Проект IDCAP: Подобряване на цифровите компетенции на възрастни

Проект номер: 2018-1-PL01-KA204-051003

Как да защитя устройството си?

Област на компетентност: Защита на устройства

Съдържание

Въведение

Този модул обхваща най-важните теми, които си заслужават вниманието при ежедневна работа с цифрови устройства: вашия смартфон, таблет, лаптоп и настолен компютър.

Целите на модула са:

- да се обяснят методи за защита на устройствата от физически достъп до други - ПИН кодове, въвеждане на парола, пръстови отпечатъци, разпознаване на лица;
- да научи как да предпазвате цифровите устройства от дистанционен достъп от други потребители - инсталиране и използване на антивирусни програми и приложения. Безопасно изтегляне на приложения и документи на устройство;
- да обясни ползите от архивирането на информацията на цифрови устройства и да предложи технически възможности.

1. Физическа сигурност на устройствата

Много хора днес имат компютър, мобилен телефон и някои други устройства, които искат да предпазят от вреда. Заплахите са: физическа активност на човека (безразсъдство, невнимание, неуспех, неизправност), зловреден софтуер (вируси), хакери, природни явления / катастрофи, технически неизправности и др. Както всяко важно нещо, ние искаме да запазим данните в безопасност. Има много начини да защитите вашето устройство: чрез криптиране на вашето устройство, използване на ПИН код, използване на ключалки за пръстови отпечатъци, разпознаване на лица, функцията „намери моето устройство“, заключване и изтриване на вашите данни.

Фактори, които могат да увеличат физическата сигурност на вашите устройства:

- пароли / ПИН;
- специални устройства и софтуер;
- охрана на помещенията;
- правилно използване на оборудването (в съответствие с ръководствата с инструкции);
- защита срещу пожар или влага.

Когато използвате пароли / ПИН и / или специален софтуер / пръстови отпечатъци, устройството не може да се използва в случай на кражба. Също така, има програми за проследяване на откраднато устройство.

Примери да отключите телефона си:

Защита на информацията чрез използване на външно хранилище за данни:

- Копирайте само файлове към / от външно хранилище за данни (като CD, DVD или USB флаш устройства) за конкретни задачи,
- Когато свързвате външен източник за данни към вашия компютър, сканирайте го с антивирусна програма,
- Внимавайте изключително много, когато използвате външно устройство за съхранение на данни, предоставено от приятели и познати,
- Не съхранявайте ненужна важна и чувствителна информация на вашите устройства.

2. Шивроване

Шифроването е процес на криптиране на четлива информация, така че тя може да бъде прочетена само от някой, който има таен код или ключ за дешифриране. Това е начин за скриване / заключване на информацията, докато кодът не бъде въведен и информацията се преобразува обратно в четлив текст. Много хора използват криптиране на данни за сигурността на чувствителните данни.

Имате възможност да шифровате както данните, които съхранявате на своите устройства, така и данните, които изпращате. Има няколко метода за криптиране. Например FDE е шифроване на пълен диск, използвано за шифроване на целия диск във вашата система. Това означава, че цялата информация, а не само част от нея, е скрита.

HTTPS онлайн криптиране се използва за защита на данните, които се изпращат. Това означава, че информацията е криптирана по пътя от

браузъра към началната страница. Имейлите и други комуникационни програми също предлагат методи за криптиране, които трябва да зададете сами. Ключът към успешното криптиране е да запазите ключа / паролата си сигурни и да ги направите много сложни - възможно най-дълго и по друг начин защитени. Можете да използвате мениджъра на пароли, за да запомните пароли.

Шифроването може да работи, ако устройството ви е защитено. Основното съображение е да се уверите, че устройството е безкомпромисно, без вируси или не е компрометирано по друг начин. Редовно се уверявайте, че устройството няма достъп до нежелани лица. Не забравяйте, че ако приложението / програмата, която искате да използвате, не предлага криптиране, разгледайте други опции. Важно е да използвате защитени приложения / софтуер, които не ви застрашават.

3. ПИН код/рисунка

ПИН код е специален механизъм за сигурност, който се прилага за упълномощаване на вашата банкова сметка, устройство или друга чувствителна информация. ПИН кодът не трябва да се разкрива на никого. Препоръчително е да го промените по същия начин като промяната на паролата си. Трябва да запомните своя ПИН код. За да се предпазите, не плащайте от обществени компютри или от непознати устройства. Има програми, които могат да четат всичко, което потребителят въвежда с помощта на клавиатурата - включително ПИН кодове. Затова използвайте ПИН кода само на личните си устройства.

ПИН код с рисунка също са на разположение, така че бъдете внимателни, тъй като хората са склонни да ги създават твърде прости, стандартни, а екранът на устройството трябва да се почиства редовно, за да се

предотврати проследяването му с влачене на линии. Когато въвеждате щифт или чертеж, препоръчително е да покриете едната ръка с другата, докато пишете, и да се уверите, че екранът на устройството не е прекалено ярък и ясно се вижда от други ъгли.

4. Пръстов отпечатък

Сензор за пръстови отпечатъци се предлага за няколко устройства. Това е биометрично устройство, което помага бързо да се идентифицира човек. Може да се настрои на почти всички интелигентни устройства, които имат вграден сензор за пръстови отпечатъци. Отпечатъците могат да бъдат по-малко сигурни от сложен ПИН код, комбинация или парола. Има няколко начина за физическо премахване на пръстовия отпечатък от устройството. Имайте предвид, че премахването на пръстовия отпечатък може да се извърши и от други ежедневни неща. Ако устройството ви не е защитено, пръстовият ви отпечатък може да се чете като всякаква информация от вашето устройство.

За типа удостоверяване с пръстов отпечатък се използва двуфакторен процес на оторизация. Това означава, че обикновено се използва и ПИН кодът. Ако устройствата не могат да разпознаят / разчитат пръстовия отпечатък, тогава се използва ПИН кодът. Също така, след актуализации или включване, ПИН кодът се използва за целите на сигурността.

Ако решите да използвате пръстовия си отпечатък като метод за отключване на вашето устройство, отидете в настройките на устройството и следвайте съответните стъпки. Първата настройка е много важна - пръстите ви се сканират. Препоръчително е да поддържате телефона в естествено положение и да се уверите, че следвате всички стъпки, изисквани от вас.

Възможно е да има проблеми с използването му, ако сензорът е повреден, замърсен или не е извършена необходимата актуализация на устройството.

Няколко компании предпочитат да заменят пръстовия си отпечатък с инструмент за разпознаване на лица.

5. Лицево разпознаване

Разпознаването на лица е вид удостоверяване, за което е необходима камера. Възможно е да отключите устройството си или да се свържете с конкретни приложения, като покажете лицето си на камерата. Експерти, работещи върху изкуствен интелект от много години, вече признават, че разпознаването на лица е един от най-безопасните начини за свързване със системата.

За да настроите разпознаване на лица, се нуждаете от подходящо устройство, камера и настройка на лицето - ще трябва да сканирате лицето си от всички страни, за да бъде разпознато от вашето устройство.

В повечето случаи системата за разпознаване на лица на евтин телефон използва само насочена напред камера и някои не толкова сложни алгоритми - и може би дори светкавица, за да направи по-добра снимка. Обаче конвенционална 2D камера без инфрачервен сензор и точков проектор може лесно да бъде заблудена чрез показване на снимка.

Ако изберете разпознаване на лице като механизъм за безопасност, препоръчително е да използвате висококачествено устройство. Уверете се, че работи. Експертите все още работят по подобряването на тази система. Те признават, че разпознаването на лица ще се използва в бъдеще за достъп до конкретни уебсайтове, пазаруване на артикули и други дейности.

6. Как да намерите телефона си

Съществуват програми, които са предназначени да намират и управляват телефона ви по всяко време. Тази функция се използва, ако телефонът ви е загубен или откраднат. Можете да намерите, изтриете данни, да видите заряда на батерията и да се свържете с Wi-Fi мрежа. Имайте предвид, че функциите могат да варират в зависимост от операционната система. Има както вградени програми, които ви помагат да следите активността на телефона си, така и такива, които могат да бъдат изтеглени отделно и са достъпни за закупуване.

За да използвате тази функция, трябва да я включите (на вашето устройство) и да проучите възможностите на устройството. Използвайте търсенето в интернет, за да разберете всичко за вашето устройство или да се консултирате с човека, който може да ви помогне да го направите.

Google също е услуга, която ви позволява дистанционно да заключвате, да се обаждате, да излизате и др. Вашето устройство може да бъде намерено чрез Интернет. Практиката показва, че тази функция се използва главно за заключване на устройството и излизане от определени профили, но не винаги е възможно физически да се намери устройството. Има няколко програми, които таксуват тази функция. Програмата на Apple се нарича „Find My iPhone“, програмата на Microsoft е „My Windows Phone“, а Google предлага „Find My Device“. Това са само няколко от многото програми.

7. Безопасно използване на мобилни приложения

Важно е да получите мобилни приложения от сигурен и надежден източник. Престъпниците са се научили да създават и разпространяват заразени мобилни приложения, които приличат на истинските. Ако инсталирате такова заразено приложение, престъпниците могат да поемат контрола върху вашето устройство.

За устройства на Apple, изтегляте само приложения за iPad и iPhone от Apple App Store. В този магазин Apple е провел проверки за сигурност на всички мобилни приложения преди тяхното пускане. Apple не може да „хване“ всички заразени приложения, но такава управлявана среда драстично намалява риска от инфекция. Ако Apple намери заразено приложение в магазина си, то ще бъде незабавно премахнато от магазина. Windows Phone използва подобен подход за управление на приложения.

Android ви дава възможност да изтеглите приложението от всяка точка на интернет. Трябва да бъдете по-предпазливи по отношение на приложенията, които инсталирате, тъй като не всички те са тествани. Google поддържа магазин за приложения - Google Play и приложенията му имат поне основна проверка на сигурността. Препоръчително е да използвате приложения само от Google Play. Избягвайте приложения от други уебсайтове, тъй като е сравнително лесно да разпространявате злонамерени приложения, които заразяват вашето мобилно устройство. За повече защита инсталирайте антивирусен софтуер на вашето мобилно устройство.

Разрешения. След като инсталирате приложението от надежден източник, конфигурирайте го според вашите предпочитания и нужди за поверителност. Винаги обмисляйте, преди да дадете разрешение на приложение - искате ли да му дадете разрешение и наистина ли се нуждаете от приложението. Ако оставите приложението винаги да знае местоположението ви, можете да разрешите на разработчика на приложението да проследява движението ви или дори да продавате тази информация на други.

Актуализации. Мобилните приложения трябва да се актуализират редовно. Престъпниците винаги търсят уязвимости в приложенията. Повечето устройства ви позволяват да актуализирате приложенията автоматично. Ако това не е възможно, проверявайте за актуализации на приложения поне веднъж на две седмици. И накрая, когато дадено приложение се

актуализира, винаги преглеждайте какви промени се правят в разрешенията за приложението.

8. Заключване и изчистване

Заключването на вашето устройство е много лесен начин да се предпазите от повреда или разкриване на информация. Освен това, физически свързвайки устройството към бюрото, работното място има тенденция да обезкуражава крадците да получат устройството. Само специален ключ може да го отключи.

Има различни начини, които могат да защитят нашето устройство не само физически. Потребителят не трябва да напуска работното си място с незащитена работна станция: за временно отсъствие – **Заключете компютъра си; (Windows + L), задръжте бутона за изключване по-дълго – излезте или изключете**. За телефони и таблети можете да настроите устройството ви да се заключва автоматично след определен брой секунди. Повечето устройства имат един, лесен за достъп бутон за изключване, който улеснява процес.

Неизключването на вашето устройство може да причини други хора да пречат на вашето устройство. Когато приключите с работата си, е по-безопасно да изключите устройството напълно. Загубата на вашата интернет връзка предотвратява достъпа на устройството до хакери. Ако устройството е включено, винаги се увеличава рискът.

Изтриването е действието, което прави информацията за твърдия диск нечетлива. Това означава, че данните са като изтрити, но е възможно да ги възстановите с помощта на подходяща програма. Когато подменяте устройство, твърдия диск, препоръчително е да го почистите възможно най-много. Най-сигурният начин обаче е да унищожите физически твърдия си диск, за да сте сигурни, че вашите файлове не са възстановени.

9. Вируси и антивирусни програми

Киберпрестъпността получава контрол чрез инсталиране на злонамерен софтуер на компютри или устройства. Това позволява на престъпника да наблюдава вашата онлайн активност, да краде пароли или файлове и да използва вашата система, за да атакува други.

Зловреден софтуер (Malware) е основно компютърен софтуер, използван за незаконни цели. Терминът идва от комбинацията на думата „софтуер“ и „злонамерен“. Кибер престъпниците инсталират злонамерен софтуер на компютри или устройства, за да получат контрол над тях. Веднъж инсталиран, зловредният софтуер позволява на престъпника да наблюдава вашата онлайн активност, да краде пароли или файлове и да използва вашата система, за да атакува други. Зловредният софтуер може да зарази всяко устройство, от компютри на Apple до охранителни камери.

Криптиращите вируси са специален вид зловреден софтуер, който сега се разпространява активно в Интернет, заплашвайки документи и други файлове на жертвите.

Защитете се - спрете зловредния софтуер!

За съжаление антивирусните програми не могат да спрат целия зловреден софтуер. Киберпрестъпниците непрекъснато разработват нов и усъвършенстван софтуер, който може да избегне антивирусните програми. Разбира се, разработчиците на антивирусни програми непрекъснато подобряват и своите решения. Кибер престъпници използват уязвимости във вашия софтуер. Колкото по-нова / текуща версия на софтуера имате, толкова по-малко уязвимост има. Поради това се препоръчва:

- Поддържайте актуалните си операционни системи, приложения, браузъри, разширения и други приложения. Най-простото решение обикновено е инсталирането на автоматични актуализации.

Често срещаният начин, по който киберпрестъпниците заразяват компютри и мобилни устройства, е чрез разработването на фалшив софтуер или мобилни приложения, като ги прави достъпни в интернет и подвежда хората да ги инсталират доброволно.

- Изтегляйте и инсталирайте програми само от надеждни онлайн магазини и изучавайте рецензии на програми и избягвайте тези, които са малко използвани или имат само няколко положителни отзива.
- Изтрийте приложение, което вече не ви е необходимо.
- Киберпрестъпниците често манипулират хората, за да създадат свой собствен зловреден софтуер, например, те могат да ви изпратят имейл, който съдържа прикачен файл или връзка в текста и може да изглежда така, сякаш е дошъл от приятел или от вашата банка. За съжаление, когато щракнете върху връзка или изтеглите прикачен файл, на вашата система се инсталира зловреден софтуер.
- Редовно архивирайте системите и файловете си в облака или офлайн, например на външен твърд диск.

10.Лицензирани и не-лицензирани програми

Ако програмата има цена, тя трябва да бъде закупена и изтеглена законно. Също така трябва да обърнете внимание къде изтегляте програмите си. Не правете това на подозрителни уебсайтове - това може да застраши вашето устройство и друг софтуер на вашия компютър. Потребителите на компютри трябва да вземат предвид законите за авторското право, които се прилагат за книги, видео и музикални дискове и касети и софтуер. Копирането,

разпространението или използването на компютърни програми без разрешението на притежателя на авторските права се нарича пиратство.

Незаконното използване на компютърни програми е например:

- Инсталиране на един законно закупен компактдиск със софтуер на множество компютри, ако лицензът или споразумението гласи, че той може да бъде инсталиран само на един компютър;
- Копирайте програмата за инсталиране и разпространение без разрешението на автора;
- Инсталиране на софтуер от незаконно закупен диск.
- Изтегляне на незаконни копия на компютърни програми от Интернет.

Предлага се софтуер и други видове файлове (текстове, изображения и др.) да се изтеглят безплатно през Интернет. Издателите им не винаги имат правото да ги разпространяват за използване от други. Следователно трябва да се уверите, че имате законно право да правите копия, преди да изтеглите.

11. Изтегляния

Изтеглянето е процес на съхраняване на файлове от мрежов сървър на устройство за съхранение. Изтеглянето на файлове се изисква, ако потребителят иска да получи файлове, предлагани на уебсайта, като документи, снимки, музика, видео и софтуер.

За да запазите файл или изображение на вашия компютър или устройство, изтеглете го. Файлът ще бъде запазен на мястото за изтегляне по подразбиране.

Можете да изтеглите различни типове файлове:

Тип	Формат	Пример
Text	Docx, txt	Kopsavilkums.docx
Picture	Jpg. Gif, png.	IMG0034.jpg
Audio	Mp3, wma	Voice.mp3
Video	Avi, mpg, mpeg	Ceplis.avi
Programs	Exe	Skype.exe
Archive	Zip, rar	Arhivs.zip

Опцията за изтегляне на файл може да бъде посочена по различни начини, но обикновено се характеризира с връзка или бутон за изтегляне (Изтегляне).

12. Браузери

Браузърът е приложение за преглед на уеб страници. За да видите уеб страница, тя първо се изтегля или предава от глобалния уеб сървър на компютъра на потребителя, преди да бъде отворена.

За да използвате интернет услугите, имате нужда:

- Програмируемо устройство с възможност за мрежова връзка;
- Доставчик на интернет услуги (ISP), който гарантира, че устройството може да бъде свързано към Интернет (може да е необходим допълнителен хардуер);
- интернет браузър.

Някои примери за браузъри:

Не е безопасно да отваряте която и да е страница, защото има рискове страницата да съдържа вируси, които също могат да отварят измамни страници, които подвеждат информация.

Има признаци, по които можете да предположите, че дадена уеб страница е защитена. Двете най-прости функции, които показват сигурността на дадена страница, се показват в адресната лента:

- **https** преди адрес (показва, че информацията се предава на компютъра в криптирана форма);
- Нормално заключеният символ "заключване" (символът за заключване може да варира в различните интернет браузъри).

Изтеглянето на страница спира, ако:

- Изтеглянето се забавя;
- открие по време на изтеглянето, информацията, необходима за страницата, липсва.

Страницата трябва да се обнови, ако:

- Страницата не можа да се зареди. Например, някои изображения имат квадратчета с червени кръстове на страницата или не е налична цялата информация;
- Страницата не е била преглеждана от потребителя от известно време и информацията на страницата се е променила през това време (страницата не се актуализира автоматично).

13. Копия на данни

Важно е да съхранявате данни не само на компютър, но и на друго място. В този случай винаги е възможно да възстановите важни данни в случай на проблеми с компютъра.

Данните обикновено се съхраняват на компютър:

- снимки;
- работни документи;
- важни програми, софтуер;
- видео, аудио проекти;
- имейл архив и имейли на приятели.

Ако смятате, че не се нуждаете от копия на данни, не забравяйте, че има много начини да загубите важни документи.

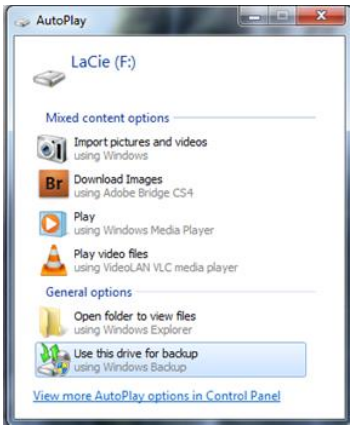
- Най-простият начин да загубите всичките си данни е да загубите компютъра си или ако той бъде откраднат (това важи повече за лаптопите).
- Има възможност случайно да изтриете данни или да копирате нещо друго във важни документи.
- Компютърът ви може да бъде заразен и зловредният софтуер може да повреди определени данни или дори да повреди твърдия ви диск.
- Възможно е да има някои технически проблеми (включително счупване на твърдия диск - нищо не е вечно), които могат да доведат до загуба на някои данни.

Как да направим копия на данни.

На компютър с Windows:

- **Закупете външно устройство за съхранение**. Това може да бъде всяко USB флаш устройство или външен твърд диск. Желателно е да закупите устройство, което има поне два пъти повече място от паметта на вашия компютър.

- Първият път, когато свържете външно устройство за съхранение към вашия компютър, то ви предлага опцията да го използвате като място за съхранение на данни. Ако тази опция не се появи, просто напишете името на програмата в прозореца за търсене "Архивиране".



- Ще се отвори следният прозорец, където ще трябва да кликнете върху „Настройване на архивиране“. След това ще трябва да изберете на кой външен диск искате да архивирате данните си. В крайна сметка ще трябва да кликнете върху „Запазване на настройките и стартиране на архивиране“.
- След като изпълните тези стъпки, Windows ще направи първото резервно копие на вашите данни (ключът е да не премахвате външния диск за съхранение!). Можете да изберете „Промяна на графика“ по-долу и ще се появи следното изображение. Фигурата показва, че имате възможност да изберете график, когато копията на данните ще бъдат възстановени. Предлага ви се възможност да правите това веднъж на ден, седмично и месечно. Основното нещо, което трябва да запомните, е, че устройството, на което архивирате, трябва да бъде свързано към компютър в избрания час и ден.

Компютър с Mac операционна система.

Това е почти същото като при компютър с Windows. Когато поставите външен диск за съхранение, ще можете да го използвате като място за архивиране. Трябва да го изберете или да преминете през Системни

предпочитания -> Машина на времето. След това изберете необходимия външен диск за съхранение и направете копие на данните върху него.

Копиране на данни от мобилен телефон.

Много удобен начин за архивиране на вашите контакти и календар е с вашия акаунт в Google (имейл в Gmail). С настройката за акаунт и синхронизация можете да включите функцията за архивиране по всяко време. Ако имате достъп до него от телефона си, трябва да се появи акаунт в Google. Предимството на използването на такова копиране на контакти е, че когато смените телефона, данните автоматично ще бъдат копирани в новото устройство. В интернет можете да видите информация за вашите контакти вляво, като кликнете върху Gmail. Освен възможностите, които предлага Google, има и други видове софтуер, които предлагат опции за архивиране. Единият вариант е просто да копирате важни данни, като свържете телефона си с компютър. Можете също така да намерите отделни програми в Интернет, които осигуряват резервни копия. Ако търсите подходящ за вас, важно е да се уверите, че е подходящ за операционната система на вашия компютър.

Копиране на данни в Интернет.

Безплатно тази услуга обикновено се предлага с ограничения на паметта (приблизително 5GB-7GB). Използването на тази услуга ви позволява да съхранявате най-важните си данни в Интернет, което означава, че можете да получите достъп до тях от всяко място и от вашия компютър. Доставчикът на услуги гарантира, че тези данни се съхраняват в криптирана форма. Примери за такива доставчици на услуги са www.mimedia.com и www.backup.comodo.com. Разбира се, този тип съхранение на данни е удобен по отношение на достъпа, но не са изключени различни проблеми със сигурността.

Ако има загуба на данни, е лесно да се възстанови от резервно копие. В Windows въведете "Архивиране" в търсенето в менюто "Старт" и след това

щракнете върху "Възстановяване на моите файлове". На компютри Mac, натиснете "Time Machine" и след това "Enter Time Machine". Или просто вземете външното си устройство за съхранение, където сте архивирали данните си, свържете го с компютъра си и копирайте необходимите файлове.

Предимства от правенето на копия на данни.

- **Морална полза** - не е нужно да се притеснявате, че нещо ще се случи с вашия компютър; можете да бъдете сигурни, че вашите важни данни няма да бъдат загубени никъде!
- **Финансова изгода** - Ако имате проблеми с вашия твърд диск, може да е доста скъпо да имате услуги на професионалист за възстановяване на тези данни. Ако имате резервно копие на вашите важни данни, няма да имате нужда от такива услуги.

14. Устройство с достъп до ниски нива на системата (Rooted device)

Достъпът до ниски нива е процес, който позволява на потребителите на смартфони, таблети и други устройства, работещи с мобилни операционни системи Android, да получат привилегирован контрол (известен като root достъп) в различни подсистеми на Android. Целта на този процес е да се преодолеят ограниченията, наложени от производителите на определени устройства. По този начин достъпът ви позволява да променяте или замествате системни приложения и настройки, да стартирате специализирани приложения, които изискват разрешения на ниво администратор, или да извършвате други действия, които не са достъпни за друг редовен потребител на Android. В Android достъпът до ниски нива

може също така да улесни напълно премахването и подмяната на операционната система на вашето устройство, обикновено с по-нова версия на текущата операционна система.

Заключение

Чрез изучаването на темите, разгледани в модула, обучаемите знаят как да осигурят физическа сигурност на устройствата и разбират принципите на криптиране. Обучаемите могат да разпознават и използват техники за защита на цифровите устройства - разпознаване на лица, въвеждане на парола, рисуване на фигури на екрана на цифрово устройство и отпечатъци.

Използвайки описаните техники в модула, е възможно да намерите изгубения телефон. Обучаемите се информират за различни видове вируси, застрашаващи устройствата и възможностите да ги избегнат. За да поддържат сигурността на устройствата, потребителите трябва също да обръщат внимание на изтеглянията и да използват само законни и лицензирани програми. След предоставена информация обучаемите могат да овладеят принципите на използване на антивирусни програми и приложения, да разберат разликата между уеб браузърите и тяхното използване.

И накрая, учащите са наясно как да архивират информацията на своето цифрово устройство и също така разбират предназначението на вкорененото устройство.

Библиография

- Pieslēdzies, Latvija! (n.d.). *Esiet sveicināti datorskolā! Mācies pats*. [Online Course]. 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-vidē!* (n.d.). [e-learning environment]. 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. (n.d.). Uzdevumi.lv. https://www.uzdevumi.lv/
- 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