BROSZURA INFORMACYJNA – POWIAT OPOLSKI

„ZAGROŻENIA W CYBERŚWIECIE - JAK CHRONIĆ SIĘ PRZED MANIPULACJĄ I OSZUSTWAMI INTERNETOWYMI?”

Autorka: Beata Gędźba-Kaczmarek - psycholożka, doradczyni zawodowa, nauczycielka, ekspertka ds. edukacji w powiecie opolskim

Projekt A.3.1.1.: „Wsparcie rozwoju nowoczesnego kształcenia zawodowego, szkolnictwa wyższego oraz uczenia się przez całe życie”

WPROWADZENIE

Internet stał się nieodłącznym elementem codziennego życia. Dzięki niemu możemy utrzymywać kontakt z rodziną, dokonywać zakupów, korzystać z usług bankowych, zdobywać informacje czy rozwijać swoje zainteresowania. Wraz z rosnącymi możliwościami pojawiają się jednak również nowe zagrożenia.

Cyberprzestępcy coraz częściej wykorzystują nie tylko luki techniczne, lecz przede wszystkim ludzkie emocje, zaufanie i niewiedzę. Szczególnie narażoną grupą są seniorzy, którzy często nie dorastali w świecie nowych technologii i nie zawsze potrafią rozpoznawać współczesne metody oszustw internetowych.

Dodatkowym czynnikiem zwiększającym ryzyko stania się ofiarą cyberprzestępstwa mogą być samotność, potrzeba kontaktu z innymi ludźmi, większa ufność wobec autorytetów oraz chęć niesienia pomocy potrzebującym.

Skuteczna ochrona przed zagrożeniami w cyberprzestrzeni wymaga połączenia trzech elementów:

- edukacji i świadomości zagrożeń,
- stosowania odpowiednich zabezpieczeń technicznych,
- wsparcia rodziny, przyjaciół i społeczności lokalnej.

PSYCHOLOGICZNE ASPEKTY MANIPULACJI W CYBERŚWIECIE:

Świat wirtualny może być piękny, obfity w treści, obrazy, dźwięki, może oferować nam bogactwo wiedzy, mnóstwo atrakcji i przyjemności. Nie możemy jednak zapominać o tym, że może się on okazać jednocześnie niebezpieczny i zgubny, jeśli nie nauczymy się odpowiednio korzystać z jego dobrodziejstw. Musimy wiedzieć, jak rozpoznawać mechanizmy stosowane przez cyberprzestępców do tego, by pozbawić nas kontroli i sprawstwa, by nami manipulować i skłaniać do podejmowania działań, które służą zaspokajaniu ich potrzeb i realizacji ich celów.

Cyberprzestępcy doskonale wiedzą, jak wykorzystywać nasze postawy, sytuację życiową, schematy myślowe, nasze emocje, nieuwagę i brak krytycznego myślenia. Im bardziej będziemy świadomi zagrożeń i mechanizmów, jakimi się posługują, tym trudniej będzie im nas oszukać. Na co zatem warto zwrócić uwagę i o czym powinniśmy wiedzieć, by nie stać się łatwym celem, a nasze zasoby – łupem cyberprzestępców?

ZAGROŻENIA W SIECI – NAJCZĘSTSZE FORMY CYBERNĘKANIA I CYBERPRZESTĘPCZOŚCI:

- **Cyberstalking, cyberbullying** – nękanie, groźby, upokarzanie w sieci. Cyberstalking polega na prześladowaniu ofiary za pomocą wiadomości, komentarzy czy śledzenia jej działań online. Cyberbullying to agresja wobec osób, zwłaszcza dzieci i młodzieży, przez hejt, ośmieszanie czy publikowanie kompromitujących treści. Warto zwracać uwagę na zmiany w zachowaniu bliskich – nagły spadek ich aktywności w mediach społecznościowych, unikanie rozmów czy mniejsza samoocena mogą oznaczać, że stali się ofiarą cyberprzemocy.
- **Hejt, trolling** – obraźliwe komentarze, prowokowanie konfliktów. Trolle internetowe często działają anonimowo, celowo wywołując kłótnie i wzbudzając negatywne emocje. Hejt ma destrukcyjny wpływ na psychikę ofiar, często prowadzi do depresji, izolacji społecznej, a nawet myśli samobójczych.
- **Grooming, sexting** – manipulowanie ofiarami w celu uzyskania od nich intymnych materiałów. Grooming to zdobywanie zaufania ofiary, zwłaszcza dzieci, w celu ich wykorzystania. Sexting polega na wysyłaniu nagich zdjęć, co może prowadzić do szantażu. Przestępcy często wykorzystują fałszywe profile i aplikacje do nawiązywania kontaktów z młodymi użytkownikami Internetu.
- **Phishing** – jedna z najczęściej spotykanych form cyberprzestępczości. Polega na wysyłaniu fałszywych wiadomości e-mail lub komunikatów w mediach społecznościowych, które wyglądają jak oficjalne wiadomości od zaufanych instytucji. Mogą to być też telefony np. od „wsparcia technicznego". Oszuści podszywają się pod banki, firmy kurierskie lub instytucje i próbują wyłudzić poufne informacje. Często stosują presję czasu – aby skłonić ofiarę do pochopnego działania, grożą np. natychmiastowym zablokowaniem konta, utratą danych lub zasobów, w tym finansowych. Celem jest nakłonienie użytkownika do kliknięcia w link, pobrania załącznika, podania danych logowania, przekazania danych osobowych. Szczególną odmianą phishingu jest **smishing**, czyli phishing realizowany za pomocą wiadomości SMS.
- **Złośliwe oprogramowanie** – malware, wirusy, trojany, ransomware. Programy te mogą kraść dane lub blokować dostęp do komputera. Za ich przywrócenie żąda się od ofiar zapłacenia okupu. Nieświadome pobranie pliku lub kliknięcie w podejrzany link może skutkować zainfekowaniem urządzenia. Malware to oprogramowanie stworzone w celu wyrządzenia szkody użytkownikowi lub przejęcia jego danych. Najczęstsze rodzaje:
  - ✓ **Ransomware -** blokuje dostęp do plików poprzez ich zaszyfrowanie. Przestępcy żądają następnie okupu za odzyskanie danych.
  - ✓ **Spyware -** potajemnie śledzi aktywność użytkownika i przechwytuje informacje.

- ✓ **Trojany -** podszywają się pod legalne programy i umożliwiają przejęcie kontroli nad urządzeniem.
- ✓ **Oszustwa na zdalną pomoc -** przestępca przekonuje ofiarę do zainstalowania programu umożliwiającego zdalny dostęp do komputera. Po uzyskaniu dostępu może przejąć dane osobowe, hasła oraz środki finansowe.

- **Oszustwa inwestycyjne, fałszywe sklepy internetowe, loterie, spadki** – wyłudzanie pieniędzy przez obietnice wysokich zysków lub sprzedaż nieistniejących produktów. Fałszywe platformy inwestycyjne kuszą wysokimi zyskami, a nieistniejące sklepy internetowe przyciągają niskimi cenami. Ofiara otrzymuje wiadomość o wygranej w konkursie, wygranej na loterii, odziedziczeniu majątku. Aby odebrać nagrodę, musi najpierw uiścić opłatę administracyjną lub podać dane osobowe. Jest to klasyczna forma wyłudzania pieniędzy i danych. Cyberprzestępcy tworzą ponadto profesjonalnie wyglądające sklepy oferujące atrakcyjne produkty w wyjątkowo niskich cenach. Po dokonaniu płatności towar nie zostaje dostarczony, kontakt ze sprzedawcą urywa się, a dane płatnicze mogą zostać wykorzystane do kolejnych oszustw.
- **Oszustwa „na rodzinę" lub „na bliską osobę, na przykład „na wnuczka":** –Przestępca kontaktuje się telefonicznie lub przez komunikator pdając się za członka rodziny. Są to najczęściej SMS-y i telefony od rzekomych krewnych proszących o pieniądze. Oszuści podszywają się pod członków rodziny i informują o nagłej sytuacji wymagającej pilnej pomocy finansowej. Coraz częściej wykorzystuje również sztuczną inteligencję do imitowania głosu bliskiej osoby.
- **Oszustwa romantyczne/randkowe** – manipulowanie uczuciami dla wyłudzenia pieniędzy. Oszuści na portalach randkowych budują fałszywe relacje romantyczne, by po pewnym czasie prosić o pomoc finansową. Cyberprzestępcy nawiązują długotrwałe relacje przez Internet. Budują więź emocjonalną, zdobywają zaufanie, a następnie proszą o wsparcie finansowe, tłumacząc się chorobą, wypadkiem, problemami zawodowymi, koniecznością zakupu biletu. Ofiary często tracą oszczędności życia.
- **Fake news, clickbait** – dezinformacja, szerzenie sensacyjnych treści w celu manipulacji opinią publiczną. Fake newsy mogą być wykorzystywane do szerzenia strachu, wpływania na wybory polityczne lub promowania określonych produktów i usług.
- **Fałszywe oferty pracy („praca z domu")** – wyłudzenie danych osobowych lub opłat za „materiały szkoleniowe" lub „materiały do pracy".
- **Oszustwa charytatywne** – fałszywe zbiórki, wyłudzanie darowizn na nieistniejące cele. Oszuści wykorzystują tragedie, katastrofy i ludzką empatię. Tworzą fikcyjne zbiórki pieniędzy, które często wyglądają bardzo wiarygodnie. Wpłacone środki nie trafiają jednak do potrzebujących.
- **Kradzież wizerunku, tożsamości, wyłudzenie danych** – fałszywe profile, przejęcie tożsamości, kradzież zdjęć do oszustw internetowych. Coraz częstsze są przypadki wykorzystywania cudzych zdjęć w celu wyłudzenia pieniędzy lub oszukania innych osób na portalach randkowych i społecznościowych. Kradzież tożsamości polega na wykorzystaniu cudzych danych osobowych bez wiedzy i zgody właściciela. Przestępcy mogą wykorzystać:

- imię i nazwisko,
- numer PESEL,
- adres zamieszkania,
- zdjęcia,
- numer telefonu,
- dane bankowe.

Skutkiem może być:

- zaciągnięcie kredytu na dane ofiary,
- zakładanie fałszywych kont,
- dokonywanie zakupów,
- wyłudzanie świadczeń.

Warto pamiętać, aby nie publikować w mediach społecznościowych zdjęć dokumentów, biletów, kart pokładowych czy informacji umożliwiających identyfikację.

NOWE ZAGROŻENIA W CYBERŚWIECIE – SZTUCZNA INTELIGENCJA, DEEPFAKE I MEDIA SPOŁECZNOŚCIOWE

Cyberprzestępczość w erze sztucznej inteligencji

Rozwój sztucznej inteligencji (AI) przynosi wiele korzyści w codziennym życiu, edukacji, medycynie czy biznesie. Niestety, nowoczesne technologie są wykorzystywane również przez cyberprzestępców. Dzięki narzędziom opartym na sztucznej inteligencji oszuści mogą tworzyć coraz bardziej wiarygodne wiadomości, nagrania głosowe, zdjęcia i filmy, które trudno odróżnić od prawdziwych.

Współczesne oszustwa internetowe stają się coraz bardziej zaawansowane, a ich celem jest wzbudzenie zaufania oraz skłonienie ofiary do przekazania pieniędzy, danych osobowych lub poufnych informacji.

DEEPFAKE – KIEDY NIE MOŻNA WIERZYĆ WŁASNYM OCZOM I USZOM

Deepfake to technologia wykorzystująca sztuczną inteligencję do tworzenia bardzo realistycznych filmów, zdjęć lub nagrań dźwiękowych przedstawiających osoby, które w rzeczywistości nigdy nie wypowiedziały danych słów ani nie wykonywały określonych czynności. Przestępcy mogą wykorzystywać deepfake do:

- podszywania się pod członków rodziny,
- fałszywych rozmów telefonicznych,
- wyłudzania pieniędzy,
- rozpowszechniania nieprawdziwych informacji,
- szantażu,
- niszczenia reputacji konkretnych osób.

Coraz częściej zdarzają się sytuacje, gdy senior otrzymuje telefon od osoby, której głos brzmi identycznie jak głos wnuka lub córki. Rozmówca twierdzi, że znajduje się w nagłej sytuacji i pilnie potrzebuje pieniędzy. W rzeczywistości jest to wygenerowany komputerowo głos. Dlatego każdą prośbę o pieniądze należy zawsze zweryfikować poprzez bezpośredni kontakt z bliską osobą pod znanym numerem telefonu.

OSZUSTWA Z WYKORZYSTANIEM SZTUCZNEJ INTELIGENCJI

Nowoczesne narzędzia AI pozwalają przestępcom tworzyć:

- profesjonalne wiadomości e-mail bez błędów językowych,
- fałszywe strony internetowe,
- realistyczne zdjęcia osób, które nie istnieją,
- automatyczne rozmowy telefoniczne,
- chatboty podszywające się pod pracowników instytucji.

W rezultacie coraz trudniej rozpoznać oszustwo wyłącznie na podstawie wyglądu wiadomości czy strony internetowej. Dlatego należy zachować szczególną ostrożność nawet wtedy, gdy komunikat wydaje się profesjonalny i wiarygodny.

ZAGROŻENIA W MEDIACH SPOŁECZNOŚCIOWYCH

Portale społecznościowe stały się ważnym miejscem kontaktów międzyludzkich. Jednocześnie są przestrzenią, w której działają cyberprzestępcy. Najczęstsze zagrożenia obejmują:

- fałszywe profile,
- kradzież tożsamości,
- oszustwa inwestycyjne,
- oszustwa romantyczne,
- wyłudzanie danych osobowych,
- rozpowszechnianie fałszywych informacji.

Przestępcy często tworzą profile przedstawiające atrakcyjne, sympatyczne osoby, aby zdobyć zaufanie użytkowników. Po pewnym czasie proszą o pomoc finansową lub próbują uzyskać dostęp do prywatnych informacji.

FAKE NEWS – DEZINFORMACJA W SIECI

Fake news to celowo rozpowszechniana nieprawdziwa lub zmanipulowana informacja. Może dotyczyć:

- zdrowia,
- polityki,
- finansów,
- katastrof,
- wydarzeń społecznych.

Fałszywe informacje często mają wywołać silne emocje – strach, złość lub współczucie – ponieważ emocjonalne treści są częściej udostępniane. Przed przekazaniem informacji dalej warto:

• sprawdzić źródło wiadomości,
• porównać informacje z innymi źródłami,
• zweryfikować datę publikacji,
• sprawdzić, czy informacja pojawia się na wiarygodnych portalach.

OSZUSTWA INWESTYCYJNE W MEDIACH SPOŁECZNOŚCIOWYCH

Rosnącą popularnością cieszą się oszustwa związane z inwestowaniem. W ostatnich latach znacząco wzrosła liczba oszustw związanych z inwestycjami reklamowanymi na Facebooku, Instagramie czy innych portalach społecznościowych. Przestępcy wykorzystują wizerunki znanych osób, ekspertów lub celebrytów, sugerując ich udział w inwestycjach. Najczęściej obiecują:

• szybkie wzbogacenie się lub pomnożenie oszczędności,
• wysokie zyski bez ryzyka,
• gwarantowany zwrot inwestycji.

Najczęściej dotyczą one kryptowalut, akcji, nieruchomości, funduszy inwestycyjnych. Pamiętajmy: jeśli oferta wydaje się zbyt dobra, by była prawdziwa, najczęściej jest oszustwem. Prawdziwe inwestowanie zawsze wiąże się z ryzykiem. Obietnica dużych zysków przy zerowym ryzyku powinna być sygnałem ostrzegawczym.

CYFROWA ODPORNOŚĆ – NOWA KOMPETENCJA XXI WIEKU

Współczesny użytkownik Internetu powinien rozwijać tzw. odporność cyfrową, czyli zdolność do bezpiecznego funkcjonowania w środowisku online. Odporność cyfrowa obejmuje:

• krytyczne myślenie,
• analizowanie informacji,
• rozpoznawanie manipulacji,
• świadome korzystanie z technologii,
• umiejętność ochrony własnych danych,
• odpowiedzialne zachowanie w sieci.

Jest to jedna z najważniejszych kompetencji współczesnego społeczeństwa informacyjnego.

WPŁYW SPOŁECZNY, MANIPULACJA I SOCJOTECHNIKA – BROŃ CYBERPRZESTĘPCÓW

Podstawowe pojęcia związane z narzędziami, które wykorzystują przestępcy i cyberprzestępcy, by oszukać swoje ofiary, zaangażować je w pożądane przez siebie działania lub zmusić do określonych zachowań:

- **Socjotechnika** – technika manipulacji człowiekiem wykorzystująca mechanizmy reakcji psychologicznych – np. regułę konsekwencji (skłonienie do drobnej decyzji, która prowadzi do większej), regułę zaangażowania (oszustwa romantyczne), presję grupy czy efekt nowości.
- **Technika „stopy w drzwiach"** – psychologiczna technika manipulacji, która polega na nakłonieniu kogoś do współpracy najpierw przez przedstawienie prośby, którą można uznać za niewielką lub rozsądną, a następnie zwiększenie żądania, aby osoba zgodziła się na tę drugą, większą propozycję. Nazwa tej techniki pochodzi od czynności wkładania stopy w drzwi, aby uniemożliwić ich zamknięcie. Ta technika wykorzystuje zasadę konsekwencji i zaangażowania, aby osoba podjęła działanie, które na początku by odrzuciła. Ta technika ma na celu osłabienie oporu osoby, przekonanie jej do współpracy i rozbudzenie potrzeby bycia konsekwentnym w działaniu.
- **Technika „drzwiami w twarz"** – psychologiczna technika manipulacji, która jest przeciwieństwem reguły „stopy w drzwiach". W tym przypadku osoba manipulująca zaczyna od wysunięcia bardzo poważnego i nierealistycznego żądania, które prawdopodobnie zostanie odrzucone, a następnie prezentuje błahą prośbę, którą naprawdę chce osiągnąć, i wywołuje w ten sposób poczucie zobowiązania do jej spełnienia (osoba, która nie zgodziła się spełnić pierwszej prośby, czuje się winna lub zobowiązana i chętniej zgadza się spełnić drugą, mniej wymagającą zaangażowania, wysiłku lub środków prośbę).
- **Inżynieria społeczna:** Inżynieria społeczna jest jedną z najskuteczniejszych metod stosowanych przez cyberprzestępców. Polega na manipulowaniu ludźmi w taki sposób, aby dobrowolnie przekazali poufne informacje lub wykonali określone działania korzystne dla oszusta. Jest to metoda wykorzystywana przez cyberprzestępców, której celem jest manipulacja ludźmi, aby uzyskać od nich dostęp do bankowości elektronicznej lub poufne informacje, takie jak hasła do kont internetowych, numery kont bankowych, dane kart płatniczych czy dane osobowe (na przykład numer PESEL, adres), lub ukierunkować ich na pożądane przez siebie zachowanie, na przykład wpłacenie lub przelanie pieniędzy. Inżynieria społeczna opiera się na zrozumieniu ludzkich emocji, zachowań i słabych stron, co sprawia, że jest trudna do zwalczania za pomocą tradycyjnych środków technicznych. Jest to jedna z najbardziej skutecznych i niebezpiecznych technik stosowanych w cyberprzestępczości, ponieważ atakuje bezpośrednio człowieka, a nie jego systemy informatyczne czy programy antywirusowe. Cyberprzestępcy wykorzystują wiedzę z zakresu psychologii, komunikacji oraz ludzkich zachowań. Psychologiczne mechanizmy wyłudzania danych za pomocą inżynierii społecznej obejmują wykorzystanie ludzkich cech i sposobów postępowania, m.in. zaufania, chęci pomocy, ciekawości czy strachu. Dlatego nawet najlepszy program antywirusowy nie zastąpi zdrowego rozsądku, ostrożności i wiedzy użytkownika.
- **Wpływ społeczny** – może być nieświadomy (nieintencjonalny) lub świadomy (zamierzony). Wpływ społeczny bywa nieświadomy np. w sytuacji, gdy osoba nie zdaje sobie sprawy z tego, że jej zachowanie czy wygląd oddziałuje na sposób myślenia innych ludzi (np. kobieta może nie wiedzieć, że jej atrakcyjność wpływa na postrzeganie jej jako osoby mądrej i/lub kompetentnej). Świadomy wpływ społeczny to manipulacja, w wyniku

której jednostka, grupa czy instytucja wywołuje zmiany w sferze poznawczej, emocjonalnej i/lub behawioralnej człowieka.

- **Manipulacja** – celowe oddziaływanie na myśli, emocje lub zachowania innych osób w sposób ukryty lub podstępny, aby osiągnąć określony cel, często kosztem manipulowanego. Aby wpłynąć na decyzje ofiary, stosuje się różne techniki, takie jak wzbudzanie strachu, poczucia winy czy fałszywego zaufania. Manipulacja opiera się na wykorzystywaniu psychologicznych reguł i mechanizmów (lubienie i sympatia, autorytet, niedostępność, wzajemność, zaangażowanie i konsekwencja, słuszność i jej społeczny dowód).

Manipulacja zaufaniem: Przestępcy bardzo często podszywają się pod znane i zaufane instytucje, takie jak: banki, urzędy, firmy kurierskie, operatorów telefonicznych, Policję, ZUS, GUS, NFZ. Wykorzystują logotypy, profesjonalnie wyglądające strony internetowe oraz oficjalnie brzmiące komunikaty, aby wzbudzić zaufanie i uśpić czujność ofiary.

Manipulacja emocjami: Silne emocje ograniczają zdolność racjonalnego myślenia. Oszuści doskonale o tym wiedzą. Im silniejsza reakcja emocjonalna, tym większe prawdopodobieństwo podjęcia pochopnej decyzji. Podejmowane przez nich próby wywołania silnych emocji mogą sprawić, że osoba stanie się mniej podejrzliwa i bardziej skłonna do podjęcia ryzyka. Często wykorzystywane są emocje, takie jak **sympatia, ciekawość** (np. kliknięcie w clickbait – sensacyjne nagłówki i fałszywe artykuły mające na celu przyciągnięcie kliknięć i generowanie przychodów z reklam) czy **chęć zysku** (np. fałszywe nagrody i „łatwe pieniądze" – kuszenie szybkim zyskiem, bazujące na naszej naturalnej skłonności do unikania wysiłku przy zdobywaniu korzyści). Emocje najczęściej wykorzystywane przez przestępców do manipulowania ludźmi to:

Strach i poczucie zagrożenia: Jedną z najczęściej stosowanych technik jest wzbudzanie lęku. Przestraszona osoba często działa impulsywnie i bez weryfikacji przekazuje dane lub wykonuje polecenia oszustów. Atakujący mogą wywoływać strach u ofiar przez wysyłanie do nich e-maili lub wiadomości tekstowych zawierających fałszywe alarmy bezpieczeństwa, groźby lub ostrzeżenia dotyczące bezpieczeństwa sieciowego, np. o możliwych konsekwencjach w przypadku nieprzestrzegania ich instrukcji. Mogą zagrozić m.in. utratą danych, naruszeniem prywatności, stratami finansowymi, blokadą konta bankowego lub działaniem ze strony organów ścigania. Osoba pod wpływem strachu może być skłonna podjąć pochopne decyzje i udzielić informacji wymaganych przez atakującego.

Przykładowe komunikaty:

- „Twoje konto bankowe zostało zablokowane."
- „Wykryto podejrzaną aktywność."
- „Grozi Ci kara finansowa."
- „Policja prowadzi postępowanie przeciwko Tobie."

Niepewność – tworzenie niejasnych, niepokojących sytuacji może spowodować u ofiary poczucie dezorientacji i zagubienia, co czyni ją bardziej podatną na manipulację. Aby wprowadzić ofiarę w stan lęku i niepokoju, atakujący mogą wykorzystać jej brak pewności co do rzeczywistych konsekwencji działań.

Wstyd i poczucie winy: Manipulanci mogą sugerować, że odmowa pomocy lub brak odpowiedzi świadczy o egoizmie albo może zaszkodzić innym osobom. Takie działania mają wywołać dyskomfort psychiczny i skłonić ofiarę do działania. Atakujący mogą próbować wywołać także poczucie wstydu i winy u ofiary przez sugestię, że nieudzielenie odpowiedzi na ich prośby lub pytania może mieć negatywne konsekwencje dla innych osób lub dla niej samej. Takie manipulacje mogą sprawić, że osoba zdecyduje się udzielić wymaganych informacji.

Empatia, współczucie, chęć pomocy: Wiele osób ma naturalną potrzebę pomagania innym. Oszuści wykorzystują tę cechę, tworząc historie o ciężkiej chorobie, tragedii rodzinnej, katastrofach, zbiórkach dla potrzebujących. W rzeczywistości pieniądze trafiają do przestępców. Atakujący mogą próbować zyskać zaufanie ofiary, wywołując u niej uczucia współczucia lub empatii. Mogą to robić przez podszycie się pod potrzebującą pomocy osobę lub organizację, która rzekomo cierpi na skutek braku informacji lub wsparcia. Atakujący mogą zaaranżować sytuację, w której ofiara musi natychmiastowo udzielić wsparcia, np. przez przesłanie informacji uwierzytelniających.

PSYCHOLOGIA OSZUSTW INTERNETOWYCH – DLACZEGO DAJEMY SIĘ NABRAĆ?

Poczucie pilnej konieczności / brak czasu na przemyślenie / presja czasu: Cyberprzestępcy wywierają presję czasu. Mogą informować na przykład, że: „Oferta jest ważna tylko przez kilka minut", „Konto zostanie zablokowane", „Konieczne jest natychmiastowe działanie". Celem jest uniemożliwienie spokojnego przemyślenia sytuacji. Oszuści wymagają natychmiastowej reakcji, co ogranicza racjonalne myślenie i sprawia, że podejmujemy decyzje impulsywnie. Atakujący często wywołują uczucie pilnej konieczności lub tworzą sytuacje, które sugerują nagłą potrzebę podjęcia działań lub szybkich decyzji bez zastanowienia. Mogą np. twierdzić, że konto bankowe jest zagrożone lub że istnieje pilna potrzeba aktualizacji hasła czy przesłania skanu podpisu. Mogą sugerować, że konto zostało zhakowane lub zablokowane, a jedynym sposobem na jego odblokowanie jest natychmiastowe przekazanie poufnych informacji, podanie swoich danych osobowych lub finansowych. Atakujący mogą podkreślać, że ofiara powinna działać szybko, aby uniknąć szkód lub niebezpieczeństwa. Mogą to robić przez tworzenie fałszywych limitów czasowych lub stresujących scenariuszy. Wszystkie te techniki opierają się na wykorzystaniu naturalnych reakcji ludzkich na sytuacje stresujące i poczucia pilnej konieczności, co może prowadzić do podejmowania pochopnych decyzji i ujawniania poufnych informacji. Aby się przed tym uchronić, ważne jest, aby zachować zdrowy sceptycyzm wobec niespodziewanych wiadomości, zwłaszcza tych wywołujących silne emocje i zawsze potwierdzać autentyczność żądań przed podjęciem jakichkolwiek działań.

Społeczny dowód słuszności: Ludzie często kierują się zachowaniem innych. Atakujący mogą wykorzystać zjawisko społecznego oddziaływania przez zasugerowanie, że wielu ludzi już podjęło daną akcję (np. udzieliło informacji lub pomocy), co może wpłynąć na decyzję ofiary. Społeczny dowód słuszności to psychologiczny fenomen, w którym ludzie patrzą na działania innych jako wskazówkę lub wsparcie dla swoich własnych zachowań. W praktyce oznacza to, że jeśli duża grupa ludzi robi coś lub wyraża określone przekonania, to istnieje większa tendencja do tego, aby inni bezrefleksyjnie przyjęli te same działania czy przekonania uznając je za słuszne. Widząc, że inni ludzie uwierzyli w jakąś ofertę lub skorzystali z usługi, jesteśmy bardziej skłonni postąpić podobnie, nie analizując zagrożeń. Oszuści wykorzystują ten mechanizm, informując na przykład, że: „Tysiące osób już skorzystało.", „Wszyscy inwestują w ten projekt.", „Setki osób wpłaciły pieniądze." Ma to wywołać przekonanie, że skoro inni to robią, musi być to bezpieczne.

Efekt autorytetu – ludzie łatwiej wierzą informacjom pochodzącym od „ekspertów" (np. oszuści podszywający się pod instytucje państwowe, urzędników, naukowców itp.). Jeśli oszust podszywa się pod eksperta lub przedstawiciela zawodu zaufania społecznego (np. bankiera, funkcjonariusza policji, pracownika GUS, lekarza, prawnika), wówczas ofiara rzadziej kwestionuje jego wiarygodność. Atakujący mogą próbować zbudować zaufanie przez fałszywe sytuacje, stosując chwytliwe nagłówki, logo, rekwizyty, przebranie lub inne elementy sugerujące autentyczność. W tym przypadku atakujący wykorzystują naszą podatność społeczną (ludzie są naturalnie skłonni do zaufania i współpracy) oraz uległość wobec autorytetów.

Reguła wzajemności – mówi ona, że każdej osobie, która wyświadczyła nam jakieś dobro, trzeba się odwdzięczyć. Choć taki gest powszechnie postrzegany jest jako dowód kurtuazji, to równie dobrze można wykorzystać go do osiągnięcia własnych korzyści. Ludzie mają bowiem bardzo silne poczucie zobowiązania i czasem są w stanie spełnić czyjąś prośbę, nawet jeśli wiedzą, że źle postępują. Wystarczy więc, by ktoś oddał nam drobną przysługę, a już ma pretekst, aby w przyszłości domagać się od nas czegoś w zamian. Jeśli ktoś np. „podaruje" nam coś za darmo (np. promocyjne próbki, bonusy), czujemy się zobowiązani do odwzajemnienia, np. przez dokonanie płatności.

Reguła konsekwencji i zaangażowania – ta technika manipulacji wynika z powszechnej dla ludzi cechy, aby za wszelką cenę dążyć do zgodności swoich działań z powziętą wcześniej decyzją. Względy społeczne i kulturowe nakazują nam konsekwentne trzymanie się swoich wyborów, nawet jeśli w dłuższej perspektywie wymagają one działań sprzecznych z naszym interesem. W praktyce oznacza to, że gdy dana osoba zobowiąże się do wykonania czegoś, później z reguły nie wycofuje już swojej deklaracji. Oszust często nakłania do poczucia zobowiązania przez konsekwencje lub zaangażowanie w pewne działania.

Reguła sympatii – jednym z najprostszych sposobów przekonania kogoś do określonego zachowania jest… zaprzyjaźnienie się z nim. Ludzie z reguły chętniej ulegają wpływom osób, które znają i lubią. Ta powszechna obserwacja otwiera szerokie pole do manipulacji. Badania naukowe dowiodły, że wystarczy, aby manipulator był do nas podobny (miał zbliżony do nas

styl ubierania, zainteresowania, poglądy), a jesteśmy bardziej skłonni spełnić jego prośbę. Podobnie działają na nas komplementy.

Efekt bańki informacyjnej i potwierdzenia – wierzymy w informacje, które pasują do naszych przekonań, ponieważ nasz mózg unika dysonansu poznawczego czyli napięcia psychicznego, które pojawia się w sytuacji sprzeczności, niezgodności lub braku spójności informacji.

JAK CHRONIĆ SIĘ PRZED MANIPULACJĄ W CYBERPRZESTRZENI?

Edukacja, świadomość i ostrożność w działaniu są kluczowe dla zapobiegania tego rodzaju atakom. Osoby korzystające z sieci powinny być świadome zagrożeń związanych z inżynierią społeczną oraz manipulacjami stosowanymi przez oszustów i zawsze zachowywać ostrożność w udzielaniu poufnych informacji, szczególnie w odpowiedzi na niespodziewane e-maile, wiadomości czy telefony.

Zasady rozpoznawania oszustw:

- ✓ Zwracaj uwagę na adres URL, certyfikaty bezpieczeństwa i inne wskaźniki wiarygodności.
- ✓ Bądź nieufny/a wobec „zbyt dobrych ofert" i pamiętaj, że zbyt atrakcyjne oferty często są oszustwem. Należy zawsze zachować zdrowy rozsądek i sceptycyzm zanim podejmiemy decyzję o skorzystaniu z takiej „wyjątkowej" oferty.
- ✓ Korzystaj z niezależnych źródeł i recenzji w celu oceny wiarygodności usług i produktów.
- ✓ Rób zakupy tylko na renomowanych stronach internetowych.
- ✓ Sprawdzaj opinie innych klientów oraz bezpieczeństwo płatności.

Sygnały ostrzegawcze:

- ✓ Nietypowe wiadomości e-mail;
- ✓ Podejrzane adresy internetowe;
- ✓ Nieoczekiwane wiadomości;
- ✓ Prośby o podanie haseł;
- ✓ Żądania szybkiego działania;
- ✓ Groźby i naciski;
- ✓ Błędy gramatyczne i ortograficzne w komunikatach;
- ✓ Nienaturalny styl wypowiedzi lub dobór słów;

- ✓ Brak adekwatnych informacji od nadawcy;
- ✓ Nieoczekiwane zmiany w rachunkach czy transakcjach finansowych;
- ✓ Prośby o kliknięcie w linki lub otwarcie załączników.

PODSTAWOWE ZASADY CYBERBEZPIECZEŃSTWA

Twórz silne, unikalne hasła do różnych kont i regularnie je zmieniaj, korzystaj z menedżerów haseł, które ułatwiają zarządzanie skomplikowanymi hasłami, **stosuj uwierzytelnianie dwuskładnikowe (2FA) na ważnych kontach,** takich jak e-mail, bankowość internetowa i media społecznościowe. Osoba tak logująca się do serwisu musi potwierdzić swoją tożsamość na dwa sposoby, np. przez e-mail i SMS. Dwuskładnikowe uwierzytelnianie znacząco zwiększa bezpieczeństwo kont. Nawet jeśli ktoś pozna hasło, nie zaloguje się bez dodatkowego kodu potwierdzającego

Hasło powinno:

- mieć co najmniej 12 znaków,
- zawierać małe i wielkie litery,
- zawierać cyfry i znaki specjalne,
- być unikalne dla każdego konta.

Aktualizuj urządzenia

Regularnie aktualizuj:

- system operacyjny,
- przeglądarkę internetową,
- program antywirusowy,
- aplikacje.

Aktualizacje usuwają luki bezpieczeństwa wykorzystywane przez cyberprzestępców.

Korzystaj z renomowanego oprogramowania ochronnego

Dobrze zabezpieczony komputer lub telefon powinien posiadać:

- aktualny program antywirusowy,
- ochronę przed phishingiem,
- zaporę sieciową (firewall).

JAK CHRONIĆ SWOJĄ PRYWATNOŚĆ W INTERNECIE?

Aby zwiększyć bezpieczeństwo, warto stosować kilka podstawowych zasad:

- Unikaj podejrzanych linków, nie otwieraj załączników z nieznanych źródeł, nie używaj publicznych sieci Wi-Fi do logowania się na konta;
- Nigdy nie podawaj swoich danych osobowych nieznanym osobom przez telefon, e-mail ani w mediach społecznościowych;
- Nie publikuj nadmiernej ilości informacji o sobie;
- Ogranicz widoczności profilu w mediach społecznościowych;
- Regularnie aktualizuj ustawienia prywatności;
- Nie udostępniaj zdjęć dokumentów;
- Ostrożnie podchodź do próśb o pieniądze;
- Sprawdzaj wiarygodność nowych znajomości internetowych;
- Dbaj o bezpieczeństwo techniczne – korzystaj ze wsparcia technicznego i z bezpiecznych przeglądarek internetowych z funkcjami blokowania reklam i ochroną przed phishingiem. Używaj i regularnie aktualizuj renomowane oprogramowanie antywirusowe i antyphishingowe, które chroni przed złośliwym oprogramowaniem i próbami wyłudzania danych;
- Regularnie sprawdzaj źródła informacji, ucz się o nowych zagrożeniach, czytaj ostrzeżenia o popularnych oszustwach, zyskaj wiedzę o najnowszych metodach oszustw internetowych, takich jak fałszywe e-maile od banków, oszustwa związane z wygranymi w konkursach czy fałszywe oferty sprzedaży.
- Bądź świadomy – chroń siebie i innych! Cyberprzestępczość stale ewoluuje, dlatego kluczowe jest bycie na bieżąco z zagrożeniami. Dbaj o swoje dane, bądź czujny i edukuj innych. Bezpieczeństwo w sieci zaczyna się od Ciebie!

CO ROBIĆ, GDY PODEJRZEWASZ OSZUSTWO?

Jeżeli podejrzewasz próbę wyłudzenia:

1. Nie odpowiadaj na wiadomość.
2. Nie klikaj w linki.
3. Nie pobieraj załączników.
4. Skontaktuj się bezpośrednio z instytucją, która rzekomo wysłała wiadomość.
5. Zmień hasła do swoich kont.
6. Powiadom rodzinę.
7. Zgłoś incydent odpowiednim służbom.

Podejrzane wiadomości SMS można zgłaszać do **CERT Polska pod numer 8080**.

Zgłaszaj podejrzane aktywności/incydenty (np. podejrzenia kradzieży tożsamości, oszustwa finansowego, nietypowe wiadomości, telefony bądź strony internetowe) odpowiednim służbom i organom, takim jak banki, firmy technologiczne czy Policja. W przypadku utraty pieniędzy lub danych należy niezwłocznie skontaktować się z bankiem oraz zgłosić sprawę Policji.

Informuj bliskich, ale także znajomych i swoją społeczność o próbach oszustwa.

ROLA RODZINY I SPOŁECZNOŚCI

Bezpieczeństwo seniorów w sieci nie zależy wyłącznie od nich samych. Bardzo ważne jest wsparcie dzieci, wnuków, przyjaciół, organizacji senioralnych, instytucji lokalnych. Warto regularnie rozmawiać o nowych zagrożeniach, wspólnie analizować podejrzane wiadomości oraz pomagać w rozwiązywaniu problemów technicznych. Otwarte rozmowy mogą skutecznie zapobiec wielu oszustwom.

PAMIĘTAJ: Jeżeli wiadomość lub telefon wywołuje silne emocje, presję czasu lub obiecuje wyjątkowe korzyści – zatrzymaj się i zastanów. Cyberprzestępcy najczęściej nie atakują komputerów. Atakują emocje, zaufanie i pośpiech. Najlepszą ochroną jest zasada: **ZATRZYMAJ SIĘ – POMYŚL – SPRAWDŹ – DOPIERO POTEM DZIAŁAJ.**

PODSUMOWANIE

Cyberprzestępczość jest jednym z najpoważniejszych wyzwań współczesnego świata cyfrowego. Oszuści coraz częściej wykorzystują nie zaawansowane technologie, lecz psychologiczne mechanizmy wpływu społecznego, emocje i zaufanie ludzi.

Najskuteczniejszą ochroną jest połączenie wiedzy, ostrożności i wsparcia ze strony bliskich. Świadomość metod działania cyberprzestępców pozwala rozpoznawać zagrożenia, podejmować bezpieczne decyzje oraz korzystać z Internetu w sposób odpowiedzialny i bezpieczny.

Pamiętajmy – w cyberświecie najważniejszym zabezpieczeniem jest świadomy użytkownik.