenie chłodnym okiem na propozycje rekrutera i podstawowa wiedza na temat praw pracowniczych. Pamiętajmy, które informacje na etapie rekrutacji muszą pozostać tajne.

O DWÓCH TAKICH, KTÓRZY UKRADLI 2 MLN ZŁ

Marcin Mój

Największe szwindle w historii polskiej cyberprzestępczości to zazwyczaj oszustwa konsumenckie. Zakładanie podrabianych sklepów z elektroniką, masowe oszustwa „na kuriera", SMS-owe niedopłaty za prąd – trzeba przyznać, że oszustom nie brakuje kreatywności i odwagi. Szczególnie tym, którzy w pięciu skokach postanowili ukraść 2 mln zł z kont polskich gmin. Jak im się to udało?

Ćwierć miliona w Błażowej

W spokojnej podkarpackiej gminie życie płynęło swoim tempem. Mieszkańcy przygotowywali się do świąt, a zapach świerku unosił się w powietrzu. Woń szwindla zaczęła przebijać się do atmosfery, gdy do gminy zgłosił się jeden z robotników czekających na swoją wypłatę. Gminny sekretarz zaczął sprawdzać poprawność danych w wychodzących przelewach i po krótkim śledztwie wszystko wyszło na jaw. W 10 przypadkach dane do przelewów zawierały podmienione numery kont, a od listopada 2013 r. do świąt z gminy zniknęło 256 tys. zł. Nie był to najlepszy prezent na Gwiazdkę dla mieszkańców Błażowej.

Belsk Duży – skok mały

Kolejną ofiarą polskiego „Profesora" i spółki została mazowiecka gmina. W myśl zasady „zwycięskiego składu się nie zmienia" hakerzy zaatakowali w ten sam sposób. Atak na komputery urzędników, podmienianie numerów kont bankowych przez złośliwe oprogramowanie i... liczenie zysków. Skradzione 79 tys. zł z gminy Belsk Duży zasiliły konta zrekrutowanych do akcji bezdomnych, a później zostały wymienione na kryptowaluty.

Luka w Gidle

Tym razem przenosimy się do województwa łódzkiego. Rok 2014. Spokojne lato w gminie Gidle. Dzieciaki wyjechały na letnie kolonie, nauczyciele odpoczywają, czekając przy okazji na swoje letnie wynagrodzenia. Niestety – 317 tys. zł przeznaczone na ten cel padło łupem hakerów. Wykonano 20 transakcji i jak za dotknięciem magicznej różdżki – wypłat nie było. Pojawiło się za to mnóstwo pytań: kto, kiedy i jak? Szczęście w nieszczęściu – po kilku przesunięciach budżetu pracownicy otrzymali swoje premie, ale luka w Gidle została.

Rzęsisty płacz w Rząśni

Październik 2014 r. – urzędnicy zlecają w systemie bankowości elektronicznej dwa duże przelewy dla swoich kontrahentów. W grze 495 tys. zł, które zamiast trafić na docelowe konta zasiliły rachunki przestępców. Złodzieje musieli się poczuć wyjątkowo pewnie, przejmując pół miliona w dwóch transzach – takie kwoty łatwiej wytropić niż kilkadziesiąt mniejszych przelewów.

Grande finale w Jaworznie

Niemalże rok od pierwszego skoku w Błażowej hakerzy uderzyli po raz piąty. W styczniu 2015 r. Urząd Miejski w Jaworznie padł ofiarą przestępstwa. „Najprawdopodobniej w chwili wykonywania przelewu doszło do włamania na konto magistratu i kradzieży 940 tys. złotych" – mówiła tamtejsza policja. Pieniądze miały zasilić konto firmy Drogopol, ale niestety obrały inną drogę.

Od przelewów na kilkanaście tysięcy po milion złotych za jednym zamachem. Apetyt rośnie w miarę jedzenia. Tak było również w tym przypadku. Po kradzieży w Jaworznie policja zidentyfikowała sprawców. Na początku w ręce organów ścigania trafiło kilku bezdomnych, tzw. słupów, na których dane zostały założone złodziejskie konta. Później śledztwo doprowadziło do dwóch informatyków spod Warszawy, którzy zostali zatrzymani przez policję i przetransportowani do aresztu.

Organizatorami wszystkich pięciu napadów okazali się dwaj znani w Polsce hakerzy ukrywający się pod pseudonimami Kyber oraz The Venom Inside. W dniu zatrzymania mieli kolejno 21 i 25 lat. Kradzieży dokonano poprzez podmianę numeru docelowego rachunku bankowego. To z kolei udało się za pomocą konia trojańskiego, który zamieniał numery konta w schowku. Łup następnie trafiał na giełdę bitcoin, gdzie zamieniał się w kryptowalutę. Można powiedzieć, że po zatrzymaniu przez organy ścigania niewiele się zmieniło. Przestępcy cały czas byli w sieci – tyle że policyjnej.

FAŁSZYWA CZY PRAWDZIWA? ZNAJDŹ RÓŻNICE

Zespół OLX

Na pewno zdarzyło ci się kiedyś powiedzieć „cześć" na ulicy do nieznajomego, który wyglądał niemal jak dawno niewidziany kolega z poprzedniej pracy. Jeśli tak, to pewnie znasz towarzyszące tej pomyłce uczucie będące mieszanką zaskoczenia i zakłopotania. Podobnie jest ze stronami internetowymi, na których wpisujemy nasze dane, bo przecież są prawie identyczne. To „prawie" robi różnicę. Jak rozpoznać podróbkę od oryginału?

Mówi się, że w internecie jest wszystko. Są też, niestety, generatory stron, na których można stworzyć stronę do złudzenia podobną do innej. Żeby skutecznie dokonywać oszustw w sieci. Najłatwiej jest podszywać się pod te strony internetowe, których mnóstwo ludzi używa w celu dokonywania płatności lub robienia szeroko pojętych zakupów, np. pod banki, serwisy sprzedażowe czy ogłoszeniowe.

Skopiowanie takiej strony trwa dosłownie kilka sekund, ale diabeł tkwi w szczegółach. Po czym więc najłatwiej rozpoznać fałszywkę? Potraktujmy to jak zabawę w „znajdź różnice" polegającą na porównywaniu dwóch zestawionych ze sobą obrazków. Podobnie jak w tej popularnej grze, także w internetowym śledztwie warto szukać różnic tam, gdzie najłatwiej je wprowadzić. A więc w adresie strony, czyli w linku, który widnieje w pasku na górze wyszukiwarki. Dobrze najpierw wiedzieć, na jakiej stronie chcemy być. Przykładowo: https://mojaulubionastrona.pl/

Weźmy ten adres pod lupę. W linku najważniejsza jest domena, która musi znaleźć się między drugim a trzecim ukośnikiem. Teraz trzeba przyjrzeć się dokładnie literom z adresu. Czy „O" nie zastępuje symbol zero „0"? Czy małe „l" nie jest zastąpione dużym „i"? Czy „H" nie udaje symbol „#" itd. W przypadku serwisu OLX często wystarczy, że oszuści podmienią w linku jedną literę, dodadzą kilka symboli i gotowe. Czasem trudno wyłapać te subtelne różnice. Na szczęście korzystanie z internetu na co dzień to nie żaden egzamin, dlatego OLX przygotował legalną ściągę. Nazywa się sprawdzacz linków, znajduje się pod adresem https://pomoc.olx.pl/hc/pl i można w nim wpisać albo wkleić każdy link, który próbuje udawać serwis ogłoszeniowy.

Jeśli okaże się, że to podróbka, na stronie pojawi się komunikat o następującej treści:

> Podany przez Ciebie link nie należy do OLX. Jeśli otrzymałeś/-aś go w celu odbioru płatności w ramach transakcji w serwisie, istnieje wysokie prawdopodobieństwo, że jest fałszywy. Zachowaj ostrożność i nie podawaj na stronie żadnych danych. Jeśli chcesz zgłosić link do OLX – byśmy mogli podjąć odpowiednie działania – kliknij „Zgłoś".

A sam link podświetli się na czerwono. Nie dziś, oszuście!

Dodaj do ulubionych

Najlepiej po prostu nie klikać w linki z e-maili, SMS-ów, wiadomości na WhatsApp. Jest prosty sposób, by ograniczyć ryzyko klikania. Wystarczy strony, z których często korzystamy, dodać do ulubionych. Jeśli korzystasz z banku, którego adres to https://bank.pl/, zapisz ją w zakładkach przeglądarki, a w celu dokonania płatności loguj się zawsze poprzez stronę przypisaną tej zakładce. W ten sposób ograniczysz pokusę klikania w niepotrzebne, błędne linki przesłane od nieznajomych, którzy czyhają na twoje pieniądze.

Przykładowe strony w domenie olx.pl:

https://pomoc.olx.pl/
https://blog.olx.pl/
https://przesyłki.olx.pl/

Przykładowe fałszywe strony:

https://olx.pl-safedeal24-postakceptacja.xyz/
https://olx-pl.10343.site/
https://olx.pl.dostawa-safe.club/

Pamiętajmy, że OLX nie generuje linków do opłacenia zakupu za pośrednictwem Przesyłki OLX. Wszystko odbywa się w serwisie – przy płaceniu za towar jedynymi przekierowaniami są DotPay (ssl.dotpay.pl/) oraz Adyen (eu.adyen.link/). A adresy, które są związane z Przesyłkami OLX, to:

https://marketplace.olx.pl/
https://delivery.olx.pl/
https://przesylki.olx.pl/.

Jeśli jakakolwiek strona wzbudza nasze wątpliwości, nie uzupełniajmy na niej żadnych danych. Uważajmy oraz przestrzegajmy innych przed oszustwami. Przezorny zawsze ubezpieczony!

POKAŻ POLICJI, JAK DAŁEŚ SIĘ OSZUKAĆ! BĄDŹ MĄDRY PO SZKODZIE

Cezary Kolasa

Kto padł ofiarą oszustwa, może zechcieć szybko usunąć ślady świadczące o tym, jak łatwo dał się złapać w pułapkę. Ten błąd może słono kosztować. Po przechytrzeniu przez oszusta warto działać w swojej sprawie i zebrać dowody, które będą przydatne policji.

Jak wynika z raportu „Krajobraz bezpieczeństwa polskiego internetu w 2020 roku", dwa lata temu zarejestrowano ponad 10 tys. incydentów naruszających bezpieczeństwo w sieci, co daje wzrost o ponad 60 proc. w porównaniu z danymi z 2019 r. Zarówno w 2020 r., jak i w 2019 najczęstszym rodzajem ataku był phishing.

Wyłudzenie danych, włamanie na konto bankowe i kradzież – każdy może paść ofiarą oszustów. Niestety czasem dajemy się nabrać w tak naiwny sposób, że aż wstyd nam się przyznać przed sobą, a co dopiero przed innymi. Tymczasem stwierdzenie faktu i szybka reakcja to podstawy. Oszukany powinien natychmiast po zorientowaniu się, że padł ofiarą cyberprzestępstwa, podjąć odpowiednie kroki, które pomogą w złapaniu oszusta i być może w odzyskaniu utraconych środków.

Oszczędź sobie kłopotów!

Po pierwsze zmień hasło do logowania w bankowości internetowej i do e-maila. Zadbaj o to, by było bezpieczne. Jeśli udostępniłeś dane karty płatniczej lub podejrzewasz, że mogły zostać skradzione, możesz ją zastrzec samodzielnie lub z pomocą banku. Możesz ją też zablokować. To drugie rozwiązanie jest odwracalne. Zastrzegając kartę, sprawisz, że już nikt nigdy nie będzie mógł z niej korzystać. Ważne, by działania podejmować niezwłocznie, a więc zaraz po tym, jak zorientujemy się, że zostaliśmy poszkodowani.

Zastrzeżenie karty nie tylko uniemożliwi złodziejowi kradzież środków z konta, lecz także przeniesie odpowiedzialność za bezpieczeństwo naszych pieniędzy na bank. Jak wynika z ustawy o elektronicznych urządzeniach płatniczych, z chwilą zastrzeżenia karty to bank ponosi odpowiedzialność za nieuprawnione transakcje i jest zobowiązany zwrócić nam środki, które wyjdą z konta bez naszej wiedzy.

Jeśli nie jesteśmy w stanie dokonać tych czynności samodzielnie, np. w aplikacji bankowej, skontaktujmy się z bankiem. Numer na infolinię banku, z którego usług korzystamy, warto mieć wpisany na stałe w telefonie!

A teraz spacer na komisariat

Kiedy pieniądze są już bezpieczne, sprawę należy zgłosić na policję. Do wizyty na posterunku trzeba się jednak dobrze przygotować. Wyrzuty sumienia albo dobre rady znajomych mogą zachęcić nas do usunięcia śladów naszej nieroztropności. Tymczasem kasowanie phishingowego SMS-a, wiadomości z komunikatorów, takich jak WhatsApp lub Messenger, e-maila nie jest dobrym pomysłem. Usuwając je, pozbywamy się dowodów! Szanse na złapanie oszusta rosną, jeśli policja otrzyma przydatne informacje. Należą do nich: linki prowadzące do fałszywych płatności lub stron udających strony prawdziwych firm, numery telefonów, adresy e-mailowe oraz treść otrzymanych komunikatów. W przypadku transakcji internetowych przydadzą się również numer rachunku, na który przelaliśmy pieniądze, dokładny czas transakcji i potwierdzenie przelewu.

Uwaga! Nie wystarczy przepisać danych i numeru telefonu. Oszuści są na tyle sprytni, że potrafią podszyć się pod innych, np. pod bank, urząd albo firmę kurierską. Taki zabieg hackowania numeru nazywa się spoofingiem. Zdarza się też, że e-maile od oszustów kamuflowane są dobrze znanym nam adresem. W takim przypadku po kliknięciu w nagłówek wiadomości polecenia „rozwiń szczegóły" możemy znaleźć konkretny adres, a być może nawet IP sprawcy. Zachowajmy więc wszystkie dane w formie zrzutu ekranów, wydruku wiadomości, nie usuwajmy dowodów!

Po zgłoszeniu policja przejmuje inicjatywę, zabezpiecza materiał dowodowy, uruchamia swoje procedury – kontaktuje się z bankiem, operatorami telekomunikacyjnymi, hostingami domen, przesłuchuje świadków, zabezpiecza monitoringi. Rola poszkodowanego jednak w tym miejscu się nie kończy. Zgodnie z prawem przysługuje mu bowiem tzw. inicjatywa dowodowa, co oznacza, że można samemu być aktywnym w toku postępowania i zbierać kolejne dowody.

Serwis OLX na wniosek upoważnionych do tego organów ścigania (policji i prokuratury) udostępnia wszelkie dane teleinformatyczne potrzebne w śledztwie.

KOMENTARZ EKSPERTA

W informatyce socjotechniką określa się sztukę manipulacji ludźmi w celu nakłonienia ich do podjęcia określonych działań lub ujawnienia poufnych informacji. W atakach socjotechnicznych kluczowe są umiejętności oddziaływania na ludzi w celu np. skłonienia ich do wykonania określonych czynności czy podania określonych informacji. Do najczęstszych ataków opartych na inżynierii społecznej można zaliczyć phishing – czyli atak wykorzystujący inżynierię społeczną w celu wyłudzenia poufnych informacji poprzez podszycie się pod inny, zaufany podmiot.

Jak wskazują raporty zespołu CERT Polska, udział phishingu we wszystkich obserwowanych incydentach rośnie – w latach 2018–2020 stanowiły kolejno 44 proc., 54 proc. i 73 proc. Z uwagi na to, że scenariusze ataków opartych na socjotechnice są bardzo zróżnicowane, różna będzie kwalifikacja prawna konkretnego czynu. Jeśli działanie sprawców polega na nieuprawnionym uzyskaniu danych do logowania do konta poczty elektronicznej ofiary poprzez przełamanie lub ominięcie zabezpieczeń – wypełni znamiona czynu z art. 267 § 1 Kodeksu karnego (określanego jako hacking). Znamiona oszustwa, tj. czynu z art. 286 § 1 k.k., zostaną wypełnione, jeśli sprawca w celu osiągnięcia korzyści majątkowej doprowadzi inną osobę do niekorzystnego rozporządzenia mieniem poprzez wprowadzenie jej w błąd lub wykorzystanie błędu. Jeśli zaś sprawca w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody bez upoważnienia wpłynie na automatyczne przetwarzanie danych – popełni oszustwo komputerowe, tj. czyn z art. 287 § 1 k.k.

W Polsce obserwuje się ataki zarówno o charakterze globalnym, jak i lokalnym. Oprócz globalnych przestępców zajmujących się dystrybucją złośliwego oprogramowania czy atakami nakierowanymi na poufność danych istotnym zagrożeniem jest również działalność polskich cyberprzestępców, którzy zajmują się głównie popełnianiem oszustw (np. prowadzą fałszywe sklepy internetowe, dokonują oszustw na portalach aukcyjnych lub ogłoszeniowych, w social mediach), infekują użytkowników internetu złośliwym oprogramowaniem, przejmują dane do logowania, a także dokonują kradzieży z włamaniem do środków z rachunków bankowych.

Jednym z częstszych ataków na obywateli Polski jest wykorzystanie scenariuszy, w których sprawcy wykorzystują tzw. fałszywą bramkę płatności i przy użyciu różnych metod socjotechnicznych przekonują ofiary do dokonania płatności online. W tym celu wysyłają wiadomości SMS z odnośnikiem do strony podszywającej się pod stronę pośrednika płatności i banków. Jeśli ofiara na fikcyjnej stronie banku poda login i hasło do bankowości elektronicznej, sprawcy dokonają transferu środków z jej rachunku bankowego.

Kolejnym bardzo popularnym scenariuszem jest atak polegający w pierwszej fazie na uzyskaniu bez uprawnienia danych do logowania do portali społecznościowych z wykorzystaniem fikcyjnej strony imitującej panel logowania, zaś w drugiej fazie – wykorzystaniu przejętych kont do przejmowania kont innych osób oraz dokonywania oszustw.

W 2021 r. wzrosła również liczba ataków na osoby sprzedające towary za pośrednictwem platform sprzedażowych i ogłoszeniowych. Ze sprzedającym, tuż po wystawieniu przez niego oferty sprzedaży, za pośrednictwem komunikatora internetowego kontaktuje się osoba, która twierdzi, że jest zainteresowana zakupem, i wysyła link do opłacenia przesyłki w celu wyłudzeniu danych karty płatniczej sprzedawcy lub danych do logowania do bankowości elektronicznej.

Ponieważ większość ataków opiera się na socjotechnice, zwiększenie świadomości użytkowników internetu w zakresie aktualnych zagrożeń znacząco ograniczyłoby skutki działania cyberprzestępców.

AUTOR KOMENTARZA

Doktor hab. inż. Agnieszka Gryszczyńska z Katedry Prawa Informatycznego, Wydział Prawa i Administracji UKSW

DZIEŃ DOBRY! DZWONIĘ Z BANKU...

Jolanta Kikiewicz

Oszuści telefoniczni często podszywają się pod pracowników banków. Na wyświetlaczu telefonu ofiar pojawia się zapisany wcześniej numer tej instytucji. Pseudopracownik banku na wstępie rozmowy ostrzega, że nastąpiła próba włamania na konto odbiorcy czy wnioskowania o kredyt. Oszuści są na tyle wiarygodni, że wiele osób od razu wierzy w telefoniczne kłamstwo. Najczęściej chodzi o wyłudzenie pieniędzy i danych.

Oszuści chcący wykraść dane i pieniądze od klientów banków wykorzystują coraz nowsze sposoby. Wiedzą, że prawdziwi pracownicy składają klientom oferty na terenie placówki lub w rozmowie telefonicznej. Dlatego przestępcy wykorzystują nowy rodzaj podstępu, czyli vishing: voice phishing (phishing głosowy). Do prób wyłudzenia dochodzi za pośrednictwem rozmowy telefonicznej.

Jak przebiega standardowa rozmowa z pseudopracownikiem banku? Większość z nich odbywa się według następującego scenariusza:

1. Na ekranie telefonu wyświetla się zapisany przez odbiorcę numer banku lub numer, który po sprawdzeniu w internecie okazuje się numerem banku, ponieważ oszuści potrafią przejąć numer z wykorzystaniem specjalnego oprogramowania.
2. Odbiorca słyszy standardowy komunikat ostrzegający o nagrywaniu rozmowy.
3. Oszust przedstawia się z imienia i nazwiska, informuje, jaki bank reprezentuje, oraz wyjaśnia, że nastąpiła próba włamania na konto bankowe lub próba wykonania przelewu czy zaciągnięcia kredytu.
4. Pyta rozmówcę o jego nawyki w zakresie bezpieczeństwa. Sprawia wrażenie osoby, która troszczy się o bezpieczeństwo klienta banku.
5. Zapewnia, że dzięki wczesnej interwencji banku włamanie na konto klienta nie powiodło się.
6. Prosi o ściągnięcie oprogramowania na telefon lub komputer za pomocą linku, który wkrótce wyśle SMS-em. Gwarantuje, że oprogramowanie ma na celu wzmocnienie systemu ochrony danych i pieniędzy klienta.
7. Kiedy rozmówca uruchamia złośliwe oprogramowanie, przestępca zyskuje dostęp do jego danych i konta bankowego.
8. Oszust może również poprosić o podanie numeru BLIK do wykonania szybkiej transakcji lub numeru karty debetowej czy kredytowej.

Zarówno banki, jak i policja zapewniają, że prawdziwy pracownik banku nie będzie wymagał od klienta podania wrażliwych danych przez telefon ani ściągania dodatkowego oprogramowania. Zwykle zapyta jedynie o datę urodzenia lub kilka liczb z numeru PESEL, ewentualnie o zabezpieczający dostęp do danych kod, ustalony przy zakładaniu konta w placówce banku. Pracownik nie poprosi przez telefon o podanie pełnego PESEL-u, numeru dowodu lub paszportu czy kodu CVC/CVV naszej karty płatniczej lub kredytowej.

Każdy z etapów opisanej wyżej rozmowy powinien wzbudzić podejrzenia. Najistotniejsze jest przerwanie rozmowy, zanim dojdzie do pobrania złośliwego oprogramowania, a następnie niezwłoczne poinformowanie banku o próbie kradzieży.

ODBIERZ OSZUSTOM ARGUMENTY DZIĘKI PRZESYŁCE OLX

Zuzanna Pawłowska

Delegacja, niespodziewany wyjazd, urlop, pośpiech – fałszywi sprzedawcy rzucają wymówkami jak z rękawa, byle tylko zniechęcić cię do osobistego odbioru, przekierować do fałszywej strony i wyłudzić przelew. Jeśli już dla niepoznaki zgodzą się na spotkanie, to zwykle pada: „Przydałaby się jakaś zaliczka, żebym miał pewność, że odbierzesz". W to, że „by się mu przydała", jak najbardziej wierzymy. Ale w jego dobre intencje już niekoniecznie...

Nie da się całkowicie ochronić kupujących przed oszustwem. Sami prowadzą konwersację ze sprzedającym i decydują o przebiegu transakcji. Mają jednak dostęp do funkcjonalności, które mogą zmniejszać opisywane ryzyko. Przykładowo serwis OLX wprowadził dwie usługi – Przesyłkę OLX oraz Pakiet Ochronny. Na czym polegają?

Łatwe zakupy z Przesyłką OLX

Przesyłka OLX pozwala obu stronom – kupującemu i sprzedającemu – na komfortową transakcję i sprawny przebieg całego procesu. Zobacz, jak działa ta opcja.

1. Przy wybranym ogłoszeniu klikasz w przycisk „Kup z Przesyłką OLX".
2. Uzupełniasz dane, wybierasz punkt odbioru paczki, płacisz za zamówienie.
3. Pieniądze nie trafiają od razu do sprzedającego! Musi zaakceptować twoją ofertę, a potem poczekać, aż odbierzesz paczkę.
4. Śledzisz drogę swojej przesyłki w zakładce „Twoje Przesyłki" / „Kupujesz".
5. Status przesyłki zmienia się na „Gotowa do odbioru" – możesz ją wtedy zabrać z wybranego przez siebie punktu.
6. W ramach Pakietu Ochronnego wybierasz na swoim koncie OLX (w zakładce z twoimi przesyłkami) przycisk „Przedmiot jest OK" lub „Zgłoś" – masz na to 24 godziny.

Jeśli wszystko jest w porządku, operator płatności wysyła zapłatę do sprzedającego. Powinna do niego trafić w ciągu trzech dni roboczych. Opcja Przesyłki OLX dostępna jest dla sprzedawców w wybranych kategoriach. Jeśli sprzedawca jej nie włączył, nie oznacza to od razu, że masz do czynienia z oszustem. Jeśli rozmowa wydaje się podejrzana (np. sprzedawca unika odbioru osobistego, wywiera na tobie presję, aby wykonać przelew, zanim cokolwiek otrzymasz), a do tego sprzedawca nie udostępnia opcji Przesyłki OLX – lepiej odpuść. „Niesamowita okazja!" na pewno jeszcze się nadarzy.

Pomocne wsparcie, czyli Pakiet Ochronny

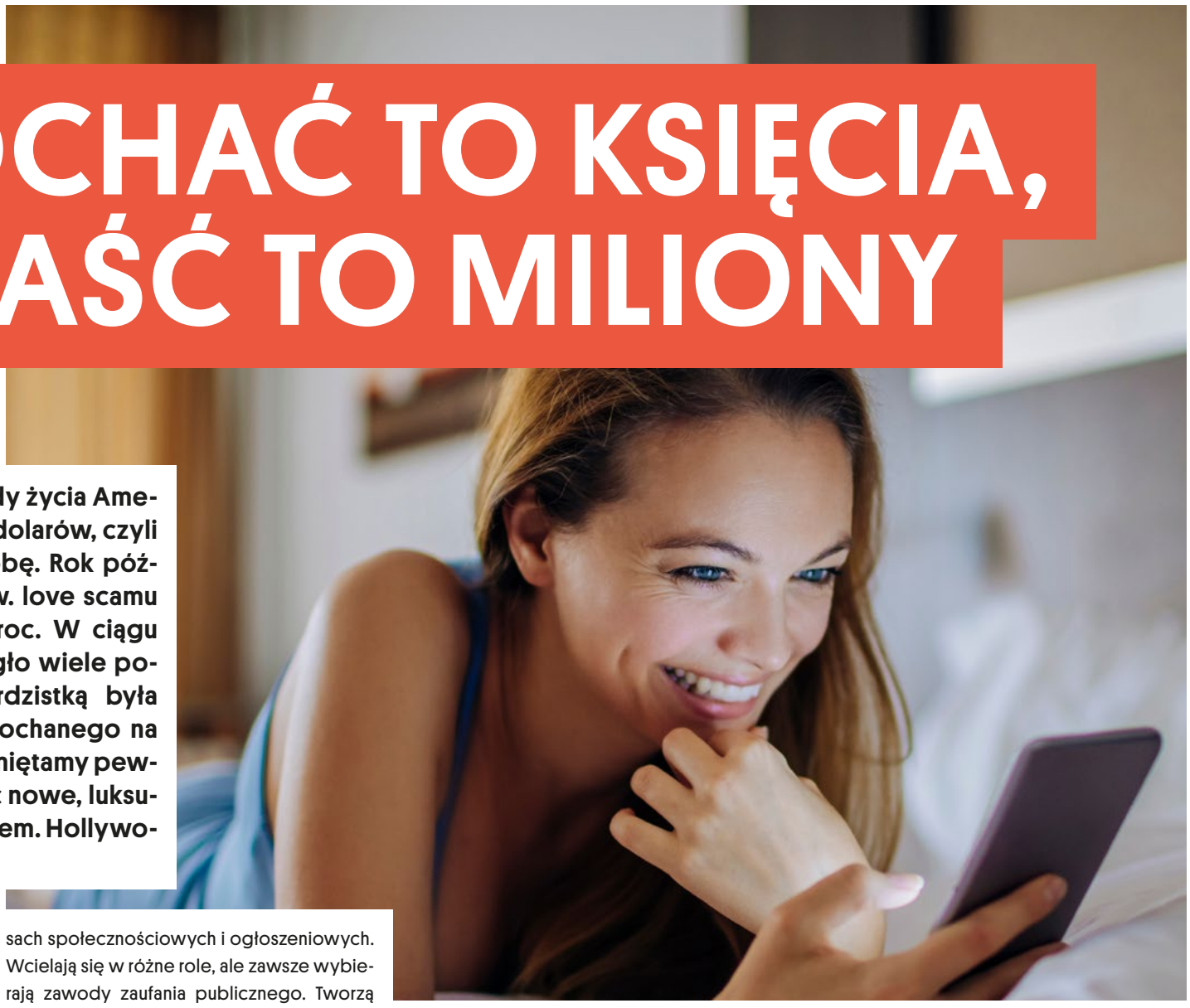
Oszuści potrafią robić dobrą minę do złej gry do samego końca. Otrzymasz nawet prawdziwe potwierdzenie wysyłki. Problem w tym, że w paczce może kryć się zupełnie coś innego, niż zamawiałeś. I wcale nie będzie to miła niespodzianka... W serwisie OLX możesz skorzystać z Pakietu Ochronnego, aby zgłosić nadużycie i odzyskać wpłacone pieniądze. Kiedy zadziała Pakiet Ochronny? Jeśli kupiłeś przedmiot z opcją Przesyłka OLX, a paczka jest pusta lub otrzymasz inny towar niż zamawiany przedmiot ogłoszenia, bo zamiast konsoli dostałeś worek ziemniaków, zgłoś naruszenie.

Pamiętaj, że masz dobę, aby w serwisie OLX zaznaczyć „Przedmiot jest OK" lub „Zgłoś". To od tej decyzji zależy, czy sprzedający otrzyma przelew, czy transakcja zostanie wstrzymana aż do rozpatrzenia twojego wniosku. W razie zgłoszenia nadużycia odpowiedź otrzymasz najpóźniej w ciągu 14 dni.

Po upływie 24 godzin – jeśli nie podejmiesz żadnej decyzji – przyciski przestaną być aktywne, a pieniądze automatycznie trafią na konto sprzedającego.

Warto korzystać z pomocnych narzędzi, które oferuje OLX. Dzięki nim – nawet jeśli stracisz na chwilę czujność i złapiesz się w sidła oszusta – nie dasz mu tak łatwo wygrać!

JAK KOCHAĆ TO KSIĘCIA, JAK KRAŚĆ TO MILIONY



Zuzanna Pawłowska

W 2018 r. za romantyczne przygody życia Amerykanie zapłacili w sumie 143 mln dolarów, czyli średnio po 2600 dolarów na osobę. Rok później suma wyłudzona od ofiar tzw. love scamu powiększyła się o prawie 40 proc. W ciągu ostatnich lat polskie media obiegło wiele podobnych historii. Chociaż rekordzistką była gdańszczanka oszukana przez ukochanego na 200 tys. złotych, to wszyscy zapamiętamy pewną 35-latkę, która miała rozpocząć nowe, luksusowe życie z samym Willem Smithem. Hollywoodzkie marzenia słono kosztują.

„Długo zastanawiałam się, jaki błąd popełniłam, że relacja została zerwana", „nadal nie mogę przestać go kochać i myślę, że byłabym w stanie mu wybaczyć" – wyznają uczestniczki badania „Oszustwa romantyczne online – studium przypadku" przeprowadzonego w 2019 r. Psychologowie zwracają uwagę, że dla tak oszukanych kobiet straty finansowe są często dużo mniej dotkliwe niż emocjonalne i moralne. Rana po związku z cyberoszustem prowadzi czasem do stanów depresyjnych i na długo hamuje kobietę przed otwarciem się na inne relacje. Ofiary love scamu doświadczają całego wachlarza emocji, nierzadko skrajnych. Czują paraliżujący wstyd przed rodziną i znajomymi, biorą na siebie winę za całą sytuację, ale tęsknią też za ukochanym i desperacko próbują znaleźć sposób na uratowanie związku. Jakiego związku?

Jak szybko sprawdzić wiarygodność rozmówcy? Pokonać go jego własną bronią, czyli wykorzystać siłę internetu. Warto wyszukać w Google otrzymane zdjęcia, wpisać adres e-mail lub fragment rozmowy.

Ma w sobie to coś

Internetowy flirt, a zaraz potem wielka miłość z uczestnikiem misji humanitarnej na terenie państwa dotkniętego konfliktem zbrojnym albo amerykańskim żołnierzem, korespondentem wojennym, lekarzem, opływającym w dostatek spadkobiercą królewskiego dziedzictwa lub ustawionym prawnikiem z Dubaju. Oszuści poszukują ofiar nie tylko na portalach randkowych, lecz także na serwisach społecznościowych i ogłoszeniowych. Wcielają się w różne role, ale zawsze wybierają zawody zaufania publicznego. Tworzą fikcyjne profile w mediach społecznościowych, wykorzystując – i czasem nieco modyfikując – zdjęcia innych osób. Bywają na tyle bezczelni, że podszywają się nawet pod gwiazdy Hollywood. Tak jak w słynnej historii z Willem Smithem. Oszust podający się za aktora nawiązał kontakt z 35-latką na Instagramie i tak ją zmanipulował, że ta uwierzyła w swój bajkowy romans. Upoważnił ją (zapewne w dowód miłości) do odbioru przesyłki, w której miały się znaleźć: 3 mln dolarów w gotówce, diamenty o wartości 6 mln i dokumenty rozwodowe. Aby odebrać paczkę, Polka musiała opłacić wydanie specjalnego certyfikatu – przelała więc na podany numer konta 45 tys. zł.

Kogo oszuści obierają za cel? Zazwyczaj samotne kobiety, chociaż potrafią uwieść też mężczyzn. Przyjmuje się, że najbardziej podatne na oszustwa są osoby w grupie wiekowej między 40. a 70. rokiem życia. Poziom wykształcenia nie odgrywa tak istotnej roli jak samo obycie ze specyfiką sieciowych interakcji. Przede wszystkim jednak podatnymi na manipulacje kochanków-oszustów czynią nas temperament, struktura psychiczna i aktualny moment życiowy (np. dotkliwa samotność, pragnienie ustatkowania). Potencjalne ofiary są często osobami impulsywnymi, ugodowym, o obniżonej samoocenie. Zwykle są nastawione do życia skrajnie idealistycznie.

(Nie)śmiałe początki

Pani Ania, 42-letnia warszawianka, wspomina, że kiedy na portalu randkowym napisał do niej John – amerykański lekarz przebywający na misji w Syrii – od razu poczuła z nim silną więź. Rozpoczęli intensywną korespondencję e-mailową. John szczegółowo opowiadał o swoim życiu, wysyłał zdjęcia, dzielił się codziennością. Wkrótce zaczął zapewniać o swojej tęsknocie i potrzebie kontaktu. To był według pani Ani mężczyzna inny niż wszyscy. Nie bał się swoich uczuć i wiedział, jak podtrzymać temperaturę związku. Po paru tygodniach zaczęli snuć plany wspólnego życia w Polsce.

Sprytne testowanie

Jane – czarująca, brytyjska pielęgniarka pomagająca dzieciom w Jemenie – po paru tygodniach miała pana Michała w garści. Pięćdziesięciolatek z Wielkopolski nie wahał się długo, kiedy kobieta poprosiła go o drobne finansowe wsparcie. Chodziło o dołożenie się do zakupu leków dla afrykańskich sierot. Jane oczywiście obiecała, że wkrótce odda dług, jak tylko spłynie przelew od instytucji humanitarnej wspierającej jej działalność. Pan Michał jednak nawet tego nie oczekiwał. Prosiła go przecież jego ukochana, dzięki której wreszcie mógł zapomnieć o ciężkim rozwodzie.

Honey, I'm home!

Zarówno John, jak i Jane obiecywali szybki przylot do Polski, aby rozpocząć wymarzone życie ze swoimi wybrankami. Wielki przyjazd jednak się komplikował, a oni byli ofiarami niesłychanie dramatycznych wydarzeń (ktoś ich okradł, pobił, nagle ciężko zachorowali...). Za każdym razem niezbędna była finansowa pomoc. Scenariusze niefortunnych wypadków, które opóźniały przylot do Polski, zmieniały się dopóty, dopóki pani Ania i pan Michał brali udział w tej cynicznej grze i przelewali pieniądze.

Zanim złamie ci serce

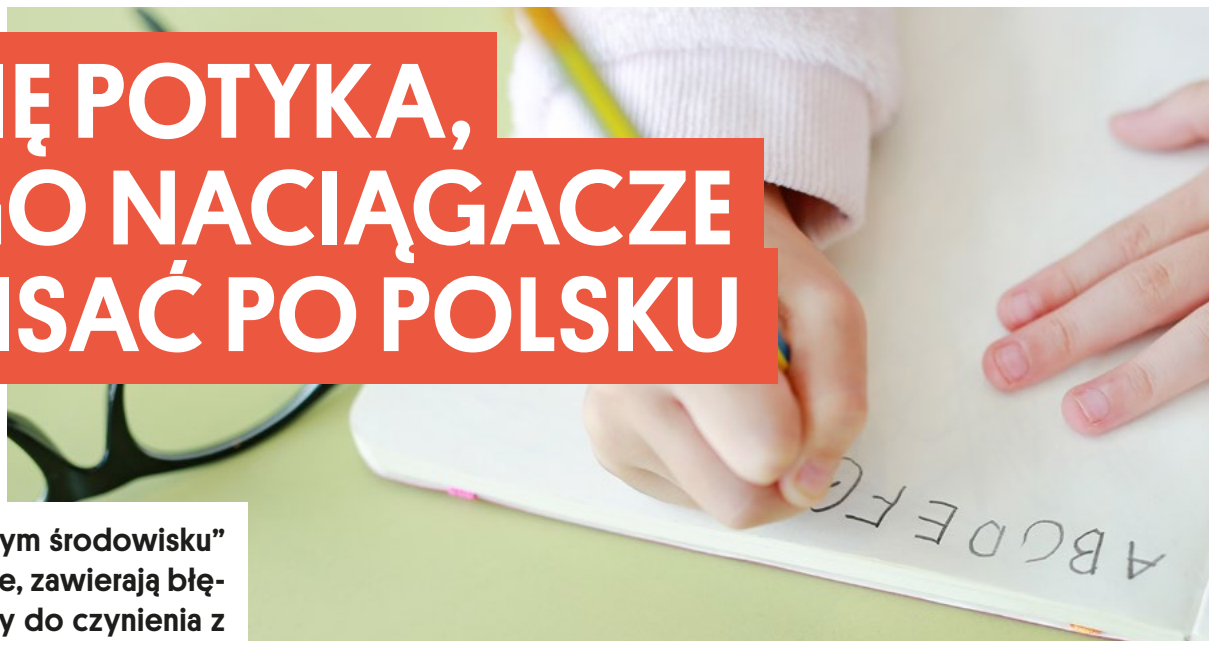
Czułe słówka potrafią omamić, dlatego trzeba czytać między wierszami i uważnie obserwować. Kiedy powinna zapalić się czerwona lampka? Gdy internetowy rozmówca unika spotkania twarzą w twarz (choćby w formie wideorozmowy), nie chce zgodzić się na rozmowę telefoniczną (bo np. dowódca armii zabrania tego typu połączeń ze względu na bezpieczeństwo misji). Podejrzenie powinna wzbudzić prośba o zakup drobnego sprzętu (np. telefonu komórkowego, zegarka) czy o pieniądze. Oszust zwykle nie chce przelewu na konto, tylko korzysta z międzynarodowych transferów lub doładowania kart podarunkowych.

Jak szybko sprawdzić wiarygodność rozmówcy? Pokonać go jego własną bronią, czyli wykorzystać siłę internetu. Warto wyszukać w Google otrzymane zdjęcia, wpisać adres e-mail lub fragment rozmowy. Często już to wystarczy, aby znaleźć ostrzeżenia innych użytkowników na jego temat.

Miłość jest ślepa

Oszustwo „na romans" wydaje się najbardziej perfidnym ze wszystkich cyberprzestępstw – wykorzystuje dotkliwą próżnię w emocjonalnym życiu wielu osób i daje nadzieję. Zachłyśnięcie się niespodziewaną, idealną miłością dość skutecznie paraliżuje zdolność racjonalnego myślenia. Dlatego często przy internetowych romansach nieocenione jest trzeźwe spojrzenie zaufanej osoby. Potrafi ono odebrać czar fałszywemu kochankowi i ściągnąć urok z ofiary.

GRAMATYKA SIĘ POTYKA, CZYLI DLACZEGO NACIĄGACZE NIE POTRAFIĄ PISAĆ PO POLSKU



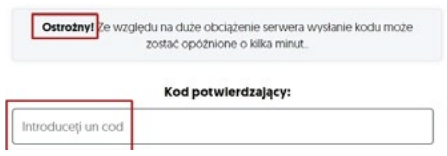
Jolanta Kikiewicz

„Kasa, przelew, dostawa odbywa się w bezpiecznym środowisku" – jeżeli otrzymane komunikaty brzmią niepoprawnie, zawierają błędy i podejrzane zwroty, to istnieje ryzyko, że mamy do czynienia z phishingiem, czyli próbą wyłudzenia danych lub pieniędzy. Istnieją różne przykłady tego typu przestępstwa, a błędne konstrukcje językowe to dobra wskazówka do rozpoznania wiadomości od oszusta.

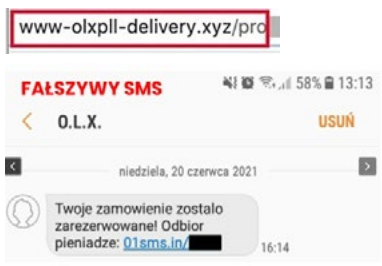
Komunikaty od oszustów bywają bezosobowe: naciągacze podszywający się pod OLX często tworzą przyciski, formułując komunikat w bezokoliczniku. Dla polskiego użytkownika może to brzmieć dziwnie, np. zamiast komunikatu „OK" lub „AKCEPTUJĘ" pojawią się polecenia „ZROBIĆ", „POTWIERDZAĆ" lub „GOTOWOŚĆ".

Tygiel językowy phishingowców

Bywa, że w obrębie jednego komunikatu możemy się spotkać z kilkoma różnymi językami. O ile do łączenia polskiego z angielskim już się przyzwyczailiśmy, tak polski z rumuńskim wydaje się być już dość egzotyczny, czego przykład widzimy poniżej:



Takiej mieszanki językowej nie ma na prawdziwych, bezpiecznych stronach OLX. Według raportu firmy Barracuda z 2020 r. Polska jest najbardziej narażona na ataki z Litwy, Łotwy, Serbii, Ukrainy i Rosji. Jeżeli linki przesłane w SMS-ie czy e-mailu nie wskazują na polską domenę olx.pl (o tym, jak ją rozpoznać, piszemy w tekście na stronie 10), są to fałszywe odnośniki do złośliwego oprogramowania lub innych form phishingu:



Naciągacze nie dbają o poprawną polszczyznę, bo szkoda im na to środków i czasu. Komunikaty tworzą w pośpiechu, żeby móc jak najszybciej czerpać korzyści z fałszywych treści. Często nie mają świadomości, że popełniają błędy. I nie widzą też konieczności stosowania poprawych językowo konstrukcji, skoro ludzie i tak dają się oszukać. A zdarza się, że są to po prostu oszuści z różnych zakątków świata, którzy najzwyczajniej nie mówią poprawnie w języku polskim.

Witaj w oszustwie. Niezgrabny język naciągaczy

Język komunikatów phishingowych często zawiera nieodpowiednią odmianę przez przypadki, choć na pierwszy rzut oka może być ona mało zauważalna, jak w zdaniu: „Podaj dane, które wymaga wybrany bank". Jeżeli treść przesłana w SMS-ie, e-mailu czy komunikacie sprawia wrażenie pisanej na kolanie, prawdopodobnie nie jest to wiadomość od prawdziwego nadawcy. Niektóre cechy fałszywych komunikatów można poznać po podejrzanym układzie tekstu. W treści brakuje wielkich liter na początku zdań, a podpunkty rozpoczynają się raz małą, a raz dużą literą. Jeszcze trudniejsze do wykrycia mogą być podwójne spacje, których nie brakuje w phishingowych komunikatach.

Poprawne powitanie to połowa sukcesu na drodze do efektywnej komunikacji. W phishingu trudno o zgrabnie sformułowane przywitanie. Zwrot do odbiorcy w wołaczu zanika w komunikatach od naciągaczy. Przywitania rozpoczynają się często od znanego wielu osobom koszmarka językowego: niechlubnego „Witaj!", „Witaj, drogi sprzedawcy!" czy „Witam, zespół OLX przeprasza". Zwyczajowo witać może gospodarz w swoim domu, ale jedyne schronienie, jakie naciągacze oferują swoim ofiarom, to kryjówka dla skradzionych danych i pieniędzy.

Niezgrabnie sformułowane komunikaty to domena phishingowców. Źle użyte bezokoliczniki, błędny szyk, mieszanka różnych języków – na takie cechy charakterystyczne fałszywych komunikatów warto uważać, aby nie paść ofiarą oszustów. Kluczem do sukcesu są świadomość wykorzystywanych przez phishingowców metod, wzmożona ostrożność i językowa czujność.

„JAK WRÓCĘ Z RADOMIA...", CZYLI TAK TRZYMAJ, DROGI UŻYTKOWNIKU OLX-A

Zespół OLX

Jest taka scena w filmie „Hallo Szpicbródka (...)" z 1978 r., w której narzeczony głównej bohaterki zwraca się z pytaniem do krawca Salomonowicza, czy ten byłby łaskaw pożyczyć mu 50 zł. „Może i mógłbym, ale dopiero jak wrócę z Radomia" odpowiada pytany, a ciągnięty dalej za język o to, kiedy się wybiera, ripostuje: „Nie zamierzam". Ten dialog lubi parafrazować w wymianie wiadomości z oszustami część użytkowników OLX-a, a potem chwalić się w przesłanych do nas albo krążących po sieci zrzutach ekranu.

Kiedy jako marka piszemy i mówimy, że bezpieczeństwo użytkowników jest dla nas na pierwszym miejscu, na takim efekcie zależy nam najbardziej. Z OLX-a korzysta 14 mln użytkowników każdego miesiąca. Wymieniają setki milionów wiadomości i pytań, wysyłają do siebie miliony paczek. Oferujemy im narzędzia do bezpiecznych transakcji, ale OLX to tak naprawdę gra zespołowa. Bez pomocy tych, którzy korzystają z naszego serwisu, byłoby nam zdecydowanie trudniej usprawniać jego działanie i wyłapywać podejrzane oferty. Jak grać w naszej drużynie? Oto kilka przykładów:

„Cześć, chciałam zgłosić, że rano było podobne ogłoszenie o sprzedaży dość drogiego markowego swetra, pani kazała zapłacić BLIK-iem, a teraz jest to samo ogłoszenie, te same zdjęcia, ale w innym mieście. Dostałam info od was, że to może być oszustwo i nie wpłaciłam, pozdrawiam, Kasia".

„Brawo, wielki szacun za zgłaszanie podejrzanych ludzi. Potem właśnie OLX dzięki takim akcjom wyśle ostrzeżenie i można się jakoś uchronić przed oszustami!".

„Dzień dobry, dzisiaj dostałem powiadomienie od OLX, że oferta wynajmu nieruchomości może być oszustwem. Jestem z Krakowa, a identyczne było dostępne w Warszawie. Proszę o szybkie zablokowanie gościa".

„Blokujecie, czy co jest z Wami? Przedmiot kradziony albo podpucha! Kto normalny nową konsolę sprzedaje za trzy stówki?! Jeszcze zdjęcie jak z katalogu xD Pozdro, Kuba".

I wreszcie: „Wczoraj wieczorem zakupiłam kuchenkę zabawkową dziecięcą na OLX, pani ze Szczecina. Nie chciała wysłać za pobraniem, więc dokonałam przelewu. Dzisiaj o 7.30 dostałam alert bezpieczeństwa od olx.pl, żeby zaprzestać konwersacji z użytkownikiem, zablokować przelew, jeśli to możliwe, i zgłosić sprawę na policji. Oczywiście ogłoszenie zniknęło z OLX-a. Numer konta był wysłany do mnie na maila przez oszustkę. Potem sprawdziłam też na stronie jakitobank.pl i pod numerem znajdują się dwa komentarze, że to przekręt".

To tylko kilka przykładów z wysyłanych do nas w setkach dziennie wiadomości z grup oraz komentarzy w mediach społecznościowych w reakcji na podejrzane ogłoszenia lub e-maile. Część z nich to odpowiedzi na wysyłane przez nas ostrzeżenia. Część to reakcja na powiadomienia, jakie ukazują się na czacie aplikacji, choćby po próbie wklejenia numeru karty kredytowej lub wpisaniu słów CVC, BLIK albo PIN. Część to odzew na nasze kampanie edukacyjne, np. wiadomości zaczynające się od słów: „Widziałem wasz spot o bezpieczeństwie w sieci. Fajny. A tutaj przesyłam zrzut ekranu, jak jakiś cwaniak chce wydębić ode mnie telefon na fejkowy przelew. Was pozdrawiam, jego nie".

Dziękujemy i też Was wszystkich pozdrawiamy! A oszustów nie.

Tak wygląda przycisk umożliwiający zgłoszenie naruszenia, który jest przy każdym ogłoszeniu na dole po prawej stronie:

Formularz kontaktowy dotyczący pomocy dostępny jest tutaj: https://pomoc.olx.pl/

*Imiona autorów wiadomości i podane przez nich nazwy miast zostały zmienione.

KRZYŻÓWKA

PIONOWO:

(1) początkowa wpłata
(3) inaczej Messenger, Gadu-Gadu, Skype
(4) podstawiona osoba wykorzystywana przez przestępców
(6) nieuczciwe wykorzystywanie sytuacji dla osiągnięcia własnych celów
(7) podszywanie się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji
(8) czynność mająca na celu uwiarygodnienie tożsamości użytkownika internetu
(9) metody i działania mające na celu przekonanie jednostek lub mas do swoich racji
(11) zbiór programów wprowadzonych do komputera
(15) program do zainstalowania w telefonie umożliwiający korzystanie z różnych narzędzi
(17) zespół powołany do reagowania na zdarzenia naruszające bezpieczeństwo w sieci

POZIOMO:

(2) oszustwo lub nadużycie
(5) niechciane wiadomości
(10) program, który naśladuje zachowania użytkowników w sieci
(12) inaczej oszustwo w internecie
(13) kod będący w wyłącznym posiadaniu osoby chcącej się uwierzytelnić
(14) inaczej autoryzacja użytkownika
(16) dodatek do numeru karty bankowej zabezpieczający transakcje
(18) czynność zachodząca między sprzedającym i kupującym
(19) oszuści czekają, aż w niego klikniesz
(20) coś nieprawdziwego, podróbka

1	2	3	4	5	6	7	8	9	10	11		12		13	14	15	16	17

ZGARNIJ NAGRODY!

Rozwiązanie krzyżówki prosimy przesłać na adres e-mailowy Pauliny Rezmer z OLX:

prezmer@olx.pl

Dla pierwszych 10 osób, które prześlą prawidłowe rozwiązanie, czekają nagrody.

HOROSKOP

Baran: Czas sprzyja realizacji marzeń i celów. Podczas zakupów na OLX-ie upolujesz same perełki, ale uważaj! Jeśli ktoś namówi cię na podanie danych karty bankowej, zgłoś to do Obsługi Klienta OLX!

Byk: Poświęć czas na wewnętrzny rozwój. Znajdź chwilę na relaks i spróbuj wyjechać. Uważaj, bo możesz napotkać na swojej drodze pułapki. Nie daj się nabrać oszustom czyhającym na moment twojej słabości. Nigdy nie wpłacaj całej kwoty z góry.

Bliźnięta: Łatwość w nawiązywaniu nowych znajomości może wyprowadzić cię na manowce. Korzystając z OLX-a, rozmowy z użytkownikami prowadź tylko na czacie w aplikacji. Inaczej z pozoru atrakcyjna znajomość może się dla ciebie skończyć wielkim rozczarowaniem.

Rak: W tym miesiącu zawładnie tobą... lenistwo! Nie oznacza to, że masz lekceważyć zasady bezpieczeństwa podczas robienia zakupów w sieci. Uważaj na podejrzane linki przesyłane z niewiadomych źródeł.

Lew: Twoja pewność siebie może cię kiedyś zgubić! W tym miesiącu będziesz jednak w świetnej formie i zanim kupisz cokolwiek na OLX-ie, sprawdzisz staż sprzedającego.

Panna: Twoja obsesja na punkcie doskonałości może przynieść ludziom wymierne korzyści. Widzisz podejrzaną stronę, która tylko udaje OLX-a? Pokaż im, kto tu rządzi! Z godnym siebie uporem zgłoś ją w formularzu na olx.pl/pomoc.

Waga: Zawsze rozważna Waga zastanawia się trzy razy, zanim podejmie decyzję. Tak będzie i w tym miesiącu. Słysząc niepokojące wieści o tzw. phishingu, Waga będzie jeszcze bardziej czujna niż zwykle. I bardzo dobrze!

Skorpion: Z takim temperamentem nikt ci nie podskoczy! A już na pewno nie żaden oszust. Doskonale znasz wszystkie zasady bezpieczeństwa na OLX-ie, dlatego jesteś w stanie przewidzieć każdy ruch przeciwnika, którego (oczywiście) zmiażdżysz.

Strzelec: Ten czas będzie dla ciebie pełen doskonałych ofert i wysokich zarobków. Sprzedając na OLX-ie, uważaj na innych, którzy próbują podszyć się pod firmy kurierskie. Wszelkie próby kontaktu spoza aplikacji odrzucaj z premedytacją.

Koziorożec: W tym miesiącu masz szansę pokazać bliskim swój odważny charakter. Zaproszeniu do przeniesienia komunikacji poza serwis OLX powiedz stanowcze „nie". Twoja determinacja może sprawić, że urośniesz w oczach innych i unikniesz nieplanowanych wydatków. A wiemy, że to pieniądze kochasz najbardziej.

Wodnik: W tym miesiącu twoja niezawodna intuicja przestanie działać. Schowaj dumę do kieszeni i w przypadku próby oszustwa nie działaj samodzielnie, tylko skorzystaj z zasobów Centrum Pomocy OLX. Zobaczysz, wyjdzie ci to na dobre!

Ryby: Niedokończone sprawy będą dawały o sobie znać. Nie przeszkodzi ci to jednak w rozwoju zawodowym. Nie poddawaj się od razu. Trzymaj rękę na pulsie, a wszystko ułoży się po twojej myśli. Uważaj tylko na oferty pracy, w których ktoś prosi cię o skan dowodu. To pułapka!

KURIER SPECJALNY

Redaktor naczelny:
Paulina Rezmer
prezmer@olx.pl

Nadzór merytoryczny:
Ewa Lepczyk-Żerdzicka
Piotr Chochłow

Współpracownicy:
Zespół OLX

Adres:
ul. Królowej Jadwigi 43
61-871 Poznań
www.olx.pl

Wydawca:
dotpr Skowronek, Łaźniewski sp.j.,

Adres:
ul. Jana Henryka Dąbrowskiego 308
60-406 Poznań
www.dotrelations.pl

SEZON NA... LESZCZA. KALENDARIUM OSZUSTÓW

Zespół OLX

Okazji do przekrętów w sieci nigdy nie brakuje. Ale są takie okresy, w których przestępcza aktywność szczególnie się wzmaga. Zwłaszcza sezonowe wydarzenia, będące dla całego świata pretekstem do zakupów, sprawiają, że naciągacze czują się jak ryby w wodzie. Na co i kiedy mogą chcieć nas złowić oszuści?

Styczeń to czas postanowień noworocznych, a dla wielu również czas na zmianę pracy. Wtedy szczególnie wzmożoną aktywność wykazują przestępcy, którzy pod przykrywką atrakcyjnej oferty zatrudnienia oczekują przesłania skanów dowodów, paszportów, prawa jazdy albo zaświadczenia o niepełnosprawności. Mogą też domagać się opłaty za udostępnienie materiałów szkoleniowych lub przesłania danych osobowych pod pozorem uwiarygodnienia kandydata, np. w trakcie rozmowy rekrutacyjnej online. Niestety zbyt często okazuje się to skutecznym wabikiem.

Luty – walentynki są okazją do sprawienia bliskim i kochanym ekskluzywnych prezentów, takich jak biżuteria, perfumy, zegarki czy luksusowe kosmetyki. Ostrożnie! Oszuści mogą chcieć nas skusić „świetnymi okazjami" i produktami z najwyższej półki w najniższych, nierzeczywistych wręcz cenach. Nie dajmy się uwieść.

Maj ze swoim słynnym już długim weekendem to nie tylko grillowanie z przyjaciółmi, lecz także krótkie wypady na łono natury w pogoni za pierwszymi ciepłymi promieniami słońca. Uwaga na szczególnie tanie oferty nieistniejących noclegów! Ta sama przestroga powinna nam towarzyszyć przy planowaniu wakacyjnych wyjazdów. Nim zaczniemy zacierać ręce na gorące letnie okazje i wynajmiemy kilkuosobowy domek z basenem i sauną za 200 zł za dobę, warto najpierw przemyśleć to na chłodno.

Dzień Dziecka, czyli **1 czerwca**, to w kalendarzu rodziców data szczególna, bo kto nie chce sprawić radości swoim pociechom? Ostrzegamy jednak przed topowymi zabawkami w zaniżonych cenach. Inwestycja w Lego jest dziś pewniejsza niż inwestycja w złoto, inwestujmy więc z zimną krwią.

Ci, którzy urlopu nie spędzają na dalekich Malediwach, **w okresie wakacyjnym** często planują urządzanie ogrodu albo tarasu. To okazja do przekrętów na basenach i meblach ogrodowych, trampolinach dla dzieci i narzędziach. Zachowajmy czujność, gdy ktoś zaproponuje nam wysyłkę rattanowych foteli do paczkomatu, kiedy tylko zrobimy mu szybki przelew za pomocą podejrzanego linka.

Wrzesień to ostatni dzwonek dla studentów szukających mieszkania. I choć pandemia nieco zachwiała rynkiem najmu nieruchomości, to u podstaw przekrętu czyhającego na akademicką młodzież wciąż leży ten sam modny patent: „Potrzebna zaliczka w wysokości miesięcznego czynszu na poczet oględzin mieszkania i rezerwacji terminu, bo na pana miejsce już jest 10 chętnych". Wpłacisz i egzamin z czujności koncertowo oblany.

Październik i listopad to czas jesiennych porządków. Coraz częściej korzystamy z pomocy zewnętrznych usługodawców. Zanim jednak wpuścimy pomocników do domu czy ogrodu, sprawdźmy opinię na ich temat i zweryfikujmy wiarygodność firmowych danych.

Podobna reguła dotyczy tych, którzy w miesiącach poprzedzających sezon budowlany (**kwiecień, maj**) i remontowy (dodatkowo **listopad i grudzień**) poszukują fachowców. Prośba o zaliczki przed przystąpieniem do pracy i wymigiwanie się od spisania umowy to dla usługobiorcy sygnały do szybkiej ewakuacji.

Koniec roku jest dla oszustów internetowych czasem złotych żniw. Zapraszają nas do krainy atrakcyjnych prezentów (biżuteria, gry, elektronika, vouchery podarunkowe i bilety) w bardzo atrakcyjnych cenach. Pobudka, nowy smartfon za 200 zł nie istnieje! Kusząco może też wyglądać specjalistyczny sprzęt do uprawiania sportów zimowych oferowany za nieco mniej specjalistyczne pieniądze. Albo uroczy domek w górach na sylwestra ze znajomymi, który możesz mieć już za ułamek rynkowej ceny, jeśli tylko wpłacisz całą kwotę awansem na podany już w pierwszej wiadomości numer konta bankowego. Ach, gdyby tylko była to prawda...

PIŁKARSKI NIKODEM DYZMA. HISTORIA MISTRZA KONTUZJI

Marcin Mój

Ginga – podstawowy ruch w capoeirze, który nadaje płynność i charakterystyczną dynamikę. Niektórzy twierdzą, że to coś więcej. To brazylijski styl życia objawiający się w tańcu, chodzie, podejściu do świata. W Brazylii mówi się, że to nie oni wymyślili piłkę nożną, ale dodali do niej gingę – dlatego jest taka magiczna. Każdy chłopiec urodzony w kraju kawy marzy o byciu zawodowym piłkarzem – tak było również z Carlosem Henrique Raposo, znanym dziś w piłkarskim świecie jako największy oszust w historii piłki nożnej.

Mały cesarz

Raposo dorastał na ulicach Rio de Janeiro. Trenował w młodzieżowej drużynie Botafogo. Wybijając się na tle rówieśników, zyskał przydomek „Kaiser", czyli cesarz – po niemieckim wirtuozie futbolu, Franzu Beckenbauerze. „To nie ja nadałem sobie tytuł Kaisera. Nazwano mnie tak, bo coś w sobie miałem" – mówił po latach piłkarz. Niestety „to coś" z wiekiem zaczęło gasnąć. W nastoletnim wieku Kaiser nie był już dobrze zapowiadającym się piłkarzem, a jednym z wielu. Mimo to nie chciał porzucać marzenia o karierze. Chciał zostać piłkarzem, nie potrafiąc za dobrze grać w piłkę, dlatego postanowił inną metodą przedrzeć się do piłkarskiej elity. Dowiadywał się, w jakich hotelach mają zgrupowania piłkarze brazylijskich drużyn, wynajmował pokoje znajdujące się piętro niżej i organizował imprezy, na które zapraszał gwiazdy. W ten sposób poznał Bebeto, Renato Gaucho czy Romario – przyszłe gwiazdy światowej piłki, które rekomendowały pracodawcom swojego kumpla.

Pokaźne CV

Jego piłkarska droga zaczęła się w meksykańskim Puebla. Tam spędził dwa lata, a następnie wrócił do Brazylii. Jako „doświadczony zawodowiec" spróbował swoich sił w Botafogo, ale po dwóch latach bez zagranego spotkania... kupiło go Flamengo (tak, ten sam klub, do którego przeszedł ostatnio Sousa). Mając „brazylijski Real Madryt" w CV, było już z górki. Po Flamengo „cesarza" witali kibice Bangu AC. Po pobycie w Bangu AC Kaiser trafił do Fluminense, a potem do Vasco da Gama. Po wyczerpaniu prawie wszystkich możliwych opcji na grę w Rio po zawodnika zgłosiło się amerykańskie El Paso Sixshooters. U zmierzchu swojej legendarnej kariery zaliczył jeszcze krótkie kontrakty w dwóch brazylijskich drużynach America FC i Guarana FC. Jego kariera obejmowała 9 klubów, trwała niemal 20 lat i nie doczekała się ani jednego zawodowego spotkania. Takiego CV nie mają niektórzy mistrzowie świata i legendy tej dyscypliny sportu. Nasuwa się jedno pytanie: jak?

Wachlarz kłamstw

Tak naprawdę plan Kaisera był banalnie prosty. Mając wizerunkowe zaplecze i piłkarskie znajomości nabyte w młodości, nie miał problemu z tym, żeby podpisać kontrakt – miał problem z tym, żeby go wypełnić, ale tak naprawdę nigdy nie chciał tego robić. „Podpisywałem umowę, brałem zaliczkę i to mi wystarczało. Nie zamierzałem wypełniać kontaktu. Chciałem jak najszybciej się wyrwać" – tłumaczył zawodnik. Po przyjściu do klubu momentalnie łapał kontuzje. Tamtejsze czasy były idealnym środowiskiem do tego typu oszustw. Wiedza medyczna na temat kontuzji była stosunkowo niewielka – zawodnik mógł udawać i nikt nie mógł zarzucać mu kłamstwa. Poza tym Kaiser wiedział, co robi. Symulował bóle mięśniowe – najtrudniejsze do zdiagnozowania, a fałszywe zaświadczenia o kontuzjach przynosił od lekarza, który tak naprawdę był dentystą. Dodając do tego powszechny brak dostępu do informacji i brak komunikacji między klubami – w każdym kolejnym zespole Raposo mógł tworzyć swoją historię na nowo. Nawet współczesny futbol zna kontrakty, które zdominowały kontuzje. Jeden z najlepszych zawodników świata – Eden Hazard trafił do Realu Madryt w sierpniu 2019 r. Od tamtego czasu miał 15 kontuzji, omijając ponad 60 meczów swojego zespołu. Oczywiście w przypadku Kaisera nie obyło się bez ekstremalnych sytuacji. W filmie dokumentalnym „Kaiser – historia oszusta wszech czasów" piłkarze opisują dziesiątki sytuacji, w których piłkarz był blisko wpadki, ale zawsze udawało mu się wyjść obronną ręką. W jednym z meczów działacze byli tak zdeterminowani, żeby w końcu sprawdzić go w grze, że pomimo narzekań Kaiser miał trafić na boisko. Co zrobił? W trakcie rozgrzewki pobiegł w kierunku trybuny gości, wdał się w bójkę z kibicami przeciwnej drużyny... i otrzymał czerwoną kartkę. „Wszystkie moje kluby świętowały dwa razy. Kiedy mnie kupowały i kiedy się mnie pozbywały" – mówi w dokumencie brazylijski Nikodem Dyzma.

W swojej niemal 20-letniej karierze zawodnik zwiedził 9 klubów na kilku kontynentach. Spełnił swoje sny, zasmakował wszystkiego, co w piłkarskiej karierze najlepsze, poza jednym – graniem w piłkę.