Проект IDCAP: Подобряване на цифровите компетенции на възрастни

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

Как да защитя личните си данни?

Област на компетентност: Защита на личните данни и поверителността

Съдържание

Въведение

Модулът обхваща ключови теми в областта на личните данни и защитата на поверителността. Целите на модула са:

- да обсъдят принципите за сигурност в цифрова среда и да информират за потенциални заплахи - кражба на информация, фалшиви имейли и други;
- да представим основните принципи за сигурност при използването на технологията - какви правила трябва да се спазват при използване на интернет в публично достъпни Wi-Fi мрежи, какво е сигурна връзка и какви са несигурни прикачени файлове към имейл?
- да се обясни използването на безопасни пароли - кои са принципите, които трябва да следвате при създаването на пароли? Как да използваме безопасно паролите в ежедневието?

1. Въведение в сигурността в цифрова среда

1.1. Компютърна сигурност

Компютърната сигурност означава, че нашият компютър е защитен срещу неоторизиран достъп, използване, разкриване, намеса, изменение или унищожаване. Възможно е и е необходимо да се погрижите за собствената си информация и компютърна сигурност. Информацията, съхранявана на компютър и публикувана в Интернет, може да повлияе на личното благосъстояние, здравето и дори живота. Има много заплахи - заплахи за поверителността, пробиване или хакване на пароли, разкриване на лична информация, вируси, качване, изтегляне и изпращане на злонамерени файлове и злонамерени хора, които искат вреда.

В интернет, имаме достъп до социални мрежи, онлайн чатове, форуми, специални програми за чат (като Skype), игри и др. Ако необходимите стандарти за сигурност не са изпълнени, хората с лоши намерения могат не само да научат за личните ви данни, но и да използват вашата самоличност (да се представят за вас).

Компютърните вируси са се превърнали в „класическа стойност“. Използват се различни методи, например потребителят получава имейл с връзка към популярен уебсайт като Youtube или Facebook с примамлив филм или изображение. Опитът да го гледате заразява беззащитния компютър на потребителя само с едно кликване на мишката.

Прикачени файлове в имейли са особено опасни, защото могат да съдържат вируси и друг злонамерен софтуер. Отварянето на прикачен файл в имейл може автоматично да инсталира злонамерен софтуер на вашия компютър и дори няма да го забележите. Такъв злонамерен

софтуер може да повлияе на компютърни файлове, да открадне пароли или да ви шпионира, така че трябва да сте особено внимателни, когато получавате съобщения с прикачени файлове от неизвестни получатели.

Съвети за справяне с нежелани прикачени файлове към имейл:

Съвет	**Обяснение**
Никога не отваряйте подозрителни прикачени файлове към имейл	Дори ако получите имейл от някой, когото познавате, няма гаранция, че лицето действително го е изпратило. Злонамереният софтуер може автоматично да ви изпраща съобщения, които съдържат вируси. Когато получавате имейл с прикачен файл, най-добре е да помолите самия подател да се увери, че е изпратил имейл.
Актуализирайте антивирусната програма	Ако антивирусната програма не се актуализира, тя не може да защити компютъра ви от вируси.
Оставете защитната стена (*firewall)* включена	Компютърната защитна стена помага да се предотврати достъпът на хора или злонамерен софтуер до компютъра ви през интернет.

Съвет	Обяснение
Ако е възможно, преди да изтеглите прикачени файлове към имейл, проверете за вируси	Много онлайн доставчици на електронна поща автоматично проверяват прикачените файлове, преди да ги изтеглят. Ако компютърът ви подкани да проверите за вируси, като изтеглите прикачени файлове, направете това сами.

1.2. Защита на данните – фишинг(phishing)

Фишингът е вид киберпрестъпления, които съчетават набор от социално инженерство и технически инструменти за кражба на чувствителна, лична и финансова информация от жертва. Нападателят се опитва да се представи за истинска организация, доверен орган или познато лице.

Повечето жертви на фишинг се насърчават да кликват върху имейли със следните теми:

- ✓ Официално известие за изтичане на данни
- ✓ Известие за доставка на UPS 1ZBE312TYI00015011B23
- ✓ ИТ напомняне: Вашата парола ще изтече след по-малко от 24 часа
- ✓ Трябва незабавно да смените паролата си
- ✓ Моля, прочетете важното известие от вашия администратор

Как да разпознаем фишинга:

Прекалено е хубаво, за да е истина. Това са съобщения, писма, обаждания, които ви казват, че сте спечелили от лотарията или че сте били избрани произволно за получаване на награда или услуга.

Бърза оферта. Фрази: "последен шанс", "само 1 час", "само днес" и така нататък показва случай на фишинг. Измамниците използват манипулация, която създава усещане за спешност. При получаване на този тип съобщение е препоръчително да проверите истинността на информацията директно при компанията или доставчика на услуги.

Скрити връзки с други ключови думи. Много измамници използват прости ключови думи, фрази, които ще ви отведат до измамен сайт. Тези връзки често крият напълно различен сайт от това, което мислите. Много добър начин да се уверите, че това, което отваряте, е да кликнете НА ДЕСНИЯ бутон на мишката и да изберете опцията Inspect. Вижте каква връзка е свързана с тази връзка или ключова дума. Какво крие? Бъдете внимателни, защото неточностите в правописа често крият фалшиви връзки.

Странни прикачени файлове. Ако не очаквате конкретна информация, не трябва да разглеждате прикачени файлове към имейл. Един от методите на киберпрестъпността е да прикачите файл, който може да съдържа злонамерен софтуер, към невинно съобщение. Препоръчително е да проверите подателя, целта на съобщението, преди да го отворите. Единственият сигурен формат, който може да бъде отворен от .txt файл.

Как да избегнем фишинг:

Съвет	**Обяснение**
Бъдете нащрек	Винаги четете внимателно имейли от приятели и непознати
Внимавайте с различните комуникационни канали	Обърнете внимание на различни видове комуникация - имейли, реклами, телефонни обаждания и други видове комуникация, които изискват всякаква финансова информация.

Кликвайте внимателно	Избягвайте да кликвате върху „активиране на съдържанието“, което ви позволява да активирате допълнителни връзки между различни документи.
Не кликвайте на подозрителни връзки	Избягвайте да кликвате върху връзки в имейли, приложения за съобщения или реклами. Изследвайте връзките поотделно, като използвате всички налични ресурси.
Проверете надеждността на подателя	Уверете се, че имейлът е от надежден източник.

Ако сте жертва на фишинг:

1) Променете паролите за вашите приложения и онлайн акаунти с помощта на друг телефон или компютър.
2) Сканирайте компютъра си за вируси и проверете за злонамерен софтуер.
3) Съобщете за кражба на данни в полицията и запазете копие от заявлението.
4) Докладвайте пред вашата организация / банка или компетентния орган.

1.3. Безопасност на компютърните потребители - Информация, публикувана в социалните мрежи

Има два начина да разгледаме концепцията за компютърна сигурност на потребителите. Възможно е да се говори за потенциала на компютъра да застраши здравето на потребителя му, като например възможността от токов удар, дори и лек. Най-често срещаният риск за дадено лице обаче е рискът от самостоятелно публикувана информация.

Често липсва информираност колко различни заплахи представляват социалните мрежи.

Социалните мрежи са важна част от ежедневието днес - потребителите са свикнали да:

- Общуват;
- Получават информация;
- Публикуват и споделят информация и т.н..

Има два вида заплахи за социалните мрежи: **технологични** и **организационни** заплахи.

Технологичните заплахи са свързани с различни технологии и тяхното използване в социалните мрежи. **Организационните заплахи** са свързани с поведението, действията и дейностите на потребителя в Интернет. Начало на организационна заплаха обикновено се започва от някой друг в социалната мрежа.

Най-често срещаните заплахи в социалните мрежи са:

- ✓ различни видове зловреден софтуер или вируси;
- ✓ фишинг атаки - фишинг съобщения или имейли, съдържащи връзки към уебсайтове, заразени със злонамерен софтуер;

- ✓ изпращане на спам;
- ✓ скрити кликвания, които карат потребителя да щракне върху нещо различно от първоначално предвиденото от потребителя;
- ✓ различни видове ковани профили - някои от които са полуавтоматизирани или напълно автоматизирани, а други са изкуствени;
- ✓ изводи за изводи са техники за извличане на данни и информация, които анализират наличните данни, за да получат допълнителна информация за жертвата. В социалните мрежи те се използват за препращане и идентифициране на личната и чувствителна информация на потребителите, която потребителят не е избрал да споделя, като религиозни вярвания и сексуална ориентация. Атаката в социалната мрежа се основава на информация, налична в профилите на жертвата и неговите приятели.
- ✓ кибермобинг - емоционално унижение с използване на съвременни технологии. Възбрана, унижение, секстинг, тормоз, изпращане на гадни снимки, подигравки, лъжа за самоличност, за да се получи лична информация, достъп до информация на други хора, проследяване и т.н.

За да се избегнат заплахи, могат да се използват различни решения, предлагани от социалните мрежи:

- механизми за удостоверяване,
- блокиране на потребители,
- лични настройки на потребителите,
- опция „докладване на потребител“.

Изброените решения могат да се използват успешно за защита на потребителя от фалшиви профили, емоционално насилие, наивно и рисково поведение.

Различни компании за решения за сигурност - AVG, Avira, Kaspersky, Panda, McAfee, Symantec - предлагат решения за интернет защита на потребителите на социални мрежи. Техният софтуер обикновено включва антивирусна програма и защитна стена, понякога предлагащи антиспам и антифишинг защита за потребителите на Интернет. Такъв софтуер помага на потребителите на социални мрежи да защитават личните си компютри от заплахи като злонамерен софтуер, скрити кликвания и фишинг.

Съвети за безопасно комуникиране в социалните мрежи

Тип	**Пример**
Постване (публикуване)	Помислете внимателно, преди да публикувате информация. Всичко, което публикувате, вероятно ще стане обществено достояние в даден момент и може да повлияе негативно на вашата репутация и бъдеще. Бъдете внимателни - други също могат да публикуват за вас. Може дори да се наложи да помолите някой да изтрие информацията, която са публикували за вас.
Поверителност	На практика всички социални мрежи имат допълнителни опции за поверителност - настройвайте ги, когато е възможно. Например, уебсайтът наистина ли трябва да знае вашето местоположение? Редовно проверявайте опциите за поверителност и се уверете, че работят по начина, по който мислите.
Пароли	Защитете акаунтите си в социалната мрежа с достатъчно дълга и уникална парола или паролна фраза. Паролната фраза е парола, която се състои от няколко думи, което улеснява запомнянето и

Тип	Пример
	записването, но много по-трудно се досеща за кибер престъпниците.
Измама	Подобно на имейлите, известията в социалната мрежа могат да се използват за различни опити за измама. Например злонамерен човек може да се опита да се промъкне във вашата парола или информация за кредитна карта. Внимавайте с връзките, които получавате.
Контакти	Не се свързвайте с непознати и съмнителни лица. Създаването на фалшиви профили е много просто и много хора го използват, за да излъжат своята самоличност. Целта на тези профили е да заблудят, да спечелят доверието ви и да го използват срещу вас.
Условия за ползване	Запознайте се с условията за социални мрежи - всичко, което публикувате, може да стане собственост на социалната мрежа.
Работа	Ако искате да публикувате нещо за вашата работа, първо разберете дали е приемливо за вашето ръководство.

Персонализирана измама

Новата форма на киберпрестъпления - персонализирани измами - става все по-популярна. Кибер престъпниците събират или купуват информация за милиони хора и след това използват тази информация за персонализиране на атаки. Колкото повече знаете за подобни атаки, толкова по-лесно ще бъде да ги откриете и спрете.

Измамите с имейли и телефони не са новост, киберпрестъпниците от години се опитват да заблудят хората. Примерите включват „Вие сте спечелили от лотарията“ или известната измама на принца на Нигерия. Но при тези традиционни атаки киберпрестъпниците не знаят с какво ще имат работа. Те просто правят общ имейл и го изпращат на милиони хора. Тъй като тези измами са толкова общи и еднакви, те обикновено са лесни за разпознаване. Персонализираната измама е различна, първо се разследва киберпрестъпността и се изготвя имейл, подходящ за всяка жертва. Те правят това, като събират информация или купуват база данни с имена, пароли, телефонни номера и друга информация на хората. Такава информация е лесно достъпна благодарение на много хакнати уебсайтове. Също така той често е свободно достъпен на сайтове за социални мрежи и публично достъпни ресурси на публичните власти.

Атаката работи по този начин: те намират или купуват информация за потребителските имена и пароли на хората, получени от хакнати уебсайтове, след което намират вашия имейл адрес и информация, свързана с вас, в такава база данни и ви я изпращат (както и на всички останали в тази база данни) - имейл с информация за вас, включително паролата, която сте използвали в хакнатия уебсайт. Кибер престъпниците ви дават тази парола като „доказателство“, че компютърът или устройството ви са били хакнати, което очевидно е погрешно. Киберпрестъпниците също твърдят, че сте се промъкнали в порнографски материали в Интернет след хакване. Имейлът заплашва, че ако не платите откупа, доказателства за вашите срамни онлайн дейности ще бъдат изпратени на вашето семейство и приятели.

Ключът е, в този и почти всички подобни случаи киберпрестъпниците не са хакнали вашето устройство. Те дори не знаят кой сте или какви уебсайтове посещавате. Измамниците просто се опитват да използват някои от нещата, които знаят за вас, за да ви сплашат и да ви накарат да повярвате, че са ви

хакнали машината и да ви накарат да им платите. Не забравяйте, че лошите могат да използват същите техники за измамни телефонни разговори.

Какво да направя? Разпознайте такива имейли и телефонни обаждания като измамни. Естествено е да изпитвате страх, когато някой разполага с вашата лична информация. Но помнете, подателят лъже! Атаката е част от автоматизирана масирана кампания, а не опит за атака срещу вас. В днешно време за престъпниците става все по-лесно да намират или купуват лична информация, така че се пригответе за по-персонализирани атаки в бъдеще.

Признаци за разпознаване на атака:

- Винаги бъдете подозрителни, когато получите много спешен имейл, съобщение или телефонно обаждане. Когато някой използва емоции като страх или спешност, той се опитва да ви накара да побързате.
- Всеки, който иска плащане в криптовалута BitCoin, карти за подарък или други непроследими платежни инструменти.
- Ако получите подозрителен имейл, направете търсене в Google, за да видите дали някой е съобщавал за подобна атака.

Always try to use long, unique passwords for each of your online accounts. Can't remember all the passwords? Use the password manager. In addition, use 2-step authentication whenever possible.

1.4. Цифров отпечатък

Цифровият отпечатък е информация, която съзнателно или несъзнателно оставяме във виртуалната среда - визуална, аудио и писмена информация. Има и информация, която не се генерира самостоятелно, а е създадена от родители, приятели, работа и т.н. Липсата на дигитален отпечатък днес

може да бъде невъзможна, но прекалената активност в социалните мрежи може да има и негативни последици.

Цифровият отпечатък се основава на вашата дейност в Интернет: навици за пазаруване, медии, използване на устройства, избрани от вас платформи.

2. Основни принципи за безопасно използване на технологиите

2.1. Интернет връзка

За да попречите на други хора да използват чужди данни за удостоверяване, като потребителско име и парола, **трябва да сте сигурни, че сърфирате сигурно**!

Докато сърфирате, уеб браузърът съхранява информация за уеб страниците, които посещавате, на твърдия диск на потребителя, която може да бъде разделена на три типа:

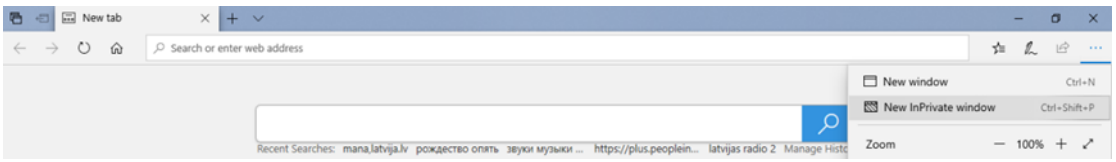
a) Списък на страниците, които посещавате, или История на страниците, които посещавате.
b) Информация, съдържаща се в уеб страници, която обикновено се съхранява в така наречената Cachememory. Това обикновено е папка, наречена Временни интернет файлове.
c) Бисквитки - малки текстови файлове. Тези файлове записват, пароли, списък на посетените страници и датите на гледане. Браузърите прехвърлят тази информация обратно към интернет сървърите. Обикновено, когато отворите уебсайт в браузъра си, имате възможност да приемете / откажете използването на

бисквитки. Препоръчително е да приемете използването на бисквитки на уебсайтове, към които планирате да се върнете отново.

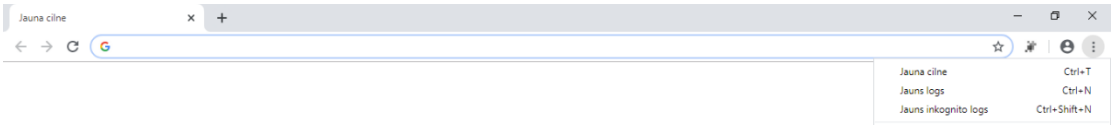
Когато използвате публичен компютър, имайте предвид, че други хора ще могат да преглеждат историята на браузъра на сайтовете, които клиентът е посетил, както и изтеглените файлове. Препоръчително е да изчистите историята на браузъра си Ctrl + H и бисквитките, за да избегнете неприятни ситуации. В много браузъри можете да направите това, като натиснете Ctrl + Shift + Delete на клавиатурата.

Ако не искате браузърът ви да записва вашата история на активност и потребителски имена и пароли, препоръчваме да използвате частно сърфиране. Частното сърфиране може да има различно име във всеки браузър, но същността му е една и съща във всички браузъри. Изображенията по-долу показват някои примери за това как да отворите прозорец за частно сърфиране.

Microsoft Edge



Google Chrome



Не забравяйте да защитите вашата самоличност, пароли и кодове за сигурност. Тези данни могат да се използват от неоторизирани лица.

Следните основни насоки се препоръчват при използване на Интернет:

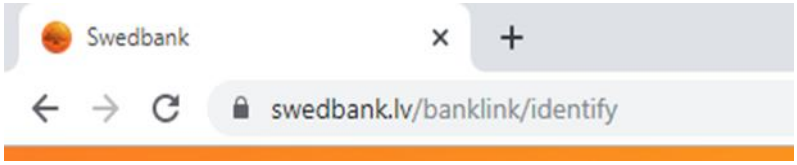
- Не давайте вашата лична карта, ПИН кодове и други данни за достъп на други лица;
- Не публикувайте в Интернет и не изпращайте копия на документи (паспорт, лична карта, шофьорска книжка) чрез електронна поща, приложения за комуникация или социални мрежи;
- Не препращайте пароли и друга лична информация в имейли или съобщения от комуникационни приложения (WhatsApp, Viber, Messenger и др.) И социални мрежи (Facebook, Twitter и др.);
- Не отваряйте прикачени файлове, когато получавате подозрителни имейли;
- Не казвайте на другите твърде много за живота си в Интернет и социалните мрежи, особено за финансовото си състояние, нови неща, напускане на дома и т.н .;
- Помислете добре какви снимки да публикувате в интернет и как тяхното публикуване може един ден да повлияе на живота на човек, като взаимоотношения с приятели, роднини, колеги, настоящи или бъдещи работодатели;
- Когато получавате имейл от публичен орган или банка с молба да изпратите личните си данни на органа, никога не трябва да го правите, тъй като органът никога няма да поиска данните под формата на имейл;
- Когато се свързвате с електронни услуги, уверете се, че други хора не могат да видят данните за достъп, които сте въвели, и информацията, получена в резултат на електронната услуга;
- Уверете се, че на компютъра ви е свързана антивирусна програма, свързана с интернет;
- Изключете компютъра за една нощ, за да спестите не само електричество, но и да намалите риска компютърът да бъде хакнат и използван незаконно.

2.2. Сигурна връзка - уеб страници със сертификати за сигурност

Сигурност означава защита на данните, съхранявани в компютърни мрежи и компютърни системи, от повреда, загуба или неоторизиран достъп. В днешно време бързата наличност на компютърните мрежи и особено на Интернет призовава този въпрос да бъде все по-често разглеждан. Основният проблем със сигурността в компютърните мрежи е тяхната защита срещу неразрешена употреба, например при извършване на електронни плащания има вероятност данните да бъдат откраднати и злоупотребени.

Шифроването се използва за защита на данни или съдържание на съобщения срещу неразрешена употреба. Шифроването е процес на обработка на данни и съобщения от създателя или подателя на съобщението. За да използвате такива данни или съдържание на съобщение, те трябва да бъдат дешифрирани. Ключът за криптиране се използва за криптиране и декриптиране на данните.

Уебсайтовете, които обменят криптирани съобщения, се наричат **защитени уебсайтове**.



Сигурната връзка обикновено е представена от икона 

Рискове, свързани с онлайн дейности:

- неволно разкриване на лична информация. За да използвате услугите, предлагани на уебсайтове, често трябва да се регистрирате с личната си информация, като име, дата на раждане, адрес. Преди

да предоставите тази информация, уверете се, че сайтът е надежден и сигурен;

- тормоз или сплашване чрез разпространение на злонамерени слухове или чрез изпращане на съобщения за заплаха;
- потенциално насилие. Използвайки социални мрежи като Facebook.com и създавайки нови контакти, можете да срещнете потенциален насилник, побойник и т.н. Следователно е необходимо да помислите каква информация да предоставите за себе си и да оцените критично направените предложения.

В случай на измама, тормоз и емоционално унижение, информирайте правоприлагащите органи, като полицията.

Безопасност на децата в интернет

Препоръчват се следните мерки за защита на децата от негативни ефекти при използване на Интернет:

- Поставете компютъра в стая, където могат да се наблюдават дейностите на детето в мрежата;
- Създаване на детски потребителски акаунти с ограничени права на компютърни потребители;
- Ограничете сърфирането, като включите филтри, които забраняват достъпа до уебсайтове, съдържащи детско съдържание (наркотици, порнография, реч на омразата, оръжия и др.);
- Ограничете използването на вредни игри, като забраните игрите на определени теми;
- Ограничете използването на компютър, като зададете график за използване на вашия компютър;
- Например: Потребителски акаунти и семейна безопасност.

2.3. Wi-fi

Ако вашият компютър, таблет или смартфон поддържа WiFi (безжичен интернет), можете да използвате интернет, без да се налага да свързвате допълнителен кабел към вашето устройство.

WiFi може да се използва както у дома, така и извън него. Ако искате да използвате WiFi извън дома си, често можете да виждате различни WiFi мрежи на вашите устройства, но не всички ще имат достъп, тъй като мрежата може да е защитена с парола.

На много места, например, кафенета, магазини, паркове, имате възможност да използвате безплатен обществен WiFi. Най-добрият начин за безопасно използване на обществени WiFi връзки на публично място е да откриете паролата и да използвате безплатна връзка чрез криптиран достъп. Публично достъпният WiFi все още е един от най-често използваните начини за незаконно свързване с вашето мобилно устройство и достъп до личните ви данни.

2.4. Прикачени файлове към имейл, включени връзки и спам съобщения

Спам или нежелана поща се нарича спам и боклук. Спамерите могат лесно и евтино да изпращат имейли до хиляди хора едновременно. Такива писма са анонимни.

Как да се борим срещу спама:

a) **Използвайте блокер за нежелана поща**. Блокиращият спам може значително да намали входящия спам. Повечето доставчици на електронна поща, като Google Gmail, имат автоматичен блокер за спам. Ако е необходимо, могат да се използват и допълнителни програми, които блокират спама. Обаче и в този случай има вероятност да ги получите.

b) **Не отговаряйте на спам**. Ако получите интересно спам съобщение, може да се изкушите да отговорите на него или да кликнете върху връзката, за да се откажете от получаването на допълнителни имейли. Отговаряйки на спама или кликвайки върху връзка, вие несъзнателно заявявате, че този имейл адрес работи и че в бъдеще на него ще се изпраща нов спам.

c) **Деактивирайте изображенията**. Имейлът може да съдържа изображения, които спамерът може да проследява. Когато отворите спам и позволите да се изтеглят изображения към него, вие посочвате, че сте готови да получавате нов спам.

d) **Деактивирайте екрана за показване на съобщения**. Когато щракнете върху буква, тя автоматично се показва в прозореца на презентацията. Разглеждането на нежелана поща може да доведе до получаването на допълнителен спам.

e) **Проверявайте редовно папката със спам**. Понякога блокерите за нежелана поща блокират не само спама, но и законните имейли. Затова трябва да проверявате папката си с нежелана поща възможно най-често, за да избегнете пропускането на важно съобщение. Проверете настройките на вашия имейл клиент за това кои имейли ще бъдат разрешени и кои ще бъдат блокирани.

✉	Създайте множество имейл адреси, за да ги използвате за различни цели.
✉	Не разкривайте личния си имейл адрес в публични мрежи.
✉	Не създавайте кратки имейл адреси. Много спамери изпращат имейли на произволни имейли. Колкото по-кратък е адресът, толкова по-лесно е да се открие.
✉	Ако искате да пуснете реклама в Интернет, създайте нов имейл адрес за тази цел.

✉	Ако трябва да разкриете своя имейл адрес, направете го в по-неразбираема форма, като firstname.lastname@mail.com, като пишете като firstname-lastname-et-mail-dot-com.
✉	Не използвайте личния си имейл адрес, когато се регистрирате за обществени мрежи.
✉	Не рискувайте да използвате опцията „отписване“, тъй като това често само насърчава да ви изпраща повече спам.
✉	Променете личния си имейл адрес, ако е бил открит и има много спам.

2.5. Сигурни пароли

Избраните от вас пароли са най-важният и основен щит за защита на вашите акаунти. Използвайте прост, но сигурен начин за създаване и съхраняване на всичките си пароли.

Стъпки за опростяване на паролите:

1. *Паролни фрази*

Най-важната характеристика на паролите е, че те трябва да са достатъчно дълги, колкото повече знаци има в паролата, толкова по-добре. Те се наричат фрази за парола, вид защитена парола, която използва кратки изречения или случайни думи:

- *Време е за силно черно кафе!*
- *липсващ-охлюв-обхождане-плаж*

И двете пароли са защитени, с над 20 знака и двете пароли са лесни за запомняне, лесни за писане, но трудни за разбиване. Ще срещнете уеб

сайтове или ситуации, които изискват използването на символи, цифри или главни букви за паролата. Но не забравяйте, че ключът към паролата е дължината!

2. *Мениджъри на пароли*

Нуждаете се от уникална парола за всеки от акаунтите си. Ако използвате една и съща парола за множество акаунти, излагате на голям риск. Всичко, от което кибер-нападателят се нуждае, е да хакне уебсайта, който използвате, да открадне всички пароли, включително вашата, и след това да използвате паролата си, за да влезете във всичките си други акаунти. Това се случва по-често, отколкото можете да си представите. Възможно е да проверите www.haveibeenpwned.com колко уебсайтове, които използвате, са хакнати и паролите ви може да са компрометирани. В такива случаи едно от решенията е да се използва мениджър на пароли. **Password Manager е специална компютърна програма, която съхранява всичките ви пароли по сигурен, криптиран начин**. Трябва да запомните само една парола - за вашия мениджър на пароли.

След това Password Manager автоматично извлича вашите пароли до подходящите сайтове, когато имате нужда от тях, и ви удостоверява. Те имат и други функции, като например възможността да запазите отговорите си на въпроси за сигурност, да ви предупреждават, ако използвате повторно паролата си, функция за генериране на пароли, която ще ви позволи да създавате и използвате защитени пароли и много други. Повечето мениджъри на пароли също сигурно синхронизират между различни устройства, така че имате лесен и сигурен достъп до вашите пароли, без значение каква система използвате.

Запишете паролата си за мениджър на пароли на хартия и я съхранявайте на сигурно място у дома. Някои мениджъри на пароли дори ви позволяват да отпечатате инструмент за възстановяване на

диспечер на пароли. По този начин, ако забравите паролата си за мениджър на пароли, имате план за архивиране. Също така, при спешни случаи, когато е необходимо, вашите доверени хора ще могат да получават информация от ваше име.

3. *Двукратно удостоверяване*

Проверката в две стъпки (често наричана двукратно удостоверяване или многократно удостоверяване) осигурява допълнителен слой сигурност. Това изисква две неща, когато влезете в акаунтите си, паролата и цифровия код, които ще бъдат генерирани на вашето смарт устройство или изпратени на телефона ви. Този процес гарантира, че дори ако кибер-нападателите са получили вашите пароли, те няма да имат достъп до вашите акаунти. Двукратното удостоверяване е лесно да се настрои и обикновено трябва да го използвате само веднъж, когато упълномощавате от ново устройство. Ако използвате мениджър на пароли, препоръчително е да го защитите както със сигурна фраза за парола, така и с двукратно удостоверяване.

Опростеното **удостоверяване в две стъпки** означава, че освен да въведете нещо, което знаете (парола), вие го потвърждавате и с нещо, което имате (например код от мобилен телефон). Има и оторизация в три стъпки, при която трябва да потвърдите достъпа с нещо, което е подходящо за вас - например с пръстов отпечатък. Предимството на 2-стъпковото удостоверяване е, че хакерът се нуждае и от достъп до вашето мобилно устройство, за да проникне в акаунта ви.

3. Използване на пароли

3.1. Пароли: Първата стъпка в сигурността

Има два вида пароли: защитени и несигурни. Повечето хора използват несигурни пароли - пароли, които са кратки, лесни за запомняне, съдържат лична информация (като име, фамилия, година на раждане, важна дата,

имена на домашни любимци, фамилни имена) или дори същата парола се използва за множество акаунти.

Хакерите често използват софтуер за откриване на пароли, който проверява много пароли, докато намерят правилната. Несигурните пароли могат да бъдат открити много бързо. Създаването на защитени пароли намалява вероятността престъпниците да разкрият паролата ви и да откраднат лична и финансова информация.

За да защитите данните си, има основни принципи за сигурност, които трябва да се спазват при използване на парола:

- Когато въвеждате паролата си, внимавайте да не позволявате на други хора да виждат как пръстите ви се движат по клавиатурата или екрана на вашия смартфон;
- Променяйте паролата си на всеки 3 месеца;
- Внимавайте да не запазите автоматичен достъп до акаунта. Винаги използвайте бутоните Exit, Logout или End job;
- Избягвайте да използвате пароли в интернет сайтовете с безплатен достъп.

3.2. Принципи на създаване на сигурна парола

Когато създавате потребителски акаунт в социалните мрежи, като използвате интернет банка или друг портал за самообслужване, трябва да се регистрирате с вашето потребителско име, парола и други подробности.

Съвет	**Обяснение**
Никога не използвайте лична информация	Не използвайте имена, рождени дни или фамилни имена като пароли. Личната информация често е публично достъпна,

Съвет	Обяснение
	така че можете да познаете паролата много бързо.
Използвайте по-дълги пароли	Паролата трябва да е с дължина поне шест знака. За да направите паролата си по-сигурна, можете да използвате 12 или повече знака, за да въведете паролата си.
Избягвайте да записвате пароли на вашия бележник или телефон	Ако все пак искате да запишете паролата си, пазете я на сигурно място и не я показвайте на никого. Препоръчително е да шифровате паролите си и да не записвате самата парола.
Използвайте произволно избрани пароли	Случайните пароли са най-сигурните. Вместо да мислите за собствените си пароли, можете да използвате генератори на пароли. Случайните пароли са по-трудни за запомняне, защото са създадени от устройства.
Не използвайте едни и същи пароли за множество акаунти	Ако някой разкрие паролата за един акаунт, паролите за другите акаунти също ще бъдат уязвими.
Не използвайте думи, които могат да бъдат намерени в околната среда	Например парола teacher1 ще бъде несигурна парола.
Включете цифри, символи и малки букви в паролите	За да създадете сигурна парола, можете да замените буквите с различни символи, например въз основа на думата Monday! и заместваики буквите „о“ и „а“, можете да

Съвет	Обяснение
	създадете следната защитена парола M0nd @ y!

3.3. Казус и практически упражнения

Г-н Браун, мъж в най-добрите си години, най-накрая реши да започне да използва електронни услуги и е готов да се регистрира за уебсайта на Дирекцията за безопасност на движението по пътищата (CSDD), за да може да разбере за себе си и колата си дистанционно в бъдеще.

За да създадете или активирате своя CSDD акаунт, при първото влизане в уебсайта трябва да се регистрирате с вашия имейл, да създадете своя собствена парола и да я въведете. След като акаунтът е създаден за първи път, достъпът до вашия акаунт в CSDD ще продължи както с установения достъп, така и с вашия достъп до Интернет банкиране.

Задачата на ситуацията е г-н Браун да измисли парола за новосъздадения акаунт на CSDD в хола си на компютъра си, така че никой да не може да го отгатне.

Общата сцена – Г-н Браун седи в хола на провинциалната си къща зад отворен лаптоп. На заден план има диван, на който спи мързелива персийска котка на име Рудис. Госпожа Браун седи на другия край на дивана и плете шапка. Г-н Браун има черно куче на име Poga, което лежи в краката му. Някъде на заден план камина пука топло, а над нея виси трофеят за лов на Браун, глава на лос с рога. Едната стена на хола е заета от рафт за книги, където можете да видите разпознаваеми произведения на различни писатели. На кориците на някои книги можете да видите техните портрети, например Шекспир, Достоевски, Чехов и др. На другата стена има снимка

на семейство Браун, където можете да видите техните възрастни деца и внуци. Има дори лятна снимка на г-н Браун и съпругата му, позиращи на Ниагарския водопад. Малко по-нататък виси бръшлян, висящ на рафт, а на перваза на прозореца расте кактус.

1) Всеки от важните ключови обекти (елементи) на семейната къща на Браун може да бъде разгледан като възможна лоша или добра версия на паролата:

- Котка Рудис: *Rudis* / **RuD! $**
- Хоби на съпругата: Knitting /**Kn*tt*ng**
- Растение в стаята: Cactus / **sutcac**
- Ловен трофей: Trophy / **Tr0fhy**
- Куче Рога: Poga / **50g** @
- Внук12: Grandson12 / **Gr@nds0n**
- Съпруга Rosalie: Rosalie / **R0s@lie**
- Чехов: Chekhov / **Ch3kh0v**
- Достоевски: Dostoevsky / **D0$t0j3v$ky**

Заключение

Този модул съдържа три важни теми, свързани с личните данни и защитата на поверителността. Като основите за сигурността на вашия компютър и основните принципи за защита на данните. За да се избегне фишинг, учащите се запознаха с начините, по които киберпрестъпниците действат, за да крадат информация. Като се има предвид, че един от най-важните проблеми на защитата на личните данни в днешно време е публикуването и споделянето на твърде лична информация в различни социални мрежи, този модул предоставя и насоки за безопасност на тази тема.

За безопасно използване на цифрови устройства извън дома, този модул обхваща темите за интернет връзките и основните принципи за безопасно използване на Wi-Fi. Бяха обяснени и признаците на несигурни имейли и нежелана поща и бяха предоставени съвети за правилното и сигурно използване на паролите.

В заключителния раздел на модула се разглеждат примери за създаване на пароли и се описва ситуацията - как се създават пароли, какъв вид пароли трябва да се имат предвид и кои трябва да се избягват!

Библиография

- *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/
- Pieslēdzies, Latvija! (n.d.). *Esiet sveicināti datorskolā! Mācies pats*. [Online Course]. 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. (n.d.). Uzdevumi.lv. https://www.uzdevumi.lv/
- Latvijas Drošāka interneta centrs. (n.d.). Drossinternets.lv. www.Drossinternets.lv
- Draudzīgs internets. (n.d.). *Interneta Drosības ABC*. Draudzigsinternets.lv. www.draudzigsinternets.lv