Transkrypcja cyklu audycji „Bezpieczne Złotówki” realizowanego w rozgłośni Radia Złote Przeboje we współpracy z Fundacją THINK! To sześć odcinków rozmów z ekspertami o tym, jak chronić pieniądze przed cyberoszustami.

Odcinek 1. Gość – Karol Bojke

Prowadzący: Szybkie płatności mobilne to jedna z najszybszych i najwygodniejszych metod płacenia za codzienne zakupy. Jednak jak każda inna działalność związana z finansami, nie jest wolna od ryzyka. Jak chronić się przed oszustami i co zrobić, gdy ktoś poprosi nas o podanie kodu do płatności? Na te pytania odpowiada Karol Bojke z CERT Polska. Jak najczęściej wyglądają oszustwa na kody do płatności mobilnych?

Karol Bojke: Oszustwa na szybki przelew to klasyczny przykład socjotechniki. Przestępcy manipulują faktami, podszywają się pod inne osoby lub instytucje, a często też podmieniają kwotę uzgodnionej transakcji. Ich ulubionym sposobem jest wykorzystanie przejętych kont w mediach społecznościowych. Kiedy uzyskają dostęp do takiego konta, masowo rozsyłają do wszystkich znajomych wiadomości z prośbą o szybki przelew. Jako pretekst podają konieczność opłacenia rachunków, niedziałającą kartę płatniczą, która zaskoczyła ich przy kasie w sklepie, albo chęć pożyczenia pieniędzy na parę dni. Jeśli znajomy prosi nas o kod płatności lub przelew, skontaktujmy się z nim za pośrednictwem innego środka komunikacji, na przykład telefonicznie. Jest duża szansa, że nic nie wie o tej prośbie, a rozmowa z nami pozwoli mu zareagować i ochronić też innych swoich znajomych. Jeszcze inni oszuści ogłaszają się jako sprzedawcy towaru, biletów na koncert czy ubrań, a może przecenionej elektroniki. Namawiają na okazję, proszą o kod do płatności, ale próbują finalnie zrealizować transakcję na dużo wyższą kwotę niż umówiona.

Prowadzący: Czy są sytuacje, w których można bezpiecznie przekazać komuś kod płatności przez telefon? Na przykład naszemu dziecku, które chce zapłacić za posiłek w szkole?

Karol Bojke: Jak najbardziej. Nie obawiajmy się korzystać z tej metody przekazywania swoich środków. Kiedy ktoś wykorzystuje podany przez nas kod płatności, dostajemy w aplikacji bankowej prośbę o zatwierdzenie transakcji wraz z jej szczegółami. W tym miejscu dajmy sobie pół minuty na weryfikację. Czy zgadza się kwota? Czy odbiorca rzeczywiście jest tym, do którego powinny trafić nasze pieniądze? Szczególne podejrzenie powinny wzbudzić w nas próby wypłaty pieniędzy z bankomatów. Przestępcy lubią ten mechanizm, bo odbiorca przelewu znika z gotówką i bardzo trudno go potem odnaleźć.

Prowadzący: Co zrobić, jeśli zdamy sobie sprawę, że podaliśmy kod oszustowi?

Karol Bojke: Przede wszystkim nie panikujmy. Samo podanie kodu nie oznacza, że ktoś ma dostęp do naszego konta. Jak już wspomniałem, żeby wyłudzić nasze pieniądze, przestępcy muszą zrealizować transakcję, którą my musimy zatwierdzić. Wystarczy, że odmówimy, żeby nasze środki pozostały bezpieczne. Następnie zgłośmy tę sytuację do właściwej instytucji, tak żeby pomóc chronić innych. Konto oszusta możemy zgłosić administracji portalu, na którym się ogłasza, jego personalia – policji, a jeśli do podania kodu zachęcano nas na

przykład na stronie internetowej, to także do zespołu CERT Polska, czuwającego nad bezpieczeństwem polskiego internetu.

Odcinek 2. Gościni – Klaudia Sibielak

Prowadzący: Powszechnie znana prawda mówi, że pośpiech jest złym doradcą, zwłaszcza gdy w grę wchodzą pieniądze. Klaudia Sibielak, ekspertka od inwestowania z Finax, opowie o tym, jak inwestować, aby nasze oszczędności nie trafiły w ręce oszustów. Dlaczego inwestowanie pod wpływem emocji to nie jest dobry pomysł?

Klaudia Sibielak: Emocje w inwestowaniu są po prostu złym doradcą, bo często prowadzą nas do impulsywnych decyzji, które mają negatywny wpływ na nasze portfele. Dla przykładu: nawet przy niewielkich spadkach my, pod wpływem paniki, możemy sprzedać nasze aktywa po niekorzystnej cenie albo – wręcz przeciwnie – podążając za tłumem w euforii, możemy zacząć inwestować zdecydowanie zbyt ryzykownie. To, o czym warto pamiętać, to że inwestowanie to nie jest sprint, to maraton – czyli liczy się tu chłodna głowa i przemyślana strategia. Jeżeli działamy pod wpływem impulsów, to niestety na ogół będzie to działać na naszą niekorzyść.

Prowadzący: Jak odróżnić prawdę od fałszu? Kiedy powinna zapalić nam się czerwona lampka, że możemy mieć do czynienia z fałszywą ofertą inwestycyjną?

Klaudia Sibielak: Po pierwsze, jeżeli ktoś obiecuje ci, że zarobisz szybko, dużo i bez żadnego ryzyka – po prostu uciekaj. Na rynkach finansowych to po prostu nie jest realne. Uważaj też na nieznane firmy bez licencji. Bądź ostrożny, jeżeli ktoś obiecuje ci gwarantowane zyski albo wywiera presję na szybką decyzję. Najlepiej zawsze sprawdź, kto stoi za daną ofertą i czy podlega odpowiedniemu nadzorowi, na przykład przez Komisję Nadzoru Finansowego.

Prowadzący: Jakie sztuczki stosują najczęściej cyfrowi oszuści, proponując nam fałszywe inwestycje?

Klaudia Sibielak: Oszuści często podszywają się pod znane firmy, kontaktują się wówczas z nami przez komunikatory albo media społecznościowe, a nawet tworzą fałszywe strony internetowe, które mogą wyglądać naprawdę profesjonalnie. Kuszą nas też różnymi niepowtarzalnymi okazjami, gwarantowanym zyskiem albo modnymi tematami, takimi jak na przykład inwestowanie w kryptowaluty albo w sztuczną inteligencję. Lubią też stosować presję czasu po to, by skłonić nas do jak najszybszego podjęcia decyzji, zanim zdążymy jeszcze wszystko dobrze przemyśleć.

Odcinek 3. Gościni – Monika Przestrzelska

Prowadzący: Cyberprzestępcy często liczą na to, że machniemy ręką na drobne straty finansowe. Wyciągają od nas pojedyncze złotówki, na przykład poprzez popularny schemat oszustwa na dopłatę do paczki. Coś, co może być dla nas niewielką kwotą, w rękach przestępców rośnie do ogromnych sum, a wszystko przez efekt skali, w jakiej działają cyfrowi oszuści. O tym, dlaczego liczą oni na naszą bierność, opowie aspirant Monika Przestrzelska z Centralnego Biura Zwalczania Cyberprzestępczości Policji. Dlaczego cyfrowi przestępcy schylają się po niewielkie kwoty? Jednym z popularnych przykładów takich przestępstw jest oszustwo na wynoszącą kilka złotych dopłatę do paczki. Otrzymujemy od oszusta komunikat, że jeśli nie zapłacimy, to paczka do nas nie dotrze.

Monika Przestrzelska: Wiadomość z dopłatą do paczki to chyba już wszystkim znany sposób oszustwa. Był taki czas, gdy te wiadomości oszuści wysyłali masowo, licząc na to, że jakaś część z tych osób rzeczywiście da się po prostu oszukać i zrobi przelew na te parę złotych. Oszuści schylają się po te niewielkie kwoty, ponieważ nie wzbudzają one w nas większych podejrzeń. Przy małej kwocie, a oszukanej większej liczbie osób, robi się już duża suma, dlatego dla oszustów ma to sens. Zgłoszenie kradzieży nawet na niewielką kwotę, jak na przykład 10 zł, ma sens. Każda próba oszustwa, a tym bardziej oszustwo dokonane, powinno być zgłoszone. Nie zgłaszając tego rodzaju incydentów, dajemy przestępcom pewnego rodzaju ciche przyzwolenie na dalszą działalność. Dziś oszukują na niewielką kwotę, a jutro oszukają na większą. Zgłaszając sprawę, w pewnym stopniu przyczyniamy się do ukrócenia przestępczego procederu, ale też możemy uchronić w ten sposób innych.

Odcinek 4. Gość – Robert Stankiewicz

Prowadzący: Internet pełen jest reklam, gwarantowanych zysków i rzekomych ekspertów inwestycyjnych. Jak odróżnić prawdziwą giełdę od oszustwa i inwestować bezpiecznie? O tym opowie Robert Stankiewicz, dyrektor działu komunikacji i marketingu Giełdy Papierów Wartościowych. Jak rozpoznać, że platforma inwestycyjna, na którą trafiliśmy, działa legalnie i rzeczywiście ma związek z Giełdą Papierów Wartościowych?

Robert Stankiewicz: Przede wszystkim należy pamiętać, że Giełda Papierów Wartościowych w Warszawie nie prowadzi działalności maklerskiej ani rachunków papierów wartościowych. Giełda nie oferuje zakupu instrumentów finansowych wprost. Nie dzwonimy do klientów. Nie mamy konsultantów telefonicznych ani elektronicznych, którzy dzwonią i namawiają bezpośrednio na inwestycje na warszawskim parkiecie. Jeżeli ktoś do Państwa dzwoni i podaje się za Giełdę Papierów Wartościowych – uwaga, to jest na pewno oszustwo. GPW nie robi takich rzeczy.

Odcinek 5. Gość – Piotr Mieczkowski

Prowadzący: Coraz częściej słyszymy o oszustwach z użyciem sztucznej inteligencji. Technologia pozwala tworzyć fałszywe nagrania głosowe czy materiały wideo, nierzadko

wykorzystujące wizerunek znanych osób. Takie ataki przybierają na sile, bo AI umożliwia ich masowe i tanie przygotowanie. Cel jest jeden: nasze pieniądze.

Piotr Mieczkowski: Przede wszystkim sztuczna inteligencja przyspiesza tworzenie fałszywych wiadomości, tak zwanych deepfake'ów, czyli realistycznych nagrań głosowych lub wideo, które wyglądają jak prawdziwe. Oszuści podszywają się pod bliskich, celebrytów czy instytucje, by wzbudzić zaufanie. Dzięki AI mogą też masowo generować fałszywe wiadomości czy strony internetowe, które wyglądają profesjonalnie, co czyni oszustwa trudniejszymi do wykrycia.

Odcinek 6. Gościni – Anna Bichta

Prowadzący: Latem oszuści nie biorą urlopu. Liczą, że czas wakacji uśpi naszą czujność. Oferują kuszące oferty miejsc noclegowych, które tak naprawdę nie istnieją, albo chcą nam odsprzedać w promocyjnej cenie bilety na koncert, których w rzeczywistości nie posiadają. Na co uważać na wczasach? Rozmawiamy o tym z Anną Bichtą, prezeską Fundacji THINK!. Co sprawia, że wakacje to złote żniwa cyfrowych oszustów?

Anna Bichta: Wakacje to czas, kiedy najchętniej planujemy wypoczynek i na chwilę zapominamy o codziennych obowiązkach. Chcemy żyć pełnią życia, więc nie myślimy zbyt wiele o niebezpieczeństwach. Jesteśmy bardziej spontaniczni, co sprzyja impulsywnym zakupom. Cyfrowi oszuści o tym wiedzą i potrafią to wykorzystać. Efekty widzimy w policyjnych kronikach. To historie oszustw na fałszywe noclegi, bilety czy oferty sklepów internetowych – i setki, a nawet tysiące straconych złotych.

Ministerstwo Finansów
FUNDUSZ EDUKACJI FINANSOWEJ
think!
Sfinansowano ze środków Funduszu Edukacji Finansowej, którego dysponentem jest Minister Finansów i Gospodarki. Realizatorem Kampanii jest Fundacja Think!