Bezpieczne Pokolenia

Bezpieczeństwo w Internecie i walka z dezinformacją –

PORADNIK

2022

Bezpieczeństwo w Internecie i walka z dezinformacją – poradnik

Autorzy:
Michał Horajski
dr Patryk Tomaszewski

2022

1. Czym jest bezpieczeństwo w Internecie?

Jak wskazuje Strategia Cyberbezpieczeństwa RP - rozwój społeczny i gospodarczy w coraz większym stopniu zależny jest od szybkiego i nieskrępowanego dostępu do informacji oraz jej wykorzystania w zarządzaniu, produkcji, sektorze usług oraz sektorze publicznym. Dynamiczny rozwój systemów informacyjnych służy rozwojowi gospodarki, w szczególności w obszarze komunikacji, handlu, transportu czy też usług finansowych. Z wykorzystaniem technologii cyfrowych tworzących cyberprzestrzeń - kształtowane są relacje społeczne, a usługi w sieci Internet stały się narzędziem do wpływania na zachowania grup społecznych, a także oddziaływania w sferze politycznej. Dlatego należy pamiętać, że obszarem ważnym z punktu widzenia bezpieczeństwa jest również cyberbezpieczeństwo rozumiane jako obszar bezpieczeństwa, obejmujący proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości jak i jego elementów (struktur państwowych, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej oraz będących w ich dyspozycji systemów teleinformatycznych i zasobów informacyjnych).

Cyberprzestrzeń to interaktywna domena stworzona z cyfrowych sieci, która jest wykorzystywana do przechowywania, modyfikowania oraz przekazywania informacji. Jej częścią jest Internet, ale zawierają się w niej także inne systemy informacyjne, które obsługują biznes, infrastrukturę oraz wspomagają świadczenie usług. Cyfrowe sieci już dziś podbudowują proces zaopatrywania naszych domów w energię elektryczną oraz wodę, pomagają organizować dostawy żywności oraz innych dóbr do sklepów oraz służą za niezbędne narzędzie biznesowe. Cyberprzestrzeń ma postać przestrzeni wirtualnej, która służy komunikowaniu się, a nie zmaterializowanej wyodrębnionej przestrzeni fizycznej, ale pamiętać trzeba przy tym, że jej byt jako obszaru wymiany

- nieuprawniony dostęp do zasobów sieci (włamania na czyjeś konta, przeglądanie zasobów dysków);
- kradzież informacji i danych;
- niewłaściwe wykorzystanie aplikacji działających w systemie (niezgodnie z ich licencjami);
- świadome wykorzystywanie luk systemów i oprogramowania;
- Ponadto wskazuje się awarie sprzętu (komputery, serwery), łączy, czy też oprogramowania.

Nieuprawniony dostęp do zasobów sieci oznacza, iż użytkownik do tego nieupoważniony jest w stanie pozyskiwać informacje, do których nie powinien mieć dostępu, łamie zazwyczaj zabezpieczenia, często przy użyciu złośliwego oprogramowania (tzw. robaki lub oprogramowanie szpiegujące).

Kradzież informacji i danych przez użytkowników wewnętrznych oznacza działalność mającą na celu pozyskiwanie danych a w szczególności danych poufnych. Celem może być np. uzyskania wpłaty pieniędzy na konto osoby, która pozyskała dane, wykorzystanie tych danych w celu oszustwa, czy też wyłudzenia, a czasami kompromitacji: instytucji, czy też osoby prywatnej.

Przytoczony już wcześniej Maciej Marczyk pisał: “Niewłaściwe wykorzystanie aplikacji działających w systemie oznacza, iż użytkownicy mogą nieświadomie wykorzystywać oprogramowanie w ten sposób, że narażają funkcjonowanie całego systemu otwierając drogę do ujawnienia informacji nie tylko swoich, lecz również informacji, które mogą być utajnione”.

informacji uzależniony jest od istnienia urządzeń technicznych natury fizycznej, zlokalizowanych na terytorium określonego państwa, przynależnych niekiedy nawet do określonych instytucji publicznych.

Jak słusznie zauważył Maciej Marczyk: "z cyberprzestrzenią nieodłącznie związane jest pojęcie anonimowości, które odnosi się do możliwości zachowania anonimowości użytkowników cyberprzestrzeni. Należy jednak zaznaczyć, że anonimowość nie wynika z samej istoty cyberprzestrzeni, lecz ze słabości konstrukcji Internetu. Aterytorialność cyberprzestrzeni sprawia, że wszelka aktywność użytkowników w jej obszarze nie nakłada na nich ograniczeń w postaci chociażby granicy geograficznej czy też politycznej. W rzeczywistości oznacza to, że z każdego miejsca na świecie możliwe jest dokonanie połączenia z globalną siecią".

Wraz z rozwojem Internetu zaczęło dochodzić do większej liczby przestępstw z tym obszarze nazywanych cyberprzestępstwami. Wśród cyberprzestępstwa są takie które mogą się odbywać wyłącznie dzięki użyciu cyberprzestrzeni, jak i takie które po prostu przeniosły się do świata wirtualnego.

W pierwszej grupie są np. zamachy skierowane na systemy komputerowe i sieci teleinformatyczne, dane i programy komputerowe, a więc grupę czynów określanych powszechnie jako przestępstwa stricte komputerowe lub przestępstwa przeciwko bezpieczeństwu przetwarzanej informacji. W drugiej np. kradzieże tożsamości, oszustwa, sprzedaż nielegalnych towarów (narkotyków, leków, oprogramowania komputerowego, podróbek towarów).

W przypadku zagrożeń wewnętrznych odnoszących się do środowiska sieci i systemów komputerowych (czyli tego co jest wewnątrz sieci) będą wszelkie działania zachodzące wewnątrz danego systemu teleinformatycznego. Wśród nich wyróżnić można:

Niewłaściwe korzystanie z aplikacji może prowadzić do:

- dostępu osób trzecich do informacji prywatnych, firmowych czy innych poufnych danych;
- ujawnienia haseł do systemów czy innych aplikacji;
- umożliwienia monitorowania urządzeń poprzez inne aplikacje działające w tle systemów operacyjnych;
- umożliwienia śledzenia położenia danego użytkownika;
- umożliwienia uszkodzenia urządzeń teleinformatycznych;
- wykorzystania prawdziwej tożsamości użytkownika do innych celów.

2. Podstawowy podział i charakterystyka cyberprzestępczości

W najbardziej uproszczony sposób cyberprzestępczość można podzielić na dwie podstawowe kategorie:

- przestępstwa charakterystyczne dla cyberprzestępczości,
- przestępstwa popełniane z wykorzystaniem sieci Internet.

Pierwszą kategorię stanowią przestępstwa, w których przedmiotem ataku jest sam komputer oraz szeroko pojęte przetwarzanie danych w systemach informatycznych. Do tej grupy można zaliczyć takie czyny, jak:

- podawanie się za inną osobę, fałszywe profile,
- nieuprawnione uzyskanie informacji (hacking),
- podsłuch komputerowy (sniffing),
- udaremnienie uzyskania informacji,
- udaremnienie dostępu do danych informatycznych,
- sabotaż komputerowy,
- rozpowszechnianie złośliwych programów oraz cracking,
- stosowanie tzw. narzędzi hackerskich,
- oszustwo komputerowe.

Do drugiej kategorii należy zaliczyć przestępstwa, w których komputer jest jedynie środkiem do jego popełnienia. W tej grupie można wymienić takie działania, jak:

- obraza uczuć religijnych (przestępstwa przeciwko wolności sumienia i wyznania chronione prawnie zgodnie z Konstytucją RP),

- składanie propozycji obcowania płciowego z małoletnim. W Kodeksie karnym w art. 200b, uregulowano publiczne nawoływanie do pedofilii. Kto publicznie propaguje lub pochwala zachowania o charakterze pedofilskim, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

- publiczne propagowanie faszystowskich lub innych totalitarnych ustrojów państwa lub nawoływanie do nienawiści na tle różnic narodowościowych, etnicznych, rasowych, wyznaniowych albo ze względu na bezwyznaniowość.

- zbywanie własnego lub cudzego dokumentu stwierdzającego tożsamość, a także fałszowanie np. faktur lub podawanie w nich nieprawdziwych informacji (przestępstwa przeciwko wiarygodności dokumentów - czyli przestępstwa karalne z art. 270. 270a, 271a KK).

- oszustwa popełniane za pośrednictwem Internetu, np. sprzedaż towaru innego niż reklamowany, brak wysłania towaru, twierdzenie, że jakiś towar został wysłany, gdy faktycznie tak nie było.

Z punktu widzenia bezpieczeństwa obywatela najważniejsze aspekty to:

- ochrona swojej prywatności w cyberprzestrzeni;

- nienarażenie swoich pieniędzy na ryzyko kradzieży;

- ochrona przed cyber uzależnieniem i cyberprzemocą;

- ochrona przed dezinformacją w cyberprzestrzeni.

Twoja cyberprywatność – oznacza, że chronisz swój wizerunek i swo-

ich bliskich w przestrzeni internetowej.

Warto wiedzieć, że uzależnienie od Internetu ma swoje źródła w nadużywaniu dostępu do Internetu, a skutki negatywne mają wpływ na:

- rodzinę i bliskich;
- zdrowie psychiczne;
- aktywności społeczne i więzi międzyludzkie;
- aspekty ekonomiczne (gry w cyberprzestrzeni, w tym gry hazardowe).

3. Dezinformacja w Internecie

Czy wiesz czym jest dezinformacja i jakie skutki może przynieść?

Dezinformacja to świadomie opracowana lub przekazywana fałszywa informacja lub celowy i intencjonalny proces dystrybucji fałszywych lub wprowadzających w błąd informacji.

Świetnym źródłem treści dezinformujących jest dziś Internet. Definicje skupiają się na komponencie fałszywych informacji. Ostatecznym celem jest wpływanie na opinię publiczną, procesy decyzyjne i działania jednostek, całych społeczeństw i rządów. Swoim zasięgiem dezinformacja obejmuje zakres od manipulacji i innych form tzw. dywersji ideologicznej, przez finansowanie ruchów politycznych czy grup terrorystycznych, w tym nawet zabójstwa na zlecenie.

W życiu codziennym najczęściej dezinformacja ma prowadzić do zainteresowania się jakimś produktem, co może przynieść efekt w postaci jego masowego zakupu. Dezinformatorzy posługując się Internetem wprowadzają opinię publiczną np. w panikę, co powoduje masowe zakupy danego produktu.

Pojawia się wydająca się na prawdziwą i sprawdzoną informacja, że:

1. ceny danego produktu wzrastają;
2. dany produkt ma wspaniałe właściwości np. lecznicze;
3. dany produkt może być niebezpieczny dla życia lub zdrowia.

Taka informacja rozsiewa się wśród ludzi drogą „głuchego telefonu", pojawiają się informacje: wiem, że tak będzie, mam sprawdzone źródło wiedzy, już inni się zabezpieczają, czas na nas. Dezinformacja doprowadza do błędnego nieprawdziwego postrzegania rzeczywistości, do

nieracjonalnych zachowań, w tym paniki.

W polskich dyskontach półki pustoszeją mimo jasnej diagnozy ekspertów: „cukru nam nie zabraknie", a nastroje konsumentów podsycają fake newsy. Obawy o brak artykułów na sklepowych półkach w Polsce to nie pierwszyzna. Kupujący szturmowali markety i stacje paliw w pierwszych dniach pandemii COVID-19 oraz tuż po wybuchu wojny w Ukrainie.

Warto odnieść się również do pojęcia "fake newsów".

Fake news to nieprawdziwa lub częściowo nieprawdziwa wiadomość, często o charakterze sensacyjnym, publikowana w mediach z intencją wprowadzenia odbiorców w błąd w celu osiągnięcia korzyści finansowych, politycznych lub prestiżowych.

Należy odróżniać takie nieprawdziwe i wprowadzające w błąd treści od humoru czy satyry.

Fake newsy są tworzone, a następnie rozpowszechniane, m.in. z powodów politycznych, finansowych, ideologicznych (poglądów i przekonań), a także dla rozrywki, zabawy,

Również niektóre osoby lub instytucje mogą nazywać fake newsami wiadomości prawdziwe z powodu negatywnej dla tych osób lub instytucji zawartości.

Poniżej wskazano istotne zasady opisujące jak uchronić się przed fake newsami.

Zasada nr 1: „Hej, poczekaj!"

Obejrzałeś właśnie artykuł, zdjęcie czy wideo, które wywołało w Tobie emocje? Poczekaj! Odetchnij, weź 3 głębokie wdechy i zastanów się czy to na pewno prawda! Najważniejszym zadaniem fake newsa jest

wywołać w Tobie emocje! Prawdziwe emocje niestety są o wiele mniej emocjonujące, dlatego to kłamstwo choć ma krótkie nogi to łatwiej rusza w świat, dzięki ładunkowi emocji jaki w sobie niesie!

Przykład z życia? 30 października odbyły się wybory prezydenckie w Brazylii. Część zwolenników ustępującego prezydenta protestowała, nie zgadzając się z werdyktem. No więc gdzie tu haczyk?

Jeden z portali opublikował filmik przedstawiający tłumy Brazylijczyków na ulicach z opisem „Wszystkie media całkowicie ignorują demonstracje i powstanie Brazylijczyków". Chwyta za serce? Owszem. Czy jest prawdziwe? Nie. Nagranie nie ma żadnego związku z wyborami i zostało nagrane 7 września przy okazji obchodów Święta Niepodległości.

Zasada nr 2: „Dobra ściema zaczyna się od nagłówka!"

Ile razy zdarzyło nam się przeczytać nagłówek artykułu , a następnie podrzucić go znajomym, rodzinie lub udostępnić na tablicy w mediach społecznościowych? No właśnie. A więc zasada nr 2 - zanim udostępnisz cokolwiek - zapoznaj się z całym materiałem! Pamiętajcie, że portale informacyjne żyją z wyświetleń, dlatego chwytliwy, tzw. clickbaitowy, tytuł to podstawa wielu artykułów. A to, że nie zawsze w pełni odnoszą się do tego, co jest w środku? No cóż, trzeba było przeczytać całość!

Przetestujcie tę zasadę sami – wejdźcie na kilka portali informacyjnych, przejrzyjcie tytuły artykułów, a później przeczytajcie, co w sobie zawiera reszta materiału. Sami się zdziwicie!

Zasada nr 3: „Czy to w ogóle aktualne?"

Kluczowym elementem informacji jest przekazanie aktualnego statusu wydarzeń czy wiedzy jaki na dany temat mamy – no i bardzo dobrze,

prawda? Jednak w warunkach dynamicznych zmian jak dopiero rozwijająca się epidemia wcześniej nieznanej choroby lub konflikt albo katastrofa naturalna dziejąca się właśnie gdzieś na świecie powoduje, że wcześniej podana informacja może się zdezaktualizować w przeciągu dni czy nawet godzin! Dlatego tak ważne jest sprawdzenie zanim udostępnicie cokolwiek czy informacja jest jeszcze aktualna! Któż z nas nie był sfrustrowany w 2020 roku, gdy media przekazywały jakąś informację, a tydzień później wiedza ta stawała się nieaktualna. Ale pamiętajmy – nauka cały czas pozyskuję nowe informacje i zdarza się, że musimy zdementować wcześniejsze.

Spróbujcie sami zobaczyć, jak jest z tym zdezaktualizowaniem. Możecie w tym celu poprzeglądać portale informacyjne o koronawirusie z marca 2020, a potem np. maja, czerwca czy października. Ba, jeśli skończyliście już szkolną edukację to zobaczcie ile informacji z tamtych czasów przestało być obowiązującym dogmatem!

Zasada nr 4: „Amerykańskie badania mówią, że...”

Wiadomo, że jeśli jacyś amerykańscy naukowcy coś powiedzieli to wiadomo, że tak było... Pamiętajcie! Jeśli gdziekolwiek ktoś pisze, że ktoś, coś powiedział/napisał/zbadał to warto, aby podał źródło swoich informacji. Skąd o tym w ogóle wie? W jaki sposób się o tym dowiedział? Czy jest to jakiś niepodważalny obiektywny fakt czy tylko subiektywna opinia? Czy skoro w artykule na portalu jest napisane, że badania dowodzą, że coś odkryto lub potwierdzono to czy dziennikarz uwzględnia źródło tych informacji? Czy sami mamy okazję móc spojrzeć w to badanie albo chociaż zobaczyć skąd się wzięło? Pamiętajcie, aby zawsze pytać o źródło!

Zasada nr 5: „A kto to mówi?”

Kto jest autorem informacji czy nawet mema, którego czytasz? Czy jesteśmy w stanie sprawdzić kto stworzył informację, którą czytasz? Bo jeśli anonimowe źródła donoszą, że... Miej wątpliwość i sprawdzaj kto, co pisze i na jakie źródła

się powołuje! O ile bez problemu możemy sprawdzić autora artykułu na portalu informacyjnym to już posty lub memy rozprzestrzeniające się w mediach społecznościowych często są anonimowym dziełem, dlatego z dystansem podchodźmy do informacji, nowinek, opinii, tego, co lekarz nam nie powie z przypadkowych postów w mediach społecznościowych!

Zróbcie sami takie ćwiczenie. Wpiszcie jedną z tych fraz w wyszukiwarkę i zobaczcie, ile artykułów będzie właśnie zawierała treść o tych jakże niepodważalnych źródłach informacji jak brat koleżanki czy osoba z bliskiego otoczenia.

Wśród wymienianych przez ekspertów sposobów na przeciwdziałanie dezinformacji jest m.in. fact-checking, czyli szczegółowa weryfikacja informacji, np. poprzez porównywanie źródeł, sprawdzanie obrazów, weryfikację prawdziwości źródła. Nieodłącznym elementem walki z dezinformacją jest również edukacja społeczeństwa. Niestety, w zalewie informacji zdarza się, że sami powielamy fake newsy, przez ich udostępnianie na portalach społecznościowych. Tu dobrym rozwiązaniem jest korzystanie ze sprawdzonych źródeł, mediów, do których mamy zaufanie, czy dziennikarzy, których cenimy.

Dezinformacja służyć może działaniom mającym na celu manipulowaniu opinią publiczną i nie tylko w przypadku danego produktu, ale także może zniechęcać nas do pójścia do wyborów, może prowadzić do niechęci wobec konkretnej grupy narodowościowej czy religijnej. Dezinformacja to narzędzie, które łatwo infekuje właśnie internet a my mamy kłopoty z odróżnieniem faktów od przekłamań, kłamstw i półprawd. Stajemy się nie tylko ofiarami dezinformacji ale czasami ślepym narzędziem w jej propagowaniu – sprawdzajmy informacje, nie dajmy się ponieść emocjom. Nie wszystkie informacje z Internetu ale też innych źródeł to prawda – pamiętajmy, że jesteśmy podatni na manipulację.

4. Scenariusze działań oszustów - przykłady zagrożeń

1) Metoda „na wnuczka”

Wykorzystywanie bliskich relacji – często relacji rodzinnych jest niestety bardzo popularną metodą mającą na celu oszukanie drugiej osoby. Często policja ma do czynienia z przestępstwem oszustwa, wyłudzenia pieniędzy bądź danych wrażliwych za pomocą tzw. „metody na wnuczka”. Ten rodzaj oszustwa jest niezwykle niebezpieczny gdyż wykorzystuje bliską relację i zaangażowanie emocjonalne, co bardzo często powoduje, że starsza osoba zaczyna działać pod wpływem wysokich emocji nie analizując możliwych zagrożeń i nie stosując podstawowych czynników bezpieczeństwa, które pozwalają ograniczyć ryzyko oszustwa.

Oszustwo „na wnuczka” to sposób na wyłudzanie pieniędzy czy danych wrażliwych od osób starszych. Pomimo ostrzeżeń pojawiających się w telewizji, prasie czy w radiu, wciąż wielu seniorów daje się nabrać na te profesjonalnie zorganizowane przedstawienia. Należy przede wszystkim zauważyć, że oszuści bardzo często zmieniają narracje i metody jakich używają, aby przekonać starsze osoby do ujawnienia swoich danych czy przekazania pieniędzy pod pozorem pomocy najbliższej rodzinie.

Oszuści mając świadomość coraz większej dostępności informacji wśród osób starszych, dlatego wciąż zmieniają historie i metody, które pozwalają im na wpływanie na starsze osoby tak aby powierzyły im swoje oszczędności w poczuciu pomocy swoim najbliższym. Warto pamiętać, że oszuści bardzo często przed podjęciem próby wyłudzenia pieniędzy dokonują swoistego „sprawdzenia” ofiary i tutaj pojawia się kilka czynników które powodują, że osoba starsza może być bardziej narażona na tego typu oszustwo.

Osobami najbardziej narażonymi na tego typu działalność są samotne osoby starsze, jednocześnie posiadające rodzinę – niekoniecznie mieszkającą w tej samej miejscowości. Warto tutaj też brać pod uwagę czynnik sąsiedzki – zwłaszcza jeżeli ktoś obcy wypytuje o jakieś pozornie nieistotne informacje dotyczące sąsiadki czy sąsiada o którym wiemy, że mieszkają samotnie, zwłaszcza jeżeli ktoś chce poznać np. imiona jego najbliższych, wiek, miejsce zamieszkania, szczegóły dotyczące pracy czy studiów na jakich jest ich wnuk czy wnuczka. Takie zainteresowanie obcych osób powinno budzić nasze podejrzenia.

Metoda ta nazywana jest najczęściej; „na wnuczka" od bardzo popularnej formy oszustwa – czyli podszywania się pod wnuczka starszej osoby, który to „wnuczek" lub „wnuczka" potrzebuje bardzo pilnie pewnej sumy pieniędzy. Oczywiście oszuści mogą tutaj zmieniać historię bardzo dynamicznie i oprócz fałszywego „wnuczka" bardzo często zaangażowane są też inne postronne osoby które mogą też w imieniu tej bliskiej osoby dzwonić do ofiary – w ten sposób może być tłumaczony fakt, że ofiara nie rozpoznaje głosu bliskiej osoby.

PAMIĘTAJ ABY ZWRACAĆ UWAGĘ NA DZIWNE PYTANIA I ZACHOWANIA OBCYCH OSÓB!

Zachowania na które szczególnie powinniśmy zwrócić uwagę w przypadku takiego kontaktu: w rozmowie dzwoniący prosi o udzielenie pilnej pożyczki, stosując różnorodne opowieści. Bardzo często jest to próba wykorzystania współczucia – np. choroba, potrzeba pilnego zakupu, opłaty za dodatkowe zajęcia na studiach. Zdarza się, że dzwoniący nie wskazuje żadnego celu, na który potrzebuje pieniędzy, lecz niemal zawsze prosi o dyskrecję wobec innych członków rodziny. Zapewnia także o bardzo szybkim i osobistym zwrocie gotówki.

UWAGA!

Oszuści wykonują do swoich ofiar bardzo dużo połączeń telefonicznych, w krótkich odstępach czasu w celu wywarcia presji psychologicznej i nakłonienia do szybkiego przekazania pieniędzy. Takie częste telefony mają, także utrudnić osobie oszukiwanej nawiązanie kontaktu z członkami rodziny, rzekomo proszącymi o pomoc finansową.

Często oprócz pożyczki na cele związane np. ze zdrowiem czy studiowaniem oszuści grając na emocjonalnym przywiązaniu ofiary do rodziny budują scenariusze oparte także np. o to że bliska osoba – syn/ córka spowodowali wypadek, za który będą ścigani przez policję. Jednak mogą uniknąć tych problemów, tylko muszą szybko zapłacić osobie, która teoretycznie jest poszkodowana w tym zdarzeniu – pojawia się tutaj obawa o odpowiedzialność, poczucie chęci pomocy. Bardzo często przy tego typu oszustwie wszystko dzieje się niezwykle szybko, a oszuści obserwując reakcje ofiary potrafią także zwiększać swoje żądania finansowe. Kiedy nie jest możliwe sprostanie wymaganiom stawianym przez oszustów, zaczynają oni żądać np. biżuterii.

UWAŻAJ NA FAŁSZYWE PROBLEMY TWOICH BLISKICH!

Innym przykładem oszustwa opartego na zaufaniu do członków bliskiej rodziny jest prośba związana z problemami rodzinnymi/ zdrowotnymi z czym wiąże się najczęściej ze strony oszustów przekonywanie ofiary, aby wszystko pozostało w tajemnicy pomiędzy nimi:

„bardzo proszę niech to zostanie na razie między nami”.

„proszę nie mów o tym nikomu – wiesz jak trudna jest to dla mnie sytuacja”

Ten prosty zabieg ma zapewnić oszustom więcej czasu na przeprowadzenie całego scenariusza przestępstwa. Czasami oszuści wykorzystują bliską relację ofiary nie tylko z rodziną, ale z np. z przyjaciółką – w takich sytuacjach pojawiają się prośby o wsparcie ze strony fałszywej przyjaciółki lub jej fałszywych członków rodziny – co dodatkowo utrudnia możliwość weryfikacji przez ofiarę, że ma do czynienia z oszustami.

ZWRACAJ UWAGĘ NA NIETYPOWE PROŚBY!

Aby uwiarygodnić całą sytuację zdarza się, że gotówka i kosztowności przekazywane są nie tylko w miejscu zamieszkania oszukiwanej osoby albo na ulicy, ale także w placówkach bankowych. W tym czasie bardzo często budowane jest większe poczucie zaufania ofiary do oszusta. Zdarza się, że sprawcy przyjeżdżają po swoje ofiary taksówkami, z którymi razem jadą np. do banku w celu dokonania przelewu lub pobrania gotówki. Podczas takiego spotkania oszuści bardzo często udają, że mają stały kontakt z bliską osobą dla której mają zostać przekazane pieniądze.

KIEDY ZNAJOMI LUB BLISCY PROSZĄ O PIENIĄDZE ZA POMOCĄ KOMUNIKATORA – ZADZWOŃ DO NICH ŻEBY TO POTWIERDZIĆ.

Wraz z rozwojem bankowości internetowej i coraz szerszym dostępem do mediów społecznościowych, wzrostem dostępności do płatności mobilnych wzrasta także liczba przestępstw opartych nie tylko o połączenia telefoniczne od fałszywej rodziny, ale także coraz częściej obserwowane są oszustwa oparte o komunikatory internetowe – polega to na prostym przejęciu konta bliskiej osoby i rozpoczęciu konwersacji – podobnie jak przypadku rozmowy na początku oszust stara się uwiarygodnić więc rozpoczyna rozmowę od jednego z wątków na temat którego faktycznie wcześniej była prowadzona rozmowa. Przy tak zbudowanym zaufaniu po krótkiej rozmowie pojawiają się kwestie

potrzeb finansowych. Tego typu oszustwo może dotyczyć nie tylko seniorów, ale najczęściej dotyczy rodzeństwa lub wykorzystuje relacje dzieci i rodziców. Oszust podszywa się pod córkę lub syna i prosi o dokonanie szybkiej płatności np. za zakupy za pomocą aplikacji BLIK. Oprócz popularnych komunikatorów możliwe jest także wykorzystanie adresów e-mail należących do bliskich osób.

PAMIĘTAJ:

1. **nie przekazuj pieniędzy obcym osobom, ani nie podpisuj dokumentów;**
2. **zadzwoń do osoby bliskiej lub pod inny znany Ci numer telefonu;**
3. **powiadom policję, dzwoniąc pod numer 112 lub 997.**

2) Metoda na znajomość na portalach społecznościowych, pomoc fikcyjnym potrzebującym

Dobre serce, chęć niesienia pomocy, dobroczynność to wspaniałe postawy, ale mogą zostać wykorzystane przez oszustów i należy o tym pamiętać. Pamiętajmy, że cechami charakterystycznymi wyłudzeń i oszustw jest używanie socjotechniki i manipulacji psychologicznych.

Pomoc fikcyjnym potrzebującym ma poruszyć nasze serce. Możemy otrzymać e-mail z prośbą o wsparcie schroniska dla zwierząt, pomoc osobom ciężko chorym, a także oszust może podszyć się pod osobę zakochaną, która chce spędzić z nami życie i przyjechać do Polski. Ten ostatni sposób to oszustwa na tzw. „żołnierza z Afganistanu".

A czym są oszustwa na tzw. „wygraną w loterii"? Użytkownik otrzymuje wiadomość e-mail z informacją, o rzekomej wygranej w loterii i prośbą o dane osobowe w celu przekazania zwycięzcy wysokiej nagrody. 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.

STOSUJ ZAWSZE ZASADĘ OGRANICZONEGO ZAUFANIA!

Nie wierz w możliwość wygranej w loterii, nie dawaj wiary, że otrzymałeś spadek od dalekich krewnych z zagranicy, gdzie w e-mailu oszust pisze, że aby spadek dostać wystarczy tylko podać swoje dane osobowe, wpłacić niewielką kwotę w celu np. opłacenia prawnika. Dzięki dobremu sercu, wierze w ludzi podajemy swoje dane wrażliwe, które mogą być wykorzystane np. w celu zaciągnięcia kredytu, gdy zaś wpłacamy pieniądze możemy być pewni, że zostały one od nas wyłudzone.

W mediach społecznościowych pojawia się co jakiś czas fala fałszywych akcji, których celem jest zbiórka pieniędzy. Schemat działania jest za każdym razem zbliżony: atakujący zakładają grupy i dodają w nich zaledwie kilka postów. Wpisują też informacje dotyczące tego, jak można przelewać pieniądze, oraz dodają wyciskające łzy komentarze.

Grupy oszustów działają zwykle bardzo podobnie. W ich nazwach znajduje się prośba o pomoc, a opublikowane posty opisują poruszające historie, zwykle o nieuleczalnie chorych dzieciach, których cierpienie ilustrują umieszczone na stronie zdjęcia i filmy.

Podobna sytuacja dotyczy zbiórek już nie na dzieci, ale zwierzęta przetrzymywane w złych warunkach, cierpiące i poszukujące domu lub poprawy ich losu. Tu także przestępcy zazwyczaj wstawiają np. na portalach społecznościowych tylko dwa, trzy posty i zdjęcie cierpiących zwierząt, oczekując, że nazwa zwierzęcia, jego zdjęcie przyciągną naszą uwagę a w konsekwencji podyktuje wpłatę pieniędzy.

PAMIĘTAJ ŻEBY PATRZEĆ KRYTYCZNIE I ANALIZOWAĆ TREŚCI W INTERNECIE!

Oczywiście obok takich fałszywych grup istnieją też prawdziwi ludzie, którzy mają realne problemy i również zbierają pieniądze na chorych, zwierzęta, czy też ratowanie zabytków. Dlatego najważniejsze jest to, aby nie ignorować automatycznie wszystkich próśb o pomoc, jakie spotkamy w Internecie. Jak rozpoznać osoby prowadzące działalność charytatywną i pomocową od oszustów?

Jeśli grupa została założona zaledwie trzy lub cztery tygodnie temu i opublikowała tylko trzy posty, ale przeczytało je i podało dalej wiele osób (czasami nawet kilka tysięcy), najprawdopodobniej należy ona do oszustów. Prawdziwe społeczności potrzebują czasu na rozwinięcie skrzydeł, a ich organizatorzy publikują znacznie więcej informacji. Użycie szokujących filmów, niskiej jakości zdjęć czy wzbudzających smutek opisów ma na celu zachęcenie do spontanicznego działania, aby nie było czasu na chwilę krytycznego zastanowienia się czy historia jest prawdziwa. W takich postach próbujących wzbudzić naszą litość pojawia się też mnóstwo wykrzykników, a tekst pisany jest wielkimi literami.

Długo istniejące organizacje zazwyczaj nie uciekają się do takich środków, ponieważ dla nich ważniejsze jest zbudowanie wiarygodnej i pełnej zaufania relacji z darczyńcami oraz możliwość pomagania potrzebującym również w przyszłości. Dlatego opowiadają one historie swoich pacjentów prostym językiem, nie piszą z nadmiernymi emocjami, a także udostępniają szczegółowe opisy tego, w jaki sposób można dokonać płatności i na co zostaną wydane zebrane pieniądze.

Oszuści chcą zebrać tyle pieniędzy, ile tylko można, zanim grupa zostanie zamknięta, więc stosują presję emocjonalną.

3) Oszustwa wykorzystujące zaufanie do instytucji państwowych i finansowych

Metody oszustw wykorzystujących zaufanie do instytucji państwowych czy banków są niestety coraz bardziej oryginalne, a także wraz z rozwojem i popularnością bankowości internetowej dotykają coraz częściej seniorów. Oszuści podobnie jak w innych przypadkach opierają się tutaj o swego rodzaju zaufanie do instytucji kierując zawsze tak rozmowę aby ofiara była przekonana, że ma do czynienia z profesjonalnym przedstawicielem jakiegoś urzędu lub banku.

Coraz więcej instytucji oraz firm – zwłaszcza z branży finansowej stara się informować i ostrzegać swoich klientów o zagrożeniach jakie płyną ze strony oszustów. Zakład Ubezpieczeń Społecznych apeluje do swoich klientów o ostrożność przy otwieraniu i odpowiadaniu na e-maile, które wydają się być korespondencją z ZUS. Dokładnie zwracajmy uwagę na adres, z którego przychodzą e-maile. Oszustwa związane z wykorzystaniem wiadomości przypominających wiadomości z ZUS coraz częściej trafiają także do seniorów. Wysyłane wiadomości informują o pilnej konieczności spłaty zaległości składkowych. Część e-maili sugeruje ponowne wypełnienie formularza zgłoszenia do ubezpieczeń społecznych ZUS ZUA, który jest załącznikiem do e-maila. Umieszczone w stopce korespondencji logotypy (ZUS i PUE – Platforma Usług Elektronicznych) sugerują, że nadawcą jest sam Zakład. Gdy jednak przyjrzymy się dokładnie adresowi nadawcy, nie powinniśmy mieć wątpliwości, że korespondencja elektroniczna nie pochodzi z Zakładu Ubezpieczeń Społecznych. Na swoich stronach internetowych ZUS informuje, że bardzo często oszuści posługują się dwoma adresami: składki@ubezpieczenia.pl i zus.@zua.pl. Jak widać żaden z adresów nie ma stosowanego przez Zakład rozwinięcia „zus.pl".

Na swoich stronach internetowych ZUS informuje i przypomina: "Kontakt elektroniczny ze strony Zakładu możliwy jest jedynie w sytuacji gdy klient posiada profil na Platformie Usług Elektronicznych i wyraził zgodę na taką

formę kontaktu. ZUS ostrzega by w żadnym przypadku nie odpowiadać na maile, które teoretycznie pochodzą z Zakładu Ubezpieczeń Społecznych, ani nie otwierać zawartych w tej korespondencji załączników. Korespondencja tego typu ma bowiem najczęściej na celu zainfekowanie komputera lub uzyskanie dostępu do danych wrażliwych, które zapisane są w jego pamięci."

KIEDY NIE MASZ PEWNOŚCI CO DO INFORMACJI JAKĄ OTRZYMAŁEŚ Z URZĘDU – NIE REZYGNUJ Z WERYFIKACJI!

W przypadku kiedy pojawiają się jakieś wątpliwości co do pochodzenia/autentyczności wiadomości elektronicznej z Zakładu Ubezpieczeń Społecznych, najlepiej jest skontaktować się telefonicznie z najbliższą placówką ZUS lub Centrum Obsługi Telefonicznej pod numerem: 22 560 16 00.

Niestety oszuści wykorzystują zaufanie seniorów do Zakładu Ubezpieczeń Społecznych na bardzo wiele różnych sposobów. ZUS na swoich stronach internetowych informuje, iż pojawiły się przypadki oszustów podających się za pracowników ZUS oferujących pomoc w uzyskaniu unijnego świadczenia 500 plus. Oszuści w tym przypadku zapukali do drzwi seniorki i zapowiedzieli wizytę lekarza orzecznika ZUS, który miałby ją za chwilę przebadać. W celu uspokojenia i wzbudzenia zaufania oszuści w tego typu przypadkach informują, że lekarz orzecznik ZUS był również u sąsiadki, lub w klatce obok.

Zakład Ubezpieczeń Społecznych informuje: "Pracownicy ZUS, lekarze orzecznicy ZUS, nie odwiedzają emerytów i rencistów w ich domach. Taka wizyta może się zdarzyć tylko wtedy, jeśli ktoś starał się o rentę, świadczenie uzupełniające dla osób niezdolnych do samodzielnej egzystencji lub świadczenie rehabilitacyjne, a jego stan zdrowia nie pozwalał na badanie w placówce ZUS. Jednak w takiej sytuacji o terminie badania klient zawsze był wcześniej informowany listownie." Coraz częściej oszuści wykorzystują metody tzw. spoofingu telefonicznego. Polega on na podszywaniu się pod dowolny numer lub

nazwę kontaktu. Pomimo, że telefon odbiorcy wyświetla daną informację o dzwoniącym lub piszącym wiadomość, w rzeczywistości dzwoni lub pisze ktoś inny. W ten sposób coraz częściej oszuści podszywają się pod konsultantów banków czy przedstawicieli urzędów. Oszustwo może polegać na kontakcie telefonicznym i próbie pozyskania danych wrażliwych, które następnie przez oszustów będą mogły być wykorzystane w celu dokonanie przestępstwa np. zaciągnięcia w imieniu ofiary zobowiązania pożyczki o której to pożyczce ofiara nie będzie miała świadomości. Ta metoda wykorzystywana jest również przez oszustów do próby pozyskania danych do logowania do systemów informatycznych PUE ZUS.

Oszuści celem zdobycia danych seniorów wykorzystują także nowe świadczenia jakie pojawiły się w ostatnim czasie: 13 oraz 14 emeryturę. W związku z tymi świadczeniami pojawili się oszuści podający się za konsultantów ZUS, którzy informowali emerytów o tym, że ze względu na błędne dane nie będą mogli otrzymać świadczenia. W ten sposób próbowali wyłudzić od seniorów ich dane wrażliwe. Niektórzy oszuści oprócz pozyskiwania danych oferowali pomoc przy wypełnieniu wniosku o 13 i 14 emeryturę, a nawet próbowali pobierać opłaty za takie fikcyjne wypełnienie wniosku.

Pamiętajmy, że w sprawie 13 czy 14 emerytury nie składa się żadnych wniosków, ZUS sam weryfikuje uprawnienia. Nie dajmy się więc też oszukać na ewentualnie oferowaną pomoc w napisaniu niepotrzebnego wniosku.

Osobiste odwiedzenie klientów przez pracowników ZUS w ich domach jest wyjątkowo rzadkie a ZUS sprawy z klientami załatwia listownie lub w swoich placówkach, a także poprzez uwierzytelniony profil na Platformie Usług Elektronicznych.

Bardzo częstym rodzajem oszustw wykorzystujących wiadomości

e-mail są oszustwa związane z podszywaniem się pod banki lub inne instytucje finansowe. W przypadku powoływania się na bank oszuści najczęściej używają poczty elektronicznej celem zainfekowania komputera szkodliwym oprogramowaniem. Oprócz tego coraz częściej stosowana jest również metoda zwana „oknem szpiegowskim" – ang. SpyWindow. Polega ona na tym, że oszuści podają się za pracowników banku i zachęcają do otworzenia teoretycznie bezpiecznego dokumentu. Żeby to zrobić, musimy podać nasze dane do logowania. SpyWindow przesyła te dane oszustowi, a do nas przychodzi fałszywe potwierdzenie autoryzacji. Jest to szczególnie niebezpieczne, gdyż może prowadzić do przejęcia konta bankowego przez oszustów. Ofiara nie zdaje sobie sprawy z tego, że logując się udostępnia swoje dane, które następnie są wykorzystywane przez oszustów. Dlatego bardzo ważne jest aby sprawdzać jakie rzeczy autoryzujemy w Internecie.

4) Metoda na firmy prywatne - prąd, odbiór paczek, dopłaty do rachunków / stalking telefoniczny związany z promocjami, oferowania badań medycznych

Jak wskazywano oszuści od zawsze próbują wykorzystać naszą łatwowierność. W dzisiejszych "informatycznych" i dynamicznych czasach musimy być wyjątkowo czujni. Szczególnie narażone są tu osoby starsze, które nie mają tak dużego doświadczenia w różnych narzędziach komunikacji elektronicznej. Seniorzy są też bardziej ufni co konsekwentnie wykorzystują złodzieje. Niestety cały czas jest to ogromny problem w naszym kraju. Ponad 85 milionów złotych co roku jest wyciąganych przez przestępców z kont i portfeli seniorów w Polsce. Sposób oszustw jest cała masa, a przestępcy ciągle szukają czegoś nowego. Nie zmienia się jedno - polowanie na nasze pieniądze.

Jednym z urządzeń, który bardzo pomaga oszustom jest nasz telefon. Przestępcy nie muszą nawet znać naszego numeru, wysyłają setki jak nie tysiące fałszywych wiadomości w nadziei, że ktoś się nabierze.

Jedną z najpopularniejszych metod oszustwa “na sms” jest podszywanie się pod dostawcę prądu, gazu lub usług telefonicznych i innych mediów.

Na przykład taka wiadomość: „PGE-obrót: Na dzień 17.03 (tu pojawia konkretna data z nieodległej przyszłości) zaplanowano odłączenie energii elektrycznej! Prosimy o uregulowanie należności”.

Na pierwszy rzut oka wszystko wygląda niczym zwykła wiadomość tekstowa wysłana od operatora energii elektrycznej. Jej treść jest krótka, ale starannie przemyślana, uwagę zwracają konkretnie dobrane słowa. Dodatkowo w wiadomości pojawia się link, który należy kliknąć, aby uregulować nieistniejący dług.

Pod żadnym pozorem nie wolno otwierać takiego linku ani tym bardziej dokonywać za jego pośrednictwem przelewu. Nie tylko możemy stracić przelane środki, ale co bardziej ryzykowne, przestępcy mogą w takiej sytuacji przejąć dostęp do naszego konta co może mieć katastrofalne skutki.

PAMIĘTAJ!

Twoi dostawcy usług nigdy nie wysyłają linków do przelewów. Jeśli masz wątpliwości czy naprawdę masz zaległości skorzystaj z tradycyjnych form kontaktu - telefon lub wizyta w Biurze Obsługi Klienta. Także nigdy nie odpisuj na takie SMSy, po weryfikacji najlepiej go skasować, a numer z którego przyszedł zablokować. Jeśli nie wiesz jak to zrobić poproś kogoś zaufanego albo pracownika w punkcie obsługi operatora. UWAGA! Nie sugeruj się nadawcą wiadomości, oszuści mogą tak spreparować wiadomość żeby wyglądała jak najbardziej wiarygodnie.

Według podobnego mechanizmu działa metoda “na kuriera”. Dostajemy wtedy fałszywego SMSa, aby zapłacić, ew. dopłacić za odbiór

zamówionej paczki. Przestępcy liczą na nasze roztargnienie i pośpiech - niestety to działa, bo stale dochodzi do takich wyłudzeń.

Oszuści działają także w bardziej tradycyjny sposób. Przestępcy na przykład podszywają się pod kuriera! Ubierają się wtedy w prawdziwy mundur z terminalem płatniczym i dostarczają paczkę za pobraniem, czyli taką za którą trzeba zapłacić. Właśnie w ten sposób oszukują i kradną pieniądze. Koszt takiej paczki zaczyna się od 99 zł i osiąga często poziom kilkuset złotych. Co znajduje się w środku? Śmieci lub zużyte, zupełnie niepotrzebne materiały.

Złodzieje wykorzystują fakt, że sąsiedzi lub członkowie rodzin często odbierają za nich przesyłki. W latach poprzednich szczególnie w okresie przedświątecznym często dochodziło do takich oszustw, gdy wielu z nas robi zakupy przez Internet.

PAMIĘTAJ!

Warto tu przyjąć jedną prostą zasadę: Nigdy NIE płacimy za cudze przesyłki, chyba że wcześniej dana osoba sama nas o tym uprzedziła.

Seniorzy co zrozumiałe starają się dbać o zdrowie. Złodzieje to wiedzą i wykorzystują to przy okazji różnych prób wyłudzenia pieniędzy. Jedną z takich metod oszustwa to fałszywa oferta pakietów medycznych. Złodzieje dzwonią do osoby starszej z propozycją bezpłatnego badania dla seniorów, potem jest rozmowa o stanie zdrowia i wreszcie bardzo atrakcyjna oferta pakietu medycznego. W sytuacji gdzie na wizytę u lekarza trzeba czasami czekać tygodniami, oferta wielu dostępnych specjalistów będzie zawsze bardzo kusząca. Aby mieć dostęp do takiej nieistniejącej usługi trzeba zapłacić z góry - gotówką, kilka nawet kilkanaście tysięcy złotych. W wielu przypadkach oszukani nie dysponując takimi środkami, biorą kredyty. Wszystko w takich przypadkach wygląda bardzo wiarygodnie, dobry profesjonalny kontakt, precyzyjna umowa, czasami fałszywa strona internetowa. Niestety firma w ogóle nie istniała lub zniknęła natychmiast po transakcji. W takiej sytuacji wpłacone pieniądze są praktycznie nie

do odzyskania.

Dużą czujność musimy zachować także przy wszelkiego rodzaju bezpłatnych badaniach albo prezentacjach na które zapraszani są seniorzy. Niejednokrotnie po spotkaniu wychodzą z horrendalnie drogim kompletem garnków, pościeli, urządzeniem do magnetoterapii czy umową na pakiet usług pseudomedycznych. Nierzetelni sprzedawcy ukrywają handlowy cel spotkania, wprowadzają w błąd co do właściwości oferowanych produktów, wmawiają zły stan zdrowia. Nigdy nic na takich pokazach nie podpisujmy!

Podsumowując, aby zapewnić sobie bezpieczeństwo musimy wprowadzić zasadę ograniczonego zaufania. Szczególnie należy zachować czujność jeśli mamy komukolwiek przekazywać pieniądze. Zastanów się chwilę! Zachowaj zdrowy rozsądek i dużą dozę ostrożności. Nie ulegaj presji, nie daj skusić się pozornie atrakcyjnym ofertom, nie działaj pod wpływem chwili! To może być oszustwo!

Rozmawiajmy z rodziną, znajomymi, dzielnicowym. Lepiej dwa razy sprawdzić, niż stracić często oszczędności całego życia.

Zapamiętajmy następujące zasady:

- Nie otwieramy żadnych linków wysłanych sms lub przez inne komunikatory.
- Nigdy nie wykonujemy transakcji bankowych na podstawie linków wysłanych w wiadomościach.
- Nic samodzielnie nie podpisujemy - zawsze trzeba się skonsultować ze znajomymi lub rodziną.
- Weryfikujemy rozmówców a w razie wątpliwości, prosimy aby zadzwonił ew. przyszedł w innym terminie.
- Zawsze bądź ostrożny jeśli ktoś oferuje ci prezenty za przyjście na spotkanie, jeśli idziesz na takie spotkanie - nie idź sam.
- O każdej podejrzanej sytuacji informujemy policję. Im szybciej to zrobimy, tym większe szanse na ustalenie sprawców i ich zatrzymanie, a tym samym udaremnienie dalszych oszustw.

5. Jak się zabezpieczać – czyli profilaktyka bezpieczeństwa w sieci.

1) Bezpieczne hasła

Większość usług internetowych, z których korzystamy wymaga od nas założenia konta, a następnie logowania się do niego za pomocą ustawionego przez nas loginu i hasła. To właśnie hasło jest swego rodzaju szyfrem i zabezpieczeniem do naszych danych, dlatego niezwykle ważne jest, aby było one silne i trudne do złamania. Jak zatem stworzyć takie hasło? Przede wszystkim powinno być trudne do odgadnięcia dla osób trzecich, ale łatwe do zapamiętania dla nas i składać się z co najmniej 12 znaków. Powinno być unikalne – jedno hasło do jednej usługi. Możemy zakładając hasła pomóc sobie kojarząc je z ulubioną książką, miejscem lub filmem.

2) Programy antywirusowe

Jednym z najczęściej stosowanych sposobów, które chronią nasz sprzęt przed zainfekowaniem złośliwym oprogramowaniem są programy antywirusowe. Ważne, aby korzystać z nich w czasie rzeczywistym, używać ich do skanowania dysku, a przede wszystkim pamiętać o ich aktualizowaniu. Dzięki temu nasz antywirus będzie mógł na bieżąco odpowiadać na różne zagrożenia, zwłaszcza te najnowsze. Aby zwiększyć swoje bezpieczeństwo, zachęcamy również do korzystania z zapory sieciowej.

3) Aktualizuj swoje urządzenia, programy i aplikacje, z których korzystasz

Niestety nie zawsze urządzenia, oprogramowanie lub aplikacje, z których korzystamy są w pełni bezpieczne. Zdarza się, że znajdują się w nich błędy i luki bezpieczeństwa, które bardzo często są wykorzystywane przez cyberprzestępców. Regularna aktualizacja systemu operacyjnego, programów, aplikacji i przeglądarek internetowych z ja-

kich korzystamy może uchronić nas przed atakiem cyberprzestępców. Aktualizacje zawierają poprawki, które chronią przed podatnościami i błędami. Jeśli nie będziemy ich stosować, nasze urządzenia mogą zostać zainfekowane.

4) Pomyśl zanim klikniesz, czyli zasada ograniczonego zaufania

Jedną z zasad, o których powinniśmy pamiętać korzystając z internetu, to zasada ograniczonego zaufania. Rozwiązania technologiczne nie wystarczą, aby ustrzec się przed różnymi atakami cyberprzestępców. Musimy pamiętać, że oni stale szukają nowych sposobów i technik, by nas oszukać. Próbują nas zmanipulować, nakłonić do podjęcia działań, które mogą prowadzić do utraty naszych danych lub pieniędzy. Wykorzystują nasze emocje, naiwność oraz brak czasu i życie w biegu. Dlatego jeśli otrzymasz wiadomość, która nakłania Cię do podjęcia natychmiastowych działań, zastanów się czy jest ona prawdziwa. Uważaj również na różnego rodzaju wyjątkowe oferty, wygrane w loterii czy możliwość zainwestowania w kryptowaluty i inne sposoby na szybkie wzbogacenie się. Nie wchodź na strony, które wydają Ci się podejrzane i masz wątpliwości, czy są bezpieczne.

5) Dbaj o swoją prywatność w sieci

O tym, że anonimowość w sieci nie istnieje, wie już większość z nas. Każda nasza aktywność w internecie, zostawia po nas ślad cyfrowy. Istnieją jednak różne sposoby, by móc zwiększyć swoją prywatność w sieci. Jak to zrobić? Przede wszystkim pomyśl, zanim udostępnisz swoje zdjęcia, filmy lub inne informacje o sobie.

Zweryfikuj, czy adres e-mailowy nie jest podejrzany, a w treści nie ma błędów i literówek – bardzo często przekręcane/zamieniane miejscami są litery lub nazwy wskazując na instytucje państwowe

Zadzwoń do danej instytucji w celu zweryfikowania zaistniałego zda-

rzenia, aby potwierdzić że taka wiadomość faktycznie została do Ciebie wysłana – jednak pamiętaj aby nie korzystać z numerów telefonów podanych w podejrzanej wiadomości

Zachowaj spokój i do czasu uzyskania całkowitej pewności nie wykonuj żadnych czynności.

Skontaktuj się z kimś zaufanym z rodziny, znajomych i opowiedz o zdarzeniu.

Jeżeli stałeś się ofiarą oszustów, skontaktuj się natychmiast ze swoim bankiem. Zmień hasła do wszystkich kont bankowych, poczty elektronicznej i innych portali.

6. Co ma zrobić ofiara cyberataku, cybeprzestępstwa?

Poważnym błędem, jaki ofiara cyberataku – organizacja lub osoba fizyczna – może popełnić, jest lekceważenie zagrożenia i marginalizacja problemu. Choć jeszcze kilka lat temu w Polsce nie było organów badających przestępstwa w sieci i ustalenie ich sprawcy było bardzo trudne, obecnie pojawiło się na tym polu wiele zmian. Niewątpliwie miały na to wpływ aspekty prawne, w tym m.in. uchwalenie ustawy o Krajowym Systemie Cyberbezpieczeństwa.

Za przeprowadzanie ataków cybernetycznych grozi kara pozbawienia wolności do 3 lat. Podstawą prawną jest art. 268a Kodeksu Karnego (Niszczenie danych informatycznych). Ze względu na to atak, jego próbę lub podejrzenie ataku powinno się niezwłocznie zgłosić na policję. Organem odpowiedzialnym za tego rodzaju zgłoszenia jest Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV.

Każdy incydent bezpieczeństwa, niezależnie od tego, czy dotyczy firmy, organizacji czy osoby prywatnej, należy zgłosić do dowolnej jednostki CSIRT, np. do Netia CSIRT. Do CSIRT można też zgłaszać wia-

domości zawierające niepokojące treści i odnośniki, złośliwe domeny internetowe czy fałszywe sklepy internetowe.

Zawiadomienie o przestępstwie

Zawiadomienie o przestępstwie powinno zawierać jak najwięcej konkretnych informacji.

Jeżeli uważasz, że jesteś w stanie sam wyczerpująco opisać, co się wydarzyło (a zdarzenie nie wymaga natychmiastowych działań organów ścigania), możesz wysłać pocztą, mailem, faksem czy też przynieść osobiście do jednostki policji napisane przez siebie zawiadomienie o przestępstwie.

Można zatelefonować na numer 997 lub 112.

Państwa bezpieczeństwo jest najważniejsze.

Dbajmy o #BezpieczniePokolenia

Bibliografia

1. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024.

2. Jak chronić się przed atakami cyberprzestępców? Jak chronić się przed atakami cyberprzestępców? - Legalis Administracja.

3. M. Marczyk, Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru, "Przegląd Teleinformatyczny", nr 1-2, 2018.

4. #Metoda na... czyli metody oszustw w sieci, na które trzeba uważać. Poradnik dla seniora.

5. Strony internetowe: www.zus.pl , www.policja.pl , www.bswiecbork.pl , www.zus.info.pl, www.puck.policja.gov.pl , www.businessinsider.com.pl, www.gov.pl, www.samorzad.gov.pl, www.lodz.pl, www.krakow.tvp.pl.

Projekt „Bezpieczne Pokolenia” jest dofinansowany ze środków Ministerstwa Edukacji i Nauki w ramach programu „Międzypokoleniowe Centra Edukacyjne - wsparcie integracji międzypokoleniowej”.

2022