„Bezpieczeństwo w sieci” – artykuł przygotowany w ramach dotacji celowej dla Powiatu Wieruszowskiego.

Omawiając temat bezpieczeństwa w sieci musimy zastanowić się nad wszystkimi czyhającymi na użytkownika niebezpieczeństwami. W poniższym artykule przedstawimy Państwu podstawowe zagrożenia, oraz sposoby jak je rozpoznać i prawidłowo na nie zareagować, tak aby to bezpieczeństwo sobie zapewnić.

Podstawowe oszustwa w sieci to „spam” i „phishing” – masowe rozsyłanie wiadomości email i „łowienie nas na wędkę” oszustów wyłudzających dane.

Celem takich wiadomości jest uzyskanie dostępuo kont użytkowników lub do ich numerów kart płatniczych, wyłudzenie pieniędzy, kradzież tożsamości.

Przedstawię kilka najpopularniejszych obecnie sposobów dokonywania tych oszustw.

1. Fałszywe powiadomienia dotyczące mediów społecznościowych

Na naszej skrzynce lub komunikatorze pojawiają się :

- fałszywe wiadomości od znajomych,

- powiadomienia o umieszczeniu Waszego zdjęcia i konieczności potwierdzenia tego umieszczenia,

- informacje mające wzbudzić strach, obawę – np. o zauważeniu podejrzanej aktywności na portalu

Pojawia się link do kliknięcia.

Po kliknięciu w link pojawia się strona do złudzenia przypominająca stronę nam znajomą np. portalu internetowego – pojawiają się okienka w których powinniśmy wpisać login i hasło.

My wpisujemy – a oszuści już nimi dysponują.

Tym sposobem sami podajemy oszustom nasze dane, które pozwalają przejąć posiadane przez nas na rachunkach pieniądze lub **przejąć wirtualną tożsamość**, co pośrednio może prowadzić również do utraty pieniędzy, a także może narazić ofiarę oszusta na utratę dóbr osobistych, choćby dobrego imienia itp.

Jeżeli zdążymy się zorientować – jedynym „ratunkiem” jest jak najszybsza zmiana haseł w prawdziwym portalu.

2. Fałszywe powiadomienia z popularnych serwisów i od sprzedawców

W tym oszustwie pojawia się spam, czyli rozsyłanie masowo e-maili, które dotyczą m.in. :

- sklepów internetowych,
- usług transportowe (popularne były informacje o linkach do przesyłki kurierskiej, o konieczności dopłaty faktury za taką przesyłkę)
- strony umożliwiające rezerwację – np. usług hotelowych
- platformy multimedialne
- strony z ofertami pracy i innych usług internetowych

System działa każdorazowo tak samo – dla przeciętnego użytkownika strona jest nieodróżnialna od oryginalnej, proszeni jesteśmy o login i hasło i tym samym dajemy przestępcom narzędzie do tego żeby mogli nas okraść.

Pojawiają się faktury z możliwością opłaty – np. faktury za telefon komórkowy – trzeba każdorazowo sprawdzić czy wiadomość pochodzi od naszego dostawcy usług. Gdy dochodzi do przekierowania na stronę banku należy sprawdzić czy połączenie jest szyfrowane (czy znajduje się kłódka przed adresem strony).

3. Wyłudzanie danych bankowych

W tym przestępstwie celowniku jest Wasz rachunek bankowy i powiązane z nim karty bankowe a w efekcie pozbawienie Was środków na tym rachunku.

Pojawia się fałszywa wiadomość, łudząco podobna do wiadomości oryginalnejz banku.
Również w tym przypadku wiadomość ta ma wzbudzić w nas obawę – tematyka dotyczy podejrzanej aktywności na koncie, podejrzanej transakcji kartą, koniecznością potwierdzenia tożsamości.

Znowu proszeni jesteśmy o podanie naszych danych numeru karty, numeru CVV/CVC, daty ważności karty. Podanie tych danych jest równoznaczne

z podaniem danych do naszych finansów złodziejom, to tak jakbyśmy dali złodziejowi klucz do naszego domu.

4. Oszustwo na dziedzica, „nigeryjskiego księcia", na spadek

W tym rodzaju przestępstwa otrzymujemy e-mail z obietnicą **zdobycia fortuny** od krewnego lub prawnika działających w imieniu zmarłego milionera w zamian za dokonanie „drobnej" płatności z góry, za czynności kancelaryjne.

W mojej ocenie oszustwo to jest łatwiejsze do rozpoznania, ponieważ treść samego pisma nie jest bardzo wiarygodna. Z reguły wiemy czy wśród krewnym mamy bogatych zagranicznych krewnych, e-maile napisane są językiem nie do końca poprawnym gramatyczne.

W celu odebrania spadku, najpierw należy tym „prawnikom wysłać szczegółowe informacje na swój temat (informacje odnośnie paszportu, danych konta itp.) oraz „niewielką kwotę" na załatwienie formalności.

Skutek – najmniejszy i najłagodniejszy to **przepadek** wpłaconej kwoty.

Niestety im więcej danych ujawniamy tym większe niebezpieczeństwo że zakres przestępstwa będzie większy i bardziej dla nas dotkliwy.

5. Oszustwo z ofertą atrakcyjnej pracy

Oszustwo to polega na przesłaniu na adres e-mail oferty bardzo atrakcyjnej pracy. Sprawcy zazwyczaj oferują wysokie wynagrodzenia lub proponują pracę nie wymagającą od przyszłych „pracowników" dużego wysiłku. Oferty pracy przychodzą na adresy e-mailowe w postaci spamu lub ogłoszeń, itp. Ofiara wysyła swoje CV, **kopię dokumentów tożsamości**, numer swojego konta bankowego i telefon kontaktowy.

Pracodawca oferuje atrakcyjną pracę, ofiara przechodzi proces rekrutacji i otrzymuje wymarzona pracę, najczęściej za granicą. Dalej pracodawca prosi jedynie o „wpłacenie niewielkiej kwoty" np. na zakup biletu lotniczego, wykupienie wizy, pozwolenia na pracę czy opłacenia wynajętego mieszkania. Po wpłaceniu pieniędzy oczywiście można się z nimi pożegnać, ponieważ na tym kończy się kontakt z „pracodawcą".

6. Fałszywe oferty sprzedaży

Na czym polega takie oszustwo ?

Najczęściej oszuści zamieszczają bardzo atrakcyjną finansowo ofertę sprzedaży np. samochodu, sprzętu komputerowego, powystawowego, drogiego aparatu fotograficznego na portalu aukcyjnym. Ofiara kontaktuje się z oszustem w celu dokonania zakupu. Odbiór osobisty nie jest możliwy,

a oszust przesyła jedynie zdjęcia i informuje ofiarę że przebywa właśnie za granicą i zależy mu na szybkiej sprzedaży.

Gdy ofiara się waha, żeby się uwiarygodnić swoje działaniaoszust proponuje dokonanie transakcji poprzez „zaufaną firmę pośredniczącą". Firma ta ma gwarantować dostawę do klienta. Gdy próbujemy sprawdzić taką firmę i wchodzimy na jej stronę wszystko wygląda bardzo wiarygodnie, i solidnie. A na stronie jest dużo pozytywnych opinii. Niestety wszystko to jest przygotowane przez sprawców jako dekoracja do oszustwa.

Ofiara wysyła pieniądze i na tym kontakt się urywa.

7. Naruszenie praw autorskich

Formą zagrożenia bezpieczeństwa w sieci może być również naruszenie naszych dóbr autorskich godnie z ustawą przedmiotem prawa autorskiego jest każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od swojej wartości, przeznaczenia i sposobu wyrażenia.

Naruszenie tych praw ukrywa się najczęściej pod popularnym pojęciem „piractwa" i zagrożone jest zarówno od strony prawa karnego jak i prawa cywilnego (możliwość dochodzenia odszkodowania).

Jak się zachować gdy zdarzają się takie sytuacje?Jak się zachować po otrzymaniu oszukańczego e-maila?

- Gdy otrzymasz wiadomość e-mail z powiadomieniem od jakiejś firmy czy serwisu, sprawdź, czy została ona wysłana z poprawnego adresu.
- Jeżeli np. bank potrzebuje od nas danych i mamy wątpliwość co do nadawcy tej wątpliwości można do banku pójść lub zadzwonić i wyjaśnić sprawę – często wtedy dowiadujemy się, że bank nie wysyłał do nas żadnych wiadomości
- Gdy klikniesz łącze w takiej wiadomości, upewnij się, że przechodzisz na prawdziwą stronę, a nie specjalnie spreparowaną.
- Najlepiej usunąć podejrzane wiadomość nie otwierając.
- **Pamiętacie właściwie żadna z legalnie funkcjonujących firm, czy banków, nie żąda podawania takich informacji drogą e-mail !**

Jak rozpoznawać cyberoszustwa i jak reagować?

- **Wyłudzenie danych do rachunku bankowego – karty płatniczej -** należy jak najszybciej zastrzec dane w banku, zmienić hasła do rachunku , uruchomić „alert kredytowy" który zabezpieczy nas przed zaciągnięciem pożyczki przez oszusta na nasze dane -– jeżeli zrobimy to szybko jest szansa na zabezpieczenie.

Proszę pamiętać, że w przypadku jeżeli **dobrowolnie udostępnimy** komuś nasze dane do logowania, dane do karty czy PIN, lub otworzymy

podejrzany załącznik i padniemy ofiarą przestępstwa – to najczęściej odpowiedzialność **banku będzie całkowicie wyłączona** i nie odzyskamy naszych pieniędzy.

- **oszustwa związane z procesem rekrutacji** - Właściwie żaden pracodawca nie wymaga od pracownika wcześniejszej wpłaty na jego konto. Są pracodawcy oferujący prace za granicą - najczęściej mają biuro w Polsce, tu przeprowadzają proces rekrutacji, są wpisane do KRS lub Ewidencji Działalności Gospodarczej
- **Oszustwa związane z nabyciem spadku po bogatym krewnym** – gdyby to była prawda to firma prawnicza bezpośrednio się z Wami skontaktuje ☺ i przedstawi stosowne dokumenty. Nie należy przekazywać danych osobowych i środków finansowych.
- **Z wielką uwagą i ostrożnością należy podchodzić do przesyłania dużych kwot za zakupy przez niezabezpieczone transakcje** – są serwisy w których transakcje są ubezpieczone a sprzedawcy są zarejestrowani – żaden serwis nie jest w stanie zapewnić w 100 % bezpieczeństwa, jest ono jednak zminimalizowane
- **Nie należy płacić z góry za „wielkie okazje”** gdy nie macie Państwo możliwości zweryfikowania kontrahenta, czy choćby obejrzenia towaru – istnieje duże ryzyko że takie ukrywanie się sprzedawcy spowodowane być może jego nieuczciwymi zamiarami w transakcji

Co zrobić gdy padniemy ofiarą takiego przestępstwa:

- jak najszybciej zmienić hasło (jeżeli jest to jeszcze możliwe),

- niezwłocznie należy zainterweniować w banku, jak najszybciej zastrzec kartę, zablokować dostęp do rachunku, włączyć „alert kredytowy”

- każdy 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.

W zależności od kwoty jakiej oszustwo dotyczy może być ono wykroczeniem (do 500 zł) lub przestępstwem (powyżej 500 zł).

Należy zgłaszać wszelkie czyny oszustów, nawet jeśli kwota jakiej ono dotyczy nie jest bardzo duża, dlatego że tym samym zwiększamy prawdopodobieństwo ich wykrycia i uniemożliwienia dalszego popełniania przestępstw.

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.

Należy pamiętać o zabezpieczeniu dowodów:

- wydrukować e-mail, link do strony, dane kontaktowe, dokumentację potwierdzającą dokonanie płatności, im więcej tych danych mamy i przekażemy organom ścigania, tym większa szansa na ujęcie i ukaranie sprawcy.

Przede wszystkim jednak należy w wielką ostrożnością podchodzić do wiadomości otrzymywanych z nieznanych źródeł, do załączników w nieznanym formacie, do informacji o „wielkich okazjach" i spadkach po nieznanych wujkach milionerach.

W przypadku problemów prawnych, potrzeby pomocy zapraszamy do korzystania z punktów nieodpłatnej pomocy prawnej i nieodpłatnego poradnictwa obywatelskiego.

Na stronie https://darmowapomocprawna.ms.gov.pl/znajduje się prosta wyszukiwarka w której znajdziecie Państwo wszystkie dostępne w Polsce punkty tej pomocy.