KPP GOSTYŃ

https://gostyn.policja.gov.pl/wl4/profilaktyka/profilatyka-ogolna/182738,OSZUSTWA-INTERNETOWE-JAK-SIE-BRONIC-JAK-POSTEPOWAC-BEDAC-POKRZYWDZONYM.html
2022-11-29, 13:06

OSZUSTWA INTERNETOWE - JAK SIĘ BRONIĆ? JAK POSTĘPOWAĆ BĘDĄC POKRZYWDZONYM?

Globalna sieć komputerowa – Internet stał się nieodłączną częścią naszego codziennego życia. Wykorzystywany jest w pracy, do nauki, wymiany informacji lub jako forma relaksu, czy zabawy. Niestety z Internetu korzystają również osoby, które wykorzystują go do popełniania przestępstw. Za pośrednictwem Internetu, tak jak i w świecie rzeczywistym, popełniana jest cała gama różnego rodzaju przestępstw, jednak użytkownicy Internetu nie zawsze zdają sobie z tego sprawę jak łatwo można stać się ofiarą cyberprzestępczości.

Ofiary cyberprzestępczości to najczęściej ofiary oszustw. Oszustwa internetowe stanowią przeważającą grupę przestępstw, która w bardzo szybkim tempie się rozwija i ewoluuje w coraz bardziej złożone formy. Poniżej opisane są niektóre rodzaje oszustw internetowych, metody działania sprawców oraz sposoby postępowania umożliwiające uniknięcia oszustwa i pozostania jego ofiarą.

Phishing

Przy tego rodzaju oszustwach sprawca posługując się ogólnie dostępnymi usługami internetowymi zmierza do wprowadzenia ofiary w błąd i wyłudzenia wrażliwych danych osobowych lub finansowych, tj. numer karty kredytowej, hasła, loginy, numery PIN. Dane, które pozwalają przejąć posiadane pieniądze, lub przejąć wirtualną tożsamość, co pośrednio może prowadzić też do utraty pieniędzy, a także może narazić ofiarę na utratę dobrego imienia itp. Często ofiara oszustwa dostaje wiadomość e-mail, mówiącą, aby się zalogować i potwierdzić swoje dane bankowe, dane do konta e-mail itd. Sprawcy potrafią tworzyć fałszywe maile, które do złudzenia przypominają oficjalne wiadomości od różnych organizacji i instytucji, takich jak banki, towarzystwa ubezpieczeniowe. Aby zmylić odbiorców, wykorzystują logo organizacji, instytucji czy podmiotu oraz imitują styl i szatę graficzną jej korespondencji. Wiadomość zwykle sugeruje użytkownikowi, aby kliknął odsyłacz w celu wprowadzenia swoich informacji osobistych. Po wejściu na link sugerowany
w korespondencji, nawet bez wprowadzania swoich danych, następuje zainstalowanie na komputerze użytkownika złośliwego oprogramowania wykonującego funkcje zdefiniowane przez sprawców („koń trojański").

W jaki sposób uniknąć tego oszustwa? Jeżeli użytkownik otrzymał wiadomość od firmy, banku lub operatora poczty elektronicznej, z której usług nie korzysta – powinien zachować ostrożność przy jej odczytywaniu lub usunąć taką korespondencję. W przypadku otrzymania wiadomości od nadawcy podającego się za operatora poczty elektronicznej czy banku, w którym użytkownik posiada konto, należy go dokładnie przeczytać. Oszuści często nazywają używane przez siebie strony internetowe wykorzystywane do działań oszukańczych, bardzo podobnie do tych oryginalnych, np. http://twiter.com/ zamiasthttp://twitter.com/. Ponadto jeżeli nadawca prosi o podanie loginu, hasła itp. to również powinno wzbudzić naszą czujność ponieważ żadna z legalnie funkcjonujących firm, czy banków, nie żąda podawania takich informacji! Jeżeli mamy wątpliwości co do autentyczności wiadomości należy sprawdzić ją na oficjalnej stronie firmy, wpisując jej adres w wyszukiwarce, nigdy za pomocą linku podanego w otrzymanej wiadomości! Należy pamiętać, że przestępcy zainteresowani są wszelkiego rodzaju danymi, nie tylko związanymi z systemami płatności internetowych. Dlatego oszuści wykorzystując wyżej opisane metody wyłudzają nasze dane dotyczące kont poczty elektronicznej, portali społecznościowych, czy też gier on-line.

Kradzież tożsamości oraz „pranie pieniędzy”

Do tego typu przestępstw dochodzi często poprzez przesłanie do użytkowników ofert atrakcyjnej pracy. Sprawcy zazwyczaj oferują wysokie wynagrodzenia lub proponują pracę nie wymagającą od przyszłych „pracowników” dużego wysiłku. Oferty pracy przychodzą na adresy mailowe w postaci spamu lub ogłoszeń, itp. Ofiara wysyła swoje CV, kopię dokumentów tożsamości, numer swojego konta bankowego i telefon kontaktowy. Zdarzają się nawet przypadki gdzie oszust wymaga od aplikantów założenia konta bankowego na swoje dane osobowe, a następnie wysłanie otrzymanej karty bankomatowej wraz z kodem PIN. Jeżeli użytkownik spełni wymagania, oszust ma wszystko co potrzebne aby posłużyć się tożsamością ofiary do popełniania innych przestępstw. Po wyłudzeniu tych informacji oszust może dalej wykorzystywać nieświadomość użytkownika. W przypadku fałszywych ofert pracy, zadaniem ofiary jest zazwyczaj przesyłanie pieniędzy, wpływających na konto, do wskazanych przez oszustów osób czy banków. Przy czym przesyłanie pieniędzy odbywa się za pośrednictwem systemu płatności uniemożliwiającego identyfikację odbiorcy, np.Western Union. Ofiara jest przekonana, że pieniądze pochodzą z legalnie działających firm, przesyła pieniądze w żądane miejsce za co pobiera prowizję. Ofiary nie zdają sobie sprawy, że uczestniczą w procesie tzw. „prania pieniędzy”, pochodzących z przestępstwa. Slangowo osoba zajmująca się przesyłaniem pieniędzy nazywa się *money mule (muł pieniężny)* -takie działanie w myśl przepisów polskiego prawa również jest karalne.

Fałszywe oferty pracy wykorzystywane są również do wyłudzania pieniędzy. Odbywa się to w podobny sposób. Oszust wysyła bardzo korzystną ofertę pracy za granicą. Ofiara odpowiada na ofertę, bardzo łatwo przechodzi rekrutację,
a następnie ma zgłosić się do pracy. Oszust zapewnia, że wszystko jest już załatwione, prosi jedynie o wpłacenie niewielkiej kwoty np. na zakup biletu lotniczego, wykupienia wizy, pozwolenia na pracę czy opłacenia wynajętego mieszkania. Przestępstwo takie jest formą „oszustwa nigeryjskiego”.

Jak się chronić przed kradzieżą tożsamości? Przede wszystkim, jak zawsze trzeba zachować zdrowy rozsądek. Nie można ufać ofertom firm, które dają bardzo atrakcyjne zarobki, przy minimalnym nakładzie pracy np. wykonywanie przelewów
w zamian za prowizje. To oszustwo – „prania pieniędzy”, w którym stajemy się współsprawcą i możemy za to ponieść odpowiedzialność! Nie można odpowiadać na maile, które są spamem, gdyż uczciwi pracodawcy nie korzystają z tego typu działań w procesie rekrutacji. Nie należy wysyłać swojego CV nieznanym firmom a tym bardziej szczegółowych danych swoich kart kredytowych. Należy zwracać uwagę na adres e-mail,czy należy rzeczywiście do wskazanej w wiadomości firmy, ewentualnie kto jest właścicielem strony internetowej podanej w ogłoszeniu. Nie można poprzestawać jedynie na kontakcie drogą poczty elektronicznej. W przypadku ofert pracy wskazanym jest kontakt telefoniczny i osobisty w siedzibie firmy. Zazwyczaj w procesie rekrutacji firmy organizują rozmowy kwalifikacyjne i dopiero po tym etapie podejmują decyzje o zatrudnieniu pracownika. Ponadto trzeba zwracać uwagę czy firma podaje adres swojej siedziby, numery NIP, REGON. Są to dane, które można sprawdzić i potwierdzić ich autentyczność. Można też sprawdzić opinie internautów o firmie na różnych forach – często tam właśnie demaskowani są oszuści.

Fałszywe oferty kupna/sprzedaży

Oszustwa dokonywane za pośrednictwem ofert kupna/sprzedaży są jedną z najstarszych metod wyłudzania pieniędzy. Najczęściej oszuści zamieszczają bardzo atrakcyjną finansowo ofertę kupna np. samochodu lub motocykla na portalu aukcyjnym. Ofiara kontaktuje się z oszustem w celu dokonania zakupu, a oszust chce otrzymać pieniądze jak najszybciej poprzez Western Union. Odbiór osobisty nie jest możliwy, gdyż oszust bardzo często przebywa właśnie za granicą i zależy mu
na szybkiej sprzedaży samochodu. W celu uwiarygodnienia swojej oferty, oszuści proponują dokonanie transakcji poprzez zaufaną firmę pośredniczącą tzw. „Escrow Service”, która ma gwarantować dostawę samochodu do klienta. Przy czym firma „Escrow Service” nie istnieje, jest stworzona przez oszusta. Ofiara wysyła pieniądze i na tym kontakt się urywa.

Drugą wersją tego oszustwa (choć dużo rzadszą) jest zamiar dokonania przez oszusta zakupu np. samochodu, bądź

innego towaru jaki potencjalna ofiara oferuje do sprzedaży przez portal ogłoszeniowy lub aukcyjny. Schemat jest bardzo podobny. Oszust prosi o przesłanie towaru za granicę i proponuje zabezpieczenie transakcji poprzez Escrow Service – firmę pośredniczącą, gwaranta bezpiecznej transakcji. Ofiara dostaje maile od fałszywego Escrow Service, informujące że wpłata została dokonana i można wysyłać towar. Oczywiście pieniądze nigdy nie docierają do ofiary. Czasem pokrzywdzeni otrzymują wiadomości e-mail z darmowych skrzynek mailowych, imitujących znane instytucje bankowe.

Jak uniknąć tego oszustwa? Nie wierzyć w super oferty! Oferty sprzedaży samochodów w zaniżonej cenie nie odpowiadającej wartości rzeczywistej powinny wzbudzić naszą podejrzliwość. Zawsze należy dążyć do kontaktu osobistego
i możliwości obejrzenia auta. W żadnym wypadku nie wysyłać pieniędzy „z góry", za jakikolwiek towar poprzez Western Union, Money Gram, czy do niesprawdzonego Escrow Service. Tak jak i w innych przypadkach należy dokonać wszelkich możliwych sprawdzeń osoby sprzedającej, czy firm pośredniczących w sprzedaży.

Oszustwo nigeryjskie - tzw. oszustwo 419

Oszustwo nigeryjskie (z ang. 419 Fraud, West African Fraud) - oszustwo na zaliczkę jest znane od XVI wieku, wówczas znane było pod nazwą Listu Hiszpańskiego Więźnia, a do jego popełnienia wykorzystywano pisanie i wysyłanie listów. Obecnie oszuści wykorzystują w tym celu pocztę elektroniczną. Rozsyłają wiadomości, w których piszą, że znaleźli się w bardzo trudnej sytuacji (pomysłowość jest zadziwiająca, potrafią podawać się za byłych ministrów, prawników czy nawet naszych dalekich krewnych) i proszą o pomoc w podjęciu dużej sumy pieniędzy, czy też spadku. Ofiara jest zapewniana, że otrzyma dużą część przedmiotowej kwoty w zamian za wpłacenie kwoty na np. opłaty skarbowe czy prawników prowadzących sprawę spadkową. Jest to jedna z wielu form tego oszustwa.

Jak sie chronić przed oszustwem? Przede wszystkim nie odpowiadać na takie wiadomości, nie wierzyć w możliwość łatwego zdobycia majątku „dalekich krewnych", usuwać z konta korespondencję spamową oraz zachować środki ostrożności opisane powyżej. Więcej informacji na temat tego typu oszustw można uzyskać z opracowania pt. „Jak uniknąć oszustwa nigeryjskiego" -http://www.policja.pl/portal/pol/1218/39219/Jak_uniknac_quotoszustwa_nigeryjskiegoquot.html

Oszustwo z wykorzystaniem „SMS".

Proste oszustwo polegające na wyłudzeniu pieniędzy od osób, które za skorzystanie z usług dostępnych na różnego rodzaju stronach internetowych płacą wysyłając wiadomość tekstową SMS. Internauci otrzymują wiadomość e-mail zachęcającą np. do wykonania testu na inteligencję i sprawdzenia swojego IQ. Aby otrzymać rozwiązanie testu należy wysłać płatną wiadomość SMS, której cena nie jest jasno sprecyzowana np. wymaga się od użytkownika aby zachował ściśle określony, kilkuetapowy sposób wysłania wiadomości. W efekcie rachunek za tę usługę zaskakuje niemile. Kolejny przykład to wysyłanie e-kartek. Cena za wysłanie takiej kartki nie jest wysoka, wynosi kilkadziesiąt groszy. Za wysłanie płaci się SMS-em, który w rzeczywistości kosztuje użytkownika nie kilkadziesiąt groszy ale kilkadziesiąt złotych. Powodem tego jest zapis w regulaminie, według którego użytkownik płaci za sto takich kartek, o czym nie miał pojęcia.

Jak walczyć z oszustwem? Należy zawsze czytać regulamin! W regulaminie muszą być podane dokładne warunki użytkowania, sposoby i terminy płatności oraz cennik usług. Autor takiej strony (pod warunkiem, że nie jest to strona założona
na kilka dni) liczy na to, że użytkownicy akceptują regulamin bez jego czytania. Kartka kosztuje kilkadziesiąt groszy, ale dopiero w regulaminie napisane jest, że użytkownik zgadza się na automatyczny zakup większej ilości kartek np. 100 sztuk. Brak zapoznania się z treścią regulaminu skutkuje brakiem podstaw do roszczeń z tytułu strat finansowych.

Oszuści Internetowi cały czas prześcigają się w tworzeniu nowych sposobów wyłudzania danych osobowych, czy pieniędzy. Często wykorzystują sprawdzone wcześniej metody, wprowadzając jedynie niewielkie zmiany, które usypiają czujność użytkowników Internetu. Oto kilka przykładów:

- Oszustwa na tzw. „Wygraną w loterii”- są podobne do oszustwa nigeryjskiego. Użytkownik otrzymuje wiadomość e-mail z informacją, o rzekomej wygranej w loterii i prośbą o dane osobowe w celu przekazania zwycięzcy wysokiej nagrody. Tak jak w przypadku oszustwa nigeryjskiego - ofiary proszone są o zaliczkę na pokrycie opłat bankowych oraz w niektórych przypadkach również o dane osobowe itp. Podane przez użytkowników dane mogą być ponadto wykorzystane do kradzieży tożsamości i dokonania innych przestępstw;

- Oszustwo na tzw. odszkodowanie: przestępstwo bazujące na „oszustwie nigeryjskim”. Użytkownik otrzymuje wiadomość e-mail informującą o rzekomym utworzeniu funduszu wypłacającego odszkodowania ofiarom oszustwa nigeryjskiego. Ofiara może otrzymać wysokie odszkodowanie, ale tak jak w przypadku klasycznego oszustwa nigeryjskiego, musi oczywiście wpłacić niewielką kwotę manipulacyjną;

- Oszustwa na tzw. „zakochaną dziewczynę”, z użytkownikiem adresu e-mail, kontaktuje się osoba podająca się za młodą kobietę, pochodzącą z jednego z krajów, np. zza wschodniej granicy. Następnie po wymianie korespondencji kobieta wyznaje,
że jest bardzo zakochana i chce jak najszybciej przyjechać do kraju ofiary. W ostatniej chwili okazuje się, że młoda kobieta nie ma pieniędzy na podróż. Prosi więc o gotówkę na opłacenie biletów lotniczych, wizy itp. Po wpłaceniu pieniędzy kontakt się urywa.

Jak widać oszuści Internetowi potrafią być bardzo pomysłowi i bezczelni. Jednak niektóre metody wyłudzania danych osobowych, czy pieniędzy stosowane są niezmiennie przy wielu rodzajach oszustw. Czasami oszustwo rozpoznamy nie
na podstawie informacji zawartych w wiadomości e-mail, ale sposobu, w jaki wiadomość została napisana, oraz rozkładu tekstu. Taka szybka analiza otrzymanej wiadomości może uchronić przed niepotrzebnymi problemami. Dlatego należy zwracać uwagę na to czy otrzymana wiadomość jest zaadresowana indywidualnie na nasze dane, czy jest to masowa wysyłka do wielu osób. Należy również zwrócić uwagę na nadawcę wiadomości, czy jest to znany nam adres, czy pochodzi od firmy, która podaję się jako jej nadawca. Żadna poważna firma nie wysyła wiadomości e-maili z darmowego konta pocztowego, np. gmail.com. Oszuści w celu przyciągnięcia uwagi użytkownika niektóre ze słów piszą wielkimi literami lub świadomie stosują błędną pisownię aby obejść zabezpieczenia antyspamowe.

Postępowanie osoby pokrzywdzonej

Osoba, która stała się ofiarą oszustwa internetowego (cyberprzestępstwa) ma prawo złożyć zawiadomienie o popełnieniu przestępstwaw jednostce Policji lub w prokuraturze, najlepiej najbliższej dla miejsca zamieszkania lub miejsca,
w którym w danym momencie się znajduje. Ze względu na możliwość utraty lub zniszczenia danych informatycznych zawiadomienie o popełnieniu tego typu przestępstwa, należy złożyć możliwie w jak najkrótszym czasie od momentu jego ujawnienia. Zwiększa to szanse organów ścigania na zabezpieczenie kompletnego materiału dowodowego i ustalenie sprawcy.

Na jakie dane i informacje powinna zwrócić uwagę osoba pokrzywdzona? W pierwszej kolejności dane dotyczące domeny (adresu strony www., adresu e-mail), na której pokrzywdzony znalazł ofertę. W przypadku portali aukcyjnych podstawową rzeczą jest zebranie wszelkich danych dotyczących przedmiotu kupna/sprzedaży oraz osoby sprzedającej. A więc ustalenie numeru aukcji (ewentualnie danych charakterystycznych dotyczących sprzedawanego przedmiotu zamieszczonych w opisie), daty rozpoczęcia i zakończenia aukcji, daty przystąpienia do aukcji, ceny i opisu przedmiotu aukcji, itp. Następnie wszystkie dane osobowe i kontaktowe podane przez sprzedającego, tj. imię i nazwisko, adres zamieszkania lub prowadzenia działalności (NIP, REGON), numery telefonów, kont bankowych, login (nazwa użytkownika), adres poczty elektronicznej (identyfikator użytkownika komunikatora GaduGadu, Skype). Znaczenie ma również sposób w jaki pokrzywdzony logował się na stronie przedmiotowej aukcji, czy np. był to znany portal aukcyjny, czy przekierowanie z linku zamieszczonego w treści otrzymanej wiadomości. Pokrzywdzony powinien zabezpieczyć ten link np. poprzez wydrukowanie dokładnego adresu podanego przez sprawcę. Jeżeli w trakcie trwania aukcji lub po jej zakończeniu pokrzywdzony kontaktował się ze sprawcą, wówczas powinien zachować treść korespondencji aby było możliwe ustalenie kiedy i w jaki sposób była prowadzona korespondencja (adres e-mail, komunikatory internetowe,

wiadomości tekstowe SMS). Jeżeli pokrzywdzony wpłacił pieniądze, należy zachować wszelką dokumentację potwierdzającą w jaki sposób, kiedy i gdzie dokonano płatności. Do składanego zawiadomienia pokrzywdzony powinien załączyć wydruki: strony głównej aukcji, zdjęć zamieszczonych na stronie, danych i komentarzy dotyczących sprzedającego (ewentualnie strony sprzedającego), wydruk korespondencji, potwierdzenia wpłaty itp. Przy wykonywaniu wydruków korespondencji elektronicznej należy pamiętać by były one wykonane z uwzględnieniem nagłówka rozszerzonego (właściwości/źródła) wiadomości, który wskazuje „wirtualną" jej drogę. Jak widać pokrzywdzony może we własnym zakresie zabezpieczyć wiele danych dotyczących sprzedającego. Informacje uzyskane od pokrzywdzonego, już w momencie składania zawiadomienia, mają decydujący wpływ na dalsze postępowanie dowodowe i wykrycie sprawcy przestępstwa.

Podsumowując, użytkownicy Internetu powinni przestrzegać kilku prostych zasad bezpieczeństwa:

1. *Należy korzystać z programu antywirusowego, regularnie aktualizowanego, co zapewni skuteczną ochronę przed wieloma różnymi zagrożeniami internetowymi (wirusami, robakami, trojanami itp.).*

2. *Nie należy otwierać linków lub załączników podanych w wiadomościach e-mail, które wzbudzają wątpliwości, ponieważ mogą one zawierać szkodliwe oprogramowanie lub będą łączyły nas z fałszywymi adresami służącymi do wyłudzenia pieniędzy lub kradzieży tożsamości.*

3. *Wszelkich płatności bankowych dokonywać z wykorzystaniem protokołu https (oznaczony ikoną w kształcie kłódki), który zapewnia bezpieczeństwo transmisji danych. Warto też wyświetlić certyfikat poświadczający bezpieczną transmisję danych, gdyż bardziej wyrafinowani sprawcy przestępstw potrafią użyć protokołu https, ale nie posiadają certyfikatu bezpieczeństwa.*

Cyberprzestępcy stosują odpowiednio sformułowane zwroty lub tworzą bardziej rozbudowane i złożone fabuły w celu wzbudzenia zaufania. Oszuści wykorzystują łatwowierność, chęć pomocy innym, chęć szybkiego wzbogacenia, pośpiech, czy ciekawość. Należy pamiętać, że wyłącznikiem logicznego myślenia i czujności jest najczęściej chciwość. Przede wszystkim musimy być jednak świadomi tego, że bezpieczeństwo w wirtualnej przestrzeni zależy od samych jej użytkowników. Nie pomogą nam żadne zabezpieczenia systemowe jeżeli sami nie zachowamy należytej ostrożności i zdrowego rozsądku.

Opracowano:

Wydział Wsparcia Zwalczania Cyberprzestępczości

Biura Kryminalnego

Komendy Głównej Policji