Uniwersytet Ekonomiczny w Katowicach
Informatyka, semestr 1
Studia stacjonarne II stopnia

Przedmiot: Inżynieria bezpieczeństwa

Temat:

Bezpieczeństwo informacji w internecie.

Opracował: Tomasz Chmiel

Rok akademicki: 2023/2024

Spis treści

Wstęp.....3
Najpopularniejsze cyberzagrożenia.....4
Facebook, czyli najciemniej pod latarnią.....5
Bezpieczeństwo systemu płatności mobilnych BLIK.....6
Atak na klientów ING.....8
Sztuczna inteligencja – pomoc czy zagrożenie?.....10
Zasady bezpiecznego korzystania z internetu.....10
Podsumowanie.....11
Źródła:.....12

Wstęp

Wraz z dynamicznym postępem technologicznym i nieustającymi przemianami świata cyfrowego, bezpieczeństwo informacji w sieci stało się jednym z nadrzędnych zagadnień debaty publicznej. Trzecia rewolucja przemysłowa, związana z epoką komputerów, znacząco odmieniła nasze postrzeganie dostępu do informacji i komunikacji. Jednakże dopiero w dobie czwartej rewolucji przemysłowej, określanej okresem zanikania bariery ludzie/maszyny, jako społeczeństwo stoimy przed wyjątkowo wymagającym wyzwaniem cybernetycznym. Czwarta rewolucja przemysłowa to nie tylko kolejny etap rozwoju technologicznego, lecz przełom, który zmienia sposób, w jaki funkcjonujemy zarówno w świecie fizycznym, jak i wirtualnym. Maszyny stają się inteligentniejsze, zdolne do samodzielnego uczenia się i podejmowania decyzji. Ludzie zaś stopniowo integrują się z technologią, co prowadzi do nowych, imponujących możliwości, ale jednocześnie niesie ze sobą poważne wyzwania, zwłaszcza w kontekście bezpieczeństwa informacji. Niestety, wyniki badań ankietowych i eksperymentów społecznych nie pozostawiają wątpliwości co do tego, że dla większości ludzi internet wciąż jawi się jako bezpieczne i beztroskie miejsce, gdzie można swobodnie czerpać korzyści z cyfrowego świata, nie myśląc o problemach i zapominając o jakimkolwiek ryzyku odbywanej przyjemności. Potwierdzają to badania, które wykazały, że społeczeństwo XXI wieku bardziej obawia się braku dostępu do sieci, niż wszelkiego rodzaju ataków, czy wyłudzeń. Kiedy jakiś czas temu Facebook miał globalną awarię wielu użytkowników nerwowo odświeżało aplikację. Sprawdzało połączenie internetowe, szukało informacji, dlaczego serwis nie działa. Dowiodło to, że FOMO jest bliżej niż się wydaje. Fear of missing out (FOMO), oznacza lęk przed wypadnięciem z obiegu. To obawa, że coś istotnego nam umknie, kiedy nie będziemy online. Problem ten dotyczy znacznej liczby polskich internautów – już 14% z nich charakteryzuje się wysokim poziomem FOMO, a kolejne 67% doświadcza go w średnim nasileniu. W grupie młodych ludzi, w wieku 15–19 lat, wysokiego i średniego poziomu FOMO doświadcza aż 94%. Niemniej jednak, prawda jest taka, że serwisy internetowe, mimo swojej użyteczności oraz licznych korzyści, niosą ze sobą poważne zagrożenia, których skutki mogą być odczuwalne przez długie lata. W kontekście tych wyzwań, kolejne części referatu skoncentrują się na bardziej szczegółowym przedstawieniu problemów i zagrożeń czyhających w sieci. Będzie to miało na celu zwiększenie świadomości i umożliwienie uniknięcia potencjalnych ataków w przyszłości. Jednak w trakcie zagłębiania się w tematykę cyberbezpieczeństwa staje się jasne, że rozwiązanie istniejących problemów i zagrożeń jest nadzwyczaj trudne oraz wymaga nie tylko ogromnej wiedzy technicznej, ale także strategicznego podejścia do kwestii bezpieczeństwa informacji. Z tego powodu, nie można obiecać, że po lekturze tego referatu

staniesz się ekspertem w dziedzinie bezpieczeństwa online, któremu żaden atak nie jest straszny. Aczkolwiek zdecydowanie warto poświęcić czas na zapoznanie się z jego treścią, ponieważ dostarczy ona sporo wartościowych informacji dotyczących zagrożeń i środków ochronnych w cyberprzestrzeni.

Najpopularniejsze cyberzagrożenia

Zanim zostaną przedstawione możliwe ataki, zagrożenia i metody jak im przeciwdziałać, warto skupić się nad czysto teoretycznym aspektem cyberbezpieczeństwa, rozbierając to słowo na jego składowe. **Cyber** - «pierwszy człon wyrazów złożonych wskazujący na ich związek z informatyką, a zwłaszcza z internetem». **Bezpieczeństwo -** «to stan w którym jednostka, grupa społeczna, organizacja, państwo nie odczuwa zagrożenia swego istnienia lub podstawowych interesów; sytuacja w której występują formalne, instytucjonalne i praktyczne gwarancje ochrony.» W dalszej części pracy bardzo dobitnie będzie przedstawione to, iż różnie bywa z tą gwarancją ochrony w internecie, a w zasadzie, że jest to swego rodzaju oksymoron. Ale jakich konkretnie ataków, a co za tym idzie zagrożeń bezpieczeństwa informacji możemy doświadczyć w sieci?

Phishing to próba wyłudzenia informacji, takich jak loginy i hasła do kont internetowych, numery kart kredytowych i PESEL. Przestępcy podszywają się w mailach lub SMS-ach pod znane firmy czy urzędy. Możesz np. dostać mail, który udaje wiadomość od kuriera. W mailu znajduje się z kolei link, pod którym masz dopłacić drobną kwotę do przesyłki. Link prowadzi jednak do strony, którą phisherzy wykorzystują do zbierania danych. Poufne informacje hakerom udostępnia sama ofiara – przykładowo logując się do serwisu, który postrzega jako autentyczny i zweryfikowany.

Spear phishing można określić jako bardziej zaawansowaną formę phishingu. Polega na dostosowaniu treści wysyłanego maila do zainteresowań adresata – hakerzy robią przegląd profili społecznościowych potencjalnej ofiary i jeżeli znajdą informacje o jej zainteresowaniach, uwzględniają je w proponowanym linku, załączniku.

Ransomware to złośliwe oprogramowanie, które może zaszyfrować pliki i utrudnić dostęp do systemu komputerowego. Zazwyczaj uniemożliwia korzystanie ze smartfona, laptopa czy tabletu, ponieważ na ekranie wyświetlają się informacje o konieczności zapłacenia okupu, by odzyskać dostęp do plików zaszyfrowanych przez hackerów.

Malware – termin ten jest bardzo szeroki i obejmuje zarówno fragmenty kodu, jak i programy szkodzące systemowi. Należy pamiętać, że malware nie jest tylko jednym typem oprogramowania, ale grupą różnych programów o zróżnicowanych funkcjach, które łączy jeden

cel. Jest nim atak na wewnętrzny system urządzenia. W zależności od typu złośliwe oprogramowanie może dążyć do uszkodzenia podstawowych funkcjonalności systemu, skasowania danych, otworzeniu, tzw. tylnych drzwi do kolejnych ataków, blokady komputera lub atakowania reklamami.

Ataki DDoS polegają na tym, że atakujący przeciążają system komputerowy lub sieć, generując ogromny ruch z wielu źródeł jednocześnie. To prowadzi do utraty dostępności usług dla uczciwych użytkowników. Ataki DDoS mogą być stosowane w celu zablokowania dostępu do ważnych zasobów online lub usług, co wpływa negatywnie na funkcjonowanie systemów i organizacji.

Facebook, czyli najciemniej pod latarnią

Wielu wydaje się, że niebezpiecznie w sieci robi się dopiero po kliknięciu w podejrzany link albo gdy wyświetlane treści nie są family-friendly. Lecz fakty są takie, że internetowi oszuści idą tam, gdzie mogą znaleźć najwięcej potencjalnych ofiar. Dlatego Facebook, z którego korzysta prawie 3 miliarda ludzi jest idealnym miejscem na polowanie. Użytkownicy spędzają tam dużo czasu, czując się pewnie, bo gdzie jak gdzie ale na tym najpopularniejszym serwisie społecznościowym włos nam z głowy nie powinien spaść. Większość ataków które zostaną opisane będzie się opierać na olbrzymiej naiwności społeczeństwa, a uniknięcie ich wymaga jedynie odrobiny zdrowego rozsądku.

„Zobacz jak wygląda pijana miss Polski bez ubrań". „Luksusowa posiadłość za jedną trzecią ceny – najatrakcyjniejsze licytacje komornicze w Twojej okolicy". Do tego ciekawe, nie rzadko ocenzurowane zdjęcie i spora liczba kliknięć takiego „artykułu" gwarantowana. Jednak co naprawdę się stanie gdy klikniemy interesujący nas nagłówek. Kto liczył na gorące fotki lub interes życia mocno się zawiedzie. W najlżejszej sytuacji zostaniemy przekierowani na stronę pełną pustych reklam pojawiających się praktycznie wszędzie, a których zamknięcie wymaga znalezienie mikroskopijnego krzyżyka. Gorzej gdy ktoś postarał się bardziej i po kliknięciu zostaniemy poprowadzeni do strony udającej serwis YouTube. Tam pojawi się informacja o braku możliwości obejrzenia materiału bez instalacji specjalnego rozszerzenia. Emocje wzrastają, bo przecież wystarczy pobrać jakąś śmieszną wtyczkę i treść się pojawi. W rzeczywistości jeśli użytkownik zdecyduje się na ten krok, z jego konta zaczną być udostępniane fałszywki podobne do tych, na które sam się nabrał, a jego urządzenie zostanie zainfekowane przez złośliwe oprogramowanie mogące kontaktować się ze znajomymi zaatakowanej osoby. Pro wadzi to do sytuacji w której nasz znajomy otrzymuje wiadomość bezpośrednio od nas z treścią: "Cześć nie wiem czy wiesz o tej stronie http://4g831.9ou.info ale ktoś tam wrzucił twoje

przerobione zdjęcie z fb. Słaba akcja także lepiej cos z tym zrób." Albo krócej: „To ty? <emotikon zaskoczenia> http://pinp.eu.wow2314.2.ou.al”. Gdybyśmy dostali takie coś od nieznajomego to pewnie szybko zapaliłaby się lampka ostrzegawcza, że przecież to jakiś wirus. Ale skoro to nasz dobry kolega nam wysłał. W takim razie coś musi być na rzeczy. Po kliknięciu w link zostaniemy przeniesieni do podrobionego panelu logowania do Facebooka, który wykrada nasze dane (oczywiście dopiero gdy poprawnie wpiszemy login i hasło). Jest też alternatywna wersja w której zostaniemy poproszeni o podanie swojego numeru telefonu na który zostanie wysłany kod. Niestety jeśli wpiszemy szyfr otrzymany smsem wcale nie wyświetli się wspomniane wcześniej nasze zdjęcie tylko zapiszemy się do płatnej usługi Premium, której regulamin zapewne wyświetlił się chwilowo małymi literami na dole strony. Jeśli na swoim urządzeniu mobilnym nie mamy ustawionego limitu płatnych subskrypcji to taka nie uwaga może kosztować nas nawet do 1200 złotych miesięcznie.

Bezpieczeństwo systemu płatności mobilnych BLIK

Internetowi złodzieje nie spoczęli na laurach wymyślając nowy, lepszy sposób na uszczuplenie portfeli naiwnych użytkowników dzieła Zuckerberga. Wykorzystali do tego wprowadzony w 2015 roku system płatności mobilnych BLIK. Sposób działania jest stosunkowo prosty. Oszust włamuje się na konto lub tak jak zostało to opisane w poprzednim akapicie dane logowania otrzymuje bezpośrednio od zmanipulowanej osoby. Następnie wysyła do znajomych wiadomość prosząc o kod BLIK pod pretekstem zgubienia/zapomnienia portfela, pilnej pożyczki lub po prostu kłopotów finansowych. Poniżej znajduje się przykładowa konwersacja.

Takiej i podobnych rozmów można znaleźć w sieci mnóstwo. Zadaniem hackera jest sprawić aby czytelnik nie nabrał żadnych podejrzeń. Nie ma w nich podejrzanych linków czy treści mogących wzbudzić niepokój. Co prawda temat pożyczania pieniędzy sam w sobie jest

dość kontrowersyjny ale skoro prosi nas o to brat, przyjaciel albo mama to dlaczego mielibyśmy tego nie zrobić. Samo wysłanie kodu do osoby która się podszywa nie kończy ataku. By pieniądze zniknęły na dobre z naszego konta musimy jeszcze płatność w aplikacji mobilnej banku potwierdzić. Robi się to dosłownie jednym kliknięciem dlatego jeśli lampka awaryjna nie zapaliła nam się wcześniej, teraz raczej już się nie to nie stanie. Najgorsze w tym wszystkim jest to, że jeśli mu na to pozwolimy to oszust w ten sposób może wypłacić całe nasze oszczędności. Jednak oczywistym jest, że dużo łatwiej przyjdzie każdemu pożyczyć znajomemu 50 złotych niż 5 tysięcy. Dlatego nowocześni złodzieje poszli krok dalej. Tym razem kontaktują się z potencjalną ofiarą drogą telefoniczną, podając się za pracownika banku. Informują rozmówcę iż jego konto bankowe zostało zaatakowane i jedynie bardzo szybka reakcja pozwoli nie stracić majątku. Teraz najważniejszy moment całej operacji. Są dwie opcje, albo zorientować się że to ściema i zakończyć rozmowę, albo potraktować to poważnie i wywołać w sobie lęk, który w połączeniu ze stresem, okaże się najgorszym doradcą. Presja czasu i widmo olbrzymiej straty, też robi swoje. W poprzednio omawianym przykładzie użytkownik mógł zadać kilka pytań: „Po co Ci te pieniądze?", „Nie możesz podejść do bankomatu?" albo „Jeśli to faktycznie Ty to wyślij mi swoje zdjęcie z towarem który chcesz zakupić.". Teraz sytuacja jest zgoła odmienna. Dużo łatwiej o pomyłkę, zrobienie czegoś głupiego gdy działamy w nerwach pod wpływem impulsu. Plan działania oszusta jest prosty. Wystraszyć ofiarę, a następnie sprawić aby posłusznie wykonywała jego kolejne polecenia. Po raz kolejny pojawiają się dwa warianty. Pierwszy polega na tym że zmanipulowana osoba jest proszona o przelanie oszczędności na rzekomo bezpieczne konto swojego banku, a następnie środki zostaną mu zwrócone. Chyba nikt nie będzie zaskoczony informacją, że te pieniądze już nie wrócą do właściciela. Drugą, nieco bardziej ambitną metodę działania złodziei opisuje podkarpacka policja. Zaatakowana została 39-letnia mieszkanka powiatu jarosławskiego. Z relacji kobiety wynikało, że odebrała telefon od mężczyzny, który przedstawił się jako pracownik banku, w którym miała konto. Samo połączenie wydawało się wiarygodne, ponieważ oprócz numeru na wyświetlaczu pojawiła się identyfikacja banku. Dzwoniący podał, że ktoś w Krośnie próbował zalogować się na konto pokrzywdzonej i chciał wypłacić z niego 700 zł. Aby zweryfikować tą informację mężczyzna zasugerował aby kobieta pobrała i zainstalowała aplikację bankową. Dalej czytamy, iż zaniepokojona sytuacją i niczego nieświadoma kobieta, zgodnie z podanymi podczas rozmowy instrukcjami, zainstalowała na swoim smartfonie aplikację QuickSupport, celem zablokowania swojej karty do rachunku. Była przekonana, że jest to pracownik banku i pomaga w blokadzie rachunku. Nie wiedziała, że w ten sposób oddała kontrolę nad swoim telefonem oszustowi. Kosztowało ją to ponad 30 tys. zł., które zostały pobrane z jej konta bankowego. Sama instalacja aplikacji nie sprawi że w magiczny sposób konto zostanie

wyczyszczone, natomiast pozwala ona na zdalne przejęcie pulpitu. Oszust może odczytać smsy z kodami do weryfikacji transakcji w bankowości elektronicznej. Ofiara traci możliwość reakcji i zanim się zorientuje, oszuści dokonują szeregu przelewów na rachunki kryptowalutowe, czy też zaciągają zobowiązania finansowe, które natychmiast wypłacają lub przelewają na inne, trudne do wyśledzenia rachunki. Po przejęciu pulpitu i danych logowania, z perspektywy banku operacje wykonywane przez oszusta wyglądają jak zlecone osobiście przez „prawdziwego klienta". Dlatego banki nie są w stanie skutecznie przeciwdziałać takim atakom, bo formalnie klient wykonał operacje samodzielnie, która nie różni się niczym szczególnym od zwyczajowych.

Atak na klientów ING

Zostając w temacie bankowości omówiony zostanie jeden z najlepiej przygotowanych ataków phishingowych, który swoją formą i dbałością o szczegóły budzie niepokój, gdyż tym razem powiedzenie „tylko głupi by się na to nabrał" jest nie trafione. Do masy Polaków została wysłana tak wyglądająca wiadomość:


Od: "ING" <[redacted]>
Data: 1 grudnia 2018 17:14:58 CET
Do: <[redacted]>
Temat: Blokada konta ING
Odpowiedz-do: "ING" <[redacted]>

ING

ING BANK ŚLĄSKI

fot. niebezpiecznik.pl

Blokada konta ING Bank Śląski

W trosce o bezpieczeństwo naszych odbiorców zablokowaliśmy konto w ING Bank Śląski, powodem jest włamanie do konta.
W celu odblokowania dostępu prosimy o weryfikację właściciela konta, logując się na:

Zaloguj aby odblokowac

Zespół ING BANK ŚLĄSKI

Więcej informacji można uzyskać dzwoniąc na infolinię pod numer: 801 222 222.
Prosimy, nie odpowiadaj na tą wiadomość - została wysłana automatycznie.

[redacted]

Oczywiście osoby nie korzystające z usług ING zapewne od razu wyczuły, że to jakieś oszustwo

i zignorowały wiadomość. Natomiast posiadającym oszczędności w skarbcach tego właśnie banku mogło skoczyć ciśnienie bo przecież mowa o włamaniu na konto więc to bardzo poważna sprawa. Klikając w „Zaloguj aby odblokować" zaatakowany zostanie przekierowany na stronę, którą już dobrze zna. Problem w tym, iż choć witryna do złudzenia przypomina tą na której zawsze bezpiecznie logował się do placówki, to tak naprawdę jest to kopia użyta przez złodziei w celu uzyskania informacji pozwalających przejąć finanse ofiary. Po podaniu loginu wyświetla się prośba o hasło wyglądająca w ten sposób:

Najprawdopodobniej ponad 95% zaatakowanych użytkowników zapaliła się w tym momencie czerwona lampka, bo przecież nigdy nie trzeba było podawać całego hasła, a jedynie kilka proszonych pozycji. Co jeśli kompletne hasło zostało wpisane? W tym momencie przestępca oczywiście loguje się podanymi przez ofiarę danymi na jej konto w prawdziwym serwisie ING. Aby okradana osoba nie uciekła (bo przecież jeszcze potrzebny jest kod z SMS-a), przestępca pokazuje jej odliczanie z informacją o treści: „Twoje konto jest aktualnie weryfikowane przez pracownika banku, możesz zostać poproszony o dodatkowe informacje. Prosimy o cierpliwość." Pod tekstem znajduje się czasomierz ustawiony na 2-3 minuty, tak aby oszust miał czas na zlecenie przelewu. Po chwili oczekiwania ofiara zostaje poproszona o wprowadzenie kodu który otrzymała SMSem. Jakby tego było mało zostaje poproszona o ponowne wpisanie kodu SMS tylko nowego. Dzieje się tak, gdyż na niektórych kontach przestępca musi wykonać 2 operacje aby okraść ofiarę. Sama definicja odbiorcy zaufanego nie wystarczy — konieczne może być zerwanie lokaty na koncie ofiary, podbicie limitu dziennego przelewu lub przekazanie dodatkowego kodu autoryzacji jeśli systemy banku stwierdzą anomalię. Na tym kończy się atak, który choć został dobrze zaplanowany to ma w sobie wiele błędów. Ofiara ma kilka okazji, aby zorientować się, że to oszustwo. Po pierwsze e-mail

przychodzi ze złego adresu, po drugie przekierowuje do niepoprawnego serwisu, w którym — po trzecie — trzeba wprowadzić wszystkie znaki hasła. No i po czwarte — ewentualne fałszywe operacje potrzebują kodu z SMS-a, a tam jest napisane do czego on służy.

Sztuczna inteligencja – pomoc czy zagrożenie?

Sztuczna inteligencja nie stanowi zagrożenia sama w sobie. Przynajmniej na razie. Wykorzystanie narzędzi takich jak ChatGPT pokazuje, że technologia ta może być użyteczna w codziennych czynnościach, usprawniając wyszukiwanie informacji czy wspomagając proces nauki nowych umiejętności. Niestety, jak każde potężne narzędzie, może być również wykorzystane w celach niekoniecznie dobrcyh. Przestępcy internetowi, korzystając z aplikacji takich jak ChatGPT, potrafią zwiększyć wiarygodność swoich działań. Dotychczas generowane przez nich maile często ujawniały się brakiem gramatycznej poprawności, gdyż były tłumaczone przez darmowe translatory. Zastosowanie sztucznej inteligencji, zwłaszcza w przypadku ChatGPT, zmienia tę sytuację. To narzędzie świetnie radzi sobie z redagowaniem treści, szczególnie w języku angielskim, umożliwiając oszustom masowe wysyłanie wiadomości z próbami oszustw na światową skalę. Chester Wisniewski, dyrektor ds. technologii w firmie Sophos, zauważa, że możliwości wykorzystania sztucznej inteligencji przez internetowych oszustów są jeszcze szersze. Narzędzia te umożliwiają na przykład generowanie twarzy nieistniejących osób. Kolejnym krokiem może być wykorzystanie ChatGPT do stworzenia kompletnego fałszywego profilu firmy, łącznie z biografiami pracowników, profilami w mediach społecznościowych i stroną internetową. W przypadku korespondencji z botem opartym na zaawansowanej sztucznej inteligencji, trudno jest zorientować się, czy rozmawiamy z człowiekiem czy z maszyną. Aby skutecznie zwalczać tego typu oszustwa, konieczne może być opracowywanie narzędzi, które potrafią rozpoznawać treści generowane przez sztuczną inteligencję. Choć takie aplikacje już istnieją, jak np. DetectGPT czy modele językowe OpenAI, to wciąż nie są one wystarczająco dobre i mylą się zbyt często, by móc im zaufać i traktować jako wiarygodne pomoce.

Zasady bezpiecznego korzystania z internetu

Wyłudzenie danych, kradzież danych, bezpieczeństwo informacji, cyberbezpieczeństwo to bardzo często utarte frazesy, które powtarzane są w mediach z miernym dzisiaj skutkiem. A sprawa jest poważna i każdego kolejnego dnia staje się co raz poważniejsza. Poprzez nieumyślne oddanie komuś swoich danych osobowych można stracić nie tylko czas np. przy wyrabianiu nowego dowodu, ale i być ofiarą wyłudzenia kredytu, dokonania drogich zakupów,

czy założenia fałszywej działalności biznesowej. Aby zadbać o swoje bezpieczeństwo w Internecie, należy przestrzegać tych kilku ważnych zasad:

- Korzystaj z mocnych haseł - przez zwrot mocne hasło należy rozumieć zbiór znaków w postaci liter, cyfr i znaków specjalnych, który liczy sobie ich łącznie więcej niż sześć.
- Stosuj oprogramowanie antywirusowe - do pewnego stopnia oprogramowanie antywirusowe stanowi barierę ochronną naszych urządzeń przed niechcianymi szkodliwymi programami. Im większa baza informacji o wirusach w danym oprogramowaniu antywirusowym, tym lepiej antywirus zablokuje złośliwe oprogramowanie.
- Nie otwieraj podejrzanych maili - Na skrzynki pocztowe przychodzi nieskończona ilość reklam, newsletterów i spamu. Nie zawsze można się przed tym wszystkim obronić, ale z pewnością możemy obronić się przed atakami hackerskimi, na które wystawia my się przez klikanie w linki z podejrzanych maili.
- Aktualizuj przeglądarkę i system operacyjny - Warto pamiętać, że bycie na bieżąco z aktualizacjami, to bycie na bieżąco z zabezpieczeniami. Czyli utrudniamy pracę złodziejom. Gra warta świeczki.
- Nie klikaj w wyskakujące ekrany i podejrzane reklamy - najczęściej takie reklamy spotkamy na stronach, które przeglądarka uzna za niebezpieczne, ale zdarzają się również takie wpadki na bezpiecznych stronach.
- Nie podawaj swoich danych osobowych w internecie - Wyjątkiem mogą być strony rządowe oraz zakupy online. Pamiętaj, że takie organy jak policja, czy służba zdrowia nigdy nie proszą nas o dane osobowe, numer konta bankowego, czy drugie imię cioci.

Podsumowanie

Internet to niewątpliwie wspaniały wynalazek, otwierający światu nowe możliwości komunikacji, dostępu do informacji i rozrywki. Jednak równocześnie stanowi potężne niebezpieczeństwo dla naszego bezpieczeństwa cyfrowego. W trakcie korzystania z sieci niezbędne jest zachowanie ostrożności, ponieważ bagatelizowanie zagrożeń może prowadzić do różnych form nieszczęść. Ochrona prywatności, świadome korzystanie z danych osobowych oraz unikanie podejrzanych stron internetowych to kluczowe elementy, które każdy powinien mieć na uwadze. W dobie rozwiniętych technologii, edukacja cyfrowa staje się kluczowa, aby skutecznie radzić sobie z cyberzagrożeniami. Warto więc być świadomym użytkownikiem, ciesząc się korzyściami, jakie niesie ze sobą internet, jednocześnie biorąc odpowiedzialność za własne bezpieczeństwo w świecie cyfrowym.

Źródła:

- https://niebezpiecznik.pl/ artykuł: Atak na klientów ING
- https://www.ing.pl/ Treści informacyjne o banku i bezpiecznej bankowości.
- https://nety.pl/cyberbezpieczenstwo/ artykuły: „Zasady bezpiecznego korzystania z bankowości elektronicznej” oraz „Zasady ogólne korzystania z sieci Internet”
- https://pl.wikipedia.org/wiki/Cyberbezpieczństwoi
- https://pl.wikipedia.org/wiki/Bezpieczeństwo_teleinformatyczne
- https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo artykuły: „Oszuści podszywają się pod firmy kurierskie.” Oraz „Cyberwojna w Ukrainie. Rząd zaskoczony skutecznością działań.”
- https://www.gov.pl/web/baza-wiedzy/ artykuły: cyberbezpieczeństwo , czym jest phishing ,internet
- https://powerdmarc.com/pl/ransomware-vs-malware-vs-phishing/
- https://www.dobreprogramy.pl/sztuczna-inteligencja-a-bezpieczenstwo
- Książka: „Wyloguj swój mózg” Anders Hansen, wydawnictwo „znak”
- Książka: „Cyberbezpieczeństwo” redakcja naukowa: Cezary Banasiński i Marcin Rojsz czak
- https://4fun.tv/news/will-smith-oszustwo-chelm-35-latka-stracila-kilkadziesiat-tysiecy
- https://zabrze.policja.gov.pl/k29/informacje/wiadomosci/335405,Nie-daj-sie-oszukac-sprzedajac-cos-w-internecie.html
- https://www.gov.pl/web/baza-wiedzy/fomo---czyli-strach-przed-tym-co-nas-omija