Projekt IDCAP: Poprawa kompetencji cyfrowych u osób dorosłych

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

Jak chronić moje urządzenie?

Obszar kompetencji: Urządzenia zabezpieczające

Wprowadzenie

Moduł ten obejmuje najważniejsze tematy warte uwagi podczas codziennej pracy z urządzeniami cyfrowymi: Twój smartfon, tablet, laptop i komputer stacjonarny.

Celem modułu jest:

- wyjaśnienie metod ochrony urządzeń przed fizycznym dostępem innych osób - kody PIN, wprowadzanie hasła, pobieranie odcisków palców, rozpoznawanie twarzy;
- nauczyć jak chronić urządzenia cyfrowe przed dostępem innych użytkowników na odległość - instalacja i wykorzystanie programów i aplikacji antywirusowych. Bezpieczne pobieranie aplikacji i dokumentów na urządzenie;
- w celu wyjaśnienia korzyści płynących z tworzenia kopii zapasowych informacji o urządzeniu cyfrowym i zaoferowania możliwości tehnologicznych.

1. Fizyczne bezpieczeństwo urządzeń

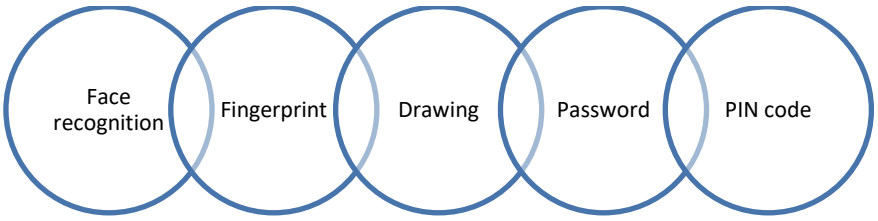
Wiele osób ma dziś komputer, telefon komórkowy i inne urządzenie, które chcą chronić przed krzywdą. Zagrożeniami są: ludzka aktywność fizyczna (lekkomyślność, nieostrożność, awaria, wadliwe działanie), złośliwe oprogramowanie (wirusy), hakerzy, zjawiska naturalne / katastrofy, awarie techniczne, itp. Jak każda ważna rzecz, chcemy, aby dane były bezpieczne. Istnieje wiele sposobów ochrony urządzenia: poprzez szyfrowanie urządzenia, użycie kodu PIN, użycie blokady odcisków palców, rozpoznawanie twarzy, funkcja "znajdź moje urządzenie", blokowanie i usuwanie danych.

Czynniki, które mogą zwiększyć fizyczne bezpieczeństwo Twoich urządzeń:

- Hasła / PINy;
- specjalne urządzenia i oprogramowanie;
- bezpieczeństwo pomieszczeń;
- prawidłowe użytkowanie sprzętu (zgodnie z instrukcją obsługi);
- ochrona przed ogniem lub wilgocią.

W przypadku użycia haseł / PIN-ów i / lub specjalnego oprogramowania / odcisków palców, urządzenie nie może być użyte w przypadku kradzieży. Dostępne są programy do śledzenia skradzionego urządzenia.

Przykłady do odblokowania telefonu:



Ochrona informacji za pomocą zewnętrznego nośnika danych:

- Kopiowanie plików do/z zewnętrznego nośnika danych (takiego jak płyty CD, DVD lub pamięci USB) tylko w przypadku określonych zadań,
- Podczas podłączania zewnętrznego magazynu danych do komputera należy go przeskanować za pomocą programu antywirusowego,
- Należy zachować szczególną ostrożność przy korzystaniu z zewnętrznych nośników danych udostępnionych przez przyjaciół i znajomych,
- Nie należy niepotrzebnie przechowywać ważnych i wrażliwych informacji na urządzeniach.

2. Szyfrowanie

Szyfrowanie to proces szyfrowania informacji możliwych do odczytania, tak aby mogły być odczytane tylko przez osobę posiadającą tajny kod lub klucz szyfrujący. Jest to sposób na ukrycie/zablokowanie informacji do momentu wprowadzenia kodu i ponownego przekształcenia informacji w czytelny tekst. Wiele osób korzysta z szyfrowania danych w celu zapewnienia bezpieczeństwa danych wrażliwych.

Masz możliwość szyfrowania zarówno danych przechowywanych na Twoich urządzeniach, jak i wysyłanych danych. Istnieje kilka metod szyfrowania. Na przykład, FDE jest pełnym szyfrowaniem dysku używanym do szyfrowania całego dysku w systemie. Oznacza to, że wszystkie informacje, nie tylko niektóre, są ukryte.

Do ochrony przesyłanych danych stosuje się szyfrowanie HTTPS online. Oznacza to, że informacje są szyfrowane w drodze z przeglądarki do strony głównej. Wiadomości e-mail i inne programy do komunikacji również oferują metody szyfrowania, które należy ustawić samodzielnie. Kluczem do udanego szyfrowania jest zabezpieczenie klucza / hasła i uczynienie go bardzo skomplikowanym - tak długo, jak to możliwe i w inny sposób bezpiecznym. Możesz użyć menedżera haseł, aby zapamiętać hasła.

Szyfrowanie może działać, jeśli urządzenie jest bezpieczne. Podstawową kwestią jest upewnienie się, że urządzenie jest bezkompromisowe, wolne od wirusów lub nie jest narażone na szwank w żaden inny sposób. Regularnie upewnij się, że urządzenie nie jest dostępne dla osób niepożądanych. Pamiętaj, że jeśli aplikacja / program, którego chcesz używać nie oferuje szyfrowania, to rozważ inne opcje. Ważne jest, aby używać bezpiecznych aplikacji/programów, które nie stanowią zagrożenia dla Ciebie.

3. Kod PIN/rysunek

Kod PIN to specjalny mechanizm zabezpieczający, który jest stosowany do autoryzacji konta bankowego, urządzenia lub jakichkolwiek poufnych informacji. Kod PIN nie może być nikomu ujawniony. Zaleca się jego zmianę w taki sam sposób jak zmianę hasła. Musisz zapamiętać swój kod PIN. Aby chronić siebie, nie należy dokonywać płatności z publicznych komputerów ani z nieznanych urządzeń. Istnieją programy, które potrafią odczytać wszystko, co użytkownik wprowadza za pomocą klawiatury - również kody PIN. Dlatego należy używać kodu PIN tylko na swoich prywatnych urządzeniach. Dostępne są również **rysunkowe kody PIN**, więc należy być ostrożnym, ponieważ ludzie mają tendencję do tworzenia ich zbyt prostych, standardowych, a ekran urządzenia musi być regularnie czyszczony, aby zapobiec śledzeniu go przez linie przeciągania. Podczas wprowadzania pinezki lub rysunku zaleca się przykrycie jednej ręki drugą podczas pisania i upewnienie się, że ekran urządzenia nie jest zbyt jasny i dobrze widoczny pod innymi kątami.

4. Odcisk palca

Czujnik odcisków palców jest dostępny dla kilku urządzeń. Jest to urządzenie biometryczne, które pomaga szybko zidentyfikować daną osobę. Można go

ustawić na prawie wszystkich urządzeniach inteligentnych, które mają wbudowany czujnik linii papilarnych. Pobieranie odcisków palców może być mniej bezpieczne niż skomplikowany kod PIN, kombinacja lub hasło. Istnieje kilka sposobów na fizyczne usunięcie odcisku palca z urządzenia. Należy pamiętać, że zdejmowanie odcisków palców może być również wykonywane z innych codziennych rzeczy. Jeśli Twoje urządzenie nie jest bezpieczne, Twój odcisk palca może być odczytany jako dowolna informacja z Twojego urządzenia.

Dwuczynnikowy proces autoryzacji jest używany dla typu autoryzacji odcisków palców. Oznacza to, że zwykle używany jest również kod PIN. Jeśli urządzenia nie potrafią rozpoznać/odczytać odcisku palca, wówczas używany jest kod PIN. Ponadto, po aktualizacji lub włączeniu zasilania, kod PIN jest wykorzystywany do celów bezpieczeństwa.

Jeśli zdecydujesz się na użycie odcisku palca jako metody odblokowania urządzenia, przejdź do ustawień urządzenia i wykonaj odpowiednie kroki. Pierwsza konfiguracja jest bardzo ważna - Twoje palce są skanowane. Wskazane jest, aby utrzymać telefon w naturalnej pozycji i upewnić się, że wykonujesz wszystkie wymagane od Ciebie kroki.

Mogą wystąpić problemy z jego użytkowaniem, jeżeli czujnik jest uszkodzony, zabrudzony lub nie została przeprowadzona wymagana aktualizacja urządzenia. Niektóre firmy wolą wymienić swój odcisk palca na narzędzie do rozpoznawania twarzy.

5. Rozpoznawanie twarzy

Rozpoznawanie twarzy to rodzaj uwierzytelniania, które wymaga użycia kamery. Jest to opcja odblokowania urządzenia lub połączenia z określonymi aplikacjami poprzez pokazanie twarzy w aparacie. Eksperci pracujący od wielu lat nad sztuczną inteligencją uznają, że rozpoznawanie twarzy jest jednym z najbezpieczniejszych sposobów łączenia się z systemem.

Aby skonfigurować rozpoznawanie twarzy, potrzebne jest odpowiednie urządzenie, aparat i konfiguracja twarzy - aby urządzenie mogło ją rozpoznać, należy zeskanować twarz ze wszystkich stron.

W większości przypadków tani system rozpoznawania twarzy w telefonie wykorzystuje tylko aparat skierowany do przodu i niektóre niezbyt zaawansowane algorytmy - a może nawet lampę błyskową, aby zrobić lepsze zdjęcie. Jednak konwencjonalny aparat 2D bez czujnika podczerwieni i projektora punktowego można łatwo oszukać, wyświetlając zdjęcie.

W przypadku wybrania rozpoznawania twarzy jako mechanizmu zabezpieczającego, zaleca się stosowanie urządzenia wysokiej jakości. Upewnij się, że to działa. Eksperci wciąż pracują nad udoskonaleniem tego systemu. Uznają oni, że rozpoznawanie twarzy będzie w przyszłości stosowane w celu uzyskiwania dostępu do określonych stron internetowych, artykułów sklepowych i innych działań.

6. Znalezienie twojego telefonu

Programy są przeznaczone do lokalizacji i zarządzania telefonem w dowolnym momencie. Funkcja ta jest używana w przypadku zgubienia lub kradzieży telefonu. Możesz zlokalizować, usunąć dane, sprawdzić poziom naładowania baterii i połączyć się z siecią Wi-Fi. Należy jednak pamiętać, że funkcje mogą się różnić w zależności od systemu operacyjnego. Istnieją zarówno wbudowane programy, które pomagają śledzić aktywność telefonu, jak i takie, które można oddzielnie pobrać i zakupić.

Aby skorzystać z tej funkcji, należy ją włączyć (na urządzeniu) i zbadać możliwości urządzenia. Skorzystaj z wyszukiwarki internetowej, aby dowiedzieć się wszystkiego o swoim urządzeniu lub skonsultuj się z osobą, która może Ci w tym pomóc.

Google również jest usługą, która pozwala na zdalne blokowanie, dzwonienie, wylogowywanie i wiele więcej. Twoje urządzenie można znaleźć przez Internet. Praktyka pokazuje, że funkcja ta jest używana głównie do blokowania urządzenia

i wylogowania się z niektórych profili, ale nie zawsze jest możliwe fizyczne znalezienie urządzenia. Istnieje kilka programów, które pobierają opłaty za tę funkcję. Program firmy Apple nazywa się "Find My iPhone", program firmy Microsoft to "My Windows Phone", a Google oferuje "Find My Device". To tylko kilka z wielu programów.

7. Bezpieczne korzystanie z aplikacji mobilnych

Ważne jest, aby aplikacje mobilne pochodziły z bezpiecznego i niezawodnego źródła. Przestępcy nauczyli się tworzyć i rozpowszechniać zainfekowane aplikacje mobilne, które wyglądają jak prawdziwe. Jeśli zainstalujesz taką zainfekowaną aplikację, przestępcy mogą przejąć kontrolę nad urządzeniem.

W przypadku urządzeń Apple, z Apple App Store można pobrać tylko aplikacje na iPada i iPhone'a. W tym sklepie firma Apple przeprowadziła badania bezpieczeństwa wszystkich aplikacji mobilnych przed ich udostępnieniem. Apple nie może "złapać" wszystkich zainfekowanych aplikacji, ale takie zarządzane środowisko znacznie zmniejsza ryzyko infekcji. Jeśli Apple znajdzie zainfekowaną aplikację w swoim sklepie, zostanie ona natychmiast usunięta ze sklepu. Windows Phone stosuje podobne podejście do zarządzania aplikacjami.

Android daje Ci wybór, aby pobrać aplikację z dowolnego miejsca w Internecie. Musisz być bardziej ostrożny z aplikacjami, które instalujesz, ponieważ nie wszystkie z nich są testowane. Google prowadzi sklep z aplikacjami - Google Play i jego aplikacje mają co najmniej podstawową kontrolę bezpieczeństwa. Zaleca się korzystanie z aplikacji tylko z Google Play. Unikaj aplikacji z innych stron internetowych, ponieważ stosunkowo łatwo jest dystrybuować złośliwe aplikacje, które zainfekowały Twoje urządzenie mobilne. Dla większej ochrony zainstaluj oprogramowanie antywirusowe na swoim urządzeniu mobilnym.

Zezwolenia. Po zainstalowaniu aplikacji z zaufanego źródła, skonfiguruj ją zgodnie z Twoimi preferencjami i potrzebami w zakresie prywatności. Zawsze zastanawiaj się przed udzieleniem pozwolenia na aplikację - czy chcesz udzielić jej pozwolenia i czy naprawdę go potrzebujesz. Jeśli poinformujesz aplikację, aby zawsze znała Twoją lokalizację, możesz umożliwić jej twórcy śledzenie Twojego ruchu, a nawet sprzedać te informacje innym.

Aktualizacje. Aplikacje mobilne muszą być regularnie aktualizowane. Przestępcy zawsze szukają słabych punktów w aplikacjach. Większość urządzeń pozwala na automatyczne aktualizowanie aplikacji. Jeśli nie jest to możliwe, sprawdzaj aktualizacje aplikacji co najmniej raz na dwa tygodnie. Wreszcie, gdy aplikacja jest aktualizowana, zawsze sprawdzaj, jakie zmiany są wprowadzane w uprawnieniach aplikacji.

8. Zablokować i wytrzeć

Blokowanie urządzenia jest bardzo prostym sposobem na zabezpieczenie się przed uszkodzeniem lub ujawnieniem informacji. Ponadto, fizycznie łącząc urządzenie z biurkiem, miejsce pracy ma tendencję do zniechęcania złodziei do uzyskania urządzenia. Tylko specjalny klucz może go odblokować.

Istnieją różne sposoby, które mogą chronić nasze urządzenie nie tylko fizycznie. Użytkownik nie może opuścić swojego miejsca pracy z niezabezpieczoną stacją roboczą: na czas tymczasowej nieobecności - zablokować **komputer; (Windows + L), dłużej - wylogować się lub wyłączyć**. W przypadku telefonów i tabletów można ustawić automatyczne blokowanie urządzenia po upływie określonej liczby sekund. Większość urządzeń posiada pojedynczy, łatwo dostępny przycisk wyłączania, który ułatwia ten proces.

Niewyłączenie urządzenia może spowodować, że inne osoby będą zakłócać pracę urządzenia. Kiedy skończysz pracę, bezpieczniej jest całkowicie wyłączyć urządzenie. Utrata połączenia internetowego uniemożliwia dostęp do urządzenia przez hakerów. Utrzymywanie włączonego urządzenia zawsze zwiększa ryzyko.

Wytarcie to działanie polegające na uczynieniu informacji z dysku twardego nieczytelnymi. Oznacza to, że dane są tak samo usunięte, ale możliwe jest ich odzyskanie przy pomocy odpowiedniego programu. Podczas wymiany urządzenia, dysku twardego, wskazane jest, aby oczyścić go w jak największym stopniu. Najbezpieczniejszym sposobem jest jednak fizyczne zniszczenie dysku twardego, aby upewnić się, że pliki nie zostaną przywrócone.

9. Wirusy i antywirusy

Cyberprzestępczość zyskuje kontrolę poprzez instalację złośliwego oprogramowania na komputerach lub urządzeniach. Dzięki temu przestępca może monitorować Twoją aktywność w Internecie, kraść hasła lub pliki, a także używać Twojego systemu do atakowania innych.

Złośliwe oprogramowanie to w zasadzie oprogramowanie komputerowe używane do celów niezgodnych z prawem. Termin ten pochodzi z połączenia słów "oprogramowanie" i "złośliwe". Cyberprzestępcy instalują złośliwe oprogramowanie na komputerach lub urządzeniach, aby uzyskać nad nimi kontrolę. Po zainstalowaniu, złośliwe oprogramowanie pozwala przestępcy na monitorowanie Twojej aktywności w Internecie, kradzież haseł lub plików, a także na wykorzystywanie Twojego systemu do atakowania innych. Złośliwe oprogramowanie może zainfekować każde urządzenie, od komputerów Apple po kamery bezpieczeństwa.

Wirusy szyfrujące są szczególnym rodzajem złośliwego oprogramowania, które obecnie aktywnie rozpowszechnia się w Internecie, stanowiąc zagrożenie dla dokumentów ofiar i innych plików.

Chroń się. - Zatrzymaj malware!

Niestety, programy antywirusowe nie są w stanie zatrzymać całego złośliwego oprogramowania. Cyberprzestępcy stale rozwijają nowe i wyrafinowane oprogramowanie, które może omijać programy antywirusowe. Oczywiście, twórcy programów antywirusowych również stale ulepszają swoje rozwiązania.

Cyberprzestępcy wykorzystują luki w twoim oprogramowaniu. Im nowszą / aktualną wersję oprogramowania posiadasz, tym mniej luk w nim jest luk. Dlatego jest ona zalecana:

- Aktualizuj na bieżąco swoje systemy operacyjne, aplikacje, przeglądarki, rozszerzenia i inne aplikacje. Najprostszym rozwiązaniem jest zazwyczaj zainstalowanie automatycznych aktualizacji.

Powszechnym sposobem, w jaki cyberprzestępcy zarażają komputery i urządzenia mobilne, jest tworzenie fałszywego oprogramowania lub aplikacji mobilnych, udostępnianie ich w Internecie oraz oszukiwanie osób, które dobrowolnie je instalują.

- Pobieraj i instaluj programy tylko z zaufanych sklepów internetowych, badaj opinie o programach i unikaj tych, które są mało używane lub mają tylko kilka pozytywnych opinii.
- Usuń aplikację, której już nie potrzebujesz.
- Cyberprzestępcy często manipulują ludźmi w celu stworzenia własnego złośliwego oprogramowania, na przykład, mogą wysłać Ci e-mail, który zawiera załącznik lub link w tekście i może wyglądać, jakby pochodził od znajomego lub Twojego banku. Niestety, po kliknięciu na link lub pobraniu załącznika, złośliwe oprogramowanie jest instalowane w Twoim systemie.
- Regularnie wykonuj kopie zapasowe systemów i plików, zarówno w chmurze, jak i w trybie offline, np. na zewnętrznym dysku twardym.

10. Programy licencjonowane i nielicencjonowane

Jeśli program ma swoją cenę, musi być zakupiony i legalnie pobrany. Należy również zwrócić uwagę na to, gdzie pobierane są programy. Nie należy tego robić na podejrzanych stronach internetowych - może to stanowić zagrożenie dla

urządzenia i innego oprogramowania na komputerze. Użytkownicy komputerów muszą wziąć pod uwagę przepisy dotyczące praw autorskich odnoszące się do książek, płyt i kaset wideo i muzycznych oraz oprogramowania. Kopiowanie, dystrybucja lub używanie programów komputerowych bez zgody właściciela praw autorskich jest nazywane piractwem.

Nielegalne korzystanie z programów komputerowych jest, na przykład, nielegalne:

- Instalacja jednej legalnie zakupionej płyty CD z oprogramowaniem na wielu komputerach, jeśli licencja lub umowa przewiduje, że może ona być zainstalowana tylko na jednym komputerze;
- Skopiuj program do instalacji i dystrybucji bez zgody autora;
- Instalacja oprogramowania z nielegalnie zakupionego dysku.
- Pobieranie nielegalnych kopii programów komputerowych z Internetu.

Oprogramowanie i inne rodzaje plików (teksty, obrazy, itp.) są oferowane do bezpłatnego pobrania przez Internet. Ich wydawcy nie zawsze mają prawo do rozpowszechniania ich w celu wykorzystania przez innych. Dlatego też przed pobraniem należy upewnić się, że jest się prawnie upoważnionym do wykonywania kopii.

11. Pliki do pobrania

Pobieranie to proces przechowywania plików z serwera sieciowego na urządzeniu pamięci masowej. Pobieranie plików jest wymagane, jeśli użytkownik chce uzyskać pliki oferowane na stronie, takie jak dokumenty, zdjęcia, muzyka, filmy i oprogramowanie.

Aby zapisać plik lub obraz na komputerze lub urządzeniu, pobierz go. Plik zostanie zapisany w domyślnej lokalizacji pobierania.

Można pobierać różne typy plików:

Typ	Format	Przykład
Tekst	Docx, txt	Kopsavilkums.docx
Zdjęcie	Jpg. Gif, png.	IMG0034.jpg
Audio	Mp3, wma	Voice.mp3
Wideo	Avi, mpg, mpeg	Ceplis.avi
Programy	Exe	Skype.exe
Archiwum	Zip, rar	Arhivs.zip

Opcję pobierania plików można określić na różne sposoby, ale zazwyczaj charakteryzuje się ona linkiem lub przyciskiem Pobierz (Download).

12. Przeglądarki internetowe

Przeglądarka jest aplikacją do przeglądania stron internetowych. Aby wyświetlić stronę internetową, jest ona najpierw pobierana lub przesyłana z globalnego serwera WWW do komputera użytkownika przed jej otwarciem.

Aby móc korzystać z usług internetowych, musisz:

- Programowalne urządzenie z możliwością podłączenia do sieci;
- Dostawca usług internetowych (ISP), który zapewnia, że urządzenie może być podłączone do Internetu (może być wymagany dodatkowy sprzęt);
- Przeglądarka internetowa.

Niektóre przykłady przeglądarek zawierają:

Otwieranie jakiejkolwiek strony nie jest bezpieczne, ponieważ istnieje ryzyko, że strona zawiera wirusy, które mogą również otwierać oszukańcze strony, które fałszują informacje.

Istnieją znaki, dzięki którym można założyć, że strona internetowa jest bezpieczna. Dwie najprostsze funkcje, które wskazują na bezpieczeństwo strony, są wyświetlane na pasku adresu:

- **https** przed adresem (oznacza, że informacja jest przesyłana do komputera w postaci zaszyfrowanej);
- Normalnie zablokowany symbol "blokady" (symbol blokady może się różnić w różnych przeglądarkach internetowych).

Pobieranie strony zatrzymuje się, jeśli:

- Pobieranie jest opóźnione;
- wykryje podczas pobierania, brakujące informacje wymagane dla strony.

Strona wymaga odświeżenia, jeśli:

- Strona nie załadowała się. Na przykład, niektóre obrazy mają kwadraty z czerwonymi krzyżykami na stronie lub nie wszystkie informacje są dostępne;
- Strona nie była oglądana przez użytkownika od pewnego czasu, a informacje na niej zawarte zmieniły się w tym czasie (strona nie aktualizuje się automatycznie).

13. Kopie danych

Ważne jest, aby przechowywać dane nie tylko na komputerze, ale także w innym miejscu. W tym przypadku zawsze istnieje możliwość odtworzenia ważnych danych w przypadku jakichkolwiek problemów z komputerem.

Dane zazwyczaj przechowywane na komputerze:

- Zdjęcia;
- Dokumenty robocze;

- ważne programy, oprogramowanie;
- projekty wideo, audio;
- archiwum e-mailowe i e-maile przyjaciół.

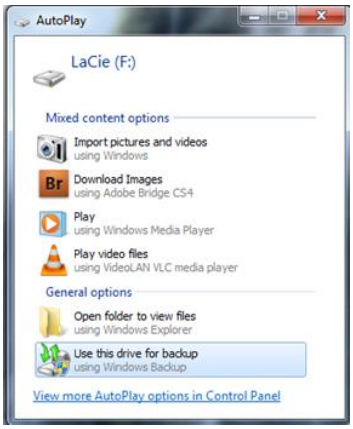
Jeśli uważasz, że nie potrzebujesz kopii danych, pamiętaj, że istnieje wiele sposobów na utratę ważnych dokumentów.

- Najprostszym sposobem na utratę wszystkich danych jest utrata komputera lub jego kradzież (dotyczy to w większym stopniu laptopów).
- Istnieje możliwość przypadkowego usunięcia danych lub skopiowania czegoś innego w ważnych dokumentach.
- Komputer może być zainfekowany, a złośliwe oprogramowanie może uszkodzić niektóre dane lub nawet uszkodzić dysk twardy.
- Mogą wystąpić pewne problemy techniczne (w tym uszkodzenie dysku twardego - nic nie jest trwałe), które mogą spowodować utratę niektórych danych.

Robienie kopii danych.

Do komputera z systemem Windows:

- **Zakup zewnętrznego urządzenia magazynującego**. Może to być dowolny dysk USB flash lub zewnętrzny dysk twardy. Pożądane jest zakupienie urządzenia, które ma co najmniej dwa razy więcej miejsca niż pamięć komputera.
- Przy pierwszym podłączeniu zewnętrznego urządzenia pamięci masowej do komputera, oferuje ono możliwość wykorzystania go jako miejsca do przechowywania danych. Jeśli ta opcja się nie pojawi, wystarczy wpisać nazwę programu w oknie wyszukiwania "Kopia zapasowa".



- Otworzy się następujące okno, w którym należy kliknąć na "Ustawianie kopii zapasowej". Następnie należy wybrać, na który dysk zewnętrzny chcesz utworzyć kopię zapasową swoich danych. Na koniec należy kliknąć na "Save Settings and Run Backup".
- Po wykonaniu tych czynności Windows wykona pierwszą kopię zapasową danych (kluczem jest nie usuwanie zewnętrznego dysku twardego!). Możesz wybrać poniżej "Zmień harmonogram" i pojawi się następujący obrazek. Rysunek pokazuje, że użytkownik ma możliwość wyboru harmonogramu, kiedy kopie danych zostaną przywrócone. Można to zrobić raz dziennie, raz w tygodniu i raz w miesiącu. Należy przede wszystkim pamiętać, że urządzenie, z którego tworzona jest kopia zapasowa, musi być podłączone do komputera o wybranej godzinie i dniu.

Wykonywanie kopii danych na komputerze Mac OS.

Jest to bardzo podobne do tego, co z komputerem z systemem Windows. Po włożeniu zewnętrznego dysku twardego będziesz mógł używać go jako miejsca do tworzenia kopii zapasowych. Musisz go wybrać lub przejść przez Preferencje systemowe -> Time Machine. Następnie wybierz wymagany zewnętrzny dysk twardy i zrób kopię danych na nim.

Robienie kopii danych na telefonie komórkowym.

Bardzo wygodnym sposobem tworzenia kopii zapasowych kontaktów i kalendarza jest korzystanie z konta Google (Gmail e-mail). Dzięki ustawieniom Konto i synchronizacja możesz w każdej chwili włączyć funkcję tworzenia kopii

zapasowych. Konto Google powinno być wyświetlane obok Twoich kont, jeśli uzyskałeś do niego dostęp z telefonu. Zaletą korzystania z takiego kopiowania kontaktów jest to, że po zmianie telefonu dane zostaną automatycznie skopiowane na nowe urządzenie. W Internecie informacje o swoich kontaktach można wyświetlać po lewej stronie, klikając przycisk Gmail. Oprócz możliwości, jakie oferuje Google, istnieją również inne rodzaje oprogramowania, które oferują opcje tworzenia kopii zapasowych. Jedną z nich jest po prostu skopiowanie ważnych danych poprzez podłączenie telefonu do komputera. W Internecie można również znaleźć pojedyncze programy, które umożliwiają tworzenie kopii zapasowych. Jeśli szukasz takiego programu, który jest odpowiedni dla Ciebie, ważne jest, aby upewnić się, że jest on odpowiedni dla systemu operacyjnego Twojego komputera.

Wykonywanie kopii danych w Internecie.

Usługa ta jest zazwyczaj dostępna za darmo z ograniczeniami pamięci (około 5-7GB). Korzystanie z tej usługi pozwala na przechowywanie najważniejszych danych w Internecie, co oznacza dostęp do nich z dowolnego miejsca i z komputera. Usługodawca zapewnia, że dane te są przechowywane w formie zaszyfrowanej. Przykładami takich usługodawców są www.mimedia.com i www.backup.comodo.com. Oczywiście ten rodzaj przechowywania danych jest wygodny pod względem dostępu, ale nie są wykluczone różne kwestie bezpieczeństwa.

Jeśli nastąpi utrata danych, można je łatwo przywrócić z kopii zapasowej. W systemie Windows, wpisz "Backup" w menu startowym wyszukiwania, a następnie kliknij "Restore My Files". Na komputerach Mac wcisnąć "Time Machine", a następnie "Enter Time Machine". Albo po prostu zabierz ze sobą zewnętrzne urządzenie pamięci masowej, na którym utworzyłeś kopię zapasową danych, podłącz je do komputera i skopiuj potrzebne pliki.

Korzyści z wykonywania kopii danych.

- **Korzyść moralna** - nie musisz się martwić, że nic się nie stanie z Twoim komputerem; możesz być pewny, że Twoje ważne dane nigdzie nie zostaną utracone!
- **Korzyść finansowa** - Jeśli masz problemy z dyskiem twardym, korzystanie z usług profesjonalisty w celu przywrócenia tych danych może być dość kosztowne. Jeśli masz kopię zapasową swoich ważnych danych, nie będziesz potrzebował takich usług.

14. Urządzenie zakorzenione

Korzeniowanie to proces, który pozwala użytkownikom smartfonów, tabletów i innych urządzeń z systemem operacyjnym Android uzyskać uprzywilejowaną kontrolę (tzw. dostęp root) nad różnymi podsystemami Android. Celem tego procesu jest przezwyciężenie ograniczeń nakładanych przez producentów na niektóre urządzenia. Tak więc, rootowanie pozwala zmieniać lub zastępować aplikacje systemowe i ustawienia, uruchamiać wyspecjalizowane aplikacje, które wymagają uprawnień na poziomie administratora, lub wykonywać inne działania, które nie są dostępne dla innego zwykłego użytkownika Androida. Na systemie Android, kibicowanie może również ułatwić całkowite usunięcie i zastąpienie systemu operacyjnego urządzenia, zazwyczaj z nowszą wersją jego obecnego systemu operacyjnego.

Podsumowanie

Uczniowie poznając tematy poruszane w module, wiedzą jak zapewnić fizyczne bezpieczeństwo urządzeń, a także rozumieją zasady szyfrowania. Uczniowie potrafią rozpoznawać i stosować techniki ochrony urządzeń cyfrowych - rozpoznawanie twarzy, wprowadzanie hasła, rysowanie sylwetki na ekranie urządzenia cyfrowego oraz pobieranie odcisków palców.

Dzięki zastosowaniu opisanych w module technik, możliwe jest zlokalizowanie zgubionego telefonu. Uczniowie są informowani o różnych rodzajach wirusów zagrażających urządzeniom i możliwościach ich uniknięcia. W celu zachowania bezpieczeństwa urządzeń, użytkownicy powinni również zwracać uwagę na pobieranie i korzystanie wyłącznie z legalnych i licencjonowanych programów. Po uzyskaniu tych informacji uczeń może opanować zasady korzystania z programów i aplikacji antywirusowych, określić różnice pomiędzy przeglądarkami internetowymi a ich użytkowaniem.

Wreszcie, uczniowie są świadomi tego, jak tworzyć kopie zapasowe informacji na swoich urządzeniach cyfrowych, a także rozumieją przeznaczenie urządzeń zakorzenionych.

Bibliografia

- Pieslēdzies, Latvija! (n.d.). *Esiet sveicināti datorskolā! Mācies pats*. [Kurs online]. Tet.lv. https://www.tet.lv/piesledzies-latvija/materiali/start/
- Swedbank. (n.d.). *Swedbank privātpersonām*. Swedbank.lv. https://www.swedbank.lv/private
- 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/
- *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/
- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. (n.d.). Cert.lv. https://www.cert.lv/lv
- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. (n.d.). Esidross.lv. https://www.esidross.lv/
- Uzdevumi.lv. Uzdevumi.lv. (n.d.). Uzdevumi.lv. https://www.uzdevumi.lv/ (nd.).
- Baltijas Biroju Tehnoloģijas. (n.d.). *Astoņas digitālās prasmes, kas jāmāca bērniem*. Smartboard.lv. https://smartboard.lv/zinas/astonas-digitalas-prasmes-kas-jamaca-berniem/
- Brečko, B., Ferrari, A. (2016) *Patērētāju digitālo kompetenču sistēma.* https://publications.jrc.ec.europa.eu/repository/bitstream/JRC103155/lfna28133lvn.pdf