Bezpieczeństwo w sieci

ZADANIE JEST FINANSOWANE Z BUDŻETU PAŃSTWA W RAMACH DOTACJI CELOWEJ PRZEKAZANEJ MIASTU PIOTRKÓW TRYBUNALSKI

OPRACOWANIE WYKONAŁA

FUNDACJA MŁODZI LUDZIOM

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

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

Poniżej omówionych zostanie kilka najpopularniejszych obecnie sposobów dokonywania oszustw.

Należy jednak pamiętać, że nie jest to katalog zamknięty i korzystając z sieci należy ciągle zachowywać czujność i zdrowy rozsądek, ponieważ kreatywność przestępców jest bardzo duża i ciągle pojawiają się nowe metody 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 transportowych (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. Wyłudzenie danych bankowych

W tym przestępstwie na 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 oryginalnej z banku.

Również w tym przypadku wiadomość ta ma wzbudzić w nas obawę – tematyka dotyczy podejrzanej aktywności na koncie, podejrzanej transakcji kartą, konieczności 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.

- Oszustwo to powinno być łatwiejsze do rozpoznania, ponieważ treść samego pisma nie jest bardzo wiarygodna. Z reguły wiemy czy wśród rodziny mamy bogatych zagranicznych krewnych, e-maile napisane są językiem nie do końca poprawnym gramatyczne.

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

- Skutek – najmniejszy i najłagodniejszy to **utrata** 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 niewymagającą 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 wymarzoną pracę, najczęściej za granicą. Dalej pracodawca prosi jedynie o „wpłacenie niewielkiej kwoty” np. na zakup biletu lotniczego, wykupienie wizy, pozwolenia na pracę czy opłacenie wynajętego mieszkania. Po wpłaceniu pieniędzy kontakt
z „pracodawcą” urywa się.

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, oszust 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 wszystkie te działania mają na celu uwiarygodnienie oszustwa.

- Ofiara wysyła pieniądze i na tym kontakt się urywa.

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 przestępstwa w 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 dotyczą nie jest wysoka. Dzięki takim działaniom oczywiście 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 takich danych mamy i przekażemy organom ścigania, tym większa szansa na ujęcie i ukaranie sprawcy.
- Przede wszystkim jednak, należy z wielką ostrożnością podchodzić do wiadomości otrzymywanych z nieznanych źródeł, do załączników o nieznanym formacie, do informacji o „wielkich okazjach" i spadkach po nieznanych osobach.
- W przypadku problemów prawnych i potrzeby pomocy zapraszamy do korzystania z punktów nieodpłatnej pomocy prawnej i nieodpłatnego poradnictwa obywatelskiego.