SENIORZY DLA SENIORÓW
KURS
SILNI W SIECI

Kurs: "Silni w Sieci"

Spis Treści

Projekt "Silni w Sieci"

Projekt „Seniorzy dla Seniorów", to wyjście poza klasyczne akcje czy kampanie edukacyjne. Ten projekt daje Seniorom konkretne narzędzia do samostanowienia i samoobrony na własnych zasadach. Daje możliwość realizowania siebie, rozwijania się i dbania o siebie nawzajem.

Autorzy Projektu chcą rozwijać kompetencje cyfrowe, wspierać gotowość, odporność Seniorów podczas korzystania z Internetu.

Seniorzy, jak pokazuje ich uczestnictwo w zajęciach organizowanych przez Uniwersytety Trzeciego Wieku i aktywność w działaniach organizacji pozarządowych chcą być jak najdłużej samodzielni. Podejmować aktywności w dogodny dla siebie sposób, dostosowany do możliwości bez stawiania barier wynikających z ograniczeń wiekowych.

Autorzy Projektu dostrzeli siłę inicjatyw senioralnych i potencjał Seniorów do jednoczenia się i wspólnego działania. Dlatego projekt opiera się na tutoringu rówieśniczym jako najlepszej formie przekazywania wiedzy i umiejętności w środowisku senioralnym.

Dofinansowane przez Unię Europejską

Partnerzy projektu

OSTROWIEC ŚWIĘTOKRZYSKI

CIRSA

UNIWERSYTET TRZECIEGO WIEKU WSBIP OSTROWIEC ŚWIĘTOKRZYSKI

GOŁUCHOWSKI

INICJATYVA TEZAURAS

SENASIS KĖDAINIŲ TREČIOJO AMŽIAUS UNIVERSITETAS

Dlaczego cyberprzestępstwa działają?

IINFORMACJA DLA WYKŁADOWCY:
Rodzaj aktywności: wykład, przedstawienie i omówienie przykładów, dyskusja
Czas: 60 minut

Kto z nas tego nie słyszał: "Nie jesteś online? Nie istniejesz". Cyberprzestrzeń stała się tak realna, jak ja i Ty, rozrosła się i przekroczyła granice, w sposób, w jaki jeszcze 15 lat temu byśmy nie pomyśleli. Możemy protestować ale cyberprzestrzeń kształtuje naszą rzeczywistość, widzimy to na każdym kroku. Z pewnością, wielu z nas, zgodzi się ze stwierdzeniem, że Internet daje nam niesamowite możliwości, jak: utrzymywanie ciągłego kontaktu z naszymi bliskimi i przyjaciółmi, pomimo geograficznej odległości; nauki nowych rzeczy; łatwiejszego podróżowania; poznawania nowych ludzi; dzielenia się naszą wiedzą; publikowania ważnych rzeczy; odkrywania świata, a nawet pomagania ludziom w nim żyjącym. Wielu również zgodzi się z tym, że aby dotrzeć do tych wartościowych elementów, musimy najpierw przebrnąć przez morze niepotrzebnych, a nawet szkodliwych treści, które często odwracają naszą uwagę, sprawiając że przeglądamy memy, albo oglądamy filmiki z kotami przez kilka godzin. Jest również i trzecia strona, na którą nikt z nas nie chciałby trafić – cyberprzestępczość.

Ponieważ skala cyberprzestępczości wciąż rośnie, badacze coraz częściej przyglądają się motywacjom złodziei, korzystając z profilowania psychologicznego. Przestępcy szukają luk w zabezpieczeniach, błędów w oprogramowaniu lub też błędów wynikających z braku wiedzy użytkowników, bramy do czyiś zasobów. Z jednej strony, anonimowość, potencjalnie małe ryzyko bycia złapanym i proporcjonalnie wysoki zysk, z drugiej dokonanie cyberataku na dużą skalę, daje przestępcom możliwość bycia zauważonym i bycia sławnym, pieniądze stają się wtedy jedynie dodatkiem.
My, jako prywatni użytkownicy, możemy stać się ofiarami hakerów na wielu różnych poziomach. Najbardziej prawdopodobne jest, że spotkamy przestępcę, który pragnie jedynie zysku finansowego, używając do tego przeróżnych narzędzi i metod, aby osiągnąć swój cel.

Badaczka, Lisa O'Reilly w jednym ze swoich artykułów, przedstawiła 9 punktów, odpowiadających na pytanie, dlaczego cyberataki są tak skuteczne:

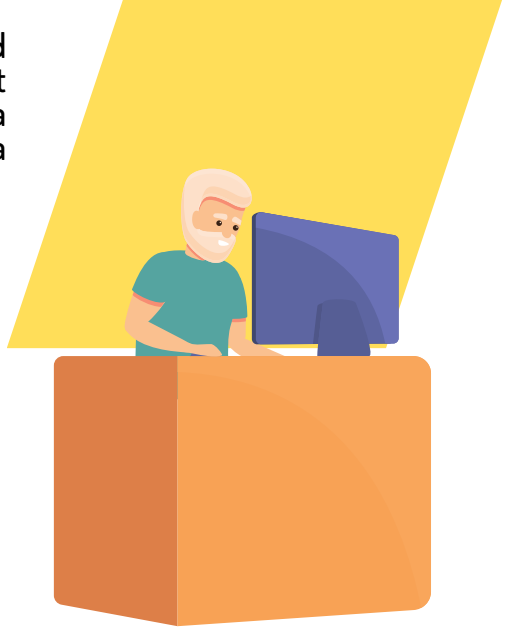
- Cyberprzestępcy są inteligentni i zdolni. Sieć cyberprzestępców jest bardzo dobrze zorganizowania, opiera się na współpracy jej członków i przede wszystkim jest świetnie opłacana. Co więcej, obecnie posiadają oni technologiczne zasoby aby rozbudować i użyć nowych, wyrafinowanych sposobów atakowania innych. Nie oznacza to jednak, że My nie jesteśmy inteligentni, ale pamiętajmy, przestępcy żyją z oszukiwania innych. Nieustannie pracują nad nowymi metodami. Pomyśl o tym jak o typowej pracy, w której dochód zależy od kreatywności i godzin pracy.
- Przestępcy naprawdę dobrze zarabiają na swojej pracy dlatego są zmotywowani i żądni wyników.
- Organizacje popełniają błędy. Badacze wskazują, że wiele organizacji nie posiada odpowiednich zabezpieczeń, ani planów awaryjnych dla zapewnienia operacyjności. Brak odpowiednich systemów i przeszkolonych pracowników, stwarza niebezpieczną lukę dla tych, którzy jej szukają.

- Użytkownicy popełniają błędy. Często to właśnie my, użytkownicy, robimy coś, co może zostać wykorzystane przez przestępców do zdobycia naszych danych: np. udostępnianie loginów, danych z dokumentów tożsamości, używanie tego samego hasła do wielu/wszystkich kont, klikanie podejrzanych linków, używanie niezautoryzowanych urządzeń i aplikacji, odrzucanie aktualizacji oprogramowania itp.
- Dostawcy usług popełniają błędy. Nawet duże firmy, zajmujące się tworzeniem programów, mogą zrobić coś, co narazi ich użytkowników na cyberataki.
- Większość rozwiązań bezpieczeństwa cybernetycznego NIE działa w czasie rzeczywistym. Osoby odpowiedzialne za cyberbezpieczeństwo zawsze są o krok w tyle za przestępcami.

Cyberprzestępcy używają również tzw. inżynierii społecznej, taktyki polegającej na manipulowaniu ludźmi, poprzez np.: stworzenie przekonujących historii, które pozwolą na zdobycie czyjegoś zaufania; tworzenia „zasłony dymnej" dla prawdziwych zamiarów; wzbudzenia poczucia pośpiechu i strachu. Takie sposoby pomagają w wyłudzeniach danych i pieniędzy od ofiar.
Kiedy pomyślimy o bezgranicznym charakterze cyberprzestrzeni i tym samym braku ograniczeń również dla cyberprzestępczości możemy odczuwać strach, przytłoczenie, myśleć, że nie mamy żadnych możliwości obrony, jesteśmy zdani na nieubłaganą statystkę, możemy jedynie czekać i mieć nadzieję, że skutki ataku na nas nie będą, aż tak dramatyczne. Najgorsze jednak co możemy zrobić, to pozostać w tym poczuciu niemocy i nie prosić o pomoc, nie szukać jej. Walka z cyberprzestępczością jest naszym wspólnym obowiązkiem, musimy pomagać sobie nawzajem, pokonywać nasze lęki i wstyd, które łączą się ze strachem przed staniem się ofiarą, lub z faktu stania się nią.

Będzie w błędzie, ten kto uważa, że jedynie starsze osoby są ofiarami cyberprzestępstw. FBI w swoim corocznym raporcie (ostatni z 2021 roku), przedstawia dokładne dane dotyczące zgłaszanych przestępstw w USA, zestawiając je z wiekiem ofiar i całkowitymi stratami w podziale na grupy wiekowe. Okazuje się, iż istotnie Seniorzy stanowią największą grupę w podanych badaniach, nie są jednak jedyną grupą. Trywializmem będzie stwierdzenie że nawet młodzi ludzi, dorastający w erze Internetu, stają się ofiarami, ciągle doskonalących się w swoim fachu, cyberprzestępców. Cytując za portalem fully-verified.com, jedną z najbardziej popularnych metod oszukiwania ludzi są strony internetowe i aplikacje mobilne, których „młode pokolenie" używa każdego dnia.
Oszustwa działają, ponieważ imitują rzeczywistość. Znalezienie różnicy wymaga od nas niemal detektywistycznego zmysłu, spostrzegawczości, świadomości i wiedzy co pracownicy danych instytucji mogą od nas wymagać, a czego nie. Pośpiech i strach towarzyszy cyber-oszustwom na każdym kroku. Przestępcy chcą wprowadzić element nagłości, strachu, że jeśli czegoś nie zrobimy, stracimy coś cennego. W takiej sytuacji, niewiele osób jest w stanie zachować zimną krew i zachować się racjonalnie, nasza podświadomość przejmuje nad nami kontrolę, chcąc uchronić nas przed stratami. Przestępcy wykorzystują mechanizmy obronne, w które wyposażyła nas natura, przeciwko nam.

Badacz Eddy Willems opisuje sześć kluczowych zasad wpływu, które wyjaśniają psychologiczny aspekt cyberprzestępstw. Możemy to określić jako esencja odpowiedzi na pytania, dlaczego cyberprzestępstwa działają?



1 **Zasada wzajemności.** oznacza, że ludzie czują się zobowiązani wobec kogoś, kto albo coś dla nich zrobił, albo coś im zaoferował lub dał, bezinteresownie. Wyobraź sobie taką sytuację: Klient został poinformowany, że doradca bankowy uratował jej/jego oszczędności, teraz poprosi o coś drobnego, na przykład zalogowanie się do konta bankowego, lub podanie mu danych bankowych. Kwestionowanie dobrych intencji tej osoby, w sytuacji, w której uratował Klienta przed oszustem, wydaje się absurdalne. Dajemy oszustowi, to co chce, bo z naszej perspektywy wydaje się to nieszkodliwe.

2 **Konsensus.** Gdy nie jesteśmy pewni jakieś kwestii, decyzji, szukamy potwierdzenia u innych osób. Nawet jeśli jesteśmy przekonani co do pewnych rzeczy, często czyjaś opinia lub opinia grupy, potrafi być bardzo przekonująca. Pamiętasz ogromną skalę dobrowolnej pomocy Polek i Polaków dla Ukrainy po rosyjskiej agresji w lutym 2022 roku? Wiele osób założyło wtedy organizacje charytatywne zbierające pieniądze i pomoc rzeczową, która znacznie przyczyniła się do polepszenia dramatycznej sytuacji osób dotkniętych wojną. Cyberprzestępcy wykorzystali również i tą sytuację, szukając zysku, oszukując tych który z dobroci serca przekazywali datki na rzecz pomocy krajowi ogarniętemu wojną.

3 **Zasada konsekwencji.** Lubimy działać zgodnie z wcześniej wypowiedzianymi poglądami, chcemy zachować spójność między tym co mówimy, a tym co robimy. Poprzez zaangażowanie, odczuwamy presję zachowania się w określony sposób. Wyobraźmy sobie sytuację, rozmawiamy przez telefon z kimś kto podał się za pracownika organizacji pozarządowej, pyta się czy uważamy pomoc dla Ukrainy za słuszną, zgadzamy się z tym twierdzeniem, następnie ta osoba prosi nas o niewielki datek, na wsparcie tej sprawy. Chcąc zachować spójność pomiędzy tym co przed chwilą powiedzieliśmy, a tym jak się zachowamy, nawet czując się niepewnie w przekazywaniu pieniędzy w taki sposób, bardziej prawdopodobne jest, że mimo tych obaw, przekażemy datek. Zwłaszcza jeśli nasz rozmówca użyje zdań typu: „każdy ma swój wkład", „nikt nie odmawia pomocy", „osoby dobrego serca wpłacają nawet drobną kwotę".

4 Często dla wzmocnienia zasady konsekwencji używa się **zasady autorytetu** – a więc ktoś wspiera swoje słowa lub swoją prośbę czyimś autorytetem, np. polityka, naukowca, a nawet celebryty. Nasza podświadomość ma tendencję, do przyjmowania zewnętrznych opinii osób uznawanych za znane i/lub szanowane jako priorytetowe, mogą to również być osoby wobec których odczuwamy sympatię, współczujemy im, lub zwyczajnie lubimy.

5 **Niedostatek.** Kiedy wiemy, że mamy ograniczony czas, lub jego brak, na działanie, jesteśmy bardziej skłonni przyjąć czyjąś propozycję rozwiązania problemu. Przykładem są maile phishingowe, rzekomo pochodzące od organów podatkowych, wzywające ludzi do szybkiej odpowiedzi poprzez kliknięcie w link, w przeciwnym razie grozi kara grzywny. Najczęściej klikamy bez zastanowienia się nad możliwymi konsekwencjami, w końcu każdy z nas boi się Skarbówki.

Nikt z nas nie jest w ciągłej gotowości, czekając na atak na każdym kroku, sprawdzając za każdym razem zieloną kłódkę, literując każdy link, który otrzymamy lub prosząc dzwoniącego do nas przedstawiciela, aby zweryfikował autentyczność swoich uprawnień. Oszuści stają się coraz mądrzejsi i wykorzystują przewagę jaką dają im nowe technologie, nowe produkty, czy wydarzenia na świecie. Tworzą autentycznie brzmiące historie, które przekonają nas do przekazania im naszych pieniędzy lub danych osobistych. Wykorzystują nasz brak wiedzy, chęć pomocy innym i strach.

Często wiele ofiar cyberprzestępstw mówi o odczuwaniu traumy, uczucia bezbronności, strachu przed ponownym staniem się ofiarą. Zupełnie jakby ktoś dokonał na nich fizycznego rabunku, grożąc nożem lub bronią w ciemnej alejce. Uczucie strachu jest realne, nawet jeśli przestępstwo zostało popełnione w cyberprzestrzeni.

Poczucie winy i wstydu, często jest potęgowane, poprzez brak wsparcia od bliskich i przyjaciół, a nawet obwiniania nas za stanie się ofiarą. Ma to miejsce często w przestrzeni społecznej, jak i również np. w miejscu naszej pracy, zwłaszcza jeśli przedmiotem ataku były dane firmy lub urzędu dla której/którego pracujemy.

Pandemia Covid-19 ukazała w jak elastyczny i kreatywny sposób przestępcy dopasowują się do nowych, często dramatycznych okoliczności, jak choroby, katastrofy, ubóstwo, wojna i wykorzystują je do swoich celów. Wydaje się że granice człowieczeństwa i współczucia nie istnieją dla tych osób, co dodatkowo może potęgować nasz strach.
Stygmatyzacja ofiar cyberprzestępstw stwarza niebezpieczną sytuację, w której ludzie będą się bali zgłaszać naruszenie prawa, będą bowiem woleli cierpieć samotnie, niż narazić się na wyśmianie. Trudno się dziwić takiej postawie, patrząc na komentarze pod różnymi wiadomościami o tym, że ktoś stał się ofiarą przestępstwa, np. przekazując fałszywemu policjantowi sporą kwotę. Fala hejtu jaka wylewa się na bezbronne osoby jest wręcz niewyobrażalna i niezwykle obrzydliwa. Działania takie, niestety będą prowadzić do niezgłoszenia przestępstwa, mniejszej wykrywalności a w konsekwencji do upośledzenia całego systemu przeciwdziałającego cyberprzestępczości. Instytucje zapewniające bezpieczeństwo, nie będą działać efektywnie i uczyć się walki z nowymi metodami oszustw, jeśli nie będą otrzymywać informacji o nich. Jednocześnie, nie możemy zapomnieć o wpływie, jaki zamknięcie się na świat i próba poradzenia sobie samemu z faktem stania się ofiarą może mieć dla osób bezpośrednio dotkniętych przestępstwem. Depresja, lęki, załamanie nerwowe mogą być tylko jedynymi z wielu negatywnych implikacji.

Budujący jest fakt, iż coraz częściej możemy spotkać się z trendem walki z cyberzagrożeniami również przez prywatne firmy i korporacje. Banki, policja, rządowe instytucje, a nawet placówki medyczne starają się mieć swój cenny wkład w ochronę obywateli i klientów przed negatywnymi następstwami cyberataków. Jednakże, skoro ten temat zyskuje na popularności i wydaje się wszechobecny w przestrzeni publicznej, dlaczego skala strat wciąż rośnie? Czy te działania są nieefektywne, chybione, nie trafiają do odbiorców, są zbyt trudne do zrozumienia i wdrożenia przez zwykłych obywateli?

Przede wszystkim, są adresowane do ogólnego odbiorcy, nie uwzględniając różnic i potrzeb poszczególnych grup. Zakładają, że krótką informacją "nie rób tego", "rób to", "bądź ostrożny" zbudują bezpieczne zachowania. Cyberzagrożenia są spersonalizowane, uderzają w konkretnego użytkownika, a cyberprzestępcy potrafią poświęć sporo czasu, aby poznać cel swojego ataku.

Pozostała jeszcze jedna kwestia, którą należy omówić. Mówiliśmy już o psychologicznym aspekcie przestępstw i stawania się ich ofiarą, będziemy później omawiać konkretne sytuacje i to jak im zapobiegać. Musimy jednak poświęcić jeszcze trochę czasu na kwestie związane z emocjami i uczuciami jakie mogą towarzyszyć ludziom, którzy padli ofiarą cyberprzestępców. Naszą rolą bowiem, będzie nie tylko tworzenie świadomej społeczności, dzielącej się najlepszymi praktykami, ale także tworzenie bezpiecznej społeczności, która rozumie, co dzieje się w głowie osoby, która została oszukana oraz jak pomóc takiej osobie, lub sobie samemu. Poniżej znajdują się wskazówki i pytania, na które warto odpowiedzieć w przypadku stania się ofiarą cyberprzestępstwa. Poniższe uwagi można przekazać innym osobom, które zostały oszukane w sieci.

- Określ, jak się czujesz i jakie towarzyszą ci myśli? Pamiętaj, że nie jesteś sam.
- Przypomnij sobie swoje mocne strony, osiągnięcia, jako kontrast to tego co straciłeś/aś w wyniku stania się ofiarą cyberprzestępstwa.
- Unikaj obwiniania się za zaistniałą sytuację. Poświęć czas na to, aby przemyśleć czego nauczyłeś/aś się przez tę sytuację, jak możesz to wykorzystać pozytywnie, kogo możesz uchronić przed taką sytuacją, z wiedzą którą teraz posiadasz.
- Poszukaj wsparcia i pomocy, aby uniknąć ponownego stania się ofiarą lub jeśli tego potrzebujesz wsparcia w walce z negatywnymi myślami i obwinianiem się.
- Wybacz sobie błędy które popełniłeś/aś, bądź dla siebie dobry/a, nie oceniaj się, bądź uważny/a na swoje myśli i uczucia, zaakceptuj swoje niedoskonałości, w końcu jesteśmy tylko ludźmi i popełniamy błędy. Pozwól sobie na odczucia strachu, smutku, nawet żałoby. Jeśli czujesz, że te uczucia cię przytłaczają, poproś o pomoc.
- Szukaj wsparcia w swoim otoczeniu, jeśli nie możesz na nie liczyć, wśród najbliższych, poproś o pomoc w grupach wsparcia, u swojego lekarza, wśród swoich znajomych, w organizacjach pozarządowych.
- Nie wahaj się szukać profesjonalnej pomocy, jeśli czujesz, że dane wydarzenie negatywnie wpływa na twoje samopoczucie zgłoś się z tym problemem do lekarza. Przecież, gdyby ktoś napadł Cię na ulicy i pobił nie wstydził/a byś się z tym iść do lekarza/szpitala, tym bardziej nie wstydź się psychologicznej traumy po zdarzeniu w cyberprzestrzeni.

Celem tego projektu, Edukatorów i wszystkich osób, które będą miały dostęp do tych treści jest budowanie świadomości zwłaszcza wśród lokalnych społeczności, edukowanie, pokazywanie jak unikać przestępstw w Internecie, jak przeciwstawiać się nowym wyzwaniom, ale również jak wspierać i być przy osobach, które stały się ofiarą cyberprzestępstw.

Pamiętaj, to że przestępstwo miało miejsce w wirtualnej przestrzeni nie znaczy, że uczucia towarzyszące osobom poszkodowanym nie są realne.

Projekt ten ma też za zadanie zwiększyć świadomość społeczną i przeciwdziałać stygmatyzacji osób poszkodowanych. Zgłębienie tematów związanych z cyberprzestępczością pozwoli nam odzyskać poczucie sprawczości w walce z wrogiem, operującym w wirtualnej przestrzeni.

Sprawdź materiały dodatkowe do tego Modułu

Typy oszustw – mechanizmy

INFORMACJA DLA WYKŁADOWCY
Rodzaj aktywności: warsztat
Czas: 3h
Wykładowco:
1. Rozdaj karty z przykładami i ćwiczeniami.
2. Przedstaw poniższy materiał.
3. Nawiązuj do przykładów i ćwiczeń, wtedy gdy w tekście poniżej zauważysz informację, aby zobaczyć lub wykonać ćwiczenia/przykłady. omawiaj je wspólnie z uczestnikami.
4. Pilnuj czasu – masz do dyspozycji 3 godziny w systemie 45minut nauki, 15 minut przerwy.

Istnieje wiele różnych metod oszukiwania w sieci, cyberprzestępcy wdrażają coraz to nowsze sposoby, aby wykraść pieniądze, dane osobowe czy zastraszyć użytkowników, aby uzyskać to czego potrzebują. Dla celów tego kursu, podzieliliśmy znane metody na kilka kategorii.

- Kradzież danych osobowych;
- Oszustwa dotyczące sprzedawania i kupowania online;
- Oszustwa romantyczne;
- Oszustwa charytatywne;
- Oszustwa inwestycyjne i dot. zarabiania/oszczędzania;
- Oszustwa dot. szukania pracy;
- Oszustwa dot. niespodziewanych wygranych, spadków, nagród;
- Niebezpieczne SMS-y;

01 KRADZIEŻ DANYCH OSOBOWYCH

Dlaczego ktokolwiek miałby chcieć kraść czyjeś dane osobowe? Komu jest potrzebny numer dowodu osobistego czy paszportu? Dane osobowe przeciętnych obywateli mają dużą wartość dla przestępców. Głównym motywem działań wielu cyberprzestępców są pieniądze, a numer dokumentów często połączony jest z kontem bankowym. Kiedy przestępcy zyskają dostęp do twoich dokumentów, numeru karty kredytowej, danych logowania do twojego konta bankowego lub maila, mogą dokonać przelewów, zakupów, otwierać nowe konta, brać pożyczki. W ten lub inny sposób, mogą sprawić, że stracisz pieniądze lub zostaniesz zmuszona/y do spłacania nie swoich kredytów.

Dlaczego złodzieje potrzebują danych osobowych:

1. Aby podszyć się pod daną osobę i wyłudzić kredyt/pożyczki;
2. Twoje dane mogą być użyte do uzyskania dostępu do innych sfer twojego wirtualnego życia, w tym dostępu do bankowości, szczegółów kart kredytowych;
3. Aby kraść dane osobiste innych osób powiązanych z tobą, jak rodzina, przyjaciele, współpracownicy;
4. Aby zaszkodzić twojej reputacji, spowodować publiczne upokorzenie - forma znęcania się w wirtualnym świecie;
5. Aby uzyskać dostęp do innych informacji np. zawodowych, zwłaszcza jeśli zajmujemy wyższe stanowisko.
6. Aby uzyskać dostęp do historii finansowej i używać jej przeciwko nam;
7. Aby ukraść nasze konto w mediach społecznościowych, zwłaszcza jeśli posiadamy wielu obserwujących, aby sprzedać takie konto, lub dokonywać z naszego konta prób wyłudzeń na innych użytkownikach.

Przypominasz sobie jakiekolwiek doniesienia dotyczące kradzieży lub wycieku danych użytkowników na dużą skalę? Takie problemy miał m.in. Sony PlayStation Network, Uber, Yahoo, hotel Marriott, a nawet popularny Facebook. Może ci się wydawać, że w żaden sposób nie ucierpiałeś w tych wydarzeniach. Możesz mieć rację, pomyśl jednak o skali, o milionie danych, które trafiły w przestrzeń, do których dostęp mieli wszyscy, zwłaszcza ci którym zależy na czyjeś szkodzie. Nie wszyscy zostali poszkodowani w tym samym stopniu. Wiele osób straciło wskutek tych działań swoje konta, zaczęło otrzymywać maile i wiadomości z dziwnymi linkami i treściami, prośbami o płatności, wymuszeniami.

To że nie straciliśmy ani złotówki z naszego konta bankowego, nie oznacza że nie ponieśliśmy strat w wyniku działań cyberprzestępców.
Mówiąc o kradzieży danych osobowych, należy wspomnieć o atakach phishingowych. To rodzaj wymuszenia, podczas którego przestępcy stosując metody inżynierii społecznej, wykorzystując mechanizmy psychologiczne, oszukują ludzi celem zdobycia takich danych jak: loginy, hasła, dane kart kredytowych. Sprawcy podstępem zmuszają ludzi do otwierania niebezpiecznych linków, takie sytuacje często maja miejsce w sferze sprzedawania i kupowania online.

WYKONAJ ĆWICZENIE NR 1

02 KUPOWANIE I SPRZEDAWANIE

Zgodnie ze wszelkimi przewidywaniami, sprzedaż w Internecie będzie branżą dynamicznie rosnąca w nachodzących latach. Oznacza to, że skala oszustw i prób wyłudzeń w tym zakresie również będzie rosnąć. Coraz więcej osób kupuje online, wśród nich również seniorzy. Obecnie osoby starsze, nie czują się już obco w sieci, coraz częściej używają komputerów, smartfonów, konsol, wiedzą jak kupować w Internecie i nie boją się dokonywać innych operacji w wirtualnej rzeczywistości. Seniorzy stają się istotną grupą, której obecność jest coraz mocniej akcentowana. Jednocześnie stając się celem cyber-złodziei.
Na popularności zyskuje również, łączenie kart bankowych z różnego rodzajami kont. Zdarzają się sytuacje, w których z uwagi na nie wystarczające zabezpieczenia, nasze dane stają się łupem przestępców. Co zrobić, aby uniknąć takich sytuacji? Moglibyśmy odpowiedzieć, wystarczy nie podpinać kart do różnych kont i zapewne mielibyśmy rację, jednakże, od kiedy decyzje w naszym imieniu podejmują przestępcy? Czy mamy nakładać na siebie ograniczenia z uwagi na czyjeś nielegalne działania?
O tym jak zapobiegać utracie naszych danych opowiemy w module 3. Teraz skupimy się na omówieniu najczęstszych rodzajów oszustw.

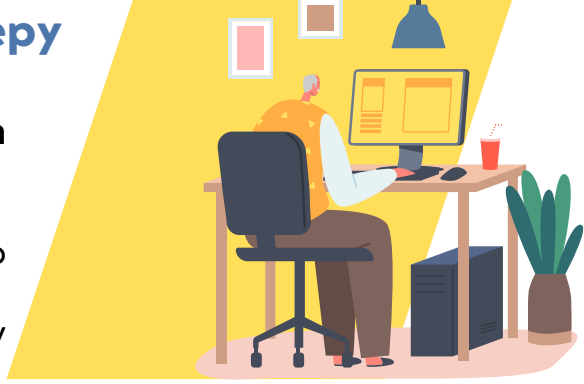
Sprzedawanie przedmiotów

Oszustwa podczas sprzedaży przedmiotów są bardzo popularną formą wyłudzenia na platformach sprzedażowych, takich jak np. Vinted czy Olx. W zdecydowanej mierze są to portale dla prywatnych użytkowników, choć nie tylko. Kiedy próbujemy coś sprzedać, jak nasze stare ubrania, zabawki lub inne przedmioty, oszuści mogą próbować dotrzeć do nas na wiele sposobów i skutecznie wyłudzić nie tylko dany przedmiot, ale ukraść dane kart kredytowych czy login/hasło do konta bankowego. Poniżej przedstawiamy schemat typowego oszustwa na portalu sprzedażowym:

Schemat oszustwa na portalu sprzedażowym:

1. Rozmawiamy z osobą potencjalnie zainteresowaną kupnem, dowiadujemy się, że nie zależy jej na negocjacjach, akceptuje cenę, ewentualne defekty, jest skupiona na zakończeniu transakcji najszybciej jak to możliwe.
2. Po zaakceptowaniu warunków sprzedaży, otrzymujemy za pomocą danego komunikatora link. Kupujący prosi nas o jego kliknięcie, mówiąc, że pieniądze zostaną automatycznie przelane na nasze konto.
3. Zdarza się również, że potencjalny kupujący robi wiele błędów językowych, źle odmienia lub używa danych słów, zupełnie jakby nie znał dobrze naszego języka.
4. Niektórzy, dla uśpienia naszej czujności, odwołują się do zasady ograniczonego zaufania, ponieważ wybierając przedmioty o dużej wartości, proszą o metodę wysyłki „za pobraniem". Wydaje się nam to rozsądne, w końcu, aby odebrać przedmiot będą musieli zapłacić kurierowi. Zanim nabierzemy wątpliwości dostajemy gotowy list przewozowy lub link do strony na której ma się on wygenerować. Informacja o tym jak płatności są realizowane są często ukryte, lub nieczytelne, otrzymujemy normalną etykietę, niestety przewoźnik nie pobierze od kupującego żadnych pieniędzy.
5. Klikając link, możemy również zostać przekierowani na stronę, na której na naszym komputerze zostanie zainstalowane złośliwe oprogramowanie lub na której po wpisaniu naszych danych zostaną one skopiowane.

Specjalne okazje i fałszywe sklepy



Jak poznać, że mamy do czynienia z fałszywym sklepem?

- Strona internetowa nie zawsze jest dopracowana;
- Nazwa sklepu całkowicie nieznana lub jest łudząco podobna nazw innych sklepów;
- Posiada bardzo korzystne ceny, znacznie niższe niż w innych dobrze znanych witrynach sprzedażowych;
- Pojawia się problem z płatnością, którą chcemy realizować w znany nam sposób. E-sklep proponuje nam inną mniej znaną formę, realizuje opcje tylko "za pobraniem". Opcja "za pobraniem" nie jest bezpiecznym rozwiązaniem, gdyż aby sprawdzić co jest w paczce, musimy odebrać ją od kuriera i zapłacić. Jeśli w paczce jest np. sam papier a nie produkt, kurier nie przyjmie zwrotu.
- Strona banku do szybkich płatności na którą przekierowało nam ze strony e-sklepu jest podejrzana, wygląda inaczej niż zawsze, ma błędny adres.

Często otrzymujemy maila z potwierdzeniem złożenia zamawiania, dla uśpienia naszej czujności. Jest to jednak ostatnia wiadomość jaką otrzymamy z tego sklepu. Niekiedy po dłuższym czasie otrzymamy wiadomość, o przedłużających się dostawach z uwagi na różne czynniki. Wierzymy, że kupiliśmy coś w normalnym sklepie, przesyłka jednak nigdy do nas nie dotrze. Kontakt z dostawcą nagle się urwie, możemy też otrzymać dodatkowe wiadomości o zatrzymaniu paczki w urzędzie celnym i konieczności dopłaty. Przesyłka w rzeczywistości, nigdy nie została nadana, możemy również otrzymać paczkę z parą skarpet, zamiast nowym iPhonem za którego zapłaciliśmy.

WYKONAJ ĆWICZENIE NR 2

03 RANDKI I ROMANSE ONLINE

Przez ostatnie kilka lat byliśmy świadkami niezliczonej ilości oszustw opartych na fałszywych historiach miłosnych, oszustwa romantyczne online, są według portalu statista.com na trzecim miejscu pod względem wyłudzonych kwot przez cyberprzestępców. Metodę tą opisano po raz pierwszy w 2008 roku, od tego czasu ogromna liczba osób, w zdecydowanej większości kobiet, choć nie tylko, została brutalnie oszukana. Internet jest ogromną częścią naszego życia, stąd też powszechny jest trend przeniesienia do niego również życia miłosnego.

Oszustwa tego typu zazwyczaj przebiegają podobnie:

1. Otrzymujemy wiadomość w mediach społecznościowych lub na portalu randkowym, na którym mamy konto.
2. Nasz rozmówca najczęściej jest z innego kraju lub ma niezwykle ciekawą i nietypową pracę, połączoną z ciągłymi wyjazdami, poświęceniami, odizolowaniem, często również niebezpieczną, z pewnością ekscytującą.
3. Rozmawiacie przez dłuższy czas, wiele dni, może nawet tygodni, czy miesięcy, oszust zdobywa nasze zaufanie, może nawet uczucie, nie mamy powodu podejrzewać oszustwa.
4. Angażujemy się emocjonalnie w relację – do czego oszust próbował doprowadzić od samego początku. Bardzo dobrze wie, że osobie z którą czujemy się związani znacznie ciężej odmówić, zwłaszcza jeśli od dłuższego czasu szukaliśmy bratniej duszy, lub jesteśmy w trudnej sytuacji osobistej.
5. Mogą zdarzyć się rozmowy video przez komunikatory, wysyłanie zdjęć, nasz „partner" wydaje się być bardzo zaangażowany, jest czarujący, czujemy, że spotkaliśmy odpowiednią osobę, obiecuje spotkanie, zapewnia o uczuciach, zaangażowaniu, obiecuje wspólną przyszłość, wszystkie plany jednak krzyżuje jego wymagająca praca.
6. Po zyskaniu naszego zaufania lub nawet miłości, otrzymujemy często dramatyczną prośbę o pomoc, zazwyczaj kiedy w końcu nasz partner miał możliwość przyjechać do nas. Dowiadujemy się osoba ta ma poważny problem, została obrabowana, potrzebuje pieniędzy na samolot lub inny środek transportu, została niesłusznie aresztowana na lotnisku, potrzebuje pieniędzy na kaucję lub przekupienie urzędnika, lub została porwana.

Zdarza się również, że otrzymujemy prośbę o dostęp do konta bankowego, dokonanie przelewu z naszego konta w imieniu tej osoby, wzięcia pożyczki, wysłania kopii dokumentu tożsamości, aby poświadczyć za kogoś, zakup danego przedmiotu. Prośba często połączona jest z poczuciem pośpiechu i zagrożenia, tak abyśmy nie byli w stanie przeanalizować sytuacji i podejść do sprawy racjonalnie. Oszust chce, aby to emocje, często pochopne i irracjonalne nami kierowały.

Skala oszustw romantycznych wciąż rośnie, swój „rozkwit" miała w czasach pandemii, zwłaszcza w okresach twardych lockdownów. Wtedy też brak możliwości spotkania się osobiście nie budziła większych podejrzeń z uwagi na drastyczne restrykcje, problemy zdrowotne lub kwarantanny. Jednocześnie ludzie zamknięci w swoich domach znacznie bardziej odczuwali samotność, zwracali się więc w stronę jedynego miejsca które nie było ograniczone pandemią, w którym mogli z kimś porozmawiać.

Jak poznać, że ktoś z naszych bliski może być zaangażowany w oszustwo romantyczne:

1. Stają się skryci, nie chcą rozmawiać o swojej relacji, lub ją idealizują, wyszukują wymówek, usprawiedliwiając swojego partnera przed innymi, dlaczego nie może przyjechać, lub komunikuje się wyłącznie wiadomościami tekstowymi. Mogą również reagować złością lub wrogością, lub uciekać od rozmów kiedy pojawia się temat ich partnera.
2. Mogą wyrażać ogromne zaangażowanie emocjonalne i przywiązani do osoby, której nigdy nie spotkały na żywo.
3. Wysłały lub planują wysłać tej osobie pieniądze, mogą nawet chcieć wziąć pożyczki, aby pomóc swojemu wirtualnemu partnerowi.

Jeśli nie masz pewności co do charakteru onlinowej relacji, poszukaj znaków ostrzegawczych tzw. czerwonych flag:

1. Bądź podejrzliwy/a w sprawie jakikolwiek próśb o pieniądze, zwłaszcza jeśli pochodzą one od osób, które znasz tylko wirtualnie.
2. Poproś o radę osoby z zewnątrz, kogoś bliskiego, przyjaciela, członka rodziny, kto bezstronnie oceni sytuację.
3. Sprawdź tę osobę w Internecie, często zdjęcia profilowe mogą nie być oryginalne, użyj wyszukiwania obrazem w przeglądarkach internetowych, możesz odkryć informacje zupełnie odmienne od tego co wmawia ci osoba po drugiej stronie ekranu.

WYKONAJ ĆWICZENIE NR 3

04 FAŁSZYWA DOBROCZYNNOŚĆ

Oszuści nie znają granic w poszukiwaniu nowych metod oszukiwania ludzi. Fałszywa dobroczynność jest niezwykle efektywna, zwłaszcza połączona z metodami manipulacji. Odwołuje się bowiem do ludzkiej dobroci, bazuje na drobnych, mało podejrzanych prośbach, jak potencjalnie niskie kwoty dotacji. W swoim zaufaniu do organizacji charytatywnych, nie możemy sobie nawet wyobrazić, że ktoś używałby czyjeś choroby lub cierpienia, aby zarobić na tym pieniądze.

Oszuści zdają sobie również sprawę, że istnieją określone sytuacje, które dosłownie otwierają serca i portfele ludzi, jak krzywda dzieci, katastrofy naturalne w innych państwach, czy konflikty zbrojne. Niektórzy oszuści perfekcyjnie kopiują lub podszywają się pod prawdziwe instytucje, często też wykorzystując ich metody, jak bezpośrednie prośby, wysyłane np. mailowo, czy aukcje charytatywne. Zdarza się, że oszuści działają pod szyldem prawdziwej działalności, zarejestrowanej organizacji, która być może nawet w pewnym niewielkim stopniu, realizuje działania charytatywne, w rzeczywistości odsetek realnego wsparcia tej organizacji jest znikomy.

Oszuści stosują podobne metody:

- Presja czasu – podobnie jak w poprzednich metodach, naciski, pośpieszanie, wprowadzanie uczucia braku czasu, jest oznaką potencjalnie niebezpiecznej sytuacji. Żadna prawdziwa organizacja charytatywna nie będzie od nas wymagać płatności w tej chwili, nie będzie wywierać na nas presji, jej przedstawiciele poświęcą nam czas, opowiedzą o działaniach, wyślą ulotkę, przedyktują adres strony internetowej, ich media społecznościowe będą najczęściej uzupełniane regularnie, przez dłuższy czas, będą mieli dostępne sprawdzone, powszechnie znane i stosowane oraz bezpieczne metody przekazania datków.
- Przestępcy często będą chcieli zmusić nas do metod płatności, których cofnięcie lub wstrzymanie nie będzie możliwe, podobnie jak namierzenie odbiorcy.
- Oszuści dobrze przygotowują się do swojej roli, mają odpowiedzi na wiele pytań, jakie może zadać osoba po drugiej stronie.
- Z drugiej strony jeśli zapytamy o niewygodne informacje, np. pozwalające ich szybko odnaleźć w Internecie, lub takie na które nie byli gotowi, często odmawiają, zasłaniając się naglącym czasem, brakiem środków, brakiem wiedzy, z uwagi na fakt, iż są np. nowymi wolontariuszami w organizacji, dbają o środowisko nie mając ulotek itp.
- Posiadają różnorodne certyfikaty, czy nagrody, ale zazwyczaj obcojęzyczne, utrudniające identyfikację, bardzo ogólne, niejasne.
- Oszuści wiedzą, iż należy uśpić racjonalną część naszego mózgu, wprowadzając zamęt, pośpiech, strach, emocjonalność, abyśmy nie myśleli nad tym co robimy, aby to podświadomość kierowana prostymi komunikatami wykonała to o co przestępca prosi.

05 INWESTYCJE

WYKONAJ ĆWICZENIE NR 4

Nasza codzienność często skupia się na pieniądzach, myślimy o tym jak się wzbogacić, skąd wziąć pieniądze na remont, podróże. Jako ludzie też lubimy proste rozwiązania, często niewymagające od nas zbyt wiele wysiłku. Kiedy słyszymy i widzimy nagłówek artykułu, mówiący o „wysokich zyskach, wyjątkowej opcji zwiększenia swoich zarobków, nieprawdopodobnej okazji, o której mało kto wie" nasza podświadomość reaguje zainteresowaniem i chęcią zgłębienia tej niesamowitej okazji na wzbogacenie się.

Oszustwa inwestycje, opierają się na działaniach mających na celu zyskanie naszych pieniędzy, skuszeni wysokimi zyskami, inwestujemy całość swoich oszczędności, a nawet zaciągamy kredyty wierząc, że zwrot z inwestycji, pozwoli je od razu spłacić.

Jak zazwyczaj wyglądają oszustwa inwestycyjne:

1. Często wyglądają bardzo realistycznie, z wieloma technicznymi, finansowymi szczegółami, których nie do końca rozumiemy. Cyberprzestępcy są dobrze przygotowani, maja doświadczenie w tworzeniu fałszywych historii, brzmiących bardzo realistycznie, popierają je fałszywymi dokumentami, danymi.

2. Odwołują się do naszej próżności, trudnej sytuacji, twierdząc że jesteśmy szczęściarzami, że byliśmy na tyle mądrzy, że zdecydowaliśmy się wziąć udział w danej inwestycji, oferty często wydają się zbyt dobre, zyski niezwykle wysokie, mało ograniczeń, duże możliwości, często nie są potrzebne, żadne dodatkowe dokumenty, zgody, w końcu czujemy że szczęście się do nas uśmiechnęło, że znaleźliśmy wyjątkową okazję.

3. Presja czasu, wymuszająca szybkie działania, w końcu inwestycje są dynamiczne, więc nie podejrzewamy przekrętu. Wielokrotnie widzieliśmy propozycje „stworzone tylko dla nas", „zachowaj dyskrecję, im więcej osób wie o tej formie inwestycji, tym mniejsze zyski", „jesteś jedną z niewielu osób, która o tym wie", czujemy się wyjątkowi, zachęcani z każdej strony do dalszych działań, niemalże czujemy już zysk w naszym portfelu.
4. Wykorzystują prawdziwe zdarzenia, nowe technologie, a nawet plotki o sytuacji finansowej, np. rynek krypto walut. Cyberprzestępczość bazuje na znanych historiach, o których wszyscy słyszeli, podając przykłady osób, które wiele zarobiły na krypto walutach lub innych spekulacjach. Internet pełen jest poradników, w których słyszymy, że tylko szybkie, często ryzykowne działania przynoszą zyski, w końcu nikt nie wzbogacił się ciężką pracą. Decydujemy się więc na działania, którym nie do końca ufamy, ale wierzymy że i nam przyniosą fortunę. Cyberprzestępcy wzmacniają w nas poczucie zadowolenia z dokonywanych inwestycji, przekonując nas do dalszych kroków, stosując różne metody, doprowadzają do sytuacji, w której nie możemy się już wycofać, boimy się to zrobić, nie wiemy jak, aż w końcu tracimy całe oszczędności, będąc przekonanym, że musieliśmy popełnić gdzieś błąd.

06 PRACA I ZATRUDNIENIE

Jak ktoś może zarobić na fałszywych ogłoszeniach o pracę? Aby odpowiedzieć na to pytanie, musimy sobie przypomnieć, że nasze dane osobiste mają dużą wartość, a złodzieje mogą na nich dużo zarobić, lub wykorzystać je do innych celów. Po drugie, oszuści multiplikują swoje zyski, poprzez pozyskiwanie nieznacznych kwot, od znacznej ilości osób, prosząc o niewielkie kwoty np. wpisowe, kaucje, zabezpieczania, wykonanie niewielkiego przelewu dla potwierdzenia danych bankowych, który potem zostanie zwrócony. Nie wzbudzają większych kontrowersji, nawet jeśli osoby rekrutujące się spotykają się z taką działalnością pierwszy raz.
Często będąc na emeryturze lub rencie, chcielibyśmy zarobić dodatkowe środki, które ułatwią nam funkcjonowanie. Szukamy wtedy prac nie wymagających od nas zbyt wyczerpujących działań fizycznych, mówimy sobie, że być może uda się znaleźć dodatkowe środki, w prostych pracach w sieci, klikanie reklam, wypełnianie ankiet itp. Pierwotnie szukając czegoś szybkiego, łatwego i średnio płatnego, znajdujemy prace, która wydaje się spełnieniem wszystkich naszych oczekiwań, podobnie jak w powyższych przypadkach, prawie zbyt idealna, by była prawdziwa.

Występuje kilka podstawowych typów oszustw związanych z pracą:

1. **Praca w domu** – oszuści zaoferują prace wykonywaną z domu, nie wymagającą zbyt dużego wysiłku, ale za to dobrze płatnej, zwłaszcza jeśli poznamy tajniki zawarte w instruktażu, który, aby otrzymać, musimy dokonać niewielkiej wpłaty. Ostatecznie nie otrzymamy żadnych materiałów lub nic niewarte ulotki. Nawet jeśli wykonany daną pracę, nie otrzymamy wynagrodzenia albo otrzymamy tylko część z uwagi na niedotrzymanie standardów pracodawcy. Pozwanie ich również nie przyniesie efektów, ponieważ często spółka nie istnieje, lub nie podpisaliśmy żadnej umowy.

2. **Mały wysiłek, wielki zysk** – przed rozpoczęciem niezwykle rentownej pracy, potencjalny pracodawca prosi nas o wysłanie dodatkowych dokumentów, skanu dowodu, zarejestrowania się na darmowej platformie, wyciągając od nas cenne informacje lub instalując na naszym urządzeniu złośliwe oprogramowanie.

3. **Płatność, jako potwierdzenie zaangażowania** – twój pracodawca, zatrudni cię w trybie pracy zdalnej, ale chce, abyś przyjechał do głównego biura w innym mieście, jednocześnie prosi o pokrycie kosztów transportu i zakwaterowania, jako potwierdzenie, że nie wycofamy się z rekrutacji w istniej chwili. Oczywiście zwrot kosztów otrzymamy od razu po podpisaniu umowy, lub z pierwsza wypłatą. Niestety nigdy do tego nie dochodzi.

Dlaczego to działa?

Oszuści doskonale wiedzą jak podszywać się pod prawdziwe firmy, przemawiać do naszej podświadomości, odnosić się do naszych emocji i potrzeb. Jak i o co prosić, abyśmy wykonali daną prośbę bez dłuższej chwili zawahania, ponieważ nie wzbudza ona naszych podejrzeń, z naszej perspektywy jest drobnostką, wobec tego co możemy zyskać. Usypiają naszą czujność, stosując zabiegi manipulacyjne, ostatecznie więc nie czujemy się oszukiwani, lub negujemy nasze odczucia.

ZOBACZ PRZYKŁAD NR 1

07 NIEOCZEKIWANE WYGRANE, SPADKI, NAGRODY, PODATKI, NIEDOPŁATY

„Gratulujemy! Zostałeś zwycięzcą głównej nagrody, wystarczy kliknąć, aby stać się posiadaczem 1 miliona złotych" – brzmi kusząco prawda? Pieniądze nie są jedyną przynętą, stosowana przez oszustów, mogą to być nagrody rzeczowe, telefony, słuchawki, buty, samochód, wycieczki all inclusive. Przestępcy, chcąc zmusić nas do kliknięcia w podejrzany link, użyją wielu metod, aby osiągnąć swój cel. Ponownie niestety, nasz mózg nie zawsze będzie naszym sprzymierzeńcem w takiej chwili. Ludzie mają skłonności, aby wierzyć w nieoczekiwany uśmiech losu, chęć wzbogacenia się małym kosztem.

Często spotykane próby wyłudzeń: spadki, rabaty, podatki, wygrane.

Spadki – skontaktowała się z tobą nieznajoma osoba, twierdząc, że odziedziczyłeś wysoką kwotę, będąc jedynym żyjącym spadkobiercą zmarłej osoby. Prawie bez żadnych zbędnych kwestii dokumentacyjnych, pieniądze są prawie twoje, wystarczy, że dokonasz drobnej płatności, za jakieś zawiłe kwestie urzędowe lub prześlesz skan dokumentu tożsamości, w innym razie odziedziczona fortuna przejdzie na Skarb Państwa. Być może ktoś z nas otrzymał kiedyś taką wiadomość. Siedząc tutaj, możemy powiedzieć, to śmieszne, nie można dać się nabrać na coś takiego. Pamiętajmy jednak, że oszuści potrafią być niezwykle przekonujący, potrafią również wykorzystywać Internet do zrobienia nawet niewielkiego przeglądu danej osoby, aby znaleźć elementy, które można użyć, wybierając odpowiednią metodę oszustwa. Mogą również trafić na osobę, która np. znajduje się w bardzo ciężkiej sytuacji materialnej, potrzebuje pieniędzy, jest zdesperowana. Wiele osób pomyśli pewnie, to w takim razie kwestia statystki, nikt dla kilkudziesięciu złotych nie będzie tracił czasu na przeszukiwanie czyiś profili społecznościowych, albo liczył na łut szczęścia, że trafią na osobę, w trudnej sytuacji. Pamiętajcie jednak, że osoby żyjące z oszustw internetowych, są często wysoce zmotywowane do dokonywania różnych przekrętów, na różna skalę, o różnym charakterze. Nie wszyscy hakerzy czają się wyłącznie na wielkie spółki i banki, wielu z nich specjalizuje się w okradaniu zwyczajnych ludzi, takich jak ja czy wy.

Rabaty i podatki – oszuści mogą podszywać się pod pracowników instytucji państwowych, jak np. urzędy celne lub skarbowe, zgłaszając się do ciebie z informacją o braku płatności, niedopłacie, zatrzymaniu jakieś paczki, konieczności zapłaceniu dodatkowych ceł, inaczej przesyłka zostanie zniszczona. Mogą się podszywać również pod kierownika sklepu, dyrektora marketingu, od których otrzymujemy specjalne rabaty za zakupy w danej sieci.

Zawsze jest jednak pewne „ale" – musimy kliknąć link, zarejestrować się na danej stronie, zadzwonić podać dane, wykonać jeden mały krok, a otrzymamy nagrodę. Oczywiście pod drugiej stronie jest osoba, która chętnie przeprowadzi nas krok po kroku po uciążliwej rejestracji. Oszustwa tego typu są niezwykle skuteczne. Z jednej strony groźba o potencjalnej karze z urzędu skarbowego lub celnego, za brak zapłacenia podatku, opłaty urzędowej, należności celnych, zwłaszcza jeśli w wiadomości dostaniemy ostrzeżenie o możliwych konsekwencjach prawnych lub finansowych, np. obarczenie nasz kosztami postępowania, lub kosztami utylizacji przesyłki, za którą powinniśmy dopłacić. Wobec tego konieczność przelania na podane konto kwoty kilku, kilkunastu złotych nie wydaje się dużym obciążeniem. Kwota jest niewielka, a potencjalnie zyskujemy. W sytuacji dziwnej paczki, jeśli faktycznie nie oczekujemy na żadną zagraniczną paczkę, możemy sądzić, że zaszła jakaś pomyłka i za małą dopłatę kilku złotych, możemy otrzymać coś wartościowego. Z kolei kwestie związane z rabatami, wydają się nieszkodliwe, kto będzie próbował oszukać nas dając nam rabat do Lidla? Zapominamy jednak, że złodzieje mogą np. chcieć wyciągnąć od nas dane, które posłużą im np. do wyłudzenia innych ważniejszych informacji. Mając na oku nagrodę jaką możemy zyskać, zapominamy, o kosztach jakie możemy ponieść.

Niedopłaty za rachunki – wyjątkowo częstym sposobem oszukiwania ludzi są również, najczęściej wiadomości sms o braku płatności za nośniki energii, jak gaz, prąd, lub inne opłaty np. woda, ogrzewanie, zmiany w systemie płatności twojej raty kredytowej, zmianie w wysokości czynszu. Za każdym razem będzie to jednak informacja o niedopłacie, oraz konieczności jej pilnego uregulowania, w przeciwnym razie albo odetną nam dane źródło energii, albo sprawa zostanie skierowana do windykacji, a my umieszczeni na liście wierzycieli. Jak w wielu innych przypadkach, wprowadzenie pospiechu, niepokoju, ewentualnej kary za zwłokę, sprawiają, iż zaczynamy postępować irracjonalnie. Nie sprawdzimy nr telefonu lub adresu mailowego z którego otrzymaliśmy niepokojąca wiadomość. Nie zdziwią nas literówki w załączonym linku, nie zastanowi nas dziwna nazwa faktury, albo fakt, że przecież regularnie opłacamy rachunki, zwłaszcza jeśli kwota niedopłaty jest niewielka, będziemy chcieli jak najszybciej opłacić zaległość unikając nieproporcjonalnie dużej kary w stosunku do „przewinienia".

Wygrane na loteriach – nie pamiętasz kiedy ostatni raz „puściłeś lotka", lub wysłałeś smsa do loterii w radio, ale nagle dostajesz wiadomość, że wygrałeś/aś spora sumę, aby odebrać nagrodę, ponownie musisz wykonać małą, nieistotną rzecz, ale uwaga, czas jest ograniczony, jeśli nie zrobisz tego w przeciągu kilku minut, ktoś może odebrać ci główną wygraną. Przestępcy zadbają, o to abyś nie czuł/a podejrzeń co do autentyczności zwycięstwa, mogą podszywać się pod istniejące loterie, nawet te bardzo popularne. Będą prosić o twoje dane, potencjalnie nieszkodliwe informacje, drobne działania, zalogowanie się, podanie loginu, danych do przelewu, nr karty, kliknięcie linku, przejścia do strony. Na każdym, będą cię prowadzili I zapewniali o autentyczności sytuacji, gratulowali, mówili jakim jesteś szczęściarzem/szczęściarą, będą pytać co zrobisz z takimi pieniędzmi, zastosują wiele technik, abyś tylko nie nabrał/a podejrzeń i wykonała to o co proszą. Ostatecznie jednak znikną wraz z twoimi danymi lub pieniędzmi, a ty nigdy nie otrzymasz nagrody, o której tak gorąco zapewniali oszuści.

ZOBACZ PRZYKŁAD NR 2

08 NIEBEZPIECZNE SMS-y

Według badania Urzędu Komunikacji Elektronicznej w 2022 roku 97% Polaków korzystało z telefonii komórkowej, a 79% z Internetu. Daje to ogromne pole do wymuszeń i oszustw zwłaszcza na użytkownikach telefonów komórkowych, ponieważ prawie każdy Polak powyżej 15 roku życia go posiada. Wpisując w wyszukiwarkę hasło "oszustwa smsowe" otrzymujemy ogrom informacji mówiących o coraz większej liczbie wymuszeń, nowych sposobach na oszukiwanie ludzi, wzrastającej liczbie ukradzionych środków i straconych danych. Skoro złodzieje są coraz bardziej kreatywni, pomaga im w tym również sztuczna inteligencja, to jakie mamy szanse?
Możesz się zdziwić, ale duże. Świadomość, ostrożność i powątpiewanie będą twoją tarczą w Sieci.
Oszuści wykorzystują coraz to nowe sposoby na oszukiwanie ludzi, wciąż jednak używają tych najbardziej sprawdzonych. Spójrz na poniższe wyliczenie, zobacz czy otrzymałeś/łaś:

- SMS z ostrzeżeniem o odłączeniu danego medium z powodu niezapłacenia rachunków;
- SMS z informacją o zatrzymaniu twojej paczki lub listu, w urzędzie celnym, pocztowym, z powodu niedopłaty, przekroczenia dopuszczalnej wagi, braku poprawnych danych adresowych;
- SMS o nieodebranym połączeniu, szczególnie gdy wiesz że takiej próby nie było;
- SMS z wiadomością, o nieudanej próbie logowania do portalu internetowego;
- SMS z popularnych platform społecznościowych, że ktoś próbował włamać się na Twoje konto, lub ktoś oznaczył Cię na zdjęciu, nagraniu, lub że naruszone zostały standardy bezpieczeństwa przez Twoje konto;
- SMS z ostrzeżeniem, że wyciekł Twój numer PESEL;
- SMS z urzędów, instytucji państwowych, wymagający twojej natychmiastowej interwencji;
- SMS z informacją, iż w sieci krążą Twoje nagrania, zdjęcia lub inna forma wykorzystania Twojego wizerunku;
- SMS z wiadomością dot. aktualnych wydarzeń np. wojny na Ukrainie lub pandemii, Narodowego Spisu Powszechnego, zwroty podatków itp. gdzie jesteś wzywany do podjęcia jakieś akcji np. przekazania danych czy środków finansowych.

Wiadomości SMS od oszustów mogą zawierać różną treść, ale zazwyczaj są krótkie, pisane zwięźle, bez dodatkowych tłumaczeń. Najczęściej zawierać będą też kilka kluczowych elementów:

1. Komunikat o zdarzeniu, np.: czegoś nie dopilnowaliśmy, ktoś próbuje nas okraść, coś powinniśmy zrobić, lub powstrzymać np. złodzieja próbującego wykraść nasze dane.
2. Groźba konsekwencji, np. wstrzymana paczka, odcięcie prądu, wykorzystanie naszych danych przez złodzieja;
3. Wezwanie do przeciwdziałania konsekwencjom - najczęściej krótki tryb rozkazujący: „Kliknij poniższy link" lub po prostu sam link sugerujący aby w niego kliknąć.

Cyber złodzieje tak formują treść, żeby wzbudzić w nas strach, niepewność, obawę przed konsekwencjami. Oszuści chcą abyśmy zadziałali szybko, bez namysłu, instynktownie kliknęli link, aby odsunąć od siebie negatywne następstwa. Często SMSy takie nie pozwalają na dokładniejszą identyfikację nadawcy, ich ogólność sprawia, że od razu przypisujemy im pochodzenie od naszego dostawcy mediów, od kuriera od naszej paczki itd.

Materiały źródłowe

https://www.czerwona-skarbonka.pl/gdzie-zglosic-oszustwa-internetowe/
https://www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y
https://www.dobreprogramy.pl/cert-polska-zacheca-do-zglaszania-sms-owych-oszustw-oto-numer-ktory-warto-zapisac,6632502848059904a

Niezależnie od tego czy mamy do czynienia z fałszywym SMS-em lub wiadomością e-mail, działania które powinniśmy podjąć będą podobne:

- Zwróć uwagę na pisownię, gramatykę, interpunkcję, brak polskich znaków, sposób budowania zdań. Czy wydaje Ci się on podejrzany? Pamiętaj, że wielu oszustów nie zna języka polskiego i generują komunikaty w oparciu o internetowe tłumaczenie;
- Dokładnie zastanów się nad treścią wiadomości, czy zamawiałeś/łaś jakąś paczkę ostatnio, czy zdarzyło ci się przegapić termin płacenia rachunków? Nie zakład od razu swojej winy;
- Upewnij się że treść SMS na pewno dotyczy twojej osoby, czy jest na tyle ogólna, że może być adresowana do każdego? Czy SMS zawiera Twój numer konta klienta, numer paczki, inne dane pozwalające Ci stwierdzić, że SMS jest z instytucji, organizacji, firmy z którą współpracujesz?
- Nie daj się zwieść na prawie darmową wygraną, lub otrzymanie paczki wskutek czyjegoś błędu. Wygrane zazwyczaj się nie zdarzają, podobnie jak wzbogacenie się przez czyiś błąd. Pamiętaj, że cyber oszuści działają na dużą skalę, jeśli tysiąc osób zapłaci choćby 1 zł, to złodzieje uzyskają duży zysk.
- Pamiętaj aby nigdy nie klikać linków które przychodzą do ciebie w jakichkolwiek wiadomościach. Jeśli np. oczekujesz takiej wiadomości, to: przeczytaj uważnie co znajduje się w nazwie linku, czy są tam dane/nazwa instytucji; literówki i dziwne nazwy powinny wzbudzić twoją natychmiastową podejrzliwość.
- Pamiętaj, że zawsze możesz zadzwonić na oficjalny numer infolinii danej instytucji, lub skontaktować się z firmą, która rzekomo, wysłała ci SMSa. Nie dzwoń nigdy na numer z którego otrzymałeś wiadomość lub połączenie – nawet jeśli nasz telefon wyświetla nazwę kontaktu.
- Jeśli SMS wyda Ci się podejrzany lub masz pewność, że to próba oszustwa – możesz zgłosić taką wiadomość, a następnie zablokować dany numer.

Jak zgłosić próby wyłudzeń?

- Pierwszym odruchem będzie zgłoszenie sprawy na Policję, pamiętaj jednak aby nie blokować numeru 112. Zadzwoń bezpośrednio lub pójdź na najbliższy komisariat Policji.
- Możesz również zgłosić podejrzany SMS do Zespołu reagowania na incydenty bezpieczeństwa komputerowego CSIRT NASK, a w szczególności do CERT Polska będącego częścią NASK.

- Uruchomili oni specjalny numer telefony 799-448-084 na który możesz przekazać wiadomość w pełnym jej brzmieniu, aby specjaliści określili jej charakter i w razie potrzeby dodali do bazy niebezpiecznych numerów, które następnie są aktualizowane przez operatorów telefonii komórkowych – stąd czasami twój telefon od razu informuje Cię, że dzwoniący lub piszący numer może być próbą Oszustwa lub Spamu.
- Na podany numer CERT POLSKA, można przesłać uzyskaną niepewną wiadomość SMS poprzez funkcję „przekaż dalej". Można wysłać do 3 podejrzanych wiadomości w ciągu 4 godzin. Ważne jest aby wysyłać tam wiadomości wyłącznie noszące znamiona oszustwa, próby wyłudzenia, nie np. wiadomości SPAM od naszego operatora. Należy pamiętać, również iż wyłącznie przekazanie wiadomości w jej pełnym brzmieniu umożliwi jej poprawną weryfikację.

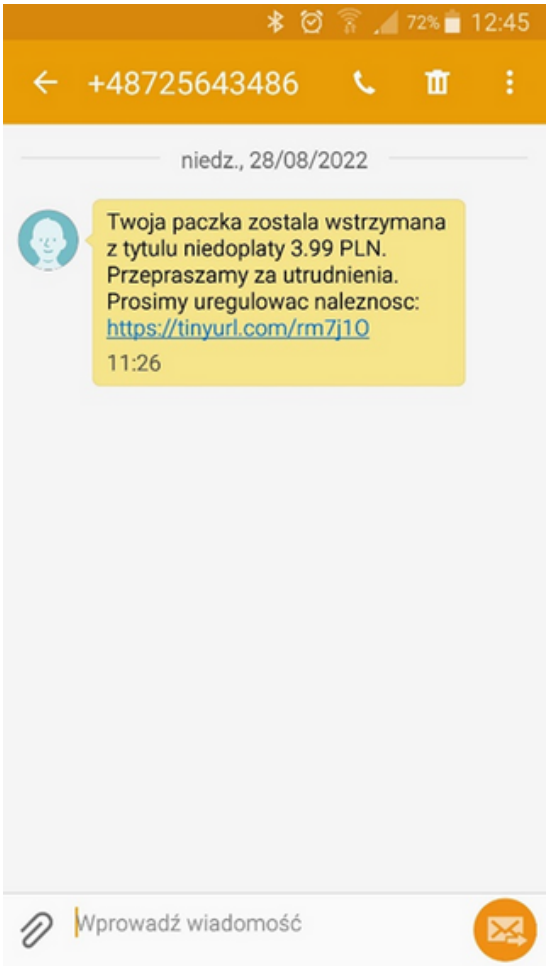
Świadomość, ostrożność i powątpiewanie, pomogą w przeanalizowaniu sytuacji, w której ktoś być może chce wyłudzić od nas nasze dane, lub ukraść nasze pieniądze.

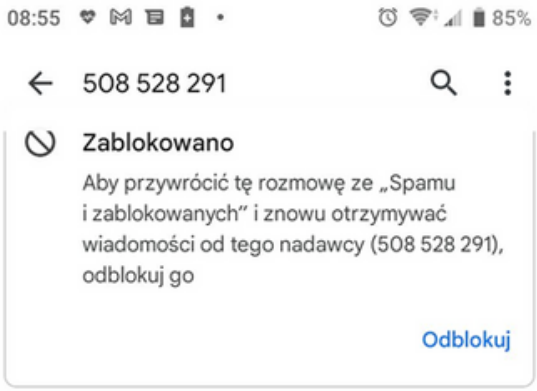
Świadomość – jeśli wiemy, że tego typu oszustwa występują i są niezwykle częste, będziemy czujniejsi, kiedy taką wiadomość otrzymamy.

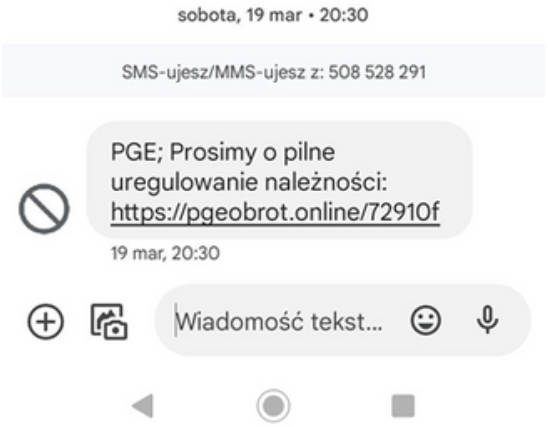
Ostrożni – nie będziemy od razu, bez wahania klikać w dołączony link.

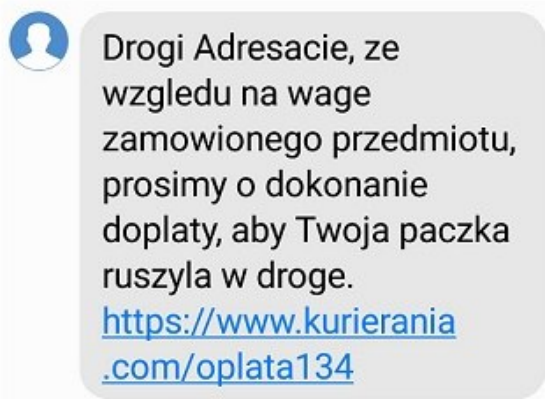
Powątpiewanie – zastanowimy się czy na pewno to co jest zawarte w tym SMS-ie dotyczy nas. Zadzwonimy na oficjalną infolinię, spytamy o sytuację, upewnimy się, czy na pewno nie zapłaciliśmy rachunków, czy faktycznie została do nas nadana paczka.

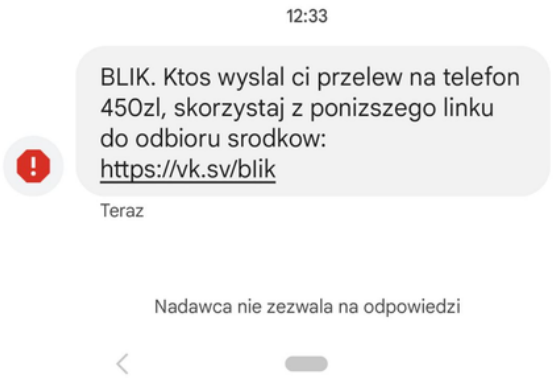
Pamiętaj, nigdy żadna instytucja nie daje swoim klientom 5 minut na odpowiedź, zgodnie z prawem zawsze powinniśmy być informowani z odpowiednim wyprzedzeniem, pozwalającym nam na zastosowanie odpowiednich, niepochopnych działań.











Materiały źródłowe

https://www.rmf24.pl/regiony/szczecin/news-policja-sms-y-o-doplacie-do-przesylki-to-oszustwo,nId,6090265#crp_state=1
https://wyborcza.biz/biznes/7,177150,28061422,podszywaja-sie-pod-blik-a-uwazaj-bo-wyczyszcza-twoje-konto.html?disableRedirects=true

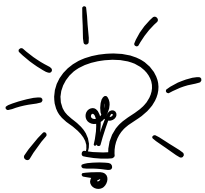
Moduł 3 JAK SIĘ BRONIĆ PRZED CYBER ZAGROŻENIAMI

Informacja dla wykładowcy:
Czas: 3h
Wykładowco:
1. Rozdaj kartę z przykładami i ćwiczeniami.
2. Daj uczestnikom wydrukowane listy kontrolne;
3. Przedstaw poniższy materiał;
4. Nawiązuj do przykładów i ćwiczeń, wtedy gdy w tekście poniżej zobaczysz informację, aby zobaczyć lub wykonać ćwiczenia/przykład. Ćwiczenia omawiaj wspólnie z uczestnikami;
5. Pilnuj czasu – masz do dyspozycji 3 godziny w systemie 45minut nauki, 15 minut przerwy.

Cyber-przestępstwa są niezwykle istotnym zagrożeniem. Każdy powinien wiedzieć jak je rozpoznać. Ich znajomość to pierwszy krok w stronę zabezpieczenia siebie i swoich danych w sieci. W tym rozdziale przygotowaliśmy 8 wskazówek w formie listy kontrolnej, która wesprze Cię w utrudnieniu pracy cyberprzestępcom.
Jest wiele rzeczy które możemy zrobić, aby ochronić siebie i swoje dane. Nie musisz się bać korzystać z Internetu, większość zagrożeń, po tym kursie zauważysz bez trudu. Pamiętaj, że nawet młodzi ludzie „urodzeni z telefonem w ręku" stają się ofiarami cyber-przestępstw. Przestępcy stale szukają sposobów na oszukanie ludzi i często są o krok przed nami. Nie znaczy to jednak że mamy ulegać strachowi i rezygnować ze zdobyczy technologicznych.

Check list - Lista kontrolna

01 UŻYWAJ ANTYWIRUSA LUB INNEGO PROGRAMU ZAPEWNIAJĄCEGO BEZPIECZEŃSTWO



Programy zapewniające ochronę w czasie rzeczywistym przed istniejącymi oraz pojawiającymi się złośliwymi oprogramowaniami, w tym oprogramowaniami szantażującymi i wirusami, oraz
programy pomagające w zabezpieczaniu prywatnych i finansowych informacji, gdy korzystamy z Internetu.

Odpowiedni program antywirusowy jest pierwszym i niezbędnym krokiem aby ochronić się w sieci, jednocześnie najłatwiejszym. Antywirus może być postrzegany jako pierwsza linia obrony, twoja tarcza przeciwko wirusom i złośliwym oprogramowaniem

Wiele darmowych programów posiada przyjaznych dla domowego budżetu opcji, zainstalowanie takiego programu jest lepszym rozwiązaniem niż nieposiadanie go w ogóle.

Bez znaczenia czy wolisz korzystać z komputera czy telefonu, możesz i powinieneś/powinnaś zabezpieczyć każde z nich. Obecnie programy antywirusowe oferują ochronę wielu urządzeń w jednej licencji.

Posiadanie takiego programu to dobry początek w blokowaniu wirusów i fałszywych stron internetowych. Obecnie jednak programy antywirusowe dają nam znacznie więcej możliwości, które powinniśmy wykorzystać aby skutecznie się chronić. Większość z nich posiada automatyczne narzędzia, które raz zainstalowane, chronią nasze urządzenie, pliki, hasła, informacje i dane, a nawet naszą tożsamość.

Pamiętaj, darmowe programy nie chronią w pełni przed różnorodnymi zagrożeniami. Aktualizacje dla darmowych oprogramowani są zwykle dodawane później niż dla płatnych opcji. Możesz dzielić się kosztami z rodziną, znajomymi, ponieważ wiele programów oferuje wiele licencji na różne urządzenia przy jednym zakupie

Nie instaluj więcej niż jednego programu antywirusowego na jednym urządzeniu – programy te mogą wzajemnie rozpoznawać się jako zagrożenie, i wzajemnie zwalczać, powodując spowolnienie twojego urządzenia.

Oto kilka podstawowych funkcji, na które każdy powinien zwrócić uwagę, wybierając dobry program antywirusowy

Skuteczność wykrywania złośliwego oprogramowania na poziomie minimum 95%

Ochrona konta mailowego – dobry antywirus będzie skanował i blokował – jeśli będzie to potrzebne – szkodliwe załączniki przed ich otwarciem

Łatwy w użytkowaniu oraz intuicyjny panel użytkowania – możesz to sprawdzić np. na darmowych wersjach antywirusa, którego chcesz kupić

Ochrona większej liczby urządzeń

02 UŻYWAJ DOBREGO, MOCNEGO HASŁA

Silne hasło to kolejny ważny krok, aby zabezpieczyć się przed cyber-przestępstwami, istnieje kilka ogólnych zasad, które powinieneś/powinnaś zastosować

Upewnij się że twoje hasło jest inne dla każdego z kont

Zapamiętywanie haseł przez przeglądarkę, z pewnością uczyni twoje życie łatwiejszym, jednocześnie jest jednak łatwym łupem dla cyber-złodziei

Hasło powinno być wystarczająco silne i regularnie zmieniane

Jeśli ciężko Ci zapamiętać hasła, zawsze możesz:

Używaj kombinacji minimum 8 liter, numerów, symboli

- użyć aplikacji do zarządzania hasłami;
- stworzyć plik z hasłami (np. Word lub Excel), ale nie przechowuj wszystkich haseł w jednym pliku na swoim komputerze lub telefonie;
- zapisywać swoje hasła w notesie, zeszycie. Unikaj zapisywania PINów do telefonu na kartkach, które trzymasz w portfelu lub zapisania hasła do bankowości elektronicznej w pliku na pulpicie
- stworzyć swój własny system tworzenia haseł, który będzie łatwy w zapamiętaniu i odtworzeniu haseł .

Hasło powinno być wystarczająco silne i regularnie zmieniane

Nigdy nie wysyłaj hasła w wiadomości e-mail

Nie wpisuj hasła, gdy ktoś patrzy Ci przez ramię

Nie wpisuj hasła na komputerze, który nie należy do Ciebie

ZOBACZ ĆWICZENIE NR 1

03 REGULARNIE AKTUALIZUJ OPROGRAMOWANIE

Cyberprzestępcy wykorzystują znane wady w oprogramowaniach, aby uzyskać łatwiejszy dostęp do twojego telefonu lub komputera. Jeśli twoje programy/aplikacje/gry, są regularnie aktualizowane, będziesz mieć najnowsze łatki bezpieczeństwa, a twoje dane będą skuteczniej chronione. Wiedz też, że cyberzagrożenia ciągle się zmieniają, oferowane w danej chwili aktualizacje, mają zabezpieczyć cię przed tymi, które w danej chwili się pojawiają, i chronić twoje urządzenia przed ich szkodliwym wpływem.

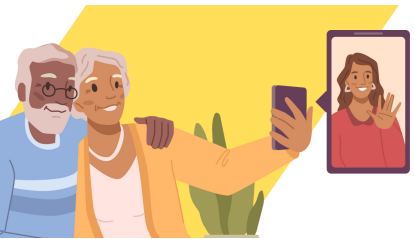
- Staraj się nie odkładać czy ignorować aktualizacji, kiedy system wysyła ci informację o pojawieniu się najnowszej aktualizacji
- Jeśli nie jesteś pewien/pewna czy aktualizacja pochodzi z bezpiecznego źródła, możesz sprawdzić stronę internetową twórcy aplikacji/programu/gry aby to zweryfikować
- Używaj aktualnych przeglądarek internetowych

WYKONAJ ĆWICZENIE 2 **POKAŻ PRZYKŁAD 1** **POKAŻ PRZYKŁAD 2**

04 ZARZĄDZAJ USTAWIENIAMI SWOICH MEDIÓW SPOŁECZNOŚCIOWYCH

Ważne, aby zapamiętać, że jeśli coś publikujemy w Internacie, zostanie tam na zawsze. Nie usuniemy tych treści całkowicie, zawsze zostanie po nich ślad. Cyberprzestępcy potrafią zdobyć twoje dane, wykorzystują wyłącznie kilka trafnych informacji. Będą starali się poznać ciebie, czasami nawet zdobyć twoje zaufanie i następnie cię oszukać, poprzez załączniki czy linki. Pamiętaj, im mniej informacji trafia do Internatu, tym lepiej.

- Pamiętaj, aby nie wrzucać do sieci swojego adresu, imienia pupila, nazwiska panieńskiego swojej matki, ponieważ często są to odpowiedzi na pytania zabezpieczające twoje konta w sieci.
- Powyższe informacje, są też często częścią naszych haseł, dlatego tak ważne jest, aby przykładać więcej uwagi do naszych haseł i jednocześnie do tego co publikujemy w sieci.
- Na pierwszy rzut oka, nieszkodliwe publikowanie zdjęć z wakacji, z dala od domu, mogą dać złodziejom cenne informacje, iż nasz dom pozostał bez opieki – media społecznościowe są istotnym narzędziem, nie tylko dla cyberprzestępców, ale także tych funkcjonując w „prawdziwym" życiu.
- Należy pamiętać, aby odpowiednio zarządzić ustawieniami prywatności dla wszystkich mediów społecznościowych, z których korzystamy, tak, aby tylko nasi znajomi, widzieli co publikujemy
- Cyber-przestępcy często tworzą nieprawdziwe konta. Jeśli otrzymasz powiadomienie o interakcji z kontem, którego właściciela nie znasz, niezależnie czy jest to wiadomość, czy zaproszenie do znajomych, zachowaj ostrożność i sprawdź kluczowe informacje o tej osobie jak zdjęcie profilowe, liczba znajomych, wspólni znajomi. Jeśli czujesz, że może to być próba wymuszenia, nie odpowiadaj na wiadomości/zaczepki ani nie dodawaj takiej osoby do znajomych



05 ZABEZPIECZAJ SWOJE KONTO MAILOWE

Kiedy mówimy o przestępczości cybernetycznej, często to właśnie maile pojawiają się jako pierwszy punkt. Niechciane reklamy, podejrzane maile i niebezpieczne załączniki – możesz dostać każdy z nich jednego dnia. Istnieje jednak kilka ogólnych zasad, których przestrzeganie pomoże Ci zapewnić bezpieczeństwo:

Nigdy nie otwieraj załączników od kogoś kogo nie znasz. Jeśli jednak zdecydujesz się je otworzyć, najpierw ostrożnie sprawdź adres mailowy, z którego otrzymałeś plik, błędy ortograficzne i literówki, pokażą ci, iż ktokolwiek wysłał tego maila, nie ma przyjaznych zamiarów:

kontakt@oraneg.pl;
info_faktury@tuaron.pl;
...@ocjk.pl;
....@rlcysystem.com

Jeśli przypadkowo otworzyłeś/otworzyłaś załączony plik/link, który prawdopodobnie jest oszustwem, wciąż możesz coś z tym zrobić. Nie panikuj. Najpierw przeskanuj swoje uprzedzenie za pomocą programu antywirusowego. Zmień hasło do swojego konta e-mail, możesz również zadzwonić do swojego banku oraz poinformować ich że stałeś/stałaś się ofiarą przestępstwa internetowego, po to, aby śledzili jakiekolwiek podejrzane ruchy na twoim koncie i je blokowali.

Najpopularniejsi operatorzy kont mailowych, poinformują się że dany załącznik jest podejrzany, jeśli widzisz taką informację, nie otwieraj tego maila i jego załączników. Jeśli nie jesteś pewien/pewna czy załącznik jest bezpieczny, sprawdź go, poprzez wykonanie telefonu lub napisanie wiadomości do nadawcy wiadomości, sprawdź dokładnie domenę z której mail został wysłany. Jeśli zdecydujesz się otworzyć załącznik/link, pamiętaj że formaty pdf są uważane za bezpieczniejsze. Nie otwieraj załączników z dziwnymi, niezrozumiałymi nazwami.

Otwieranie załączników z linka, również może być oszustwem. Pamiętaj, że zawsze jest lepiej podwójnie zweryfikować nadawcę lub treść maila, zamiast automatycznie klikać w podejrzany link.

POKAŻ PRZYKŁAD NR 3 POKAŻ PRZYKŁAD 4 WYKONAJ ĆWICZENIE NR 3

06 UNIKAJ PODEJRZANYCH PRÓŚB, INFORMACJI

Jakakolwiek prośba, informacja pośpieszająca cię, zawierająca groźbę, próbę zastraszenia albo inne kontrowersyjne treści, jak wygrana w loterii, prośbę o pomoc w znalezieniu przestępy powinny być bardzo ostrożnie sprawdzone, opierają się na inżynierii społecznej. Cyberprzestępcy chcą abyś myślał/myślała, że musisz działać, w przeciwnym razie stracisz pieniądze albo prywatne dane, lub komuś stanie się krzywda.

Jeśli ktoś prosi cię o podanie jakichkolwiek informacji, zastraszając cię, używając gróźb w stosunku do ciebie lub twojej rodziny, twoich kont itp. nie odpowiadaj, rozłącz się, zablokuj nadawcę. Jeśli nadawcą „prośby" był ktoś przedstawiający się jako osoba reprezentująca państwową instytucję czy firmę, zadzwoń lub napisz maila na telefon, adres mailowy podany na oficjalnej stronie tej instytucji/firmy. Zawsze możesz się rozłączyć i zadzwonić ponownie na oficjalny numer, lub napisać maila do obsługi klienta – lepiej zachować ostrożność, niż podać komuś nieodpowiedniemu ważne informacje.

Pamiętaj, zawsze lepiej jest, sprawdzić dwa razy, zanim przekażesz komuś swoje dane osobiste, nawet jeśli okaże się, że faktycznie musisz dokonać zmian w swoim koncie, dopłacić do danej faktury. Wciąż jednak pracownicy każdej instytucji państwowej czy prywatnej, muszą zapewnić obsługę na powszechnie przyjętym poziomie, co oznacza że nie mogą cię zastraszać, pośpieszać – twierdząc, że musisz to zrobić teraz, albo pojawią się poważne konsekwencje.

Pamiętaj, aby zawsze weryfikować informacje które udostępniasz. W czasie pandemii pojawił się ogrom fałszywych informacji, które potem często były wykorzystywane przez przestępców, wysyłających fałszywe linki, których zadaniem było zainstalowanie złośliwego oprogramowania na twoim telefonie/komórce

Ponowne wybieranie numeru, oddzwanianie na numer z którego kierowane były groźby w naszą stronę, może okazać się bezskuteczne, ponieważ cyber-przestępcy skutecznie udają przedstawicieli instytucji i firm, tak abyśmy myśleli że rozmawiamy z ich przedstawicielami. Lepiej jest rozłączyć się, oraz zadzwonić na numer podany na oficjalnej stronie internetowej danej firmy/instytucji.

POKAŻ PRZYKŁAD NR 5

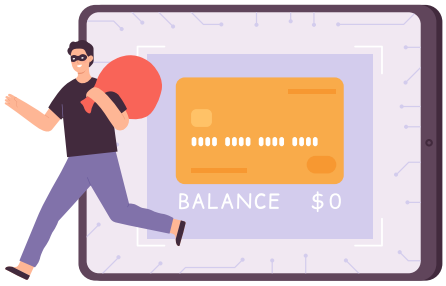
WYKONAJ ĆWICZENIE NR 4

07 ZABEZPIECZAJ SWOJE TRANSAKCJE ONLINE

Powinieneś/powinnaś zachować ostrożność podczas wykonywania transakcji online, nieważne czy są to zakupy online czy przesyłanie dokumentów drogą elektroniczną.

- Każda strona powinna posiadać certyfikat SSL, który gwarantuje bezpieczeństwo komunikacji online. Kiedy przeglądarka kontaktuje się z zabezpieczoną stroną, certyfikat SSL umożliwia połączenie szyfrowane. Jego symbolem jest kłódka w pasku adresu w przeglądarce przed „www". Zdąża się że nawet fałszywe strony posiadają symbol kłódki, jednakże te tworzone w pośpiechu mogą ich nie mieć.
- Zawsze sprawdzaj nazwę strony, której używasz, zwracaj uwagę na literówki i inne błędy gramatyczne,
- Zawsze sprawdzaj czy strona „wygląda jak zazwyczaj". Nowe przyciski, inna szata graficzna, linki mogą świadczyć o tym, że strona jest fałszywa,
- Rozważ weryfikację dwu-etapową – jak otrzymanie dodatkowego hasła/PIN-u mailem, SMS-em,
- Jeśli masz taką możliwość – rozważ użycie programów ochraniających transakcje online, wiele programów antywirusowych oferuje taką możliwość swoim użytkownikom.
- Jeśli jest to możliwe, pobieraj dokumenty potwierdzające twoją aktywność, jak faktury,
- potwierdzenia dokonania transakcji.
- Co ważne, nawet jeśli powzięte kroki, zakończą się niepowodzeniem, a Ty staniesz się ofiarą przestępstwa, uruchamiając procedurę cashback, zgłaszając roszczenia do banku czy nawet zgłaszając przestępstwo, pracownicy banku lub policjanci zapytają Cię o sposób w jaki zabezpieczyłeś/zabezpieczyłaś się online, jakie oprogramowanie antywirusowe posiadasz, o historię aktualizacji oprogramowania, sprawdzenie bezpieczeństwa stron internetowych itp.

POKAŻ PRZYKŁAD 6



08 NIE BÓJ SIĘ PROSIĆ O POMOC

Ofiary cyberprzestępstw to osoby w różnym wieku z różnych grup społecznych.

1. Jeśli nie czujesz się komfortowo pytając członków rodziny, przyjaciół albo obsługi klienta o coś co cię niepokoi, pamiętaj że nawet ci którzy wychowali się w epoce Internetu, mając swobodny dostęp do Internetu, również padają ofiarami cyber-przestępców.
2. Jeśli wydaje ci się że padłeś/padłaś ofiarą przestępstwa cybernetycznego, nie wahaj się aby poinformować o tym członków twojej rodziny, policję i odpowiednie instytucji (na przykład jeśli zostałeś/zostałaś oszukana przez kogoś kto podawał się za pracownika banku – poinformuj obsługę tego banku).
3. Jeśli kliknąłeś/kliknęłaś podejrzany link albo pobrałeś/pobrałaś szkodliwy załącznik – zatrzymaj się w tej chwili i ponownie poinformuj kogoś ze swojej rodziny, znajomych, policję czy pracownika banku.
4. Ludzie którzy stali się ofiarami cyberprzestępstw często winią samych siebie, że nie zauważyli zagrożenia, nie poprosili o pomoc, że zaufali obcej osobie. Znacznie gorzej jest jednak ukrywać te uczucia i nie pomóc innym w uniknięciu stania się ofiarą. Otrzymanie wsparcia emocjonalnego w takiej chwili jest kluczowe, zwłaszcza kiedy ofiara czuje się winna całej sytuacji.

WYKONAJ ĆWICZENIE NR 5

Ochrona danych osobowych i konsumenta

Informacja dla wykładowcy:
Czas: 60 minut
Wykładowco:
1. Przedstaw poniższy materiał;
3. Pilnuj czasu – masz do dyspozycji 45minut wykładu i 15 minut przerwy.

W Polskim prawie istnieją mechanizmy ochrony konsumentów, które mogą pomóc w walce z nieuczciwymi sprzedawcami i cyber przestępczością. Pamiętaj aby kupując cokolwiek w Internecie sprawdzić dokładnie sklep, opinie o nim, ustalić czy sklep zabezpiecza Twoje dane (zielona kłódka). Korzystaj ze sprawdzonych sklepów, podejrzanie niskie ceny lub „wyjątkowe" oferty tylko dla wybranych mogą być próbą wyłudzenia od Ciebie pieniędzy lub danych. Warto też korzystać z ochrony kupujących, które oferują niektóre e-sklepy, polega ona na tym, że sprzedawca nie otrzyma pieniędzy, dopóki nie potwierdzisz, że kupiony towar dotarł do Ciebie i jest zgodny z umową.
Warto korzystać także z praw, które jako konsumenci mamy, a które mogą pomóc nam w odzyskaniu utraconych pieniędzy lub ochronie danych osobowych.

1. ODSTĄPIENIE OD UMOWY

Zakup towaru/usługi jest pewnego rodzaju umową pomiędzy kupującym, a sprzedającym. Obie strony umawiają się, że jedna za pieniądze dostarczy dany towar lub usługę. Dlatego jeśli kupujemy coś poza lokalem przedsiębiorstwa – czyli np. w Internecie, na stronie internetowej, na Allegro, czy podczas prezentacji, targów czy przez telefon, możemy taki zakup cofnąć - odstąpić od umowy. Na takie „wycofanie się" mamy 14 dni, i co ważne, nie musimy podawać przyczyny i nie powinniśmy ponosić kosztów z wyjątkiem kosztu zwrotu towaru czyli np. kuriera lub poczty.
Odstąpienia należy dokonać na piśmie.
Pamiętaj – towar nie może być używany. Sklep nie powinien uzależniać zwrotu od posiadania oryginalnego pudełka - którego zadaniem jest wyłącznie ochrona towaru. Jednak, jeśli możesz wyślij towar do sprzedawcy w pudełku/opakowaniu w którym go otrzymałeś. Pewnych towarów nie można zwrócić np. tych wyprodukowanych na nasze specjalne życzenie, towarów higienicznych, leczniczych, niektórych usług: np. przewozu.

SPRAWDŹ PRZYKLAD NR 1

2.ŚWIADCZENIA NIE ZAMÓWIONE

Niektórzy nieuczciwi sprzedawcy lub przestępcy wysyłają nam niezamówione towary lub wykonują jakąś usługę o którą nie prosiliśmy. Gdy odbierzemy taką przesyłkę, oszuści argumentują, że zgodziliśmy się za nią zapłacić. Straszą komornikiem lub sądem, wysyłają wezwania do zapłaty. Często myślimy, że odbiór paczki jest jednoznaczny ze zgodą na przyjęcie towaru- nic bardziej mylnego. Jeśli otrzymaliśmy towar, lub została nam wykonana usługa o którą nie prosiliśmy, nie zamówiliśmy, to osoba ją wykonująca lub wysyłająca towar robi to na własne ryzyko. Nie może żądać zapłaty. A fakt odebrania przesyłki przez nas nie jest jednoznaczny z akceptacją jakichkolwiek kosztów. Jeśli jesteśmy nękani telefonami lub wezwaniami do zapłaty warto zgłosić sprawę na policję.

3. BŁĘDNY PRZELEW

Czasami dopiero po fakcie wykonania przelewu, spostrzegamy, że prawdopodobnie zostaliśmy oszukani. Wtedy, często myślimy, że nasze pieniądze przepadły, istnieją jednak sposób by utrzeć oszustom nosa. Jak najszybciej skontaktuj się z bankiem. Odpowiedz o swoich podejrzeniach i poproś o anulowanie przelewu. Niektóre przelewy można łatwo i szybko anulować, inne wiążą się z procedurą reklamacyjną, jednak najważniejsze, że dzięki temu możesz odzyskać swoje środki. Bardzo ważne jest by dokonać zgłoszenia przed „sesją ELIKSIR". Sesja ELIKSIR to moment, kiedy Twój bank księguje twój przelew. Jeśli jednak spostrzegłeś to później, nie poddawaj się. Pamiętaj też, że możesz skorzystać z porady prawnej. Banki mają więcej możliwości odzyskania środków z konta oszusta niż nam się wydaje. Najszybciej odzyskasz pieniądze jeśli zapłaciłeś kartą – wtedy powołując się na procedurę chargeback możesz sprawnie i bez większych problemów wycofać środki.

Pamiętaj by mieć jak najwięcej danych nt. potencjalnego oszusta – numer konta, godzina przelania środków, tytuł przelewu, nazwę właściciela konta.

SPRAWDŹ PRZYKLAD NR 2

4. OCHRONA DANYCH OSOBOWYCH - RODO

Dzięki RODO możemy skuteczniej chronić nasze dane osobowe. Czym właściwie jest RODO? Jest unijnym prawem regulującym zasady ochrony danych osobowych, które stosujemy od 25 maja 2018 r. Pełna nazwa RODO: Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

Według RODO – Administrator, czyli osoba, która posiada Twoje dane musi mieć konkretny cel ich pozyskania i przetwarzania. Według art. 15 RODO masz też określone prawa, m.in.: dostępu do danych, żądania ich usunięcia, czy jedno z bardziej przydatnych - dowiedzenia się skąd dana firma ma Twoje dane.

Jak w praktyce wykorzystać RODO?

- Jeśli jesteś nękany mailami, esemesami czy telefonami z ofertami, namawianiem do zakupu powołaj się na art. 15 RODO (prawo do usunięcia danych). Zażądaj usunięcia Twoich danych z bazy firmy, którą reprezentuje osoba dzwoniąca. Jeśli to nie podziała zgłoś sprawę do PUODO (Prezesa Urzędu Ochrony Danych), gdyż za nie respektowanie Twoich praw grozi kara administracyjna, a nawet w niektórych przypadkach sprawa karna.
- Możesz też uzyskać informacje o tym skąd dany podmiot ma Twoje dane. Dzięki temu możesz dowiedzieć się, czy jakaś inna firma nie pozyskała Twoich danych nielegalnie, nie zostałeś oszukany lub nie podrobiono Twojej zgody. Zażądaj od firmy, która się z Tobą kontaktuje informacji dlaczego to robią i skąd mają Twoje dane. Pamiętaj, że ogólnikowe odpowiedzi, lub zbywanie Cię, można zgłosić do PUODO.
- Możesz także wykorzystać RODO, by dowiedzieć się jakie dane ma konkretna firma np. telekomunikacyjna. Okazuje się, że przed RODO firmy zbierały bardzo dużo danych na nasz temat. Możesz od danego przedsiębiorstwa zażądać informacji jakie dane posiadają, kiedy je zebrali i do czego wykorzystują, jeśli uznasz że ilość posiadanych danych jest za duża, możesz zażądać ich usunięcia.

Nie bój się, że nie zrozumiesz odpowiedzi danej firmy lub użyją oni „prawniczego języka", RODO wprost nakazało stosowanie przyjaznych, łatwych w odbiorze komunikatów. Dodatkowo, co wynika z RODO nie musisz swojej prośby podpierać konkretnymi paragrafami – Administrator ma obowiązek odpowiedzieć na Twoje najprostsze pytanie „Jakie moje dane Państwo mają?". Jeśli przedsiębiorstwo unika odpowiedzi, zbywa Cię, nie chce podać informacji argumentując brakiem wysłania przez Ciebie specjalnego pisma, zgłoś sprawę do PUODO.

5. ZASTRZEGANIE DOWODU

Oszuści nie tylko kradną pieniądze, ale także dane osobowe. Jeśli obawiasz się, że ktoś mógł pozyskać informacje o Tobie z dowodu osobistego lub jeśli stałeś się ofiarą przestępstwa polegającego na wyłudzeniu tych danych – powinieneś zastrzec dowód osobisty w urzędzie gminy/miasta lub przez Internet. Po otrzymaniu twojego zgłoszenia urzędnik unieważni Twój dowód. Jeśli twój dowód osobisty został ukradziony - wystarczy, że zgłosisz to na Policji. Nie musisz wtedy zgłaszać utraty dokumentu w urzędzie. Dowód zostanie unieważniony z dniem zgłoszenia tego faktu Policji.

CZY ZGŁASZAĆ OSZUSTWO NA MAŁĄ KWOTĘ?

Często zastanawiamy się, czy zgłaszać oszustwo na małą kwotę. Spodziewamy się, że Policja nie przyjmie zgłoszenia albo, że będzie nam trudno to udowodnić. Niekiedy sprzedawca znika, zamyka konto, a my mamy jednie fałszywe dane i numer telefonu, który nie odbiera. Ważne, jest by zrozumieć, że oszustwo internetowe niczym nie różni się od zwykłego - oszust, by odnieść korzyść majątkową, wprowadzi Cię w błąd, wykorzysta Twoja pomyłkę, lub wykorzysta sytuację, że pokrzywdzony z różnych przyczyn nie jest w stanie właściwie zrozumieć swojego działania. Takie oszustwo podlega karze pozbawienia wolności od 6 miesięcy do 8 lat, a w sprawach mniejszej wagi karze grzywny, ograniczenia wolności lub więzienia do lat 2.
Wyłudzenie jest przestępstwem, a nie wykroczeniem, niezależnie od kwoty. Czyli nawet jeśli oszukano Cię na 1 zł, to jest to karalne (kwota 500 zł ma zastosowanie przy kwalifikacji kradzieży jako wykroczenia/przestępstwa). Ustalenie sprawcy oszustwa internetowego na kilkanaście złotych będzie pewnie trudne, ale być może nie jesteś jedyną oszukaną osobą, a policja może już prowadzić śledztwo, a prokuratura szuka poszkodowanych. Możemy na własną rękę w Internecie spróbować znaleźć inne osoby poszkodowane przez dany e-sklep czy oszusta. Nasze działania – zgłaszanie czy też informowanie innych ma też funkcję prewencyjną.

Polskie prawo daje nam środki do ochrony naszych danych i pieniędzy w Internecie. Znalezienie oszustów jest trudniejsze, ale nie niemożliwe. Im szybciej zadziałamy, podejmiemy akcje, zgłosimy sprawę tym lepiej dla nas. Nie bójmy się bycia ocenianym, wyśmianymi. Osoby z każdej grupy wiekowej mogą stać się ofiarą cyber-przestępców, ważne by poprosić o pomoc i korzystać ze swoich praw.

Materiały źródłowe

https://www.czerwona-skarbonka.pl/gdzie-zglosic-oszustwa-internetowe/

Jak sprawić, aby nasze otoczenie było bezpieczniejsze?

Informacja dla wykładowcy:
Czas: 2h
Wykładowco:
1. Rozdaj karty z przykładem.
2. Przedstaw poniższy materiał;
3. Nawiązuj do przykładów, filmików, wtedy gdy w tekście poniżej zobaczysz informację, aby zobaczyć przykład oraz link do filmiku na YouTube. Przykład omów wspólnie z uczestnikami;
4. Pilnuj czasu – masz do dyspozycji 2 godziny w systemie 45minut nauki, 15 minut przerwy.

Wiemy już czym jest RODO, jak unijne prawo chroni naszą prywatność i dane, poznaliśmy również, mechanizmy rządzące psychologicznymi aspektami stawania się ofiarą. Dowiedzieliśmy się z tego kursu, jak cyberprzestępcy próbują nasz oszukać i ukraść nasza dane i pieniądze oraz jak temu przeciwdziałać. Ten rozdział powie nam jak dbać o nasze otoczenie, aby stawało się coraz bezpieczniejsze, nie tylko dla nas samych, ale również dla naszej rodziny i naszych znajomych. Mahatma Gandhi powiedział kiedyś "bądź zmianą, którą pragniesz ujrzeć w świecie". Jeśli chcemy, aby świat, nasze otoczenie nasi bliscy byli bezpiecznie, również w cybernetycznym świecie, każdy z nas musi dołożyć swoją cegiełkę. Możemy to zrobić poprzez wsparcie kogoś kto stał się ofiarą przestępstwa, powiedzenie komuś o tym kursie, polecenie mu/jej podręcznika, wskazanie miejsca w którym należy szukać pomocy, zgłoszenie szkodliwego/kłamliwego postu, linka, strony internetowej, która oszukuje ludzi, zgłoszenie na Policji próby wyłudzenia.
W tym rozdziale dowiesz się więcej o:

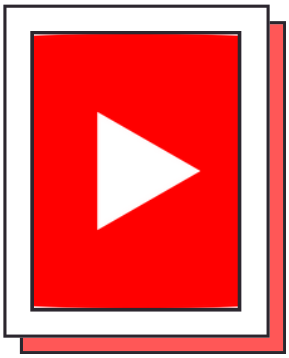
1. Mediach i platformach społecznościowych;
2. Jak pozostać bezpiecznym w mediach społecznościowych;
3. Zalety i wady mediów społecznościowych;
4. Jak zgłosić szkodliwe treści
5. Wskazówki dla użytkowników mediów społecznościowych

01 Media i platformy społecznościowe

- Sieci społecznościowe pozwalają na kontakt z naszymi bliskimi i znajomymi dzięki wielu platformom internetowym;
- Cyberprzestrzeń dalej nam wiele możliwości, które nie ograniczają się do wyłącznie osób młodych.
- Wiele platform społecznościowych opiera się na współdzieleniu pasji, zainteresowań, dzieleniem się opinii, doświadczeń, lub po prostu bycia na bieżąco z tym co dzieje się z osobami które znamy.
- Istnieją setki portali społecznościowych, w tym rozdziale poruszymy niektóre z nich, najbardziej popularne w Polsce: Facebook, YouTube, MS Teams, Skype, Instagram, WhatsApp, Pinterest, LinkedIn.

Facebook

- Nawiązywanie znajomości;
- Dzielenie się zdjęciami, opiniami, ocenami, wskazówkami;
- Tworzenie fan page, wydarzeń, grup zainteresowań;
- Znalezienie firm, artystów, polityków itd.

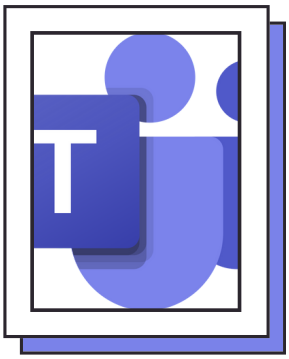


YouTube

- Dzielenie się filmami, muzyką krótkimi clipami
- Komentowanie i ocenianie treści innych użytkowników
- Bardzo szeroki zakres tematyczny od rozrywki, muzyki, gry, po treści edukacyjne, jak filmy instruktażowe, motywacyjne itp.

Skype

- Platforma umożliwiająca rozmowy głosowe i video z inna osobą, lub grupą osób, gdziekolwiek się znajdują;
- Możemy jej używać również w telefonie
- Możemy z niej dzwonić również na numer telefonu, a nie tylko skype-skype



MS Teams

- Pozwala na rozmowy głosowe i video
- Tworzenie spotkań, wydarzeń, planowanie w kalendarzu

Instagram

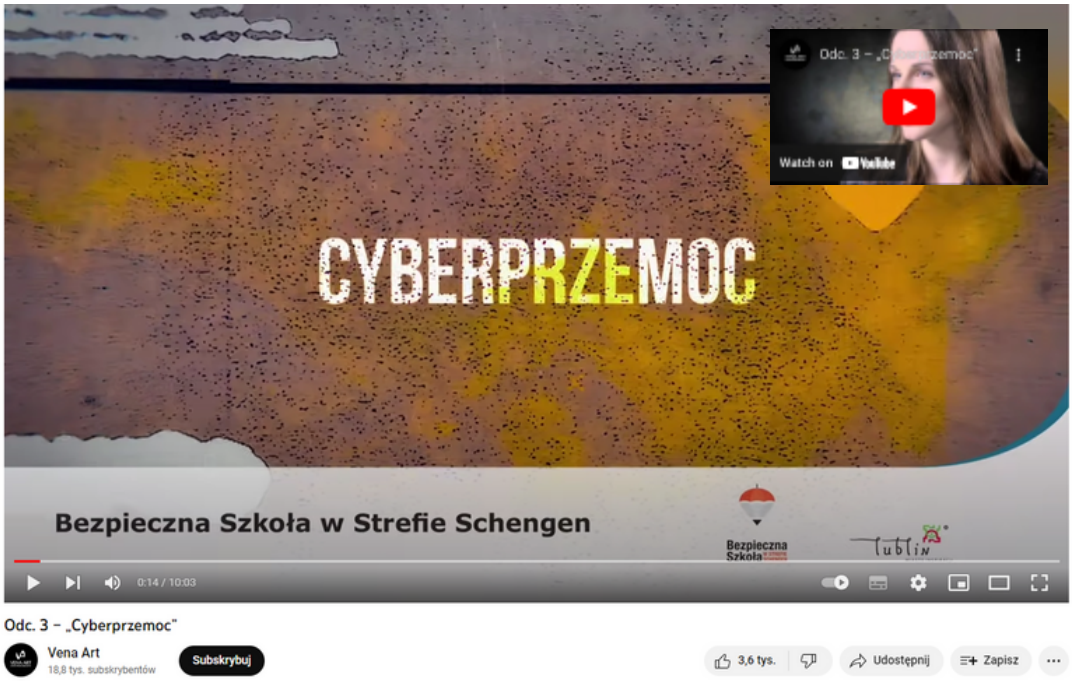
- Wrzucanie zdjęć i relacji, filmików
- Opiniowanie, ocenianie i tworzenie poleceń
- Przekazy na żywo - nagrania w czasie rzeczywistym
- Tworzeni sieci kontaktów, znajomych, followersów

Pinterest

- Dzielenie się zdjęciami, poradami, inspiracjami;
- Grupowanie według zainteresowań, pasji;
- Tworzenie bazy polubionych treści;
- Ułatwienie w poszukiwaniu interesujących zdjęć, treści graficznych.

02 Jak pozostać bezpiecznym w mediach społecznościowych

Istnieje wiele zasad bezpiecznego użytkowania w sieci, w tym kursie nieustannie namawiamy do ostrożnego i uważnego korzystania z Sieci. Jesteśmy świadomi, również że istnieje wiele cennych informacji, których treści powinny trafiać do jak najszerszej widowni. To jeden z największych plusów Internetu, cenne, edukacyjne treści, które zwiększają świadomość, poziom wiedzy i pozwalają na uchronienie siebie i innych przed krzywdą i szkodą.



https://www.youtube.com/watch?v=XMcr2-Ke3I4

03 Zalety i wady mediów społecznościowych

ZALETY

1. Pozwalają na tworzenie nowych kontaktów i podtrzymywanie relacji z rodziną i przyjaciółmi, dla osób nieśmiałych i z fobiami ułatwiają kontakt z zewnętrznym światem;
2. Ocenianie i opiniowanie miejsc podróży, restauracji, firm, usług itp.
3. Dzielenie się pasjami, ich rozwijanie, znajdowanie osób i grup o tych samych zainteresowaniach;
4. Bycie na bieżąco z najnowszymi informacjami, wydarzeniami na świecie, lokalnymi, u sławnych osób, polityków, artystów;
5. Szukanie inspiracji, motywacji;
6. Możliwość kupowania przedmiotów, usług;
7. Rozwijanie swojej firmy, budowanie swojej marki;
8. Zachęcanie do zdrowego trybu życia, bycia zdrowym fizycznie i mentalnie;
9. Walki o słuszne idee, tworzenie grup charytatywnych, wolontariackich;
10. Bywają pomocne w zlokalizowaniu zaginionych osób, np. poprzez szybkie dzielenie się informacjami.

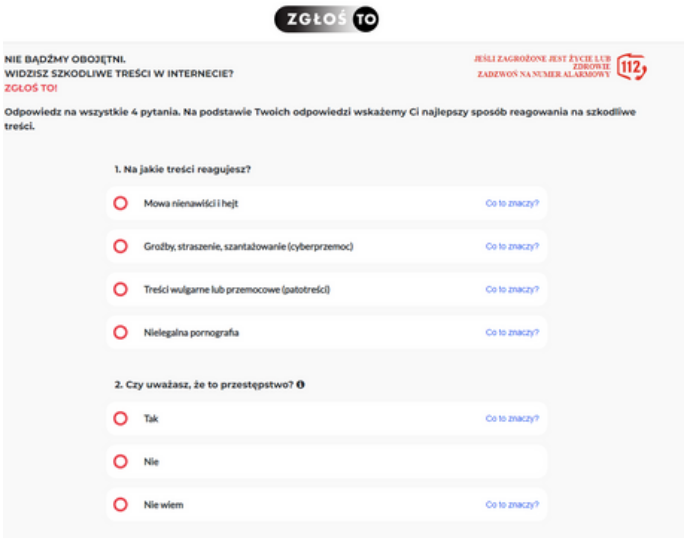
WADY

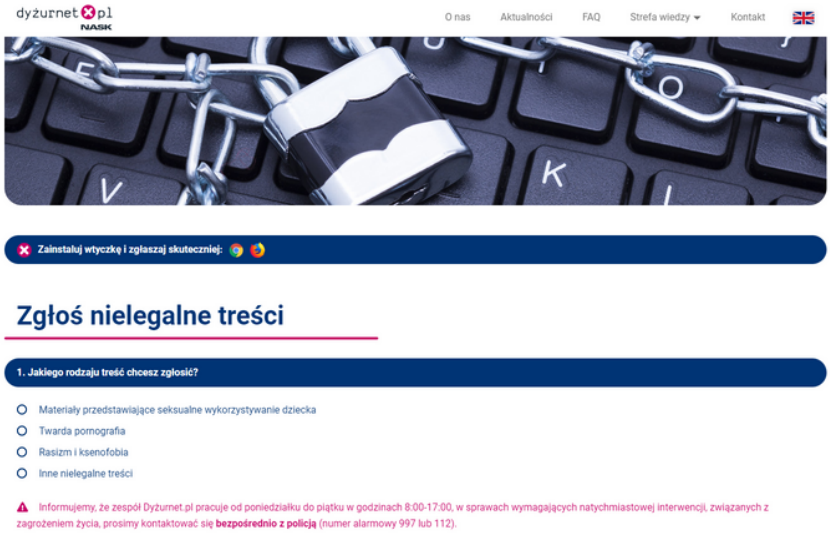
1. Podrabianie zdjęć, wykorzystywanie treści innych użytkowników;
2. Kradzieże profili, wykorzystywanie ich do oszukiwania innych użytkowników;
3. Oczernianie i szantażowanie innych użytkowników, znęcanie się online;
4. Trudności ze zrozumieniem udostępniania treści na pokaz, "iluzji sukcesu" i "instagramowego życia" i związane z tym załamania nerwowe, depresja, dążenie do nierealnego celu za wszelką cenę;
5. Rozpowszechnianie nieprawdziwych, a nawet szkodliwych informacji, często będących zagrożeniem dla zdrowia;
6. Tworzenie i rozpowszechnianie trendów szkodliwych dla zdrowia, a nawet życia;
7. Ograniczają realne relacje, spotkania twarzą w twarz;
8. Zmieniają powszechnie przyjęte metody komunikacji;
9. Negatywnie wpływają na odpoczynek, sen, zdrowie;
10. Powodują uzależnienia, przykuwają nad do naszych telefonów i komputerów;

Szkodliwy i pozytywny wpływ mediów społecznościowych zależy od nas i tego jak z nich korzystamy.

04 Jak zgłosić szkodliwe treści

"Aż 54% osób, które natrafiają w internecie na treści przemocowe, które łamią prawo zadeklarowało, że nigdzie ich nie zgłasza, w tym 30% ankietowanych stwierdziło, że ich brak reakcji wynika z niewiedzy, gdzie i jak zgłaszać takie treści.
Dlatego, aby wesprzeć ludzi w zgłaszaniu szkodliwych treści, Rzecznik Praw Obywatelskich i Fundacja Dajemy Dzieciom Siłę przy wsparciu partnerów uruchomili platformę zglos.to, zainaugurowaną podczas konferencji prasowej, w której obok organizatorów wzięli udział przedstawiciele Facebook Polska oraz Google"[1].





Materiały źródłowe

https://bip.brpo.gov.pl/pl/content/zglosto-kampania-spoleczna-rpo-i-fdds-przeciwko-szkodliwym-tresciom-w-internecie
https://www.gov.pl/web/cyfryzacja/pomoz-reaguj-zglos-nielegalne-tresci

Miejsc gdzie możemy zgłaszać niebezpieczne lub szkodliwe treści jest więcej. Każdy portal społecznościowy posiada swoje procedury i możliwości zgłaszania takich sytuacji. Nie bójmy się reagować, zawsze możesz zgłosić sprawę na policji.

SPRAWDŹ PRZYKLAD NR 1

05 Wskazówki dla użytkowników mediów społecznościowych

Bądź uważny

- Zanim coś opublikujesz, pomyśl, czy ktoś może to wykorzystać przeciwko tobie;
- Nie klikaj w nieznane linki, reklamy, itp.;
- Dokładnie sprawdzaj, z kima nawiązujesz znajomość;
- Wyłącz śledzenie lokalizacji przez media społecznościowe;
- Ogranicz widoczność swojego konta;
- Umieszczaj jak najmniej szczegółów dotyczących Ciebie i twojego życia.

Bądź nieufny

- Unikaj fałszywych kont; sprawdzaj listy znajomych, szczegóły konta, zdjęcia profilowe i inne, udostępniane treści;
- Informacje które udostępniają twoi znajomi nie musza być prawdziwe, wiele osób nie weryfikuje prawdziwości informacji;
- Nie rób nic pochopnie, skuszony/a obietnica szybkiej nagrody;
- Nie udostępniaj swoich czy czyichś prywatnych informacji, np. danych finansowych, zdrowotnych, osobistych.

Bądź ostrożny

- Nie udostępniaj wrażliwych zdjęć, np. nagich lub pokazujących twoje dokumenty;
- Ignoruj wiadomości i posty napisane dziwnym jeżykiem, z błędami, niezrozumiałe;
- Pamiętaj, jeśli dodajesz kogoś do swoich znajomych, pozwalasz na większy dostęp do swoich danych.

Uważaj co publikujesz

- Pamiętaj, to co trafia do Internetu, może posłużyć nieuprawnionym osobom do nielegalnych działań;
- Dzieląc się prywatnymi informacjami, niektórzy mogą je wykorzystać do skrzywdzenia cię lub upokorzenia;
- Twoje dane mogą ułatwić komuś podszycie się pod ciebie i oszukanie twojej rodziny lub znajomych.

Zarządzaj uprawnieniami

- Każda strona i portal daje Ci możliwość zarządzania uprawnieniami prywatności. Korzystanie z nich jest niezwykle ważne, zwłaszcza jeśli chodzi o media społecznościowe. Pozwoli Ci to na uniknięcie sytuacji, w której całkowicie obce osoby zdobędą twoje dane, lub będą monitorować twój profil.

Czy wiedziałeś, że...

- W I kwartale 2019 roku, Facebook usunął ponad 2 miliardy fałszywych kont;
- Szacuje się, że ok. 5 % kont w portalach społecznościowych jest fałszywe;
- Fałszywe konta są tworzone przez sieci cyberprzestępców i specjalne "oddziały" cybernetyczne i propagandowe w niektórych krajach, aby wpływać na opinie ludzi na szczególnie wrażliwe tematy, polaryzować i skłócać ludzi oraz rozsiewać fałszywe informacje i propagandę.

Informacja dla wykładowcy:
Czas: 2h
Wykładowco:
1. Rozdaj karty z ćwiczeniami.
2. Przedstaw poniższy materiał;
3. Nawiązuj do przykładów i ćwiczeń.
4. Pilnuj czasu – masz do dyspozycji 2 godziny w systemie 45minut nauki, 15 minut przerwy.

Współczesna cywilizacja ma do zaoferowania wiele rozwiązań znacznie ułatwiających życie. Niestety potrafi również nas rozpraszać, dekoncentrować, drenować z energii, przez co tracimy czujność i możemy paść ofiarami osób, które wykorzystują zdobycze technologiczne w złym celu.
W poniższym rozdziale znajdziecie kilka ćwiczeń, wskazówek i przykładów, które pozwolą nam potrenować naszą uważność, zdolności analityczne i obserwacyjne. Niezależnie od wieku nauka poprzez działanie przynosi dobre rezultaty. Dlatego też w ramach tworzącej się Sieci Edukatorów społecznych oraz tego kursu znajdziecie wiele ćwiczeń, pokazujących różnorodność sytuacji, które mogą przydarzyć się wam, waszej rodzinie i znajomym. Im więcej przykładów, wziętych z życia zobaczycie, tym łatwiej będzie wam rozpoznać próby oszustw i się przed nimi uchronić.

01 Połącz wyrażenia, aby utworzyły poprawne stwierdzenia:

Cyberoszuści często wykorzystują	... powinnam/powinienem od razu usuwać podejrzane e-maile
Aby uniknąć złośliwych oprogramowań	... pochodzić z legalnego źródła i być sprawdzony
Program antywirusowy, który wybrałem/am powinien ...	... oszustwa dotyczące fałszywych wygranych
Zapisywanie danych do logowania w przeglądarce, ...	... powinniśmy być krytyczni i nieufni co do tego co widzimy na ekranach
Aby uniknąć niewłaściwych treści w Internecie...	... nie jest zalecane

02 Krytyczna ocena informacji

Na co dzień nasz mózg dokonuje szybkich ocen sytuacji, swój udział w nich mają nasze doświadczenia, uprzedzenia, stereotypy. Choć część z nich postrzegamy negatywnie, pomagają nam podświadomie, szybciej i często trafniej podejmować decyzje. Dzięki takimi skrótom, nie zastanawiamy się nad tym, czy do podniesienia garnka z gotująca się wodą użyjemy gołych rąk, czy np. ręcznika kuchennego. Nasz mózg działa automatycznie, aby uchronić nas przed potencjalną krzywdą. Cyberprzestępcy doskonale wiedzą jakie mechanizmy i procesy myślowe zachodzą w ludzkim mózgu i starają się je wykorzystać przeciwko nam. Dla przykładu, poruszone wcześniej zwycięstwa w loteriach. Lubimy szybkie i łatwe nagrody i nie jest to coś czego powinniśmy się wstydzić. Masz mózg podświadomie podsuwa nam rozwiązania, które skrótowo, uzna za lepsze, skuteczniejsze, takie które pozwolą nam poczuć dopływ dopaminy - hormonu szczęścia.

Nie przejmuj się, wszyscy tak mamy. Nasz mózg po prostu nastawiony jest na efektywne, szybkie i pozytywne rezultaty, raczej niż na długie analizy, potencjalne marnowanie czasu i małą efektywność. W końcu kto nie lubi czuć się dobrze z myślą, że udało mu się coś upolować na promocji, że zaoszczędził pieniądze, zdobył coś miłego bez większego zaangażowania.

Cyberprzestępcy bazują na schematach, dają nam wizję uzyskania czegoś miłego, nagrody, promocji, zwycięstwa, kiedy rzeczywistość jest zupełnie inna.

Jeśli dodamy do tego: pośpiech, nerwowość, strach, manipulację, niepewność czy niewiedzę, nic dziwnego, że przestajemy myśleć racjonalnie, chwytamy się pierwszych rozwiązań, które wybierane emocjonalnie często są naszą zgubą. Dlatego też tak ważna jest krytyczna ocena informacji i sytuacji.

03 Gra "Prawda - Fałsz"

PRAWDA		FAŁSZ
☐	1.Podczas tworzenia hasła pamiętaj o uwzględnieniu symboli i cyfr, aby utrudnić jego złamanie.	☐
☐	2. Podczas pobierania programów z Internetu należy zawsze najpierw przeskanować komputer programem antywirusowym w celu wykrycia wirusów.	☐
☐	3. Zezwalaj przeglądarkom internetowym na zapamiętywanie nazwy użytkownika i hasła.	☐
☐	4. Prześlij dane osobowe w Internecie.	☐
☐	5. Podaj swoje hasło wszystkim i zawsze używaj tego samego hasła przez cały czas.	☐
☐	6. Otwieraj i pobieraj załączniki z nieznanego źródła, ponieważ mogą one zawierać wirusy.	☐
☐	7. Wypełniaj wszelkie ankiety internetowe, które proszą o podanie danych osobowych lub danych bankowych.	☐
☐	8. Jeśli korzystasz z pokojów rozmów, użyj hasła jako nazwy użytkownika.	☐
☐	9. Korzystaj z oprogramowania antywirusowego i regularnie je aktualizuj.	☐
☐	10. Rejestruj wszystkie transakcje dokonywane online i regularnie sprawdzaj swoje konto bankowe.	☐

04 10 sposobów na zweryfikowanie prawdziwości publikacji w Internecie

1 Czy artykuł zawiera cytaty, odniesienia i linki?

Czy brakuje nazwiska autora? 2

3 Jeśli podane jest nazwisko autora, czy jest on osobą wiarygodną, znaną?

Co można znaleźć w sekcji „O nas", "Regulamin", "Kontakt" na stronie internetowej, którą przeglądamy? 4

5 Czy w tekście występują błędy ortograficzne, gramatyczne, językowe? Czy zachowana jest poprawna konstrukcja zdań?

Czy w artykule są cytaty, które są niewłaściwie użyte lub wyrwane z kontekstu? 6

7 Czy możesz znaleźć podobny artykuł w Internecie?

Czy artykuł przedstawia tylko jedną stronę sporu? 8

9 Czy nagłówek nie pasuje do treści artykułu?

Czy historia jest całkowicie oburzająca? 10

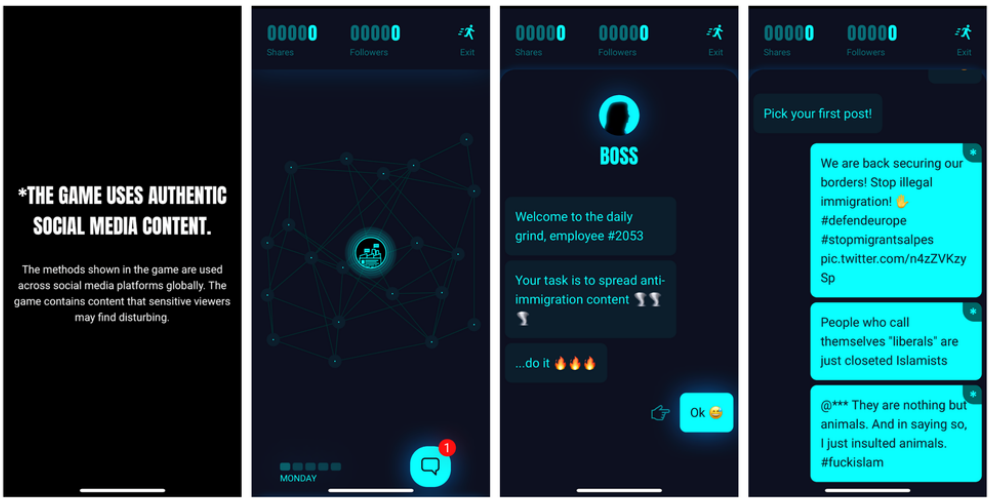
Pamiętaj! To że dana wiadomość ma wiele komentarzy i lajków, lub, że udostępnił ją ktoś z twoich znajomych, nie oznacza, że jest wiarygodna

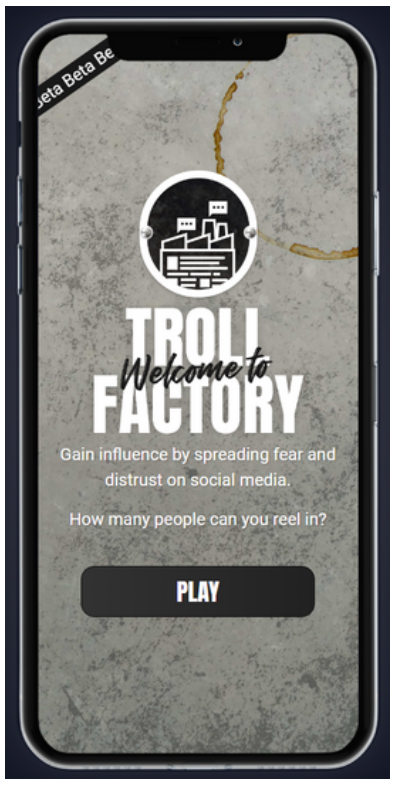
Zapewne nie raz zdarzyło Ci się zobaczyć w Internecie nagłówek o bardzo nietypowym tytule, który sprawił, że pomyślałeś/aś, "niemożliwe, muszę to sprawdzić/ muszę to przeczytać". Kiedy jednak czytasz artykuł okazuje się, że albo w ogóle nie dotyczy on tytułu, lub został on wyrwany z kontekstu, wyłącznie, aby przyciągnąć Twoją uwagę. Są jednak artykuły, których twórcy chcą imitować prawdziwe publikacje, abyś czytając go wierzył/-a w jego prawdziwość. Powyższe punkty, pozwolą Ci krytycznym okiem spojrzeć na jego autentyczność i zweryfikować, czy można czy nie należy ufać temu co jest w nim napisane.

05 Gra "Troll Factory"

Fińska firma YLE stworzyła grę, którą możemy otworzyć w przeglądarce, ukazującą wbrew pozorom proste mechanizmy polegające na szerzeniu strachu, pogardy poprzez fałszywe, lub zmanipulowane informacje w mediach społecznościowych. Znajdziecie ją pod poniższym linkiem:

https://trollfactory.yle.fi/





Chcesz wiedzieć więcej:

https://www.edukacjaprawnicza.pl/informacja-w-mediach-dezinformacja-trolling-postprawda-fake-news-deepfake/
https://trollfactory.yle.fi/

Kurs Seniorzy dla Seniorów

Dofinansowane przez
Unię Europejską

Kontakt:

www.goluchowski.edu.pl - Zakładka "Akademia"

seniorzy_edukatorzy@goluchowski.edu.pl

Akademia Nauk Stosowanych im. J. Gołuchowskiego, Rektorat
ul. Akademicka 12, Ostrowiec Świętokrzyski 27-400
z dopiskiem "Projekt Seniorzy dla Seniorów"