idea
nnovation

„Model szkolenia z zakresu bezpieczeństwa w sieci podczas pandemii”

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Unia Europejska
Europejski Fundusz Społeczny

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Społecznego

Spis treści

Opis modelu

„Model szkolenia z zakresu bezpieczeństwa w sieci podczas pandemii” powstał w ramach projektu: **POWR.04.03.00-00-0093/17**, tytuł projektu grantowego: „**Bezpiecznie w trakcie pandemii”**, współfinansowanego ze środków Europejskiego Funduszu Społecznego w ramach Programu Operacyjnego Wiedza Edukacja Rozwój.

Beneficjentem grantu jest polska firma IDEA Innovation Center Sp. z o.o. Sp. k. i stowarzyszenie portugalskie Intercultural Association Mobility Friends.

Wieloletnie doświadczenie partnerów projektu gwarantuje najwyższą adekwatność przygotowanego rozwiązania.

Przygotowany model obejmuje wybrane aspekty związane z bezpieczeństwem korzystania z cyberprzestrzeni.

W odpowiedzi na zaistniały problem, bazując na doświadczeniu tych dwóch ww. podmiotów został przygotowany model, dzięki któremu kadra merytoryczna wnioskodawcy w tym doradcy zawodowi, pośrednicy pracy, psychologowie współpracujący na stałe z wnioskodawcą osobami dotkniętymi bezrobociem oraz osobami długotrwale bezrobotnymi otrzymują gotowy program szkolenia dla osób dotkniętych bezrobociem oraz osób długotrwale bezrobotnych.

Przygotowany model składa się z następujących produktów:

- 4 moduły szkoleniowe, łącznie 4 karty pracy
- cyfrowe kompendium wiedzy dla Uczestników szkolenia w formie Q&A
- broszura dla bezrobotnych
- forum dla Uczestników szkolenia
- Wszystkie materiały dostępne są bezpłatnie do pobrania na stronie: ideainnovation.com.pl

Można je również otrzymać pisząc na adres mailowy: ideainnovation@o2.pl

Rekomendacje dotyczące wdrożenia modelu w firmach organizujących wsparcie dla osób bezrobotnych

Moduły szkoleniowe

Każdy moduł szkoleniowy składa się z 3 części/dokumentów:

- Dokument: „Przebieg warsztatów dla Uczestników szkolenia skierowanego na podniesienie kompetencji z zakresu bezpiecznego korzystania z technologii.”,
- Dokumentu: „KARTA PRACY DLA UCZESTNIKA SZKOLENIA – odpowiednio numer modułu”,
- Prezentacji dla trenera przygotowanej w POWER POINT - odpowiednio numer modułu.

Dokumentem od którego należy zapoznać się z modelem jest „Przebieg warsztatów dla Uczestników szkolenia skierowanego na podniesienie kompetencji z zakresu bezpiecznego korzystania z technologii. – odpowiedni numer modułu”. W tym dokumencie w pierwszej jego części znajduje się

- Opis sposobu realizacji modułów, zastosowanych narzędzi, metod itd.,
- Czas, który trener powinien zaplanować na realizację warsztatów z uwzględnieniem ile czasu powinna zająć teoria, a ile praktyka,
- Informacja na temat tego jakie pomoce dydaktyczne trener powinien przygotować do realizacji danego modułu,
- Opis umiejętności i wiedzy, które powinien mieć dany uczestnik po zakończeniu udziału w danym module.

W dokumencie „KARTA PRACY DLA UCZESTNIKA SZKOLENIA” znajdują się ćwiczenia do samodzielnej lub grupowej pracy dla każdego z uczestników szkolenia. Przed szkoleniem należy przygotować kopię tego dokumentu dla każdego z uczestników szkolenia.

Prezentacja w POWER POINT służy do poprowadzenia wykładu.

Trenerzy oprócz standardowych materiałów do prowadzenia warsztatów (flipchart, mazaki) będą używać komputerów i urządzeń z Androidem..

Poniżej przedstawiamy obszary przedstawiane i ćwiczone podczas każdego z czterech modułów szkoleniowych:

Moduł pierwszy

- Zagrożenia społeczne i fizyczne związane z użytkowaniem komputera , Internetu oraz smartfonów.
- Cyberprzemoc i cyberprzestępstwa.
- Zasady postępowania w przypadku zetknięcia się z cyberprzestępczością i innymi zagrożeniami.
- Typy oszustw w Internecie w tym oszustwa telefoniczne, przez SMS i pocztę elektroniczną.

Moduł drugi

- Ochrona przed szkodliwym oprogramowaniem, ochrona przed wirusami, ochrona przed oszustwami marketingowymi.
- Omówienie narzędzi służących do zabezpieczenia się przed cyberzagrożeniami,
- Omówienie sposobów wykorzystania narzędzi służących do bezpiecznego korzystania z elektronicznych urządzeń komunikacyjnych.
- Omówienie oszustw marketingowych i sposobu ochrony przed nimi.

Moduł trzeci

- Kontakt i relacje z innymi użytkownikami Internetu, dbanie o własny wizerunek w sieci, nieujawnianie wrażliwych informacji. Wiarygodność informacji w Internecie, prawa autorskie.
- Omówienie właściwej komunikacji w Internecie, netykiety.
- Omówienie ochrony informacji wrażliwych, w tym danych osobowych,
- Omówienie weryfikacji pod kątem wiarygodności uzyskanej informacji,
- Omówienie prawa autorskiego dotyczącego publikowanych materiałów.

Moduł czwarty

- Omówienie zagrożeń dla bankowości elektronicznej
- Omówienie sposobów bezpiecznej pracy z bankowością elektroniczną.
- Omówienie zagrożeń wynikających z zakupów w internecie.
- Omówienie sposobów bezpiecznego korzystania z handlu w internecie.

Cyfrowe kompendium wiedzy dla Uczestników szkolenia skierowanego na podniesienie kompetencji z zakresu bezpiecznego korzystania z technologii Q&A

Ten dokument zawiera 20 pytań i odpowiedzi.

Każda osoba uczestnicząca w szkoleniu może skorzystać z kompendium, aby uzyskać odpowiedź na nurtujące pytanie. Dokument powstał na podstawie pytań zadawanych przez uczestników – biorących udział w projektach finansowanych z EFS.

Broszura dla bezrobotnych

Celem modelu jest również zachęcenie bezrobotnych do bezpiecznego i świadomego korzystania z sieci komputerowych. Aby było to możliwe muszą posiadać wiedzę na temat zagrożeń w cyberprzestrzeni, rozpoznawania ich i sposobów zabezpieczania się przed nimi. Wszystkie te informacje znajdują właśnie w tej broszurze.

Forum dla Uczestników szkolenia skierowanego na podniesienie kompetencji z zakresu bezpiecznego korzystania z technologii

- Każdy z Uczestników może zadać pytanie w jednym z następujących obszarów w formie elektronicznej:
- Zagrożenia społeczne i fizyczne związane z użytkowaniem komputera , Internetu oraz smartfonów.
- Cyberprzemoc i cyberprzestępstwa.

- Zasady postępowania w przypadku zetknięcia się z cyberprzestępczością i innymi zagrożeniami.
- Typy oszustw w Internecie w tym oszustwa telefoniczne, przez SMS i pocztę elektroniczną.
- Ochrona przed szkodliwym oprogramowaniem
- Ochrona przed oszustwami marketingowymi.
- Ochrona przed szkodliwym oprogramowaniem, ochrona przed wirusami, ochrona przed oszustwami marketingowymi.
- Narzędzia służące do zabezpieczenia się przed cyberzagrożeniami,
- Narzędzia służące do bezpiecznego korzystania z elektronicznych urządzeń komunikacyjnych.
- Oszustwa marketingowe i sposoby ochrony przed nimi.
- Właściwa komunikacji w Internecie, netykiety.
- Ochrona informacji wrażliwych, w tym danych osobowych,
- Wiarygodność informacji w sieci,
- Prawo autorskie w sieci.
- Zagrożenia dla bankowości elektronicznej
- Sposoby bezpiecznej pracy z bankowością elektroniczną.
- Zagrożenia w handlu internetowym.
- Sposoby bezpiecznego korzystania z handlu w internecie

Adres internetowy pod którym dostępne jest forum: http:// ideainnowation.com.pl

MODUŁ 1 - Zagrożenia społeczne i fizyczne związane z użytkowaniem komputera , Internetu oraz smartfonów. Cyberprzemoc i cyberprzestępstwa. Typy oszustw w Internecie w tym oszustwa telefoniczne, przez SMS i pocztę elektroniczną. Zasady postępowania w przypadku zetknięcia się z cyberprzestępczością i innymi zagrożeniami.

Przebieg warsztatów dla Uczestników szkolenia skierowanego na podniesienie kompetencji z zakresu bezpiecznego korzystania z technologii – moduł I

Lp.	Opis sposobu realizacji modułów, zastosowanych narzędzi, metod itd.	Czas/teoria	Pomoce dydaktyczne	Nabywane umiejętności i wiedza (cele działania)
1	Omówienie czym są zagrożenia społeczne, jakie rodzaje zagrożeń występują w związku z korzystaniem z cyberprzestrzeni. Ćwiczenie numer 1 z Karty Pracy	1h/20 min.	Prezentacja, Karta pracy, Flipchart, komputer z systemem Windows, strony internetowe prezentujące ataki na żywo https://threatmap.checkpoint.com/	Uczestnik dowie się jakie rodzaje zagrożeń występują w związku z korzystaniem z cyberprzestrzeni. Pozna

				przykłady zagrożeń.
2	Przedstawienie czym jest cyberprzemoc i cybeprzestępstwa. Ćwiczenie numer 2 z Karty Pracy	2h/20 min.		Uczestnik szkolenia dowie się jakie są rodzaje cyberprzemocy i cyberprzestępstw.
3	Przedstawienie przykładów oszustw w Internecie w tym oszustwa telefonicznych, przez SMS i pocztę elektroniczną. Ćwiczenie numer 3 z Karty Pracy	2h/30 min.		Uczestnik pozna praktyczne przykłady ataków realizowanych przez cyberprzestępców.
4	Przedstawienie sposobów zabezpieczenia się przed atakami i zasady postępowania w przypadku zetknięcia się z cyberprzestępczością i innymi zagrożeniami.	2h		Uczestnik zapozna się z praktycznymi sposobami rozpoznawania i radzenia sobie z atakami cyberprzestępców. Zapozna się również ze

	Omówienie sposobów zabezpieczania się przed zagrożeniami wynikającymi z korzystania z cyberprzestrzeni.			sposobami zapobiegania zagrożeniom wynikającym z korzystania z cyberprzestrzeni.
	Podsumowanie	7h/1h 10min.		

Opis ćwiczeń do modułu pierwszego

Ćwiczenie nr 1

Zagrożenia społeczne nietechniczne - Czy spotkałeś się z przypadkiem nietechnicznego zagrożenia społecznego?

Uczestnicy szkolenia pracują najpierw indywidualnie, potem prezentacja swoich wyników na forum wszystkich uczestników.

Trener informuje, że ćwiczenie ma na celu zaprezentowanie własnych doświadczeń lub propozycji, które uświadomią innym uczestnikom rodzaje zagrożeń.

Podczas ćwiczenia uczestnicy analizują rodzaj zagrożeń społecznych następnie przedstawiają przykłady, z którymi mieli styczność lub proponują przykłady, które wymyślili na podstawie informacji zaprezentowanych przez trenera.

Ćwiczenie składa się z dwóch etapów.

1) Etap I. Uczestnicy pracują indywidualnie. Analizują przykłady zagrożeń i proponują własne, których doświadczyli lub wymyślili na podstawie informacji przekazanych przez trenera.

2) Etap II. Uczestnicy szkolenia prezentują na forum grupy swoje przykłady zagrożeń. Prowadzona jest dyskusja na temat zaprezentowanych przez uczestników propozycji..

Cel ćwiczenia:

- Zrozumienie przez uczestników szkolenia jakie rodzaje zagrożeń występują w związku z korzystaniem z cyberprzestrzeni.

Ćwiczenie nr 2

Analiza ataków cyberprzestępców na świecie.

Trener prezentuje interaktywną mapę ataków cyberprzestępców na świecie lub przekazuje link do otworzenia jej na komputerze Uczestnika. Uczestnicy szkolenia analizują mapę ataków na żywo i odpowiadają na pytania umieszczone w ćwiczeniu.

1. Jakich rodzajów ataków jest najwięcej na świecie?
2. Które kraje są aktualnie najczęściej atakowane?
3. Jakie zagrożenia najczęściej są spotykane w Polsce?

Ćwiczenie składa się z dwóch etapów.

1) Etap I. Uczestnicy pracują indywidualnie. Analizują interaktywną mapę ataków na świecie i odpowiadają na pytania zadane w ćwiczeniu.

2) Etap II. Uczestnicy szkolenia prezentują na forum grupy swoje odpowiedzi i na tej podstawie prowadzona jest dyskusja na temat ataków cyberprzestępców na świecie.

Cel ćwiczenia:

Uczestnicy uświadomią sobie realne zagrożenie ze strony ataków cyberprzestępców, zapoznają się z ich skalą i ryzykiem wystąpienia w ich w czasie korzystania z cyberprzestrzeni.

Ćwiczenie nr 3

Jak rozpoznać atak cyberprzestępców

Uczestnicy na podstawie zaprezentowanych na karcie pracy maili z cyberatakami, mają wskazać, które elementy świadczą o tym, że jest to próba ataku.

Ćwiczenie składa się z dwóch etapów.

1) Etap I. Uczestnicy pracują indywidualnie. Analizują przykłady przedstawione na karcie pracy i wskazują elementy, które świadczą według nich o tym, że jest to próba ataku.

2) Etap II. Uczestnicy szkolenia prezentują na forum grupy swoje odpowiedzi i na tej podstawie prowadzona jest dyskusja na temat ataków cyberprzestępców na świecie.Trener potwierdza odpowiedzi i wskazuje elementy, które Uczestnicy pominęli.

Cel ćwiczenia:

Uczestnicy poznają różne rodzaje ataków, uświadamiają sobie pod jakie instytucje mogą się podszywać cyberprzestępcy i uczą się rozpoznawać elementy, które świadczą o próbie ataku na użytkownika Internetu.

KARTA PRACY DLA UCZESTNIKA SZKOLENIA DO MODUŁU PIERWSZEGO

“Zagrożenia społeczne i fizyczne związane z użytkowaniem komputera , Internetu oraz smartfonów.

Cyberprzemoc i cyberprzestępstwa.

Zasady postępowania w przypadku zetknięcia się z cyberprzestępczością i innymi zagrożeniami.

Typy oszustw w Internecie w tym oszustwa telefoniczne, przez SMS i pocztę elektroniczną.”

Ćwiczenie numer 1

Zagrożenia społeczne nietechniczne - Czy spotkałeś się z przypadkiem nietechnicznego zagrożenia społecznego?

Zastanów się czy spotkałeś się w trakcie korzystania z internetu z przypadkami zagrożeń społecznych nietechnicznych wskazanych przez prowadzącego.

Zapisz przykłady dla wskazanych zagrożeń (jeżeli nie spotkałeś się z nimi to wymyśl własne przykłady):

Cyberstalking:

……
……
……

Trollowanie:

……
……
……
……

Flaming

……
……
……
……
……
……..

Ćwiczenie numer 2

Analiza ataków cyberprzestępców na świecie.

Wejdź na stronę https://threatmap.checkpoint.com/ lub https://cybermap.kaspersky.com/ i na podstawie interaktywnej mapy ataków w czasie rzeczywistym wskaż:

Jakich rodzajów ataków jest najwięcej na świecie?

……
……
……
……..

Które kraje są aktualnie najczęściej atakowane?

……
……
……
……..

Jakie zagrożenia najczęściej są spotykane w Polsce?

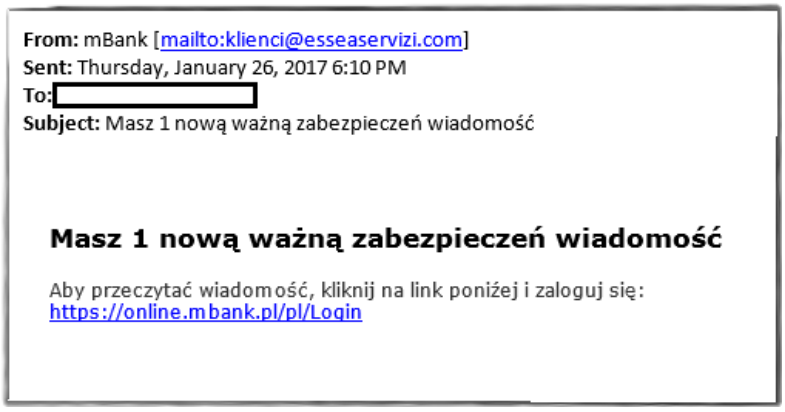
……
……
……
……..

Ćwiczenie numer 3

Jak rozpoznać atak cyberprzestępców

Na podanych poniżej przykładach wskaż co świadczy o tym, że jest to mail z próbą ataku. Zakreśl elementy, które mogą na to wskazywać.

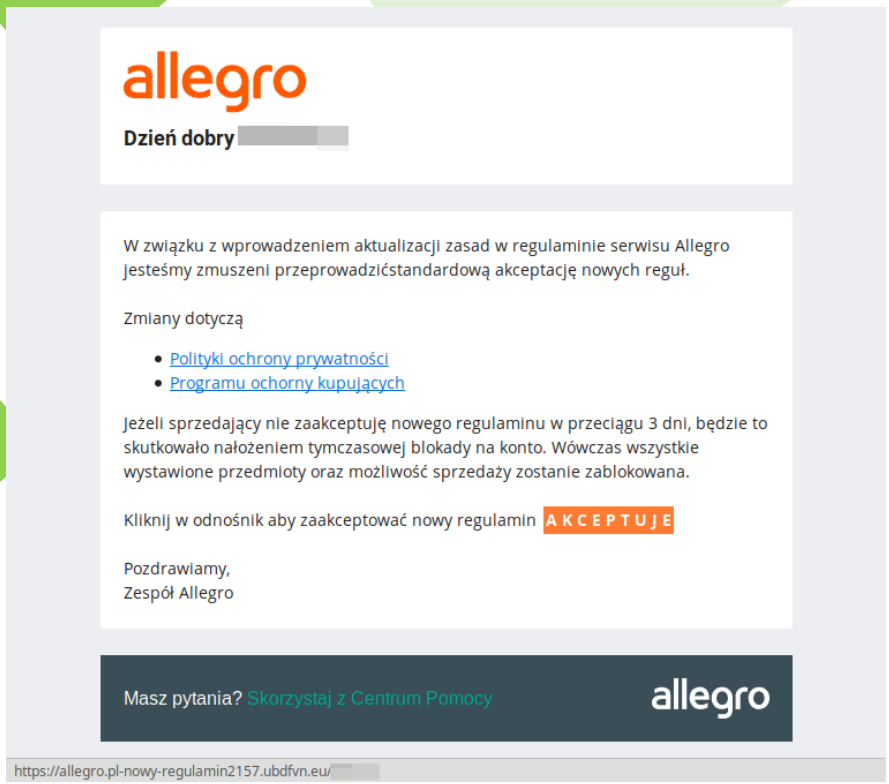
Czy otrzymałeś kiedyś jakiś szkodliwy mail? Podaj przykład innym uczestnikom szkolenia.



From: mBank [mailto:klienci@esseaservizi.com]
Sent: Thursday, January 26, 2017 6:10 PM
To: [redacted]
Subject: Masz 1 nową ważną zabezpieczeń wiadomość

Masz 1 nową ważną zabezpieczeń wiadomość

Aby przeczytać wiadomość, kliknij na link poniżej i zaloguj się:
https://online.mbank.pl/pl/Login



allegro

Dzień dobry [redacted]

W związku z wprowadzeniem aktualizacji zasad w regulaminie serwisu Allegro jesteśmy zmuszeni przeprowadzićstandardową akceptację nowych reguł.

Zmiany dotyczą

- Polityki ochrony prywatności
- Programu ochorny kupujących

Jeżeli sprzedający nie zaakceptuję nowego regulaminu w przeciągu 3 dni, będzie to skutkowało nałożeniem tymczasowej blokady na konto. Wówczas wszystkie wystawione przedmioty oraz możliwość sprzedaży zostanie zablokowana.

Kliknij w odnośnik aby zaakceptować nowy regulamin AKCEPTUJE

Pozdrawiamy,
Zespół Allegro

Masz pytania? Skorzystaj z Centrum Pomocy allegro

https://allegro.pl-nowy-regulamin2157.ubdfvn.eu/[redacted]

--- Treść przekazanej wiadomości ---
Temat: INFORMACJA O ZAMIARZE WSZCZĘCIA KONTROLI SKARBOWEJ
Data: Mon, 25 Feb 2019 04:48:58 +0100
Nadawca: Urząd Skarbowy <arahirufepe1990@o2.pl>
Adresat: [redacted]

Urząd Skarbowy odczytać zawiadomienie o zamiarze zainicjować kontroli w dniu 18.04.2019r. Wobec braku możliwości ustawienia kontaktu telefonicznego w dniach 4-7.04.2019r. i nie zastania podatnika w jego siedzibie w dniu 6.04.2019r. w celu ustalenia terminu wszczęcia kontroli. Urząd Skarbowy wyznacza termin zainicjować kontroli na 29.04.2019r. o godz. 9.00.

Jednoczesnie Urzqd Skarbowy informuje, ze zgodnie z art. 92a ustawy z dnia 13 pazdziernika 1998r. (Dz. U. z 2007 r., Nr 11, poz.74 z p6zn. zm.) w zwiqzku art. 80 ust. 1 ustawy z 2 lipca 2004 r. o swobodzie dziatalnosci gospodarczej (Dz. U. z 2007 r.. Nr 155, poz. 1095 z pozn. zm.) czynnosci kontrolnych dokonuje si$ w obecnosci kontrolowanego lub osoby przez niego upowaznionej. Oznacza to ze w wyzej wymienionym terminie jest Pani/Pan zobowiązana do obecnosci w siedzibie swojej Firmy i wspofpracy z inspektorem kontroli. Ponadto zgodnie z art. 80 ust. 3 ustawy o swobodzie dziatalnosci gospodarczej jest Pani/Pan zobowiązuje do pisemnego wskazania osoby upowaznionej do reprezentowania Pani/Pana w trakcie kontroli, w szczegolnosci w czasie Pani/Pana nieobecnosci.

Jest Pani/Pan zobowiązania do przygotowania wszystkich potrzebnych dokumentow zwiqzanych z prowadzone przez Pani/Pana Firm wymienionych w załączniku(dokumenty.rar).

Nieobecnosc Pani/Pana moze zostac uznana za stan wyczerpuje znamiona wykroczenia okreslonego w art. 98 ust. 1 pkt 3 ustawy z 13 pazdziernika 1998 r. (Dz. U. z 2007 r., Nr 11, poz. 74 z pozn. zm.).

INSPEKTOR KONTROLI
Urząd Skarbowy
mgr Marian Jakubowski

Twój dostep on-line zostala zablokowana

iPKO <noreply@xplornet.com>

Wysłano: Pt 2014-07-18 13:12

Do: undisclosed-recipients:

Twój dostep on-line zostala zablokowana

Dla Twojego bezpieczenstwa, mamy zablokowane konta.

Aby przywrócic dostep do swojego konta, kliknij: Zaloguj sie do iPKO i przystapic do procesu weryfikacji.

MODUŁ 2 - Ochrona przed szkodliwym oprogramowaniem, ochrona przed wirusami, usługi chmurowe

Przebieg warsztatów dla Uczestników szkolenia skierowanego na podniesienie kompetencji z zakresu bezpiecznego korzystania z technologii – moduł drugi

Lp.	Opis sposobu realizacji modułów, zastosowanych narzędzi, metod itd.	Czas/teoria	Pomoce dydaktyczne	Nabywane umiejętności i wiedza (cele działania)
1	Przedstawienie narzędzi antywirusowych zainstalowanych na komputerze.	1h	Prezentacja, Karta pracy, Flipchart, : komputer z systemem Windows, strona internetowa z antywirusem online https://www.virustotal.com/ , usługi chmurowe Google, urządzenie z systemem Android.	Uczestnik dowie się jakie narzędzia zainstalowane lokalnie na komputerze służą do zabezpieczenia .
2	Przedstawienie instalacji i konfiguracji programów antywirusowych zainstalowanych na komputerze. Ćwiczenie numer 1 - 3 z Karty Pracy	2h/1h		Uczestnik nauczy się jak skonfigurować usługę Windows Defender dostępną w systemie Windows 10, jak zainstalować, skonfigurować i

				obsługiwać antywirusa na przykładzie bezpłatnego programu Avast
3	Przedstawienie sposobu pracy z narzędziami antywirusowymi dostępnymi online. Ćwiczenie numer 4 z Karty Pracy	1h/30 min.		Uczestnik pozna możliwości i sposób pracy z narzędziem do skanowania antywirusowego plików i linków na przykładzie Virus Total.
4	Przedstawienie sposobu pracy z innymi narzędziami zapewniającymi bezpieczną pracę w cyberprzestrzeni - sprawdzenia czy adres z którego otrzymaliśmy wiadomość istnieje i czy adres mailowy i inne dane nie wyciekły od dostawców usług w Internecie..	1h/30 min.		Uczestnik pozna narzędzia do sprawdzania czy adres e-mail istnieje i narzędzia do weryfikacji wycieków danych osobowych od dostawców świadczących usługi w internecie oraz sposobu ich wykorzystywania.

	Ćwiczenie numer 5 z Karty Pracy			
5	Przedstawienie metod zabezpieczenia urządzeń mobilnych przed dostępem osób nieupoważnionych. Ćwiczenie numer 6 z Karty Pracy	1h/30min.		Uczestnik pozna sposób zabezpieczenia urządzeń mobilnych przed dostępem osób nieupoważnionych.
6	Przedstawienie narzędzi i sposobów pracy w usługach chmurowych. Ćwiczenie nr 7 z Karty Pracy	30 min./1h		Uczestnik pozna środowisko, narzędzia i sposób pracy w usługach chmurowych na przykładzie narzędzia Google.
	Podsumowanie	6h 30 min./3h 30min		

Opis ćwiczeń do modułu drugiego

Ćwiczenie numer 1

Konfiguracja Windows Defender

Uczestnicy szkolenia zapoznają się z narzędziem Windows Defender i skonfigurują podstawowe parametry.

Trener kontroluje pracę Uczestników i wspiera w trakcie pracy z narzędziem..

Cel ćwiczenia:

- Zrozumienie przez Uczestników czym jest narzędzie Windows Defender i nauczenie się pracy z nim.

Ćwiczenie numer 2

Instalacja programu antywirusowego

Uczestnicy szkolenia uczą się jak wyszukać, pobrać i zainstalować bezpłatne oprogramowanie antywirusowe.

Ćwiczenie składa się z trzech etapów.

1) Etap I. Uczestnicy wyszukują w sieci bezpłatny program antywirusowy Avast.

2) Etap II. Uczestnicy szkolenia pobierają program antywirusowy na komputer.

3) Etap III: Uczestnicy instalują program antywirusowy na komputerze.

Cel ćwiczenia:

Uczestnicy poznają dostępne w sieci bezpłatne oprogramowanie antywirusowe, uczą się je pobierać i instalować.

Ćwiczenie numer 3

Skanowanie programem antywirusowym.

Uczestnicy mają za zadanie zlokalizować i uruchomić zainstalowany na komputerze program antywirusowy, a następnie poznać jego konfigurację, wykorzystać do przeskanowania dowolnego pliku oraz zaktualizować bazę antywirusów.

Ćwiczenie składa się z trzech etapów.

1) Etap I. Uczestnicy lokalizują i uruchamiają program antywirusowy..

2) Etap II. Uczestnicy zapoznają się z funkcjami programu antywirusowego oraz przeprowadzają skan dowolnego pliku znajdującego się na komputerze.

3) Etap III: Uczestnicy sprawdzają aktualność bazy antywirusowej i w razie potrzeb aktualizują jej zawartość.

Cel ćwiczenia:

Uczestnicy zapoznają się z programem antywirusowym, jego konfiguracją i wykorzystaniem do skanowania plików.

Ćwiczenie numer 4

Skanowanie plików lub linków online.

Uczestnicy mają za zadanie wejść na stronę https://www.virustotal.com/gui/home/upload , a nastęnie:

Załączyć i przeskanować plik znajdujący się na komputerze.

Przeskanować dowolny link/adres strony internetowej.

Ćwiczenie składa się z dwóch etapów.

1) Etap I. Uczestnicy skanują plik za pomocą antywirusa dostępnego online.

2) Etap II. Uczestnicy skanują link za pomocą antywirusa dostępnego online.

Cel ćwiczenia:

Uczestnicy uzyskują wiedzę na temat dostępnych darmowych narzędzi online służących do skanowania niezaufanych plików i linków oraz zapoznają się ze sposobem działania skanerów online.

Ćwiczenie numer 5

Weryfikacja istnienia adresu e-mail online.

Uczestnicy mają za zadanie zweryfikować istnienie i prawidłowość adresu e-mail. Do ćwiczeń zostaną wykorzystane bezpłatne narzędzia dostępne online, służące do skanowania adresów e-mail.

Cel ćwiczenia:

Uczestnicy uzyskują wiedzę na temat dostępnych darmowych narzędzi online służących do weryfikacji adresów mailowych oraz zapoznają się ze sposobem ich działania

Ćwiczenie numer 6

Blokada ekranu urządzenia mobilnego.

Uczestnicy mają za zadanie uruchomienie narzędzia służącego do konfiguracji urządzenia mobilnego z systemem Android, następnie znalezienie ustawień służących do blokady ekranu. W ramach ćwiczeń zostaną zaprezentowane cztery metody blokady ekranu: wzorem, PIN-em, odciskiem palca i wizerunkiem twarzy. Każdy uczestnik zdecyduje się, którą z metod wybrać na swoim urządzeniu.

W trakcie ćwiczenia Trener omówi dlaczego należy blokować ekran urządzenia mobilnego oraz sposób pracy z dodatkową kartą pamięci.

Ćwiczenie składa się z dwóch etapów.

1) Etap I. Uczestnicy zapoznają się z menu konfiguracyjnym urządzenia mobilnego.

2) Etap II. Uczestnicy ustawiają blokadę ekranu wybraną przez siebie metodą.

Cel ćwiczenia:

Uczestnicy uzyskują wiedzę na temat menu konfiguracyjnego urządzenia mobilnego oraz sposobów blokady ekranu służącej do zabezpieczenia przed dostępem osób nieupoważnionych.

Ćwiczenie numer 7

Korzystanie z usług chmurowych do wymiany plików.

Uczestnicy szkolenia będą mieli za zadanie zapoznanie się z usługą chmurową oferowaną przez Google.

W trakcie ćwiczenia dowiedzą się jakie narzędzia są dostępne w usłudze, nauczą się tworzenia folderów, plików tekstowych, kalkulacyjnych i prezentacyjnych oraz poznają sposoby udostępniania dokumentów do współpracy z innymi użytkownikami.

Ćwiczenie składa się z czterech etapów.

1) Etap I. Uczestnicy logują się do usługi chmurowej i poznają jej funkcjonalności (Uczestnicy, którzy nie posiadają skrzynki mailowej w usłudze Gmail założą sobie konto dostępowe).

2) Etap II. Uczestnicy utworzą folder w usłudze Google Dysk.

3) Etap III. Uczestnicy stworzą plik tekstowy, kalkulacyjny i prezentacyjny w usłudze Google Dysk.

4) Etap IV. Uczestnicy udostępnią innym użytkownikom folder oraz wybrany plik do współpracy online.

Cel ćwiczenia:

Uczestnicy uzyskują wiedzę na temat pracy z usługami chmurowymi na przykładzie narzędzia Google Dysk. Poznają sposoby tworzenia folderów, plików i ich współdzielenia z innymi użytkownikami.

KARTA PRACY DLA UCZESTNIKA SZKOLENIA DO MODUŁU DRUGIEGO

“Ochrona przed szkodliwym oprogramowaniem, ochrona przed wirusami, usługi chmurowe”.

Ćwiczenie numer 1

Konfiguracja Windows Defender

Aby włączyć lub wyłączyć Zaporę Microsoft Defender:

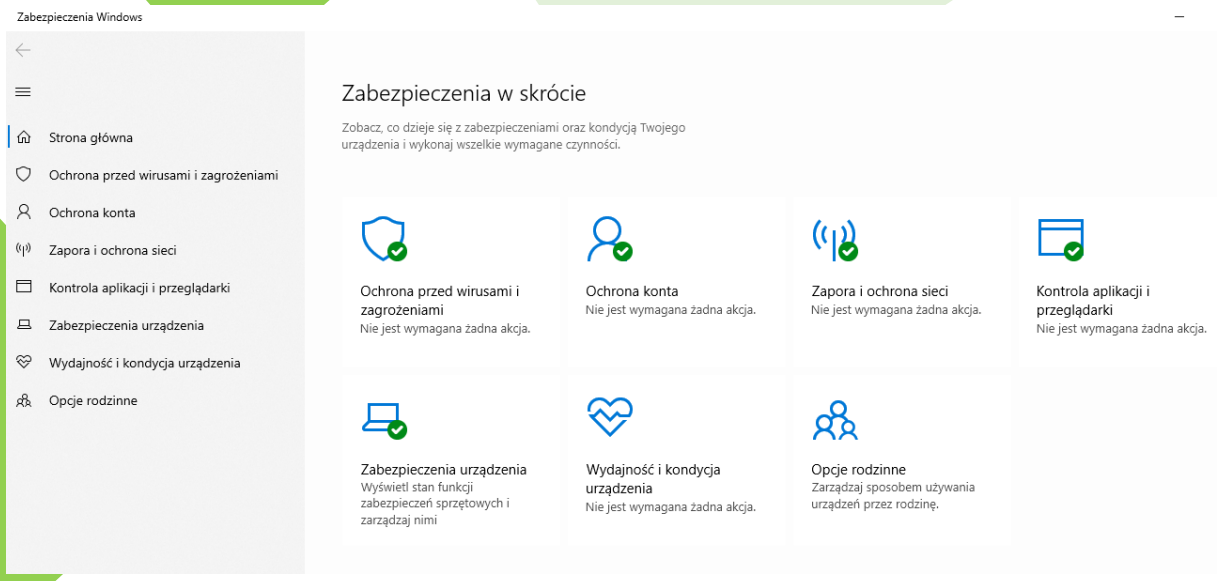
Wybierz przycisk Start > Ustawienia > Aktualizacje i zabezpieczenia > Zabezpieczenia Windows , a następnie Zapora i ochrona sieci. Otwórz ustawienia aplikacji Zabezpieczenia Windows

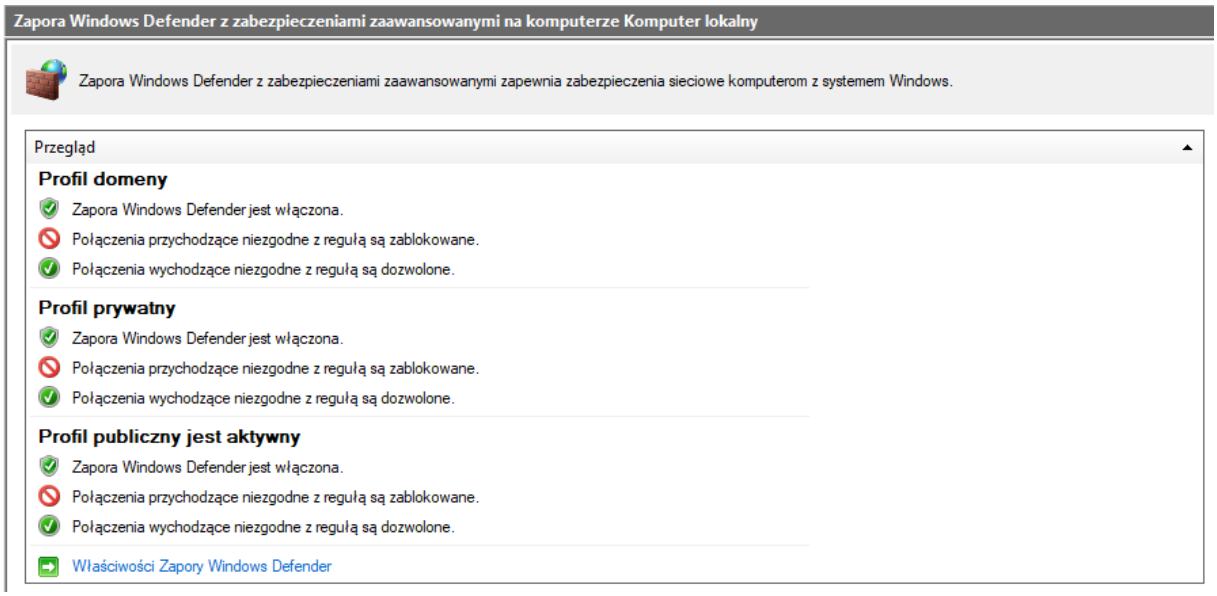
Wybierz profil sieci.

W obszarze Microsoft Defender Zapora przełącz ustawienie do pozycji Włączone. Jeśli urządzenie jest połączone z siecią, ustawienia zasad sieci mogą uniemożliwiać wykonanie tych kroków. Aby uzyskać więcej informacji, skontaktuj się z administratorem.

Aby wyłączyć tę funkcję, przełącz ustawienie do pozycji Wyłączone. Wyłączenie Zapory Microsoft Defender może spowodować, że urządzenie będzie bardziej podatne na zagrożenia związane z nieautoryzowanym dostępem (dotyczy to również sieci, jeśli występuje). Jeśli blokowana jest ważna aplikacja, można umożliwić jej dostęp przez zaporę, zamiast wyłączać całą zaporę.

Poprawnie skonfigurowana Zapora Microsoft Defender:





Ćwiczenie numer 2

Instalacja programu antywirusowego

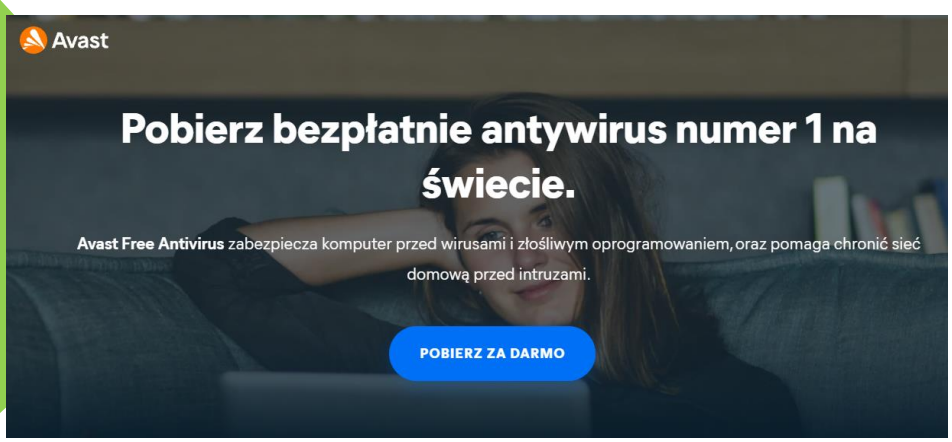
Wpisz w wyszukiwarkę internetową hasło: bezpłatny antywirus.

Znajdź interesujący Cię antywirus.

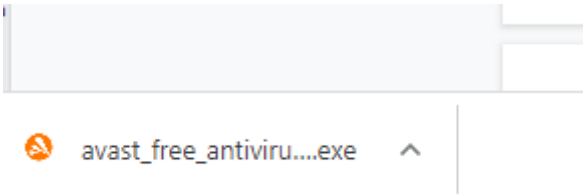
Dla przećwiczenia instalacji wykorzystamy antywirus Avast.

Link do strony instalacyjnej.

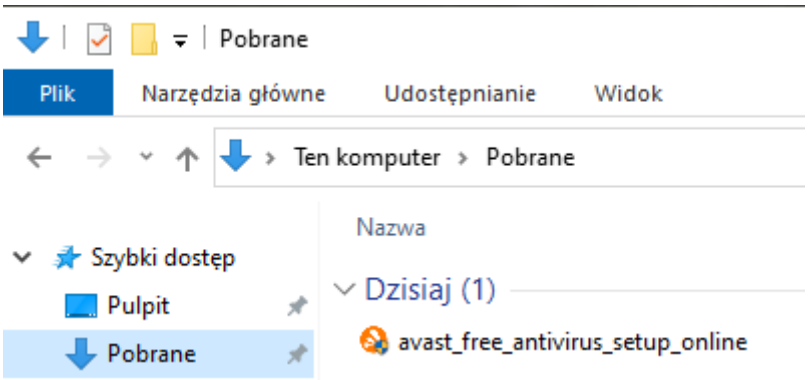
Na stronie producenta kliknij przycisk “POBIERZ ZA DARMO”



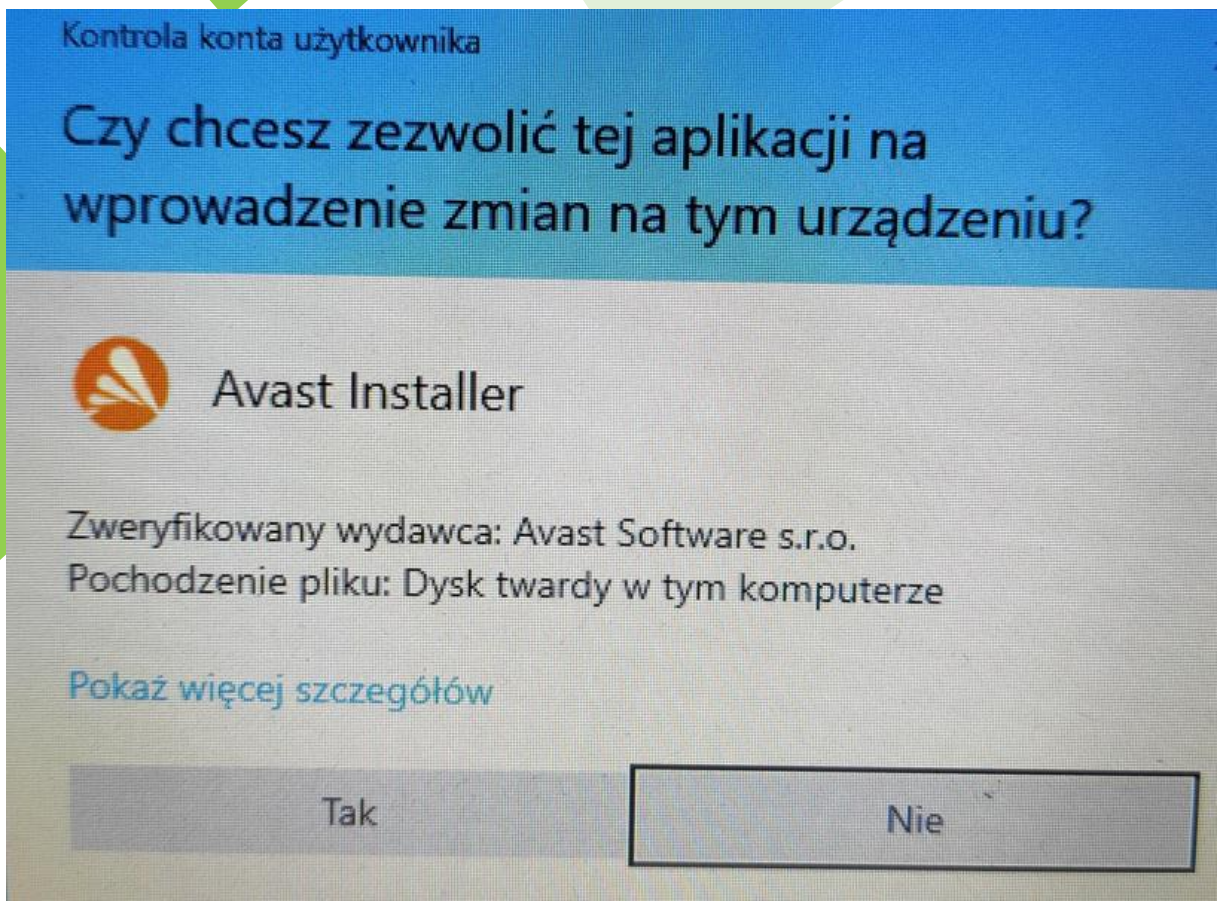
Po kliknięciu przycisku nastąpi automatyczne pobranie pliku instalacyjnego.
Plik instalacyjny możesz znaleźć w dolnym pasku przeglądarki:



lub w folderze “Pobrane”



Po kliknięciu na strzałkę rozwijającą menu z poziomu przeglądarki i wybraniu “Otwórz” lub po kliknięciu na plik w folderze “Pobrane” pojawi się okno instalacji.



Udzielamy zgody na wprowadzanie zmian na urządzeniu klikając “Tak”.

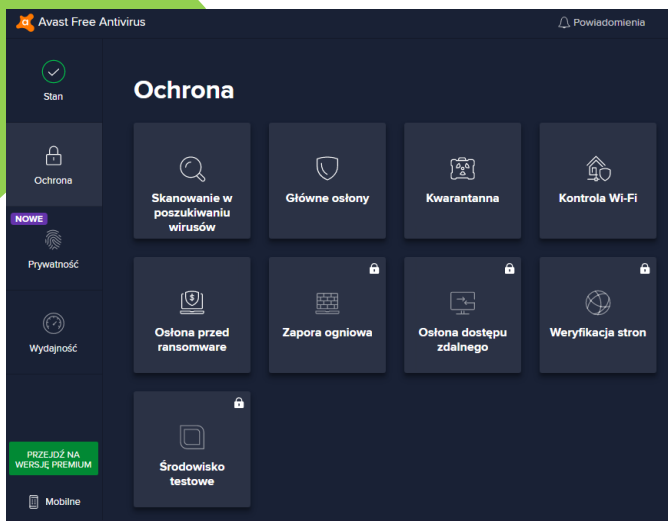
Program zainstaluje się na komputerze i będzie gotowy do użycia.

Ćwiczenie numer 3

Skanowanie programem antywirusowym.

Otwórz program antywirusowy.

Z panelu programu wybierz “Ochrona”, a następnie “Skanowanie w poszukiwaniu wirusów”



Możesz teraz wybrać skanowanie całego komputera, wybranego folderu lub pliku:

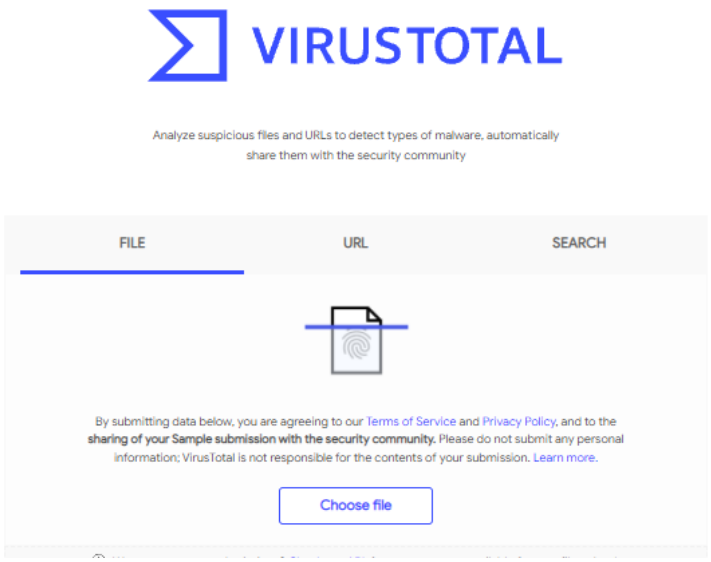
Przeskanuj teraz wybrany plik lub folder klikając na “Skanowanie lokalizacji”.

Ćwiczenie numer 4

Skanowanie plików lub linków online.

Wejdź na stronę: https://www.virustotal.com/gui/home/upload

Na stronie startowej wybierz najpierw skanowanie pliku klikając na przycisk “Choose file”:



Ćwiczenie numer 5

Weryfikacja istnienia adresu e-mail online.

Sprawdzimy jak działa weryfikacja przy użyciu darmowych narzędzi ze stron:

https://pl.infobyip.com/verifyemailaccount.php i https://verifyemail.online/

Ćwiczenie numer 6

Blokada ekranu urządzenia mobilnego.

Proszę o przygotowanie swoich urządzeń, sprawdzimy teraz ustawienia i skonfigurujemy blokadę ekranu w wybrany przez Ciebie sposób.

Ćwiczenie numer 7

Korzystanie z usług chmurowych do wymiany plików.

Ćwiczenia przeprowadzimy na usłudze chmurowej udostępnionej przez Google.

Osoby nie posiadające adresu e-mail w usłudze Google - gmail, proszę o założenia konta.

Pozostałe osoby prosze o zalogowanie się na swoje konto.

Po zalogowaniu:

Sprawdzimy jak wygląda nasz dysk Google i jego zawartość.

Stworzymy folder, w którym będziemy umieszczać pliki z naszego ćwiczenia.

Przygotujemy:

dokument tekstowy

prezentację

arkusz kalkulacyjny

Udostępnimy folder oraz plik wybranym osobom.

MODUŁ 3 - Kontakt i relacje z innymi użytkownikami Internetu dbanie o własny wizerunek w sieci, nieujawnianie wrażliwych informacji. Wiarygodność informacji w Internecie. Prawa autorskie

Przebieg warsztatów dla Uczestników szkolenia skierowanego na podniesienie kompetencji z zakresu bezpiecznego korzystania z technologii – moduł trzeci

Lp.	Opis sposobu realizacji modułów, zastosowanych narzędzi, metod itd.	Czas/teoria	Pomoce dydaktyczne	Nabywane umiejętności i wiedza (cele działania)
1	Przedstawienie sposobów komunikacji w cyberprzestrzeni i narzędzi, które do tego służą. Ćwiczenie numer 1 z Karty Pracy	2h/1 h	Prezentacja, Karta pracy, Flipchart, : komputer z systemem Windows, .	Uczestnik dowie się jak właściwie komunikować się w sieci z wykorzystaniem różnych narzędzi komunikacyjnych, jak zaprezentować własną osobę w sieci.
2	Przedstawienie zasad kulturalnej komunikacji w różnych obszarach sieci na podstawie netykiety.	1,5h/1h		Uczestnik nauczy jak w kulturalny sposób komunikować się w cyberprzestrzeni, w zależności od platformy komunikacyjnej.

	Ćwiczenie numer 2 z Karty Pracy			
3	Przedstawienie informacji na temat bezpieczeństwa danych i ochrony swojej prywatności w cyberprzestrzeni. Ćwiczenie numer 3 z Karty Pracy	1h/30 min		Uczestnik zapozna się informacjami na temat bezpieczeństwa danych i prywatności w sieci.Pozna prawo gwarantujące ochronę danych w cyberprzestrzeni. Zapozna się ze sposobami zabezpieczania swoich danych i poufności w cyberprzestrzeni.
4	Przedstawienie problemu wiarygodność informacji w sieci, występowania zjawiska fake newsów oraz sposobów weryfikowania prawdziwości informacji. Ćwiczenie numer 4 z Karty Pracy	1h/30 min.		Uczestnik zapozna się ze zjawiskiem fake newsów. Pozna sposoby rozpoznawania fałszywych informacji i weryfikacji ich prawdziwości.
5	Przedstawienie prawa autorskiego i wynikającego z	1 h/30 min.		Uczestnik zapozna się z prawem autorskim, ochroną twórczości i właściwym

	niego ochrony twórczości. Ćwiczenie numer 5 z Karty Pracy			wykorzystaniem utworów dostępnych w cyberprzestrzeni.
	Podsumowanie	6h 30 min. /3h 30 min.		

Opis ćwiczeń do modułu trzeciego

Ćwiczenie numer 1

Znajdź siebie w internecie

Uczestnicy szkolenia weryfikują w sieci informacje na swój temat. Ćwiczenie polega na sprawdzeniu w wyszukiwarkach internetowych informacji umieszczonych na temat Uczestnika. Uczestnik sprawdza informacje na podstawie danych tekstowych i wyszukiwania zdjęciem z wizerunkiem użytkownika.

Ćwiczenie składa się z dwóch etapów.

1) Etap I. Uczestnicy wyszukują w sieci informacje na swój temat

2) Etap II. Dyskusja na tema znalezionych informacji w sieci i śladzie cyfrowym.

Cel ćwiczenia:

Zrozumienie przez Uczestników, że w cyberprzestrzeni nie jest się anonimowym, że po każdym działaniu zostaje ślad cyfrowy, który może mieć wpływ na nasze przyszłe życie..

Ćwiczenie numer 2

Poprawna komunikacja z użytkownikami

Uczestnicy szkolenia początkowo indywidualnie zapoznają się z przykładami komunikatów pisanych do różnych odbiorców. Zadaniem jest przeanalizowanie treści, wskazanie niepoprawnych form i tekstów oraz zaproponowanie poprawnych sformułowań.

Następnie wyniki ćwiczenia prezentowane są w grupie i omawiane z Trenerem.

Ćwiczenie składa się z trzech etapów.

1) Etap I. Uczestnicy zapoznają się z treścią przykładowych komunikatów i zaznaczają niewłaściwą formę zastosowaną w nich zastosowaną..

2) Etap II. Uczestnicy szkolenia proponują poprawne wersje komunikatów.

3) Etap III: Uczestnicy wspólnie z trenerem omawiają wyniki i dyskutują nad sposobem właściwego tworzenia komunikatów do różnych odbiorców..

Cel ćwiczenia:

Uczestnicy poznają właściwy sposób komunikacji w Internecie, stosowanie odpowiednich form, słownictwa i tworzenia kont służących do komunikowania się z innymi użytkownikami sieci..

Ćwiczenie numer 3

Jakie dane możemy przekazywać różnym podmiotom świadczącym usługi w cyberprzestrzeni.

Uczestnicy szkolenia pracują najpierw indywidualnie, potem prezentują swoje wyniki na forum wszystkich uczestników.

Zadaniem Uczestników jest przeanalizowanie jaki zakres danych jest wymagany przy kontaktach z różnymi dostawcami usług w sieci i zaznaczenie przy wskazanych przykładach, które dane można w takim przypadku przekazać.

Ćwiczenie składa się z dwóch etapów.

1) Etap I. Uczestnicy analizują wskazany w przykładach zakres danych i zaznaczają właściwe dane, które można bezpiecznie przekazać podmiotom.

2) Etap II. Uczestnicy dyskutują na forum z jakimi przypadkami przekazywania danych do dostawców mieli do czynienia.

Cel ćwiczenia:

Uczestnicy zdobywają wiedzę na temat bezpiecznego przekazywania swoich danych, ograniczonego zaufania do odbiorców oraz dobierania odpowiedniego zakresu danych w zależności od rodzaju świadczonej w sieci usługi..

Ćwiczenie numer 4

Sprawdź wiarygodność informacji

Uczestnicy początkowo pracują indywidualnie, następnie wyniki przedstawiane są na forum grupy. Uczestnik ma za zadanie zapoznać się z treścią komunikatu i na podstawie przedstawionych przez Trenera sposobów weryfikacji prawdziwości informacji wskazać, które z nich są prawdziwe, a które nie i jakie elementy na to wskazują.

Trener proponuje Uczestnikom wskazanie przykładów fałszywych informacji, z którymi zetknęli się w trakcie korzystania z sieci.

Ćwiczenie składa się z dwóch etapów.

1) Etap I. Uczestnicy analizują przykłady i wskazują elementy, które mogą świadczyć o tym, że informacja jest prawdziwa lub fałszywa..

2) Etap II. Uczestnicy omawiają wspólnie wyniki i prezentują przykłady fałszywych informacji, z którymi zetknęli się w sieci.

Cel ćwiczenia:

Uczestnicy zapoznają się ze zjawiskiem fałszywej informacji i wynikającej z niej zagrożeń dla życia społecznego i osobistego. Poznają metody rozpoznawania prawdziwości informacji.

Ćwiczenie numer 5

Zgodność działań z prawem autorskim

Uczestnicy na początku indywidualnie wskazują poprawne odpowiedzi w opisanych na karcie przykładach. Następnie wyniki omawiane są na forum grupy.

Cel ćwiczenia:

Uczestnicy uzyskują podstawową wiedzę na temat prawa autorskiego i jego stosowania w cyberprzestrzeni.

Ćwiczenie numer 6

Blokada ekranu urządzenia mobilnego.

Uczestnicy mają za zadanie uruchomienie narzędzia służącego do konfiguracji urządzenia mobilnego z systemem Android, następnie znalezienie ustawień służących do blokady ekranu. W ramach ćwiczeń zostaną zaprezentowane cztery metody blokady ekranu: wzorem, PIN-em, odciskiem palca i wizerunkiem twarzy. Każdy uczestnik zdecyduje się, którą z metod wybrać na swoim urządzeniu.

W trakcie ćwiczenia Trener omówi dlaczego należy blokować ekran urządzenia mobilnego oraz sposób pracy z dodatkową kartą pamięci.

Ćwiczenie składa się z dwóch etapów.

1) Etap I. Uczestnicy zapoznają się z menu konfiguracyjnym urządzenia mobilnego.

2) Etap II. Uczestnicy ustawiają blokadę ekranu wybraną przez siebie metodą.

Cel ćwiczenia:

Uczestnicy uzyskują wiedzę na temat menu konfiguracyjnego urządzenia mobilnego oraz sposobów blokady ekranu służącej do zabezpieczenia przed dostępem osób nieupoważnionych.

Ćwiczenie numer 7

Korzystanie z usług chmurowych do wymiany plików.

Uczestnicy szkolenia będą mieli za zadanie zapoznanie się z usługą chmurową oferowaną przez Google.

W trakcie ćwiczenia dowiedzą się jakie narzędzia są dostępne w usłudze, nauczą się tworzenia folderów, plików tekstowych, kalkulacyjnych i prezentacyjnych oraz poznają sposoby udostępniania dokumentów do współpracy z innymi użytkownikami.

Ćwiczenie składa się z czterech etapów.

1) Etap I. Uczestnicy logują się do usługi chmurowej i poznają jej funkcjonalności (Uczestnicy, którzy nie posiadają skrzynki mailowej w usłudze Gmail założą sobie konto dostępowe).

2) Etap II. Uczestnicy utworzą folder w usłudze Google Dysk.

3) Etap III. Uczestnicy stworzą plik tekstowy, kalkulacyjny i prezentacyjny w usłudze Google Dysk.

4) Etap IV. Uczestnicy udostępnią innym użytkownikom folder oraz wybrany plik do współpracy online.

Cel ćwiczenia:

Uczestnicy uzyskują wiedzę na temat pracy z usługami chmurowymi na przykładzie narzędzia Google Dysk. Poznają sposoby tworzenia folderów, plików i ich współdzielenia z innymi użytkownikami.

KARTA PRACY DLA UCZESTNIKA SZKOLENIA DO MODUŁU TRZECIEGO

“Kontakt i relacje z innymi użytkownikami Internetu dbanie o własny wizerunek w sieci, nieujawnianie wrażliwych informacji. Wiarygodność informacji w Internecie. Prawa autorskie.”

Ćwiczenie numer 1

Znajdź siebie w internecie

Sprawdź jakie informacje znajdują się na Twój temat w sieci.

Wpisz swoje dane - imię i nazwisko - w wyszukiwarce Google i zobacz wyniki.

Czy pojawiły się Twoje profile publiczne, obrazy i wszelkie inne treści powiązane z Twoim imieniem i nazwiskiem online? Wyszukiwanie możesz ograniczyć uzupełniając innymi danymi - miastem, wiekiem, wykonywanym zawodem.

Możesz również sprawdzić wyniki wyszukiwania wykorzystując zdjęcie ze swoją podobizną.

Jakie informacje o Tobie są dostępne w sieci?

Pamiętaj, że jeżeli pojawiły się, które Ci się nie podobają, możesz podjąć niezbędne kroki, aby je usunąć, a jeśli pojawi się którykolwiek z Twoich profili w mediach społecznościowych, możesz zmienić ich ustawienia prywatności.

Ćwiczenie numer 2

Poprawna komunikacja z użytkownikami

Przeczytaj poniższe wiadomości skierowane do różnych odbiorców wskazanych w opisie. Zastanów się czy są poprawnie sformułowane, wskaż nieprawidłowe zwroty i zaproponuj poprawną formę (skreśl te, które są według Ciebie niepoprawne i napisz obok jakie Twoim zdaniem powinny być).

1. Wiadomość e-mail do Dyrektora firmy, z którą chcemy nawiązać współpracę

Witam,

chciałbym się spotkać i przedstawić moją propozycję współpracy. wydaje mi się, że powinno to być interesujące dla ciebie.

Daj znać jaki termin będzie najlepszy.

Pozdrawiam cieplutko

Sławek

2. Wiadomość e-mail wysłana przez kandydata do przyszłego pracodawcy:

Nadawca wiadomości: prociaczek@kombi.pl

Odbiorca wiadomości: rekrutacja@hotel.pl

Temat: Rekrutacja na stanowisko recepcjonisty

Treść:

Dzien Dobry :) ,

odpowiadam na państwa gloszenie bo wydaje mi sie, ze jestem idealnym kandydatem.

W załączniku moje CV, prosze o kontak mailowy na: prociaczek@kombi.pl

Pozdrawiam i mam nadzieję do rychłego zobaczenia. :)

Adam Waleczny

Ćwiczenie numer 3

Jakie dane możemy przekazywać różnym podmiotom świadczącym usługi w cyberprzestrzeni.

Wskaż które dane możesz bezpiecznie podać w trakcie rejestracji do wskazanych poniżej usług.

Pamiętaj o zasadzie minimalizowania zakresu danych obowiązującej zgodnie z Rozporządzeniem o ochronie danych osobowych (RODO).

1. Forum internetowe fanów motoryzacji:

☐ Imię

☐ Numer i seria dowodu osobistego

☐ Adres e-mail

☐ Adres zamieszkania

☐ Informacje o nałogach

2. Sklep internetowy:

☐ Imię i nazwisko

☐ PESEL

☐ Adres e-mail

☐ Adres do wysyłki zamówienia

☐ Dane karty kredytowej

3. Założenie konta bankowego

☐ Imię i nazwisko,

☐ Nazwisko panieńskie matki,

☐ Miejscowość i kraj urodzenia,

☐ Obywatelstwo,

☐ PESEL,

☐ Seria i numer dowodu osobistego/ paszportu,

☐ Numer telefonu,

☐ e-mail,

☐ Aktualny adres zamieszkania oraz adres korespondencyjny,

☐ Stan zdrowia

Czy przekazywałeś kiedyś swoje dane dostawcom usług w Internecie?

Jeżeli tak podaj jacy to byli dostawcy i jakie dane im przekazałeś.

Ćwiczenie numer 4

Sprawdź wiarygodność informacji

Poniżej znajduje się fragment informacji z sieci.

Ustal czy jest ona wiarygodna stosując poznane zasady.

Przykład 1

“W pewnym czasopiśmie znalazłem takie oto podziękowanie skierowane pod adresem zasłużonego aktora: „Dziękujemy za wszystkie role, którymi nas Pan uraczył, uracza i uraczać będzie”. Przeczytałem je i... aż mnie skręciło! A mój komputer od razu podkreślił na czerwono formy „uracza” i „uraczać będzie”. Dlaczego są one nie do przyjęcia?”

Autor: prof. Jan Miodek

Źródło:https://naszahistoria.pl/uraczyl-raczy-i-raczyc-bedzie-felieton-prof-jana-miodka/ar/10679446

Przykład 2

“Ostatnio przeprowadzone badania udowodniły, że sprzedawane w sklepach owoce cytrusowe zawierają szkodliwą substancję duosodekpotasu, która jest silnie uzależniającą. Ten sam składnik może być wytwarzany przez mózg w trakcie korzystania ze specjalnych aplikacji, które skłaniają klientów do impulsywnych zakupów w sieci produktów alkoholowych i tytoniowych. W celu ochrony przed tym zjawiskiem należy przestać kupować owoce cytrusowe zastępując je owocami z polskich sadów.:

Autor: Dr n. med. Andrzej Kapstrzyn

Źródło: www.naszezdrowiewdzisejszychczasach.pl

Napisz które elementy świadczą o tym, że informacja jest fałszywa.

Czy w czasie korzystania z sieci natknąłeś się na jakieś przypadki fałszywych informacji?

Jeżeli tak przedstaw ich przykłady.

Ćwiczenie numer 5

Zgodność działań z prawem autorskim

Wskaż, które z poniższych przykładów są lub nie są łamaniem praw autorskich:

1. Wykorzystania cudzego utworu we własnej pracy bez wskazania twórcy cytatu czy też jego źródła.

a) zgodne z prawem autorskim
b) niezgodne z prawem autorskim

2. Ściągnięcie muzyki, filmu, e-booka z sieci na własny użytek:

a) zgodne z prawem autorskim
b) niezgodne z prawem autorskim

3. Wymiana plików przez protokół peer to peer (P2P, np. BitTorrent), która polega na ściąganiu danego pliku i jednocześnie udostępnianiu go innym użytkownikom

a) zgodne z prawem autorskim
b) niezgodne z prawem autorskim

4. Sprzedaż skopiowanego oprogramowania:

a) zgodne z prawem autorskim
b) niezgodne z prawem autorskim

5. Wykorzystanie bez zgody wizerunku osoby, która otrzymała zapłatę osobie za pozowanie.

a) zgodne z prawem autorskim
b) niezgodne z prawem autorskim

6. Wykorzystanie bez zgody wizerunku osoby powszechnie znanej w sytuacji kiedy została uwieczniona w momencie pełnienia przez nią funkcji publicznych.

a) zgodne z prawem autorskim
b) niezgodne z prawem autorskim.

MODUŁ 4 - Bezpieczeństwo finansów prywatnych i w miejscu pracy, bezpieczna bankowości internetowa oraz bezpieczne zakupy

Przebieg warsztatów dla Uczestników szkolenia skierowanego na podniesienie kompetencji z zakresu bezpiecznego korzystania z technologii – moduł czwarty

Lp.	Opis sposobu realizacji modułów, zastosowanych narzędzi, metod itd.	Czas/teoria	Pomoce dydaktyczne	Nabywane umiejętności i wiedza (cele działania)
1	Przedstawienie zagrożeń dla bankowości elektronicznej.	1 h	Prezentacja, Karta pracy, Flipchart, komputer z systemem Windows, urządzenie z systemem Android	Uczestnik dowie się jakie zagrożenia dla bankowości elektronicznej może spotkać w trakcie pracy w cyberprzestrzeni.
2	Przedstawienie sposobów ochrony przed zagrożeniami dla bankowości elektronicznej.. Ćwiczenie numer 1 z Karty Pracy .	1h/1h		Uczestnik dowie się również jak chronić się przed zagrożeniami dla bankowości elektronicznej i rozpoznawać próby ataków.

3	Przedstawienie informacji na bezpieczeństwa zakupów w Internecie oraz sposobów bezpiecznego korzystania ze sklepów internetowych. Ćwiczenie numer 2 z Karty Pracy	1h/30 min		Uczestnik zapozna się aktywnością cyberprzestępców specjalizujących się w handlu internetowym. Uczestnik pozna zjawisko fałszywych sklepów i nauczy się jak je rozpoznawać.
4	Przedstawienie informacji na temat zagrożeń korzystania ze sklepów dostępnych w urządzeniach mobilnych. Ćwiczenie numer 4 z Karty Pracy	1h/30 min.		Uczestnik zapozna się ze sposobami działania cyberprzestępców w aplikacjach mobilnych oraz przykładami ataków. Pozna zjawisko fałszywych aplikacji i nauczy się je rozpoznawać.
5	Przedstawienie bezpiecznego wykonywania płatności w sklepach internetowych.	30 min.		Uczestnik zapozna się ze sposobami bezpiecznych płatności w internecie,
	Podsumowanie	4h 30 min. /2h		

Opis ćwiczeń do modułu czwartego

Ćwiczenie numer 1

Rozpoznawanie fałszywych wiadomości

Uczestnicy szkolenia otrzymują przykłady prób ataków za pośrednictwem korespondencji elektronicznej.

Zadaniem Uczestnika jest analiza przykładów, a następnie wskazanie elementów, które świadczą o próbie ataku.

Cel ćwiczenia:

Zapoznanie uczestnika ze sposobem rozpoznawania zagrożeń w codziennej korespondencji elektronicznej. Dzięki poznaniu metody analizy wiadomości będzie bardziej świadomym i bezpiecznym użytkownikiem cyberprzestrzeni.

Ćwiczenie numer 2

Sprawdzanie wiarygodności sklepu internetowego

Uczestnicy szkolenia zapoznają się indywidualnie z przykładami fałszywych stron internetowych. Zadaniem Uczestnika jest przeanalizowanie przykładów i wskazanie elementów, które świadczą o tym, że sklep jest fałszywy.

Uczestnik ma zastanowić się czy spotkał się z tego typami witryn internetowych i jakie reakcje w nim wywołały..

Cel ćwiczenia:

Uczestnik zostanie zapoznany ze sposobem rozpoznawania fałszywych stron internetowych. Dzięki poznaniu mechanizmów wykorzystanych przez cyberprzestępców staje się świadomym i bezpiecznym użytkownikiem cyberprzestrzeni.

Ćwiczenie numer 3

Sprawdzanie wiarygodności aplikacji w sklepie Google Play

Zadaniem uczestnika jest wskazanie na podstawie cech wiarygodności aplikacji, która z wyświetlonej listy popularnych aplikacji jest prawdziwa. Uczestnik uruchamia sklep Google Play, następnie wyszukuje komunikator Whatsapp i spośród wyświetlonych aplikacji ma wskazać prawdziwą. Ćwiczenie można zrealizować na urządzeniach z Androidem lub w przeglądarce komputerowej.

Cel ćwiczenia:

Uczestnicy zdobywają wiedzę na temat bezpiecznego korzystania ze sklepów dostępnych na urządzeniach mobilnych. Dzięki poznaniu cech wiarygodności aplikacji, mogą rozpoznać prawdziwe i fałszywe aplikacje dostępne w sklepach urządzeń mobilnych i świadomie z nich korzystać.

KARTA PRACY DLA UCZESTNIKA SZKOLENIA DO MODUŁU CZWARTEGO

“Bezpieczeństwo finansów prywatnych i w miejscu pracy, bezpieczna bankowości internetowa oraz bezpieczne zakupy”

Ćwiczenie numer 1

Rozpoznawanie fałszywych wiadomości

Zapoznaj się z poniższymi przykładami wiadomości i wskaż elementy, które świadczą o próbie wyłudzenia danych lub środków finansowych.

1.

OD: „Bank Polski” tomaszek@poczta.eu
Data: 30 maja 2021 12:35
DO: adreszbiorczy@gmail.com
Temat: Autoryzacja konta Bank Polski
Treść: Szanowni Państwo, Informujemy, że dostęp do konta w Banku Polskim został zablokowany!

W trosce o bezpieczeństwo klientów banku zablokowaliśmy konto w systemie BP24 internet.
Powodem blokady jest nieautoryzowany dostęp do konta. W celu odzyskania dostępu prosimy o weryfikację danych właściciela rachunku poprzez zalogowanie się na:

http://centrum-BP.email?:bank@skrzynka.com

Serdecznie pozdrawiamy, Zespół Banku Polskiego

W przypadku pytań prosimy o kontakt z naszą infolinią 345983043
Ten e-mail został wygenerowany automatycznie.
Prosimy na niego nie odpowiadać.

Bank Polski S.A z siedzibą w Poznaniu ul. Klonowa 5/6 00–999 Poznań, zarejestrowany w Sądzie Rejonowym dla Poznania pod numerem KRS 0987000025 REGON 090654372 NIP 098064327, kapitał zakładowy i wpłacony 987.457.260 zł.

2.

Od: "Orange" info@triumf.com.pl
Data: 14.02.2021
Do: yeti@trespolis.by
Temat: Zmienić rachunku banku
Treść:

Szanowny,

rachunek do plantosci za Twoje uslugi zostal zmieniony.

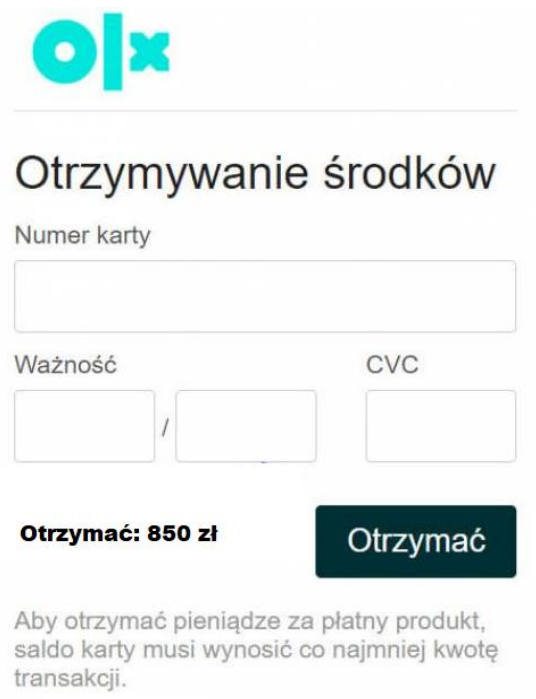
Prosze przelej pieniadze na nowy rachunek banku:

27 1140 2004 0000 3002 0135 5387

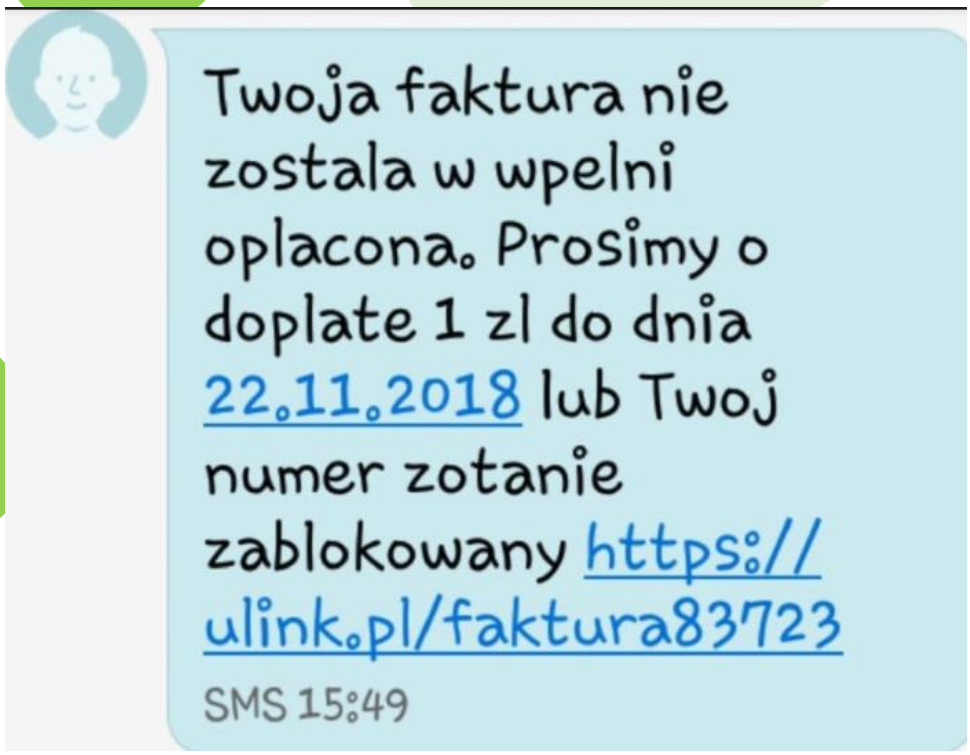
Pozdrawiamy,
Zespol Orange

Wiadomosc wygenerowana automatycznie

3.



4.



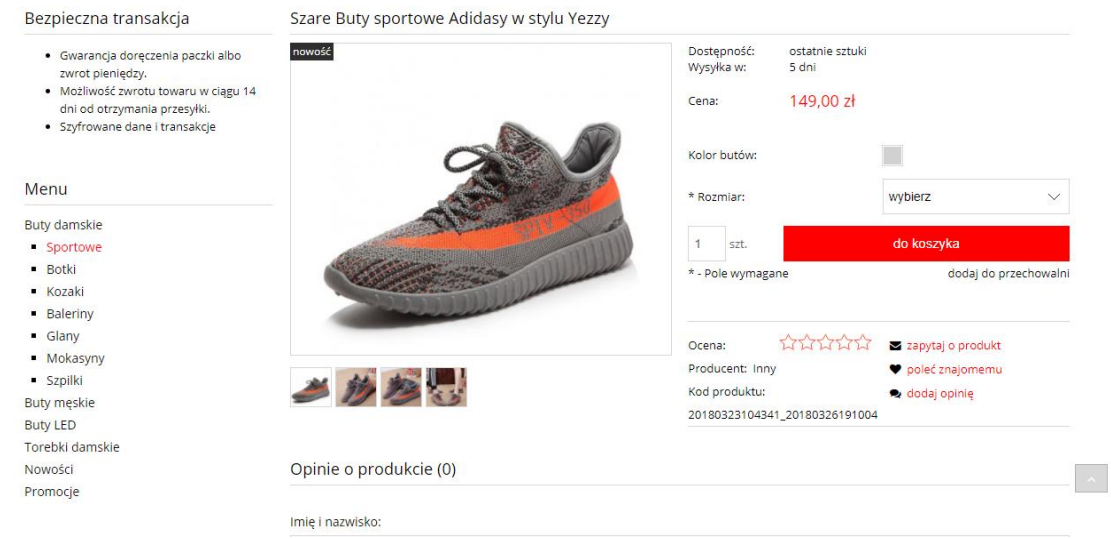
5.

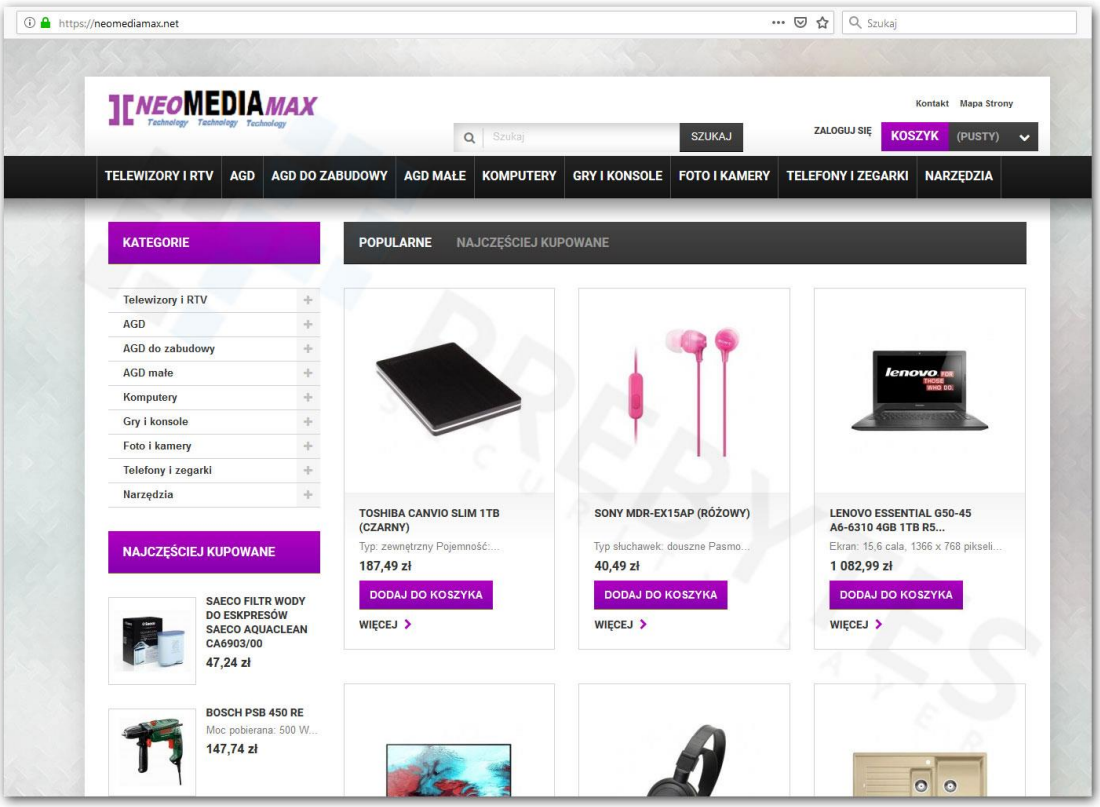
Ćwiczenie numer 2

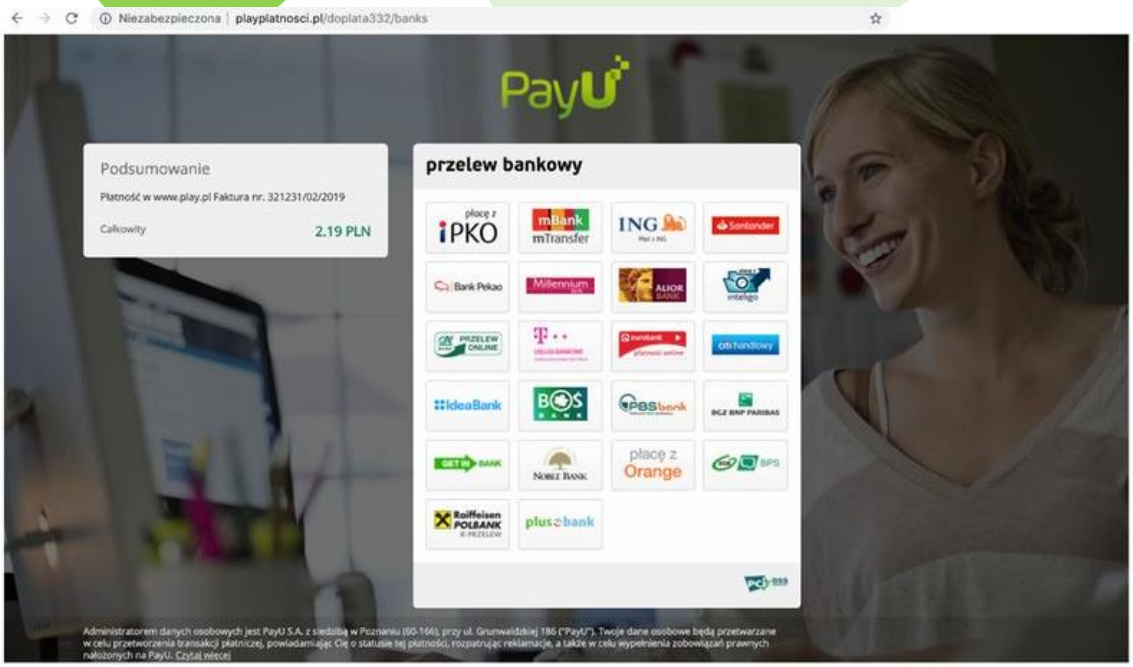
Sprawdzanie wiarygodności sklepu internetowego

Przyjrzyj się poniższym przykładom sklepów internetowych.

Wskaż co może świadczyć o tym, że są to fałszywe sklepy.







Czy w trakcie korzystania z Internetu trafiłeś na fałszywe sklepy?

Czy wzbudziły Twoje zainteresowanie i chciałeś skorzystać z ich oferty?

Ćwiczenie numer 3

Sprawdzanie wiarygodności aplikacji w sklepie Google Play

Wyszukaj w sklepie Google Play aplikację Whatsapp.

Sprawdź, która aplikacja jest prawdziwa.

Wskaż elementy, które sprawdzisz weryfikując prawdziwość aplikacji.

Czy trafiłeś kiedyś na fałszywą aplikację?

Czy pamiętasz jak się nazywała?

Kompendium dla osób bezrobotnych w formie Q&A (Pytań i odpowiedzi) dotyczące umiejętności korzystania z Internetu w sposób płynny w procesie podniesienia efektywności, jakości i atrakcyjności kształcenia swojej pozycji na rynku pracy, jego zadań, praktycznych porad w zakresie zdobytej wiedzy.

1. Co to znaczy zrobić aktualizację (ang. update) komputera lub programu?

Firmy produkujące urządzenia komputerowe i oprogramowanie często aktualizują swoje produkty w celu poprawy ochrony przed najnowszymi zagrożeniami tworzonymi przez cyberprzestępców. Aktualizacje wymagają czasem ponownego uruchomienia komputera dlatego zaplanuj je w odpowiednim momencie, żeby nie przerwać swojej pracy.

2. Co to znaczy silne hasło?

Silne hasło zawiera co najmniej 8 znakowy, przypadkowy ciąg dużych i małych liter, cyfr i symboli. Nie powinien zawierać danych osobistych jak data urodzenia, adres zamieszkania, imiona dzieci, imiona zwierząt, itp.

3. Jak bezpiecznie korzystać z publicznych sieci bezprzewodowych (Wi -fi)?

Większość urządzeń mobilnych - laptopy, smartfony - mają możliwość podłączenia się do sieci bezprzewodowych, które są dostępne w miejscach publicznych jak na przykład kawiarnie, centra handlowe, rynki miejskie, biblioteki, dworce, hotele. Najlepszym rozwiązaniem jest unikanie korzystania z takich sieci. Poza własną, domową siecią najlepiej w celach prywatnych wykorzystywać transfer dostępny w abonamencie,

Korzystając z sieci publicznej unikaj:

- logowania się na portale, z których korzystasz w sieci,
- wprowadzania numerów kart kredytowych, danych do logowania do banku, haseł.
- Używaj połączenia VPN.
- Loguj się wyłącznie na strony zabezpieczone certyfikatem bezpieczeństwa - adresy rozpoczynające się od https (s od ang. secure - bezpieczne). Pamiętaj jednak, że wyłącznie poprawnie wprowadzony adres daje gwarancję korzystania z właściwej strony. Certyfikat bezpieczeństwa może być również wykorzystany przez przestępców przy tworzeniu fałszywych stron.

4. Czy wysyłanie wrażliwych informacji w wiadomościach e-mail lub w komunikatorach jest bezpieczne?

Nie, nie powinno się wysyłać wrażliwych i poufnych informacji w wiadomościach e-mail i przez komunikatory. Nie przekazuj tą drogą danych kart płatniczych, haseł do logowania.

5. Czy mogę wykorzystywać kartę debetową w sklepach online?

Możesz, ale bezpieczniej jest płacić kartą kredytową lub kartą zasilaną środkami niezależną od rachunku bankowego.

Karty kredytowe mają ustalone limity płatności i opcję chargeback (procedura reklamacyjna inicjowana przez bank po otrzymaniu zgłoszenia od klienta

korzystającego z karty płatniczej. Pozwala na dochodzenie w jego imieniu roszczeń wobec podmiotu, który nie wywiązał się należycie (w całości lub w części) z realizacji operacji opłaconej przez posiadacza karty. Czas na zgłoszenie reklamacji w ramach procedury na ogół wynosi 120 dni od daty realizacji transakcji bezgotówkowej.

6. Otrzymałem wiadomość e-mail z załącznikiem od osoby, której nie znam. Co powinienem zrobić?

Bądź ostrożny przy otwieraniu załączników e-mai - plik, który otrzymujesz może zawierać wirusy, programy szpiegujące lub nieodpowiednią zawartość.
Tak samo bądź ostrożny odwiedzając nieznane Ci strony, pobierając oprogramowanie, korzystając z platform udostępniania i pobierania muzyki, filmów, gier, programów z nieznanymi Ci użytkownikami. Pamiętaj, że udostępnianie plików łamie prawo autorskie.

7. Jak mogę rozpoznać czy wiadomość jest fałszywa?

Weryfikację wiarygodności informacji uzyskasz dzięki następującym działaniom:

- sprawdź autora opublikowanej informacji, czy jest to osoba godna zaufania, ekspert w swojej dziedzinie,
- sprawdź datę publikacji i czas działania określonego serwisu internetowego,
- sprawdź poprawności informacji, czy nie zawiera błędów językowych,
- przeczytaj całą treść, a nie tylko nagłówek,
- sprawdź inne źródła czy potwierdzają tę informację,
- porozmawiaj z osobami, którym temat jest znany i mają wiedzę na ten temat,
- zastanów się czy opublikowana informacja nie jest żartem.

Unikaj rozpowszechniania niesprawdzonych informacji, żeby nie wzmacniać jej wiarygodności i nie spowodować paniki wśród bliskich Ci osób.

8. Czy moje dane mogą być przetwarzane bez mojej zgody?

Przetwarzanie Twoich danych osobowych jest możliwe:

- gdy przedsiębiorstwo lub organizacja zawarły z Tobą umowę – np. na dostawę towaru lub świadczenie usług (tj. gdy robisz zakupy przez internet) lub umowę o pracę
- gdy wypełniają one swoje zobowiązania prawne – na przykład jeżeli prawo wymaga przetwarzania Twoich danych, kiedy Twój pracodawca przekazuje informacje na temat Twojego miesięcznego wynagrodzenia do zakładu ubezpieczeń społecznych, aby zapewnić Ci ubezpieczenie społeczne
- gdy przetwarzanie danych leży w Twoim żywotnym interesie – np. może chronić Twoje życie
- w celu wykonania zadania w interesie publicznym – przede wszystkim w związku z realizacją zadań organów administracji publicznej takich jak szkoły, szpitale czy urzędy gminy
- jeżeli istnieje uzasadniony interes – np. jeżeli bank wykorzystuje Twoje dane osobowe, żeby sprawdzić, czy kwalifikujesz się do posiadania konta oszczędnościowego z wyższym oprocentowaniem

W pozostałych sytuacjach przed zgromadzeniem lub ponownym wykorzystaniem Twoich danych osobowych firma lub organizacja uzyskać od Ciebie zgodę na ich przetwarzanie.

9. Czy to prawda, że nie jest się anonimowym w sieci?

Tak to prawda, korzystając z sieci pozostawiamy za sobą cyfrowy ślad. Są to informacje o naszej aktywności w sieci.

Można je na podstawie adresu IP (Internet Protocol Address- numer identyfikacyjny nadawany komputerom lub innym urządzeniom łączącym się z siecią, na jego podstawie można ustalić adres, pod którym znajduje się urządzenie, a także system operacyjny, zestaw zainstalowanych czcionek i ustawienia przeglądarek internetowych.
Dodatkowo można pozyskać informacje na temat Twojego ruchu w cyberprzestrzeni - czas spędzony w internecie, odwiedzane strony, zapytania w wyszukiwarkach, dane osobowe, które podałeś na stronach internetowych, informacje, które umieszczasz w portalach społecznościowych. Ciasteczka (tzw. „cookies") pozwalają serwerom stron śledzić twoją aktywność w sieci.

Dane o użytkownikach są przechowywane ze względu na: bezpieczeństwo publiczne, badania rynku i efektywne administrowanie stron www, reklamy. Okres przechowywania takich danych według prawa europejskiego wynosi 2 lata.

10. Lubię robić zakupy internetowe w sieci, ale obawiam się podawać moje dane osobowe na różnych stronach internetowych. Jak mogę sprawdzić czy strona jest bezpieczna?

Po pierwsze rób zakupy tylko u zaufanych Ci dostawców.
Unikaj zapamiętywania Twoich danych karty płatniczej w przeglądarkach, bezpieczniej jest je za każdym razem wprowadzać ręcznie.
Sprawdzaj czy strona na którą wchodzisz posiada certyfikat bezpieczeństwa SSL (https przed adresem strony, zielona kłódka) gwarantujący szyfrowanie Twoich danych podczas przesyłania w sieci. Pamiętaj jednak, że strony przestępców też mogą posiadać taki certyfikat, gdyż może go zakupić każdy.

11. Jak mogę być pewny, że nie stracę ważnych dla mnie danych?

Korzystaj z zaufanych usług chmurowych, w których możesz utworzyć kopię zapasową ważnych dla Ciebie danych.
Dodatkowo możesz utworzyć kopie zapasowe na nośnikach fizycznych - dyski przenośne, pendrive. Pamiętaj jednak, żeby chronić je przed zagubieniem i dostępem osób nieupoważnionych.

12. Co to są pliki cookies?

.Cookie to mały plik tekstowy, który strona internetowa zapisuje na komputerze lub urządzeniu przenośnym użytkownika w chwili, gdy ten ją przegląda.
Pliki cookie administratora to pliki należące do odwiedzanej strony internetowej.
Tylko ta strona internetowa może je odczytać. Strona internetowa może ewentualnie korzystać z serwisów zewnętrznych, które również posiadają własne pliki cookie – są to pliki cookie osób trzecich.
Trwałe pliki cookie są zapisywane na komputerze użytkownika i nie są automatycznie usuwane po zamknięciu przeglądarki w przeciwieństwie do sesyjnych plików cookie, które są usuwane po zamknięciu przeglądarki.
Podczas każdych odwiedzin na stronach internetowych jest pytanie o zgodę na przetwarzanie plików cookies.
Dzięki nim strona internetowa przez pewien czas zapamiętuje preferencje użytkownika (np. nazwa użytkownika, język itp.) i nie trzeba ponownie wprowadzać tych samych danych podczas jednych odwiedzin na stronie.

Pliki cookie mogą być również używane do sporządzania anonimowych statystyk o korzystaniu z stron internetowych.

13. Jak kulturalnie komunikować się w sieci?

Najprostsza odpowiedź to tak jak w rzeczywistości - bądź kulturalny i przyjazny dla innych użytkowników.

Stosu w sieci netykietę:

- nie używaj wulgaryzmów;
- nie spamuj (m.in. nie wysyłaj niechcianych linków do stron);
- nie wysyłaj tzw. “ łańcuszków szczęścia”;
- zanim zadasz pytanie sprawdź czy w FAQ (zbiór najczęściej zadawanych pytań i odpowiedzi do nich) nie ma już takiego pytania;
- pisz wyłącznie na temat;
- nie pisz całej wiadomości wielkimi literami;
- nie trolluj i nie prowokój kłótni.
- nie nadużywaj emotek.

14. Czy moje dane w sieci są chronione?

Tak, jako Właściciel danych osobowych posiadasz prawo do:

- Informacji - kto gromadzi i przetwarza dane osobowe, wraz z ich wykorzystaniem, muszą być swobodnie dostępne i napisane jasnym, prostym językiem.
- Dostępu - osoby fizyczne mogą prosić o potwierdzenie, że ich dane są przetwarzane.
- Sprostowania - poprawienie wszelkich niekompletnych lub niedokładnych informacji, które są przetwarzane.
- Usunięcia - prawo do bycia zapomnianym, usunięcie danych gdy nie ma już uzasadnionego powodu, aby kontynuować jego przetwarzanie lub wycofana jest zgoda.
- Przenoszenia danych - umożliwia uzyskanie danych i ponowne wykorzystanie ich w innym celu i u innego Administratora.
- Sprzeciwu – prawo do sprzeciwu wobec przetwarzania jeżeli nie ma uzasadnionego powodu.

- Ochrony przed automatycznym podejmowaniem decyzji i profilowaniem. Zabezpieczenie przed wystąpieniem ryzyka podejmowania jakichkolwiek szkodliwych lub niekorzystnych decyzji bez możliwości interwencji człowieka lub możliwości uzyskania wyjaśnień.

15. Czy długa praca na komputerze ma wpływ na zdrowie?

Tak, zbyt długie korzystanie z komputera może mieć wpływ na nasze zdrowie: nadwyrężanie mięśni nadgarstka,

- naprężony kark,
- bóle dolnych części kręgosłupa,
- kłopoty ze wzrokiem,
- bóle głowy i ogólne zmęczenie organizmu,
- rezygnacja z bezpośredniego komunikowania się z ludźmi może być przyczyną depresji.

Dla zdrowia fizycznego w trakcie pracy z komputerem należy zapewnić sobie odpowiednie warunki. Stanowisko powinno umożliwiać przyjęcie odpowiedniej pozycji, zapewniać właściwe oświetlenie. Powinno się robić przynajmniej 5 minutowe przerwy co godzinę pracy. Możesz w tym przerwie wykonać proste ćwiczenia rozciągające.

16. Czy istnieją jakieś metody zabezpieczające przed aktywnością cyberprzestępców?

Nie jesteśmy w stanie zabezpieczyć się w stu procentach przed cyberprzestępstwami. Są jednak sposoby, które ograniczają do minimum ryzyko zostania ofiarą cyberataku:

- Zainstaluj program antywirusowy, włącz go i aktualizuj bazę antywirusów
- Używaj firewalla (zapora sieciowa).
- Aktualizuj system operacyjny, przeglądarki internetowe, zainstalowane oprogramowanie zgodnie z sugestiami producenta.
- Jeżeli jest to możliwe, włącz podwójną autentykację do logowania się do usług w sieci.
- Uważaj na podejrzane maile, podszywające się pod zaufane instytucje (bank, Facebook, operator sieci komórkowej), które zawierają prośbę o podjęcie działań na koncie
- Zawsze sprawdzaj dokładnie skąd została do Ciebie wysłana wiadomość - dane nadawcy oraz do kogo została wysłana, czy jesteś jej faktycznym odbiorcą. W razie wątpliwości, zanim podejmiesz jakiekolwiek działania skontaktuj się nadawcą wiadomości innym kanałem komunikacyjnym (jeżeli otrzymałeś maila to zadzwoń na znany Ci numer dostawcy usługi).
- Nie klikaj na linki zawarte w podejrzanej wiadomości. Otwórz przeglądarkę ręcznie, wprowadź w niej dane dostawcy, od którego otrzymałeś wiadomość i dopiero z tego miejsca podejmij jakiekolwiek działania.
- Pliki, oprogramowanie, aplikacje pobieraj tylko zaufanych źródeł, najlepiej ze stron producentów. Unikniesz dzięki temu pobierania dodatkowej, niechcianej zawartości oraz nielegalnych źródeł.
- Przed otwarciem załącznika z podejrzanej wiadomości przeskanuj ją programem antywirusowym.
- Unikaj korzystania z publicznych sieci WiFi. Mogą być obsługiwane przez cyberprzestępców, którzy tworzą dostępy podszywające się pod zaufane instytucje np. urzędy miasta. Najlepiej korzystać z własnych zasobów sieciowych dostępnych w domu lub na urządzeniu mobilnym.
- Używaj różnych danych do logowania do różnych usług. Nie stosuj tego samego loginu i hasła w usługach dla Ciebie wrażliwych i w usługach typu forum internetowe, sklep internetowy - są one słabiej zabezpieczone i łatwiej mogą być przejęte przez przestępców.

- W urządzeniach mobilnych ustaw blokadę ekranu za pomocą wzoru, PIN, wizerunku twarzy, odcisku palca. Dzięki temu w przypadku kradzieży lub zgubienia urządzenia osoby nieupoważnione nie będą miały dostępu do Twoich danych, które przechowujesz w pamięci telefonu - dane z przeglądarek, aplikacje zainstalowane na urządzeniu, zdjęcia, notatki, inne dane. UWAGA! Blokada ekranu nie chroni Twojej dodatkowej pamięci włożonej do urządzenia. Karta pamięci jest zewnętrznym nośnikiem, który po przełożeniu do innego daje możliwość odczytu danych.
- Sprawdzaj w internecie podejrzane numery telefonów wpisując w wyszukiwarce np. Google hasło: “Co to za numer (nr telefonu, który do Ciebie dzwonił).
- Nie podawaj swoich danych osobowych, bankowych czy karty płatniczej poza zaufanymi portalami. Nie wysyłaj swoich danych SMS czy w wiadomości e-mail.

17. Czy mogę gdzieś zgłosić podejrzenie ataku?

Tak, ataki cyberprzestępców możesz zgłosić do CERT Polska pod adresem https://incydent.cert.pl/#!/lang=pl .

Zgłoszenie ataku utrudnia działanie cyberprzestępcom i zapobiega dalszym wyłudzeniom od innych ofiar.

18. Czy pracownik banku może poprosić mnie o przesłanie mailem lub inną wiadomością moich danych karty kredytowej lub danych do logowania do usług bankowości elektronicznej?

Nie podawaj danych logowania do bankowości elektronicznej przez e-mail/telefon. Bank nigdy nie prosi klienta o login i hasło do konta internetowego ani telefonicznie, ani mailowo.

Listy, wiadomości e-mail lub telefony w takich sprawach należy traktować jako próbę wyłudzenia poufnych informacji. Nie odpowiadaj na nie.

19. Jak sprawdzić czy sklep internetowy nie jest fałszywy?

Zweryfikuj dane firmy - nazwę, NIP, adres firmy - powinny być w zakładce kontakt, w regulaminie sklepu i polityce prywatności. Dane możesz porównać w Centralnej Ewidencji i Informacji o Działalności Gospodarczej https://prod.ceidg.gov.pl/CEIDG/CEIDG.Public.UI/Search.aspx lub Krajowym Rejestrze Sądowym https://ekrs.ms.gov.pl/web/wyszukiwarka-krs/strona-glowna/ .

Sprawdź czy sklep ma regulamin, zapoznaj się z jego zapisami, porównaj je z ofertą opublikowaną przy ogłoszeniu - czas dostawy, formy płatności i wysyłki. Jeżeli sklep nie ma regulaminu lub jest napisany niepoprawną polszczyzną zrezygnuj z zakupów.

Sprawdź opinie w internecie na temat sklepu (zwracaj uwagę na liczbę opinii, daty ich wystawienia).

Sprawdź czy jest opcja płatności za pobraniem, nawet jeżeli nie chcesz tak realizować płatności. Fałszywe sklepy najczęściej oferują tylko płatność przed wysyłką.

Sprawdź na portalach społecznościowych czy sklep ma swój profil, jeżeli tak zobacz co piszą o nim inni klienci.

Nie wierz bardzo atrakcyjnym ofertom zakupu.

20. Co to są dane osobowe?

Dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania żyjącej osoby fizycznej.

Przykładowe dane osobowe:

- imię i nazwisko;
- wizerunek
- adres zamieszkania;
- adres e-mail, taki jak imię.nazwisko@firma.com;
- numer dowodu tożsamości;
- dane o lokalizacji;
- adres IP;
- identyfikator plików cookie;
- dane przechowywane przez szpital lub lekarza, które mogą jednoznacznie wskazywać tożsamość danej osoby.

Do danych osobowych nie zalicza się na przykład: numeru KRS; nieimiennego adresu e-mail (np. bok@firma.com).

Załączniki:

1. **Materiały dydaktyczne -** MODUŁ 1 Zagrożenia społeczne i fizyczne związane z użytkowaniem komputera , Internetu oraz smartfonów. Cyberprzemoc i cyberprzestępstwa. Zasady postępowania w przypadku zetknięcia się z cyberprzestępczością i innymi zagrożeniami. Typy oszustw w Internecie w tym oszustwa telefoniczne, przez SMS i pocztę elektroniczną.
2. **Materiały dydaktyczne -** Moduł 2 Ochrona przed szkodliwym oprogramowaniem, ochrona przed wirusami, usługi chmurowe.
3. **Materiały dydaktyczne -** Moduł 3 Kontakt i relacje z innymi użytkownikami Internetu dbanie o własny wizerunek w sieci, nieujawnianie wrażliwych informacji. Wiarygodność informacji w Internecie. Prawa autorskie.
4. **Materiały dydaktyczne** - MODUŁ 4 Bezpieczeństwo finansów prywatnych i w miejscu pracy, bezpieczna bankowości internetowa oraz bezpieczne zakupy.
5. **Broszura dla bezrobotnych** – Bezpieczni w sieci.

MODUŁ 1
Zagrożenia społeczne i fizyczne związane z użytkowaniem komputera , Internetu oraz smartfonów.
Cyberprzemoc i cyberprzestępstwa.
Typy oszustw w Internecie w tym oszustwa telefoniczne, przez SMS i pocztę elektroniczną.
Zasady postępowania w przypadku zetknięcia się z cyberprzestępczością i innymi zagrożeniami.

Fundusze Europejskie Wiedza Edukacja Rozwój
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Społeczny

Czego się dowiesz z modułu drugiego?

- Poznasz zagrożeniami wynikającymi z korzystania z narzędzi informatycznych.
- Poznasz przykłady cyberprzemocy i cyberprzestępstw w różnych kanałach komunikacyjnych.
- Poznasz sposobów zabezpieczenia się przed zagrożeniami w cyberprzestrzeni.

W trakcie szkolenia z modułu drugiego:

- Zapoznasz się z teorią
- Poznasz przykłady praktyczne
- Wykonasz ćwiczenia

Wprowadzenie:

Dzisiejsze czasy umożliwiają nam łatwiejszą organizację życia prywatnego i zawodowego dzięki rozwiązaniom technologicznym pozwalającym na dostęp do szerokiej informacji z całego świata, szybkiej realizacji celów i dostępności do zasobów przez całą dobę.

Rozwój elektronicznych narzędzi komunikacyjnych i systemów informatycznych służących nam prywatnie lub zawodowo, naturalnie wzbudził zainteresowanie środowiska przestępczego - cyberprzestępców.

Korzystanie z tych technologii niesie za sobą różnego rodzaju zagrożenia: psychiczne, fizyczne, społeczne, moralne i intelektualne.

Zagrożenia społeczne

Zagrożenia społeczne można podzielić na nietechniczne i techniczne.

Zagrożenia społeczne nietechniczne

Do zagrożeń nietechnicznych zalicza się

- cyberstalking (natrętne i złośliwe dręczenie ofiary),
- trollowanie (nieprzyjazne zachowania wobec innych użytkowników Internetu, które mają na celu rozbicie prowadzonej w internecie dyskusji),
- flaming (sposób prowadzenia dyskusji prowadzący do wywołania agresji),
- cyberprostytucja (uzyskiwaniu korzyści materialnych za udostępnianie, przekazywanie poprzez Internet zdjęć i filmów o charakterze erotycznym lub pornograficznym wytworzonych z własnym udziałem),
- seksting (przekazywanie za pomocą Internetu i urządzeń mobilnych swoich zdjęć, filmów lub wiadomości o charakterze seksualnym,
- grooming (wprowadzanie w błąd nieletniego dziecka do lat 15 w celu produkcji materiałów pornograficznych lub składaniu mu propozycji seksualnych przez Internet).

Zagrożenia społeczne

Przejdźmy do Ćwiczenia numer 1:

Czy spotkałeś się z przypadkiem nietechnicznego zagrożenia społecznego?

Zagrożenia społeczne techniczne

Zagrożenia społeczne techniczne związane są z działaniami cyberprzestępców.

Mają na celu:

- wyłudzenia od użytkownika danych wrażliwych,
- kradzieżą środków finansowych lub danych, wyłudzeniami

Zagrożenia fizyczne

Zagrożenie fizyczne związane jest z problemami zdrowotnymi wynikającymi ze zbyt długie korzystanie z Internetu:

- nadwyrężanie mięśni nadgarstka,
- naprężony kark, bóle dolnych części kręgosłupa,
- kłopoty ze wzrokiem, bóle głowy i ogólne zmęczenie organizmu.
- rezygnacja z bezpośredniego komunikowania się z ludźmi może być przyczyną depresji.

Zagrożenia moralne i intelektualne

Zagrożenia moralne wynikają z niewłaściwego korzystania z cyberprzestrzeni, która umożliwia dostęp do treści wątpliwych etycznie lub umieszczanych w sposób nielegalny.

Ułatwiony jest dostęp do pornografii, zawartości dewiacyjnej (tzw. “patostreamy”), materiałów nielegalnie udostępnianych w sieci (pirackie programy i filmy), zakupów przedmiotów pochodzących z kradzieży lub przemytu, informacji propagujących korzystanie z narkotyków.

Zagrożenia intelektualne wynikają z tzw. “szoku informacyjnego”, zbyt dużej ilości informacji otrzymywanych z cyberprzestrzeni,która nie stanowi wiedzy.

Cyberprzemoc

Cyberprzemoc to seria agresywnych zachowań, celowo i regularnie skierowanych przeciwko słabszej osobie, najczęściej w formie słownej w postaci komentarzy, memów, nagrań wideo, które mają spowodować poczucie zagrożenia u odbiorcy. Może również polegać na manipulowaniu czy wykluczeniu z grupy.

Cyberprzemoc

Najczęściej spotykane formy cyberprzemocy:

- poniżające filmy lub zdjęcia;
- ośmieszające, wulgarne, komentarze i posty;
- włamania na konta serwisów społecznościowych,
- flood, czyli przesyłanie dużej ilości wiadomościami na komunikatory, telefonicznie, lub SMSami,
- podszywanie się pod ofiarę w celu publikacji kompromitujących ją opinii.

Cyberprzemoc

Do cyberprzemocy zachęca przekonanie o anonimowości - działaniu z ukrycia, możliwość spokojnego zaplanowania swojego działania sprawcy oraz dostępność ofiary przez cały czas w cyberprzestrzeni. Sprawcami cyberprzemocy, mogą być osoby, których w realnym życiu byśmy o to nie podejrzewali.

Cyberprzestępstwa

Cyberprzestępczość to nielegalne działania, popełniane za pomocą technik komputerowych lub dotyczące systemów lub sieci komputerowych.

Cyberprzestępstwa

Najczęściej spotykana działania cyberprzestępców:

Phishing – atak na polegający na wyłudzeniu od użytkownika istotnych dla niego danych na przykład numer karty kredytowej lub danych do logowania do bankowości internetowej, poczty elektronicznej lub mediów społecznościowych. W tym celu cyberprzestępcy podszywają się pod znaną użytkownikowi osobę lub instytucję darzoną zaufaniem (np. bank) w wiadomości mailowej, czy poprzez fałszywą stronę internetową.

Ransomware - atak polegający na próbie wyłudzenia środków finansowych użytkownika przez rzeczywiste działanie - szyfrowanie danych na dyskach lub fałszywy szantaż, w którym cyberprzestępca informuje o posiadaniu kompromitujących materiałów na temat użytkownika.

Malware – to atak z wykorzystaniem złośliwego oprogramowania, które infekuje urządzenie. Celem jest kradzież danych, uszkodzenie plików, czy zablokowanie dostępu do urządzenia. Do tego typu oprogramowania możemy zaliczyć wirusy, robaki, trojany, spyware (oprogramowanie szpiegujące).

Hacking – to włamania, poprzez łamanie zabezpieczeń, umożliwiające zdalny, nielegalny dostęp do czyjegoś komputera.

Wyłudzenia - polegające na wysyłaniu przez cyberprzestępców wiadomości oferujących korzystną dla odbiorcy współpracę, oszustwa matrymonialne, fałszywe zbiórki charytatywne,

Cyberprzestępstwa

Inne przykłady cyberprzestępstw to oszustwa popełniane przez Internet, np. przez nieuczciwych sprzedawców na portalach aukcyjnych, naruszanie praw autorskich (nielegalne kopiowanie i rozpowszechnianie filmów, muzyki) itp.

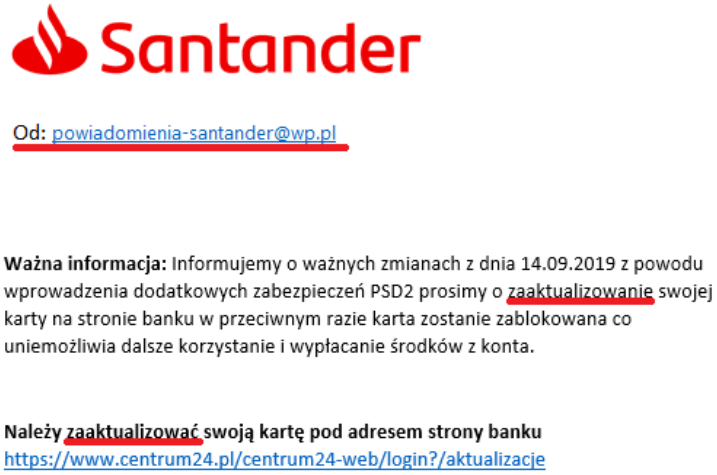
Cyberprzestępstwa

Przejdźmy do Ćwiczenia numer 2

Analiza ataków cyberprzestępców na świecie.

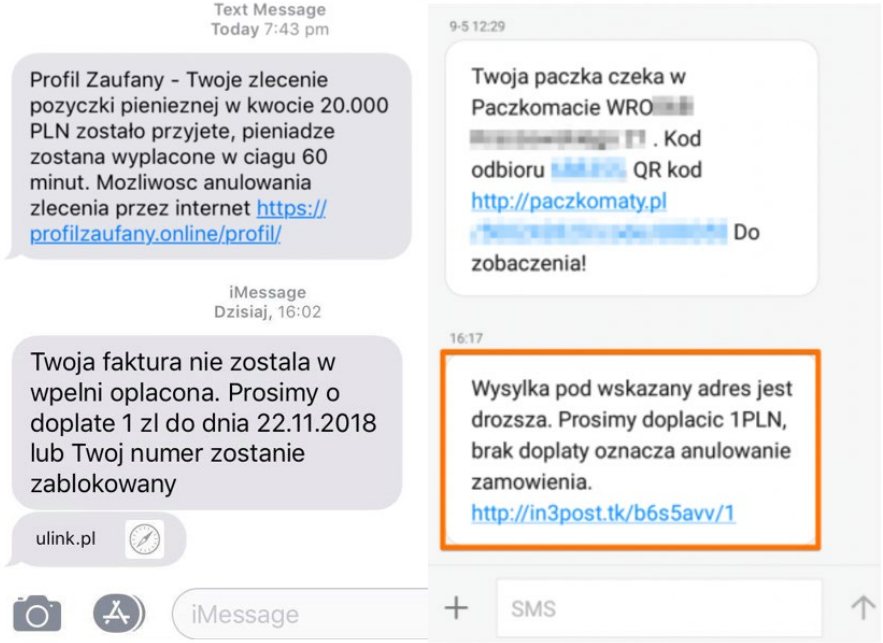
Przykłady ataków cyberprzestępców

Otrzymanie wiadomości mailowej od cyberprzestępcy podszywającego się pod bank z informacją o zmianie regulaminu usługi lub konieczności podjęcia działań na rachunku bankowym. Cyberprzestępcy umieszczają w wiadomości link przekierowujący na fałszywą stronę bankową, na której wyłudzają dane ofiary do logowania się do portalu bankowego. (na czerwono wskazane są elementy, które świadczą o fałszywej wiadomości- adres e-mail w domenie Wirtualnej Polski a nie Santander banku, błędy w treści maila).



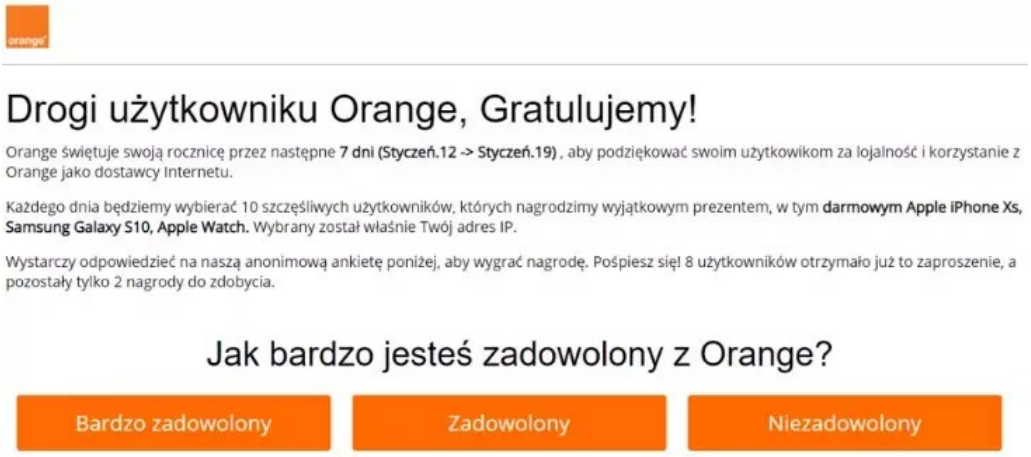
Przykłady ataków cyberprzestępców

Otrzymanie wiadomości mailowej lub SMS o zaległej płatności za usługi telekomunikacyjne lub inne. W wiadomości znajduje się link przekierowujący na fałszywą stronę służącą do płatności np. PayPal i z niej przekierowującą na fałszywą stronę banku, na której cyberprzestępcy usiłują wyłudzić dane do logowania do banku.



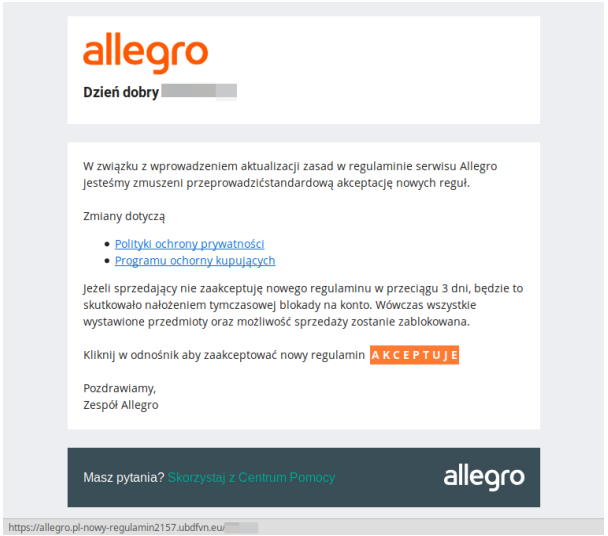
Przykłady ataków cyberprzestępców

Otrzymanie wiadomości o wygranej w konkursie lub bardzo atrakcyjnej ofercie handlowej.



Przykłady ataków cyberprzestępców

- Otrzymanie wiadomości podszywającej się pod dostawcę usług aukcyjnych np. Allegro zawierającej informację o zmianie regulaminu lub innych koniecznych działaniach na koncie, w celu wyłudzenia danych do logowania i wystawienia na koncie ofiary fałszywych ofert sprzedaży.



Przykłady ataków cyberprzestępców

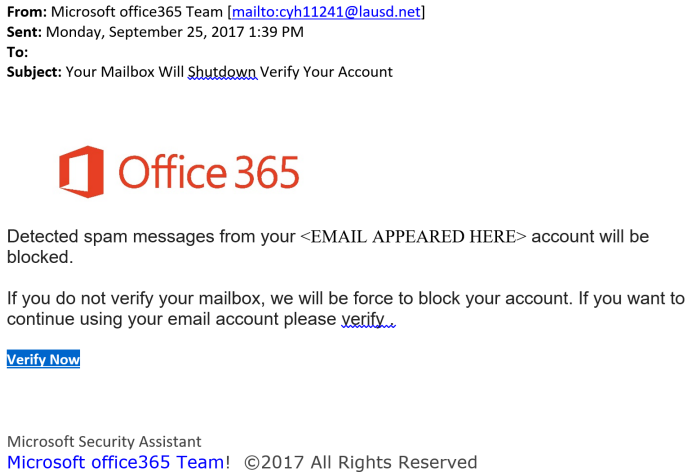
Oszustwo tzw. “przekręt nigeryjski”, próba zainteresowania użytkownika szybkim zarobkiem wynikającym z konieczności transferu znacznych środków pieniężnych w bezpieczną lokalizację. Cyberprzestępcy proszą o przelew określonej kwoty na ich konto w celu “uwiarygodnienia” danych ofiary.

Witaj

Jestem Ahmed Ali Al Sayegh, dyrektor zarządzający First Gulf Bank w Zjednoczonych Emiratach Arabskich. Piszę tę propozycję w dobrej wierze, mając nadzieję, że polegam na tobie w transakcji biznesowej, która wymaga całkowitej poufności oraz dużego zainteresowania i korzyści dla nas obu. family.In 2007, jeden Husson Nisztor, obywatel emiratu, którego nazwisko jest takie samo jak twoje i ma swój kraj w swoim pliku jako jego miejsce pochodzenia, dokonał stałego depozytu na 36 miesięcy, wycenionego na 26.700.000 dolarów z mojego banku. Zanim zostałam dyrektorem zarządzającym, byłam jego księgową. Data zapadalności tej umowy depozytowej to 27 września 2010 r. Z pewnością pan Husson Nisztor znalazł się wśród ofiar śmiertelnych podczas trzęsienia ziemi w Indonezji w 2009 r., W którym zginęło ponad 1200 osób podczas podróży służbowej. Od ostatniego kwartału 2010 r. do dzisiaj kierownictwo mojego banku znajdowało środki, by do niego dotrzeć, aby upewnić się, że przekaże depozyt lub wycofa sumę kontraktowa. Kiedy odkrvłem. że tak sie stanie.

Przykłady ataków cyberprzestępców

Otrzymanie wiadomości podszywającej się pod popularne usługi chmurowe np. Microsoft365, Google w celu przejęcia danych do logowania do usługi i z niej przejęcia danych i uwiarygodnienia się wśród kontaktów ofiary, co umożliwia dalsze rozsyłanie szkodliwych maili.



From: Microsoft office365 Team [mailto:cyh11241@lausd.net]
Sent: Monday, September 25, 2017 1:39 PM
To:
Subject: Your Mailbox Will Shutdown Verify Your Account

Office 365

Detected spam messages from your <EMAIL APPEARED HERE> account will be blocked.

If you do not verify your mailbox, we will be force to block your account. If you want to continue using your email account please verify..

Verify Now

Microsoft Security Assistant
Microsoft office365 Team! ©2017 All Rights Reserved

Przykłady ataków cyberprzestępców

Próba szantażu informującego o przejęciu komputera i zarejestrowaniu ofiary w czasie oglądania filmów dla dorosłych.

Cześć!

Jestem hakerem, który ma dostęp do Twojego system operacyjnego.
Mam też pełen dostęp do Twojego konta.

Obserwuję Cię już od paru miesięcy.
Fakty są takie, że zainfekowałem Cię oprogramowaniem przez stronę dla dorosłych.

Jeśli nie wiesz, jak to działa, to już wyjaśniam.
Wirus Trojan daje mi pełen dostęp I kontrolę nad Twoim komputerem, czy innym urządzeniem.
To oznacza, że widzę wszystko na Twoim ekranie, włączam kamerę i mikrofon, ale ty o tym nie wiesz.

Mam również dostęp do wszystkich twoich kontaktów I korespondencji.

Czemu Twój antywirus nie wykrył tego oprogramowania?
Odpowiedź: Mój program używa dysku, uaktualniam jego sygnatury co 4 godziny, więc antywirus milczy.

Wykonałem film, pokazujący, jak się zadowalasz po lewej stronie ekranu, a po prawej film, który wtedy oglądałeś.
Jednym kliknięciem myszy mogę wysłać ten film do wszystkich Twoich emaili i kontaktów w mediach społecznościowych.
Mogę również opublikować dostęp do całej twojej korespondencji i wiadomości, których używasz.

Jeśli chcesz temu zapobiec,
Przelej kwotę 925€ na mój adres bitcoin (jeśli nie wiesz, jak to zrobić, wpisz w Google: Kupienie Bitcoin").

Mój adres bitcoin (BTC Wallet) to: 1BbA6jQjnNXqK1reVTHGEsPGghXJ2rdqcq

Po otrzymaniu płatności usunę film i nigdy więcej o mnie nie usłyszysz.
Daję Ci 50 godzin (ponad 2 dni) by zapłacić.
Mam powiadomienie o odczytaniu tej wiadomości, licznik działa wraz z jej otwarciem.

Zgłaszanie tego gdziekolwiek nie ma sensu, ponieważ tego emaila nie można namierzyć, tak samo jak mojego adresu bitcoin.
Nie popełniaj błędów.

Jeśli się dowiem, że podzieliłeś się tą wiadomością z kimś innym, film natychmiast zostanie opublikowany.

Wszystkiego Najlepszego!

Przykłady ataków cyberprzestępców

Otrzymanie wiadomości podszywającej się pod organy państwowe np. ZUS, Urząd Skarbowy, Policja lub podmioty świadczące usługi bankowe, telekomunikacyjne, kurierskie , która ma na celu zainfekowanie naszych urządzeń szkodliwym oprogramowaniem ukrytym pod linkiem lub w załączniku wiadomości.

Poczta Polska [redacted]@wp.pl Pt, 8 maj 18:01

Niedostarczone przesylki na 7.05.2015, kod:158144

Poczta Polska

Kurier nie dostarczył przesyłkę do numeru zgłoszenia **RR6453614973PL** na adres **05.07.2015**, ponieważ nikt w tym czasie. Proszę zobaczyć informacje na temat wysyłki, drukowania i iść na pocztę, aby otrzymać pakiet.

Zobacz informacje

Uwaga

Jeżeli przesyłka nie dotrze w ciągu 7 dni roboczych Poczta Polska będzie miała prawo do ubiegania się koszty utrzymania przesyłka 50 zł za jeden dzień. Dziękujemy za korzystanie z naszych usług dostawy. Życząc miłego dnia Twoja Poczta Polska.

To jest generowany automatycznie e-mail, kliknij jeżeli chcesz się wypisać

Poczta Polska S.A. (c) 2015. Wszelkie prawa zastrzeżone.

From: Administracja Podatkowa
Sent: Saturday, August 31, 2013 4:33 PM
Subject: Zawiadomienie o refundacji

Data: 31 sierpnia 2013
Nasza Ref.: C/02335/14
Twój Ref.: 11T/115/10

Administracja Podatkowa

Zawiadomienie zeznanie podatkowe za rok 2012

Szanowny Panie / Szanowna Pani,

Wysylam te wiadomosc oglosic: Po ostatnim obliczenia rocznego swojej dzialalnosci fiskalnej my ustalilismy, ze sa uprawnieni do otrzymania zwrotu podatku z:

***378.81* zl**

Aby otrzymac zwrot podatku, kliknij tutaj

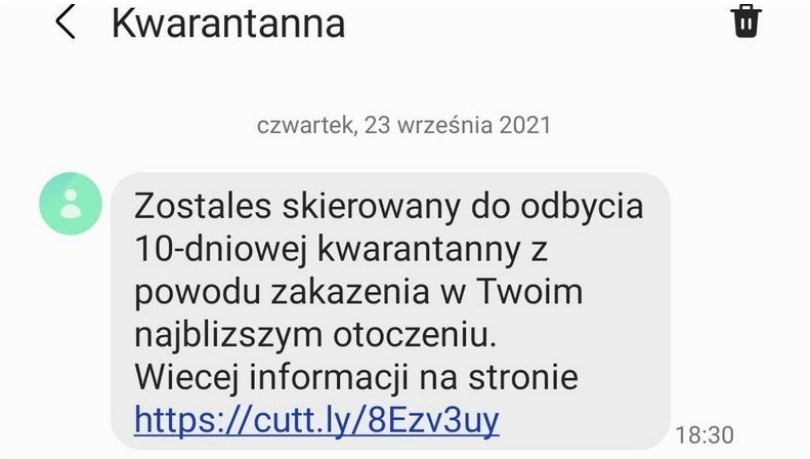
© Copyrights Ministerstwo Finansów 2011-2013

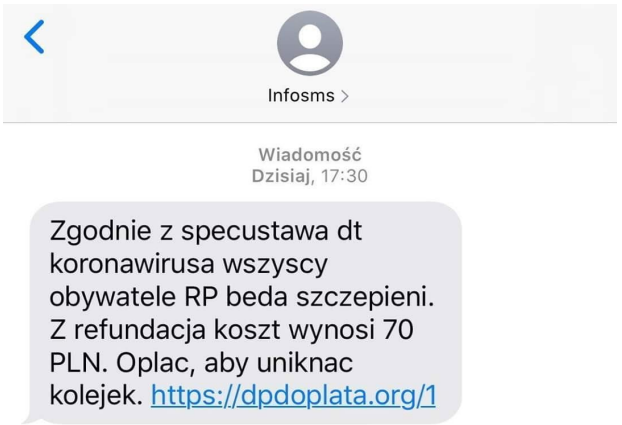
Przykłady ataków cyberprzestępców

Krótkie połączenie z nieznanego numeru z zagranicy, w celu nakłonienia ofiary do oddzwonienia na płatny numer usługi premium.

Przykłady ataków cyberprzestępców

Cybeprzestępcy często wykorzystują aktualne wydarzenia polityczne lub społeczne do prób ataków. W przypadku zmiany prawa lub innych zdarzeń przesyłają informacje, które mogą zainteresować odbiorców.





Przykłady ataków cyberprzestępców

Dzień dobry,

Urząd Ochrony Danych Osobowych szykuje podobno kontrole w naszym sektorze. Proszę o sprawdzenie, czy Państwa hasła spełniają wymagania RODO w zakresie bezpieczeństwa. Na naszej stronie umieściliśmy narzędzie do weryfikacji zgodności:

https://[redacted].php?00

Uwaga - W formularzu nie podajemy nazwy użytkownika, tylko samo hasło do weryfikacji. Przy wpisywaniu proszę się upewnić, że w pasku adresu widnieje symbol zamkniętej kłódki.

Temat **Aktualizacja danych osób ubezpieczonych** 07.04.2020, 11:

Do praca@[redacted]

Szanowni Państwo,

W związku z koniecznością wdrożenia rozporządzeń przygotowanych w ramach tarczy antykryzysowej przez rząd RP powołany został Inspektorat Kryzysowy Zakładu Ubezpieczeń Społecznych. Rolą Inspektoratu jest pomoc przedsiębiorcom oraz przeciwdziałanie nadużyciom w ramach przygotowanego pakietu ustaw.

W celu weryfikacji i aktualizacji bieżącego stanu zatrudnienia w przedsiębiorstwie "[redacted] Sp. z o.o." prosimy o pilne przesłanie nam listy osób zatrudnionych na dzień 31.03.2020. Ze względów bezpieczeństwa lista powinna zawierać jedynie imiona i nazwiska zatrudnionych, bez danych wrażliwych typu numery PESEL, NIP itp. Format pliku dowolny, ale preferowane są formaty ogólnodostępne typu plik tekstowy (.txt), arkusze Excel (.xlsx lub .xls) lub plik CSV.

--

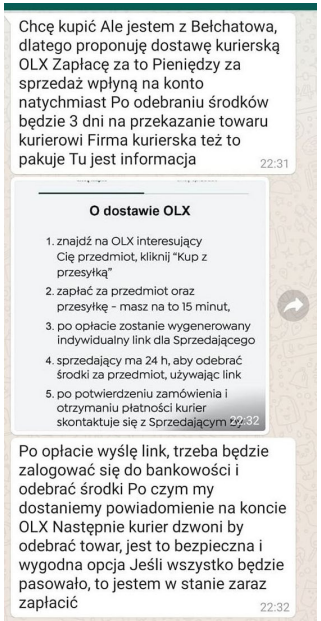
Uwaga: Ze względu na trwającą sytuację kontakt z Inspektoratem możliwy jedynie przez platformę usług elektronicznych ZUS PUE:

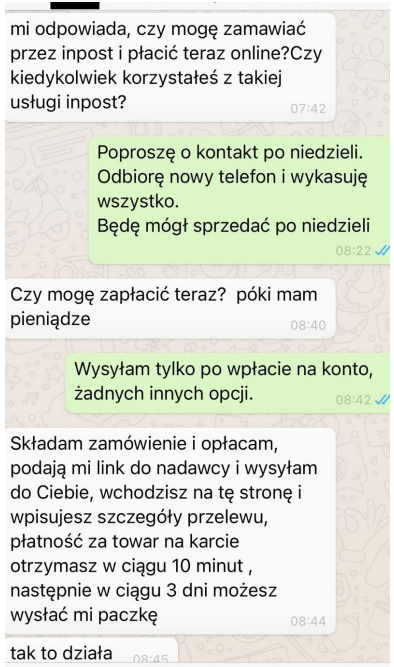
https://www.zus.pl/portal/logowanie.npi

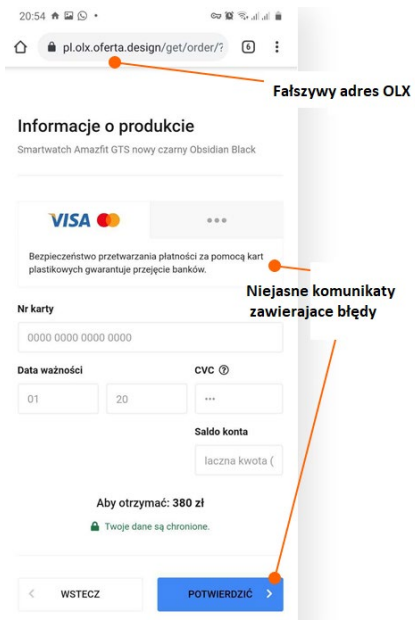
ZUS Zakład Ubezpieczeń Społecznych
Wielkopolski Inspektorat Kryzysowy

Przykłady ataków cyberprzestępców

Wyłudzenia środków finansowych lub danych karty płatniczej ogłoszeń umieszczanych w znanych portalach sprzedażowych. Przestępcy komunikują się ze sprzedającymi poza komunikatorem danej platformy sprzedażowej i proszą o podanie karty lub podają fałszywe linki do stron bankowych w celu przejęcia danych do logowania. Mogą również próbować wyłudzić sprzedawany przedmiot za pobraniem.







Przykłady ataków cyberprzestępców

Przejdźmy do Ćwiczenia numer 3

Jak rozpoznać atak cyberprzestępców

Sposoby zabezpieczenia się przed atakami cyberprzestępców

Używaj w sieci silnych haseł (w bankowości internetowej, mediach społecznościowych, poczcie elektronicznej i innych aplikacjach) - hasło składające się z co najmniej 10 znaków, zawierające duże i małe litery, znaki specjalne i cyfry, nie będące wyrazem słownikowym. np. pierwszych liter z wybranego cytatu

(Słabe hasło: kwiatek12, mocne hasło: hPpkL19560!&)

PULA ZNAKÓW, Z KTÓRYCH MOŻNA UTWORZYĆ HASŁO	LICZBA ZNAKÓW HASŁA	CZAS POTRZEBNY NA ZŁAMANIE HASŁA (komputer ze specjalnym programem, dla szybkości 1 x 10^6/s kluczy)
10 (cyfry)	8	około 2 minut
26 (małe lub duże litery)	8	około 2,5 dnia
52 (małe i duże litery)	8	około 1,5 roku
62 (litery i cyfry)	8	około 7 lat
96 (wszystkie dostępne znaki)	8	około 229 lat

Sposoby zabezpieczenia się przed atakami cyberprzestępców

- Zainstaluj program antywirusowy, włącz go i aktualizuj bazę antywirusów
- Używaj firewalla (zapora sieciowa).
- Aktualizuj system operacyjny, przeglądarki internetowe, zainstalowane oprogramowanie zgodnie z sugestiami producenta.
- Jeżeli jest to możliwe, włącz podwójną autentykację do logowania się do usług w sieci.
- Uważaj na podejrzane maile, podszywające się pod zaufane instytucje (bank, Facebook, operator sieci komórkowej), które zawierają prośbę o podjęcie działań na koncie

Sposoby zabezpieczenia się przed atakami cyberprzestępców

- Zawsze sprawdzaj dokładnie skąd została do Ciebie wysłana wiadomość - dane nadawcy oraz do kogo została wysłana, czy jesteś jej faktycznym odbiorcą. W razie wątpliwości, zanim podejmiesz jakiekolwiek działania skontaktuj się nadawcą wiadomości innym kanałem komunikacyjnym (jeżeli otrzymałeś maila to zadzwoń na znany Ci numer dostawcy usługi).
- Nie klikaj na linki zawarte w podejrzanej wiadomości. Otwórz przeglądarkę ręcznie, wprowadź w niej dane dostawcy, od którego otrzymałeś wiadomość i dopiero z tego miejsca podejmij jakiekolwiek działania.
- Pliki, oprogramowanie, aplikacje pobieraj tylko zaufanych źródeł, najlepiej ze stron producentów. Unikniesz dzięki temu pobierania dodatkowej, niechcianej zawartości oraz nielegalnych źródeł.

Sposoby zabezpieczenia się przed atakami cyberprzestępców

- Przed otwarciem załącznika z podejrzanej wiadomości przeskanuj ją programem antywirusowym.
- Unikaj korzystania z publicznych sieci WiFi. Mogą być obsługiwane przez cyberprzestępców, którzy tworzą dostępy podszywające się pod zaufane instytucje np. urzędy miasta. Najlepiej korzystać z własnych zasobów sieciowych dostępnych w domu lub na urządzeniu mobilnym.
- Używaj różnych danych do logowania do różnych usług. Nie stosuj tego samego loginu i hasła w usługach dla Ciebie wrażliwych i w usługach typu forum internetowe, sklep internetowy - są one słabiej zabezpieczone i łatwiej mogą być przejęte przez przestępców.

Sposoby zabezpieczenia się przed atakami cyberprzestępców

- W urządzeniach mobilnych ustaw blokadę ekranu za pomocą wzoru, PIN, wizerunku twarzy, odcisku palca. Dzięki temu w przypadku kradzieży lub zgubienia urządzenia osoby nieupoważnione nie będą miały dostępu do Twoich danych, które przechowujesz w pamięci telefonu - dane z przeglądarek, aplikacje zainstalowane na urządzeniu, zdjęcia, notatki, inne dane. UWAGA! Blokada ekranu nie chroni Twojej dodatkowej pamięci włożonej do urządzenia. Karta pamięci jest zewnętrznym nośnikiem, który po przełożeniu do innego daje możliwość odczytu danych.
- Sprawdzaj w internecie podejrzane numery telefonów wpisując w wyszukiwarce np. Google hasło: “Co to za numer (nr telefonu, który do Ciebie dzwonił).
- Nie podawaj swoich danych osobowych, bankowych czy karty płatniczej poza zaufanymi portalami. Nie wysyłaj swoich danych SMS czy w wiadomości e-mail.

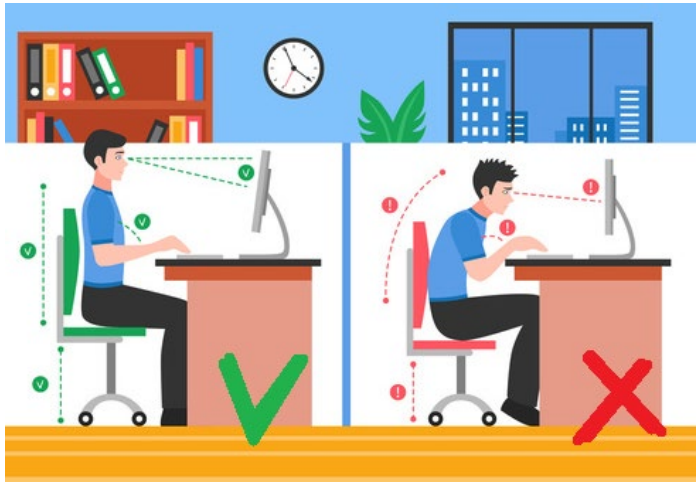
Zgłaszanie ataków cyberprzestępców

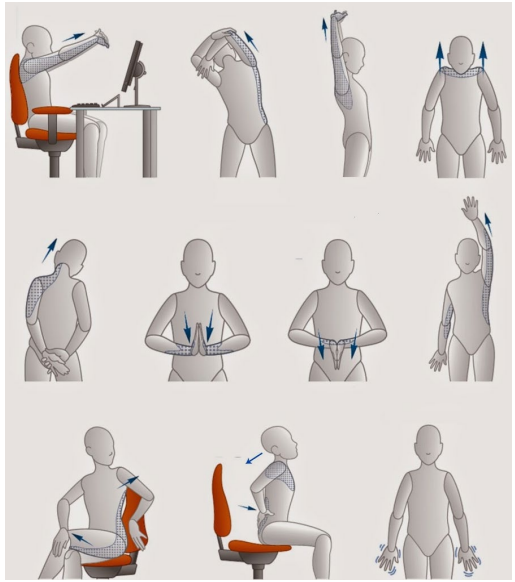
Ataki cyberprzestępców możesz zgłosić do CERT Polska pod adresem https://incydent.cert.pl/#!/lang=pl .

Zgłoszenie ataku utrudnia działanie cyberprzestępcom i zapobiega dalszym wyłudzeniom od innych ofiar.

Zdrowa praca przy komputerze

Dla zdrowia fizycznego w trakcie pracy z komputerem należy zapewnić sobie odpowiednie warunki. Stanowisko powinno umożliwiać przyjęcie odpowiedniej pozycji, zapewniać właściwe oświetlenie. Powinno się robić przynajmniej 5 minutowe przerwy co godzinę pracy. Możesz w tym przerwie wykonać proste ćwiczenia rozciągające.





Ciekawe strony na temat cyberzagrożeń

www.niebezpiecznik.pl

www.zaufanatrzeciastrona.pl

https://plblog.kaspersky.com/

Bibliografia

BIBLIOGRAFIA:

Leszczyński M., Bezpieczeństwo społeczne Polaków wobec wyzwań XXI wieku,, 2011, Difin

Lidermann K., Bezpieczeństwo informacyjne. Nowe wyzwania, Warszawa, 2017, Wydawnictwo Naukowe PWN

Opracowanie zbiorowe, Bezpieczeństwo Microsoft Windows, 2009, Wydawnictwo Naukowe PWN

Opracowanie zbiorowe, Bezpieczeństwo w sieci, 2020, Wydawnictwo Itstart

Białas A., Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie, 2017, Wydawnictwo Naukowe PWN

https://zdrowie.pap.pl/srodowisko/jak-nie-uszkodzic-kregoslupa-przy-pracy-biurowej

MODUŁ 2

Ochrona przed szkodliwym oprogramowaniem,
ochrona przed wirusami,
usługi chmurowe.

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Unia Europejska
Europejski Fundusz Społeczny

MODUŁ 2

Zapraszamy do modułu 2 szkolenia z podniesienie kompetencji z zakresu bezpiecznego korzystania z technologii.

Czego dowiesz się z tego modułu?

- Poznasz narzędzia służące do zabezpieczenia się przed cyberzagrożeniami
- Poznasz sposoby wykorzystania narzędzi służących do bezpiecznego korzystania z elektronicznych urządzeń komunikacyjnych
- Poznasz sposoby pracy w usługach chmurowych..

MODUŁ 2

W trakcie szkolenia z modułu 2:

- Zapoznasz się z wiedzą teoretyczną na temat narzędzi.
- Wykonasz ćwiczenia, które pozwolą Ci wykorzystać poznane narzędzia.

MODUŁ 2

Do bezpiecznej pracy w cyberprzestrzeni służą:

- Programy antywirusowe zainstalowane na urządzeniach.
- Antywirusy dostępne online.
- Weryfikacja adresów e-mail online
- Sprawdzanie czy Twój adres e-mail i powiązane z nim dane wyciekły z bazy dostawców, którzy zgłosili incydenty
- Zabezpieczenia urządzeń mobilnych.
- Usługi chmurowe służące do wymiany danych.

MODUŁ 2

Programy antywirusowy

to programy komputerowe, których zadaniem jest wykrywanie, zwalczanie i usuwanie wirusów komputerowych.

Programy antywirusowe często składają się z dwóch modułów:

skaner – bada pliki na żądanie lub co jakiś czas; służy do przeszukiwania zawartości dysku,

monitor– bada pliki w sposób samoczynny; służy do kontroli bieżących operacji komputera.

Ze względu na rozwijanie przez cyberprzestępców wirusów, programy antywirusowe wymagają **aktualizacji** swoich baz przez pobranie ich z Internetu,

Pakiety antywirusowe zawierają często także zaporę sieciową, moduły kontrolujące pocztę elektroniczną i pliki pobierane z sieci, moduł wykrywania i zapobiegania włamaniom,

MODUŁ 2

Programy antywirusowe instalowane na komputerze.

W przypadku Widnows 10 system ma wbudowany program Windows Defender. Dla świadomych użytkowników program spełnia minimalne zabezpieczenia.

MODUŁ 2

Przejdźmy teraz do Ćwiczenia numer 1: Konfiguracja Windows Defender

MODUŁ 2

W celu lepszego zabezpieczenia warto zainstalować dodatkowy antywirus.

Przykłady bezpłatnych antywirusów:

- Avast
- Panda Dome
- Comodo AntiVirus
- Avira Free Antivirus
- Bitdefender Antivirus Free Edition

UWAGA! Bezpłatne programy mogą być wyłącznie wykorzystywane w celach prywatnych.

W pracy wymagane jest zakup licencji na program.

MODUŁ 2

Przejdźmy teraz do Ćwiczenia nr 2: Instalacja programu antywirusowego

UWAGA! Programy pobierać najlepiej ze stron producentów. Mamy wtedy gwarancję, że pobierzemy program z legalnego źródła i nie instalujemy innych dodatkowych programów, które mogą być pobrane przy okazji.

MODUŁ 2

Programy antywirusowe pozwalają na skanowanie:

- pełne skanowanie komputera,
- wybranych lokalizacji i plików,
- ustawienia automatycznego skanowania uruchamianego przez program.

Przed otworzeniem pliku, do którego nie mamy zaufania **pamiętaj aby przeskanować go** programem antywirusowym.

MODUŁ 2

Przejdźmy do Ćwiczenia numer 3:

Skanowanie programem antywirusowym.

MODUŁ 2

Doskonałym rozwiązaniem do sprawdzania niezaufanych plików lub linków do stron internetowych są skanery antywirusowe online.

Jeden z takich bezpłatnych skanerów dostępny jest pod adresem: https://www.virustotal.com/gui/home/upload

Skaner wykorzystuje silni 

rzez wielu producentów.

MODUŁ 2

Przejdźmy teraz do Ćwiczenia numer 4

Skanowanie online plików i linków.

MODUŁ 2

Sprawdzanie czy adres e-mail istnieje.

W zapewnieniu bezpieczeństwa może pomóc Ci weryfikacja czy adresy mailowe, z których otrzymałeś korespondencję faktycznie istnieją.

Służą do tego darmowe strony internetowe.

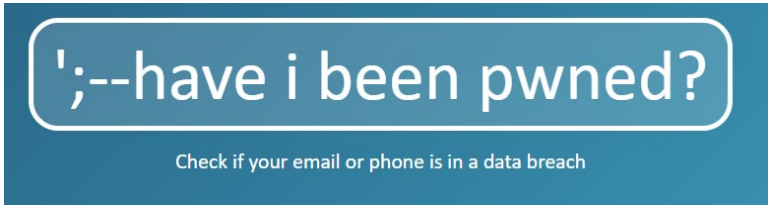
Wpisz w wyszukiwarkę hasło: “weryfikacja adresu e-mail” lub “e-mail verify” , wybierz dostępną usługę i wprowadź w niej adres e-mail, który chcesz sprawdzić.

MODUŁ 2

Czy Twoje dane wyciekły z usług oferowanych przez internet?.

W celu sprawdzenia czy Twój adres e-mail i powiązane z nim dane wyciekły z bazy danych dostawcy, który zgłosił incydent, możesz sprawdzić na stronie internetowej:

https://haveibeenpwned.com/



Wpisując swój adres e-mail i klikając na przycisk “pwned?” dowiesz się czy Twoje dane nie wyciekły w trakcie incydentów, które zgłosili dostawcy usług internetowych.

MODUŁ 2

Przejdźmy do Ćwiczenia numer 5:

Weryfikacja istnienia adresu e-mail online.

Sprawdzenie czy Twoje dane nie wyciekły z bazy firm świadczących usługi w Internecie.

MODUŁ 2

Zabezpieczenie urządzeń mobilnych

Dla zabezpieczenia swoich danych na urządzeniach mobilnych używaj blokady ekranu wzorem, hasłem, pinem lub danymi biometrycznymi (odcisk palca, wizerunkiem twarzy).

MODUŁ 2

Przejdźmy do Ćwiczenia numer 6

Blokada ekranu urządzenia mobilnego.

MODUŁ 2

Korzystanie z usług chmurowych do wymiany plików.

Dokumenty cyfrowe, pliki i zdjęcia możemy przechowywać na dysku komputera, fizycznym dysku zewnętrznym, ale też na dysku w chmurze.

Platformy chmurowe, takie jak Google, ZOHO, Microsoft 365, oferują przestrzeń dyskową oraz narzędzia do pracy w chmurze: skrzynkę mailową, współdzielony kalendarz, edytor dokumentów tekstowych online, arkusze kalkulacyjne narzędzie do tworzenia prezentacji,czat i platformę do prowadzenia wideokonferencji.

W przypadku pakietów chmurowych użytkownicy mają dostęp do plików, dokumentów i aplikacji z dowolnego urządzenia z dostępem do internetu. Mogą wspólnie prowadzić edycję jednego pliku – wprowadzone zmiany natychmiast pokażą się u wszystkich pracujących na danym dokumencie, a nowa wersja zapisze automatycznie w chmurze.

MODUŁ 2

Przejdźmy teraz do Ćwiczenia numer 7

Korzystanie z usług chmurowych do wymiany plików.

MODUŁ 2

Bibliografia:

1. Bezpieczeństwo urządzeń mobilnych. Receptury, Verma Prashant , Dixit Akshay, Wydawnicto Helion, 2021
2. Cloud Storage w domu i w pracy – Dysk Google https://www.google.com/intl/pl/drive/
3. Bezpieczeństwo w sieci, Jakub Skórka, Kacper Skórka, Marcin Kaim, Wydawnictwo Itstart, 2020
4. Zabezpieczenia systemu Windows: Program antywirusowy https://www.microsoft.com/pl-pl/windows/comprehensive-security

MODUŁ 3
Kontakt i relacje z innymi użytkownikami Internetu dbanie o własny wizerunek w sieci, nieujawnianie wrażliwych informacji. Wiarygodność informacji w Internecie. Prawa autorskie.

Fundusze Europejskie Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Unia Europejska Europejski Fundusz Społeczny

Czego się dowiesz z modułu trzeciego?

Zapraszamy do modułu 3 szkolenia z podniesienie kompetencji z zakresu bezpiecznego korzystania z technologii.

Czego dowiesz się z tego modułu?

Zapoznasz się z prowadzeniem komunikacji w Internecie we właściwy sposób.

Zapoznasz się z netykietą.

Zapoznasz się ze sposobami ochrony informacji wrażliwych, w tym danych osobowych.

Zapoznasz się ze sposobami weryfikacji informacji pod kątem jej wiarygodności.

Zapoznasz się z prawem autorskim dotyczącym publikowania materiałów w Internecie.

W trakcie szkolenia z modułu trzeciego:

- Zapoznasz się z teorią
- Poznasz przykłady praktyczne
- Wykonasz ćwiczenia

Wprowadzenie:

Komunikacja internetowa odnosi się do wielu różnych sposobów, w jakie ludzie mogą komunikować się w sieci WWW.

Narzędzia komunikacji internetowej używane w celach zawodowych i prywatnych:

- poczta e-mail,
- serwisy społecznościowe (Facebook, Twitter, Instagram, Linkedin, Goldenline, YouTube),
- komunikatory (Messenger, Hangouts, WhatsApp, Skype, Teams)
- blogi
- fora internetowe
- usługi chmurowe.

Właściwa komunikacja w Internecie

Pamiętaj, że korzystając z internetu zostawiasz za sobą tzw. “ślad cyfrowy”.

To co robimy w sieci pokazuje kim jesteśmy, czym się zajmujemy, z kim się komunikujemy, jak spędzamy wolny czas, jakie mamy zainteresowania, co nam się podoba. Te dane są wykorzystywane między innymi przez reklamodawców, w celu skutecznej promocji i sprzedaży swoich produktów i usług.

Ślad cyfrowy

Ślad cyfrowy dzieli się na dwa rodzaje informacji:

- informacje, które można uzyskać o użytkowniku Internetu na podstawie adresu IP (Internet Protocol Address- numer identyfikacyjny nadawany komputerom lub innym urządzeniom łączącym się z siecią, który zapewnia im prawidłową komunikację. posiada go każdy komputer), na jego podstawie można ustalić adres, pod którym znajduje się urządzenie, a także system operacyjny, zestaw zainstalowanych czcionek i ustawienia przeglądarek internetowych.

- informacje na temat ruchu w cyberprzestrzeni - czas spędzony w internecie, odwiedzane strony, zapytania w wyszukiwarkach, dane osobowe, które podałeś na stronach internetowych, informacje, które umieszczasz w portalach społecznościowych. Ciasteczka (tzw. „cookies”) pozwalają serwerom stron śledzić twoją aktywność w sieci.

Dane o użytkownikach są przechowywane ze względu na: bezpieczeństwo publiczne, badania rynku i efektywne administrowanie stron www, reklamy.

Dyrektywa Unii Europejskiej „o retencji danych telekomunikacyjnych” dopuszczalny maksymalny okres przechowywania danych przez operatorów przez okres 2 lat.

Ślad cyfrowy

Przejdźmy teraz do Ćwiczenia numer 1

Znajdź siebie w Internecie

Właściwa komunikacja w Internecie

Zapamiętaj te dwie reguły:

1. W sieci nie jesteś anonimowy - zostawiasz za sobą ślad cyfrowy.

1. Co raz trafi do Internetu może zostać tam na zawsze - serwisy internetowe tworzą rejestry, inni użytkownicy mogą zapisać umieszczone przez Ciebie informacje w formie zrzutu ekranu lub kopii strony.

Twoje działanie w Internecie może być później wykorzystane przez urzędy i służby państwowe, szkoły, pracodawców.

Zadbaj o swój pozytywny ślad cyfrowy

1. Pomyśl, zanim opublikujesz

Zanim opublikujesz treści online, np. zdjęcie, aktualizację statusu, zastanów się, czy chciałbyś, aby przyszli pracodawcy, uniwersytety, nauczyciele?

1. Zachowaj pozytywne nastawienie:

- Załóż bloga
- Stwórz stronę sponsorską i zbieraj pieniądze na cele charytatywne
- Stwórz i opublikuj film, aby nauczyć innych nowych umiejętności
- Publikuj zdjęcia rzeczy, które lubisz robić.

1. Dezaktywuj lub usuń stare profile

Jeśli nie korzystasz już ze swojego profilu na stronie internetowej, portalu społecznościowym lub aplikacji, upewnij się, że go dezaktywujesz. Dezaktywacja profilu spowoduje, że zawartość na nim nie będzie już dostępna do wyszukiwania. Nie będziesz mieć dostępu do usuniętego konta, a treści na nim nie będzie już można przeszukiwać. Nie ma również ryzyka włamania się na to konto bez Twojej wiedzy.

Netykieta

Netykieta to zbiór zasad pozwalający na kulturalną komunikację w cyberprzestrzeni.

Należy pamiętać, że poza zasadami netykiety obowiązują nas powszechne zasady kulturalnego zachowania.

Netykieta dla grup i list dyskusyjnych

- nie używaj wulgaryzmów;
- nie spamuj (m.in. nie wysyłaj niechcianych linków do stron);
- nie wysyłaj tzw. “ łańcuszków szczęścia”;
- zanim zadasz pytanie sprawdź czy w FAQ (zbiór najczęściej zadawanych pytań i odpowiedzi do nich) nie ma już takiego pytania;
- pisz wyłącznie na temat;
- nie pisz całej wiadomości wielkimi literami;
- nie trolluj i nie prowokój kłótni.

Netykieta dla usług interaktywnych (komunikatory, czaty, fora dyskusyjne na stronach WWW)

- korzystaj z funkcji „Szukaj” na forach, przed założeniem nowego wątku (sprawdź czy temat/problem nie był już omawiany);
- zapoznaj się z regulaminem dla danego kanału/forum/czatu
- nie nagabuj osób, które sobie tego nie życzą;
- nie pisz ciągle wielkimi literami;
- nie nadużywaj emotikon z rozwagą (mają być dodatkiem do tekstu, a nie główną treścią);
- w dyskusjach zwracaj się po nicku lub imieniu, jeśli rozmówca wyraża na to zgodę.

Netykieta w korespondencji elektronicznej (e-maile)

- stwórz odpowiedni adres swojego maila, nie używaj nazw, które mogą źle się kojarzyć lub być obraźliwe;
- jeżeli wysyłasz wiadomości do dużej, zwłaszcza nieznającej się grupy osób adresy odbiorców należy umieszczać w polu Ukryte do wiadomości;
- stosuj wszelkie zasady języka polskiego;
- załączniki o dużym rozmiarze kompresuj specjalnym programem (WinZip, 7Zip), bądź udostępniaj w chmurze;
- stosuj poprawne zwroty, nie używaj na powitanie zwrotu “Witam!”. Poprawne formy to takie, które odnoszą się do adresata, uznające typ relacji i stopień zażyłości, np. Szanowny Panie, Pani Prezes, Droga Barbaro, Cześć, Kochana.
- nadaj swojej wiadomości konkretny temat, żeby można było łatwo domyśleć się o na jaki temat będzie korespondencja i żeby można było ją łatwo w przyszłości odnaleźć;
- podpisz się pod wiadomością, w korespondencji służbowej;
- zawsze odpowiadaj na maile.

Netykieta

Przejdźm teraz do Ćwiczenia numer 2

Poprawna komunikacja z użytkownikami

Ochrona danych i prywatność w sieci

Każdy człowiek ma prawo do prywatności — obszaru, w który bez pozwolenia nie wolno wkraczać.

Istnieje kilka sfer prywatności:

- cielesna - związana z Twoją fizycznością
- terytorialna - związana z Twoją przestrzenią
- informacyjna - związana z informacjami na Twój temat np. medycznymi
- komunikacyjna - związana z Twoim komunikowaniem się z otoczeniem np. rozmowa, korespondencja pisana.

Ochrona danych i prywatność w sieci

Twoją prywatność chroni prawo.

Zapisy o ochronie prywatności znajdują się w:

- Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności: „Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji” (art. 8)
- Konstytucji RP z 1997 r.: „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym” (art. 47)
- Rozporządzeniu Parlamentu Europejskiego o ochronie danych osobowych.
- Ustawie o ochronie danych osobowych z 10 maja 2018 r.

Ochrona danych i prywatność w sieci

Dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania żyjącej osoby fizycznej.

Przykładowe dane osobowe:

- imię i nazwisko;
- wizerunek
- adres zamieszkania;
- adres e-mail, taki jak imię.nazwisko@firma.com;
- numer dowodu tożsamości;
- dane o lokalizacji;
- adres IP;
- identyfikator plików cookie;
- dane przechowywane przez szpital lub lekarza, które mogą jednoznacznie wskazywać tożsamość danej osoby.

Do danych osobowych nie zalicza się na przykład: numeru KRS; nieimiennego adresu e-mail (np. bok@firma.com).

Ochrona danych i prywatność w sieci

Do danych osobowych szczególnie chronionych, które mogą być przetwarzane tylko przez specjalne podmioty w wyjątkowych sytuacjach należą informacje: o pochodzeniu rasowym lub etnicznym; o poglądach politycznych, przekonaniach religijnych lub filozoficznych; o przynależności wyznaniowej, partyjnej lub związkowej; o stanie zdrowia; o kodzie genetycznym; o nałogach; o życiu seksualnym oraz informacje dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Ochrona danych i prywatność w sieci

Przejdźmy do Ćwiczenia numer 3

Jakie dane możemy przekazywać różnym podmiotom świadczącym usługi w cyberprzestrzeni.

Ochrona danych i prywatność w sieci

Przetwarzanie danych osobowych jest możliwe

- gdy przedsiębiorstwo lub organizacja zawarły z Tobą umowę – np. na dostawę towaru lub świadczenie usług (tj. gdy robisz zakupy przez internet) lub umowę o pracę
- gdy wypełniają one swoje zobowiązania prawne – na przykład jeżeli prawo wymaga przetwarzania Twoich danych, kiedy Twój pracodawca przekazuje informacje na temat Twojego miesięcznego wynagrodzenia do zakładu ubezpieczeń społecznych, aby zapewnić Ci ubezpieczenie społeczne
- gdy przetwarzanie danych leży w Twoim żywotnym interesie – np. może chronić Twoje życie
- w celu wykonania zadania w interesie publicznym – przede wszystkim w związku z realizacją zadań organów administracji publicznej takich jak szkoły, szpitale czy urzędy gminy
- jeżeli istnieje uzasadniony interes – np. jeżeli bank wykorzystuje Twoje dane osobowe, żeby sprawdzić, czy kwalifikujesz się do posiadania konta oszczędnościowego z wyższym oprocentowaniem

W pozostałych sytuacjach przed zgromadzeniem lub ponownym wykorzystaniem Twoich danych osobowych firma lub organizacja musi **zapytać Cię o zgodę**.

Ochrona danych i prywatność w sieci

Zgody na przetwarzanie danych osobowych musi być:

- dobrowolna - masz wolny wybór i w dowolnym czasie możesz wycofać zgodę;
- konkretna - musi być określony cel przetwarzania Twoich danych i ich zakres;
- świadoma - powinieneś znać tożsamość administratora oraz cele przetwarzania (powinien być spełniony obowiązek informacyjny);
- jednoznaczna - nie może być wątpliwości co do Twojej intencji wyrażenia zgody, w jasnym sposób muszą być ustawione opcje udzielania zgód.

Ochrona danych i prywatność w sieci

Pamiętaj, że w przypadku wysyłania newsletterów lub innego rodzaju reklam do użytkowników w polskim prawie wymagane są trzy rodzaje zgód:

- Zgodę na otrzymywanie drogą elektroniczną na wskazany powyżej adres e-mail informacji handlowych w rozumieniu Ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną o treści marketingowej pochodzących od firmy wysyłającej reklamy.
- Zgoda na wykorzystywanie przez firmę wysyłającą reklamy, telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla celów marketingu bezpośredniego w rozumieniu przepisów Ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne.
- Zgoda na przetwarzanie danych osobowych, podanych w formularzu, w celach marketingowych związanych z prezentacją aktualnej oferty firmy.

Ochrona danych i prywatność w sieci

Właściciel danych osobowych posiada prawo do:

- Informacji - kto gromadzi i przetwarza dane osobowe, wraz z ich wykorzystaniem, muszą być swobodnie dostępne i napisane jasnym, prostym językiem.
- Dostępu - osoby fizyczne mogą prosić o potwierdzenie, że ich dane są przetwarzane.
- Sprostowania - poprawienie wszelkich niekompletnych lub niedokładnych informacji, które są przetwarzane.
- Usunięcia - prawo do bycia zapomnianym, usunięcie danych gdy nie ma już uzasadnionego powodu, aby kontynuować jego przetwarzanie lub wycofana jest zgoda.
- Przenoszenia danych - umożliwia uzyskanie danych i ponowne wykorzystanie ich w innym celu i u innego Administratora.
- Sprzeciwu – prawo do sprzeciwu wobec przetwarzania jeżeli nie ma uzasadnionego powodu.
- Ochrony przed automatycznym podejmowaniem decyzji i profilowaniem. Zabezpieczenie przed wystąpieniem ryzyka podejmowania jakichkolwiek szkodliwych lub niekorzystnych decyzji bez możliwości interwencji człowieka lub możliwości uzyskania wyjaśnień.

Jak zabezpieczyć swoją prywatność w sieci

1. Przejrzyj i zabezpiecz swoje konta w mediach społecznościowych.
2. Jeżeli to możliwe ustaw podwójną autentykację do logowania się w usługach internetowych.
3. W różnych usługach używaj różnych haseł do logowania. Nie stosuj tych samych haseł w mediach społecznościowych, bankach, sklepach internetowych i forach. Pamiętaj, że każde z tych miejsc może mieć różne zabezpieczenia i Twoje dane mogą w łatwy sposób być wykradzione ze sklepu internetowego, a potem być wykorzystane do logowania się do wrażliwych dla Ciebie usług.
4. Jeżeli wszędzie używasz tych samych haseł, zmień je jak najszybciej w istotnych dla Ciebie usługach.

Jak zabezpieczyć swoją prywatność w sieci

5. Ostrożnie udostępniaj swoje dane. Zastanów się czy faktycznie są niezbędne do świadczonej dla Ciebie usługi. Jeżeli masz wątpliwości dopytaj o szczegóły dostawcę, jeżeli nie zostały rozwiane, lepiej zrezygnować z usługi.

6. Unikaj logowania się do usług na komputerach publicznych, możesz w łatwy sposób przekazać swoje dane osobom nieupoważnionym.

7. Unikaj korzystania z publicznych sieci WiFi. Cyberprzestępcy mogą tworzyć fałszywe punkty łączności, które pozwalają na dostęp do Twoich danych.

8. Twórz kopie zapasowe swoich danych.

9. Zawsze sprawdzaj jakich uprawnień dostępowych żąda od Ciebie instalowana aplikacja i czy są adekwatne do jej działania.

Jak zabezpieczyć swoją prywatność w sieci

10. Odinstaluj aplikacje, z których już nie korzystasz.

11. Wprowadzaj dane wyłącznie na szyfrowanych stronach internetowych (https, kłódka). Pamiętaj jednak, że takie zabezpieczenie nie daje gwarancji, że strona nie jest stworzona przez cyberprzestępców.

12. Nie przekazuj swoich danych poufnych telefonicznie, mailowo lub w komunikatorach. Zwłaszcza jeżeli to nie Ty inicjowałeś połączenie.

13. Nie publikuj poufnych i intymnych informacji na portalach społecznościowych.

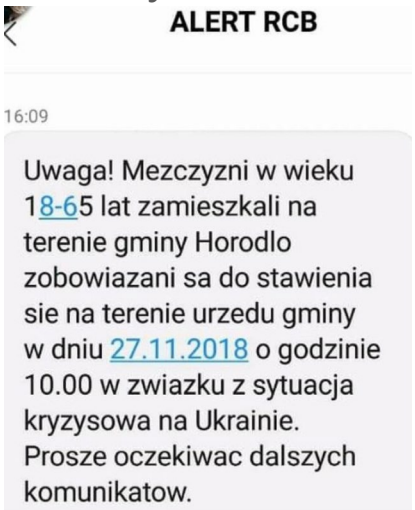
14. Nie klikaj na podejrzane linki w mailach i wiadomościach otrzymywanych na urządzenia mobilne.

15. Nie otwieraj załączników pochodzących z niezaufanych źródeł.

16. Jeżeli otrzymujesz prośbę od bliskiej Ci osoby o przelew środków pieniężnych na konto, zawsze sprawdź innym kanałem komunikacyjnym czy jest to prawda. Dzięki temu unikniesz wyłudzenia środków przez podszywające się pod Twoich bliskich osoby.

Wiarygodność informacji w sieci

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



BANKI GO NIENAWIDZĄ!
Zobacz jak zarobił $10 000 w jedno popołudnie używając jednej prostej sztuczki!

Jak upewnić się czy informacje są prawdziwe

Weryfikację wiarygodności informacji uzyskasz dzięki następującym działaniom:

- sprawdź autora opublikowanej informacji, czy jest to osoba godna zaufania, ekspert w swojej dziedzinie,
- sprawdź datę publikacji i czas działania określonego serwisu internetowego,
- sprawdź poprawności informacji, czy nie zawiera błędów językowych,
- przeczytaj całą treść, a nie tylko nagłówek,
- sprawdź inne źródła czy potwierdzają tę informację,
- porozmawiaj z osobami, którym temat jest znany i mają wiedzę na ten temat,
- zastanów się czy opublikowana informacja nie jest żartem

Unikaj rozpowszechniania niesprawdzonych informacji, żeby nie wzmacniać jej wiarygodności i nie spowodować paniki wśród bliskich Ci osób.

Na tej stronie możesz zgłosić podejrzenie fałszywej informacji i zweryfikować wiadomości, które są sprawdzane przez ekspertów: https://fakehunter.pap.pl/

Jak upewnić się czy informacje są prawdziwe

Przejdźmy do Ćwiczenia numer 4

Sprawdź wiarygodność informacji.

Prawo autorskie

Przedmiotem prawa autorskiego jest każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia (utwór).

W szczególności przedmiotem prawa autorskiego są utwory:

- wyrażone słowem, symbolami matematycznymi, znakami graficznymi (literackie, publicystyczne, naukowe, kartograficzne oraz programy komputerowe);
- plastyczne;
- fotograficzne;
- lutnicze;
- wzornictwa przemysłowego;
- architektoniczne, architektoniczno-urbanistyczne i urbanistyczne;
- muzyczne i słowno-muzyczne;
- sceniczne, sceniczno-muzyczne, choreograficzne i pantomimiczne;
- audiowizualne (w tym filmowe).

Prawo autorskie chroni twórcę automatycznie, bez konieczności spełniania jakichkolwiek formalności i obejmuje również utwory,, które nie zostały ukończone.

Prawo autorskie

Pamiętaj, że w Internecie prawo autorskie obowiązuje tak samo jak w świecie rzeczywistym.

Zgodnie z polską Ustawą z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych prawem autorskim nie są objęte:

- akty normatywne lub ich urzędowe projekty;
- urzędowe dokumenty, materiały, znaki i symbole;
- opublikowane opisy patentowe lub ochronne;
- proste informacje prasowe.

Prawo autorskie

W ramach prawa autorskiego wyróżniamy:

- autorskie prawa osobiste - nieograniczona w czasie i niepodlegająca zrzeczeniu się lub zbyciu więź twórcy z utworem, a w szczególności prawo do: autorstwa utworu, oznaczenia utworu swoim nazwiskiem lub pseudonimem albo do udostępniania go anonimowo, nienaruszalności treści i formy utworu oraz jego rzetelnego wykorzystania, decydowania o pierwszym udostępnieniu utworu publiczności, nadzoru nad sposobem korzystania z utworu.
- autorskie prawo majątkowe - twórcy przysługuje wyłączne prawo do korzystania z utworu i rozporządzania nim na wszystkich polach eksploatacji oraz do wynagrodzenia za korzystanie z utworu.

Prawo autorskie a wizerunek osoby

Wizerunek jest to podobizna konkretnej i rozpoznawalnej osoby przedstawiona za pomocą środków plastycznych - fotografii, filmu, portretu malarskiego czy rysunku.

Publikowanie i rozpowszechnianie wizerunku wymaga zgody od osoby, której podobizna jest uwieczniona.

Zgoda może być udzielana w dowolnej formie, jednak dla celów dowodowych najbezpieczniejsza jest forma pisemna.

UWAGA! Egzekwowanie prawa do ochrony wizerunku następuje wyłącznie po złożeniu stosownego wniosku przez osobę, której podobizna została opublikowana.

Prawo autorskie a wizerunek osoby

Zgodę osoby na publikację nie jest konieczna w sytuacji:

1. Kiedy osoba, której wizerunek jest rozpowszechniony otrzymała zapłatę za pozowanie i możliwość publikacji wizerunku..

2. Kiedy wizerunek należy do osoby powszechnie znanej i został sporządzony w związku z pełnieniem przez tę osobę funkcji publicznych.

3. Osoba na wizerunku stanowi jedynie szczegół całości, np. nie jest głównym tematem zdjęcia, jej brak nie ma wpływu na treść obrazu, jest jednym z uczestników masowej imprezy.

Prawo autorskie a wizerunek osoby

Przejdźmy do Ćwiczenia numer 5

Zgodność działań z prawem autorskim.

Bibliografia

https://biblioteka.womczest.edu.pl/new/wp-content/uploads/2013/09/webowa_biblioteka_informatyka_netykieta.pdf

Komunikacja językowa w Internecie, Jan Grzenia, Komunikacja językowa w Internecie, 2006

Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r.

Konstytucja Rzeczypospolitej Polskiej

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 (ogólne rozporządzenie o ochronie danych)

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych

https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_pl.htm

Fejk. Kłamstwa, w które wierzymy, Aristarco Daniele, Wydawnictwo RM, 2020

Ustawie z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych

Naruszenia praw autorskich w internecie. Aspekty prawne i procedury dochodzenia roszczeń, Magdalena Kowalczuk Szymańska, Olga Szteiner-Roszak, Difin, 2013

MODUŁ 4
Bezpieczeństwo finansów prywatnych i w miejscu pracy, bezpieczna bankowość internetowa oraz bezpieczne zakupy

Fundusze Europejskie
Wiedza Edukacja Rozwój

Rzeczpospolita Polska

Unia Europejska
Europejski Fundusz Społeczny

Czego dowiesz się z modułu 4

- Poznasz zagrożeniami dla bankowości internetowej
- Poznasz sposoby bezpiecznej pracy z bankowością internetową.
- Dowiesz się jak bezpiecznie kupować w sieci.

W trakcie szkolenia z modułu czwartego:

- Zapoznasz się z teorią
- Poznasz przykłady praktyczne
- Wykonasz ćwiczenia

Wprowadzenie

Bankowość elektroniczna (ang. e-banking) są to usługi oferowane przez banki, polegające na udostępnieniu do rachunku za pomocą urządzenia elektronicznego: komputera, bankomatu, terminalu POS, telefonu (zwłaszcza telefonu komórkowego), Internetu.

W bankowości elektronicznej możliwe są do wykonania operacje pasywne (np. sprawdzanie salda i historii rachunku) oraz aktywne (np. dokonanie polecenia przelewu, założenie lokaty terminowej).

Rodzaje zagrożeń w bankowości elektronicznej

- Wyłudzenia danych pozwalających na przeprowadzenie transakcji (phishing).
- Kradzieże z wykorzystaniem złośliwego oprogramowania.
- Kopiowanie kart płatniczych (skimming).
- Kradzieże związane z kartami zbliżeniowymi
- Kradzieże przy użyciu danych karty płatniczej
- Zagrożenia związane z płatnościami mobilnymi.
- Kradzież tożsamości.
- “Przekręty nigeryjskie”.
- Kradzieże w sklepach internetowych

Przykłady działań przestępczych

Wyłudzenie danych do logowania w trakcie połączenia telefonicznego z banku.

Przestępcy kontaktują się telefonicznie z właścicielami kont w celu uzyskania danych do logowania prezentując nową korzystną ofertę lub informując o konieczności podjęcia działań.

Zapamiętaj! Banki nigdy nie proszą o podawanie żadnych danych logowania do bankowości internetowej (loginów, haseł, kodów jednorazowych z tokenów czy SMS-ów , drogą telefoniczną lub mailową. Dane do logowania podaje się wyłącznie w internetowych serwisach bankowych lub aplikacjach banku zainstalowanych na urządzeniach mobilnych)

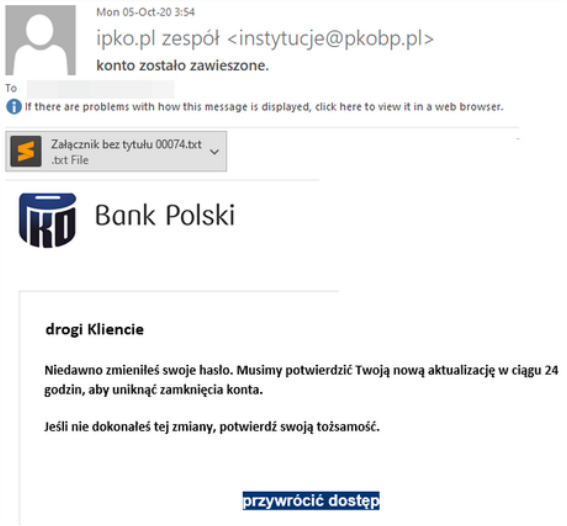
Przykłady działań przestępczych

Wyłudzenie danych do logowania w trakcie połączenia telefonicznego z banku.

Przestępcy kontaktują się telefonicznie z właścicielami kont w celu uzyskania danych do logowania prezentując nową korzystną ofertę lub informując o konieczności podjęcia działań.

Zapamiętaj! Banki nigdy nie proszą o podawanie żadnych danych logowania do bankowości internetowej (loginów, haseł, kodów jednorazowych z tokenów czy SMS-ów , drogą telefoniczną lub mailową. Dane do logowania podaje się wyłącznie w internetowych serwisach bankowych lub aplikacjach banku zainstalowanych na urządzeniach mobilnych)

Przykłady działań przestępczych



Mon 05-Oct-20 3:54

ipko.pl zespół <instytucje@pkobp.pl>

konto zostało zawieszone.

To

If there are problems with how this message is displayed, click here to view it in a web browser.

Załącznik bez tytułu 00074.txt
.txt File

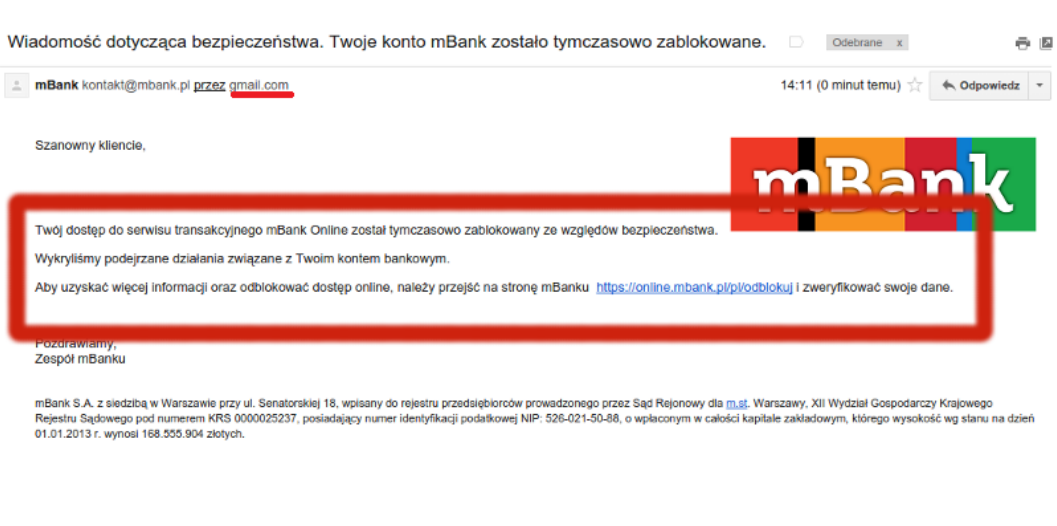
Bank Polski

drogi Kliencie

Niedawno zmieniłeś swoje hasło. Musimy potwierdzić Twoją nową aktualizację w ciągu 24 godzin, aby uniknąć zamknięcia konta.

Jeśli nie dokonałeś tej zmiany, potwierdź swoją tożsamość.

przywrócić dostęp



Wiadomość dotycząca bezpieczeństwa. Twoje konto mBank zostało tymczasowo zablokowane.

Odebrane x

mBank kontakt@mbank.pl przez gmail.com

14:11 (0 minut temu)

Odpowiedz

Szanowny kliencie,

mBank

Twój dostęp do serwisu transakcyjnego mBank Online został tymczasowo zablokowany ze względów bezpieczeństwa.

Wykryliśmy podejrzane działania związane z Twoim kontem bankowym.

Aby uzyskać więcej informacji oraz odblokować dostęp online, należy przejść na stronę mBanku https://online.mbank.pl/pl/odblokuj i zweryfikować swoje dane.

Pozdrawiamy,
Zespół mBanku

mBank S.A. z siedzibą w Warszawie przy ul. Senatorskiej 18, wpisany do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m.st. Warszawy, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000025237, posiadający numer identyfikacji podatkowej NIP: 526-021-50-88, o wpłaconym w całości kapitale zakładowym, którego wysokość wg stanu na dzień 01.01.2013 r. wynosi 168.555.904 złotych.

Przykłady działań przestępczych

From: Bank Zachodni WBK
Subject: **Important Notification from BZWBK24 Internet Banking**
Date: 24 marca 2008 07:57:51 GMT+01:00
To: Undisclosed-Recipient:
Reply-To: tfvqro@google.pl

Zbiorczy odbiorca maila, nie jest adresowany do Ciebie

Adres e-mail nie związany z bankiem

Bank Zachodni WBK

Dear Bank Zachodni WBK customer,

We recently reviewed your account, and suspect that your BZWBK Internet Banking account may have been accessed from an unauthorized computer. This may be due to changes in your IP address or location. Protecting the security of your account and of the Bank Zachodni WBK network is our primary concern.

We are asking you to immediately login and report any unnoticed password changes, unauthorized withdrawals or deposits, and check you account profile to make sure no changes have been made.

Please click the following link, to verify your account activity:

https://www.centrum24.pl/bzwbkonline/eSmart.html?typ=13 〈=en

We apologize for any inconvenience this may cause, and appreciate your assistance in helping us maintaining the integrity of the entire Bank Zachodni WBK system. Please login as soon as possible.

Thank you,
Bank Zachodni WBK Security Advisor.

Masz nowa wazna wiadomosc

PKO Bank Polski [gegfd@kiraplastininastyle.kz]
21 sierpnia 2013 13:23

Adres nie należący do banku

Brak polskich znaków

Bank Polski

Masz 1 nowa wazna wiadomosc.

Aby przeczytac wiadomosc, kliknij na link ponizej i zaloguj sie:
https://www.ipko.pl

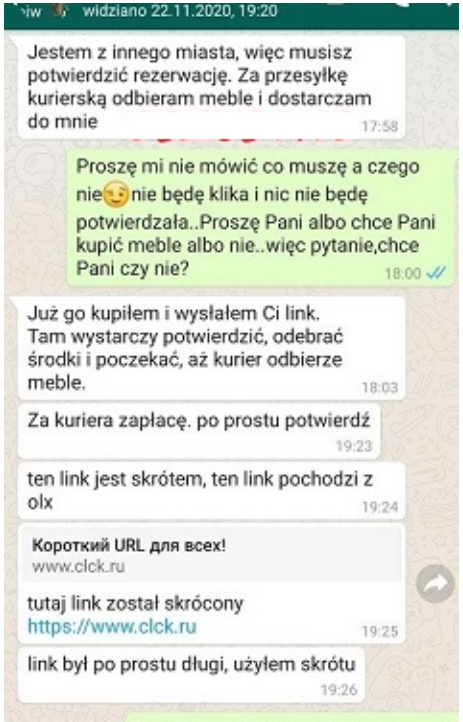
© 2013 PKO Bank Polski

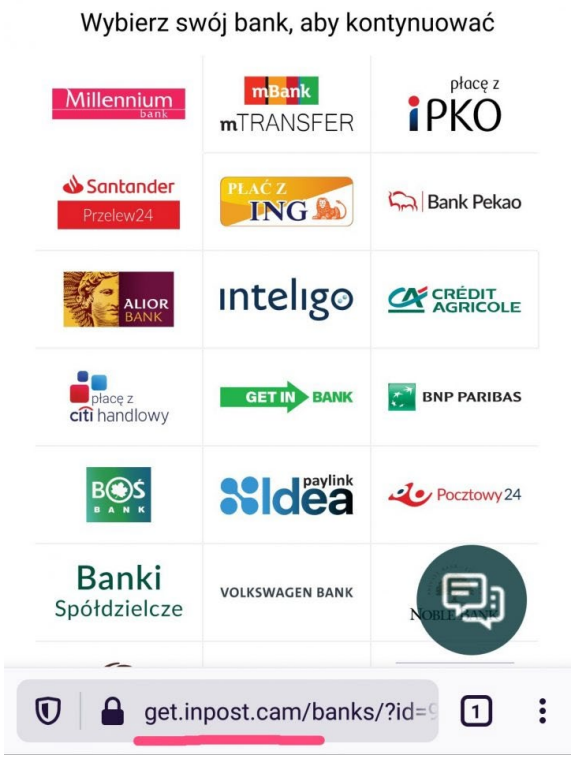
Przykłady działań przestępczych

Kopiowanie kart płatniczych (skimming) – polega na skopiowaniu danych znajdujących się na pasku magnetycznym karty płatniczej podczas korzystania z bankomatu. Przestępcy instalują specjalną nakładkę na wlot karty płatniczej który skanuj dane zapisane na pasku magnetycznym. PIN do karty wykradają przy użyciu miniaturowych kamer umieszczonych nad klawiaturą bankomatu lub fałszywej klawiaturze montowanej na oryginalnym urządzeniu.

Przykłady działań przestępczych - wyłudzenia płatności

Na dzień 10.07 zaplanowano odłączenie energii elektrycznej! Prosimy o uregulowanie należności 3.46 zł. Zapłać teraz na: https://[redacted]





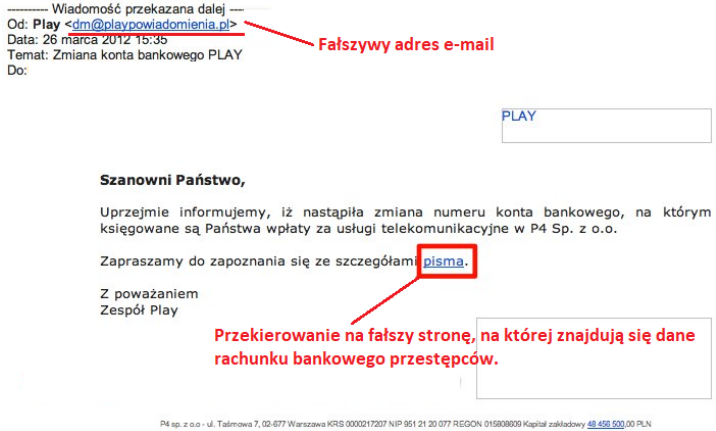
Przykłady działań przestępczych - wyłudzenia płatności

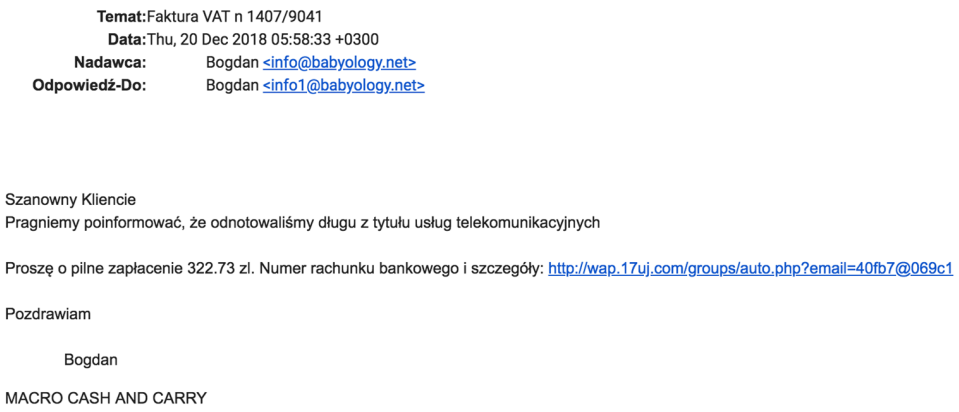
Przejdźmy do Ćwiczenia numer 1

Rozpoznawanie fałszywych wiadomości

Przykłady działań przestępczych - wyłudzenia płatności na zmianę rachunku

Uważaj na maile informujące o zmianie rachunku bankowego na płatności za usługi dostawcy. Przestępcy podszywają się pod znanych Ci usługodawców i podają swoje konto do przelewów.





Pamiętaj, żeby każdą prośbę o zmianę konta do przelewu płatności potwierdzić z wystawcą faktury telefonicznie.

Przykłady działań przestępczych - przekręt nigeryjski

Wiadomość przypomina automatyczne tłumaczenie z języka obcego (nieskładna pisownia w języku polskim) i zawiera prośbę o podanie danych niezbędnych do dokonania przelewu środków finansowych, np. w zamian za towar lub usługę (może to nosić znamiona prania pieniędzy) albo prosi o przelanie środków na numer rachunku osoby pochodzącej z innego kraju, najczęściej z Afryki.

Często proponowany nam jest przelew dużych kwot, których nadawca nie może bezpiecznie wywieźć ze swojego kraju.

UWAGA! Pojawiają się również wyłudzenia matrymonialne. Przestępcy próbują nawiązać romans, a następnie wyłudzić środki pieniężne na różne potrzeby związane z naszym kontaktem np. bilet lotniczy, który umożliwi przylot i spotkanie w świecie realnym.

Oszuści matrymonialni mogą podawać się np. amerykańskiego żołnierza, bogatego wdowca z Włoch, syryjskiego medyka.

Jak się chronić przed przestępcami

- Nie podawaj danych logowania do bankowości elektronicznej przez e-mail/telefon. Bank nigdy nie prosi klienta o login i hasło do konta internetowego ani telefonicznie, ani mailowo. Listy, wiadomości e-mail lub telefony w takich sprawach należy traktować jako próbę wyłudzenia poufnych informacji. Nie odpowiadaj na nie przekazując swoje poufne dane. Bezzwłocznie skontaktuj się ze swoim Bankiem i poinformuj o zdarzeniu.
- Wszystkie urządzenia, na których korzystamy z bankowości elektronicznej powinny mieć zainstalowane legalne oprogramowanie, które okresowo jest aktualizowane, programy antywirusowe,
- Nie otwieraj podejrzanych e-maili i załączników – wiadomości i pliki z nieznanych źródeł to potencjalne zagrożenie nie tylko dla komputerów i danych użytkownika. Usuń niezwłocznie podejrzany mail.
- Wprowadzaj ręcznie adresy stron internetowych usługodawców. Dzięki temu masz pewność, że logujesz się na właściwe konto.
- Sprawdzaj datę ostatniego logowania do bankowości elektronicznej.
- Używaj silnych, unikalne hasło do konta (hasło nie powinno składać się z wyrazów słownikowych, składać z co najmniej 8 znaków i zawierać wielkie i małych liter, cyfr i znaków specjalnych.
- Nie zapisuj nigdzie haseł służących do logowania.
- Nie używaj tych samych haseł w różnych usługach. W razie wycieku Twoich danych u jednego dostawcy, Twoje pozostałe usługi są bezpieczne.
- W przypadku podejrzenia utraty hasła zmień je jak najszybciej..

Jak się chronić przed przestępcami

- Dokładnie czytaj SMS autoryzacyjne, sprawdź czy na pewno zatwierdzasz zlecenie, które złożyłeś do banku - nazwę i kwotę operacji oraz numer rachunku odbiorcy.
- Unikaj z korzystaj z publicznych sieci WI-FI – mogą być udostępniane pod fałszywą nazwą przez przestępców lub słabo zabezpieczone przez administratora sieci.
- Korzystaj z zaufanych sklepów internetowych – dokonuj transakcji w znanych i zweryfikowanych przez siebie sklepach internetowych. W przypadku mniejszych serwisów zbadaj ich wiarygodność, na przykład dzwoniąc do takiego serwisu i weryfikując jego ofertę, warunki dokonania transakcji oraz reklamacji.
- Włącz powiadomienia SMS na temat operacji wykonywanych na Twoich koncie. W przypadku podejrzanych operacji będziesz mógł szybko zareagować.
- Ustaw limity dla transakcji kartami płatniczymi dzięki temu w przypadku utraty karty stracisz mniej środków.
- Na telefonie instaluj tylko zaufane aplikacje - sprawdzaj uprawnienia i liczbę pobrań.
- Chroń swoje dane osobowe – nasze dane osobowe to skarb i powinniśmy je chronić za wszelką cenę. Uważaj, komu podajesz adres, telefon czy numer dowodu osobistego.
- Dokumenty papierowe zawierające Twoje dane osobowe i bankowe niszcz w sposób nie pozwalający na ich odczytanie: niepotrzebne rachunki, faktury, pisma z banków itd.

Bezpieczne zakupy w sieci

Fałszywe sklepy internetowe to ataki, które mają na celu wyłudzić dane osobowe lub okraść ofiarę z pieniędzy.

Miesięcznie powstaje kilkaset fałszywych sklepów powstaje kilkaset.

Link do fałszywego sklepu może się pojawić w mediach społecznościowych, wiadomości SMS lub na komunikatorze.

Możesz również trafić na reklamę takiego sklepu na poczytnym portalu internetowym, na zaufanym blogu lub serwisie internetowym.

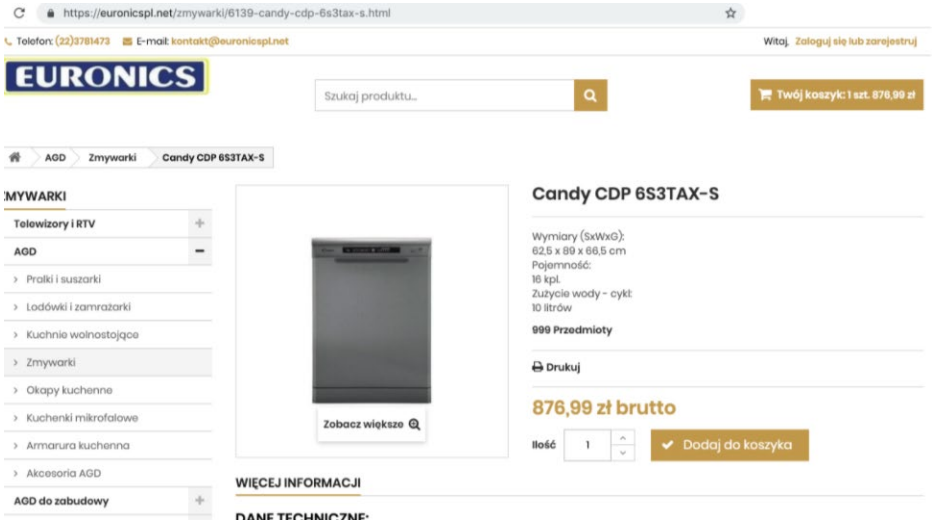
Cyberprzestępca mogą wykupić reklamę swojego fałszywego sklepu praktycznie wszędzie. Takie płatne ogłoszenia nie są w większości wypadków weryfikowane przez właścicieli stron.

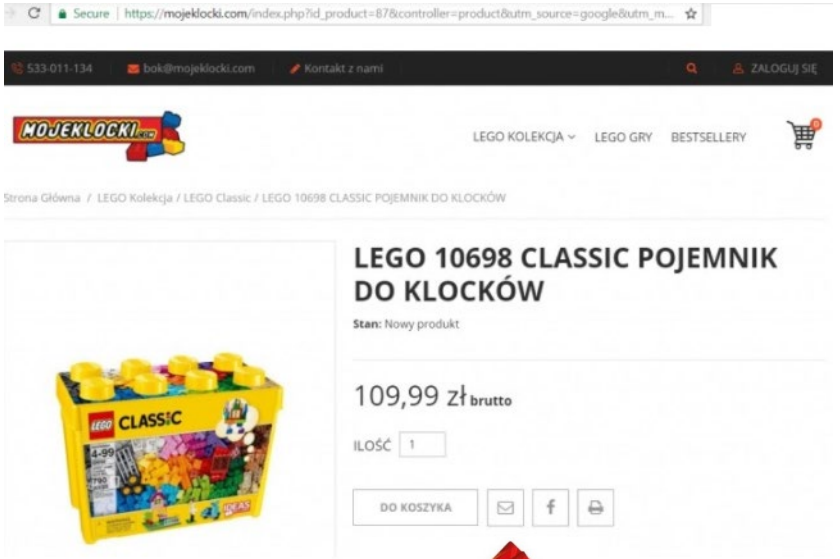
Czasem informacja o sklepie może trafić do Ciebie od Twojego znajomego, któremu przejęto konto na Facebooku.

Przestępcy kuszą ofertą, którą jest bardzo atrakcyjna dla kupującego..

Fałszywe sklepy oferują najczęściej markowe produkty (np. sprzęt elektroniczny) w bardzo okazyjnych cenach. Stosują przy tym sztuczki, które mają skłonić Cię do szybkiego złożenia zamówienia, aby skorzystać z okazji. A gdy już to zrobisz… możesz stracić oszczędności swojego życia.

Fałszywe sklepy - przykłady ataków

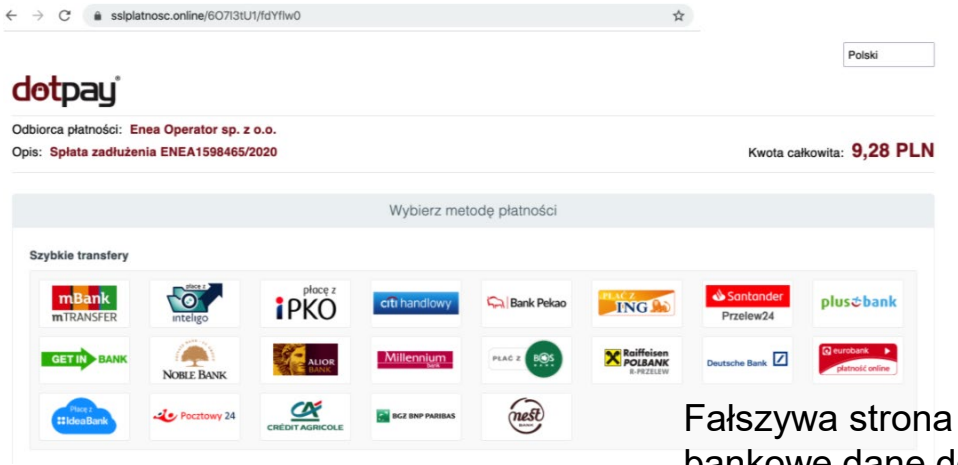




Fałszywe sklepy - jakie ryzyko niosą ze sobą

Nie otrzymasz zamówionego towaru i stracisz tylko wpłacone pieniądze.

Możesz również nie otrzymać zamówionego towaru, a przestępcy okradną Twoje konto ze wszystkich środków, które na nim się znajdowały.



Fałszywa strona do płatności wyłudzająca bankowe dane do logowania

Przykłady ataków - fałszywe sklepy

Przejdźmy do Ćwiczenia numer 2

Sprawdzanie wiarygodności sklepu internetowego.

Jak nie dać się oszukać. Sprawdź sklep!

- Zweryfikuj dane firmy - nazwę, NIP, adres firmy - powinny być w zakładce kontakt, w regulaminie sklepu i polityce prywatności. Dane możesz porównać w Centralnej Ewidencji i Informacji o Działalności Gospodarczej https://prod.ceidg.gov.pl/CEIDG/CEIDG.Public.UI/Search.aspx lub Krajowym Rejestrze Sądowym https://ekrs.ms.gov.pl/web/wyszukiwarka-krs/strona-glowna/ .
- Sprawdź czy sklep ma regulamin, zapoznaj się z jego zapisami, porównaj je z ofertą opublikowaną przy ogłoszeniu - czas dostawy, formy płatności i wysyłki. Jeżeli sklep nie ma regulaminu lub jest napisany niepoprawną polszczyzną zrezygnuj z zakupów.

Jak nie dać się oszukać. Sprawdź sklep!

- Sprawdź opinie w internecie na temat sklepu (zwracaj uwagę na liczbę opinii, daty ich wystawienia). Jeżeli sklep nie ma opinii w internecie powinno to wzbudzić Twoją czujność. Najlepiej wyszukać opinie w wyszukiwarce internetowej wpisując hasło: „nazwa sklepu + opinie” lub „adres sklepu + opinie”.
- Sprawdź czy jest opcja płatności za pobraniem, nawet jeżeli nie chcesz tak realizować płatności. Fałszywe sklepy najczęściej oferują tylko płatność przed wysyłką.
- Sprawdź na portalach społecznościowych czy sklep ma swój profil, jeżeli tak zobacz co piszą o nim inni klienci.

Jak nie dać się oszukać. Sprawdź sklep!

- Skontaktuj się ze sklepem telefonicznie lub mailowo. Brak możliwości skontaktowania się lub unikanie kontaktu powinno wzbudzić Twoją czujność.
- Możesz sprawdzić listę podejrzanych sklepów lub zweryfikować czy nie sprzedają podrabianych towarów dostępną na stronie: https://www.legalniewsieci.pl/aktualnosci/podejrzane-sklepy-internetowe

UWAGA! Przestępcy wysyłają również niezamówione “towary” za pobraniem korzystając z prawdziwych usług kurierskich. W przesyłce znajdują się bezużyteczne rzeczy lub śmieci.

Uczul swoich bliskich, żeby zawsze weryfikowali z Tobą telefonicznie czy faktycznie była zamawiana przesyłka.

Fałszywa aplikacja mobilna

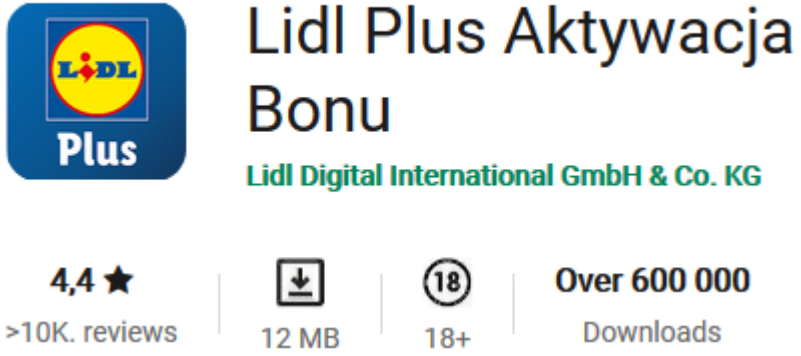
Możesz otrzymać wiadomość SMS lub e-mail z prośbą o pobranie fałszywej aplikacji.

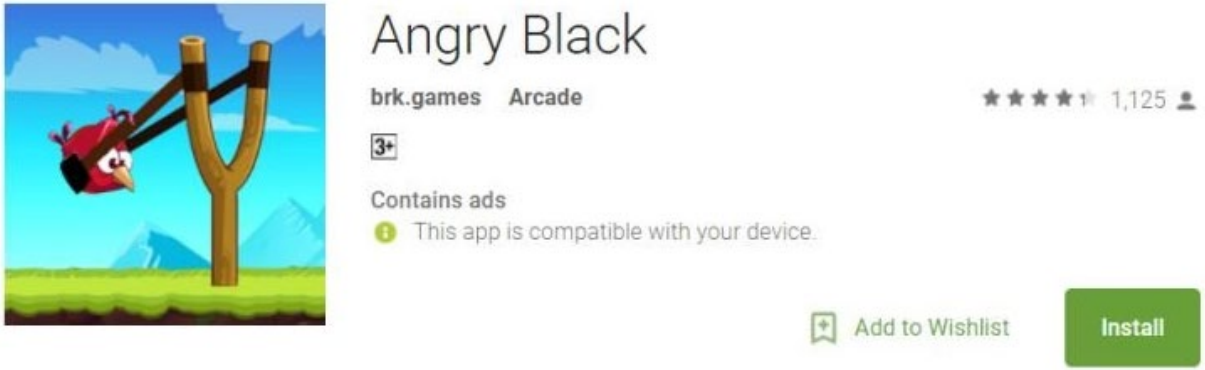
Jeżeli ja zainstalujesz zainfekujesz swój telefon szkodliwym oprogramowaniem.

Podczas instalacji taka aplikacja prosi o nadanie uprawnień „ułatwienia dostępu” lub administratora urządzenia, w celu przejęcie kontroli nad urządzeniem. Następnie wirus wykrada dane do logowania do bankowości mobilnej lub dane Twoich kart.

Fałszywe aplikacje mogą podszywają się pod bankowość mobilną, gry lub narzędzi na telefon. Cel jest jeden – zainfekowanie urządzenia

Fałszywe aplikacje - przykłady





Fałszywa aplikacja mobilna - jak się chronić

- Nie instaluj aplikacji z linków nadesłanych SMS-em, poprzez komunikatory czy też pocztę elektroniczną.
- Sprawdzaj jakie uprawnienia chce uzyskać aplikacja.
- Sprawdzaj liczbę pobrań. Fałszywe aplikacje będą miały ich niewiele.
- Zawsze sprawdzaj kto jest twórcą aplikacji.
- Zapoznaj się z opiniami innych użytkowników sklepu.
- Sprawdź nazwę czy nie zawiera błędów i nie plagiatuje nazw znanych aplikacji.
- Zapoznaj się z regulaminem usługi i licencjami.

Fałszywa aplikacja mobilna - jak się chronić

- Uważaj na programy, które chcą pobierać pliki z nieznanych źródeł.
- Jeśli cokolwiek wyda Ci się podejrzane nie instaluj aplikacji. Jeżeli jzostała zainstalowana to jak najszybciej ją odinstaluj i skontaktuj się z bankiem w celu ochrony Twojego konta.
- Sprawdzaj regularnie listę zainstalowanych aplikacji w ustawieniach telefonu i usuwaj te, których nie znasz - fałszywe aplikacje często działają „w tle”.

Fałszywa aplikacja mobilna

Przejdźmy do Ćwiczenia numer 3

Sprawdzanie wiarygodności aplikacji w sklepie Google Play

Jak bezpiecznie płacić za zakupy

Najlepiej w internecie płacić:

- kartą (dzięki procedurze chargeback możesz odzyskać pieniądze, które zapłaciłeś za zamówiony towar)
- przy odbiorze (za pobraniem) możesz zazwyczaj sprawdzić przed opłatą czy faktycznie otrzymałeś zamówiony towar.

UWAGA! Zazwyczaj w fałszywych sklepach internetowych te metody płatności są niedostępne.

Bezpieczne zakupy - procedura chargeback

Z procedury chargeback możesz skorzystać gdy:

- nie otrzymasz produktu lub usługi, za którą była płatność
- produkt lub usługa będą odbiegały od tego, co obiecywał sprzedawca lub np. towar przyjdzie uszkodzony czy niekompletny
- dokonasz zwrotu lub odstąpisz od umowy, a sprzedawca mimo to obciąży Cię płatnością lub nie będzie chciał zwrócić pieniędzy
- wystąpią błędy podczas wykonywania transakcji np. pobrana zostanie błędna kwota, odmowa autoryzacji, podwójna płatność, bankomat nie wyda pieniędzy itd.
- zostaniesz oszukany a karta zostanie obciążona bez Twojego udziału i zgody.

Bibliografia

https://zbp.pl/dla-klientow/bezpieczne-bankowanie/bankowosc-internetowa

Bankowość elektroniczna. Istota i innowacje, Andrzej Gospodarowicz, C.H. Beck, 2018

Bankowość bez tajemnic, Małgorzata Zalewska, Difin 2016

Informacja w Internecie, Karciarz Magdalena , Dutko Maciej, Wydawnictwo Naukowe PWN

Bezpieczeństwo systemu e-commerce, czyli jak bez ryzyka prowadzić biznes w internecie, Leszek Kępa, Paweł Tomasik, Sebastian Dobrzyński, Helion, 2012

https://www.knf.gov.pl/knf/pl/komponenty/img/REKOMENDACJA_dot_bezpieczenstwa_transakcji_platniczych_43526.pdf

BĄDŹ BEZPIECZNY W SIECI

BĄDŹ ŚWIADOMY

Rozsądnie korzystaj z cyberprzestrzeni.

Dbaj o bezpieczeństwo swoje i bliskich.

Zachowaj zasadę ograniczonego zaufania do nieznanych Ci osób w sieci.

Ostrożnie dziel się informacjami na swój temat w sieci.

Znaj swoje prawa.

BĄDŹ POZYTYWNY

Współtwórz bezpieczną i kulturalną cyberprzestrzeń.

Pamiętaj, że w sieci nie jesteś anonimowy.

Korzystaj w sposób legalny z sieci, nie nadużywaj jej zasobów

Dziel się wiedzą na temat zagrożeń z innymi.

Zgłaszaj incydenty by chronić innych.

Poszerzaj swoją wiedzę.

Fundusze Europejskie Wiedza Edukacja Rozwój
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Społeczny

BĄDŹ BEZPIECZNY W SIECI

BĄDŹ OSTROŻNY

Stosuj bezpiecznie urządzenia.

Chroń swoją prywatność.

Uważnie czytaj informacje.

W razie wątpliwości sprawdzaj u źródła wiarygodność informacji otrzymywanych drogą elektroniczną.

Nie wierz we wszystko co czytasz w sieci.

BĄDŹ SPRYTNY

Nie otwieraj załączników z podejrzanych wiadomości

Nie klikaj w linki pochodzące z niezaufanych źródeł.

Stosuj silne hasła.

Jeżeli to możliwe stosuj podwójne logowanie do usług.

Nie używaj tych samych haseł u różnych dostawców.

Fundusze Europejskie Wiedza Edukacja Rozwój
Rzeczpospolita Polska
Unia Europejska Europejski Fundusz Społeczny

BĄDŹ BEZPIECZNY W SIECI

BĄDŹ NOWOCZESNY

Korzystaj z chroniących cię technologii.

Korzystaj z programów antywirusowych.

Blokuj dostępy do swoich urządzeń.

Aktualizuj programy.

Korzystaj z usług chmurowych.

BĄDŹ DOKŁADNY

Sprawdzaj kto się z Tobą komunikuje w sieci.

Weryfikuj adresy mailowe i linki stron.

Adresy stron Twoich ważnych dostawców wprowadzaj ręcznie w przeglądarce.

Aplikacje pobieraj z zaufanych miejsc.