MODEL SZKOLENIA Z ZAKRESU CYBERBEZPIECZEŃSTWA

„Model powstał w ramach projektu "Cyberbezpieczeństwo w pracy i w domu" zrealizowanego w ramach finansowania z projektu Operatora Grantów – Grupa Profesja sp. z o.o. pt. „*Międzynarodowa współpraca się opłaca*. Granty na komponent współpracy ponadnarodowej dla beneficjentów projektów standardowych realizowanych w zakresie celów tematycznych 8-11 współfinansowanych z Europejskiego Funduszu Społecznego w ramach PO WER lub RPO w perspektywie finansowej 2014-2020.”

SPIS TREŚCI **STRONA**

Sesja 2. Bezpieczne usługi w sieci

CZĘŚĆ I

CYBERPRZEMOC I CYBERPRZESTĘPSTWA

SESJA 1

ZAGROŻENIA SPOŁECZNE I FIZYCZNE ZWIĄZANE Z INTERNETEM

Tematyka:

I. Internet – korzyści i zagrożenia
II. Uzależnienie od internetu
III. Negatywne treści i zachowania w internecie
IV. Zagrożenia fizyczne w cyberprzestrzeni

SESJA 2

TYPY OSZUSTW W CYBERPRZESTRZENI

Tematyka:

I. Socjotechnika a oszustwa internetowe
II. Rodzaje oszustw
III. Obrona przed oszustwami

CZĘŚĆ II

OCHRONA PRZED ATAKAMI

SESJA 1

KONTAKT I RELACJE Z UŻYTKOWNIKAMI INTERNETU

Tematyka:

I. Aktywność w sieci
II. Bezpieczeństwo i ochrona prywatności w sieci
III. Normy i zasady w relacjach z użytkownikami internetu

SESJA 2

BEZPIECZNA AKTYWNOŚĆ I WIZERUNEK W SIECI

Tematyka:

I. Wizerunek w serwisach społecznościowych
II. Prawo do ochrony wizerunku
III. Prywatność a cyfrowy ślad w sieci
IV. Wizerunek zawodowy

CZĘŚĆ III

BEZPIECZNE KORZYSTANIE Z KOMPUTERA W MIEJSCU PRACY

SESJA 1

CYBERBEZPIECZEŃSTWO - ZASADY POSTĘPOWANIA

Tematyka:

I. Cyberzagrożenia
II. Silne hasła podstawą bezpieczeństwa
III. Poczta elektroniczna
IV. Urządzenia mobilne
V. Zabezpieczenia sprzętu komputerowego i danych

SESJA 2

BEZPIECZNE USŁUGI W SIECI

Tematyka:

I. Bankowość internetowa
II. Płatności mobilne
III. Zakupy w internecie
IV. Komunikacja i praca zdalna

REKOMENDACJE DOTYCZĄCE ORGANIZACJI I REALIZACJI WARSZTATÓW

CZĘŚĆ I

CYBERPRZEMOC I CYBERPRZESTĘPSTWA

SESJA 1

ZAGROŻENIA SPOŁECZNE I FIZYCZNE ZWIĄZANE Z INTERNETEM

Tematyka:

I. Internet – korzyści i zagrożenia
II. Uzależnienie od internetu
III. Negatywne treści i zachowania w internecie
IV. Zagrożenia fizyczne w cyberprzestrzeni

SESJA 2

TYPY OSZUSTW W CYBERPRZESTRZENI

Tematyka:

I. Socjotechnika a oszustwa internetowe
II. Rodzaje oszustw
III. Obrona przed oszustwami

CYBERBEZPIECZEŃSTWO W PRACY I DOMU	
CZĘŚĆ I	CYBERPRZEMOC I CYBERPRZESTĘPSTWA
SESJA 1	ZAGROŻENIA SPOŁECZNE I FIZYCZNE ZWIĄZANE Z INTERNETEM
CZAS TRWANIA	4 GODZINY SZKOLENIOWE

TEMATYKA:

I. Internet – korzyści i zagrożenia
II. Uzależnienie od internetu
III. Negatywne treści i zachowania w internecie
IV. Zagrożenia fizyczne w cyberprzestrzeni

REZULTATY:

- Omówienie konsekwencji związanym z nadużywaniem urządzeń elektronicznych w celu korzystania z aplikacji i stron internetowych
- Przekazanie informacji na temat negatywnych treści i zachowań występujących w internecie oraz ich wpływu na nasze życie osobiste i zawodowe
- Zdobycie wiedzy na temat rodzajów zagrożeń fizycznych w cyberprzestrzeni oraz omówienie potrzeb uczestników w zakresie programu szkoleniowego

PROGRAM SESJI:

I. Internet – korzyści i zagrożenia

a. Ankieta wstępna „Zagrożenia społeczne i fizyczne związane z internetem”
b. Wstęp „Internet – jak wpływa na nasze życie osobiste i zawodowe” – dyskusja grupowa i omówienie osobistych oświadczeń uczestników
c. Ćwiczenie: „Internet – korzyści i zagrożenia”

d. Quiz „Zagrożenia społeczne i fizyczne w internecie”

II. Uzależnienie od internetu

a. Przypadek 1. – omówienie i dyskusja grupowa

a. Mini - wykład i prezentacja „Zagrożenia społeczne i fizyczne związane z internetem – Uzależnienie od internetu”

III. Negatywne treści i zachowania w internecie

a. Przypadek 2. – omówienie i dyskusja grupowa

b. Ćwiczenie „Kodeks internauty”

c. Mini - wykład i prezentacja „Zagrożenia społeczne i fizyczne związane z internetem - Negatywne treści i zachowania w internecie”

IV. Zagrożenia fizyczne w cyberprzestrzeni

a. Przypadek 3. – omówienie i dyskusja grupowa

a. Mini - wykład i prezentacja „Zagrożenia społeczne i fizyczne związane z internetem - Zagrożenia fizyczne w cyberprzestrzeni”

V. Podsumowanie zajęć

Rozdanie materiałów informacyjnych

Podsumowanie „Zagrożenia społeczne i fizyczne związane z internetem”

Ankieta końcowa „Zagrożenia społeczne i fizyczne związane z internetem”

Ankieta ewaluacyjna

MATERIAŁY:

1. Karta pracy „Zagrożenia społeczne i fizyczne związane z internetem”
2. Materiały dla uczestników „Zagrożenia społeczne i fizyczne związane z internetem”
3. Prezentacja „Zagrożenia społeczne i fizyczne związane z internetem”
4. Podsumowanie „Zagrożenia społeczne i fizyczne związane z internetem”
5. Ankiety wstępna i końcowa „Zagrożenia społeczne i fizyczne związane z internetem”
6. Ankieta ewaluacyjna

ZAGROŻENIA SPOŁECZNE I FIZYCZNE ZWIĄZANE Z INTERNETEM

Karta pracy

INTERNET – KORZYŚCI I ZAGROŻENIA

- W jaki sposób internet i możliwość korzystania z urządzeń mobilnych wpływa na nasze życie?
- Na jakie pozytywne i negatywne zjawiska warto zwracać uwagę, zarówno w przypadku osób dorosłych jak dzieci i młodzieży?

Ćwiczenie: „Internet – korzyści i zagrożenia"

Wymień korzyści i zagrożenia korzystania z internetu, zarówno te związane z naszym życiem prywatnym jak i zawodowym.

Korzyści

1. .....
2. .....
3. .....
4. .....
5. .....

Zagrożenia

1. .....
2. .....
3. .....

4. ……

5. ……

Qiuz „Zagrożenia społeczne i fizyczne w internecie”

Wpisz znaczenie poniższych terminów, związanych z zagrożeniami w internecie:

Hejt – ……

……

Fake news – ……

……

Seksting – ……

……

Scam – ……

……

Trolling – ……

……

Spam – ……

……

Phising - ……

……

Wymień inne, znane Ci zagrożenia i negatywne zjawiska występujące w internecie:

! ……

! ……

! ……

UZALEŻNIENIE OD INTERNETU

- Kiedy możemy mówić o uzależnienie od internetu?
- Jaką formę może mieć uzależnienie? Czym się przejawiać?
- Jakie są konsekwencje i zagrożenia związane z uzależnieniem od internetu?

Przypadek 1.

Wiola jest dwudziestoletnią studentką szkoły muzycznej, bardzo aktywną w mediach społecznościowych. Prowadzi swój profil na Instagramie oraz na Facebooku, gdzie regularnie zamieszcza zdjęcia i informacje dotyczące jej życia prywatnego, występów jej zespołu, koncertów w których bierze udział . Obserwuje tez profile innych osób, często komentuje posty, bierze udział w grupach dyskusyjnych itd. Pierwszą rzeczą zaraz po przebudzenia którą robi, jest sprawdzenie wiadomości, otrzymanych lajków, przejrzenie profili. W ciągu dnia robi to jeszcze kilkanaście razy. Zajmuje jej to nie tylko dużo czasu ale staje się coraz większym problemem. Przejmuje się negatywnymi komentarzami, czasem czuje się tym przytłoczona, jednak nie potrafi z tym skończyć, uważa że jest potrzebne w jej karierze, że musi być „widoczna w sieci".

Zadanie: W jaki sposób możemy chronić się przed uzależnieniem od internetu? Jakie zasady warto wprowadzić w tym celu?

→ ……

→ ……

→ ……

→ ……

Podsumowanie: Jakie zasady korzystania z internetu i urządzeń mobilnych warto wprowadzić w przypadku dzieci i młodzieży?

NEGATYWNE TREŚCI I ZACHOWANIA W INTERNECIE

Cyberprzemoc to agresja elektroniczna, której przejawami są: prześladowanie, nękanie, wyśmiewanie i zastraszanie osoby przez Internet lub narzędzia elektroniczne.

Relacje w sieci mogą mieć negatywne skutki, których warto być świadomym aby bardziej skutecznie się przed nimi chronić.

Przypadek 2.

Była impreza urodzinowa mojej koleżanki, które urządziła w popularnym pubie. Przyszło dużo znajomych, również też jacyś ludzie, których nie znałam. Dziewczyny zaczęły się wygłupiać, sporo wypiły, śpiewały piosenki, tańczyły na środku sali, trochę straciły kontrolę. Następnego dnia z przerażeniem zobaczyły, ze jeden z uczestników imprezy robił zdjęcia, które znalazły się na jego stronie na facebooku. Co gorsza, zdjęcia były udostępnione publicznie, widoczne dla wszystkich, współpracowników, przełożonych, klientów a także znajomych. Był to kolega z jej działu, który miał z moją koleżanką ostry konflikt, więc prawdopodobnie zrobił to celowo. Natychmiast w jej firmie pojawiły się złośliwe docinki, komentarze o braku kontroli, skłonności do nieodpowiedzialnej zabawy itp. Koleżanka poprosiła o natychmiastowe usunięcie zdjęć, co się stało kilka godzin później, ale dowiedziała się, że nadal są one przesyłane w prywatnej korespondencji. Bała się, że całe zajście może mieć też wpływ na jej dalsze losy w firmie, możliwość awansu, było jej też przykro.

Zadanie: Co należy zrobić w przypadku cyberprzemocy? Jak się przed nią chronić?

→ .....

→ .....

→ .....

→ .....

Ćwiczenie „Kodeks internauty”

Zadanie: W parach lub w kilkuosobowych grupach przygotujcie 10 zasad, które warto przestrzegać korzystając z internetu.

1. .....
   .....
2. .....
   .....
3. .....
   .....
4. .....
   .....
5. .....
   .....
6. .....
   .....
7. .....
   .....

8. ……
……

9. ……
……

10. ……
……

ZAGROŻENIA FIZYCZNE W CYBERPRZESTRZENI

Odrębną kategorią zagrożeń w internecie jest sytuacja, w której oszuści wzbudzają nasze zaufanie po to, aby wyłudzić nasze dane (np. hasło i login do facebooka) lub pieniądze.

Przestępcy specjalizują się w coraz to skuteczniejszych sztuczkach, które mają za zadanie uśpić naszą czujność. Arsenał cyberprzestępców jest szeroki. Warto znać rodzaje zagrożeń, z którymi muszą się mierzyć internauci.

Przypadek 3.

Mateusz jest właścicielem małego studia poligraficznego. W swojej pracy korzysta z programów komputerowych, przede wszystkim oprogramowania graficznego który służy mu do wykonywania projektów. Są one drogie, czasem więc ściąga darmowe programy z internetu. Ostatnio zwrócił uwagę, że jego laptop wolniej działa, coś dziwnego dzieje się z zapisanymi plikami. Przypomniał sobie również, że tydzień temu skończyła mu się licencja na program antywirusowy, której nie odnowił. Często pracuje poza swoim biurem, u klientów lub w domu. Dostaje także dużo maili od potencjalnych klientów z zapytaniem o usługę a także ofert handlowych. Czasem w pośpiechu otwiera je bez uważnego sprawdzenia nadawcy. Wie jak ważne jest odpowiednie zabezpieczenie laptopa, który stanowi podstawowe narzędzie jego pracy, ale zastanawia się czy jednak nie podchodzi do tego bez należytej wagi.

Zadanie: Jakie zagrożenia fizyczną są związane z aktywnością w internecie?

- ✓ ……
- ✓ ……
- ✓ ……
- ✓ ……
- ✓ ……

SŁOWNIK POJĘĆ

FOMO – uzależnienie od dostępu do informacji

FOMO, z ang. fear of missing out, to strach przed tym, że ominie nas ważna informacja lub wydarzenie, które ma duże znaczenie. Strach i dyskomfort, spowodowany strachem przed przeoczeniem informacji, objawia się niczym innym jak nieustannym sprawdzaniem ekranu telefonu.

Cyberbullying – przemoc z użyciem nowoczesnych technologii

Cyberbullying to nowoczesna forma przemocy, w której wykorzystywany jest internet lub telefony. Polega ono na powtarzaniu aktów przemocy, takich jak dręczenie, groźby czy publikowanie ośmieszających daną osobę treści.

Cyberstalking

Zjawisko natrętnego i złośliwego dręczenia pojedynczej osoby, grupy osób lub całej organizacji przy użyciu technologii informacyjnej, w szczególności Internetu. Prześladowca określany jest często jako stalker. Ofiary stalkingu mogą być namawiane albo zmuszane do wykonania jakiś czynności, szantażem bądź groźbami.

Malware

Skrót od angielskich słów malicious software – czyli złośliwe oprogramowanie mające na celu zniszczenie komputera bądź zapisanych na nim informacji. Malware obejmuje wirusy, robaki, konie trojańskie, spyware, nieuczciwe oprogramowanie typu adware oraz inne szkodliwe dla komputera oprogramowanie.

Man in the Middle

Inaczej „człowiek pośrodku”, jest to typ ataku w ramach którego w transakcji lub korespondencji między dwoma podmiotami (na przykład sklepem internetowym i klientem) uczestniczy ktoś jeszcze. Ataki tego rodzaju mają na celu przechwycenie informacji lub środków

pieniężnych. Man in the middle może mieć na celu zarówno podsłuchanie poufnych informacji, jak i ich modyfikację.

Patostreaming – niebezpieczne transmisje internetowe

Jest to transmisja internetowa, prowadzona w serwisach takich jak YouTube – udostępniających wideo strumieniowe. W trakcie transmisji publikowane są różnego typu zachowania, uznawane powszechnie za negatywne i patologiczne.

Phishing

Nazwa ataku pochodzi od słów Password (hasło) oraz fishing (wędkowanie). Oszustwa typu phishing są stosowane przez cyberprzestępców w celu nakłonienia ludzi do podania poufnych informacji. Polegają na dostarczaniu fałszywych wiadomości e-mail, które wyglądają, jakby pochodziły od znanej użytkownikowi osoby lub organizacji. Zazwyczaj zawierają one link lub załącznik, którego kliknięcie (do czego nakłania treść wiadomości) powoduje nieświadome pobranie złośliwego oprogramowania. Czasami oszustwa phishingowe polegają na utworzeniu fałszywej witryny, której nie sposób odróżnić od prawdziwej witryny. Ma ona na celu nakłonienie użytkowników do wprowadzenia danych logowania.

Ransomware

Ransomware to złośliwe oprogramowanie, które przejmuje kontrolę nad systemem i zaszyfrowuje dane, czasami atakując pojedyncze pliki. Jego celem jest zaszyfrowanie danych użytkownika, a następnie ponowne ich udostępnienie w zamian za opłatę. Tym samym za informacje wypłacany jest „okup” (ransom).

Sexting – przekazywanie treści erotycznych

Przesyłanie za pomocą Internetu i urządzeń mobilnych swoich zdjęć, filmów lub wiadomości o charakterze seksualnym. Zjawisko to dotyczy całej grupy internautów - dorosłych, dzieci i młodzieży. Często dzieje się to już na wczesnym etapie znajomości, a wiele osób wysyła tego rodzaju treści obcym osobom. Sextortion to zjawisko, polegające na szantażowaniu osoby, która przesłała erotyczne treści do kogoś innego, na przykład swoje zdjęcia.

ZAGROŻENIA SPOŁECZNE I FIZYCZNE ZWIĄZANE Z INTERNETEM

Materiały dla uczestników

UZALEŻNIENIE OD INTERNETU

Problematyczne używanie internetu jest zaburzeniem zachowania związanym z nadużywaniem urządzeń elektronicznych w celu korzystania z aplikacji i stron internetowych. Jest to groźne zjawisko ze względu na skutki społeczne, emocjonalne, rodzinne i zawodowe.

W tej sferze zespół uzależnienia od internetu nie odbiega od następstw innych uzależnień. Opisuje się kilka rodzajów uzależnienia. Są to:

- uzależnienie od sieci, które przejawia się chorobliwą chęcią bycia w sieci, sprawdzania informacji,
- uzależnienie od komputera – nie wymagające podłączenia do internetu, a samego używania komputer,
- socjomania internetowa, która jest uzależnieniem od kontaktów w sieci przy jednoczesnej nieumiejętności tworzenia więzi czy nawet podstawowej komunikacji w realnym świecie,
- erotomania internetowa, czyli uzależnienie od pornografii i aktywności seksualnej w sieci.

Objawy uzależnienia od internetu:

- bardzo mocna chęć, by korzystać z sieci, serwisów społecznościowych itp.,
- trudności w odłączeniu się od internetu,
- zespół odstawienia, np. złe samopoczucie spowodowane byciem offline,
- utrata dawnych zainteresowań,
- nienasycenie internetem: coraz dłuższe i częstsze korzystanie z sieci,

- korzystanie z sieci mimo ewidentnych negatywnych skutków (zdrowotnych, społecznych itp.).

NEGATYWNE TREŚCI I ZACHOWANIA W INTERNECIE

Relacje w sieci mogą mieć negatywne skutki, których warto być świadomym aby bardziej skutecznie się przed nimi chronić. Są to materiały pornograficzne, związane z przemocą, substancjami odurzającymi czy skrajną ksenofobią - np. wobec osób innej rasy, wiary czy orientacji seksualnej.

Mogą też zawierać wulgaryzmy czy treści obsceniczne. Cyberprzemoc to agresja elektroniczna, której przejawami są: prześladowanie, nękanie, wyśmiewanie i zastraszanie osoby przez Internet lub narzędzia elektroniczne. Wysyłanie SMSów z groźbami, wyśmiewających e-maili, nękanie na portalach społecznościowych i forach, tworzenie antystron, kradzież tożsamości, rozprzestrzenianie treści szkalujących daną osobę – to zachowania typowe dla stalkera, czyli człowieka dopuszczającego się agresji online.

Cyberbullying – przemoc z użyciem nowoczesnych technologii

Cyberbullying to nowoczesna forma przemocy, w której wykorzystywany jest internet lub telefony. Polega ono na powtarzaniu aktów przemocy, takich jak dręczenie, groźby czy publikowanie ośmieszających daną osobę treści. Może też być bardziej zawoalowana: polegać na wykluczeniu z grupy, manipulowaniu czy nienawiązywaniu relacji. Cyberprzemoc ma najczęściej formę słowną – pojawia się np. w komentarzach, na memach czy nagraniach wideo.

Najpopularniejsze formy cyberprzemocy z nich to:

- publikowanie poniżających filmów lub zdjęć;
- publikowanie ośmieszających, wulgarnych, komentarzy i postów;
- włamania na konta serwisów społecznościowych;

- flood, czyli atakowanie wiadomościami w komunikatorze, telefonami, SMSami
- podszywanie się pod inne osoby;
- wykluczanie z internetowych społeczności.

Hejt – mowa nienawiści

Polega ono na okazywaniu pogardy i złości w internecie. Hejt może być skierowany do przedstawicieli danej płci czy narodowości, jednak jego ofiarą często padają przypadkowe osoby, szukające porady czy chcące wypowiedzieć się na dany temat. Zjawisko hejtu jest niestety coraz bardziej powszechne, występuje przede wszystkim w mediach społecznościowych czy w serwisach, w których prowadzone są dyskusje światopoglądowe.

Cyberstalking

Zjawisko natrętnego i złośliwego dręczenia pojedynczej osoby, grupy osób lub całej organizacji przy użyciu technologii informacyjnej, w szczególności Internetu. Prześladowca określany jest często jako stalker. Cyberstalking to nękanie, np. poprzez pisanie za pomocą komunikatorów, wysyłanie niechcianych wiadomości e-mail, rozsyłanie korespondencji do losowych adresatów w imieniu osoby nękanej oraz wbrew jej woli, jak również komentarze na forach internetowych, wysyłanie prezentów przez Internet etc.

Patostreaming – niebezpieczne transmisje internetowe

Jest to transmisja internetowa, prowadzona w serwisach takich jak YouTube – udostępniających wideo strumieniowe. W trakcie transmisji publikowane są różnego typu zachowania, uznawane powszechnie za negatywne i patologiczne. To na przykład libacje alkoholowe, zażywanie narkotyków, przemoc, w tym przemoc domowa, wulgaryzmy czy transmitowanie niebezpiecznych zachowań w internecie, na przykład nawoływania nieletnich do aktywności seksualnej.

Sexting – przekazywanie treści erotycznych

Przesyłanie za pomocą Internetu i urządzeń mobilnych swoich zdjęć, filmów lub wiadomości o charakterze seksualnym. Należy pamiętać o tym, że osoba po drugiej stronie może wykorzystać zdjęcia czy filmy w dowolny sposób, np. może szantażować, w celu wyłudzenia pieniędzy lub kolejnych zdjęć.

ZAGROŻENIA FIZYCZNE

Cyberprzestępczość to nielegalne działania, popełniane za pomocą technik komputerowych lub dotyczące systemów lub sieci komputerowych, czyli specyficzne dla cyberprzestrzeni. Arsenał cyberprzestępców jest szeroki. Oto główne rodzaje zagrożeń, z którymi muszą się mierzyć internauci:

- **Wirus komputerowy** – szkodliwy program przenoszący się poprzez pliki i powielający się. Wirusy komputerowe wykorzystują systemy operacyjne oraz aplikacje, aby się replikować.
- **Konie trojańskie** – oprogramowanie, podszywające się pod interesujące użytkownika aplikacje, implementujące szkodliwe, ukryte przed użytkownikiem funkcje.
- **Spam** – niechciane lub niepotrzebne wiadomości elektroniczne, najczęściej wysyłane masowo do internautów.
- **Phishing** – wyłudzanie informacji poprzez wiadomości mailowe poprzez podawanie się za inną osobę lub instytucję.
- **Keylogger** – program szpiegujący, rejestrujący znaki wciskane na klawiaturze przez użytkownika. Najczęściej wykorzystywane przy przechwytywaniu danych logowania, takich jak nazwy i hasła.

- **Spyware** – oprogramowanie szpiegujące, które gromadzi i udostępnia informacje o komputerze lub sieci bez zgody i wiedzy użytkownika.
- **Ataki DDoS** – ataki hakerskie, które są kierowane na usługi sieciowe lub systemy komputerowe i mają na celu zajęcie wolnych zasobów, aby uniemożliwić funkcjonowanie całej usługi w Internecie.
- **Man in the Middle** - inaczej „człowiek pośrodku", jest to typ ataku w ramach którego w transakcji lub korespondencji między dwoma podmiotami (na przykład sklepem internetowym i klientem) uczestniczy ktoś jeszcze.

Socjotechniki

Współczesne cyberataki coraz częściej wykorzystują nieświadomość internautów. Socjotechniki są najczęściej praktykowane przez osoby wykradające poufne dane i wiążą się z konsekwencjami dla użytkownika. Zagrożenie ciężko rozpoznać, a atak może być prowadzony przez długi czas. Ofiara często jest zmanipulowana, a atakujący może podawać się za kogoś innego lub wykorzystywać kradzioną tożsamość. Często można spotkać się z tego typu praktyką w kontekście banków, poprzez tzw. phishing, podszywanie się pod firmy i wysyłanie wiadomości do użytkowników z prośbą o podanie pewnych pilnych danych, hasła dostępu do konta w celu „weryfikacji rachunku" albo zmian systemowych (technicznych, programowych).

Kradzież danych poufnych

Najczęstsze problemy o charakterze konsumenckim w Internecie to pozyskiwanie danych osobowych bez wiedzy użytkownika, np. podczas wypełniania formularzy rejestracyjnych, zamówienia w sklepach internetowych, poprzez tzw. cookies, czyli pliki, które zapisywane są automatycznie na dysku twardym i gromadzące podstawowe dane o użytkowniku.

Starajmy się ograniczać umieszczanie w sieci naszych danych wrażliwych takich jak: dane personalne, numery telefonów, adresy mailowe, dane kart płatniczych oraz zdjęcia i filmy,

szczególnie tych osobistych, pamiętając o tym, że mogą je przejąć i wykorzystać różne osoby, często nam wrogie. Także korzystanie z publicznych niezabezpieczonych sieci Wi-Fi może być ryzykowne. Użytkownik korzystający z takiej sieci, wystawia swe zasoby cyfrowe zapisane w pamięci komputera, bądź smartfona na widok hakerów. Cyberprzestępcy mogą wówczas śledzić aktywność użytkownika online, a nawet przejąć jego dane czy hasła dostępu np. do bankowości online. Również korzystanie z usług chmurowych, mimo iż z roku na rok coraz bardziej niezawodne, obarczone jest pewnym ryzykiem, że przechowywane w sieci dane zostaną utracone (na przykład w wyniku awarii pamięci serwera) lub przejęte przez inne osoby.

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ I

CYBERPRZEMOC I CYBERPRZESTĘPSTWA

SESJA 1

ZAGROŻENIA SPOŁECZNE I FIZYCZNE ZWIĄZANE Z INTERNETEM

PODSUMOWANIE

1. Ochronę antywirusową najlepiej zainstalować
    a. W laptopie
    b. W smartfonie
    c. W każdym urządzeniu, którego używamy do łączenia się z Internetem

2. Jaka metoda daje nam stuprocentowe bezpieczeństwo poruszania się po sieci?
    a. Instalacja oprogramowania antywirusowego
    b. Częsta zmiana haseł
    c. Nie ma stuprocentowej pewności, w Internecie zawsze obowiązuje zasada ograniczonego zaufania

3. Cyberstalking, to:
    a. wyłudzanie danych osobistych i informacji majątkowych
    b. uwodzenie przez Internet
    c. nękanie, zastraszanie, szantaż, przy pomocy Internetu i innych mediów elektronicznych

4. Nieustanna chęć sprawdzenia najnowszych informacji dotyczących znajomych na portalu społecznościowym to jeden z objawów:
    a. cyberholizmu
    b. stresu
    c. narcyzmu

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ I

CYBERPRZEMOC I CYBERPRZESTĘPSTWA

SESJA 1

ZAGROŻENIA SPOŁECZNE I FIZYCZNE ZWIĄZANE Z INTERNETEM

PODSUMOWANIE

1. Ochronę antywirusową najlepiej zainstalować
    a. W laptopie
    b. W smartfonie
    c. W każdym urządzeniu, którego używamy do łączenia się z Internetem

2. Jaka metoda daje nam stuprocentowe bezpieczeństwo poruszania się po sieci?
    a. Instalacja oprogramowania antywirusowego
    b. Częsta zmiana haseł
    c. Nie ma stuprocentowej pewności, w Internecie zawsze obowiązuje zasada ograniczonego zaufania

3. Cyberstalking, to:
    a. wyłudzanie danych osobistych i informacji majątkowych
    b. uwodzenie przez Internet
    c. nękanie, zastraszanie, szantaż, przy pomocy Internetu i innych mediów elektronicznych

4. Nieustanna chęć sprawdzenia najnowszych informacji dotyczących znajomych na portalu społecznościowym to jeden z objawów:
    a. cyberholizmu
    b. stresu

c. narcyzmu

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ I

CYBERPRZEMOC I CYBERPRZESTĘPSTWA

SESJA 1

ZAGROŻENIA SPOŁECZNE I FIZYCZNE ZWIĄZANE Z INTERNETEM

ANKIETA WSTĘPNA

OCENA WIEDZY I UMIEJĘTNOŚCI PRAKTYCZNYCH							
W każdym z pytań prosimy o zaznaczenie znakiem „X” odpowiedzi na poszczególne pytania w skali 7-punktowej gdzie: 1 - oznacza „zdecydowanie źle”, 2 - „źle”, 3 - „raczej źle”, 4 - „ani dobrze, ani źle”, 5 - „raczej dobrze, 6 – „dobrze”, 7 - „zdecydowanie dobrze”.							
Pytanie	***1***	***2***	***3***	***4***	***5***	***6***	***7***
1. Jak Pani / Pan ocenia swoją wiedzę na temat zagrożeń społecznych występujących w cyberprzestrzeni?	☐	☐	☐	☐	☐	☐	☐
2. Jak Pani/Pan ocenia swoją znajomość objawów uzależnienia od internetu?	☐	☐	☐	☐	☐	☐	☐
3. Jak Pani/Pan ocenia swoją znajomość konsekwencji uzależnienia od internetu?	☐	☐	☐	☐	☐	☐	☐
4. Jak Pani / Pan ocenia swoją wiedzę na negatywnych treści i zachowań występujących w internecie?	☐	☐	☐	☐	☐	☐	☐
5. Jak Pani / Pan ocenia swoją wiedzę na temat zagrożeń fizycznych w cyberprzestrzeni?	☐	☐	☐	☐	☐	☐	☐

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ I

CYBERPRZEMOC I CYBERPRZESTĘPSTWA

SESJA 1

ZAGROŻENIA SPOŁECZNE I FIZYCZNE ZWIĄZANE Z INTERNETEM

ANKIETA KOŃCOWA

OCENA WIEDZY I UMIEJĘTNOŚCI PRAKTYCZNYCH							
W każdym z pytań prosimy o zaznaczenie znakiem „X" odpowiedzi na poszczególne pytania w skali 7-punktowej gdzie: 1 - oznacza „zdecydowanie źle", 2 - „źle", 3 - „raczej źle", 4 - „ani dobrze, ani źle", 5 - „raczej dobrze, 6 – „dobrze", 7 - „zdecydowanie dobrze".							
Pytanie	***1***	***2***	***3***	***4***	***5***	***6***	***7***
1. Jak Pani / Pan ocenia swoją wiedzę na temat zagrożeń społecznych występujących w cyberprzestrzeni?	□	□	□	□	□	□	□
2. Jak Pani/Pan ocenia swoją znajomość objawów uzależnienia od internetu?	□	□	□	□	□	□	□
3. Jak Pani/Pan ocenia swoją znajomość konsekwencji uzależnienia od internetu?	□	□	□	□	□	□	□
4. Jak Pani / Pan ocenia swoją wiedzę na negatywnych treści i zachowań występujących w internecie?	□	□	□	□	□	□	□
5. Jak Pani / Pan ocenia swoją wiedzę na temat zagrożeń fizycznych w cyberprzestrzeni?	□	□	□	□	□	□	□

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ I CYBERPRZEMOC I CYBERPRZESTĘPSTWA

SESJA 1 ZAGROŻENIA SPOŁECZNE I FIZYCZNE ZWIĄZANE Z INTERNETEM

ANKIETA EWALUACYJNA

PROWADZENIE SZKOLENIA

1. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **wiedzę i przygotowanie merytoryczne** osoby prowadzącej szkolenie?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

2. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **umiejętność przekazania wiedzy** przez osobę prowadzącą szkolenie?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

3. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **kontakt i umiejętność pracy z grupą** osoby prowadzącej szkolenie?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

PROGRAM SZKOLENIA I MATERIAŁY DYDAKTYCZNE

4. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **przydatność szkolenia** w względem potrzeb uczestników?

Zdecydowanie nieprzydatne	*Raczej nieprzydatne*	*Trudno powiedzieć*	*Raczej przydatne*	*Zdecydowanie przydatne*
1	2	3	4	5

5. Proszę ocenić na pięciostopniowej skali, w jakim stopniu szkolenie pogłębiły Pani/Pana **wiedzę teoretyczną** z omawianego na szkoleniu obszaru?

Niewystarczająco	*Wystarczająco*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

6. Proszę ocenić na pięciostopniowej skali, w jakim stopniu przeprowadzone szkolenie pogłębiło Pani/Pana **umiejętności praktyczne** z omawianego na warsztatach tematu?

Niewystarczająco	*Wystarczająco*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

7. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **jasność i zrozumiałość** wykorzystanych **kart pracy**?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

8. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **przydatność ćwiczeń** w zdobyciu wiedzy i umiejętności z zakresu tematyki szkolenia ?

Zdecydowanie nieprzydatne	*Raczej nieprzydatne*	*Trudno powiedzieć*	*Raczej przydatne*	*Zdecydowanie przydatne*
1	2	3	4	5

9. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **jasność i zrozumiałość** wykorzystanej **prezentacji multimedialnej**?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

10. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **jasność i zrozumiałość materiałów dla uczestników**?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

CYBERBEZPIECZEŃSTWO W PRACY I DOMU	
CZĘŚĆ I	CYBERPRZEMOC I CYBERPRZESTĘPSTWA
SESJA 2	TYPY OSZUSTW W CYBERPRZESTRZENI
CZAS TRWANIA	4 GODZINY SZKOLENIOWE

TYPY OSZUSTW W CYBERPRZESTRZENI

TEMATYKA:

I. Socjotechnika a oszustwa internetowe
II. Rodzaje oszustw
III. Obrona przed oszustwami

REZULTATY:

- Omówienie różnych metod socjotechnik stosowanych przez przestępców internetowych
- Zdobycie wiedzy na temat rodzajów oszustw w cyberprzestrzeni oraz stosowanych form manipulacji
- Przekazanie informacji na zasad postępowania w sytuacji zagrożenia oszustwem internetowym
- Podniesienie świadomości na temat cyberbezpieczeństwa

PROGRAM SESJI:

I. Socjotechnika a oszustwa internetowe

a. Ankieta wstępna „Typy oszustw w cyberprzestrzeni”
b. Przypadek 1. – omówienie i dyskusja grupowa
c. Ćwiczenie „Socjotechniki”
d. Mini - wykład i prezentacja „Typy oszustw w cyberprzestrzeni - Socjotechnika a oszustwa internetowe”

II. Rodzaje oszustw

a. Przypadek 2. – omówienie i dyskusja grupowa
b. Mini - wykład i prezentacja „Typy oszustw w cyberprzestrzeni - Rodzaje oszustw”

III. Obrona przed oszustwami

a. Ćwiczenie „Nie daj się oszustom”
b. Mini - wykład i prezentacja „Typy oszustw w cyberprzestrzeni - Obrona przed oszustwami”

IV. Podsumowanie zajęć

Rozdanie materiałów informacyjnych
Podsumowanie „Typy oszustw w cyberprzestrzeni”
Ankieta końcowa „Typy oszustw w cyberprzestrzeni”
Ankieta ewaluacyjna

MATERIAŁY:

1. Karta pracy „Typy oszustw w cyberprzestrzeni”
2. Materiały dla uczestników „Typy oszustw w cyberprzestrzeni”
3. Prezentacja „Typy oszustw w cyberprzestrzeni”
4. Podsumowanie „Typy oszustw w cyberprzestrzeni”
5. Ankiety wstępna i końcowa „Typy oszustw w cyberprzestrzeni”

6. Ankieta ewaluacyjna

TYPY OSZUSTW W CYBERPRZESTRZENI

Karta pracy

SOCJOTECHNIKA A OSZUSTWA INTERNETOWE

Internet stał się narzędziem do osiągania różnych celów, często też i negatywnych. Oszuści wybierają właśnie tę drogę dzięki możliwości dotarcia do ogromnej liczby osób. Najlepszą obroną przed takimi oszustwami jest znajomość stosowanych taktyk i zachowanie nieufności w stosunku do tego rodzaju wiadomości e-mail, sms-ów, linków oraz postów.

Przypadek 1.

Paweł otrzymał maila o treści - „Uwaga! Ostateczne wezwanie do wpłaty. Termin uregulowania należności minął w dniu 30 Lipiec 2020. Nie uregulowanie należności w wysokości 1 000 PLN do w ciągu 3 dni od otrzymania tej wiadomości spowoduje wpisanie Twojej firmy do bazy dłużników oraz oczekuj odpowiedzialności karnej. Szczegóły znajdź w załączonym pliku”. Dbając o wizerunek swojej firmy, szybko pobrał załącznik do powyższej wiadomości i spróbował go otworzyć, nie zważając na ostrzeżenia zgłaszane przez zainstalowany na jego komputerze program antywirusowy. Spróbował zadzwonić pod wskazany w wiadomości numer telefonu, którego nikt nie odbierał, zajął się zupełnie innymi sprawami – akurat miał w planach właśnie wykonanie kilku przelewów. Jakież było jego zdziwienie, gdy po kilku dniach wszedł na swój rachunek bankowości internetowej i zobaczył, że w historii operacji widnieją przelewy do osób, o których nigdy nie słyszał. Udał się do placówki swojego banku, gdzie został poinformowany, że ostatnie przelewy, które przekazywał (w swoim mniemaniu) do swoich kontrahentów w rzeczywistości trafiły zupełnie gdzie indziej. Zadzwonił do znajomego informatyka, który poinformował go, że jest to typowy sposób działania szkodliwego oprogramowania wykradającego pieniądze z kont klientów banków. Natychmiastowa diagnoza komputera

przeprowadzona przez owego znajomego potwierdziła jego najgorsze przypuszczenia. Jego komputer padł ofiarą wirusa, a on sam został skutecznie okradziony przez przestępców.

Zadanie: Jakie zagrożenia mogą być są związane z aktywnością w internecie?

- ✓ ……
- ✓ ……
- ✓ ……
- ✓ ……

Ćwiczenie „Socjotechniki”

Socjotechnika to jedna z najgroźniejszych broni w arsenale cyberprzestępcy. Jest rodzajem ataku psychologicznego polegającym na tym, że atakujący nakłania swoją ofiarę do wykonania jakiejś czynności. Może zdarzyć się przy użyciu niemal każdej technologii, w tym ataków phishingowych poprzez e-mail, SMS, wiadomość na portalach społecznościowych jak Facebook czy Twitter lub czatach internetowych.

Zadanie: Jakie mogą być typowe metody socjotechniczne stosowane przez cyberprzestępców?

- ✓ ……
- ✓ ……
- ✓ ……
- ✓ ……

W jaki sposób możemy się przed nimi chronić?

- ✓ ……
- ✓ ……

- ✓ ……
- ✓ ……

RODZAJE OSZUSTW

Phishing czyli tzw. łowienie, to jeden z najpopularniejszych sposobów oszustów. Polega na zdobywaniu nieuczciwymi metodami poufnych informacji, dotyczących określonej osoby. Najczęściej oszuści podają się za godną zaufania firmę, lub osobę, która potrzebuje w danym momencie określonych danych osobistych.

Przypadek 2.

Maria jest podekscytowana. Właśnie dostała e-maila z radosną informacją: jeżeli poda swoje imię i nazwisko, adres i numer telefonu, firma „Spełniamy marzenia" prześle jej bilety na koncert ulubionego zespołu. Powinna tylko otworzyć przesłany link i zalogować się na stronie internetowej firmy promocyjnej podać swoje dane, konieczne do wydania biletu oraz wpisania na listę VIP. Jednak jej koleżanka z biura, której opowiedziała o mailu, zauważyła, że może być to próba wyłudzenia danych, że nie powinna ryzykować.

Zadanie: Na co powinniśmy uważać w korespondencji mailowej ?

- ✓ ……
- ✓ ……
- ✓ ……
- ✓ ……

Jakich zasad powinniśmy przestrzegać ?

- ✓ ……

✓ .....

✓ .....

✓ .....

OBRONA PRZED OSZUSTWAMI

Ćwiczenie „Nie daj się oszustom”

Zadanie: W parach lub w kilkuosobowych zespołach przygotujcie zasady, które warto przestrzegać aby ustrzec się przed oszustwami internetowymi.

1. .....

   .....

2. .....

   .....

3. .....

   .....

4. .....

   .....

5. .....

   .....

6. ……

……

7. ……

……

SŁOWNIK POJĘĆ

Nigeryjski szwindel

Rodzaj spamu-oszustwa polegający na wciągnięciu ofiary w fikcyjny transfer wielkiej kwoty pieniędzy (rzędu kilku milionów USD) najczęściej z któregoś z krajów afrykańskich (początkowo głównie do Nigerii).

Phishing

Nazwa pochodzi od *password* („hasło”) oraz *fishing* („wędkowanie”). Istotą ataku jest próba pozyskania hasła użytkownika, które służy do logowania się na portalach społecznościowych bądź do serwisów. Po uzyskaniu dostępu, przestępca może wykraść dane osobowe i w tym celu dokonywać oszustw.

Socjotechnika

Jest rodzajem ataku psychologicznego polegającym na tym, że atakujący nakłania swoją ofiarę do wykonania jakiejś czynności.

Scam

Oszustwo polegające na wzbudzeniu czyjegoś zaufania, a następnie wykorzystaniu tego zaufania do wyłudzenia pieniędzy lub innych składników majątku

Spam

Niechciane lub niepotrzebne wiadomości elektroniczne.

Złośliwe oprogramowanie

Szkodliwe oprogramowanie (ang. malware – zbitka słów malicious „złowrogi, złośliwy” i software „oprogramowanie”) ogół programów mających szkodliwe działanie w stosunku do systemu komputerowego lub jego użytkownika.

TYPY OSZUSTW W CYBERPRZESTRZENI

Materiały dla uczestników

SOCJOTECHNIKA A OSZUSTWA INTERNETOWE

Istnieje wiele rodzajów oszustw internetowych, ale wszystkie one mają jedną wspólną cechę: próbują nakłonić Cię do ujawnienia swoich prywatnych informacji lub zapłacenia za coś, czego nie otrzymasz. Wiele oszustw internetowych może sprawiać wrażenie świetnych ofert, wszystko co musisz zrobić to tylko wpłacić małą zaliczkę, aby pokryć tzw. opłaty manipulacyjne.

Oszustwa internetowe mogą przybrać formę złośliwego oprogramowania, aby ukraść hasła i zdobyć dostęp np. do kont bankowych lub będą opierać się na fałszywych e-mailach i socjotechnice w celu wyłudzenia pieniędzy. Podszywają się również pod szefów, dyrektorów, kolegów z danej organizacji, którzy wysyłają maile do swoich podwładnych lub współpracowników. Częstą praktyką jest wysyłanie maili i SMS-ów w imieniu podmiotów cieszących się zaufaniem: instytucji finansowych, serwisów ogłoszeniowych czy organów państwowych.

Mogą pojawić się prośby na przykład, aby zalogować się na konto lub by przesłać poufne dla danej organizacji informacje. W celu zmylenia odbiorców oszuści zwykle dołączają do nich logo imitujące styl i szatę graficzną danej instytucji. Inny typ to oszustwa, które polegają na zainstalowaniu złośliwego oprogramowania na komputerze. Zachęcają one do pobrania pliku, który pomoże w naprawieniu zainfekowanego komputera po tym jak pokażą wyskakujące okno informujące o zagrożeniu. Musisz tylko pobrać fałszywy program antywirusowy.

Eksperci wskazują również, że coraz częściej oszuści starają się podszyć pod bliskie odbiorcy osoby i wykorzystują różnego rodzaju socjotechniki do manipulacji. Celem cyberprzestępców jest skłonienie ofiar, by reagowały na e-maile bezwiednie, bez należytej uwagi, wykorzystując na ogół autorytet wysoko postawionej w organizacji osoby. Oszuści internetowi cały czas prześcigają się w tworzeniu nowych sposobów wyłudzania danych osobowych, czy pieniędzy.

Scam

Scam to oszustwo polegające na wzbudzeniu czyjegoś zaufania, a następnie wykorzystaniu tego zaufania do wyłudzenia pieniędzy lub innych składników majątku. Bardzo często oszuści posługują się portalami społecznościowymi, na których informacje bardzo szybko się rozchodzą, zyskują duże zainteresowanie i zasięg.

→ Typowy mechanizm tego oszustwa polega na proponowaniu ofierze udziału w ogromnych zyskach w zamian za rzekome pośrednictwo wymagające zainwestowania proporcjonalnie niewielkich własnych środków w różnego rodzaju koszty operacyjne. Oszust wciela się zwykle w postać spadkobiercy, wcześniej oszukanego przedsiębiorcy, potomka ofiary zamachu stanu itp.

→ W oszukańczej wiadomości może być na przykład prośba o kliknięcie odnośnika i podanie numeru karty kredytowej, aby otrzymać nagrodę. Oczywiście żadna nagroda nie zostanie przesłana. Zamiast tego nadawca takiej wiadomości przechwytuje numer karty kredytowej.

→ Inną taktyką jest informowanie, że nasze konto na witrynie zostanie zamknięte, a żeby tego uniknąć, należy kliknąć odnośnik i podać ponownie nazwę użytkownika i hasło. (Podanie tych danych umożliwia przechwycenie naszych danych logowania).

→ Często też jesteśmy proszeni o wsparcie finansowe osób znajdujących się w trudnych sytuacjach. Pomysły są różne: najpopularniejsze są historie o spadkach, które mogą trafić w nasze ręce w zamian za pomoc w opłaceniu prowizji dla firmy ubezpieczeniowej lub jakiejś jej części.

→ Pojawiają się również opowieści o chorych dzieciach żyjących w niedostatku oraz ich rodziców, których nie stać na leczenie i hospitalizację, a rzekome choroby ich dzieci wymagają podjęcia natychmiastowych zabiegów lekarskich. Na dowód starają się

przesyłać spreparowane rachunki za dokonane leczenie oraz oferują podzielenie się pieniędzmi z ubezpieczenia, które mają otrzymać.

RODZAJE OSZUSTW

Poczta elektroniczna to obecnie najpopularniejsze narzędzie cyberprzestępców i najprostszy sposób dystrybucji złośliwego oprogramowania: w linkach i załącznikach. Jedna z metod, tzw. phishing, za pomocą linku odsyła do fałszywej strony banku, firmy czy urzędu, która po zalogowaniu przez użytkownika przejmuje jego dane uwierzytelniające lub infekuje samo urządzenie.

Phishing czyli tzw. łowienie, to jeden z najpopularniejszych sposobów oszustów. Choć ciągle się zmienia i przybiera coraz to nowsze formy, to jego głównie działanie polega na wyłudzaniu poufnych danych, czyli np. loginów i haseł do poczty e-mail, danych osobowych, danych logowania do bankowego konta, numerów kart kredytowych czy PIN. Bardzo często cyberprzestępcy wysyłają spam do dużej liczby osób, podając fałszywą stronę i podającą się za konkretny bank czy sklep internetowy. Po wejściu ofiary na fałszywą stronę przechwytywane są informacje wpisywane przez ofiarę (taka sytuacja może dotyczyć chociażby nieprawdziwej informacji o dezaktywacji konta i prośbie ponownego wpisania wszystkich danych osobistych).

- <u>Fałszywe powiadomienia z mediów społecznościowych</u>

Oszuści aktywnie wysyłają fałszywe powiadomienia, podszywając się pod popularne sieci społecznościowe. Poruszają w nich temat nowych znajomych, ich aktywności, komentarzy czy polubień. Takie wiadomości często trudno jest odróżnić od oryginalnych; zwykle jedyną różnicą jest to, że zawierają odnośnik phishingowy, który niełatwo jest rozpoznać. Po kliknięciu go ofiara jest nakłaniana do wprowadzenia swojej nazwy użytkownika i hasła na fałszywej stronie logowania.

Innym częstym wariantem są wiadomości pochodzące rzekomo z sieci społecznościowych, bazujące na strachu. Informują one na przykład, że na koncie odbiorcy wiadomości

zarejestrowano podejrzaną aktywność lub że wprowadzono nową funkcję, a użytkownicy, którzy nie wyrażą na nią zgody, zostaną zablokowani. W każdym przypadku wiadomość zawiera przycisk z łączem prowadzącym do phishingowej strony logowania.

- Phishing bankowy

Phishing, którego celem jest zdobycie informacji na temat karty płatniczej danej osoby, nadal należy do najpopularniejszych oszustw. Fałszywe wiadomości mogą być wysyłane w imieniu banków lub systemów płatności. Najczęściej temat tych wiadomości jest związany z blokowaniem konta lub „podejrzaną aktywnością" wykrytą na koncie osobistym odbiorcy.

Pod pretekstem przywrócenia dostępu, potwierdzenia tożsamości czy anulowania transakcji użytkownik jest proszony o wprowadzenie szczegółowych informacji dotyczących karty płatniczej (często kodu CVV/CVC) na fałszywej stronie banku. Po odebraniu tych danych przestępcy natychmiast wypłacają pieniądze z konta ofiary.

- Niebezpieczne załączniki

W imieniu różnych instytucji i przedsiębiorstw oszuści internetowi wysyłają do swoich ofiar e-maile z plikami, które mają na celu zainfekowanie ich urządzeń. Załącznik jest najczęściej spakowany lub zawiera nietypowe rozszerzenie. Złośliwe oprogramowanie, atakujące komputer lub telefon, po otwarciu pliku może podmieniać linki do stron bankowości internetowej, przechwytywać hasła lub wyświetlać komunikaty, sugerujące konieczność zainstalowania specjalnego oprogramowania antywirusowego. W rzeczywistości jest to kolejny wirus, który infekuje urządzenie użytkownika w celu przekierowania kodów SMS, przechwytywania informacji wrażliwych czy wręcz jego przejęcia.

- Fałszywe powiadomienia z serwisów poczty e-mail

Oszuści wykorzystują tego rodzaju spam do gromadzenia nazw użytkowników i haseł do usług e-mail. Najczęściej użytkownicy są nakłaniani do przywrócenia swojego hasła lub zwiększenia miejsca w skrzynce pocztowej, która podobno jest zapchana. W tym drugim przypadku łącze phishingowe obiecuje znaczące zwiększenie dostępnej przestrzeni.

- Prośby o przelewy

Bardzo popularną metodą phishingu jest podszywanie się pod firmy telekomunikacyjne czy kurierskie, a nawet instytucje rządowe, aby poprosić użytkowników o uregulowanie rachunku lub dopłatę do usługi. Z pozornie wiarygodnego adresu otrzymujemy wtedy fałszywy numer konta albo link do panelu, w którym mamy zatwierdzić przelew.

Znane są też sytuacje podszywania się pod Ministerstwo Finansów i prośby o wpłatę za wpis do rejestru REGON lub podanie danych karty kredytowej celem zwrotu nadpłaty podatku.

- Oszustwa na konkursy

Nieomal każdy z nas nie dostał SMS-a o treści "Gratulacje, wygrałeś Superkonkurs! Aby odebrać nagrodę, wyślij SMS na numer…"? Odesłanie SMS-a będzie nie tylko bardzo kosztowne, ale i rozpocznie serię kolejnych, dodatkowo płatnych wiadomości np. z odpowiedziami na zadawane pytania. Równie popularne są konkursy wyskakujące nam w okienkach na stronach internetowych lub przychodzące za pośrednictwem poczty elektronicznej - zaangażowanie się w nie, poza stratą pieniędzy, może wiązać się z wgraniem złośliwego oprogramowania. Należy również uważać z oddzwanianiem na numery, od których mamy nieodebrane połączenia. Oszuści podszywają się pod numer przypominający numer krajowy, ale w rzeczywistości jest to numer kraju, gdzie połączenia są bardzo kosztowne.

- Oszustwo na „nigeryjskiego księcia"

Ofierze obiecuje się ogromną nagrodę, jeśli zgodzi się pomóc pechowemu milionerowi wypłacić pieniądze ulokowane w kontach różnych banków. W tym celu należy oczywiście najpierw wysłać szczegółowe informacje na swój temat (informacje odnośnie paszportu, danych konta itp.) oraz niewielką kwotę na załatwienie formalności Ofiara jest zapewniana, że otrzyma dużą część przedmiotowej kwoty w zamian za wpłacenie kwoty na np. opłaty skarbowe czy prawników prowadzących sprawę spadkową. Jest to jedna z wielu form tego oszustwa.

- Prośba o pomoc od znajomego

Przestępcy połączyli jeden z najwygodniejszych sposobów wykonywania przelewów, BLIK, oraz ufność, jaką pokładamy w mediach społecznościowych i komunikatorach, by stworzyć nową metodę phishingu. Podszywając się pod znajomego, dzięki przejęciu lub stworzeniu fałszywego profilu takiej osoby, kontaktują się z ofiarą i proszą o pilny przelew określonej kwoty. Argumentują swoją potrzebę sytuacją losową: kradzieżą portfela, problemem z powrotem do domu itp. Z reguły prośby te dotyczą małych kwot, wiążą się z naciskami na szybką reakcję i są uzupełniane zapewnieniami o zwrocie pożyczonych środków już następnego dnia. Oszuści proszą nas o przekazanie kodu BLIK, a po zatwierdzeniu przez nas transakcji w aplikacji bankowej (czasami kilkukrotnego z powodu rzekomego niezadziałania poprzedniego kodu) szybko wypłacają gotówkę z bankomatu.

- Fałszywe oferty pracy

Phishing może przyjąć również formę fałszywej, najczęściej bardzo atrakcyjnej oferty pracy. Naszą podejrzliwość powinny wzbudzić: bardzo atrakcyjne warunki łączące się z brakiem oczekiwań i gwarancją pracy jedynie kilka godzin w tygodniu, zakres obowiązków, który obejmuje wykorzystanie naszego prywatnego konta i pośredniczenie przy przelewach pieniężnych, brak opisu wymagań i zakresu obowiązków, otrzymanie niespodziewanej wiadomości od rekrutera. W dobie bezpośredniej rekrutacji zdarza się to coraz częściej, ale jeśli oferta nie jest związana z naszym doświadczeniem zawodowym, a za nadawcą nie stoi żadna znana nam firma, lepiej mieć się na baczności. Oferty pracy mogą być też wykorzystane do typowych ataków phishingowych, takich jak niebezpieczne linki lub zainfekowane pliki.

Tego typu oszustw przestępcy dopuszczają się nie tylko poprzez udostępnianie ogłoszeń na portalach rekrutacyjnych czy na grupach na Facebooku (proponując najczęściej pracę bez wychodzenia z domu i ogromne prowizje), ale też w bezpośrednich, nierzadko bardzo przekonujących mailach lub wiadomościach na Linkedinie czy innych portalach zawodowych.

OBRONA PRZED OSZUSTWAMI

- Loguj się na swoje konto bankowe tylko przez stronę banku lub aplikację, nigdy z linków przesyłanych w wiadomościach.
- Żadna instytucja finansowa nie poprosi Cię w wiadomości o podanie danych do logowania, hasła, kodów autoryzacyjnych lub danych kart płatniczych, więc nigdy ich nie wysyłaj.
- Nie otwieraj załączników od nieznajomych ani tych, które znajomi wysłali Ci niespodziewanie - ich poczta elektroniczna mogła zostać zainfekowana.
- Dokładnie sprawdzaj adres nadawcy, porównuj korespondencję z wcześniejszymi mailami.
- Jeśli coś wzbudzi Twój niepokój, zadzwoń do instytucji, która rzekomo wysłała wiadomość i wyjaśnij wątpliwości. Numer telefonu sprawdź na oficjalnej stronie internetowej, zamiast dzwonić pod numer podany w komunikacie.
- Nie odpowiadaj na maile o nagrodach, których nie starałeś się wygrać
- Jeśli z takowych nie korzystasz, zablokuj u swojego operatora telekomunikacyjnego wiadomości i połączenia głosowe o podwyższonej opłacie (tzw. usługi PREMIUM), a także wychodzące połączenia międzynarodowe.

- Jeśli Twój znajomy prosi Cię o przelew przez Internet lub podanie wrażliwych danych, skontaktuj się z nim w inny sposób, na przykład zadzwoń, aby upewnić się, że to on jest nadawcą danej wiadomości.
- Zadbaj o silne hasło i, jeśli jest to możliwe, ustaw dwuetapowe uwierzytelnienie.
- Nigdy nie loguj się do swojego konta na obcych urządzeniach. Jeśli nie masz innego wyjścia, najlepiej ustaw wcześniej podwójne uwierzytelnienie i otwórz stronę logowania w trybie incognito.

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ I

CYBERPRZEMOC I CYBERPRZESTĘPSTWA

SESJA 2

TYPY OSZUSTW W CYBERPRZESTRZENI

PODSUMOWANIE

1. Jak rozpoznać zaufaną stronę internetową?
    a. posiada kłódkę czyli certyfikat bezpieczeństwa
    b. rozpoczyna się od https:// - czyli jest szyfrowana
    c. obie powyższe odpowiedzi są prawidłowe

2. Jakie informacje powinniśmy zachować tylko dla siebie, nawet jeśli rozmawiamy z konsultantem na infolinii banku?
    a. Datę urodzenia i posiadane produkty bankowe
    b. Nazwisko panieńskie matki
    c. Login i hasło do e-bankowości

3. Ikona zamkniętej kłódki w pasku adresu przeglądarki informuje użytkownika, że:
    a. strona jest zabezpieczona certyfikatem bezpieczeństwa i połączenie jest szyfrowane
    b. witryna została zamknięta ze względów bezpieczeństwa
    c. kliknięcie jakiekolwiek linku na stronie spowoduje zainstalowanie konia trojańskiego lub robaka na naszym komputerze

4. Phishing to:
    a. wirus niszczący pliki w komputerze
    b. wyłudzanie informacji osobistych przez podszywanie się pod stronę np. banku
    c. system chroniący przed wyłudzeniami danych

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ I

CYBERPRZEMOC I CYBERPRZESTĘPSTWA

SESJA 2

TYPY OSZUSTW W CYBERPRZESTRZENI

PODSUMOWANIE

1. Jak rozpoznać zaufaną stronę internetową?
    a. posiada kłódkę czyli certyfikat bezpieczeństwa
    b. rozpoczyna się od https:// - czyli jest szyfrowana
    c. obie powyższe odpowiedzi są prawidłowe

2. Jakie informacje powinniśmy zachować tylko dla siebie, nawet jeśli rozmawiamy z konsultantem na infolinii banku?
    a. Datę urodzenia i posiadane produkty bankowe
    b. Nazwisko panieńskie matki
    c. Login i hasło do e-bankowości

3. Ikona zamkniętej kłódki w pasku adresu przeglądarki informuje użytkownika, że:
   a. **strona jest zabezpieczona certyfikatem bezpieczeństwa i połączenie jest szyfrowane**
   b. witryna została zamknięta ze względów bezpieczeństwa
   c. kliknięcie jakiekolwiek linku na stronie spowoduje zainstalowanie konia trojańskiego lub robaka na naszym komputerze

4. Phishing to:
   a. wirus niszczący pliki w komputerze
   b. wyłudzanie informacji osobistych przez podszywanie się pod stronę np. banku
   c. system chroniący przed wyłudzeniami danych

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ I

CYBERPRZEMOC I CYBERPRZESTĘPSTWA

SESJA 2

TYPY OSZUSTW W CYBERPRZESTRZENI

ANKIETA WSTĘPNA

OCENA WIEDZY I UMIEJĘTNOŚCI PRAKTYCZNYCH							
W każdym z pytań prosimy o zaznaczenie znakiem „X” odpowiedzi na poszczególne pytania w skali 7-punktowej gdzie: 1 - oznacza „zdecydowanie źle”, 2 - „źle”, 3 - „raczej źle”, 4 - „ani dobrze, ani źle”, 5 - „raczej dobrze, 6 – „dobrze”, 7 - „zdecydowanie dobrze”.							
Pytanie	***1***	***2***	***3***	***4***	***5***	***6***	***7***
1. Jak Pani / Pan ocenia swoją znajomość technik	□	□	□	□	□	□	□

socjotechnicznych stosowanych przez cyberprzestępców?							
2. Jak Pani/Pan ocenia swoją wiedzę na temat pishingu w korespondencji elektronicznej?	☐	☐	☐	☐	☐	☐	☐
3. Jak Pani/Pan ocenia swoją wiedzę na temat innych typów oszustw internetowych?	☐	☐	☐	☐	☐	☐	☐
4. Jak Pani / Pan ocenia swoją wiedzę na temat zasad cyberbezpieczeństwa?	☐	☐	☐	☐	☐	☐	☐
5. Jak Pani / Pan ocenia swoją umiejętność radzenia sobie w sytuacji wystąpienia zagrożenia oszustwem internetowym?	☐	☐	☐	☐	☐	☐	☐

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ I

CYBERPRZEMOC I CYBERPRZESTĘPSTWA

SESJA 2

TYPY OSZUSTW W CYBERPRZESTRZENI

ANKIETA KOŃCOWA

OCENA WIEDZY I UMIEJĘTNOŚCI PRAKTYCZNYCH							
W każdym z pytań prosimy o zaznaczenie znakiem „X" odpowiedzi na poszczególne pytania w skali 7-punktowej gdzie: 1 - oznacza „zdecydowanie źle", 2 - „źle", 3 - „raczej źle", 4 - „ani dobrze, ani źle", 5 - „raczej dobrze, 6 – „dobrze", 7 - „zdecydowanie dobrze".							
Pytanie	***1***	***2***	***3***	***4***	***5***	***6***	***7***
1. Jak Pani / Pan ocenia swoją znajomość technik socjotechnicznych stosowanych przez cyberprzestępców?	☐	☐	☐	☐	☐	☐	☐
2. Jak Pani/Pan ocenia swoją wiedzę na temat pishingu w korespondencji elektronicznej?	☐	☐	☐	☐	☐	☐	☐
3. Jak Pani/Pan ocenia swoją wiedzę na temat innych typów oszustw internetowych?	☐	☐	☐	☐	☐	☐	☐
4. Jak Pani / Pan ocenia swoją wiedzę na temat zasad cyberbezpieczeństwa?	☐	☐	☐	☐	☐	☐	☐
5. Jak Pani / Pan ocenia swoją umiejętność radzenia sobie w sytuacji wystąpienia zagrożenia oszustwem internetowym?	☐	☐	☐	☐	☐	☐	☐

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ I CYBERPRZEMOC I CYBERPRZESTĘPSTWA

SESJA 2 TYPY OSZUSTW W CYBERPRZESTRZENI

ANKIETA EWALUACYJNA

PROWADZENIE SZKOLENIA

1. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **wiedzę i przygotowanie merytoryczne** osoby prowadzącej szkolenie?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

2. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **umiejętność przekazania wiedzy** przez osobę prowadzącą szkolenie?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

3. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **kontakt i umiejętność pracy z grupą** osoby prowadzącej szkolenie?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

PROGRAM SZKOLENIA I MATERIAŁY DYDAKTYCZNE

4. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **przydatność szkolenia** w względem potrzeb uczestników?

Zdecydowanie nieprzydatne	*Raczej nieprzydatne*	*Trudno powiedzieć*	*Raczej przydatne*	*Zdecydowanie przydatne*
1	2	3	4	5

5. Proszę ocenić na pięciostopniowej skali, w jakim stopniu szkolenie pogłębiły Pani/Pana **wiedzę teoretyczną** z omawianego na szkoleniu obszaru?

Niewystarczająco	*Wystarczająco*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

6. Proszę ocenić na pięciostopniowej skali, w jakim stopniu przeprowadzone szkolenie pogłębiło Pani/Pana **umiejętności praktyczne** z omawianego na warsztatach tematu?

Niewystarczająco	*Wystarczająco*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

7. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **jasność i zrozumiałość** wykorzystanych **kart pracy**?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

8. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **przydatność ćwiczeń** w zdobyciu wiedzy i umiejętności z zakresu tematyki szkolenia ?

Zdecydowanie nieprzydatne	*Raczej nieprzydatne*	*Trudno powiedzieć*	*Raczej przydatne*	*Zdecydowanie przydatne*
1	2	3	4	5

9. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **jasność i zrozumiałość** wykorzystanej **prezentacji multimedialnej**?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

10. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **jasność i zrozumiałość materiałów dla uczestników**?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

CZĘŚĆ II

OCHRONA PRZED ATAKAMI

SESJA 1

KONTAKT I RELACJE Z UŻYTKOWNIKAMI INTERNETU

Tematyka:

I. Aktywność w sieci
II. Bezpieczeństwo i ochrona prywatności w sieci
III. Normy i zasady w relacjach z użytkownikami internetu

SESJA 2

BEZPIECZNA AKTYWNOŚĆ I WIZERUNEK W SIECI

Tematyka:

I. Wizerunek w serwisach społecznościowych
II. Prawo do ochrony wizerunku
III. Prywatność a cyfrowy ślad w sieci
IV. Wizerunek zawodowy

CYBERBEZPIECZEŃSTWO W PRACY I DOMU	
CZĘŚĆ II	OCHRONA PRZED ATAKAMI
SESJA 1	KONTAKT I RELACJE Z UŻYTKOWNIKAMI INTERNETU
CZAS TRWANIA	4 GODZINY SZKOLENIOWE

KONTAKT I RELACJE Z UŻYTKOWNIKAMI INTERNETU

TEMATYKA:

I. Aktywność w sieci
II. Bezpieczeństwo i ochrona prywatności w sieci
III. Normy i zasady w relacjach z użytkownikami internetu

REZULTATY:

- Omówienie rodzajów serwisów społecznościowych oraz oferowanych usług i możliwości dla użytkowników
- Analiza korzyści i zagrożeń związanych z aktywnością w serwisach społecznościowych
- Zdobycie wiedzy na temat zasad bezpiecznej aktywności i ochony prywatności w internecie
- Przekazanie informacji na temat netykiety - norm i zasad obowiązujących w internecie i mediach społecznościowych
- Rozwój umiejętności budowania pozytywnych relacji z użytkownikami internetu

PROGRAM SESJI:

I. Aktywność w sieci

a. Ankieta wstępna „Kontakt i relacje z użytkownikami internetu”

b. Wstęp „Serwisy społecznościowe” - dyskusja grupowa, omówienie osobistych doświadczeń uczestników
c. Quiz
d. Mini - wykład i prezentacja „Kontakt i relacje z użytkownikami internetu – Aktywność w sieci”
e. Przypadek 1. – omówienie i dyskusja grupowa

II. Bezpieczeństwo i ochrona prywatności w sieci

a. Mini - wykład i prezentacja „Kontakt i relacje z użytkownikami internetu – Bezpieczeństwo i ochrona prywatności w sieci”
b. Przypadek 2. – omówienie i dyskusja grupowa

III. Normy i zasady w relacjach z użytkownikami internetu

a. Ćwiczenie „Social media – korzyści i zagrożenia”
b. Ćwiczenie „Netykieta”
c. Mini-wykład i prezentacja „Kontakt i relacje z użytkownikami internetu – Normy i zasady w relacjach z użytkownikami internetu”

IV. Podsumowanie zajęć

Rozdanie materiałów informacyjnych
Podsumowanie „Kontakt i relacje z użytkownikami internetu”
Ankieta końcowa „Kontakt i relacje z użytkownikami internetu”
Ankieta ewaluacyjna

MATERIAŁY:

1. Karta pracy „Kontakt i relacje z użytkownikami internetu”
2. Materiały dla uczestników „Kontakt i relacje z użytkownikami internetu”
3. Prezentacja „Kontakt i relacje z użytkownikami internetu”
4. Podsumowanie „Kontakt i relacje z użytkownikami internetu”
5. Ankiety wstępna i końcowa „Kontakt i relacje z użytkownikami internetu”
6. Ankieta ewaluacyjna

KONTAKT I RELACJE Z UŻYTKOWNIKAMI INTERNETU

Karta pracy

AKTYWNOŚĆ W SIECI

Serwisy społecznościowe - kanały komunikacji w internecie pomiędzy ludźmi, które umożliwiają interakcję oraz dzielenie się wiadomościami o sobie za pomocą różnych narzędzi, takich jak blogi, fora, komunikatory, opcje udostępniania zdjęć, filmików wideo, plików muzycznych, itd.

Qiuz

Wpisz poniżej, do czego służą i jakie możliwości dają wymienione portale społecznościowe:

Facebook – .....

.....

YouTube – .....

.....

Instagram – .....

.....

Twitter – .....

.....

Pinterest – .....

.....

LinkedIn – .....

.....

TikTok - .....

.....

Profil w serwisach społecznościowych

- Dlaczego tak chętnie korzystamy z serwisów społecznościowych?
- Jakie są zalety i wady tworzenia i korzystania z prywatnych profili w serwisach społecznościowych typu facebook?

Przypadek 1.

Dorota jest mamą dwuletniej córeczki. Prowadzi publiczny i widoczny dla wszystkich profil na Facebooku, gdzie zaprosiła do znajomych całą swoją rodzinę, przyjaciół, sąsiadów i kolegów z obecnej i byłej pracy, ze studiów itd. Jest to ponad kilkaset osób, często mało jej znanych. Od jej urodzenia informuje ich na bieżąco o tym, że córeczka zrobiła pierwszy krok, wyszedł jej ząbek, nauczyła się siusiać na nocnik, dokumentuje rodzinne imprezy, wyjścia do parku, zabawy w piaskownicy. Robi jej wiele zdjęć, które nieomal codziennie zamieszcza na portalu. Cieszy się, kiedy się podobają się innym, nawet osobom nieznajomym. Ostatnio dyskutowała ze swoim mężem na ten temat, czy jest z jej strony właściwe zachowanie, czy nie powinna ograniczyć widoczność profilu lub ograniczyć ilość zdjęć.

Zadanie: Jakie powinny być zasady zamieszczania prywatnych zdjęć i informacji na portalach społecznościowych?

→ ……

→ ……

→ ……

→ ……

→ ……

Podsumowanie: Jakie konsekwencje teraz i w przyszłości może mieć nieprzemyślane zamieszczanie informacji na portalach społecznościowych?

BEZPIECZEŃSTWO I OCHRONA PRYWATNOŚCI W SIECI

- Jakie są zagrożenia związane z naszą aktywnością w sieci?
- O czym należy pamiętać nawiązując nowe znajomości?
- Jakie mogą być konsekwencje ujawniania zbyt wielu informacji na swój temat?

Przypadek 2.

Julia jest studentką I roku filologii polskiej. Uwielbia spędzać wolny czas na forum internetowym. Jej kolega zauważył, że kiedy się na nie loguje, posługuje się swoim imieniem i wiekiem (Julka2000). W postach zamieszczanych na forum pisze o swoich zainteresowaniach, zawodach pływackich, miejscach gdzie spędza czas np. pubach, imprezach. Ostatnio podała też nazwę ulicy, na której mieszka, i pochwaliła się, że za dwa tygodnie wyjeżdża w góry.

Zadanie: W jaki sposób powinniśmy chronić swoją prywatność na forach i portalach internetowych, jakich informacji nie należy podawać?

- ✓ ……
- ✓ ……
- ✓ ……
- ✓ ……

Zadanie: Jakie zasady powinny obowiązywać w przypadku dzieci i młodzieży?

- ✓ ……
- ✓ ……
- ✓ ……

✓ .....

NORMY I ZASADY W RELACJACH Z UŻYTKOWNIKAMI INTERNETU

- Jakie pozytywne i negatywne zjawiska związane są z aktywnością w portalach społecznościowych?
- W jaki sposób wpływają one na nasze życie i kontakty z innymi ludźmi?
- Jakie są zagrożenia, szczególnie w przypadku dzieci i młodzieży?

Ćwiczenie „Social media – korzyści i zagrożenia"

Zadanie: Wymień korzyści i zagrożenia związane z korzystaniem z portali społecznościowych i komunikatorów.

Korzyści

1. .....
2. .....
3. .....
4. .....
5. .....

Zagrożenia

1. .....
2. .....
3. .....
4. .....
5. .....

Ćwiczenie „Netykieta”

Zadanie: W parach lub w kilkuosobowych grupach przygotujcie 10 zasad netykiety, czyli zachowań które powinny być przestrzegane w relacjach z innymi użytkownikami internetu.

1. ……
   ……
2. ……
   ……
3. ……
   ……
4. ……
   ……
5. ……
   ……
6. ……
   ……
7. ……
   ……
8. ……
   ……
9. ……
   ……
10. ……

SŁOWNIK POJĘĆ

Administrator

Administrator to osoba, która zarządza danym profilem.

Ban

Ban to zawieszenie konta przez administratorów. Może być spowodowane publikowaniem treści naruszających regulamin portalu

Dostęp do informacji

Wiele serwisów społecznościowych zapewnia użytkownikowi wybór, kto może oglądać ich profil. Dzięki temu, że oznaczą swoje profile jako prywatne tylko upoważnione przez nie osoby mogą oglądać ich profile.

Fałszywe konta

Fałszywe konta to konta na Facebooku, Instagramie lub innych portalach społecznościowych, zakładane przez osoby podszywające się pod inną osobę.

Flame war

Inaczej „flaming", w wersji spolszczonej „flejm", to kłótnia internetowa, zwana też „wojną na obelgi", mająca miejsce przede wszystkim w mediach społecznościowych, na forach i grupach dyskusyjnych oraz w sekcji komentarzy pod wpisami blogowymi.

Hashtag

Jest to słowo poprzedzone symbolem kratki # z ang. *hash*. Służy on do grupowania określonych treści oraz informacji.

News Feed

Miejsce, w którym wyświetlają się aktywności naszych znajomych, a także posty stron, które polubiliśmy. Jest to główna, środkowa tablica, która wyświetla się zaraz po zalogowaniu.

Oś czasu

Z języka angielskiego Timeline, na Facebooku pełni funkcję tablicy, na której znajdują się wszystkie posty, zdjęcia, filmy, udostępnione treści, wydarzenia utworzone przez użytkownika lub stronę. Wszystko uporządkowane jest chronologicznie od wydarzeń najstarszych do najnowszych. Każdy profil i fanpage na Facebooku posiada swoją własną oś czasu.

Pin

Najważniejszy element serwisu społecznościowego Pinterest. Jest to materiał wizualny (najczęściej występujący w postaci infografiki) „przypinany" przez użytkownika do jego profilu. Zgodnie z przeznaczeniem strony, które sprowadza się do hasła *pin interest*, piny mają odzwierciedlać pasje użytkowników serwisu i obrazować ich główne obszary zainteresowań.

Podcast

Inaczej „podcasting", w języku polskim „podkast"/"podkasting", to internetowy odpowiednik audycji radiowej. Publikacja dźwiękowa o dowolnej tematyce, przyjmująca różnorodne formy, zazwyczaj udostępniana w odcinkach. Osobę, prowadzącą podcast, nazywa się hostem.

Snapchat

Aplikacja mobilna, umożliwiająca wysyłanie zdjęć i filmików (potocznie nazywanych „snapami"), które na ekranie odbiorcy wyświetlają się nie dłużej niż dziesięć sekund.

Social media

Platformy, portale oraz aplikacje internetowe, które pozwalają utrzymywać długofalowe relacje z wieloma użytkownikami sieci, w czasie rzeczywistym. Ich kluczowym atrybutem jest możliwość tworzenia oraz udostępniania treści, takich jak zdjęcia, materiały wideo, artykuły oraz komentarze.

Storytelling

Dosłownie „opowiadanie historii". W języku marketingu oznacza to takie kreowanie treści tworzonych przez markę – reklam, postów w mediach społecznościowych, blogowych notek, wszelkiego rodzaju publikacji papierowych i wielu innych – aby składały się one na spójną opowieść na temat tej marki.

TikTok

Aplikacja pozwalająca na tworzenie materiałów wideo, zsynchronizowanych z fragmentami utworów muzycznych i ich modyfikację za pomocą udostępnianych przez platformę narzędzi. Nagrania udostępniane na TikTok`u nie mogą być dłuższe niż 15 sekund.

Trolling

Inaczej trollowanie, to określenie odnoszące się do aspołecznego zachowania w sieci (negującego zasady netykiety), w tym również w serwisach społecznościowych. Głównym celem trolla (osoby trollującej) jest zburzenie lub zaburzenie porządku dyskusji poprzez dodawanie nieadekwatnych komentarzy, często obrażających lub ośmieszających innych uczestników panelu oraz nieuzasadnione działanie, pełne przekory, buntu lub arogancji.

Tweet

Krótka wiadomość tekstowa, umieszczana w serwisie Twitter. Jest to odpowiednik posta na Facebooku, jednak wyróżnia się skondensowaną formą, nieprzekraczającą 280 znaków (łącznie ze spacjami).

Viral

Interesująca lub zabawna treść, najczęściej w formie zdjęcia, mema czy materiału video, która szybko rozprzestrzenia się w internecie.

Vlog

Forma internetowej aktywności, która rozprzestrzeniła się na fali popularności kanałów streamingowych, w tym przede wszystkim serwisu YouTube. Osoby prowadzące tego typu

działalność nazywane są „vlogerami", a tworzone przez nich materiały nierzadko odnoszą sukces komercyjny, stając się ich głównym źródłem zarobku i w pełni profesjonalną twórczością.

KONTAKT I RELACJE Z UŻYTKOWNIKAMI INTERNETU

Materiały dla uczestników

AKTYWNOŚĆ W SIECI

Serwis społecznościowy to rodzaj portalu internetowego, który jest współtworzony przez grupę osób o podobnych zainteresowaniach lub poglądach. Tworzą go komunikatory do rozmów, fora i listy dyskusyjne. Istotą serwisów społecznościowych jest interakcja pomiędzy użytkownikami.

Są to kanały komunikacji między ludźmi, które umożliwiają interakcję oraz dzielenie się wiadomościami o sobie za pomocą różnych narzędzi, takich jak blogi, fora, komunikatory, opcje udostępniania zdjęć, filmików wideo, plików muzycznych, itd. Przejawia się ona m.in. w tworzeniu list znajomych, wysyłaniu wiadomości prywatnych pomiędzy użytkownikami, a także w sprawnym przepływie informacji, która odbywa się głównie za pomocą forów dyskusyjnych, blogów i stron pogawędek.

Media społecznościowe są obecnie stałym elementem naszego życia. Internet daje możliwość kontaktu z osobami, z którymi nie widujemy się na co dzień, poznawania osób o podobnych do naszych zainteresowaniach oraz podglądania tego, co polecają nasi znajomi. Trudno nie zauważyć, że powoli przesuwa się granica prywatności obowiązująca na portalach społecznościowych. Opublikowana w Internecie informacja żyje własnym życiem. Może również stanowić zagrożenie dla naszego bezpieczeństwa, gdy ujawniamy zbyt wiele informacje dotyczących naszego życia prywatnego.

Facebook, Instagram i inne media społecznościowe są obecne w wielu obszarach naszego życia - szukamy w nich rozrywki, śledzimy poczynania naszych znajomych, dzielimy się swoimi opiniami, podtrzymujemy kontakt z naszymi bliskimi, a nawet nawiązujemy znajomości. Niewielu z nas ma jednak świadomość, co może nam grozić. Oprócz wycieku wrażliwych danych czy udostępnianych przez nas informacji, źródłem niebezpieczeństwa jest również nasze zaufanie do znajomych.

Przegląd serwisów społecznościowych

- **Facebook**

  To platforma, na której można dzielić się treścią ze znajomymi, organizować wydarzenia, obserwować świat lub prowadzić rozbudowane kampanie reklamowe, przez co jest tak popularna i chętnie wykorzystywana nie tylko przez osoby prywatne, ale także wiele firm.

- **Twitter**

  Ten portal społecznościowy służy do zamieszczania chwytliwych i jednocześnie wyczerpujących temat wpisów, które następnie mogą kierować dalej, oczywiście jeśli do takiego postu dołączymy link. Jest jeszcze jedna charakterystyczna rzecz dla tego serwisu - używanie hashtagów w zamieszczanych wpisach, które pozwalają użytkownikom dużo szybciej natrafić np. na twój post, poruszający konkretny temat.

- **Instagram**

  Instagram to jeden z najpopularniejszych i najczęściej używanych serwisów do publikacji zdjęć i krótkich filmików. Jest także jednym z głównych kanałów, na których znani i lubiani (celebryci, blogerzy, vlogerzy) reklamują produkty lub usługi popularnych marek. Zasada działania serwisu jest prosta: robimy zdjęcie, dobieramy efekty i nakładamy filtry, hashtagujemy i publikujemy.

- **Youtube**

Jego głównym celem jest udostępnianie i oglądanie materiałów wideo. Serwis ten nieustannie zyskuje na popularności. Portal ten pozwala na subskrypcję ulubionych kanałów oraz wystawianie komentarzy do zamieszczanych tam treści.

- **LinkedIn**

  Portal społecznościowy, który specjalizuje się w kontaktach zawodowych i biznesowych. Jest to też największa na świecie sieć profesjonalna, gdzie profile prowadzą nie tylko osoby prywatne, które skrupulatnie przez lata budują tu swoje idealne CV, ale także headhunterzy i firmy, którzy chcą usprawnić proces rekrutacji oraz zbudować profesjonalny wizerunek przedsiębiorstwa.

- **Pinterest**

  Pinterest to agregat treści wizualnych. Użytkownicy serwisu gromadzą wiele zdjęć w poszczególnych katalogach, a następnie dzielą się nimi z pozostałymi odbiorcami, którzy mogą lajkować i komentować materiały.

- **Snapchat**

  Szczególnie popularny wśród młodego pokolenia. Głównym celem aplikacji jest udostępnienie możliwości szybkiego przesyłania plików multimedialnych, które w równie szybki sposób znikają z historii serwisu i przestają być widoczne dla użytkowników. Serwis oferuje takie narzędzia jak geofiltry czy maski, które pozwalają użytkownikom na jeszcze ciekawsze przedstawienie publikowanych treści.

- **Tumblr**

  To platforma mikroblogowa. Można dodawać na niej zdjęcia, filmy, cytaty, notatki lub muzykę. Użytkownicy serwisu mogą udostępniać dalej publikowane przez siebie treści, komentować czyjeś posty, lajkować inne wpisy oraz dostosowywać wygląd swoich mikroblogów do własnych koncepcji.

- **TikTok**

Aplikacja pozwalająca na tworzenie materiałów wideo, zsynchronizowanych z fragmentami utworów muzycznych i ich modyfikację za pomocą udostępnianych przez platformę narzędzi. Nagrania udostępniane na TikTok`u nie mogą być dłuższe niż 15 sekund.

BEZPIECZEŃSTWO I OCHRONA PRYWATNOŚCI W SIECI

Trudno nie zauważyć, że powoli przesuwa się granica prywatności obowiązująca na portalach społecznościowych. Opublikowana w Internecie informacja żyje własnym życiem. Może również stanowić zagrożenie dla naszego bezpieczeństwa, gdy ujawniamy zbyt wiele informacje dotyczących naszego życia prywatnego.

Może się też zdarzyć, że naruszy ona prawo lub wyrządzi szkodę innym użytkownikom sieci i spowoduje kłopoty. Oto przykłady informacji, których opublikowanie rodzi najpoważniejsze konsekwencje:

→ treści dotyczące osób prywatnych (np. zdjęcia, korespondencja) – mogą naruszać prywatność osoby, której dotyczą;

→ treści naruszające prawa autorskie lub znaki towarowe – teksty, muzyka, zdjęcia, filmy

→ treści satyryczne – mogą balansować na cienkiej granicy między żartem a treściami obraźliwymi. Mogą też naruszać prawa autorskie.

→ treści oszczercze, obraźliwe, mogą naruszyć dobra osobiste pomawianej lub

obrażanej osoby,

→ treści nawołujące do przemocy – mogą naruszyć dobra osobiste ale również prawo karne (jeśli np. podżegają do nienawiści na tle rasowym czy religijnym).

→ Treści niejawne (np. tajne dokumenty, informacje będące tajemnicą handlową firm). Zdarza się, że naruszają nie tylko tajemnicę, ale również prawa osób, których dane pojawiają się w tych dokumentach.

W każdym przypadku odpowiedzialność za opublikowanie treści naruszających prawo lub prawa innych osób ponosi w pierwszym rzędzie sam publikujący.

NORMY I ZASADY W RELACJACH Z UŻYTKOWNIKAMI INTERNETU

Netykieta to zasady zachowania, które odpowiadają na pytanie: jak zachowywać się w internecie? Nie ma jednej ustalonej odgórnie netykiety. W sieci obowiązują nas jednak te same zwyczaje, które stosujemy w życiu: dobre maniery, kultura. Najważniejsze, żeby pamiętać o drugim człowieku, szanować go i traktować kulturalnie.

Podstawowe zasady netykiety

- **Szanuj innych i traktuj ludzi tak, jak chcesz aby traktowali Ciebie**

Dotyczy to wszystkiego, co robisz w sieci, wszystkich serwisów i typów aktywności. Internet to nie tylko wirtualne połączenia i boty: to przede wszystkim ludzie, którzy wymagają szacunku.

- **Sprzeciw się hejtowi**

Postępując zgodnie z zasadami netykiety - nawet jeśli spotka Cię hejt, nie odpłacaj pięknym za nadobne. Nie daj się sprowokować, nie publikuj poniżających komentarzy czy grafik.

- **Nie trolluj**

Trollowanie - to publikowanie zaczepnych treści wyłącznie po to, by wywołać reakcję. Nie rób tego, dyskutuj merytorycznie, elegancko i kulturalnie. Trzymaj się faktów. Zamiast kogoś poniżyć, zostań lepiej mistrzem retoryki. Nawet jeśli trollowanie przynosi popularność, będzie to tylko krótkotrwały rozgłos.

- **Uważaj na fake newsy**

Trafiasz w sieci na szokującą wiadomość, w emocjach podajesz dalej. Z czasem okazuje się, że to nieprawda, ktoś publikuje krótkie sprostowanie – ale obraz pozostał w głowach wielu. Zanim opublikujesz jakąś szokującą wiadomość, sprawdź, czy podają ją przynajmniej dwa poważne źródła, np. różne media.

- **Szanuj prawo do własności w sieci**

Jeśli publikujesz obrazek czy wypowiedź, podaj autora i źródło. Postępują zgodnie z netykietą i nigdy nie przywłaszczaj sobie cudzych treści: to nic innego jak kradzież. Nie pozwalaj też innym na wykorzystanie Twoich autorskich treści bez zezwolenia.

- **Dbaj o prywatność swoją i innych**

Nie publikuj wiadomości, które dostałeś przez prywatny kanał. Jeśli jest to konieczne, nigdy nie pokazuj innym adresu, nazwiska ani żadnych danych nadawcy.

- **Respektuj zasady grupy**

Poszczególne grupy w sieci mają różną kulturę i swoje zasady netykiety. Zacznij od zapoznania się z zasadami grupy. Jeśli masz wątpliwość, czy możesz opublikować daną treść – spytaj o to administratora. Sprawdź też, jaki jest w danej społeczności styl wypowiedzi. Dopasuj się do zasad, które zostały ustalone przez założycieli.

- **Postuj odpowiedzialnie**

Zastanów się dwa razy, zanim coś opublikujesz. Czy ta treść nadawałaby się, by pokazać ją

znajomym? Czy jej treść nie byłaby zbyt głupia lub wstydliwa? Czy Twoja społeczność ma ochotę to czytać i oglądać? Unikaj *offtopów* (*off-topic*, OF – dygresja), czyli publikowania wiadomości niezwiązanych z tematem w ściśle tematycznych grupach czy na forach.

- **Uważaj z ironią i sarkazmem**

W komunikacji bezpośredniej mimika, wzrok i gesty mają dużo większe znaczenie dla całości wypowiedzi niż sama jej treść. Tekst pisany rządzi się innymi prawami niż mówiony, ironia, sarkazm, specyficzny ton wypowiedzi – tu bardzo łatwo o nieporozumienia.

- **Miej umiar**

Życie nie kończy się na świecie wirtualnym. W wielu sytuacjach – na przykład ostrych dyskusji – warto po prostu skończyć rozmowę, wylogować się i pójść na spacer lub porozmawiać z kimś bliskim.

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ II

OCHRONA PRZED ATAKAMI

SESJA 1

KONTAKT I RELACJE Z UŻYTKOWNIKAMI INTERNETU

PODSUMOWANIE

1. Który numer możemy udostępnić znajomym na Facebooku bez obawy o bezpieczeństwo?
    a. PESEL
    b. Numer dowodu
    c. Żadne z powyższych

2. Jaka metoda daje nam stuprocentowe bezpieczeństwo poruszania się po sieci?
    a. Instalacja oprogramowania antywirusowego
    b. Częsta zmiana haseł
    c. Nie ma stuprocentowej pewności, w Internecie zawsze obowiązuje zasada

ograniczonego zaufania

3. Które z poniższych haseł można uznać za bezpieczne?
    a. Zuziamalik22
    b. &&@22Rt1k0rK!
    c. qwerty

4. Czy ciasteczko w przeglądarce to:
    a. mały plik zapisywany przez przeglądarkę, który pozwala na śledzenie aktywności w sieci
    b. niespodzianka, zwykle gra lub łamigłówka
    c. zabawny mem

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ II

OCHRONA PRZED ATAKAMI

SESJA 1

KONTAKT I RELACJE Z UŻYTKOWNIKAMI INTERNETU

PODSUMOWANIE

1. Który numer możemy udostępnić znajomym na Facebooku bez obawy o bezpieczeństwo?
    a. PESEL
    b. Numer dowodu
    c. Żadne z powyższych

2. Jaka metoda daje nam stuprocentowe bezpieczeństwo poruszania się po sieci?
    a. Instalacja oprogramowania antywirusowego
    b. Częsta zmiana haseł

c. Nie ma stuprocentowej pewności, w Internecie zawsze obowiązuje zasada ograniczonego zaufania

3. Które z poniższych haseł można uznać za bezpieczne?
   a. Zuziamalik22
   b. &&@22Rt1k0rK!
   c. qwerty

4. Czy ciasteczko w przeglądarce to:
   a. mały plik zapisywany przez przeglądarkę, który pozwala na śledzenie aktywności w sieci
   b. niespodzianka, zwykle gra lub łamigłówka
   c. zabawny mem

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ II

OCHRONA PRZED ATAKAMI

SESJA 1

KONTAKT I RELACJE Z UŻYTKOWNIKAMI INTERNETU

ANKIETA WSTĘPNA

OCENA WIEDZY I UMIEJĘTNOŚCI PRAKTYCZNYCH							
W każdym z pytań prosimy o zaznaczenie znakiem „X” odpowiedzi na poszczególne pytania w skali 7-punktowej gdzie: 1 - oznacza „zdecydowanie źle”, 2 - „źle”, 3 - „raczej źle”, 4 - „ani dobrze, ani źle”, 5 - „raczej dobrze, 6 – „dobrze”, 7 - „zdecydowanie dobrze”.							
Pytanie	***1***	***2***	***3***	***4***	***5***	***6***	***7***

1. Jak Pani / Pan ocenia swoją znajomość serwisów społecznościowych oraz oferowanych usług i możliwości dla użytkowników?	□	□	□	□	□	□	□
2. Jak Pani/Pan ocenia swoją wiedzę na temat korzyści i zagrożeń związanych z aktywnością w serwisach społecznościowych?	□	□	□	□	□	□	□
3. Jak Pani/Pan ocenia swoją wiedzę na temat zasad bezpiecznej aktywności i ochony prywatności w internecie?	□	□	□	□	□	□	□
4. Jak Pani / Pan ocenia swoją wiedzę na temat zasad norm i zasad obowiązujących w internecie i mediach społecznościowych?	□	□	□	□	□	□	□
5. Jak Pani / Pan ocenia swoją umiejętność umiejętności budowania pozytywnych relacji z użytkownikami internetu?	□	□	□	□	□	□	□

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ II

OCHRONA PRZED ATAKAMI

SESJA 1

KONTAKT I RELACJE Z UŻYTKOWNIKAMI INTERNETU

ANKIETA KOŃCOWA

OCENA WIEDZY I UMIEJĘTNOŚCI PRAKTYCZNYCH
W każdym z pytań prosimy o zaznaczenie znakiem „X” odpowiedzi na poszczególne pytania w skali 7-punktowej gdzie: 1 - oznacza „zdecydowanie źle”, 2 - „źle”, 3 - „raczej źle”, 4 - „ani dobrze, ani źle”, 5 - „raczej dobrze, 6 – „dobrze”, 7 - „zdecydowanie dobrze”.

Pytanie	*1*	*2*	*3*	*4*	*5*	*6*	*7*
1. Jak Pani / Pan ocenia swoją znajomość serwisów społecznościowych oraz oferowanych usług i możliwości dla użytkowników?	□	□	□	□	□	□	□
2. Jak Pani/Pan ocenia swoją wiedzę na temat korzyści i zagrożeń związanych z aktywnością w serwisach społecznościowych?	□	□	□	□	□	□	□
3. Jak Pani/Pan ocenia swoją wiedzę na temat zasad bezpiecznej aktywności i ochony prywatności w internecie?	□	□	□	□	□	□	□
4. Jak Pani / Pan ocenia swoją wiedzę na temat zasad norm i zasad obowiązujących w internecie i mediach społecznościowych?	□	□	□	□	□	□	□
5. Jak Pani / Pan ocenia swoją umiejętność umiejętności budowania pozytywnych relacji z użytkownikami internetu?	□	□	□	□	□	□	□

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ II OCHRONA PRZED ATAKAMI

SESJA 1 KONTAKT I RELACJE Z UŻYTKOWNIKAMI INTERNETU

ANKIETA EWALUACYJNA

PROWADZENIE SZKOLENIA

1. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **wiedzę i przygotowanie merytoryczne** osoby prowadzącej szkolenie?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

2. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **umiejętność przekazania wiedzy** przez osobę prowadzącą szkolenie?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

3. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **kontakt i umiejętność pracy z grupą** osoby prowadzącej szkolenie?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

PROGRAM SZKOLENIA I MATERIAŁY DYDAKTYCZNE

4. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **przydatność szkolenia** w względem potrzeb uczestników?

Zdecydowanie nieprzydatne	*Raczej nieprzydatne*	*Trudno powiedzieć*	*Raczej przydatne*	*Zdecydowanie przydatne*
1	2	3	4	5

5. Proszę ocenić na pięciostopniowej skali, w jakim stopniu szkolenie pogłębiły Pani/Pana **wiedzę teoretyczną** z omawianego na szkoleniu obszaru?

Niewystarczająco	*Wystarczająco*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

6. Proszę ocenić na pięciostopniowej skali, w jakim stopniu przeprowadzone szkolenie pogłębiło Pani/Pana **umiejętności praktyczne** z omawianego na warsztatach tematu?

Niewystarczająco	*Wystarczająco*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

7. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **jasność i**

zrozumiałość wykorzystanych **kart pracy**?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

8. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **przydatność ćwiczeń** w zdobyciu wiedzy i umiejętności z zakresu tematyki szkolenia ?

Zdecydowanie nieprzydatne	*Raczej nieprzydatne*	*Trudno powiedzieć*	*Raczej przydatne*	*Zdecydowanie przydatne*
1	2	3	4	5

9. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **jasność i zrozumiałość** wykorzystanej **prezentacji multimedialnej**?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

10. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **jasność i zrozumiałość materiałów dla uczestników**?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ II	OCHRONA PRZED ATAKAMI

SESJA 2	BEZPIECZNA AKTYWNOŚĆ I WIZERUNEK W SIECI

CZAS TRWANIA	4 GODZINY SZKOLENIOWE

BEZPIECZNA AKTYWNOŚĆ I WIZERUNEK W SIECI

TEMATYKA:

I. Wizerunek w serwisach społecznościowych
II. Prawo do ochrony wizerunku
III. Prywatność a cyfrowy ślad w sieci
IV. Wizerunek zawodowy

REZULTATY:

- Analiza wpływu aktywności w serwisach społecznościowych na kształtowanie wizerunku w internecie
- Zdobycie wiedzy na temat prawa do ochrony wizerunku w internecine
- Omówienie zagrożen i konsekwencji cyfrowego śladu w sieci
- Przekazanie informacji na zasad kształtowania profesjonalnego wizerunku zawodowego w sieci

PROGRAM SESJI:

I. Wizerunek w serwisach społecznościowych

a. Ankieta wstępna „Bezpieczna aktywność i wizerunek w sieci”
b. Wstęp „W jaki sposób profil na portalach społecznościowych może wpływać na nasz wizerunek?” - dyskusja grupowa, omówienie osobistych doświadczeń uczestników
c. Przypadek 1. – omówienie i dyskusja grupowa
d. Mini - wykład i prezentacja „Bezpieczna aktywność i wizerunek w sieci – Wizerunek w serwisach społecznościowych”

II. Prawo do ochrony wizerunku

a. Przypadek 2. – omówienie i dyskusja grupowa
b. Mini - wykład i prezentacja „Bezpieczna aktywność i wizerunek w sieci – Prawo do ochrony wizerunku”

III. Prywatność a cyfrowy ślad w sieci

a. Przypadek 3. – omówienie i dyskusja grupowa
b. Mini-wykład i prezentacja „Bezpieczna aktywność i wizerunek w sieci - Prywatność a cyfrowy ślad w sieci”

IV. Wizerunek zawodowy

a. Zadanie – „Profesjonalny wizerunek zawodowy”
b. Mini-wykład i prezentacja „Bezpieczna aktywność i wizerunek w sieci – Wizerunek zawodowy”

V. Podsumowanie zajęć

Rozdanie materiałów informacyjnych

Podsumowanie „Bezpieczna aktywność i wizerunek w sieci”

Ankieta końcowa „Bezpieczna aktywność i wizerunek w sieci”

Ankieta ewaluacyjna

MATERIAŁY:

1. Karta pracy „Bezpieczna aktywność i wizerunek w sieci”
2. Materiały dla uczestników „Bezpieczna aktywność i wizerunek w sieci”
3. Prezentacja „Bezpieczna aktywność i wizerunek w sieci”
4. Podsumowanie „Bezpieczna aktywność i wizerunek w sieci”
5. Ankiety wstępna i końcowa „Bezpieczna aktywność i wizerunek w sieci”
6. Ankieta ewaluacyjna

BEZPIECZNA AKTYWNOŚĆ I WIZERUNEK W SIECI

Karta pracy

WIZERUNEK W SERWISACH SPOŁECZNOŚCIOWYCH

- W jaki sposób profil na portalu społecznościowych może wpływać na postrzeganie naszej osoby, zarówno w sytuacjach prywatnych jak i zawodowych?
- Jakie informacje możemy uzyskać na podstawie

profili społecznościowych?

Przypadek 1.

Tomek jest absolwentem Technikum Samochodowego. Prowadzi publiczny i widoczny dla wszystkich profil na Facebooku, gdzie zaprosił do znajomych ponad 1000 osób. Jest zagorzałym kibicem piłki nożnej, chodzi na mecze swojego ukochanego klubu, co również dokumentuje licznymi zdjęciami. Jest osobą o bardzo zdecydowanych poglądach, lubi komentować różne wydarzenia polityczne w kraju, czy sytuacje które mają miejsce w jego dzielnicy. Jest aktywny na forach i grupach dyskusyjnych, gdzie zamieszcza liczne komentarze, które wzbudzają liczne, często burzliwe reakcje.

Zadanie: Zastanów się i napisz, o czym powinniśmy pamiętać prowadząc profil na portalach społecznościowych?

→ ……

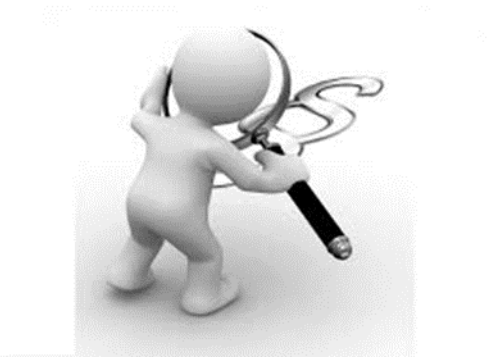
→ ……

→ ……

→ ……

Podsumowanie: Jaki wpływ na nasz wizerunek, może mieć treść i forma informacji zamieszczanych w serwisach społecznościowych?

PRAWO DO OCHRONY WIZERUNKU



- Czym jest wizerunek?
- Co to znaczy rozpowszechnianie wizerunku?
- W jakich sytuacjach może dojść do naruszenia prawa do ochrony wizerunku?
- Jakie mogę być konsekwencje naruszenia prawa do ochrony wizerunku?

Przypadek 2.

Była impreza urodzinowa mojej koleżanki z pracy, które urządziła w popularnym pubie. Przyszło dużo znajomych, również też jacyś ludzie, których nie znałam. Dziewczyny zaczęły się wygłupiać, sporo wypiły, śpiewały piosenki, tańczyły na środku, trochę straciły kontrolę. Robiły sobie śmieszne zdjęcia, w dość wyzywających pozach, zaczęły tańczyć na barze, atmosfera była gorąca. Następnego dnia z przerażeniem zobaczyły, ze znalazły się one na profilu jednej z osób obecnych w pubie. Co gorsza, były one udostępnione publicznie, widoczne dla wszystkich, w tym pracowników firmy, przełożonych, klientów. Zaczęły dostawać maile ze złośliwymi uwagami, stało się to również tematem licznych plotek. Bały się też poważniejszych konsekwencji swojej mało odpowiedzialnej zabawy.

Zadanie: Wymień przykłady sytuacji, w których może dojść do naruszenia prawa do ochrony wizerunku?

→ ……

→ ……

→ ……

→ ……

Podsumowanie: Co należy zrobić w sytuacji naruszenia prawa do ochrony wizerunku? Jakie działania możemy i powinniśmy podjąć?

PRYWATNOŚĆ A CYFROWY ŚLAD W SIECI

- Jakie informacje udostępniamy o sobie, korzystając z przeglądarki internetowej, smartfonów i aplikacji?
- Jakie konsekwencje może mieć ujawnianie informacji o sobie w sieci?

Przypadek 3.

Hanna już od kilku lat biega w weekendy po lesie. Na urodziny dostała w prezencie smartfona. Zainstalowała aplikację do śledzenia postępów w bieganiu. Podczas instalacji wyraziła zgodę na to, by aplikacja miała dostęp do informacji w jej telefonie, m.in. informację o lokalizacji. Za każdym razem, kiedy idzie pobiegać, bierze ze sobą telefon. Aplikacja zlicza przebiegnięte kilometry, rejestruje trasę jej biegu, spalone kalorie. Te informacje automatycznie zamieszczane są na portalu społecznościowym, na którym Justyna ma konto. Dzięki temu wszyscy jej znajomi wiedzą, kiedy Hanna biega. Cieszy się, kiedy dostaje pozytywne komentarze z uznaniem dla jej postępów. Z niektórymi osobami umawia się na swojej planowanej trasie. Wymienia się również z nimi informacjami na temat najnowszego sprzętu sportowego, planowanych startów, najnowszych nowinek dietetycznych, zabiegów rehabilitacyjnych i polecanych salonów masażu?

Zadanie: Jakie informacje o Hannie można uzyskać na podstawie historii treningów i jej wpisów?

→ ……

→ ……

→ ……

→ ……

Podsumowanie: Jakie mogą być konsekwencje związane z zamieszczaniem informacji w sieci np. poprzez wykorzystywane aplikacje?

WIZERUNEK ZAWODOWY

- Czy warto kreować swój wizerunek zawodowy w sieci np. w portalach społecznościowych?
- O czym należy pamiętać zamieszczając informacje na swój temat w mediach?
- W jaki sposób może to wpływać na nasze życie zawodowe?

Zadanie: Zastanów się i wymień zasady tworzenia profesjonalnego wizerunku w sieci.

Należy:

1. ……

2. ……

3. ……

4. ……

Warto / można:

1. ……

2. ……

3. ……

4. ……

Nie wolno:

1. ……

2. ……

3. ……

4. ……

SŁOWNIK POJĘĆ

Autonomia informacyjna

Ważny aspekt prywatności, prawo do samodzielnego decydowania o ujawnianiu informacji na swój temat oraz do kontrolowania informacji dotyczących własnej osoby.

Cookies (tzw. ciasteczka)

Niewielkie pliki tekstowe wysyłane przez odwiedzany serwis internetowy do urządzenia internauty (komputer, smartfon itp.). W większości przeglądarek internetowych można: kasować pliki typu cookies z twardego dysku komputera (z poziomu ustawień przeglądarki), zablokować pliki typu cookies lub ustawić ostrzeżenie przed zapisaniem ich na dysku.

Cyfrowy ślad

Informacje na temat aktywności konkretnych osób w sieci, magazynowane na serwerach dostawców Internetu i właścicieli stron. Tworzą go m.in. zdjęcia, informacje o kupionych produktach, nicki, wpisy na blogach, ale również dane, które zostawiamy w sieci mimowolnie, np. adres IP czy informacja o systemie operacyjnym, z którego korzystamy.

Dane osobowe

Wszelkie informacje dotyczące konkretnej osoby fizycznej – zidentyfikowanej (np. takiej, którą znamy bezpośrednio) lub możliwej do zidentyfikowania (czyli takiej, którą można wskazać na podstawie posiadanych informacji). Dane osobowe podlegają ochronie i nie mogą być zbierane bez odpowiedniej podstawy prawnej (np. zgody osoby, której dotyczą).

Dobra osobiste

Przysługujące każdemu człowiekowi dobra o charakterze niemajątkowym, chronione prawem cywilnym. Należą do nich m.in. zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, prawo do prywatności, poczucie przynależności do płci.

Mem internetowy

Popularna internetowa forma komentowania rzeczywistości, zazwyczaj przybierająca formę graficzną (rysunek, zdjęcie) z nałożonym krótkim tekstem. Memy charakteryzują się dużym potencjałem wiralnym – powielane i komentowane przez użytkowników sieci mogą dotrzeć do szerokich rzesz odbiorców.

Ochrona wizerunku

Wizerunek każdej osoby (czyli jej podobizna utrwalona np. na zdjęciu bądź filmie) podlega ochronie. Oznacza to, że nie może on być rozpowszechniany bez zgody danej osoby. Istnieją jednak wyjątki.

Profilowanie

Oparty na określonych algorytmach mechanizm, który służy kategoryzowaniu ludzi według ich cech, zachowań, preferencji, stosowany m.in. w marketingu internetowym. Jest stosowany m.in. w marketingu internetowym w celu prezentowania reklam dopasowanych jak najściślej do potrzeb określonych użytkowniczek i użytkowników sieci.

Prywatność

Sfera życia człowieka, w którą nie należy wkraczać bez pozwolenia. Ma ona swój aspekt cielesny, terytorialny, informacyjny i komunikacyjny. Prywatność jest chroniona przez prawo (m.in. przez Konstytucję RP i akty prawa międzynarodowego). Ograniczenie prawa do prywatności możliwe jest tylko w określonych sytuacjach.

Wizerunek

Utrwalona podobizna człowieka przedstawiająca cechy wyglądu, które pozwalają na jego identyfikację. Na wizerunek składają się zarówno cechy naturalne, m.in. rysy twarzy, postaci czy budowa ciała, jak i dodane, np. fryzura, makijaż, ubranie, okulary (o ile są charakterystyczne dla danej osoby). Wizerunek podlega ochronie prawnej. Wizerunek każdej osoby (czyli jej podobizna utrwalona np. na zdjęciu bądź filmie) podlega ochronie. Oznacza to, że nie może on być rozpowszechniany bez zgody danej osoby.

BEZPIECZNA AKTYWNOŚĆ I WIZERUNEK W SIECI

Materiały dla uczestników

WIZERUNEK W SERWISACH SPOŁECZNOŚCIOWYCH

W Internecie każdy z nas kształtuje swój wizerunek: udzielając się na forach dyskusyjnych, komentując artykuły, korzystając z portali społecznościowych, prowadząc blogi. Ważne aby robić to świadomie i z dbałością o możliwe konsekwencje.

Serwisy społecznościowe:

- ogólne serwisy społecznościowe – np. Facebook
- biznesowe serwisy społecznościowe np. LinkedIn
- fotograficzne serwis społecznościowe np. Instagram, Snapchat
- społeczności kontentowe np. YouTube, Pinterest
- mikroblogi np. Twitter

Jak świadomie korzystać z serwisów społecznościowych?

→ Zanim założysz konto, zastanów się, czy jest to wybór odpowiedni dla Ciebie? Może lepiej wyrazisz siebie za pomocą innego medium, np. bloga?

→ Zadbaj o swoją prywatność: ogranicz widoczność wpisów do grona swoich znajomych, możliwość oznaczania Cię na zdjęciach i we wpisach; akceptuj zaproszenia tylko od osób, które rzeczywiście znasz.

→ Zanim opublikujesz jakąś informację czy zdjęcie, zastanów się, jakie to może mieć konsekwencje dla Ciebie i innych. Czy chciałbyś(-abyś), żeby każdy mógł za kilkanaście lat znaleźć tę informację w sieci?

→ Wykorzystuj pozytywny potencjał portali: wyszukuj i dziel się wartościowymi informacjami.

PRAWO DO OCHRONY WIZERUNKU

Dobra osobiste

Każdemu człowiekowi przysługuje prawo do ochrony wizerunku, który jest jednym z dóbr osobistych. Dobra osobiste to przysługujące każdemu człowiekowi dobra o charakterze niemajątkowym, chronione prawem cywilnym. Należą do nich m.in. nazwisko lub pseudonim, wizerunek, prawo do prywatności.

Dobra osobiste podlegają ochronie na podstawie przepisów prawa cywilnego – osoba, która uważa, że ktoś je narusza, może dochodzić swoich praw w sądzie: żądać zaprzestania takich działań, odszkodowania lub zadośćuczynienia. Ochronę taką przewiduje także ustawa o prawie autorskim i prawach pokrewnych.

Wizerunek jest rozumiany bardzo szeroko: mogą to być cechy twarzy i całej postaci, budowa ciała – innymi słowy cechy wyglądu, na podstawie których można kogoś rozpoznać. Wizerunek może być utrwalany na różne sposoby, np. w formie zdjęcia, obrazu, filmu, karykatury; przy pomocy różnych narzędzi, np. aparatu fotograficznego, smartfona, tabletu, drona, a także ołówka i kartki papieru.

Wizerunek każdej osoby (czyli jej podobizna utrwalona np. na zdjęciu bądź filmie) podlega ochronie. Oznacza to, że nie może on być rozpowszechniany bez zgody danej osoby.

Rozpowszechnianie wizerunku

Rozpowszechnianie wizerunku to umożliwienie zapoznania się z wizerunkiem bliżej nieokreślonemu, niezamkniętemu kręgowi osób, np. publikacja w prasie, na blogu, w otwartej grupie na portalu społecznościowym, wywieszenie na ogólnodostępnej tablicy. Rozpowszechnianie wizerunku wymaga zgody osoby na nim przedstawionej. Nie dotyczy to sytuacji, gdy osoba taka otrzymała opłatę za pozowanie. Ustawa przewiduje również kilka wyjątków dotyczących rozpowszechniania wizerunku.

Zgoda nie jest wymagana, jeżeli:

- wizerunek osoby powszechnie znanej wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych,
- osoba stanowi jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza.

Naruszenie dóbr osobistych

Osoba, która trafia w sieci na materiał, który jest widocznym naruszeniem dóbr osobistych jej lub innej osoby, przede wszystkim powinna zawiadomić administratora strony, na której znalazła daną treść. Wiele stron, zwłaszcza popularne portale społecznościowe, ułatwia zgłaszanie naruszeń, np. umieszczając służący specjalnie do tego celu przycisk albo formularz. Administrator strony powinien zareagować na zgłoszenie naruszenia.

Warto pamiętać o utrwaleniu naruszenia (np. zrobieniu zrzutu ekranu), po to by móc w przyszłości wykorzystać je jako dowód. Osoba, która uważa, że jej prawo do wizerunku zostało naruszone, może domagać się usunięcia treści, a także dochodzić odszkodowania i zadośćuczynienia w sądzie. W przypadku naruszenia dóbr osobistych można wstąpić na drogę cywilną i domagać się spełnienia określonych roszczeń.

Wizerunek w social media

Trudno wyznaczyć wyraźną granicę, gdzie zaczyna się, a gdzie kończy rozpowszechnianie wizerunku. Dostępne technologie sprawiają, że od utrwalenia wizerunku do jego rozpowszechnienia jest naprawdę niedaleko. Pokazanie zdjęcia koledze nie jest rozpowszechnianiem, ale opublikowanie go na otwartym blogu w sieci – już tak.

Opublikowanie tego samego wizerunku w zamkniętej grupie na portalu społecznościowym przynajmniej teoretycznie nie jest rozpowszechnianiem. Sytuacja jest jednak trudna do jednoznacznej oceny, gdy grupa jest duża lub dostęp do niej swobodny. Co więcej –

wystarczy, że jeden z członków grupy skopiuje wizerunek i umieści go na innym portalu, który jest publicznie dostępny, by wizerunek został rozpowszechniony.

PRYWATNOŚĆ A CYFROWY ŚLAD W SIECI

Ślad cyfrowy odnosi się do wszystkich śladów pozostawionych podczas korzystania z Internetu. Są to informacje przesyłane online, takie jak rejestracja formularzy, e-maile i załączniki, przesyłanie filmów wideo lub obrazów cyfrowych i inne formy przekazywania informacji. Wszystko to pozostawia ślady informacji osobistych o sobie i tym, co robisz, dostępne innym online.

Trzeba mieć świadomość, że w Internecie udostępniamy informacje na swój temat nie tylko samodzielnie, tj. w sposób intencjonalny (statusy, komentarze), ale także w sposób automatyczny (adres IP, język, system operacyjny) oraz półautomatyczny (geolokalizacja – np. przez Endomondo, popularną aplikację na smartfona). E-maile odebrane przez usługę Gmail są skanowane i na podstawie najczęściej występujących słów są użytkownikom dobierane reklamy. Niektóre aplikacje w smartfonie żądają m.in. dostępu do listy kontaktów czy zawartości kalendarza. Wyszukiwarka Google zapamiętuje historię zapytań, smartfon, nawet przy wyłączonej funkcji GPS, zapamiętuje lokalizacje na podstawie sieci Wi-Fi, które „spotyka" w różnych miejscach.

Nasze dane gromadzą różne podmioty, m. in. operatorzy sieci komórkowych, producenci telefonów i oprogramowania, dostawcy usług internetowych, agencje reklamowe.

Profilowanie to powszechne zjawisko polegające na zbieraniu informacji o konsumencie na podstawie jego zachowań w sieci.

To oparty na określonych algorytmach mechanizm, który służy kategoryzowaniu ludzi według ich cech, zachowań, preferencji. Jest stosowany m.in. w marketingu internetowym w celu prezentowania reklam dopasowanych jak najściślej do potrzeb określonych użytkowniczek i użytkowników sieci. Wiele sklepów działających w branży e-commerce stosuje profilowanie,

które jest skutecznym sposobem na bardziej efektywną sprzedaż produktów, przy jednoczesnym zmniejszeniu nakładów finansowych na działania promocyjne.

WIZERUNEK ZAWODOWY W SIECI

W procesie rekrutacyjnym rekruter zwykle stara się w różny sposób uzupełnić wiedzę o niektórych kandydatach i posługuje się w tym celu internetem. Serwisy społecznościowe są źródłem nieograniczonej wiedzy o użytkownikach, a beztroskie podchodzenie do kwestii udostępniania różnych treści może rzutować negatywnie na szanse kandydata do pracy.

Facebook

Profil na Facebooku może być dostępny dla każdego, kto jest zarejestrowany w serwisie. Warto zadbać o kwestię prywatności na Facebooku, m.in. o ograniczenie widoczności profilu oraz treści, jakie na nim publikujemy i udostępniamy - znajomym czy wszystkim użytkownikom serwisu społecznościowego. Po zalogowaniu się na konto w prawym górnym rogu serwisu FB, znajduje się oznaczenie kłódki. Można tam ustawić wszelkie kwestie dotyczące prywatności. Warto także wyłączyć opcję wyszukiwanie publiczne, dzięki czemu po wpisaniu imienia i nazwiska w wyszukiwarkę internetową nie będzie możliwości znalezienia naszego profilu w serwisie Facebook.

LinkedIn

Kolejnym etapem jest stworzenie profilów na portalach typu GoldenLine, Profeo i LinkedIn, a także w serwisach rekrutacyjnych. Dokładne wypełnienie rubryk, wpisanie kluczowych stanowisk i odpowiednie podsumowanie przebiegu dotychczasowej kariery zawodowej mogą stanowić o tym, czy rekruterzy znajdą nas wśród tysięcy innych zarejestrowanych osób.

Rekruter na pewno przyjrzy się zainteresowaniom i hobby kandydata; będzie chciał zobaczyć, jakim człowiekiem jest prywatnie, jaką ma osobowość. Prawdopodobnie sprawdzi też, kogo ma w swoich kontaktach oraz prześledzi ścieżkę kariery zawodowej i doświadczenie. Częstym dylematem jest kwestia wstawiania swojego zdjęcia w profilu zawodowym. Nie jest to

konieczne, ale rekruterzy lubią widzieć, jak dana osoba wygląda – to ułatwia kontakt, a także pomaga lepiej zapamiętać kandydata.

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ II

OCHRONA PRZED ATAKAMI

SESJA 2

BEZPIECZNA AKTYWNOŚĆ I WIZERUNEK W SIECI

PODSUMOWANIE

1. Jak nazywa się pojedyncze słowo poprzedzone symbolem # wykorzystywane np. w serwisach Instagram lub Facebook?
    a. placetag
    b. geotag
    c. hashtag

2. Zakaz pisania wulgaryzmów to jedna z zasad kulturalnego zachowania w Internecie czyli tzw. netykiety. Najwyższą karą za jej nieprzestrzeganie może być:
    a. grzywna
    b. ban
    c. mail od administratora

3. Korzystając z Internetu nie powinno się:
    a. dokonywać zakupów
    b. obsługiwać kont bankowych
    c. używać obraźliwych słów

4. Profilowanie to:

a. mechanizm, który służy kategoryzowaniu ludzi według ich cech, zachowań, preferencji
b. wyłudzanie danych osobistych i informacji majątkowych
c. tworzenie profilu na serwisie społecznościowym

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ II

OCHRONA PRZED ATAKAMI

SESJA 2

BEZPIECZNA AKTYWNOŚĆ I WIZERUNEK W SIECI

PODSUMOWANIE

1. Jak nazywa się pojedyncze słowo poprzedzone symbolem # wykorzystywane np. w serwisach Instagram lub Facebook?
   a. placetag
   b. geotag
   c. hashtag

2. Zakaz pisania wulgaryzmów to jedna z zasad kulturalnego zachowania w Internecie czyli tzw. netykiety. Najwyższą karą za jej nieprzestrzeganie może być:
   a. grzywna
   b. ban
   c. mail od administratora

3. Korzystając z Internetu nie powinno się:
   a. dokonywać zakupów
   b. obsługiwać kont bankowych
   c. używać obraźliwych słów

4. Profilowanie to:
   a. **mechanizm, który służy kategoryzowaniu ludzi według ich cech, zachowań, preferencji**
   b. wyłudzanie danych osobistych i informacji majątkowych
   c. tworzenie profilu na serwisie społecznościowym

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ II

OCHRONA PRZED ATAKAMI

SESJA 2

BEZPIECZNA AKTYWNOŚĆ I WIZERUNEK W SIECI

ANKIETA WSTĘPNA

OCENA WIEDZY I UMIEJĘTNOŚCI PRAKTYCZNYCH							
W każdym z pytań prosimy o zaznaczenie znakiem „X" odpowiedzi na poszczególne pytania w skali 7-punktowej gdzie: 1 - oznacza „zdecydowanie źle", 2 - „źle", 3 - „raczej źle", 4 - „ani dobrze, ani źle", 5 - „raczej dobrze, 6 – „dobrze", 7 - „zdecydowanie dobrze".							
Pytanie	***1***	***2***	***3***	***4***	***5***	***6***	***7***
1. Jak Pani/Pan ocenia swoją wiedzę na temat wpływu aktywności w serwisach społecznościowych na kształtowanie wizerunku w internecie?	□	□	□	□	□	□	□
2. Jak Pani/Pan ocenia swoją wiedzę na temat prawa do ochrony wizerunku w internecie?	□	□	□	□	□	□	□
3. Jak Pani / Pan ocenia swoją znajomość zagrożeń i konsekwencji cyfrowego śladu w sieci?	□	□	□	□	□	□	□
4. Jak Pani / Pan ocenia swoją wiedzę na temat profilowania w sieci?	□	□	□	□	□	□	□
5. Jak Pani / Pan ocenia swoją zasad kształtowania	□	□	□	□	□	□	□

profesjonalnego wizerunku zawodowego w sieci?							

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ II

OCHRONA PRZED ATAKAMI

SESJA 2

BEZPIECZNA AKTYWNOŚĆ I WIZERUNEK W SIECI

ANKIETA KOŃCOWA

OCENA WIEDZY I UMIEJĘTNOŚCI PRAKTYCZNYCH							
W każdym z pytań prosimy o zaznaczenie znakiem „X" odpowiedzi na poszczególne pytania w skali 7-punktowej gdzie: 1 - oznacza „zdecydowanie źle", 2 - „źle", 3 - „raczej źle", 4 - „ani dobrze, ani źle", 5 - „raczej dobrze, 6 – „dobrze", 7 - „zdecydowanie dobrze".							
Pytanie	***1***	***2***	***3***	***4***	***5***	***6***	***7***
1. Jak Pani/Pan ocenia swoją wiedzę na temat wpływu aktywności w serwisach społecznościowych na kształtowanie wizerunku w internecie?	□	□	□	□	□	□	□
2. Jak Pani/Pan ocenia swoją wiedzę na temat prawa do ochrony wizerunku w internecie?	□	□	□	□	□	□	□
3. Jak Pani / Pan ocenia swoją znajomość zagrożeń i konsekwencji cyfrowego śladu w sieci?	□	□	□	□	□	□	□
4. Jak Pani / Pan ocenia swoją wiedzę na temat profilowania	□	□	□	□	□	□	□

w sieci?							
5. Jak Pani / Pan ocenia swoją zasad kształtowania profesjonalnego wizerunku zawodowego w sieci?	□	□	□	□	□	□	□

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ II OCHRONA PRZED ATAKAMI

SESJA 2 BEZPIECZNA AKTYWNOŚĆ I WIZERUNEK W SIECI

ANKIETA EWALUACYJNA

PROWADZENIE SZKOLENIA

1. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **wiedzę i przygotowanie merytoryczne** osoby prowadzącej szkolenie?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

2. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **umiejętność przekazania wiedzy** przez osobę prowadzącą szkolenie?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

3. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **kontakt i umiejętność pracy z grupą** osoby prowadzącej szkolenie?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

PROGRAM SZKOLENIA I MATERIAŁY DYDAKTYCZNE

4. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **przydatność szkolenia** w względem potrzeb uczestników?

Zdecydowanie nieprzydatne	*Raczej nieprzydatne*	*Trudno powiedzieć*	*Raczej przydatne*	*Zdecydowanie przydatne*
1	2	3	4	5

5. Proszę ocenić na pięciostopniowej skali, w jakim stopniu szkolenie pogłębiły Pani/Pana **wiedzę teoretyczną** z omawianego na szkoleniu obszaru?

Niewystarczająco	*Wystarczająco*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

6. Proszę ocenić na pięciostopniowej skali, w jakim stopniu przeprowadzone szkolenie pogłębiło Pani/Pana **umiejętności praktyczne** z omawianego na warsztatach tematu?

Niewystarczająco	*Wystarczająco*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

7. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **jasność i zrozumiałość** wykorzystanych **kart pracy**?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

8. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **przydatność ćwiczeń** w zdobyciu wiedzy i umiejętności z zakresu tematyki szkolenia ?

Zdecydowanie nieprzydatne	*Raczej nieprzydatne*	*Trudno powiedzieć*	*Raczej przydatne*	*Zdecydowanie przydatne*
1	2	3	4	5

9. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **jasność i zrozumiałość** wykorzystanej **prezentacji multimedialnej**?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

10. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **jasność i zrozumiałość materiałów dla uczestników**?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

CZĘŚĆ III

BEZPIECZNE KORZYSTANIE Z KOMPUTERA W MIEJSCU PRACY

SESJA 1

CYBERBEZPIECZEŃSTWO - ZASADY POSTĘPOWANIA

Tematyka:

I. Cyberzagrożenia
II. Silne hasła podstawą bezpieczeństwa
III. Poczta elektroniczna
IV. Urządzenia mobilne
V. Zabezpieczenia sprzętu komputerowego i danych

SESJA 2

BEZPIECZNE USŁUGI W SIECI

Tematyka:

I. Bankowość internetowa

II. Płatności mobilne
III. Zakupy w internecie
IV. Komunikacja i praca zdalna

CYBERBEZPIECZEŃSTWO W PRACY I DOMU	
CZĘŚĆ III	BEZPIECZNE KORZYSTANIE Z KOMPUTERA W MIEJSCU PRACY
SESJA 1	CYBERBEZPIECZEŃSTWO - ZASADY POSTĘPOWANIA
CZAS TRWANIA	4 GODZINY SZKOLENIOWE

CYBERBEZPIECZEŃSTWO - ZASADY POSTĘPOWANIA

TEMATYKA:

I. Cyberzagrożenia
II. Silne hasła podstawą bezpieczeństwa
III. Poczta elektroniczna
IV. Urządzenia mobilne
V. Zabezpieczenia sprzętu komputerowego i danych

REZULTATY:

- Omówienie rodzajów zagrożeń w cyberprzstrzeni
- Zdobycie umiejętności stosowania skutecznych zabezpieczeń przed atakami cyberprzestępców
- Przekazanie informacji na temat zagrożeń i zasad postępowania w zakresie poczty elektronicznej i urządzeń mobilnych
- Zdobycie wiedzy na temat sposobów zabezpieczenia sprzętu komputerowego i danych

PROGRAM SESJI:

I. **Cyberzagrożenia**
   a. Ankieta wstępna „Cyberbezpieczeństwo - zasady postępowania”
   b. Wstęp „Cyberzagrożenia” – dyskusja grupowa i omówienie osobistych oświadczeń uczestników
   c. Przypadek 1. - omówienie i dyskusja grupowa

II. **Silne hasła podstawą bezpieczeństwa**
   a. Przypadek 2. – omówienie i dyskusja grupowa
   b. Mini - wykład i prezentacja „Cyberbezpieczeństwo - zasady postępowania. Silne hasła podstawą bezpieczeństwa”
   c. Ćwiczenie „Tworzenie silnego hasła”

III. **Poczta elektroniczna**
   a. Przypadek 3. – omówienie i dyskusja grupowa
   b. Mini - wykład i prezentacja „„Cyberbezpieczeństwo - zasady postępowania. Poczta elektroniczna”

IV. **Urządzenia mobilne**
   a. Przypadek 4. – omówienie i dyskusja grupowa
   b. Mini - wykład i prezentacja „„Cyberbezpieczeństwo - zasady postępowania. Urządzenia mobilne”

V. **Zabezpieczenia sprzętu komputerowego i danych**

a. Ćwiczenie „Dbaj o swoje cyberbezpieczeństwo”
b. Mini - wykład i prezentacja „Cyberbezpieczeństwo - zasady postępowania. Zabezpieczenia sprzętu komputerowego i danych”

VI. Podsumowanie zajęć

Rozdanie materiałów informacyjnych

Podsumowanie „Cyberbezpieczeństwo - zasady postępowania”

Ankieta końcowa „Cyberbezpieczeństwo - zasady postępowania”

Ankieta ewaluacyjna

MATERIAŁY:

1. Karta pracy „Cyberbezpieczeństwo - zasady postępowania”
2. Materiały dla uczestników „Cyberbezpieczeństwo - zasady postępowania”
3. Prezentacja „Cyberbezpieczeństwo - zasady postępowania”
4. Podsumowanie „Cyberbezpieczeństwo - zasady postępowania”
5. Ankiety wstępna i końcowa „Cyberbezpieczeństwo - zasady postępowania”
6. Ankieta ewaluacyjna

CYBERBEZPIECZEŃSTWO - ZASADY POSTĘPOWANIA

Karta pracy

CYBERZAGROŻENIA

- Czym są cyberzagrożenia?
- W jakich sytuacjach stwarzamy okazję dla cyberprzestępców?
- Jakie mogą być konsekwencje takiego ataku?
- Co pomaga w zwiększeniu bezpieczeństwa w sieci?

Przypadek 1.

Jan jest studentem rehabilitacji na AWF, który pracuje dorywczo jako barista. Jest bardzo towarzyską osobą, zawiera wiele nowych znajomości w pracy. Lubi wymieniać się różnymi plikami, śmiesznymi zdjęciami, jest aktywnym użytkownikiem komunikatorów. Często robi to w pracy, kiedy nie ma klientów i ma trochę wolnego czasu. Ponieważ musi oszczędzać pieniądze, często loguje się do sieci w pracy, gdzie może korzystać z bezpłatnego WI-FI. Ostatnio zwrócił uwagę, że jego laptop wolniej działa, przypomniał sobie również, że dawno nie aktualizował programów antywirusowych. Mocno go to zaniepokoiło, tym bardziej że jest

to laptop, gdzie ma wszystkie materiały ze studiów, w tym również swoją pracę licencjacką. Utrata danych oznaczałaby dla niego zaprzepaszczenie efektów kilkumiesięcznej pracy.

Zadanie: O jakich zasadach bezpieczeństwa powinniśmy pamiętać korzystając z internetu i urządzeń mobilnych?

- ✓ ……
- ✓ ……
- ✓ ……
- ✓ ……
- ✓ ……

SILNE HASŁA PODSTAWĄ BEZPIECZEŃSTWA

- Jakie są zagrożenia związane z hasłami do kont internetowych?
- Co to znaczy „słabe hasło”?
- Jakie hasła są łatwe do odgadnięcia?
- Jakie są hasła, które spełniają zasady bezpieczeństwa? Proszę podać przykłady?

Przypadek 2.

Irena założyła sobie pocztę elektroniczną. Jako login podała swoje imię i nazwisko, a hasło to jej adres (ulica i numer domu). Takie samo hasło ma też do swojego konta bankowego. Ostatnio zaczęła podejrzewać, że ktoś loguje się na jej konto. Szczególnie martwi się o środki na koncie, ponieważ wpływa tam jej renta. Zastanawia się co powinna je zrobić, aby jej dane do logowania były bezpieczne. Jej siostrzeniec zwrócił jej też uwagę, że powinna je regularnie zmieniać i nie zapisywać, np. w swoim kalendarzu, który codziennie nosi w torebce.

Zadanie: Jak tworzyć hasła internetowe, żeby były trudne do odgadnięcia przez inne osoby

lub cyberprzestepców?

- ……
- ……
- ……
- ……

Zadanie: Czego powinniśmy unikać tworząc hasła?

- ……
- ……
- ……
- ……

Ćwiczenie „Tworzenie silnego hasła”

Przy zakładaniu konta w dowolnej witrynie może pojawić się „dylemat hasła". Jest to wybór między podaniem słabego hasła, które łatwo zapamiętać, a silnego hasła, które trudno zapamiętać.

Oto przykłady słabych haseł, bardzo łatwych do odgadnięcia:
123456 , 123456789, qwerty , password , iloveyou, 111111, 123123, abc123, qwerty123, 1q2w3e4r, admin, qwertyuiop, 654321, 555555, lovely, 7777777, welcome, 888888, password1, 123qwe

Zadanie: Utwórz przykłady bezpiecznych haseł. Powinno zawierać co najmniej jeden znak z każdej z następujących grup: małe litery, DUŻE LITERY, liczby, znaki specjalne.

- ✓ .....
- ✓ .....
- ✓ .....
- ✓ .....
- ✓ .....
- ✓ .....

Możesz skorzystać z poniższych reguł, żeby je odpowiednio zmodyfikować, choć pamiętaj, że możesz zastosować swoje zasady:

- zamień a na @
- zamień s na $
- zamień spację na %
- zamień małe „o” na 0
- zamień i na !

POCZTA ELEKTRONICZNA

Poczta elektroniczna to obecnie najpopularniejsze narzędzie cyberprzestępców i najprostszy sposób dystrybucji złośliwego oprogramowania: w linkach i załącznikach.

Jedna z metod, tzw. **phishing**, za pomocą linku odsyła do fałszywej strony banku, firmy czy urzędu, która po zalogowaniu przez użytkownika przejmuje jego dane uwierzytelniające lub infekuje samo urządzenie.

Przypadek 3.

Maria jest podekscytowana. Właśnie dostała e-maila z radosną informacją: jeżeli poda swoje

imię i nazwisko, adres i numer telefonu, firma „Spełniamy marzenia" prześle jej bilety na koncert ulubionego zespołu. Powinna tylko otworzyć przesłany link i zalogować się na stronie internetowej firmy promocyjnej. Jednak jej koleżanka z biura, której opowiedziała o mailu, zauważyła, że może być to próba wyłudzenia danych, że nie powinna ryzykować.

Zadanie: Na co powinniśmy uważać w korespondencji mailowej ?

- ✓ ……
- ✓ ……
- ✓ ……
- ✓ ……

Zadanie: Jakich zasad powinniśmy przestrzegać ?

- ✓ ……
- ✓ ……
- ✓ ……
- ✓ ……

URZĄDZENIA MOBILNE

Urządzenie mobilne – przenośne urządzenie elektroniczne pozwalające na przetwarzanie, odbieranie oraz wysyłanie danych bez konieczności utrzymywania przewodowego połączenia z siecią. Przykłady urządzeń mobilnych to smartfon, tablet, GPS, smartwatch.

Aplikacja mobilna - ogólna nazwa dla oprogramowania działającego na urządzeniach przenośnych.

Przypadek 4.

Tomek uwielbia ściągać aplikacje na swojego smartfona. Kiedy ściąga kolejną fantastyczną

grę, na ekranie pojawia się napis: „Czy chcesz, żeby twoi znajomi też poznali tę grę? Jeżeli tak, udostępnij kontakty do nich". Zazwyczaj nawet tego nie czyta, od razu się zgadza. Ma w telefonie wiele aplikacji, które wykorzystuje w różnych sytuacjach, do kontaktów, robienia zakupów, sprawdzania informacji o pogodzie, zamawiania jedzenia, dojazdów, planowania treningów. Korzysta też z aplikacji bankowych, dzięki czemu ma szybki dostęp do swoich pieniędzy. Żartuje, że jego telefon to kalendarz, książka telefoniczna, trener, bankomat, osobisty asystent w jednym. I jak żona, wie o nim wszystko.

Zadanie: Jakie informacje udostępniamy informacje w urządzeniach mobilnych? W jaki sposób są one gromadzone i przez kogo?

→ ……

→ ……

→ ……

→ ……

→ ……

Podsumowanie: W jaki sposób powinniśmy chronić swoją prywatność w urządzeniach mobilnych?

ZABEZPIECZENIA SPRZĘTU KOMPUTEROWEGO I DANYCH

Ćwiczenie „Dbaj o swoje cyberbezpieczeństwo"

Zadanie: W parach lub w kilkuosobowych zespołach przygotujcie zasady, które warto przestrzegać aby należycie zabezpieczyć swój sprzęt komputerowy i dane.

1. ……

   ……

2. ……

……

3. ……

……

4. ……

……

5. ……

……

6. ……

……

7. ……

……

8. ……

……

SŁOWNIK POJĘĆ

Adres IP

IP to protokół komunikacyjny używany powszechnie w Internecie i sieciach lokalnych. Adres IP to liczba, która jest nadawana każdemu urządzeniu lub grupie urządzeń połączonych w sieci. Służy on ich identyfikacji.

Aplikacja internetowa

Program komputerowy, który pracuje na serwerze i komunikuje się poprzez sieć komputerową z hostem użytkownika komputera z wykorzystaniem przeglądarki internetowej

użytkownika, będącego w takim przypadku interaktywnym klientem aplikacji internetowej.

Aplikacja mobilna

Ogólna nazwa dla oprogramowania działającego na urządzeniach przenośnych, takich jak telefony komórkowe, smartfony, palmtopy czy tablety.

Cyberbezpieczeństwo

Ogół technik, procesów i praktyk stosowanych w celu ochrony sieci informatycznych, urządzeń, programów i danych przed atakami, uszkodzeniami lub nieautoryzowanym dostępem. Cyberbezpieczeństwo bywa także określane jako „bezpieczeństwo technologii informatycznych".

Phishing

Metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji, zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań. Jest to rodzaj ataku opartego na inżynierii społecznej.

Program antywirusowy

Program komputerowy, którego zadaniem jest wykrywanie, zwalczanie i usuwanie wirusów komputerowych.

Protokół HTTPS

(Ang. *Hypertext Transfer Protocol Secure*) – rozszerzenie protokołu HTTP. Umożliwia przesyłanie w sieci zaszyfrowanych informacji, dzięki czemu dostęp do treści mają jedynie nadawca oraz odbiorca komunikatu.

Przeglądarka internetowa

Program komputerowy służący do pobierania i wyświetlania stron internetowych udostępnianych przez serwery WWW, a także odtwarzania plików multimedialnych, często przy użyciu dodatków, zwanych wtyczkami.

Wirus komputerowy

Wirusa komputerowego zalicza się do szkodliwego oprogramowania (malware). Do zwalczania wirusów komputerowych stosuje się programy antywirusowe i skanery wykrywające szkodliwe oprogramowanie (anti-malware scanners). W zabezpieczeniu się przed wirusami pomagają również aktualizacje systemu i aplikacji.

Wirtualna sieć prywatna (od ang. virtual private network – VPN)

Tunel, przez który płynie ruch w ramach sieci prywatnej pomiędzy nadawcą i odbiorcą za pośrednictwem publicznej sieci (takiej jak Internet). Można opcjonalnie kompresować lub szyfrować przesyłane dane w celu zapewnienia lepszej jakości lub większego poziomu bezpieczeństwa

Złośliwe oprogramowanie

Szkodliwe oprogramowanie (ang. malware – zbitka słów malicious „złowrogi, złośliwy” i software „oprogramowanie”), ogół programów mających szkodliwe działanie w stosunku do systemu komputerowego lub jego użytkownika

CYBERBEZPIECZEŃSTWO - ZASADY POSTĘPOWANIA

Materiały dla uczestników

CYBERZAGROŻENIA

Wiele osób staje się ofiarami cyberprzestępców niemal na własne życzenie – nawiązując bliskie relacje z osobami poznanymi w sieci, przesyłając im pieniądze, kompromitujące fotografie, czy udostępniając dane osobowe, bądź inne ważne informacje.

Cyberbezpieczeństwo wymaga, prócz pewnej aktywności od samego użytkownika, także zachowania umiaru i zdrowego rozsądku podczas korzystania z sieci. Istnieje kilka sposobów, w jaki cyberprzestępcy mogą próbować zaatakować konta użytkowników.

Wiele z ataków opiera się na atakach celowanych w używane hasła, więc spójrzmy na kilka z nich:

- Zbyt łatwe hasła. Powinieneś postarać się, aby twoje hasło nie było łatwe do odgadnięcia. Wszyscy wiemy, że hasła chronią rzeczy, które są dla nas cenne, ale to nie powstrzymuje ludzi przed używaniem najpopularniejszych haseł, w tym „hasło", „123456", „qwerty", „piłka nożna" i tak dalej.
- Jedno hasło do wielu witryn. W mediach często pojawiają się historie o tym, że cyberprzestępcy łamią dużą liczbę haseł z witryn, które nie zapewniły im odpowiedniej ochrony. Jeśli ponownie używasz tego samego hasła w wielu witrynach (tzw. recycling hasła), a cyberprzestępcy włamują się do jednej witryny, mogą wypróbować odzyskane hasła w innych witrynach, z których korzystasz.
- Keylogging. Istnieje pewien rodzaj złośliwego oprogramowania, który raz zainstalowany w systemie próbuje rejestrować naciśnięcia klawiszy - w tym hasła. Oczywiście wpłynie to na każde wprowadzone hasło, bez względu na to, jak jest skomplikowane. Najlepszą metodą obrony tutaj jest utrzymywanie aktualnego oprogramowania.

SILNE HASŁA PODSTAWĄ BEZPIECZEŃSTWA

Rejestrując się w różnego rodzaju systemach internetowych i aplikacjach zainstalowanych na użytkowanych urządzeniach niezbędne jest wykorzystywanie hasła autoryzującego późniejszy dostęp. W związku z tym wiele osób stosuje jedno hasło do wszystkich systemów, często stanowiące prostą kombinację cyfr składających się na datę urodzenia.

Zasady używania haseł

→ W celu podniesienia poziomu bezpieczeństwa należy stosować silne hasła składające się z kombinacji co najmniej 8 znaków, w tym dużej litery, cyfry oraz znaku specjalnego.

→ To samo hasło nie powinno być używane na różnych kontach – zwłaszcza zawierających poufne informacje. Dzięki temu nawet, jeśli naruszone zostanie jedno z nich, cyberprzestępca nie będzie mógł wziąć na cel pozostałych.

→ Aby ułatwić sobie zapamiętywanie haseł, można stosować specjalne programy do zarządzania nimi. Nowe technologie umożliwiają już także uwierzytelnianie biometryczne – przez skanowanie odcisków palców czy rozpoznawanie twarzy.

→ Hasło należy zmieniać w miarę regularnie – co najmniej raz na kwartał i nie powinno być wykorzystywane do logowania w wielu miejscach.

→ Nie zapisuj haseł. Tworzenie bardzo silnego hasła i zapisywanie go na papierze jest równie złą decyzją, co tworzenie łatwego do zapamiętania hasła bez zapisywania go.

→ Zmieniaj hasło natychmiast, gdy zostanie naruszone. Jeśli masz choć cień podejrzenia, że ktoś mógł ukraść Twoje hasło, zmień je natychmiast.

→ Nie wpisuj hasła na komputerze, który nie należy do Ciebie. Hakerzy często używają programów rejestrujących naciśnięcia klawiszy (keylogger), co pozwala im zarejestrować każdy tekst wpisany w systemie, w tym hasła.

Tworzenie i zapamiętywanie silnych haseł

- Długość hasła. Wybierz hasło o długości co najmniej 8 znaków. Jeszcze lepsze jest dłuższe hasło, składające się z 12 lub 14 znaków. Pamiętaj, że niektóre witryny, systemy operacyjne lub aplikacje posiadają wymagania co do minimalnej długości hasła.
- Złożoność hasła. Hasło powinno zawierać co najmniej jeden znak z każdej z następujących grup: małe litery, DUŻE LITERY, liczby, znaki specjalne
- Użycie frazy. Wybierz łatwy do zapamiętania cytat, piosenkę lub frazę i użyj pierwszej litery z każdego słowa. Używaj liter różnej wielkości. Pamiętaj, aby uwzględnić również liczby i symbole, zastępując nimi litery lub całe słowa.
    - zamień a na @
    - zamień s na $
    - zamień spację na %
    - zamień małe „o” na 0
    - zamień i na !

Podczas tworzenia hasła zastosuj poniższe reguły:

→ Hasło nie powinno być takie samo jak nazwa użytkownika lub jego część. Hasło nie powinno być imieniem członka rodziny, znajomego ani zwierzaka.

→ Nie powinno zawierać danych osobowych Twoich lub rodziny. Mowa tu o informacjach, które łatwo zdobyć, takie jak data urodzenia, numer telefonu, numer rejestracyjny samochodu, nazwa ulicy, numer mieszkania/domu itd.

→ Nie używaj sekwencji kolejnych liter, liczb lub innych znaków. Na przykład: abcde, 12345, QWERTY

→ Nie używaj słowa ze słowników dowolnego języka oraz słów ze słownika z liczbą lub znakiem na początku lub końcu. Nie stosuj pojedynczego słowa, pisanego normalnie lub wspak, z polskiego lub obcojęzycznego słownika

POCZTA ELEKTRONICZNA

Poczta elektroniczna to obecnie najpopularniejsze narzędzie cyberprzestępców i najprostszy sposób dystrybucji złośliwego oprogramowania: w linkach i załącznikach. Jedna z metod, tzw. phishing, za pomocą linku odsyła do fałszywej strony banku, firmy czy urzędu, która po zalogowaniu przez użytkownika przejmuje jego dane uwierzytelniające lub infekuje samo urządzenie.

Nazwa phishing budzi dźwiękowe skojarzenia z fishingiem – czyli łowieniem ryb. Przestępcy, podobnie jak wędkarze, stosują bowiem odpowiednio przygotowaną „przynętę". Do tego wykorzystują najczęściej sfałszowane e-maile i SMS-y. Coraz częściej oszuści działają także za pośrednictwem komunikatorów i portali społecznościowych (np. poprzez „metodę na BLIKa").

Phishing wykorzystuje inżynierię społeczną, czyli technikę polegającą na tym, że przestępcy internetowi próbują oszukać odbiorcę wiadomości i spowodować, aby podjął działanie zgodnie z ich zamierzeniami. Cyberprzestępcy starają się wyłudzić dane do logowania, na przykład do kont bankowych lub kont społecznościowych, czy systemów biznesowych. Oszukańcze wiadomości mogą też zawierać link do strony internetowej rozprzestrzeniającej szkodliwe oprogramowanie lub mieć zainfekowany załącznik.

Jak radzić sobie z fałszywymi wiadomościami?

Wiadomości phishingowe są tak przygotowywane przez cyberprzestępców, aby wyglądały na autentyczne, ale w rzeczywistości są fałszywe. Mogą próbować skłonić do ujawnienia poufnych informacji, zawierać link do strony internetowej rozprzestrzeniającej szkodliwe oprogramowanie (często przestępcy używają podobnych do autentycznych nazw witryn) lub mieć zainfekowany załącznik. Dopóki nie ma pewności, że nadawca jest prawdziwy, nie

powinno się klikać w żadne linki ani na nie odpowiadać.

Jak rozpoznać e-mail wyłudzający informacje?

- Wiele wiadomości phishingowych ma niepoprawną gramatykę, interpunkcję, pisownię, czy też brak jest polskich znaków diakrytycznych, np. nie używa się „ą”, „ę” itd.
- Oceń, czy wygląd i ogólna jakość e-maila może pochodzić z organizacji lub firmy, od której powinna pochodzić taka wiadomość – użyte logotypy, stopki z danymi nadawcy itd.
- Sprawdź, czy e-mail jest adresowany do Ciebie z imienia i nazwiska, czy odnosi się do „cenionego klienta”, „przyjaciela” lub „współpracownika”? Może to oznaczać, że nadawca tak naprawdę cię nie zna i że jest to część oszustwa typu phishing.
- Sprawdź, czy e-mail zawiera ukryte zagrożenie, które wymaga natychmiastowego działania? Bądź podejrzliwy w stosunku do słów typu "wyślij te dane w ciągu 24 godzin" lub "padłeś ofiarą przestępstwa, kliknij tutaj natychmiast".
- Jeśli wiadomość brzmi zbyt dobrze, aby mogła być prawdziwa, prawdopodobnie nie jest ona prawdziwa. Jest mało prawdopodobne, aby ktoś chciał Ci dać pieniądze lub dostęp do tajnej części Internetu.
- Twój bank lub jakakolwiek inna instytucja nigdy nie powinna prosić Cię o podanie w wiadomości e-mail danych osobowych. Urzędy administracji publicznej nigdy nie proszą Cię przy pomocy SMS, czy maili o dopłatę do szczepionki, czy uregulowanie należności podatkowych.
- Zwracaj uwagę na linki przekazywane również między znajomymi, sprawdź, czy link faktycznie prowadzi do właściwej strony.
- Coraz częściej przestępcy, uzyskując w nielegalny sposób kontrolę nad naszymi kontami społecznościowymi, podszywają się pod naszych znajomych i rodzinę.

- Uważaj na skrócone linki, jeśli nie masz pewności, dokąd poprowadzi Cię link, najedź wskaźnikiem myszy na link (nie klikaj), a na dole przeglądarki zostanie wyświetlony pełen adres linku.

URZĄDZENIA MOBILNE

Urządzenia mobilne mogą także stanowić bogate źródło informacji zarówno o nas, jak i naszych bliskich: zawierają listy kontaktów, zdjęcia, filmy, historię lokalizacji, dane medyczne i finansowe. Niezależnie od tego, czy planujemy zabrać je ze sobą w podróż służbową czy na wakacyjny wyjazd, dobrze jest zadbać o bezpieczeństwo danych.

- Chroń urządzenia przed niepowołanym dostępem: Wymyśl i ustaw trudne do odgadnięcia hasło lub skorzystaj z możliwości jakie daje czytnik odcisku palca. Pomoże to dodatkowo chronić Twoje dane w przypadku kradzieży lub utraty urządzenia.
- Świadomie wybieraj aplikacje: Nie instaluj aplikacji spoza oficjalnego sklepu, ani takich, które wyglądają podejrzanie. Zwracaj uwagę na komunikaty, w których jesteś proszony o przyznanie uprawnień.
- Widoczny/niewidoczny: Niektóre sklepy, centra usługowe i inne odwiedzane miejsca mogą wykorzystywać Wi-Fi i Bluetooth do rejestrowania Twojego położenia, gdy znajdziesz się w ich zasięgu. Wyłączaj wspomniane funkcjonalności, kiedy z nich nie korzystasz.
- Uważaj na hotspoty Wi-Fi: Publiczne sieci bezprzewodowe bywają niebezpieczne. Kiedy jesteś do nich podłączony, przesyłane treści mogą być widoczne dla innych. Nie używaj ich w celu logowania się do ważnych serwisów, takich jak bankowość internetowa, konto pocztowe, czy serwisy społecznościowe.
- Urządzenia zawsze aktualne. Aktualizowanie na bieżąco systemu, przeglądarki

internetowej, pakietu antywirusowego i innych wykorzystywanych aplikacji pomoże ochronić Cię przed atakami i szkodliwym oprogramowaniem.

- Zachowaj porządek: Niektóre aplikacje wykorzystujemy jedynie tymczasowo, odinstaluj te, z których już nie korzystasz. Poprawi to bezpieczeństwo Twojego urządzenia.

ZABEZPIECZENIA SPRZĘTU KOMPUTEROWEGO I DANYCH

Ofiary cyberprzestępczości to najczęściej ofiary oszustw. Oszuści korzystają ze złośliwego oprogramowania, metod wyłudzania danych i socjotechniki, aby uzyskać dostęp do prywatnych danych, zazwyczaj w celu kradzieży pieniędzy. Wiele w zakresie bezpieczeństwa w sieci, zależy od samych użytkowników.

Oto najważniejsze porady:

- Zainstaluj niezawodne oprogramowanie zabezpieczające na każdym urządzeniu, które zapobiega zainfekowaniu urządzenia przez złośliwe oprogramowanie, a także zapewnia funkcję kontroli sieci Wi-Fi, która skanuje Twój domowy router w poszukiwaniu luk w zabezpieczeniach.
- Używaj silnych i unikatowych haseł. Do generowania bardzo bezpiecznych haseł używaj menedżera haseł.
- Pobieraj aplikacje tylko z zaufanych źródeł. Używaj antywirusa także na smartfonie.
- Jeśli chcesz korzystać z bezpłatnych, otwartych sieci Wi-Fi, zastanów się nad korzystaniem z wirtualnej sieci prywatnej (VPN). Sieć VPN tworzy bezpieczne, zaszyfrowane połączenie i chroni Twoje dane osobowe oraz Twoją prywatność. Gdy korzystasz z sieci VPN, przeglądasz Internet anonimowo, a Twoja lokalizacja jest zmieniania, dzięki czemu nie można Cię śledzić.
- Zastanów się dobrze, zanim otworzysz załącznik, klikniesz link lub udostępnisz poufne

informacje. Dokładnie analizuj każdą wiadomość e-mail zawierającą prośbę o podanie danych osobowych.

- Aby uniknąć ataków ransomware, zapoznaj się z ofertą oprogramowania zabezpieczającego z funkcją osłony przed ransomware, które możesz zainstalować na wszystkich swoich urządzeniach.

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ III

BEZPIECZNE KORZYSTANIE Z KOMPUTERA W MIEJSCU PRACY

SESJA 1

CYBERBEZPIECZEŃSTWO - ZASADY POSTĘPOWANIA

PODSUMOWANIE

1. Wybierz najbezpieczniejsze hasło
    a. k0ch4mMame
    b. KapustaWierszBagno!Filtr125
    c. Juleczka21

2. Jak rozpoznać zaufaną stronę internetową?
    a. posiada kłódkę czyli certyfikat bezpieczeństwa
    b. rozpoczyna się od https:// - czyli jest szyfrowana
    c. obie powyższe odpowiedzi są prawidłowe

3. Ikona zamkniętej kłódki w pasku adresu przeglądarki informuje użytkownika, że:
    a. witryna została zamknięta ze względów bezpieczeństwa
    b. kliknięcie jakiekolwiek linku na stronie spowoduje zainstalowanie konia trojańskiego lub robaka na naszym komputerze
    c. strona jest zabezpieczona certyfikatem bezpieczeństwa i połączenie jest

szyfrowane

4. Wskaż poprawny(e) adres(y)IP:
    a. 67.195.37.180
    b. IP_NET
    c. 83.25.148.44.100

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ III

BEZPIECZNE KORZYSTANIE Z KOMPUTERA W MIEJSCU PRACY

SESJA 1

CYBERBEZPIECZEŃSTWO - ZASADY POSTĘPOWANIA

PODSUMOWANIE

1. Wybierz najbezpieczniejsze hasło
    a. k0ch4mMame
    b. KapustaWierszBagno!Filtr125
    c. Juleczka21

2. Jak rozpoznać zaufaną stronę internetową?
    a. posiada kłódkę czyli certyfikat bezpieczeństwa
    b. rozpoczyna się od https:// - czyli jest szyfrowana
    c. obie powyższe odpowiedzi są prawidłowe

3. Ikona zamkniętej kłódki w pasku adresu przeglądarki informuje użytkownika, że:
    a. witryna została zamknięta ze względów bezpieczeństwa
    b. kliknięcie jakiekolwiek linku na stronie spowoduje zainstalowanie konia trojańskiego lub robaka na naszym komputerze

c. strona jest zabezpieczona certyfikatem bezpieczeństwa i połączenie jest szyfrowane

4. Wskaż poprawny(e) adres(y)IP:
   a. 67.195.37.180
   b. IP_NET
   c. 83.25.148.44.100

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ III

BEZPIECZNE KORZYSTANIE Z KOMPUTERA W MIEJSCU PRACY

SESJA 1

CYBERBEZPIECZEŃSTWO - ZASADY POSTĘPOWANIA

ANKIETA WSTĘPNA

OCENA WIEDZY I UMIEJĘTNOŚCI PRAKTYCZNYCH							
W każdym z pytań prosimy o zaznaczenie znakiem „X" odpowiedzi na poszczególne pytania w skali 7-punktowej gdzie: 1 - oznacza „zdecydowanie źle", 2 - „źle", 3 - „raczej źle", 4 - „ani dobrze, ani źle", 5 - „raczej dobrze, 6 – „dobrze", 7 - „zdecydowanie dobrze".							
Pytanie	***1***	***2***	***3***	***4***	***5***	***6***	***7***
1. Jak Pani/Pan ocenia swoją wiedzę na rodzajów zagrożeń w cyberprzestrzeni?	☐	☐	☐	☐	☐	☐	☐
2. Jak Pani/Pan ocenia swoją umiejętności stosowania skutecznych zabezpieczeń przed atakami cyberprzestępców?	☐	☐	☐	☐	☐	☐	☐
3. Jak Pani / Pan ocenia swoją wiedzę temat zagrożeń i zasad postępowania w zakresie poczty elektronicznej?	☐	☐	☐	☐	☐	☐	☐

4. Jak Pani / Pan ocenia swoją wiedzę temat zagrożeń i zasad postępowania w zakresie urządzeń mobilnych?	□	□	□	□	□	□	□
5. Jak Pani / Pan ocenia swoją wiedzę na temat sposobów zabezpieczenia sprzętu komputerowego i danych?	□	□	□	□	□	□	□

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ III

BEZPIECZNE KORZYSTANIE Z KOMPUTERA W MIEJSCU PRACY

SESJA 1

CYBERBEZPIECZEŃSTWO - ZASADY POSTĘPOWANIA

ANKIETA KOŃCOWA

OCENA WIEDZY I UMIEJĘTNOŚCI PRAKTYCZNYCH							
W każdym z pytań prosimy o zaznaczenie znakiem „X” odpowiedzi na poszczególne pytania w skali 7-punktowej gdzie: 1 - oznacza „zdecydowanie źle”, 2 - „źle”, 3 - „raczej źle”, 4 - „ani dobrze, ani źle”, 5 - „raczej dobrze, 6 – „dobrze”, 7 - „zdecydowanie dobrze”.							
Pytanie	***1***	***2***	***3***	***4***	***5***	***6***	***7***
1. Jak Pani/Pan ocenia swoją wiedzę na rodzajów zagrożeń w cyberprzestrzeni?	□	□	□	□	□	□	□
2. Jak Pani/Pan ocenia swoją umiejętności stosowania skutecznych zabezpieczeń przed atakami cyberprzestępców?	□	□	□	□	□	□	□

3. Jak Pani / Pan ocenia swoją wiedzę temat zagrożeń i zasad postępowania w zakresie poczty elektronicznej?	□	□	□	□	□	□	□
4. Jak Pani / Pan ocenia swoją wiedzę temat zagrożeń i zasad postępowania w zakresie urządzeń mobilnych?	□	□	□	□	□	□	□
5. Jak Pani / Pan ocenia swoją wiedzę na temat sposobów zabezpieczenia sprzętu komputerowego i danych?	□	□	□	□	□	□	□

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ III BEZPIECZNE KORZYSTANIE Z KOMPUTERA W MIEJSCU PRACY

SESJA 1 CYBERBEZPIECZEŃSTWO - ZASADY POSTĘPOWANIA

ANKIETA EWALUACYJNA

PROWADZENIE SZKOLENIA

1. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **wiedzę i przygotowanie merytoryczne** osoby prowadzącej szkolenie?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

2. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **umiejętność przekazania wiedzy** przez osobę prowadzącą szkolenie?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

3. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **kontakt i umiejętność pracy z grupą** osoby prowadzącej szkolenie?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

PROGRAM SZKOLENIA I MATERIAŁY DYDAKTYCZNE

4. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **przydatność szkolenia** w względem potrzeb uczestników?

Zdecydowanie nieprzydatne	*Raczej nieprzydatne*	*Trudno powiedzieć*	*Raczej przydatne*	*Zdecydowanie przydatne*
1	2	3	4	5

5. Proszę ocenić na pięciostopniowej skali, w jakim stopniu szkolenie pogłębiły Pani/Pana **wiedzę teoretyczną** z omawianego na szkoleniu obszaru?

Niewystarczająco	*Wystarczająco*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

6. Proszę ocenić na pięciostopniowej skali, w jakim stopniu przeprowadzone szkolenie pogłębiło Pani/Pana **umiejętności praktyczne** z omawianego na warsztatach tematu?

Niewystarczająco	*Wystarczająco*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

7. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **jasność i zrozumiałość** wykorzystanych **kart pracy**?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

8. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **przydatność ćwiczeń** w zdobyciu wiedzy i umiejętności z zakresu tematyki szkolenia ?

Zdecydowanie nieprzydatne	*Raczej nieprzydatne*	*Trudno powiedzieć*	*Raczej przydatne*	*Zdecydowanie przydatne*

1	2	3	4	5

9. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **jasność i zrozumiałość** wykorzystanej **prezentacji multimedialnej**?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

10. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **jasność i zrozumiałość materiałów dla uczestników**?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ III	BEZPIECZNE KORZYSTANIE Z KOMPUTERA W MIEJSCU PRACY

SESJA 2	BEZPIECZNE USŁUGI W SIECI

CZAS TRWANIA	4 GODZINY SZKOLENIOWE

BEZPIECZNE USŁUGI W SIECI

TEMATYKA:

I. Bankowość internetowa
II. Płatności mobilne
III. Zakupy w internecie
IV. Komunikacja i praca zdalna

REZULTATY:

- Omówienie zalet i rodzajów zagrożeń związanych z usługami oferowanymi w internecie i poprzez urządzenia mobilne
- Przekazanie informacji na temat zasad bezpieczeństwa w zakresie bankowości internetowej, płatności mobilnych i zakupów w sklepach internetowych
- Omówienie zasad bezpieczeństwa w zakresie komunikacji i pracy zdalnej
- Zdobycie umiejętności stosowania skutecznych zabezpieczeń przed atakami cyberprzestępców

PROGRAM SESJI:

I. **Bankowość elektroniczna**
   a. Ankieta wstępna „Bezpieczne usługi w sieci”
   b. Wstęp „Bezpieczne usługi w sieci” – dyskusja grupowa i omówienie osobistych oświadczeń uczestników
   c. Przypadek 1. - omówienie i dyskusja grupowa
   d. Ćwiczenie „Bezpieczne konto”
   e. Mini - wykład i prezentacja „Bezpieczne usługi w sieci – Bankowość internetowa”

II. **Płatności mobilne**
   a. Przypadek 2. – omówienie i dyskusja grupowa
   b. Mini - wykład i prezentacja „Bezpieczne usługi w sieci – Płatności mobilne”

III. **Zakupy w internecie**
   a. Ćwiczenie „Bezpieczne zakupy przez internet”
   b. Mini - wykład i prezentacja „Bezpieczne usługi w sieci - Zakupy w internecie”

IV. **Komunikacja i praca zdalna**
   a. Przypadek 3. – omówienie i dyskusja grupowa
   b. Mini - wykład i prezentacja „Bezpieczne usługi w sieci – Komunikacja i praca zdalna”

V. **Podsumowanie zajęć**

Rozdanie materiałów informacyjnych

Podsumowanie „Bezpieczne usługi w sieci”

Ankieta końcowa „Bezpieczne usługi w sieci”

Ankieta ewaluacyjna

MATERIAŁY:

1. Karta pracy „Bezpieczne usługi w sieci”
2. Materiały dla uczestników „Bezpieczne usługi w sieci”
3. Prezentacja „Bezpieczne usługi w sieci”
4. Podsumowanie „Bezpieczne usługi w sieci”
5. Ankiety wstępna i końcowa „Bezpieczne usługi w sieci”
6. Ankieta ewaluacyjna

BEZPIECZNE USŁUGI W SIECI

Karta pracy

BANKOWOŚĆ INTERNETOWA

- Z jakich usług finansowych możemy korzystać w internecie i w urządzeniach mobilnych typu smartfon?
- Jakie są zalety związane z usługami finansowymi dostępnymi w internecie i w urządzeniach mobilnych?

Przypadek 1.

Marta jechała samochodem po dzieci do przedszkola, kiedy usłyszała dzwonek swojego telefonu. Usłyszała miły głos osoby, która przedstawiła się jako pracownik jej banku. Poinformował ją, że w związku z pracami nad wdrożeniem nowego systemu zabezpieczeń aktualizują dane właścicieli kont. W celu potwierdzenia tożsamości, poprosił o podanie loginu do bankowości internetowej. Po chwili poinformował ją, że konieczna jest zmiana hasła, i że

względu na zwiększony poziom zabezpieczeń musi to zrobić administrator sytemu banku. Konieczne jest podanie starego hasła, aby możliwa konfiguracja systemu. Marta była trochę zaniepokojona ta rozmową, ale pracownik banku wydawał się bardzo profesjonalny. Zapewniał ją, że celem tych działań jest przeniesienie jej konta na nowoczesne, bardzo bezpieczne serwery. Na koniec poinformował ją, że został do niej wysłany kontrolny SMS i w celu ostatecznej weryfikacji, prosi o podanie zawartego w nim ośmiocyfrowego kodu. Ucieszona, że już koniec podała go. Pracownik podziękował i poinformowała, że cała operacja przebiegła poprawnie. Podziękował za współpracę i życzył miłego wieczoru. Marta była zadowolona, że jej bank jest tak nowoczesny i dba o wzmacnianie poziomu bezpieczeństwa jego pieniędzy. Po powrocie do domu postanowiła jeszcze sprawdzić, czy w związku z „przełączeniem jej konta na nowy serwer" uległ zmianie wygląd serwisu jej bankowości internetowej. Po zalogowaniu okazało się jednak, że jedyne, co uległo zmianie, to stan jej konta – zostało ono bowiem uszczuplone o 3 000 złotych.

Ćwiczenie „Bezpieczne konto"

Konto internetowe, chociaż prowadzone w świecie wirtualnym, jest realnie narażone na rabunek. Nowe technologie to nowe szanse, ale i także nowe zagrożenia. Hakerzy stosują przeróżne sztuczki, aby wyłudzić od nas informacje o naszych kontach. Szczególnie dotyczy to danych logowania i hasła.

Zadanie: Jakie zagrożenia są związane z usługami finansowymi świadczonymi w internecie?

- ✓ ……
- ✓ ……
- ✓ ……
- ✓ ……

Zadanie: Jakie o jakich zasadach bezpieczeństwa finansowego powinniśmy pamiętać?

- ✓ ……
- ✓ ……
- ✓ ……
- ✓ ……

Zapamiętaj!

Żaden bank nigdy, pod żadnym pozorem nie prosi o podawanie żadnych danych logowania do bankowości internetowej (loginów, haseł, kodów jednorazowych z kart-zdrapek ani przesyłanych SMSem itp.), czy to telefonicznie, czy poprzez pocztę elektroniczną, czy w jakikolwiek inny sposób – poza serwisem internetowym bankowości elektronicznej i udostępnianymi przez banki aplikacjami (np. instalowanymi na telefonach komórkowych).

PŁATNOŚCI MOBILNE

- Z jakich usług finansowych możemy korzystać w urządzeniach mobilnych typu smartfon?
- Jakie są zalety związane z usługami finansowymi w urządzeniach mobilnych?
- Na co warto zwracać uwagę korzystając z nich?

Przypadek 2.

Danka nigdy nie miała pamięci do liczb. Dlatego kiedy córka namówiła ją do instalacji aplikacji pozwalającej na dokonywanie płatności mobilnych na telefonie, zapisała kod PIN do tej aplikacji na kartce i umieściła ją w etui aparatu. Rzadko z niej korzystała, przyzwyczajona do kart bankomatowych i gotówki, która zawsze lubiła „mieć pod ręką”. Pewnego dnia padła ofiarą złodzieja, który wykorzystując chwilę nieuwagi ukradł jej telefon kiedy robiła zakupy w

markecie. Początkowo nie była tą sytuacją zbyt zmartwiona, był to stary aparat, która chciała wymienić na nowy model, tym bardziej że kończyła się jej umowa abonamentowa. Jakież jednak było jej zdziwienie, kiedy następnego dnia po zalogowaniu do swojego konta zobaczyła, że w ciągu ostatniej doby jej konto zostało uszczuplone o ponad 1200 złotych. Dopiero wtedy przypomniała sobie o zainstalowanej na telefonie aplikacji do płatności mobilnych (i o zapisanym w telefonie kodzie PIN).

Zadanie: Jakie są zasady bezpiecznego korzystania z płatności mobilnych?

- ✓ ……
- ✓ ……
- ✓ ……
- ✓ ……

Podsumowanie: Na jakie zagrożenia powinniśmy zwracać uwagę korzystając z płatności mobilnych?

ZAKUPY PRZEZ INTERNET

Sklep internetowy – serwis internetowy dający możliwość kupowania i sprzedawania produktów przez Internet, jedna z form handlu elektronicznego. Częścią sklepów internetowych jest strona www na której klienci zapoznają się z ofertą i składają zamówienia.

Ćwiczenie „ Bezpieczne zakupy przez internet”

Korzyści z zakupów internetowych

→ ……

→ ……

→ ……

→ ……

Ograniczenia i zagrożenia związane są z zakupami w internecie

→ ……

→ ……

→ ……

→ ……

Na co powinniśmy zwracać uwagę korzystając ze sklepów internetowych i platform sprzedażowych?

→ ……

→ ……

→ ……

→ ……

KOMUNIKACJA I PRACA ZDALNA

- Jakie są zagrożenia związane z komunikacją internetową?
- O jakich środkach bezpieczeństwa powinniśmy pamiętać pracując zdalnie?
- W jaki sposób możemy zabezpieczyć sprzęt oraz zapisane dane?

Przypadek 3.

Jacek jest księgowym, prowadzi biuro rachunkowe, gdzie wraz ze swoim zespołem obsługuje kilkunastu stałych klientów. Są to przedsiębiorstwa działające głównie w branży usługowej,

zatrudniające od kilkunastu do kilkudziesięciu osób. Prowadzi dla nich rozliczenia księgowe, kadrowe i płacowe. Podstawowym narzędziem pracy jest dla niego laptop, za pomocą którego komunikuje się ze swoimi klientami oraz gdzie ma zainstalowane programy finansowo – księgowe. Ostatnio dowiedział się, że jeden z jego klientów miał poważne problemy z systemem informatycznym, prawdopodobnie doszło do wprowadzenia wirusów i złośliwego oprogramowania. Postanowił opracować ścisłe procedury dotyczące korzystania ze sprzętu i oprogramowania, co jest szczególnie pilne w związku z pracą części personelu w trybie zdalnym.

Zadanie: Jakie powinny być zasady dotyczące bezpiecznej komunikacji zdalnej i korzystania ze sprzętu informatycznego i oprogramowania w miejscu pracy?

! ……

! ……

! ……

! ……

! ……

! ……

SŁOWNIK POJĘĆ

Certyfikat klucza publicznego

Zestaw informacji, które w ogólnym przypadku nie są możliwe do podrobienia i które służą do weryfikacji tożsamości podmiotu w internecie.

Handel elektroniczny (e-handel, ang. e-commerce)

Rodzaj handlu, prowadzony w internecie. To proces zawierania transakcji handlowych za pomocą internetu (lub innych sieci komputerowych).

Karta zbliżeniowa

Karta płatnicza pozwalająca na dokonywanie autoryzacji transakcji poprzez przyłożenie do czytnika terminala płatniczego.

Kod CVC2/CVV2

Kod zapisany na odwrocie karty płatniczej pozwalający – wraz z numerem karty, datą jej ważności oraz danymi posiadacza karty – na przeprowadzanie transakcji typu „card-not-present".

Oprogramowanie szpiegujące (Spyware)

Programy komputerowe, których celem jest gromadzenie informacji o użytkowniku oraz przesyłanie danych i informacji użytkownika lub o użytkowniku bez jego wiedzy.

Phishing

Metoda oszustwa, w której przestępca podszywa się pod inną osobę lub organizację w celu wyłudzenia określonych informacji (np. danych logowania do bankowości internetowej) lub nakłonienia ofiary do realizacji określonych działań.

Płatności mobilne

Płatności dokonywane przy użyciu telefonu komórkowego.

Procedura charge-back

Procedura realizowana w związku ze zgłoszeniem przez klienta transakcji dokonanej kartą płatniczą do banku – wydawcy karty, np. w sytuacji nieotrzymania zakupionego towaru, w wyniku której następuje zwrot środków pieniężnych z rachunku sprzedawcy na rachunek kupującego.

Skimming

Działanie przestępcze polegające na skopiowaniu przy użyciu urządzenia zainstalowanego np. na wlocie kart w bankomacie (tzw. skimmera) danych z paska magnetycznego karty płatniczej, co następnie umożliwia zdublowanie takiej karty.

Sniffing

Przechwytywanie przez nieuprawnione osoby informacji przesyłanych w lokalnych sieciach, a także sieciach WiFi. (z j. ang. węszenie, podsłuchiwanie)

Terminal POS (j. ang. Point of Sale – punkt handlowy)

Urządzenie instalowane w punktach handlowo-usługowych służące do odczytywania danych z karty płatniczej oraz do kontaktowania się z centrum autoryzacyjnym, umożliwiające dokonanie płatności za nabywany towar lub usługę w formie bezgotówkowej (przy użyciu karty płatniczej).

Transakcja typu „card-not-present"

Transakcje płatnicze realizowane bez fizycznej obecności karty u sprzedawcy, np. przez internet.

Wirtualna sieć prywatna (od ang. virtual private network – VPN)

Tunel, przez który płynie ruch w ramach sieci prywatnej pomiędzy nadawcą i odbiorcą za pośrednictwem publicznej sieci (takiej jak Internet). Można opcjonalnie kompresować lub szyfrować przesyłane dane w celu zapewnienia lepszej jakości lub większego poziomu bezpieczeństwa

BEZPIECZNE USŁUGI W SIECI

Materiały dla uczestników

BANKOWOŚĆ INTERNETOWA

Internetowy dostęp do konta bankowego, karty płatnicze czy aplikacje mobilne są już wręcz standardem w bankowości. Chętnie korzystamy z bankowości elektronicznej, kupujemy i płacimy kartami w sklepach internetowych. Zakres usług bankowych wciąż się zmienia a wraz z nimi pojawiają się nowe zagrożenia.

Zagrożenia, które mogą nas spotkać to wirusy, które nie są widoczne w momencie, kiedy logujemy się do bankowości elektronicznej, a które starają się nam wykraść login albo hasło, w celu dokonania transakcji bez naszej wiedzy, przekierowując przelew na zupełnie inny numer konta niż zakładaliśmy.

Rodzaje zagrożeń

Phishing bankowy

- Phishing, którego celem jest zdobycie informacji na temat karty płatniczej danej osoby, nadal należy do najpopularniejszych oszustw. Fałszywe wiadomości mogą być wysyłane w imieniu banków lub systemów płatności. Najczęściej temat tych wiadomości jest związany z blokowaniem konta lub „podejrzaną aktywnością" wykrytą na koncie osobistym odbiorcy. Pod pretekstem przywrócenia dostępu, potwierdzenia tożsamości czy anulowania transakcji użytkownik jest proszony o wprowadzenie szczegółowych informacji dotyczących karty płatniczej (często kodu CVV/CVC) na fałszywej stronie banku. Po odebraniu tych danych przestępcy natychmiast wypłacają pieniądze z konta ofiary. Podobnie wygląda sytuacja z systemami płatności, jednak wówczas ofiary są nakłaniane jedynie do zalogowania się do swojego konta.

Pharming

- Odmianą phishingu jest pharming, podczas którego oszuści przekierowują nas z prawidłowej strony np. banku, na ich podrobioną wersję, która ma zbierać dane osobowe. Umożliwiają to poważne wirusy i konie trojańskie. Aby się więc uchronić przed pharmingiem, należy zainstalować na komputerze program antywirusowy i aktualizować bazę złośliwych programów. Możemy również sprawdzać wiarygodność danej strony, klikając w przeglądarce na ikonę kłódki i sprawdzając dane właściciela.

Carding

- Carding to kradzież i wykorzystywanie cudzych numerów kart płatniczych. Oszuści do kradzieży numerów kart płatniczych wykorzystują wiele, często skomplikowanych metod. Dane mogą pozyskiwać np. dzięki specjalnym programom szpiegowskim, wirusom, koniom trojańskim, czy fałszowaniu wiadomości i telefonów z banków i innych instytucji. Zdarza się również, że przedrą się przez słabe zabezpieczenia sklepu internetowego lub wręcz podrobią jego stronę. Możliwe jest także zwykłe podejrzenie numeru karty w momencie, w którym płacimy nią stacjonarnie.

Scam

- Jedną z metod pozyskiwania danych jest scam, czyli wzbudzanie zaufania w celu wyłudzenia pieniędzy lub też uzyskania informacji potrzebnych do przeprowadzenia transakcji internetowych. Może to być np. wysyłanie maili i listów, oferowanie usług internetowych czy nawiązywanie kontaktu telefonicznego. Ze scamem często możemy spotkać się w spamie przesyłanym na skrzynkę mailową. Przestępcy kuszą m.in. dodatkowymi formami zarobku lub wygraną w konkursie w zamian za przekazanie danych lub zainwestowanie danej sumy. Uważać musimy również na podejrzane ankiety oraz strony www zbierające dane osobowe. Jak chronić się przed scamem? Przede wszystkim ustawmy na swojej skrzynce pocztowej wykrywanie spamu i przenoszenie go

do osobnego katalogu. Zawsze sprawdzajmy też komu i w jakim celu przekazujemy dane osobowe i numery kart płatniczych.

Zasady bezpieczeństwa

1. **Bezpieczne logowanie**

- Stwórz silne, unikalne hasło do konta – hasło do bankowości elektronicznej powinno być jedyne w swoim rodzaju: długie oraz składające się z wielkich i małych liter, cyfr i znaków specjalnych. Pamiętaj także: nie zapisuj nigdzie haseł służących do logowania i pamiętaj o ich regularnej zmianie – najlepiej raz w miesiącu.

- Sprawdzaj zabezpieczenia strony banku – podczas logowania do bankowości elektronicznej, zwróć uwagę na dwa elementy: szyfrowanie połączenia i certyfikat bezpieczeństwa. Połączenia szyfrowane rozpoznasz po symbolu kłódki w pasku adresu przeglądarki oraz „hpps" na początku adresu do strony logowania – to gwarantuje, że Twoje dane są bezpieczne. Certyfikat potwierdza, że strona jest zaufana, możemy to sprawdzić, klikając na kłódkę obok adresu witryny.

- Poufność danych - 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.

2. **Bezpieczny sprzęt**

- Zabezpiecz komputer i telefon – wszystkie urządzenia, na których korzystamy z naszego rachunku bankowego powinny być odpowiednio chronione poprzez: legalne oprogramowanie, które okresowo jest aktualizowane, programy antywirusowe, które zabezpieczą sprzęt przed wirusami oraz firewall (zapora sieciowa) służący do ochrony przed atakami z zewnątrz.

- Dbaj o swój telefon – niektóre osoby pozostają zalogowane do mobilnych aplikacji banków nawet wtedy, kiedy już z nich nie korzystają. Kiedy stracimy telefon, złodziej przejmuje kontrolę nie tylko nad urządzeniem, ale także może wykorzystać nasze konto bankowe poprzez bankowość mobilną. Pamiętaj, aby uważać na to, co dzieje się z Twoim telefonem, a ponadto zawsze wylogowuj się z aplikacji w smartfonie.

- Korzystaj z bezpiecznych sieci WI-FI – otwarte sieci bezprzewodowe np. w galeriach handlowych są zwykle darmowe, jednak logowanie się do swojego banku, kiedy jesteśmy podłączeni do takiej sieci, to spore ryzyko. Nieograniczony dostęp i brak jakichkolwiek zabezpieczeń to wyjątkowo łatwy cel dla hakerów.

3. Bezpieczne użytkowanie

- Sprawdzaj datę ostatniego logowania do bankowości elektronicznej – mało z nas zdaje sobie sprawę, że ten banalny z pozoru komunikat może nam zaoszczędzić sporo kłopotów. Warto zwrócić uwagę na informację, która pojawia się na naszym internetowym rachunku i zweryfikować, czy wtedy naprawdę korzystaliśmy z konta. Jeśli nie – należy powiadomić o tym bank i szybko zmienić hasło.

- Weryfikuj kody SMS – cyberprzestępcy dysponujący Twoim rachunkiem do potwierdzenia operacji potrzebują kodu z SMS. Jeśli haker poznał Twój numer telefonu, może także podmienić wiadomości weryfikacyjne z banku. Pamiętaj, aby dokładnie

czytać takie SMS-y i sprawdzać, czy zgadza się kwota operacji oraz numer rachunku odbiorcy.

- Włącz powiadomienia SMS – jeśli chcesz mieć pełną kontrolę nad kontem i tym, co się na nim dzieje, możesz włączyć usługę powiadamiania SMS od banku, które informują o zmianach na rachunku, Jeśli coś dziwnego zacznie dziać się na Twoim rachunku, szybko to zauważysz i będziesz mógł odpowiednio zareagować.

- Ustaw limity dla transakcji kartami płatniczymi – zbyt wysokie limity dla kart debetowych i kredytowych, szczególnie z funkcją zbliżeniową, ułatwiają złodziejom „czyszczenie" naszych kont.

PŁATNOŚCI MOBILNE

Coraz częściej korzystamy z bankowych aplikacji mobilnych umożliwiających dokonanie płatności głównie za pomocą telefonu, ale także innych urządzeń mobilnych. Cenimy sobie to rozwiązanie za wygodę i dostępność, ale zbyt rzadko rozważamy ryzyko, jakie się z nim wiąże. Taka forma płatności wiąże się mimo wszystko z ryzykiem, że np. nasze dane i pieniądze mogą dostać się w niepowołane ręce.

Rodzaje i metody płatności mobilnych

Biorąc pod uwagę sposób realizacji, możemy podzielić płatności mobilne na zdalne i zbliżeniowe.

- Płatności zdalne to te, w których lokalizacje płatnika i beneficjenta płatności nie mają znaczenia w momencie inicjowania płatności.
- Płatności zbliżeniowe to transfer danych, podczas którego lokalizacja obu stron odgrywa duże znaczenie i który zachodzi w bardzo bliskiej odległości. Tego rodzaju płatności dokonujemy za pośrednictwem technologii NFC oraz kodów QR. Technologia NFC (Near Field Communication) to bezprzewodowa technologia komunikacyjna, wykorzystująca

fale radiowe w celu wymiany danych w bliskiej odległości. W przypadku kodów QR (Quick Response) bliska odległość jest niezbędna, aby zeskanować kod, który dzięki któremu na naszym smartfonie pojawią się dane niezbędne do dokonania płatności.

Płatności mobilnych możemy dokonać na podstawie rachunku bankowego, rachunku karty płatniczej, rachunku przedpłaconego (przed dokonaniem płatności płatnik musi zasilić rachunek u operatora mobilnego) lub systemu billingowego (płatność mobilna jest doliczana do rachunku klienta operatora telefonii komórkowej). Podstawowe metody płatności mobilnych to m.in.: Apple Pay, Google Pay, Blik. Apple Pay umożliwia płacenie zbliżeniowe za pomocą m.in. iPhone'a, Apple Watcha czy iPada, natomiast Google Pay na urządzeniach z Androidem.

W obu systemach można dokonać płatności w sklepach oraz w wybranych aplikacjach mobilnych. Blick opiera się na 6-cyfrowych kodach i jest powiązany z aplikacją mobilną konkretnego banku. Kodem Blik możemy zapłacić w sklepie stacjonarnym, internetowym, a także wypłacić gotówkę z bankomatu i dokonać przelewu na telefon. Nie możemy jednak dokonać płatności zbliżeniowej.

Zasady bezpieczeństwa

Zgubienie lub kradzież urządzenia mobilnego – podobnie jak karty płatniczej – naraża nas na ryzyko dokonania płatności przez osoby trzecie. W takiej sytuacji bardzo ważne jest szybkie zgłoszenie kradzieży, zablokowanie karty oraz urządzenia mobilnego. Warto wiedzieć, że zastosowanie odpowiednich zabezpieczeń (PIN, odcisk palca) może znacznie ograniczyć ryzyko utraty funduszy. Inny rodzaj ryzyka jest związany z wyłudzeniem naszych danych niezbędnych do dokonania płatności mobilnej. Dlatego należy przestrzegać zasad bezpieczeństwa:

- Aktualne oprogramowanie antywirusowe - Na telefonie służącym do dokonywania płatności mobilnych należy zawsze instalować najnowsze aktualizacje bezpieczeństwa systemu operacyjnego.
- Blokada ekranu - Telefon z zainstalowaną aplikacją do płatności mobilnych powinien mieć włączoną blokadę ekranu, której dezaktywacja powinna wymagać wprowadzenia hasła (lub w inny sposób była możliwa do dokonania jedynie dla prawowitego właściciela telefonu).

- Bezpieczne hasło - Nie należy zapisywać hasła do aplikacji płatności mobilnych na kartce (lub innym nośniku), zwłaszcza przechowywanej wraz z telefonem, hasło do telefonu powinno być inne niż do aplikacji płatności mobilnych; hasła te powinny również być trudne do odgadnięcia. A jak zapamiętać trudny do odgadnięcia kod PIN? To – wbrew pozorom – bardzo proste. Warto sobie przypomnieć, że na ekranowej klawiaturze numerycznej telefonu do cyfr od 2 do 9 przypisanych jest po kilka liter (np. cyfrze 2 odpowiadają litery „ABC", cyfrze 3 – „DEF" itd.).
- Utrata / oddanie telefonu - Niezwłocznie po utracie telefonu, na którym zainstalowana była aplikacja płatności mobilnych, należy zgłosić ten fakt w swoim banku. Oddając telefon do serwisu warto odinstalować aplikację płatności mobilnych.

ZAKUPY W INTERNECIE

Coraz bardziej popularne zakupy i płatności internetowe mogą być ryzykowne. Ofiarą takiego oszustwa może zostać każdy i to nie tylko poprzez dokonywanie zakupów w sklepach internetowych, ale również na portalach aukcyjnych.

Zasady bezpieczeństwa

- Zaufane sklepy internetowe – 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.
- Kontrola sklepu - Przeczytaj regulamin sklepu i zasady zwrotu towarów, zweryfikuj dane rejestrowe firmy. Sprawdź opinie o sprzedawcy w niezależnych serwisach.

- Bezpieczna płatność - Za najbezpieczniejszą formę płatności w sklepach internetowych uznaje się płacenie kartą. W ten sposób, w razie gdybyśmy mieli dalsze problemy, możemy w swoim banku uruchomić procedurę tzw. charge-back.
- Zabezpiecz konto bankowe dwuskładnikowym uwierzytelnianiem z aplikacji albo kodem SMS lub zdrapką. Przed dokonaniem transakcji upewnij się, że transmisja odbywa się w bezpiecznym połączeniu za pomocą protokołu SSL/TLS.
- Płatność za pobraniem - W razie wątpliwości wybierz płatność za pobraniem albo płatność kartą (płatność kartą możesz reklamować w banku).
- Bezpieczna dostawa - Zamów dostawę z opcją sprawdzenia zawartości przesyłki.
- Historia zakupu - Zachowaj korespondencję ze sprzedawcą. W razie problemów rozpocznij procedurę reklamacji w ramach platformy handlowej, operatora płatności, zgłoś reklamację do banku, zgłoś sprawę na policję.

KOMUNIKACJA I PRACA ZDALNA

Korzystanie z publicznych niezabezpieczonych sieci Wi-Fi może być ryzykowne. Sieci WiFi wykorzystują fale radiowe do komunikacji, co także powoduje, że każdy kto jest w zasięgu ich odbioru może próbować podsłuchiwać cały ruch. W efekcie włamanie do takiej sieci nie jest szczególnie trudne, zwłaszcza, że pozwalają na to gotowe rozwiązania programowe.

Użytkownik korzystający z takiej sieci, wystawia swe zasoby cyfrowe zapisane w pamięci komputera, bądź smartfona na widok hakerów. Cyberprzestępcy mogą wówczas śledzić aktywność użytkownika online, a nawet przejąć jego dane czy hasła dostępu np. do bankowości online.

Tworzenie prywatnej sieci VPN

Można ochronić swoją prywatność i informację o czynnościach online dzięki Wirtualnej Sieci Prywatnej (VPN – Virtual Private Network). VPN to technologia która tworzy prywatny, szyfrowany tunel dla naszych działań online, czyniąc je o wiele trudniejszym dla innych do obserwowania lub monitorowania tego co robimy w internecie. Ponadto VPN ukrywa lokalizację użytkownika, utrudniając zidentyfikowanie naszego położenie stronom internetowym, które odwiedzamy. Korzystanie z VPN jest proste.

- W pierwszej kolejności należy znaleźć dostawcę usługi VPN któremu zaufamy, a następnie należy założyć konto (VPN to z reguły usługa płatna),
- Gdy już mamy konto, ściągamy i instalujemy oraz konfigurujemy oprogramowanie obsługujące dany VPN,
- Po zainstalowaniu i konfiguracji możemy połączyć się z internetem jak zawsze,
- Oprogramowanie dostawcy VPN w cichy sposób utworzy szyfrowany kanał i zacznie chronić naszą prywatność, tak że nawet nie zdążymy się zorientować.

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ III

BEZPIECZNE KORZYSTANIE Z KOMPUTERA W MIEJSCU PRACY

SESJA 2

BEZPIECZNE USŁUGI W SIECI

PODSUMOWANIE

1. Jak nazywa się trzycyfrowy kod przypisany do karty płatniczej, który wpisujemy przy transakcjach online?
    a. PUK
    b. CVC/CVV
    c. PPV

2. Jak nazywa się usługa umożliwiająca zwrot pieniędzy na kartę kredytową, gdy transakcja nie doszła do skutku?
    a. Payback
    b. Chargeback
    c. Prepaid

3. W jakiej sytuacji możemy najbezpieczniej korzystać z e-bankowości?
    a. Na urządzeniu udostępnionym przez bank np. w oddziale lub na naszym sprzęcie podłączonym do zaufanej sieci domowej
    b. Na ogólnodostępnym komputerze, na przykład w hotelu czy bibliotece
    c. Gdy łączymy się z siecią przez publiczne WiFi

4. Zaznacz sytuacje, w których wykorzystujesz dwustopniowe uwierzytelnienie:
    a. potwierdzając kodem jednorazowym wykonanie przelewu w banku
    b. pobierając gotówkę z bankomatu
    c. odblokowując telefon zabezpieczony hasłem

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ III

BEZPIECZNE KORZYSTANIE Z KOMPUTERA W MIEJSCU PRACY

SESJA 2

BEZPIECZNE USŁUGI W SIECI

PODSUMOWANIE

1. Jak nazywa się trzycyfrowy kod przypisany do karty płatniczej, który wpisujemy przy transakcjach online?
    a. PUK
    b. CVC/CVV
    c. PPV

2. Jak nazywa się usługa umożliwiająca zwrot pieniędzy na kartę kredytową, gdy transakcja nie doszła do skutku?
    a. Payback
    b. Chargeback
    c. Prepaid

3. W jakiej sytuacji możemy najbezpieczniej korzystać z e-bankowości?
    a. Na urządzeniu udostępnionym przez bank np. w oddziale lub na naszym sprzęcie podłączonym do zaufanej sieci domowej
    b. Na ogólnodostępnym komputerze, na przykład w hotelu czy bibliotece
    c. Gdy łączymy się z siecią przez publiczne WiFi

4. Zaznacz sytuacje, w których wykorzystujesz dwustopniowe uwierzytelnienie:
    a. potwierdzając kodem jednorazowym wykonanie przelewu w banku

b. pobierając gotówkę z bankomatu

c. odblokowując telefon zabezpieczony hasłem

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ III

BEZPIECZNE KORZYSTANIE Z KOMPUTERA W MIEJSCU PRACY

SESJA 2

BEZPIECZNE USŁUGI W SIECI

ANKIETA WSTĘPNA

OCENA WIEDZY I UMIEJĘTNOŚCI PRAKTYCZNYCH							
W każdym z pytań prosimy o zaznaczenie znakiem „X" odpowiedzi na poszczególne pytania w skali 7-punktowej gdzie: 1 - oznacza „zdecydowanie źle", 2 - „źle", 3 - „raczej źle", 4 - „ani dobrze, ani źle", 5 - „raczej dobrze, 6 – „dobrze", 7 - „zdecydowanie dobrze".							
Pytanie	***1***	***2***	***3***	***4***	***5***	***6***	***7***
1. Jak Pani/Pan ocenia swoją wiedzę na zagrożeń związanych z usługami oferowanymi w internecie i poprzez urządzenia mobilne?	□	□	□	□	□	□	□
2. Jak Pani/Pan ocenia swoją wiedzę na temat zasad bezpieczeństwa w zakresie bankowości internetowej?	□	□	□	□	□	□	□
3. Jak Pani/Pan ocenia swoją wiedzę na temat zasad bezpieczeństwa w zakresie płatności mobilnych?	□	□	□	□	□	□	□
4. Jak Pani/Pan ocenia swoją wiedzę na temat zasad bezpieczeństwa w zakresie zakupów w sklepach internetowych?	□	□	□	□	□	□	□
5. Jak Pani / Pan ocenia swoją wiedzę na temat zasad bezpieczeństwa w zakresie komunikacji i pracy zdalnej?	□	□	□	□	□	□	□

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ III

BEZPIECZNE KORZYSTANIE Z KOMPUTERA W MIEJSCU PRACY

SESJA 2

BEZPIECZNE USŁUGI W SIECI

ANKIETA KOŃCOWA

OCENA WIEDZY I UMIEJĘTNOŚCI PRAKTYCZNYCH							
W każdym z pytań prosimy o zaznaczenie znakiem „X" odpowiedzi na poszczególne pytania w skali 7-punktowej gdzie: 1 - oznacza „zdecydowanie źle", 2 - „źle", 3 - „raczej źle", 4 - „ani dobrze, ani źle", 5 - „raczej dobrze, 6 – „dobrze", 7 - „zdecydowanie dobrze".							
Pytanie	***1***	***2***	***3***	***4***	***5***	***6***	***7***
1. Jak Pani/Pan ocenia swoją wiedzę na zagrożeń związanych z usługami oferowanymi w internecie i poprzez urządzenia mobilne?	☐	☐	☐	☐	☐	☐	☐
2. Jak Pani/Pan ocenia swoją wiedzę na temat zasad bezpieczeństwa w zakresie bankowości internetowej?	☐	☐	☐	☐	☐	☐	☐
3. Jak Pani/Pan ocenia swoją wiedzę na temat zasad bezpieczeństwa w zakresie płatności mobilnych?	☐	☐	☐	☐	☐	☐	☐
4. Jak Pani/Pan ocenia swoją wiedzę na temat zasad bezpieczeństwa w zakresie zakupów w sklepach internetowych?	☐	☐	☐	☐	☐	☐	☐
5. Jak Pani / Pan ocenia swoją wiedzę na temat zasad bezpieczeństwa w zakresie komunikacji i pracy zdalnej?	☐	☐	☐	☐	☐	☐	☐

CYBERBEZPIECZEŃSTWO W PRACY I DOMU

CZĘŚĆ III BEZPIECZNE KORZYSTANIE Z KOMPUTERA W MIEJSCU PRACY

SESJA 2 BEZPIECZNE USŁUGI W SIECI

ANKIETA EWALUACYJNA

PROWADZENIE SZKOLENIA

1. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **wiedzę i przygotowanie merytoryczne** osoby prowadzącej szkolenie?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

2. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **umiejętność przekazania wiedzy** przez osobę prowadzącą szkolenie?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

3. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **kontakt i umiejętność pracy z grupą** osoby prowadzącej szkolenie?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

PROGRAM SZKOLENIA I MATERIAŁY DYDAKTYCZNE

4. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **przydatność szkolenia** w względem potrzeb uczestników?

Zdecydowanie nieprzydatne	*Raczej nieprzydatne*	*Trudno powiedzieć*	*Raczej przydatne*	*Zdecydowanie przydatne*
1	2	3	4	5

5. Proszę ocenić na pięciostopniowej skali, w jakim stopniu szkolenie pogłębiły Pani/Pana **wiedzę teoretyczną** z omawianego na szkoleniu obszaru?

Niewystarczająco	*Wystarczająco*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

6. Proszę ocenić na pięciostopniowej skali, w jakim stopniu przeprowadzone szkolenie pogłębiło Pani/Pana **umiejętności praktyczne** z omawianego na warsztatach tematu?

Niewystarczająco	*Wystarczająco*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

7. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **jasność i zrozumiałość** wykorzystanych **kart pracy**?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

8. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **przydatność ćwiczeń** w zdobyciu wiedzy i umiejętności z zakresu tematyki szkolenia ?

Zdecydowanie nieprzydatne	*Raczej nieprzydatne*	*Trudno powiedzieć*	*Raczej przydatne*	*Zdecydowanie przydatne*
1	2	3	4	5

9. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **jasność i zrozumiałość** wykorzystanej **prezentacji multimedialnej**?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5

10. Proszę odpowiedzieć na pięciostopniowej skali, jak ocenia Pani/Pan **jasność i zrozumiałość materiałów dla uczestników**?

Bardzo źle	*Źle*	*Średnio*	*Dobrze*	*Bardzo dobrze*
1	2	3	4	5