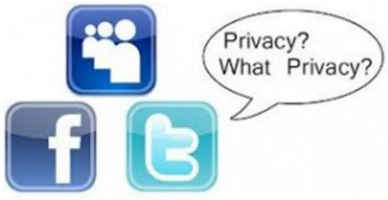
Projekt IDCAP: Poprawa kompetencji cyfrowych u osób dorosłych

Numer projektu: 2018-1-PL01-KA204-051003

Jak chronić moje dane osobowe?

Obszar kompetencji: Ochrona danych osobowych i prywatności



Wprowadzenie

Moduł obejmuje kluczowe tematy z zakresu ochrony danych osobowych i prywatności. Cele modułu są następujące:

- omawianie zasad bezpieczeństwa w środowisku cyfrowym i informowanie o potencjalnych zagrożeniach - kradzieży informacji, fałszywych pocztach elektronicznych i innych;
- przedstawienie podstawowych zasad bezpieczeństwa użytkowania technologii - jakich zasad należy przestrzegać podczas korzystania z Internetu w publicznie dostępnych sieciach Wi-Fi, co to jest bezpieczne połączenie i jakie są niezabezpieczone załączniki poczty elektronicznej?
- aby wyjaśnić użycie bezpiecznych haseł - jakich zasad należy przestrzegać przy tworzeniu haseł? Jak bezpiecznie posługiwać się hasłami w życiu codziennym?

1. Wprowadzenie do bezpieczeństwa w środowisku cyfrowym

1.1. Bezpieczeństwo komputerowe

Bezpieczeństwo komputerowe oznacza, że nasz komputer jest chroniony przed nieautoryzowanym dostępem, użyciem, ujawnieniem, ingerencją, zmianą lub zniszczeniem. Jest to zarówno możliwe, jak i konieczne, aby dbać o własne informacje i bezpieczeństwo komputerowe. Informacje przechowywane na komputerze i publikowane w Internecie mogą mieć wpływ na samopoczucie, zdrowie, a nawet życie. Istnieje wiele zagrożeń - zagrożenie prywatności, łamanie haseł lub hakerstwo, ujawnianie danych osobowych, wirusy, wgrywanie, pobieranie i wysyłanie złośliwych plików oraz złośliwe osoby, które chcą wyrządzić szkodę.

W Internecie mamy dostęp do sieci społecznościowych, czatów internetowych, forów, specjalnych programów do czatów (jak Skype), gier i innych. Jeśli nie są spełnione niezbędne standardy bezpieczeństwa, osoby o złych intencjach mogą nie tylko dowiedzieć się o Twoich prywatnych danych, ale także wykorzystać Twoją tożsamość (podszywać się pod Ciebie).

Wirusy komputerowe stały się "klasyczną wartością". Stosowane są różne metody, np. użytkownik otrzymuje e-mail z linkiem do popularnej strony internetowej, takiej jak Youtube lub Facebook z kuszącym filmem lub obrazem. Próba obejrzenia go zaraża bezbronny komputer użytkownika za pomocą jednego kliknięcia myszką.

Załączniki poczty elektronicznej są szczególnie niebezpieczne, ponieważ mogą zawierać wirusy i inne złośliwe oprogramowanie. Otwarcie załącznika w wiadomości e-mail może spowodować automatyczną instalację złośliwego oprogramowania na Twoim komputerze i nawet nie zauważysz go. Takie

złośliwe oprogramowanie może wpływać na pliki komputerowe, kraść hasła lub szpiegować użytkownika, dlatego należy zachować szczególną ostrożność przy otrzymywaniu wiadomości z załącznikami od nieznanych odbiorców.

Porady dotyczące postępowania z niechcianymi załącznikami poczty elektronicznej:

Porada	**Objaśnienie**
Nigdy nie otwieraj podejrzanych załączników do wiadomości e-mail	Nawet jeśli otrzymasz e-mail od kogoś, kogo znasz, nie ma gwarancji, że dana osoba faktycznie go wysłała. Złośliwe oprogramowanie może automatycznie wysyłać do Ciebie wiadomości zawierające wirusy. Kiedy otrzymujesz email z załącznikiem, najlepiej poprosić samego nadawcę, aby upewnił się, że wysłał email.
Aktualizacja programu antywirusowego	Jeśli program antywirusowy nie jest aktualizowany, nie może chronić komputera przed wirusami.
Zostaw włączony *firewall* na komputerze.	Zapora ogniowa komputera pomaga zapobiegać uzyskiwaniu dostępu do komputera przez Internet przez ludzi lub złośliwe oprogramowanie.
Jeśli to możliwe, przed pobraniem załączników do poczty elektronicznej	Wielu dostawców poczty elektronicznej online automatycznie sprawdza załączniki przed ich

Porada	Objaśnienie
należy sprawdzić, czy nie zawierają one wirusów.	pobraniem. Jeśli komputer poprosi Cię o sprawdzenie, czy nie masz wirusów, pobierając załączniki, zrób to samodzielnie.

1.2. Bezpieczeństwo danych - phishing

Phishing jest rodzajem cyberprzestępczości, która łączy w sobie zestaw narzędzi inżynierii społecznej i narzędzi technicznych umożliwiających kradzież wrażliwych, osobistych i finansowych informacji od ofiary. Napastnik próbuje udawać prawdziwą organizację, zaufany autorytet lub znaną osobę.

Większość ofiar phishingu zachęca się do klikania na e-maile o następujących tematach:

- ✓ Formalne zawiadomienie o wycieku danych
- ✓ Zawiadomienie o dostawie UPS 1ZBE312TYI00015011B23
- ✓ Przypominam: Twoje hasło wygaśnie w mniej niż 24 godziny.
- ✓ Musisz natychmiast zmienić swoje hasło
- ✓ Proszę przeczytać ważną informację od swojego administratora

Jak rozpoznać phishing:

Zbyt dobre, by było prawdziwe. Są to wiadomości, listy, telefony, które mówią Ci, że wygrałeś na loterii lub że zostałeś losowo wybrany, aby otrzymać nagrodę lub usługę.

Szybka oferta. Frazesy: "ostatnia szansa", "tylko 1 godzina", "tylko dzisiaj" i tak dalej wskazuje na przypadek phishingu. Oszuści używają manipulacji, które stwarzają poczucie pilności. W przypadku otrzymania tego typu wiadomości,

wskazane jest sprawdzenie prawdziwości informacji bezpośrednio w firmie lub usługodawcy.

Ukryte linki z innymi słowami kluczowymi. Wielu oszustów używa prostych słów kluczowych, zwrotów, które doprowadzą Cię do oszukańczej strony. Te linki często ukrywają zupełnie inną stronę, niż myślisz. Bardzo dobrym sposobem na upewnienie się, że otwierasz stronę, jest kliknięcie *PRAWEGO* przycisku myszy i wybranie opcji *Inspekcja.* Zobacz, jaki link jest powiązany z tym linkiem lub słowem kluczowym. Co on ukrywa? Bądź ostrożny, ponieważ nieścisłości ortograficzne często ukrywają fałszywe linki.

Dziwne załączniki. Jeśli nie oczekujesz żadnych konkretnych informacji, nie powinieneś przeglądać załączników do wiadomości e-mail. Jedną z metod cyberprzestępczości jest dołączanie do niewinnej wiadomości pliku, który może zawierać złośliwe oprogramowanie. Zaleca się sprawdzenie nadawcy, celu wiadomości przed jej otwarciem. Jedyny bezpieczny format, który może być otwarty za pomocą pliku .txt.

Jak uniknąć phishingu:

Porada	**Objaśnienie**
Bądź czujny	Zawsze uważnie czytaj maile od przyjaciół i nieznajomych.
Uważaj na różne kanały komunikacji	Zwróć uwagę na różne rodzaje komunikacji - e-maile, ogłoszenia, rozmowy telefoniczne i inne rodzaje komunikacji, które wymagają jakichkolwiek informacji finansowych.
Kliknij uważnie	Unikaj klikania na "włącz treść", co pozwala na dodatkowe linkowanie pomiędzy różnymi dokumentami.
Nie klikaj na podejrzane linki	Unikaj klikania na linki w wiadomościach e-mail, aplikacjach do wysyłania wiadomości lub reklamach.

	Przeglądaj linki indywidualnie, korzystając z wszystkich dostępnych zasobów.
Sprawdzić wiarygodność nadawcy	Upewnij się, że e-mail pochodzi z zaufanego źródła.

Jeśli jesteś ofiarą phishingu:

1) Zmieniaj hasła do swoich aplikacji i kont online za pomocą innego telefonu lub komputera.
2) Zeskanuj swój komputer w poszukiwaniu wirusów i sprawdź, czy nie zawiera on złośliwego oprogramowania.
3) Zgłoś kradzież danych na policję i zachowaj kopię wniosku.
4) Zgłoś się do swojej organizacji / banku lub właściwego organu.

1.3. Bezpieczeństwo użytkowników komputerów - Informacje zamieszczane na portalach społecznościowych

Istnieją dwa sposoby spojrzenia na koncepcję bezpieczeństwa użytkowników komputerów. Można mówić o potencjalnym zagrożeniu zdrowia użytkownika przez komputer, np. o możliwości porażenia elektrycznego, nawet jeśli jest ono niewielkie. Jednak najczęstszym zagrożeniem dla człowieka jest ryzyko związane z informacjami publikowanymi samodzielnie.

Często brak jest świadomości, jak wiele różnych zagrożeń stwarzają sieci społecznościowe.

Portale społecznościowe są ważną częścią dzisiejszego życia codziennego - są do tego przyzwyczajone:

- Porozumieć się;
- Zdobądź informacje;
- Wysyłać i udostępniać informacje itp.

Istnieją dwa rodzaje zagrożeń dla sieci społecznościowych: zagrożenia **technologiczne** i **organizacyjne**.

Zagrożenia technologiczne związane są z różnymi technologiami i ich wykorzystaniem w sieciach społecznościowych. Zagrożenia **organizacyjne związane są z** zachowaniami internautów, działaniami i czynnościami samego użytkownika. Atak zagrożenia organizacyjnego jest zazwyczaj spowodowany przez kogoś innego w sieci społecznościowej.

Najczęstszymi zagrożeniami na portalach społecznościowych są:

- ✓ różne rodzaje złośliwego oprogramowania lub wirusów;
- ✓ ataki typu phishing - wiadomości lub e-maile typu phishing zawierające linki do witryn zainfekowanych złośliwym oprogramowaniem;

- ✓ rozsyłanie spamu;
- ✓ ukryte kliknięcia, które powodują, że użytkownik klika na coś innego niż pierwotnie zamierzony;
- ✓ różne rodzaje profili kutych - niektóre z nich są półautomatyczne lub w pełni zautomatyzowane, a niektóre wykonywane są przez człowieka;
- ✓ Ataki inferencyjne to techniki eksploracji danych i informacji, które analizują dostępne dane w celu uzyskania dodatkowych informacji o ofierze. W serwisach społecznościowych są one wykorzystywane do odnoszenia się do danych osobowych i wrażliwych informacji, których użytkownik nie zdecydował się udostępnić, takich jak przekonania religijne i orientacja seksualna, oraz do identyfikacji tych informacji. Atak na serwisy społecznościowe opiera się na informacjach dostępnych na profilach ofiary i jej przyjaciół.
- ✓ cybermobbing - emocjonalne upokorzenie przy użyciu nowoczesnej technologii. Zamykanie dostępu, poniżanie, seksowanie, nękanie, wysyłanie paskudnych zdjęć, szydzenie, kłamanie na temat tożsamości w celu uzyskania informacji osobistych, dostęp do informacji o innych ludziach, śledzenie, itp.

Aby uniknąć zagrożeń, można korzystać z różnych rozwiązań oferowanych przez portale społecznościowe:

- mechanizmy uwierzytelniania,
- blokowanie użytkowników,
- osobiste ustawienia użytkowników,
- opcja "zgłoś użytkownika".

Wymienione rozwiązania mogą być z powodzeniem stosowane w celu ochrony użytkownika przed fałszywymi profilami, nadużyciami emocjonalnymi, zachowaniami naiwnymi i ryzykownymi.

Różne firmy oferujące rozwiązania bezpieczeństwa - AVG, Avira, Kaspersky, Panda, McAfee, Symantec - oferują użytkownikom sieci społecznościowych rozwiązania bezpieczeństwa w Internecie. Ich oprogramowanie zazwyczaj zawiera program antywirusowy i zaporę sieciową, czasami oferując użytkownikom Internetu ochronę przed spamem i phishingiem. Takie oprogramowanie pomaga użytkownikom serwisów społecznościowych chronić ich komputery osobiste przed zagrożeniami takimi jak złośliwe oprogramowanie, ukryte kliknięcia i phishing.

Porady dotyczące bezpiecznych portali społecznościowych

Typ	**Przykład**
Posting	Zastanów się uważnie przed zamieszczeniem informacji. Wszystko, co opublikujesz, może w pewnym momencie stać się publicznie dostępne i może mieć negatywny wpływ na Twoją reputację i przyszłość. Bądź ostrożny - inni również mogą zamieszczać o Tobie informacje. Być może będziesz nawet musiał poprosić kogoś, by usunął informacje, które o Tobie opublikował.
Prywatność	Praktycznie wszystkie portale społecznościowe mają dodatkowe opcje prywatności - ustawiaj je, gdy tylko jest to możliwe. Na przykład, czy strona internetowa naprawdę musi znać Twoją lokalizację? Regularnie sprawdzaj opcje prywatności i upewnij się, że działają one tak, jak myślisz.
Hasła	Chroń swoje konta w serwisach społecznościowych za pomocą wystarczająco długiego i unikalnego hasła lub frazy hasła. Hasło jest hasłem, które składa się z kilku słów, dzięki czemu jest łatwe do zapamiętania i zapisania, ale znacznie trudniejsze do odgadnięcia dla cyberprzestępców.

Typ	Przykład
Oszustwo	Podobnie jak e-maile, powiadomienia na portalach społecznościowych mogą być wykorzystywane do różnych prób oszustwa. Na przykład, złośliwa osoba może próbować zakraść się do Twojego hasła lub informacji o karcie kredytowej. Bądź ostrożny z linkami, które otrzymujesz.
Kontakty	Nie należy kontaktować się z obcymi i podejrzanymi osobami. Tworzenie fałszywych profili jest bardzo proste, a wiele osób wykorzystuje je do kłamania na temat swojej tożsamości. Celem tych profili jest oszukanie, zdobycie Twojego zaufania i wykorzystanie go przeciwko Tobie.
Warunki użytkowania	Zapoznaj się z terminami używanymi w serwisach społecznościowych - wszystko, co umieścisz, może stać się własnością sieci społecznościowych.
Praca	Jeśli chcesz opublikować coś na temat swojej pracy, najpierw dowiedz się, czy jest to do zaakceptowania dla Twojego kierownictwa.

Oszustwa personalne

Nowa forma cyberprzestępczości - spersonalizowane oszustwa - staje się coraz bardziej popularna. Cyberprzestępcy zbierają lub kupują informacje o milionach ludzi, a następnie wykorzystują te informacje do personalizacji ataków. Im więcej wiesz o takich atakach, tym łatwiej będzie je wykryć i powstrzymać.

Oszustwa e-mailowe i telefoniczne nie są nowe, cyberprzestępcy od lat próbują oszukiwać ludzi. Przykładem może być "Wygrałeś na loterii" lub słynne oszustwo Księcia Nigerii. Ale w tych tradycyjnych atakach cyberprzestępcy nie wiedzą, z czym będą mieli do czynienia. Po prostu robią ogólny e-mail i wysyłają go do milionów ludzi. Ponieważ te oszustwa są tak ogólnikowe i jednolite, że zazwyczaj

łatwo je rozpoznać. Oszustwa spersonalizowane są inne, cyberprzestępczość jest najpierw badana, a następnie przygotowywany jest e-mail odpowiedni dla każdej ofiary. Robią to poprzez zbieranie informacji lub kupowanie bazy danych z nazwiskami, hasłami, numerami telefonów i innymi informacjami. Takie informacje są łatwo dostępne dzięki wielu zhakowanym stronom internetowym. Są one również często swobodnie dostępne na portalach społecznościowych oraz w publicznie dostępnych zasobach władz publicznych.

Atak działa w następujący sposób: znajdują lub kupują informacje o nazwach użytkowników i hasłach uzyskanych od zhakowanych stron internetowych, następnie znajdują Twój adres e-mail i informacje o Tobie w takiej bazie danych i wysyłają je do Ciebie (jak i do wszystkich innych osób w tej bazie) - e-mail z informacjami o Tobie, w tym hasłem, którego użyłeś na zhakowanej stronie. Cyberprzestępcy podają Ci to hasło jako "dowód", że Twój komputer lub urządzenie zostało zhakowane, co jest oczywiście błędne. Cyberprzestępcy twierdzą również, że po włamaniu się do Internetu wkradałeś się do materiałów pornograficznych. E-mail grozi, że jeśli nie zapłacisz okupu, do Twojej rodziny i przyjaciół zostaną wysłane dowody Twojej haniebnej aktywności w Internecie.

Kluczem jest to, **że** w tym i prawie we wszystkich takich przypadkach, cyberprzestępcy nie włamali się do twojego urządzenia. Nie wiedzą nawet, kim jesteś i jakie strony internetowe odwiedzasz. Oszuści po prostu próbują wykorzystać niektóre z rzeczy, które o tobie wiedzą, aby cię zastraszyć i sprawić, że uwierzysz, że zhakowali twoją maszynę i każą ci za to zapłacić. Pamiętaj, że ci źli mogą używać tych samych technik do oszukańczych rozmów telefonicznych.

Co robić? Uznawać takie e-maile i rozmowy telefoniczne za fałszywe. To naturalne, że boisz się, gdy ktoś ma twoje dane osobowe. Ale pamiętaj, nadawca kłamie! Atak jest częścią zautomatyzowanej, masowej kampanii, a nie próbą ataku na ciebie. W dzisiejszych czasach przestępcom coraz łatwiej jest znaleźć

lub kupić dane osobowe, więc przygotuj się na bardziej spersonalizowane ataki w przyszłości.

Oznaki rozpoznania ataku:

- Zawsze bądź podejrzliwy, gdy otrzymujesz bardzo pilną wiadomość e-mail, wiadomość lub telefon. Kiedy ktoś wykorzystuje emocje takie jak strach lub pilność, stara się sprawić, że się spieszysz.
- Każdy, kto żąda płatności w kryptokrypcie *BitCoin*, kartach podarunkowych lub innych nietransakcyjnych instrumentach płatniczych.
- Jeśli otrzymasz podejrzaną wiadomość e-mail, zrób wyszukiwanie w Google, aby sprawdzić, czy ktoś nie zgłosił podobnego ataku.

Zawsze staraj się używać długich, unikalnych haseł do każdego z kont online. Nie możesz zapamiętać wszystkich haseł? Skorzystaj z menedżera haseł. Dodatkowo, używaj 2-stopniowego uwierzytelniania, gdy tylko jest to możliwe.

1.4. Odciski cyfrowe

Cyfrowy ślad to informacja, którą świadomie lub nieświadomie pozostawiamy w środowisku wirtualnym - informacja wizualna, dźwiękowa i pisemna. Istnieją również informacje, które nie są generowane przez samych siebie, ale tworzone przez rodziców, przyjaciół, pracę, itp. Brak śladu cyfrowego może być dzisiaj niemożliwy, ale zbyt duża aktywność w serwisach społecznościowych może mieć również negatywne konsekwencje.

Cyfrowy ślad jest oparty na Twojej aktywności w Internecie: nawyki zakupowe, media, korzystanie z urządzeń, platformy, które wybierzesz.

2. Podstawowe zasady bezpiecznego stosowania technologii

2.1. Połączenie internetowe

Aby uniemożliwić innym osobom korzystanie z cudzych danych uwierzytelniających, takich jak nazwa użytkownika i hasło, **musisz się upewnić, że przeglądasz bezpiecznie!**

Podczas przeglądania, przeglądarka internetowa przechowuje na dysku twardym użytkownika informacje o odwiedzanych stronach internetowych, które można podzielić na trzy rodzaje:

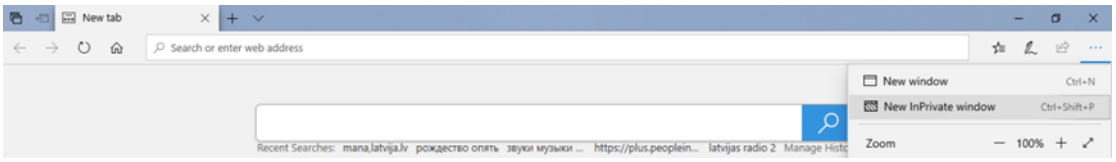
a) Lista odwiedzanych stron lub Historia odwiedzanych stron.
b) Informacje zawarte na stronach internetowych, które zwykle przechowywane są w tzw. *Cachememory*. Cachememory. Jest to zazwyczaj folder o nazwie *Temporary Internet Files*.
c) Cookies - małe pliki tekstowe. Pliki te rejestrują, hasła, listę odwiedzonych stron i daty ich przeglądania. Przeglądarki internetowe przekazują te informacje z powrotem na serwery internetowe. Zazwyczaj po otwarciu strony internetowej w przeglądarce, użytkownik ma możliwość zaakceptowania/odrzucenia plików cookie. Zalecane jest, abyś zaakceptował użycie plików cookie na stronach internetowych, do których planujesz wrócić ponownie.

Korzystając z publicznego komputera, należy mieć świadomość, że inne osoby będą mogły przeglądać historię przeglądania stron, które klient odwiedził, jak również pobrane pliki. Zaleca się wyczyszczenie historii przeglądarki **Ctrl + H** oraz plików cookie, aby uniknąć nieprzyjemnych sytuacji. W wielu przeglądarkach można to zrobić naciskając **Ctrl + Shift + Delete** na klawiaturze.

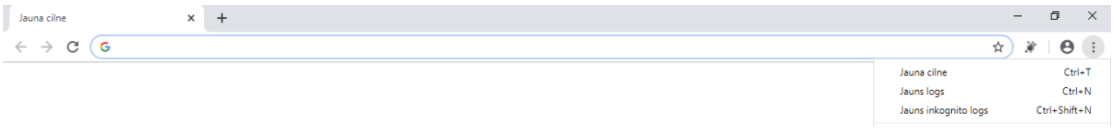
Jeśli nie chcesz, aby Twoja przeglądarka rejestrowała historię aktywności oraz nazwy użytkowników i hasła, zalecamy korzystanie z prywatnego przeglądania. Prywatne przeglądanie może mieć inną nazwę w każdej przeglądarce, ale jego

istota jest taka sama we wszystkich przeglądarkach. Poniższe ilustracje przedstawiają kilka przykładów, jak otworzyć okno prywatnego przeglądania.

Microsoft Edge



Google Chrome



Pamiętaj, aby chronić swoją tożsamość, hasła i kody bezpieczeństwa. Dane te mogą być wykorzystane przez osoby nieupoważnione.

Podczas korzystania z Internetu zalecane są następujące podstawowe wskazówki:

- Nie udostępniaj innym osobom dowodu osobistego, kodów PIN i innych danych dostępowych;
- Nie należy publikować w Internecie i przesyłać kopii dokumentów (paszport, dowód osobisty, prawo jazdy) za pośrednictwem poczty elektronicznej, aplikacji komunikacyjnych lub portali społecznościowych;
- Nie należy przekazywać haseł i innych prywatnych informacji w wiadomościach e-mail lub wiadomościach z aplikacji komunikacyjnych (WhatsApp, Viber, Messenger, itp.) i sieci społecznościowych (Facebook, Twitter, itp.);
- Nie należy otwierać załączników podczas otrzymywania podejrzanych wiadomości e-mail;

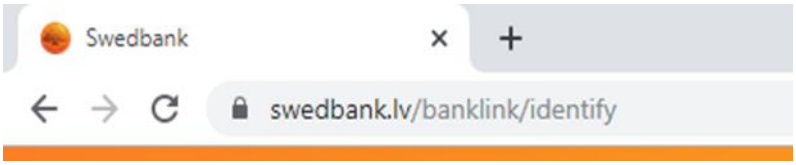
- Nie opowiadaj innym zbyt wiele o swoim życiu w Internecie i na portalach społecznościowych, zwłaszcza o swojej sytuacji finansowej, nowych rzeczach, wychodzeniu z domu, itp;
- Zastanów się dokładnie, jakie zdjęcia umieścić w Internecie i jak ich publikacja może pewnego dnia wpłynąć na życie danej osoby, np. relacje z przyjaciółmi, krewnymi, współpracownikami, obecnymi lub przyszłymi pracodawcami;
- Otrzymując e-mail od władz publicznych lub banku z prośbą o przesłanie danych osobowych do władz, nigdy nie należy tego robić, ponieważ władze nigdy nie poproszą o te dane w formie e-maila;
- Łącząc się z e-usługami, upewnij się, że inne osoby nie widzą wprowadzonych przez Ciebie danych dostępu oraz informacji uzyskanych w wyniku korzystania z e-usługi;
- Upewnij się, że masz zainstalowany program antywirusowy na swoim komputerze podłączonym do Internetu;
- Wyłączyć komputer na noc, aby nie tylko oszczędzać energię elektryczną, ale także zmniejszyć ryzyko nielegalnego włamania i użycia komputera.

2.2. Bezpieczne połączenie - strony internetowe z certyfikatami bezpieczeństwa

Bezpieczeństwo oznacza ochronę danych przechowywanych w sieciach komputerowych i systemach komputerowych przed uszkodzeniem, utratą lub nieautoryzowanym dostępem. W dzisiejszych czasach szybka dostępność sieci komputerowych, a w szczególności Internetu, wymaga coraz większej uwagi na ten problem. Głównym problemem bezpieczeństwa w sieciach komputerowych jest ich ochrona przed nieautoryzowanym użyciem, np. przy dokonywaniu płatności elektronicznych, istnieje możliwość kradzieży i niewłaściwego wykorzystania danych.

Szyfrowanie służy do zabezpieczenia danych lub treści wiadomości przed nieuprawnionym użyciem. Szyfrowanie to proces przetwarzania danych i wiadomości przez nadawcę lub inicjatora wiadomości. Aby można było wykorzystać takie dane lub treść wiadomości, muszą one zostać odszyfrowane. Klucz szyfrowania jest używany do szyfrowania i odszyfrowywania danych.

Strony internetowe, które wymieniają zaszyfrowane wiadomości, nazywane są **bezpiecznymi stronami internetowymi**.



Bezpieczne połączenie jest zazwyczaj reprezentowane przez ikonę

Ryzyko związane z działalnością w Internecie:

- nieumyślnego ujawnienia danych osobowych. Aby móc korzystać z usług oferowanych na stronach internetowych, często konieczne jest podanie swoich danych osobowych, takich jak nazwisko, data urodzenia, adres. Przed podaniem tych informacji należy upewnić się, że strona jest wiarygodna i bezpieczna;
- nękanie lub zastraszanie poprzez rozsiewanie złośliwych plotek lub wysyłanie wiadomości z pogróżkami;
- potencjalnej przemocy. Korzystając z serwisów społecznościowych, takich jak Facebook.com i nawiązując nowe kontakty, można napotkać potencjalnego sprawcę przemocy, znęcanie się, itp. Dlatego też należy zastanowić się, jakie informacje o sobie przekazać, i krytycznie ocenić złożone oferty.

W przypadku oszustwa, nękania i upokorzenia emocjonalnego należy poinformować organy ścigania, takie jak policja.

Bezpieczeństwo dzieci w Internecie

Następujące środki są zalecane w celu ochrony dzieci przed negatywnymi skutkami korzystania z Internetu:

- Umieść komputer w pomieszczeniu, w którym można monitorować aktywność dziecka w sieci;
- Tworzenie kont użytkowników dziecięcych z ograniczonymi prawami użytkownika komputera;
- Ograniczenie przeglądania poprzez włączenie filtrów, które zabraniają dostępu do stron internetowych zawierających treści dla dzieci (narkotyki, pornografia, mowa nienawiści, broń, itp.);
- Ograniczyć korzystanie ze szkodliwych gier poprzez zakazanie gier na określone tematy;
- Ograniczyć korzystanie z komputera, ustawiając harmonogram korzystania z niego;
- Na przykład: **Konta użytkowników i bezpieczeństwo rodziny**.

2.3. Wi-fi

Jeśli Twój komputer, tablet lub smartfon obsługuje WiFi (bezprzewodowy Internet), możesz korzystać z Internetu bez konieczności podłączania dodatkowego kabla do urządzenia.

WiFi może być używane zarówno w domu, jak i poza nim. Jeśli chcesz korzystać z WiFi poza domem, często widzisz różne sieci WiFi na swoich urządzeniach, ale nie wszystkie będą miały dostęp, ponieważ sieć może być chroniona hasłem.

W wielu miejscach, na przykład w kawiarniach, sklepach, parkach masz możliwość korzystania z bezpłatnego publicznego WiFi. Najlepszym sposobem na bezpieczne korzystanie z publicznych połączeń WiFi w miejscach publicznych jest znalezienie hasła i skorzystanie z bezpłatnego połączenia za pomocą szyfrowanego dostępu. Publiczne WiFi jest nadal jednym z najczęściej

stosowanych sposobów nielegalnego połączenia się z urządzeniem przenośnym i uzyskania dostępu do danych osobowych.

2.4. Załączniki poczty elektronicznej, dołączone linki i komunikaty spamu

Spam lub poczta śmieciowa nazywana jest spamem i śmieciami. Spamerzy mogą łatwo i niedrogo wysyłać e-maile do tysięcy osób jednocześnie. Takie listy są anonimowe.

Jak walczyć ze spamem:

a) **Użyj blokady antyspamowej.** Bloker spamu może znacznie zmniejszyć ilość przychodzącego spamu. Większość dostawców poczty elektronicznej, takich jak Google Gmail, posiada automatyczną blokadę antyspamową. W razie potrzeby można również użyć dodatkowych programów blokujących spam. Jednak również w tym przypadku istnieje prawdopodobieństwo ich otrzymania.

b) **Nie odpowiadaj na spam.** Jeśli otrzymasz ciekawą wiadomość spam, możesz ulec pokusie odpowiedzi na nią lub kliknąć na link, aby zrezygnować z otrzymywania kolejnych wiadomości e-mail. Odpowiadając na spam lub klikając na link, nieświadomie oświadczasz, że ten adres e-mail działa, a nowy spam zostanie wysłany na ten adres w przyszłości.

c) **Dezaktywacja obrazów.** E-mail może zawierać obrazy, które mogą być śledzone przez spamera. Kiedy otwierasz spam i pozwalasz na pobranie na niego obrazów, sygnalizujesz, że jesteś gotowy na otrzymanie nowego spamu.

d) **Dezaktywuj panel wyświetlania komunikatów**. Po kliknięciu litery jest ona automatycznie wyświetlana w oknie prezentacji. Wyświetlanie spamu może spowodować otrzymywanie kolejnych wiadomości.

e) **Regularnie sprawdzaj folder spamu**. Czasami blokery spamu blokują nie tylko spam, ale także legalne wiadomości e-mail. Dlatego należy

sprawdzać folder spamu tak często, jak to możliwe, aby uniknąć przegapienia ważnej wiadomości. Sprawdź w ustawieniach swojego klienta poczty elektronicznej, które wiadomości będą dozwolone, a które blokowane.

☑	Tworzenie wielu adresów e-mail w celu wykorzystania ich do różnych celów.
☑	Nie ujawniaj swojego prywatnego adresu e-mail w sieciach publicznych.
☑	Nie należy tworzyć krótkich adresów e-mail. Wielu spamerów wysyła e-maile na losowo wybrane adresy e-mail. Im krótszy jest ten adres, tym łatwiej go odkryć.
☑	Jeśli chcesz umieścić ogłoszenie w Internecie, stwórz w tym celu nowy adres e-mail.
☑	Jeśli musisz ujawnić swój adres e-mail, zrób to w mniej zrozumiałej formie, np. firstname.lastname@mail.com pisząc jako pierwsze imię, nazwisko, nazwisko i adres e-mail-dot-com.
☑	Nie używaj swojego prywatnego adresu e-mail przy zapisywaniu się do sieci publicznych.
☑	Nie ryzykuj korzystania z opcji "wypisz się", ponieważ często będzie to tylko zachęcać do wysyłania większej ilości spamu.
☑	Zmień swój prywatny adres e-mail, jeśli został on odkryty i ma dużo spamu.

2.5. Bezpieczne hasła

Hasła, które wybierzesz, są najważniejszą i podstawową osłoną dla ochrony Twoich kont. Użyj prostego, ale bezpiecznego sposobu tworzenia i przechowywania wszystkich swoich haseł.

Kroki w celu uproszczenia haseł:

1. *Wyrażenia dotyczące hasła*

Najważniejszą cechą haseł jest to, że muszą one być wystarczająco długie, im więcej znaków jest w haśle, tym lepiej. Są to tzw. frazy hasłowe, rodzaj bezpiecznego hasła, które używa krótkich zdań lub swobodnych słów:

- *Czas na mocną czarną kawę!*
- *zaginiony ślimak-czołgacz*

Oba hasła są bezpieczne, mają ponad 20 znaków, a oba są łatwe do zapamiętania, proste do napisania, ale trudne do złamania. Napotkasz strony internetowe lub sytuacje, które wymagają użycia symboli, cyfr lub dużych liter dla hasła. Ale pamiętaj, że kluczem do hasła jest długość!

2. *Menedżerowie haseł*

Potrzebujesz niepowtarzalnego hasła do każdego z Twoich kont. Jeśli używasz tego samego hasła dla wielu kont, narażasz się na duże ryzyko. Wszystkie potrzeby cyberprzestępcy to włamanie się na używaną przez Ciebie stronę internetową, kradzież wszystkich haseł, w tym Twojego, a następnie użycie Twojego hasła do zalogowania się na wszystkie inne konta. Zdarza się to częściej, niż możesz to sobie wyobrazić. Na stronie www.haveibeenpwned.com można sprawdzić, ile stron internetowych, z których korzystasz, zostało zhakowanych, a Twoje hasła mogły zostać naruszone. W takich przypadkach, jednym z rozwiązań jest użycie menedżera haseł. Menedżer **haseł jest specjalnym programem komputerowym, który przechowuje wszystkie Twoje hasła w bezpieczny, zaszyfrowany sposób. Wystarczy** zapamiętać tylko jedno hasło - dla swojego menedżera haseł.

Następnie program Password Manager automatycznie pobiera Twoje hasła do odpowiednich witryn, gdy są one potrzebne i uwierzytelnia Cię. Posiada on również inne funkcje, takie jak możliwość zapisywania odpowiedzi na pytania dotyczące bezpieczeństwa, ostrzegania o ponownym użyciu hasła, funkcję

generatora haseł, która pozwoli Ci na tworzenie i używanie bezpiecznych haseł i wiele innych. Większość menedżerów haseł synchronizuje się również bezpiecznie na różnych urządzeniach, dzięki czemu masz łatwy i bezpieczny dostęp do swoich haseł, niezależnie od tego, z jakiego systemu korzystasz.

Zapisz hasło managera haseł na papierze i przechowuj je w bezpiecznym miejscu w domu. Niektóre menedżery haseł pozwalają nawet na wydrukowanie narzędzia do odzyskiwania menedżera haseł. W ten sposób, jeśli zapomnisz swojego hasła do menedżera haseł, masz plan awaryjny. Ponadto, w nagłych wypadkach, w razie potrzeby, Twoi zaufani ludzie będą mogli uzyskać informacje w Twoim imieniu.

3. *Uwierzytelnianie dwuczynnikowe*

Dwustopniowa weryfikacja (często nazywana uwierzytelnianiem dwuczynnikowym lub wieloczynnikowym) zapewnia dodatkową warstwę bezpieczeństwa. Wymaga ona dwóch rzeczy podczas logowania się na konta, hasła i kodu numerycznego, który zostałby wygenerowany na Twoim smartfonie lub wysłany na Twój telefon. Proces ten gwarantuje, że nawet jeśli cyberprzestępcy uzyskają Twoje hasła, nie będą mogli uzyskać dostępu do Twoich kont. Dwustopniowe uwierzytelnianie jest łatwe do skonfigurowania i zazwyczaj wystarczy użyć go tylko raz podczas autoryzacji z nowego urządzenia. W przypadku korzystania z menedżera haseł zalecane jest zabezpieczenie go zarówno za pomocą bezpiecznego hasła, jak i uwierzytelniania dwuczynnikowego.

Uproszczone **dwuetapowe uwierzytelnianie** oznacza, że oprócz wprowadzenia czegoś, co znasz (hasła), potwierdzasz to czymś, co posiadasz (np. kodem z telefonu komórkowego). Istnieje również trzystopniowa autoryzacja, w której musisz potwierdzić dostęp za pomocą czegoś, co jest dla Ciebie właściwe - np. za pomocą odcisku palca. Zaletą 2-stopniowej autoryzacji jest to, że haker

potrzebuje również dostępu do Twojego urządzenia mobilnego, aby włamać się na Twoje konto.

3. Użycie haseł

3.1. Hasła: Pierwszy krok w kierunku bezpieczeństwa

Istnieją dwa rodzaje haseł: bezpieczne i niepewne. Większość ludzi używa niepewnych haseł - hasła, które są krótkie, łatwe do zapamiętania, zawierają dane osobowe (takie jak imię, nazwisko, rok urodzenia, ważna data, imię i nazwisko zwierzęcia, nazwisko rodowe) lub nawet to samo hasło jest używane dla wielu kont.

Hakerzy często używają oprogramowania do wyszukiwania haseł, które sprawdza wiele haseł, aż do znalezienia właściwego. Niepewne hasła mogą zostać wykryte bardzo szybko. Tworzenie bezpiecznych haseł zmniejsza prawdopodobieństwo, że przestępcy ujawnią Twoje hasło i ukradną Twoje dane osobowe i finansowe.

W celu ochrony danych osobowych, istnieją podstawowe zasady bezpieczeństwa, których należy przestrzegać podczas używania hasła:

- Podczas wprowadzania hasła, uważaj, aby nie pozwolić innym osobom zobaczyć, jak twoje palce poruszają się na klawiaturze lub ekranie twojego smartfonu;
- Zmieniaj swoje hasło co 3 miesiące;
- Należy uważać, aby nie zapisać automatycznego dostępu do konta. Zawsze używaj przycisków Exit, Logout lub End job;
- Unikaj używania haseł na stronach internetowych z wolnym dostępem.

3.2. Zasady tworzenia bezpiecznego hasła

Tworząc konto użytkownika w serwisach społecznościowych, korzystając z banku internetowego lub innego portalu samoobsługowego, należy zarejestrować się za pomocą nazwy użytkownika, hasła i innych danych.

Oświadczenie	**Objaśnienie**
Nigdy nie używaj danych osobowych	Nie używaj imion, urodzin i nazwisk jako hasła. Dane osobowe są często dostępne publicznie, więc możesz bardzo szybko odgadnąć hasło.
Używaj dłuższych haseł	Hasło musi mieć długość co najmniej sześciu znaków. Aby hasło było bezpieczniejsze, możesz użyć 12 lub więcej znaków do wprowadzenia hasła.
Unikaj zapisywania haseł w notatniku lub telefonie.	Jeśli nadal chcesz spisać swoje hasło, przechowuj je w bezpiecznym miejscu i nie pokazuj go nikomu. Zaleca się szyfrowanie haseł, a nie zapisywanie samego hasła.
Używaj losowo wybranych haseł	Losowe hasła są najbardziej bezpieczne. Zamiast myśleć o własnych hasłach, możesz użyć generatorów haseł. Losowe hasła są trudniejsze do zapamiętania, ponieważ są one tworzone przez urządzenia.
Nie używaj tych samych haseł dla wielu kont.	Jeśli ktoś ujawni hasło do jednego konta, hasła do innych kont również będą zagrożone.
Nie używaj słów, które można znaleźć w środowisku	Na przykład, hasło *nauczyciel1* będzie niepewnym hasłem.
Uwzględniać w hasłach cyfry, symbole i małe litery.	Aby utworzyć bezpieczne hasło, można zastąpić litery różnymi symbolami, na

Oświadczenie	Objaśnienie
	przykład na podstawie słowa *poniedziałek* i zastąpić litery "o" i "a", można utworzyć następujące bezpieczne hasło *M0nd@y!*

3.3. Studium przypadku i ćwiczenia praktyczne

Pan Berzins, człowiek w swoich najlepszych latach, w końcu zdecydował się na rozpoczęcie korzystania z usług elektronicznych i jest gotowy do zapisania się na stronę internetową Dyrekcji Bezpieczeństwa Ruchu Drogowego (CSDD), aby w przyszłości mógł zdalnie dowiedzieć się o sobie i swoim samochodzie.

Aby utworzyć lub aktywować swoje konto na SBDPW, przy pierwszym logowaniu na stronie musisz zarejestrować się za pomocą swojego adresu e-mail, stworzyć własne hasło i wprowadzić je. Po utworzeniu konta po raz pierwszy, dostęp do Twojego konta na SBDPW będzie kontynuowany zarówno z ustalonym dostępem, jak i z dostępem do bankowości internetowej.

Zadaniem sytuacji jest, aby Pan Berzins wymyślił hasło do nowo utworzonego konta CSDD w swoim salonie przy swoim komputerze, tak aby nikt nie mógł go odgadnąć.

Wspólna scena - pan Berzins siedzi w salonie swojego wiejskiego domu za otwartym laptopem. W tle znajduje się sofa, na której śpi leniwy kot perski o imieniu Rudis. Pani Berzins siedzi na drugim końcu kanapy i robi na drutach kapelusz. Pan Berzins ma czarnego psa o imieniu Poga leżącego u jego stóp. Gdzieś w tle trzeszczy ciepły kominek, nad którym wisi trofeum myśliwskie Berzinsów, głowa łosia z rogami. Na jednej ze ścian salonu znajduje się półka na książki, na której można zobaczyć rozpoznawalne dzieła różnych pisarzy. Na okładkach niektórych książek można zobaczyć ich portrety, na przykład Szekspira, Dostojewskiego, Czechowa itd. Na drugiej ścianie znajduje się zdjęcie

rodziny Berzinsów, gdzie można zobaczyć ich dorosłe dzieci i wnuki. Na drugiej ścianie znajduje się zdjęcie rodziny Berzinsów, na którym można zobaczyć ich dorosłe dzieci i wnuki. Nieco dalej jest bluszcz zwisający z półki i kaktus rosnący na parapecie.

1) Każdy z istotnych obiektów (elementów) klucza w domu rodziny Berzins może być oglądany jako możliwa zła lub **dobra** wersja hasła:

- Cat Rudis: *Rudis*! Rudis! **RuD! $**
- Hobby żony: Dziewiarstwo. /Kn*tt*ng
- Wewnętrzna roślina Cactus: kaktus / **sutcac**
- Trofeum łowieckie: Trofeum / **Tr0fhy**
- Psia Poga: Poga / **50g** @
- Wnuk12: Wnuk12 / **Gr@nds0n**
- Żona Rosalie: Rosalie / **R0s@lie**
- Czechow: Czechow / **Ch3kh0v**
- Dostojewski: Dostojewski / **D0$t0j3v$ky**

Podsumowanie

Moduł ten zawierał trzy ważne tematy związane z ochroną danych osobowych i prywatności. Takie jak podstawy bezpieczeństwa Twojego komputera i podstawowe zasady ochrony danych. Aby uniknąć phishingu, uczniowie zostali zapoznani ze sposobami, w jaki cyberprzestępcy działają w celu kradzieży informacji. Biorąc pod uwagę, że jednym z najważniejszych problemów ochrony danych osobowych obecnie jest umieszczanie i udostępnianie zbyt osobistych informacji na różnych portalach społecznościowych, moduł ten dostarczył również wytyczne dotyczące bezpieczeństwa tego tematu.

W celu bezpiecznego korzystania z urządzeń cyfrowych poza domem, moduł ten podjął tematykę połączeń internetowych i podstawowych zasad bezpiecznego korzystania z Wi-Fi. Wyjaśniono również oznaki niepewnej poczty elektronicznej i spamu oraz podano wskazówki, jak prawidłowo i bezpiecznie korzystać z haseł.

W końcowej części modułu omówiono przykłady tworzenia haseł i opisano sytuację - w jaki sposób tworzone są hasła, na jakie hasła należy zwracać uwagę, a których należy unikać?

Bibliografia

- *Drošība internetā.* (n.d.). Mana.latvija.lv. https://mana.latvija.lv/drosiba/
- *E-rīki jeb ceļvedis e-pakalpojumu lietošanā*. (n.d.). Mana.latvija.lv. https://mana.latvija.lv/e-riki/
- *Esiet sveicināti Mācību e-vidēbu!* (n.d.). [środowisko e-learningowe]. Macibas.mana.latvija.lv. https://macibas.mana.latvija.lv/
- Pieslēdzies, Latvija! (n.d.). *Esiet sveicināti datorskolā! Mācies pats*. [Kurs online]. Tet.lv. https://www.tet.lv/piesledzies-latvija/materiali/start/
- SEB. (n.d.). SEB *privātpersonām*. Seb.lv. https://www.seb.lv/private
- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. (n.d.). Esidross.lv. https://www.esidross.lv/
- Valsts reģionālās attīstības aģentūra. (n.d.). *Valsts pārvaldes pakalpojumu portāls.* Latvija.lv. https://www.latvija.lv/
- *Mana Latvija.lv. Dari digitāli!* (n.d.). Mana.latvija.lv. https://mana.latvija.lv/
- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. (n.d.). Cert.lv. https://www.cert.lv/lv
- Uzdevumi.lv. Uzdevumi.lv. (n.d.). Uzdevumi.lv. https://www.uzdevumi.lv/(nd.).
- Latvijas Drošāka interneta centra. (n.d.). Drossinternets.lv. www.Drossinternets.lv
- Draudzīgs internets. (n.d.). *Interneta Drosības ABC*. Draudzigsinternets.lv. www.draudzigsinternets.lv