Проект IDCAP: Подобряване на цифровите компетенции на възрастни

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

Цифрова идентичност

1. Въведение

По отношение на цифрова или базирана на интернет идентичност цифровата идентичност е информацията, която представлява реално лице или друг външен агент. Външен агент може също да бъде единична машина, система и / или приложение. ISO / IEC 24760-1 определя идентичността като „набор от атрибути, свързани с обект". В днешно време говорим за идентичност като конкретни атрибути на обект, който е заменил термина „агент". В този документ ще имаме предвид цифрови самоличност само по отношение на самоличността на физическо лице.

Тук ще ви представим основите на управлението на вашата цифрова идентичност и защо е важно тя да бъде защитена. След това ще видим по-подробно как да управлявате и интернет акаунта и кои са ключовите стъпки в процеса. По-нататък ще представим основите на сигурността и поверителността онлайн. Накрая ще обсъдим накратко проблемите с цифровия отпечатък и онлайн идентичността.

2. Управление на цифровата идентичност

Управление на релетата за цифрова идентичност на принципи, които следват повече или по-малко добре известни механизми, разработени за недигитална идентичност. Въпреки че може да изглежда сложно, помислете за вашата лична карта. Когато поискате да получите вашата лична карта, органът, който я издава, утвърждава от други органи вашия рожден ден, данъчен номер, граждански номер (където е приложимо), направете нова ваша снимка и т.н. В цифровия свят вашата цифрова самоличност може да бъде толкова проста като вашето потребителско име и парола или може да има много повече нива на сложност, които са там, за да гарантират, че собственикът на тази конкретна самоличност сте вие и само вие. Тези нива могат да включват отделен електронен подпис, маркер за „произволно“ генериране на определен цифров код, SMS потвърждение или код, изпращан до определен мобилен телефон (за който е известно, че е регистриран на конкретно лице), гласова идентификация, отговор на определен въпрос (като Какво беше първото ви име за домашен любимец?), валидиране на пръстови отпечатъци и много други. Всички тези нива са налице, за да гарантират, че само конкретното лице е упълномощено да извършва някои действия в цифровия свят.

Много хора намират тези нива за трудни за разбиране, объркващи и разочароващи. Те може да са прави, но от друга страна, човек трябва да разбере, че цифровият свят е пряко представяне на физическия свят и никой не би искал техните „цифрови“ пари да се оттичат от тяхната „реална“ банкова сметка. Институциите и особено банките поставят различни нива на сигурност не за да дразнят потребителите, а за да защитят тяхната идентичност и да гарантират правото на операции и

транзакции. Успоредно с това, все повече и повече услуги се предлагат чрез вашия мобилен телефон. Те обхващат толкова широк диапазон, че тук ще посочим само няколко като илюстрация. Мислете за тях като за услуги, които пряко влияят на вашата „реална“ банкова сметка. Някои от тези услуги, извършвани чрез смартфони (в зависимост от държавата ви на пребиваване), могат да бъдат:

- Плащане на паркинг чрез SMS съобщение
- Плащане на вашата сметка в супермаркета
- Плащане на вашите домашни сметки
- Директен превод на пари чрез специално оторизирано от банка приложение

3D удостоверено плащане на вашата VISA или Master Card - след като сте подали номера на картата, валидността и кода за сигурност, тази система изпраща SMS с 6 цифрен код, за да провери предварително мобилния телефон, което ще добави още един слой защита на вашата карта транзакции.

Билети за сухопътен транспорт и бордни карти за самолети
С „Apple pay“ и „Google Wallet“ вашият мобилен телефон се превръща в портфейл за всяко плащане, което поддържа NFC или магнитни плащания. Дори ви позволява да получавате плащания от различни интернет базирани сайтове, магазини и потребители.

Разбираемо е защо е толкова важно правилното управление на вашата цифрова идентичност и защо човек трябва да я защитава енергично.

3. Управление на интернет акаунт

Като част от вашата цифрова самоличност, вашият интернет-базиран акаунт е първа и в много случаи неизбежна стъпка. Обикновено е

свързан с имейл услуги като Gmail на Google, Yahoo mail, имейл на Microsoft и др. След като създадете такъв акаунт, към него са прикрепени поне две променливи: вашето потребителско име и вашата парола. Днес повечето доставчици изискват мобилен телефонен номер да бъде прикачен и проверен към всеки конкретен акаунт. По този начин имате 3 атрибута на акаунт за цифрова самоличност - вашето потребителско име, вашата парола и вашия мобилен телефонен номер. В много случаи тази проверка, без да ви пита и с цел допълнителна защита ви добавя не само телефонния номер, но и уникалния производствен номер на мобилен телефон, наречен IMEI - International Mobile Equipment Identity. Този номер, който се присвоява по време на производството, е необходим, за да разреши използването на мобилен телефон и през мобилна мрежа. Тази информация се криптира и съхранява в безопасност от доставчиците на интернет услуги, но все пак в някои редки случаи може да бъде откраднатата или злоупотребена (като в случая с Facebook и Cambridge Analytica, където милиони данни на потребителите са предоставени на компания, за да направете целенасочена реклама за политически цели). Ето няколко съвета, които да ви помогнат с вашата цифрова идентичност:

Потребителско име: изберете потребителско име, което ясно ви представя. Помислете, че може да използвате този конкретен имейл адрес в бъдеще и забавните имена не винаги са добре приети. Вашето потребителско име ще стои пред знака @ на вашия имейл, така че имена като easygirl @, toughguy @, yournightmare @ не само трябва да се избягват, но и изобщо трябва да ги избягвате. Когато избирате потребителското си име, не включвайте числа като рождения си ден или рождените дни на вашите близки.

Парола: Използвайте комбинация от малки букви, главни букви, цифри и специални символи като #, $, &, |, ~. Направете го поне 8 знака и променяйте често паролата си. Ако имате достъп до своя цифров акаунт

чрез мобилния си телефон, използвайте пръстов отпечатък или друга форма за удостоверяване. Не запомняйте паролата за акаунта в браузъра.

Дори и да не се изисква изрично добавете мобилния си телефон към акаунта си и го задайте като устройство по подразбиране за възстановяване на забравени пароли. Разгледайте настройките на вашия акаунт и задайте имейл и телефонен номер за възстановяване, за да удостоверите самоличността си още по-добре. Не използвайте същата парола за други акаунти като тези в социалните мрежи или игри.

4. Проблеми със сигурността и поверителността

Някои сървъри и приложения могат да събират обширна информация за конкретна употреба и потенциално могат да бъдат свързани с физическото лице и неговите / нейните дигитални навици по интернет. На ниво EC GDPR (Общ регламент за защита на данните) се опитва да се справи с това, но въпреки това се препоръчва на потребителите да внимават какво и къде споделят и правят в интернет и особено в някои социални мрежи.

За да обработите вашето цифрово съдържание, има многобройни редактори както за снимки, така и за видео, докато обикновено социалните медии предоставят възможности за проверка на правописа и за писмен текст на английски език. На цифрови снимки (и видеоклипове) можете да добавяте различни филтри, да променяте наситеността, контраста и др. Можете да използвате предоставените с вашето устройство или да инсталирате този, който ви харесва най-много. Имайте предвид, че повечето безплатни онлайн редактори обикновено имат някои ограничения и трябва да си купите такъв, за да

отключите всички функции. Тези софтуерни услуги често добавят към вашата снимка или видео написан знак, че материалът е създаден с помощта на този софтуер, което може да не ви хареса. Експериментирайте и проверявайте, докато намерите този, който отговаря на вашите нужди.

Както беше подчертано в проучване на ОИСР от 2016 г. „*Невъзможно е да се премахне изцяло рискът за цифрова сигурност при извършване на дейности, които разчитат на цифровата среда. Обаче рискът може да бъде управляван, т.е. може да бъде намален до приемливо ниво в светлината на интересите и ползите, които са заложени, и контекста* “. Съществуват обаче доста разумни и относително лесни стъпки, които може да предприеме физическо лице или организация, за да достигне задоволително ниво на цифрова сигурност и защита на поверителността. Те включват, но не се ограничават до силни пароли, строга политика за онлайн достъп, здрав разум при сърфиране в интернет, образование и обучение по най-често срещаните нишки, създаване на политика по отношение на личните данни и защитата на личните данни. Като каза, че ЕС налага най-високите стандарти за защита на личните данни и данните за поверителност в света.

Като физическо лице има лесни стъпки за ограничаване на възможността за нарушаване на поверителността. Винаги трябва да се чете внимателно политиката за бисквитките на всеки уебсайт, интернет услуга, новини и социални медийни платформи. В случай, че не искате да бъдете проследявани (т.е. някои уебсайтове събират данни за вашите навици на сърфиране, колко често посещавате даден уебсайт, какви реклами кликвате, каква информация търсите от интернет и т.н.), можете да използвате прозорец за сърфиране инкогнито, който се предлага от почти всички приложения за сърфиране като Google Chrome, Mozilla Firefox, Internet Explorer на Microsoft и т.н.

От страна на сигурността, никога не трябва да се използват едни и същи пароли за различни интернет приложения като имейл, платформи за социални медии и уебсайтове, които изискват влизане. Поддържайте паролата силна с 10 или повече знака, включително цифри, главни и малки букви и специални знаци като &, #, $, ^ и т.н. По правило не запазвайте паролите си в браузъра си, а се опитайте да ги запомните или да ги изградите според правило, което сте формулирали сами. Например:

#MyFamilyName4websiteName~mY_first.name$.

Въпреки че това може да изглежда сложно, лесно е да се запомнят правилата. Винаги когато е възможно, добавете мобилния си телефон като алтернатива за удостоверяване и възстановяване на забравена или откраднатата парола. Това ще добави още един слой лична защита, което намалява риска от злонамерено използване на вашите онлайн данни.

5. Цифров отпечатък

Цифровият отпечатък се отнася до уникалните проследими цифрови дейности на конкретен потребител в интернет. Терминът може да се намери и като цифрова сянка, отпечатък в интернет, кибер сянка и др. Въпреки че обикновено терминът се прилага за физически лица, той може да се използва и за организации, компании, корпорации, сайтове за цифрови услуги и др. Има два вида на дигитален отпечатък - активен и пасивен.

Пасивен цифров отпечатък - този термин се отнася до данни, събрани без знанието на човека. Не е задължително да бъде скрит от потребителя. Активен дигитален отпечатък е този, който потребителят умишлено споделя за себе си обикновено в социалните медии или

различни уебсайтове. Информацията за потребителя може да бъде оставена умишлено или неволно и тогава тази информация се събира активно или пасивно от други страни. Например, ако във вашия профил в социалните медии сте оставили видими всичките си имейл адреси, номера на мобилния ви телефон, адреса на живеене, работното ви място, интернет адреса на вашата компания и т.н., това ще бъде относително много лесно за компютър програма или физическо лице, за да събере много голямо количество информация за вас. В някои случаи тази информация може да включва и вашите банкови сметки или данъчни регистри, ако възникне нарушение в записите за сигурност.
Има редица проучвания, които показват, че приблизително 70% от цялото цифрово поведение на хората е съзнателно и отговорно. Въпреки това, около 30% от цифровия отпечатък на всеки човек може да бъде във форма, която никога не би била разкрита умишлено на обществеността. Това оставя доста данни за анализи на поведението при покупка, навици за онлайн покупки, хобита и други области от личния живот. Въпреки че няма нищо лошо в анализите на клиенти върху големи бази данни, когато се задействат за отделни лица, такива анализи могат да бъдат основата за кражба на самоличност, престъпни дейности и нарушения на поверителността.

Въпреки че цифровият отпечатък не е цифрова идентичност или цифров идентификатор, съдържанието и описателните данни (наричани още метаданни) оказват силно влияние върху поверителността, доверието в интернет и цифровата репутация. Интернет отпечатъци могат да се използват от компании при набиране на нов персонал, правоприлагащите органи при събирането на данни за конкретни лица не могат да се събират по друг начин, търговци - те търсят от какъв тип продукти се интересуват потребителите или които да повишат интересът на потребителите към конкретен продукт или услуга. Социалните мрежи са основният източник на такава информация. В някои случаи социалните платформи могат да събират

данни от устройството на потребителя, дори без потребителят да знае това, използвайки различни сензори на мобилните телефони или други устройства на потребителя. Например Facebook и Google събират големи количества потребителска информация, която, ако се комбинират заедно, може да опише доста подробно личността, интересите, политическите възгледи, покупателните навици и интереси на потребителя и т.н.

6. Онлайн самоличност

Онлайн самоличност е идентичността, която потребителят избира да изгради в Интернет, обикновено с цел игри. Потребителите могат да изберат да се представят с аватари (графична икона с размер), а не с реалните си снимки. Потребителите могат да използват псевдоними вместо истинските си имена. Онлайн самоличността може дори да се определя от връзките на потребителя в интернет с група хора. Онлайн самоличностите се свързват с реални потребители чрез процедури за оторизация като регистрация и влизане (потребителско име и парола), както и чрез специфичен IP адрес на машина или устройство. Такива сайтове често инсталират бисквитки за проследяване, които могат допълнително да определят онлайн поведението на потребителя и да го свържат с реален човек. Тъй като игрите често, но не винаги, са насочени към по-млада аудитория, която не е толкова внимателна в защитата си онлайн, е изключително важно понятието цифрова идентичност, онлайн идентичност и цифров отпечатък да бъде възможно най-ясно за всички, които използват интернет.

Онлайн самоличността може да бъде от идентификационните ви данни за имейл (потребителско име и парола) до акаунта в социалните медии, името на форума или профила на купувача на определен уебсайт. Той също така включва вашата история на сърфиране, IP адрес, активност

при търсене и др. Хората и организациите може да се интересуват от вашата онлайн самоличност за напълно законни или за незаконни цели (хакери). Някои от компаниите трябва да знаят вашата история на сърфиране или история на търсене, за да ви предложат като реклама по-насочени продукти или услуги, свързани с вашите нужди и интереси. Други може да се интересуват от незаконните цели да откраднат вашите данни, номер на кредитна карта и т.н.

Има различни начини, по които можете да защитите онлайн идентичността си, като силни пароли, не споделяне на твърде много лични данни в социалните мрежи, използване на режим „инкогнито“ на вашия браузър, използване на виртуални частни мрежи, криптиране на вашата комуникация и т.н. Колкото повече внимание човек обръща на своята онлайн идентичност, толкова по-защитен е той.

7. Заключение

Представихме основните концепции и знания за управлението на цифровата идентичност и интернет акаунта. Следвайки тези ключови концепции, ние описахме кои са проблемите със сигурността и поверителността на потребителите. И накрая, представихме какво представлява цифров отпечатък и онлайн идентичност.

Също така, предложихме лесни и разбираеми методи за работа с пароли, удостоверяване, цифрова идентичност, поверителност и онлайн сърфиране. След като дадено лице или организация следва тезите, това може да намали до голяма степен всички онлайн рискове. Както винаги няма решения, които да обхващат всички случаи и здравия разум, както и създаване на политики на организационно ниво, които да помогнат за борба със злонамерени действия онлайн и да повишат доверието в използването на интернет и цифровите платформи като цяло.

Накрая разгледахме онлайн самоличността и посочихме какво обхваща и как да се предпазим от незаконно използване на онлайн самоличността.

Библиография:

https://www.zdnet.com/article/identity-management-101-how-digital-identity-works/

https://www.forbes.com/sites/forbestechcouncil/2019/06/07/a-beginners-guide-to-online-privacy-12-important-tips/#5092374e53ed

https://assets.mozilla.net/pdf/IHPbriefs_Online_Privacy_March_2017.pdf

https://www.commonsense.org/education/digital-citizenship/topic/digital-footprint-and-identity

https://www.oecd-ilibrary.org/docserver/5jlwt49ccklt-en.pdf?expires=1591780736&id=id&accname=guest&checksum=AF002079529F4DE263769B3FBEB40035