ПРИРАЧНИК ЗА ДИГИТАЛНА БЕЗБЕДНОСТ

2021

Прирачникот е реализиран со поддршка на:

techsoup EUROPE

METAMORPHOSIS
Foundation for sustainable ICT solutions

Прирачник за дигитална безбедност за професори во основно и средно образование

Содржина

Вовед_____1
Што е дигитална безбедност?_____2
Физичка Безбедност_____3
Лозинки_____4
Веб прелистување_____5
Спам пораки_____6
Социјален инженеринг_____9
Злонамерен софтвер_____11
Заштита_____12
Што е интернет приватност?_____14
Закани за приватноста_____15
Трансфер на податоци_____18
Опасности при пренос на податоци_____19
Враќање на избришани податоци_____19
Сајбер насилство_____21
Интернет вознемирување / малтретирање_____23
Социјалните мрежи и видео игри_____25
Заштита и препознавање_____28
Дигитален отпечаток_____31
Видови на дигитални отпечатоци_____34
Контрола врз дигиталниот отпечаток_____34

Вовед

Живееме во време кога голем дел од нашите животи, лични и професионални, престојуваат во дигиталниот свет на Интернет. Ние го правиме нашето банкарство, купување, плаќање сметки, социјално планирање, па дури и делови од нашата работа во дигиталниот свет. Ова зголемено потпирање на интернетот и дигиталните уреди носи ризици заедно со практичноста што ја овозможува.

ДИГИТАЛНА БЕЗБЕДНОСТ

Што е дигитална безбедност?

- Дигиталната безбедност претставува логичка и физичка безбедност дигиталните уреди.
- Безбедноста на апликациите што ги користиме, како и инфомациите и податоците во нив.
- Мрежната безбедност во зависност на која мрежа сме поврзани: Домашна / Компаниска / Јавна.
- Безбедноста додека сме поврзани на интернетот.
- Оперативната сигурност.
- Едукација на крајниот корисник.

Физичка Безбедност

Физичката безбедност претставува безбедноста на самиот уред, како и физичкиот пристап до него. Во својата основа, физичката безбедност е да ги чувате вашите објекти, луѓе и средства безбедни од реални закани. Тоа вклучува физичко откривање на натрапници, заштитна од природни незгоди и одговор на тие закани.
Физички напади може да биде упад во безбеден центар за податоци или прикрадување во забранети области на зграда. Напаѓачите може да украдат или оштетат важни ИТ-средства, како што се сервери, лаптопи, мобилни уреди, да добијат пристап до важни терминали, да украдат информации преку УСБ или да испратат малициозен софтвер на вашите уреди.

Практики за подобра физичка безбедност:

- Сите дигитални уреди треба да имаат некаков вид на режим за заштита или заклучување. Пример мобилниот уред да мора да биде отворен со внесување на лозинка или пин.

- Секогаш кога ќе го напуштиме нашето работно место, нашиот уред мора да биде заклучен. Односно ако користиме Windows оперативен систем со притискање на Windows кочето и L копчето ќе ни го заклучи компјутерот т.е. ќе биде прикажан екранот за да се логираме. Се додека не сме ние во близина на нашата работна околина или уредите, треба да бидат заклучени. Откако би се вратиле на работното место да направиме мала проверка на USB портите на уредот и дали нешто било разместено.
- Нашата работна маса треба да биде чиста, да нема ливчиња или sticky notes залепени со лозинки, кориснички инфомации или пак информации што би можеле да придонесат кон погодување на нашите лозинки. Оваа практика уште е позната и како “Clean desk policy” – “Полиса на чиста маса”.
- Предноста која мобилните уреди ја имаат е тоа што сите поддржуваат механизам за следење на локацијата. Ова е корисно да биде активнирано, бидејќи кога нашиот уред би бил изгубен или пак украден, да можеме полесно да го лоцираме и пронајдеме.

Лозинки

Лозинка е запаметена тајна, типично низа карактери (букви, бројки, специјални знаци), кои обично се користат за потврда на идентитетот на корисникот. Во денешно време голем број на апликации, уреди, веб страни и платформи не принудуваат да имаме корисничка сметка и лозинка.

Практики за добри лозинки:

- Лозинката треба да биде што е можно подолга во карактери, односно минимум 8 карактери.
- Да биде што е можно по комплексна, односно да содржи комбинација од голема и мала буква, бројка и специјален знак.
- Лозинката да биде нешто што не е поврзано со самиот корисник, за да биде тешка за погодување.
- Ако апликацијата или сервисот има можност за два начини за автентикација и двата да бидат искористени. Пример Facebook овозможува од кога ќе ги внесеме инфомациите како корисничко име и лозинка, да ни испрати СМС код кој мора да го впишеме за да се логираме на Facebook.
- Ако имаме голем број на лозинки и сервиси што ги користиме, пожелно е сите тие да имаат различна лозинка.
- Ако лозинките ги зачувуваме на прелистувачите како Firefox или Chrome, да ја користиме можноста за Primary лозинка. Каде секоја сесија односно користење на прелистувачот ќе мора да да ја внесеме Primary (главната лозинка) за да можеме да ги користиме зачуваните лозинки.
- Редовно менување на лозинките, на одреден временски период препорачливо е да ја смениме лозинката.

Пример за добра “јака” лозинка е следнава: **0va-e-J@KA_l0zink@**

Веб прелистување

Секојдневно посетуваме голем број на веб страни, кои што ги користиме за читање вести, пребарување на инфомации, социјални мрежи и друго. Секоја веб страна користи протокол за комуникација, многу е битно да знаеме кои веб страни користат безбеден протокол и кои веб страни се безбедни за посета.

HTTP овозможува комуникација помеѓу различни системи. Најчесто се користи за пренос на податоци од веб-сервер на прелистувач со цел да им се овозможи на корисниците да прегледуваат веб-страници.

Проблемот со редовниот протокол HTTP е што информациите што течат од сервер до прелистувач не се криптирани, што значи дека може лесно да се украдат. **HTTPS** протоколите го поправаат ова со користење на **SSL сертификат**, кој помага да се создаде безбедна криптирана врска помеѓу серверот и прелистувачот, со што се заштитуваат потенцијалните чувствителни информации од кражба бидејќи се пренесуваат помеѓу серверот и прелистувачот.

HTTPS е особено важен за веб страниците каде што внесуваме **кориснички сметки, лозници и кредитни картички.**

Дополнителни додатоци кои можеме да ги инсталираме на прелистувачите се:

Bitdefender TrafficLight – е додаток кој ни прикажува дали страната на која сме е безбедна за посетување или не.

Avast Online Security – е додаток каде на секое пребарување и прелистување ни ги означува линковите за дали се безбедни за посета пред да ги кликнеме.

Спам пораки

Електронската пошта претставува една од најкористените алатки за комуникација денес, поради тоа е и таргет на голем број напади и се користи за различни измами. Секоја година над 50% од целокупниот број на испратени елекреонски пошти преку интернет се спам пораки.

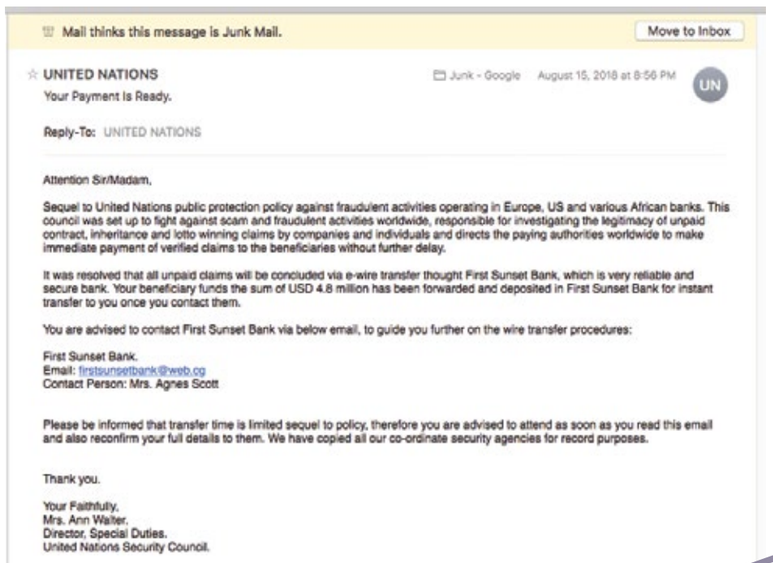
Во најголем дел од случаите спам пораките се рекламен материјал, налик во реален свет тоа би било како да добиваме флаери во нашето поштенско сандаче.

Тоа не станува проблем се додека не почнеме да добиваме голем број на спам пораки на неделно или дневно ниво.

Но, не секогаш спам пораките се рекламни, често се случува да бидат налик на антивирусни предупредувања, кои ни укажуваат дека нашиот компјутер е заразен со злонамерен софтвер и дека мора да го инсталираме нивниот антивирус за да го исчистиме. Овие пораки се **невистинити**.

Друг вид на измамни пораки како дека сме добитник на некоја материјална или парична награда, односно лотарија, која никогаш не сме ја играле.

Примери за спам пораки


Mail thinks this message is Junk Mail. Move to Inbox

UNITED NATIONS Junk - Google August 15, 2018 at 8:56 PM

Your Payment is Ready.

Reply-To: UNITED NATIONS

Attention Sir/Madam,

Sequel to United Nations public protection policy against fraudulent activities operating in Europe, US and various African banks. This council was set up to fight against scam and fraudulent activities worldwide, responsible for investigating the legitimacy of unpaid contract, inheritance and lotto winning claims by companies and individuals and directs the paying authorities worldwide to make immediate payment of verified claims to the beneficiaries without further delay.

It was resolved that all unpaid claims will be concluded via e-wire transfer thought First Sunset Bank, which is very reliable and secure bank. Your beneficiary funds the sum of USD 4.8 million has been forwarded and deposited in First Sunset Bank for instant transfer to you once you contact them.

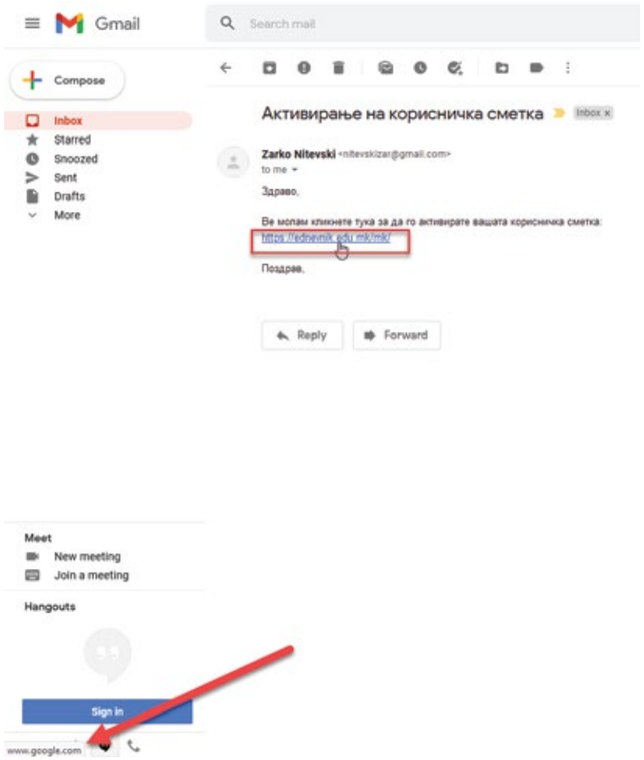
You are advised to contact First Sunset Bank via below email, to guide you further on the wire transfer procedures:

First Sunset Bank.
Email: firstsunsetbank@web.cg
Contact Person: Mrs. Agnes Scott

Please be informed that transfer time is limited sequel to policy, therefore you are advised to attend as soon as you read this email and also reconfirm your full details to them. We have copied all our co-ordinate security agencies for record purposes.

Thank you.

Your Faithfully,
Mrs. Ann Walter.
Director, Special Duties.
United Nations Security Council.



Тоа што може да се види на примерите е дека секогаш линковите во пораките се или сомнителни или не соодветствуваат со фирмата што се претставува во пораката. Често знаат да имаат печатни или граматички грешки во текстовите. И понекогаш адресата од која се испраќа пораката е сомнителна.

Практики кои треба да ги знаеме:

- Никаде јавно да не ја објавуваме сопствената електронска пошта
- Доколку се претплатиме на некоја мејлинг листа, тоа да го направиме свесно.
- Ако после некое време сакаме да се избришеме од одредена мејлинг листа, да знаеме каде тоа треба да го направиме.

Социјален инженеринг

Во контекст на безбедноста, социјалниот инженеринг е психолошка манипулација со луѓе за вршење дејства или давање на доверливи информации. Постојат голем број на начин, но најпознат и користен е Фишинг нападот.

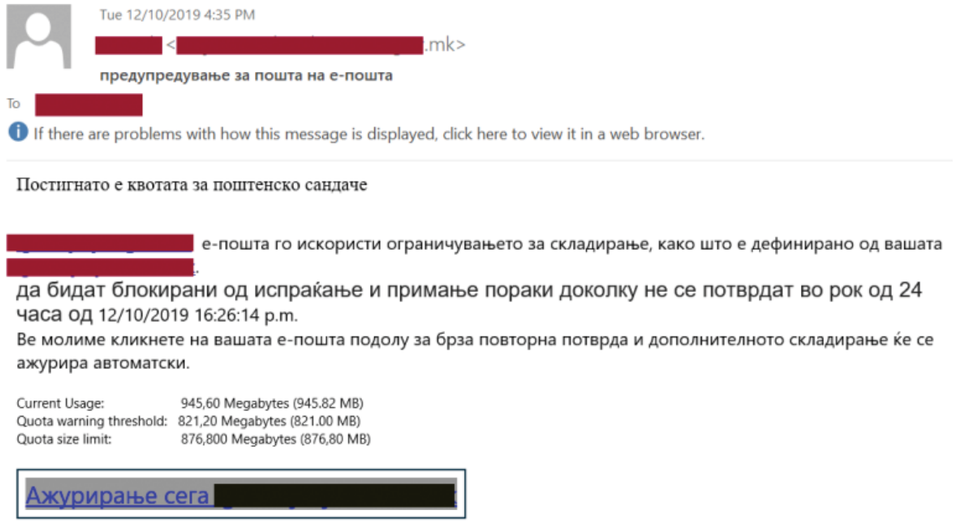
Фишинг напад

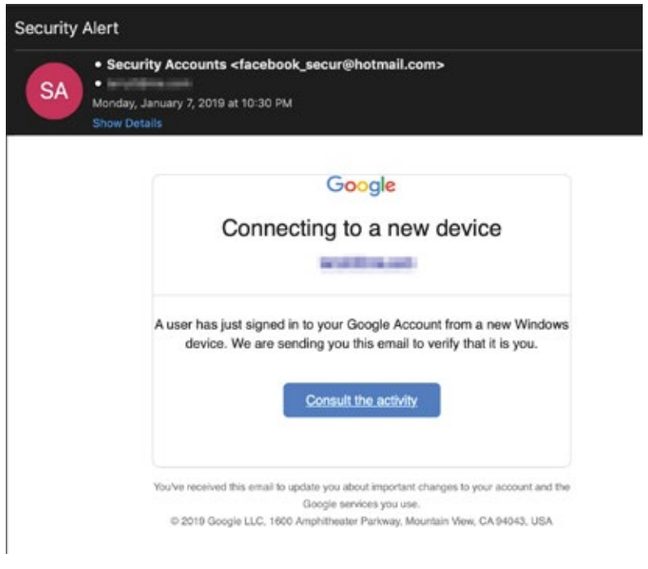
Фишинг пораките се многу слични на спам пораките, со тоа што фишинг пораките настојуваат да извлечат инофмации или пари од нас. Тоа се случува кога напаѓачот, се претставува како доверлив субјект, ја залажува жртвата да отвори е-пошта или инстант порака. Потоа, примателот е измамен да кликне на сомнителен или злонамерен линк, што може да доведе до инсталација на малициозен софтвер или пак да биде пренасочен на страна каде треба да внесе лични и сензитивни податоци.

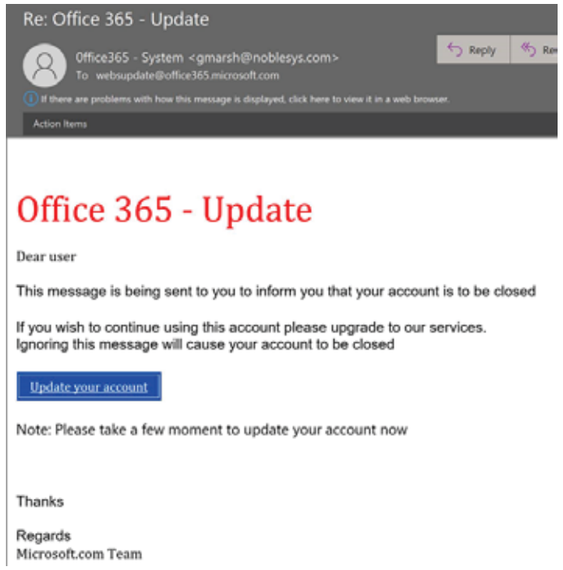
Најчесто се претставуваат како да се од банки или финансиски институции, добитник на награда, лотарија или пак некој позната страна како Facebook. Во сите ситуации наведено е дека треба да им испратиме лични инфомации како име и презиме, адреса на живеење, матичен број, лозинка, трансакциска смета итн...

Тоа што е специфично за фишингот за разлика од спам пораките, е тоа што секогаш овие инфомации мора да се испратат во што е можно пократко време, во спортивно нешто лошо ќе ни се случи нам. Како на пример: ќе изгубиме пристап до електронското сандаче или корисничката сметка, ќе изгубиме пари и друго. И сите пораки се напишани во таков однос дека мора да се рагира брзо и одма и дека е многу важно.

Примери за фишинг пораки







Од примерите можеме да заклучиме дека истите грешки што ги има во спам пораките, присутни се и тука. Како сомнителни линкови, адресата од која се испраќа пораката не соодветствува со пораката или пак е сомнителна и во текстовите има грешки.

Злонамерен софтвер

Малициозен софтвер се однесува на секоја злонамерна програма што предизвикува штета на компјутерски систем или мрежа. Напаѓа компјутер или мрежа во форма на вируси, црви, тројанци и др. Нивната мисија е често насочена кон остварување незаконски задачи како што се крадење податоци, бришење доверливи документи или додавање софтвер без согласност на корисникот.

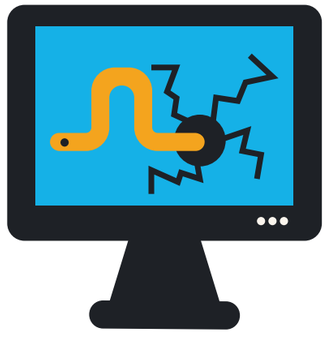
Постојат голем број на програми кои спаѓаат под слонамерен софтвер. Многу често не сме ни свесни дека имаме злонамерен софтвер додека не почне системот да станува спор или да се случуваат чудни работи со него.

Компјутерски Вирус

Вирусите можат да се реплицираат сами, но им треба начин за да се пренесат на друг домаќин. Штетите од вирусот можат да бидат едноставни како нова икона на нашата позадина, па се до исклучување на антивирусот, системски програм или пак бришење и уништување на документи.
Најчесто се пренесуваат преку симнат податок од интернет, електроска пошта или преносен медиум како ЦД и УСБ.

Компјутерски Црв

Црвите се слични како компјутерскиот вирус, со тоа што можат да се реплицираат и слободно да се движат без потреба на некаква помош. Ефектите од црвите се тоа што ги искористуваат компјутерските ресурси како на пример меморијата или процесорската моќ на компјутерот.



Рекламен софтвер - AdWare

AdWare е рекламен програм што се инсталира пропратно со некоја друга апликација без знаење на корисникот. Главната цел е прикажување на pop-up реклами кои што се досадни и нерелевантни за корисникот, како и менување на почетната страница на прелистувачот со некоја сомнителна страна.

Шпионски софтвер - Spyware

Spyware е тип на софтвер кој што има за цел да собира одредени инфомации како на пример: лозинки, историја на посетувани страни, историја на пребарувани работи, контакти, банкарски сметки и друго.
Може да препознаете ако компјутерот или интернет врската почнува да станува спора.

RansomWare

Ransomware е злонамерен софтвер кој што ги енкриптира сите податоци на компјутерот и бара одредена парична сума за да бидат декриптирани тие податоци, во спротивно ќе бидат избришани или никогаш нема да се декриптираат.
Најпознат начин на кој што се шири е преку Фишинг напад или со кликнување на сомнителни линкови и страни.

Заштита

Неколку практики за подобра заштита на нашите уреди:

- На сите уреди кои ги користиме треба да имаме инсталирано **антивирусен софтвер**. Ако користиме Windows оперативен систем, по основа го имаме Windows Defender антивирусот кој е од Microsoft и е бесплатен.
- Да правиме редовно **скенирање** на нашиот уред и нашите податоци.
- Еднаш во месецот да правиме целосно скенирање на уредот.
- Редновно да го **апдејтираме** нашиот оперативен систем.
- Редовно да ги **апдејтираме апликациите** што ги користиме и што ни се инсталирани. Како на пример: Microsoft Teams, Microsoft Office, Firefox, Chrome, Skype и други.
- Да имаме инсталирано на нашиот прелистувач додаток за **блокирање на AdWare реклами.** Добар и бесплатен предлог е **Ad-Blocker Plus** (https://adblockplus.org/).

Што е интернет приватност?

Може да биде возбудливо, збунувачко, па дури и малку страшно искуството во нашиот современ дигитален свет. Кога ги користиме социјалните медиуми, споделуваме повеќе од нашите животи од било кога, и тоа со масовна публика и големи моќни компании. Технологија за препознавање на лицето се користи за отклучување на нашиот телефон, автентикација на нашиот идентитет, читање на нашиот израз за време на интервјуа за работа и следење на нашите движења во јавноста. Интернетот на нештата поврза многу секојдневни уреди со Интернет за да ни го олесни животот, но исто така нè остава ранливи на хакирање и контрола.

Честопати е нејасно кој ги собира нашите лични информации. Какви информации тие собираат, што прават со нашите податоци, со кого ги споделуваат нашите тајни и дали имаме приватност? Нашата приватност е важна затоа што ни дава простор што треба да го развиваме како човечки суштества.

Приватноста ни дава слобода да читаме, учиме и изразуваме без да се грижиме за тоа кој може да гледа. Тоа ни дава можност да ја дадеме нашата доверба во другите, така што ќе можеме да купуваме, да се дружиме, да бидеме интимни едни со други и да формираме социјални врски што ги одржуваат нашите заедници силни, нашата демократија функционира и збогатени нашите животи. На кратко, без приватност не можеме правилно да функционираме како општество или како индивидуи.

Интернет приватност го вклучува правото на личните инфомации во врска со чување, употреба, обезбедување на трети лица и прикажување на лични информации преку интернетот. Приватноста на Интернет е подмножество на приватност на податоците. Загриженоста за приватноста е појавена уште од почетоците на мрежно поврзување на компјутерите.

Закани за приватноста

Контролата над личните информации е секогаш привлечна. Кој не би сакал поголема моќ над работите што имаат влијаат на нашите животи, но со оваа моќ често доаѓа голема обврска.

Ако не ја проверуваме таа контрола, тогаш сме изложени на ризик, компаниите можат да ја преземат нашата неактивност како попустливост, како премолчена согласност. Тоа доведува да мораме да ги прилагодите поставките за приватност на Фејсбук, исто така со Инстаграм, Твитер. Уште со Google, Amazon, Netflix, Snapchat, Microsoft, Siri, Cortana, Viber, Candy Crush, паметниот телевизор, роботот правосмукалка, Wi-Fi-то во автомобил и некој паметен гаџет на нашите деца. Некои мобилни апликации бараат над 200 дозволи? Просекот е околу пет.

Постои една поговорка која вели: ако не плаќаш за продуктот, тогаш ти си продуктот.

Начинот на кој технологиите се направени можат да влијаат на нашата приватност.

- социјалните медиуми се дизајнирани на начин за што повеќе ние споделуваме;
- компании зад социјални медиуми и други корисници ја ризикуваат вашата приватност;
- многу е тешко да се заштити себе си против ризиците на социјалните медиуми.

Толку е лесно да објавите нешто на социјалните мрежи. Секој што сака да користи услуги како Фејсбук, Твитер, или Snapchat може да создаде сметка и започнете да споделувате фотографии за неколку секунди. Буквално, секој елемент на дизајнот на социјалните мрежи е направен за да не натера да споделувате. На пример, лентата со мени за мобилната апликација Фејсбук не беше преместена на дното на екранот за естетика е да се добие тие копчиња поблиску до палците.

Социјалните медиуми можат да дадат чувство на ризик. Всушност неколку закани за што треба да размислиме. Прво, Споделување. Второ, давање согласност. Трето, лоши пријатели.

Со секое споделување ние откриваме само малку повеќе за самите нас. Ефектот е сличен на традиционални поими за надзор, каде со секое набудување на луѓето дознаваме нешто плус. Со тоа што, овој модерен надзор не тера самите да споделиме или да си кажеме

нешто. На пример, во почетокот на 2016 година, Фејсбук воведе серија од нови начини за интеракција со објава. Сега корисниците можат да реагираат со љубовна, смешна, зачудувачка, тажна или пак лута емоција на објавата. Кога ќе ни здосади интеракцијата во апликацијата се префрлуваме на други различни апликации или целосно се одјавуваме, тоа се нарекуваат досадни корисници. Заинтересираните корисници кои продолжуваат да објавуваат или произведуваат податоци се викаат интересни корисници бидејќи со нивното споделување други луѓе стануваат заинтересирани за нивните објави и така во круг.

Сега да се свртиме кон феноменот на давање согласност. Размислете за тоа мало копче што се согласувам или поле за избор што секој корисникот го кликнал како на дел од процесот на регистрација. Се согласуваме на многу постави за приватност во долги и големи текстови што се нарекуваат Услови за употреба. Ние исто така рутински се согласуваме на специфични видови на собирање на податоци од кликнување „Се согласувам“ кога апликациите бара пристап до камерата на нашиот телефон, нашата локација или нашите контакти. Поради тоа кога нешто ќе ни се случи со нашите податоци, не можеме да се жалиме бидејќи сме се согласиле сами. Може да се чувствуваме толку презаситени од илјадници барања за пристап, дозвола, и согласност да ги користиме нашите податоци што ние само велиме да затоа што сме толку изнемоштени. Исто така, триковите за дизајнот можат да нѐ наведат да кликнеме „Се согласувам“ пред да сфатиме што правиме. Копчињата, знаците и распоредот може да се манипулира за случајно да кликнеме, или значењето на важноста да се занемари. Збунувачка формулација, вгнездени менија, и други трикови се користат за да се замаглат механизмите за согласност.

Лошите пријатели се уште еден ризик во социјалните мрежи. Понекогаш пријател е погрешен збор за да ги опишете вашите социјални мрежни врски.

ТРАНСФЕР НА ПОДАТОЦИ

Трансфер на податоци

Компјутерските податоци се информации обработени или зачувани на компјутер. Оваа информација може да биде во форма на текстуални документи, слики, аудио, видео содржина софтверски програми или други видови на податоци. Компјутерските податоци се обработени од процесорот на компјутерот и се чуваат во датотеки и папки на хард дискот на компјутерот.

Пренос на податоци или пренос е секоја информација што се пренесува од една до друга локација преку некој метод на комуникација. На пример, споделување на документ преку интернет или пак некој преносен медиум како УСБ или ЦД.

Податоците можат да се пренесуваат од компјутери преку Интернет со користење на еден од следниве методи. Ако сакаме да пренесеме или испратиме податоци на Интернет, мора да ги прикачиме тие податоци на интернет. Доколку сакаме да примиме податоци од Интернет, тогаш велиме дека тие податоци ги преземаме од интернет. Исто така, можно е да se разменуваат податоци едни од други директно од своите компјутери преку Интернет. Тој начни на комуникација се нарекува peer-to-peer трансфер на податоци.

Опасности при пренос на податоци

Во текнот на целото работење со компјутери ние работиме со инфомации и податоци. Постојат голем број на опасности при трансфер на податоци, најчестите се следниве:

- Симнување или превземање на податоци од интернет
- Треба да бидеме сигурни дека од страната каде што ги симнуваме податоците се безбедни, пример ако симнуваме Microsoft Teams софтвер треба да бидеме сигурни дека го симнуваме од официјалната страна на Microsoft. Најдобро е секој симнат податок да биде скениран од страна на Антивирусот на нашиот компјутер. Скенирањето е особено важно ако користиме торент за превземање на податоци.
- Примање на податоци преку електронска пошта
- Најризични податоци на кои може да се прикачи злонамерен софтвер се Word документите (.docx), PDF документите (.pdf), софтвер (.exe) и зипувани или компресирани податоци (.zip). Секој документ на мејл што сме го добиле треба да биде скениран.
- Трансфер од преносни медиуми
- Секогаш кога ќе поврземе УСБ или вчитаме ЦД во нашиот компјутер треба да биде скенирано.

Враќање на избришани податоци

Често пати се случува да избришеме некои податоци по грешка или пак некој злонамерен софтвер ни ги избришал податоците. По некогаш постои можност да можеме да ги вратиме тие избришани податоци со помош на алатки за враќање на податоци.

Постојат голем број бесплатни и платени алатки, еден таков пример е Recuva (https://www.ccleaner.com/recuva) софтверот. Пред да пробаме да ги вратиме податоците, мора прво да го разбереме концептот како избришан податок може некогаш да се врати, а некогаш не. Кога бришеме податок на Windows ние само го бришеме индексот на тој податок, и нашиот оперативен систем не може да покажува повеќе кон него, но податокот е сеуште на хард дискот. Се додека тој податок не биде пребришан односно не биде зачуван друг податок на истата таа локација, имаме шанса да го вратиме тој избришан или изгубен податок.

САЈБЕР НАСИЛСТВО

Сајбер насилство

Во пракса, актите на сајбер насилство може да вклучуваат различни видови на вознемирување, нарушување на приватноста, сексуално злоставување и сексуално искористување и кривични дела за пристрасност против социјални групи или заедници.

Сајбер насилството исто така може да вклучува директни закани или физичко насилство, како и различни форми на компјутерски криминал.

Сајбер насилство се дели на:

- Cyberbullying и cyberharassment – Сајбер булинг и онлајн малтретирање
- Cyberstalking – Онлајн следење / демнеење
- Повреда на онлајн приватноста и говор на омрза
- Сексуална експлоатација и сексуална злоупотреба на деца преку Интернет
- Cyberthreats – Онлајн закани и Cybercriminal – Компјутерски криминал

Сајбер малтретирањето е можеби најширо ката форма на сајбер насилство и вклучува постојан и повторен курс на однесување насочен и наменет кон одредена личност, што предизвикува сериозен емоционален стрес и често страв од физичко оштетување.

Онлајн следење или демнеење е употреба на Интернет или други електронски средства за следење или малтретирање на поединец, група или организација. Може да вклучува лажни обвинувања и клевети. Може, исто така, да вклучува следење, кражба на идентитет, закани, вандализам, барање за секс или собирање информации што можат да се користат за закана, засрамување или малтретирање.

Многу форми на сајбер насилство претставуваат или се поврзани со **кршење на приватноста** на жртвите. Ова може да вклучува компјутерски упади за добивање, крадење, откривање или манипулирање со интимни податоци, истражување и емитување на лични податоци („доксинг“) или дела како што се онлајн следење / демнеење или„ revenge porn “.

Сексуална експлоатација и сексуална злоупотреба на деца преку Интернет

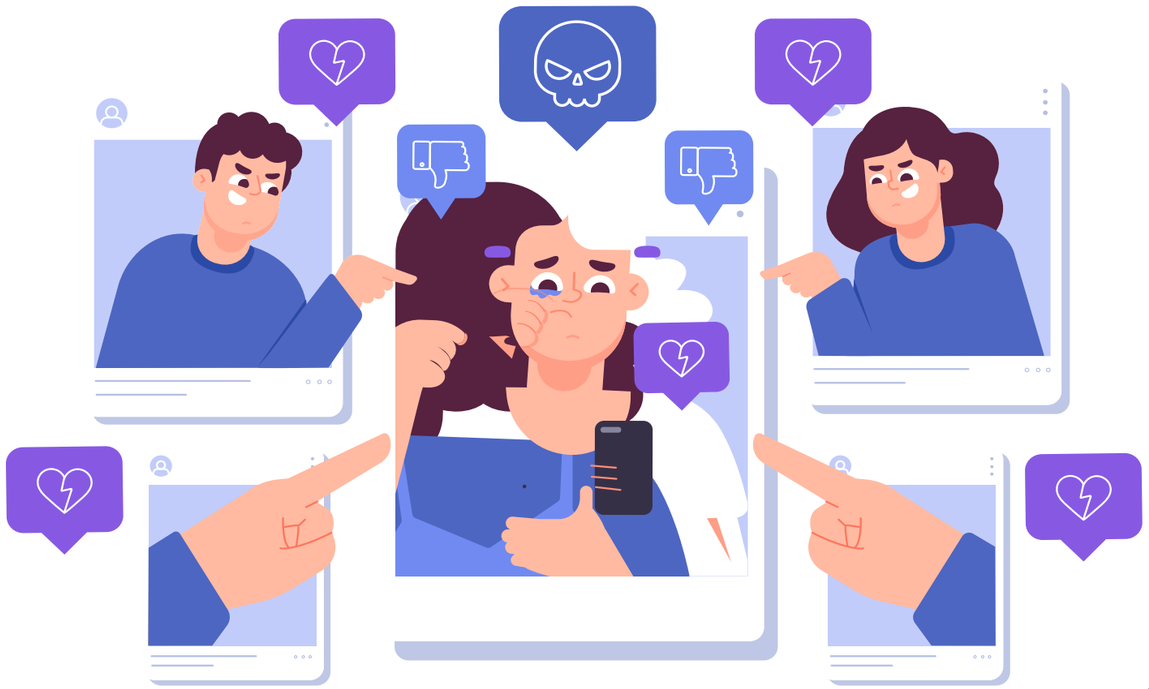
Децата се чини дека претставуваат примарна група на жртви на сајбер насилство, особено во однос на сексуалното насилство преку Интернет. И покрај тоа што „Интернет сексуалната експлоатација и сексуалната

злоупотреба на деца“ не се нужно нови и изразени форми на сексуална експлоатација и сексуално злоставување на деца, Интернетот ја зголемува достапноста до децата од страна на лица кои бараат сексуална злоупотреба и ги експлоатираат.
Интернетот го олеснуваат споделувањето на слики и видеа од сексуална злоупотреба и со тоа да се зајакне долготрајното штетно влијание од злоупотреба на деца.

Онлајн закани и Компјутерски криминал

Сајбер насилството опфаќа и директни закани за насилство или директно физичко насилство. Компјутерски системи може да се користат во врска со убиства, киднапирања, силувања и други дела на сексуално насилство или изнуда. Земајќи ја предвид дефинираната погоре дефиниција, некои форми на компјутерски криминал исто така може да се сметаат за акти на сајбер насилство, како што се нелегален пристап до интимни лични податоци, уништување на податоци, блокирање пристап до компјутерски систем или податоци, итн.

Сè уште нема стабилна лексика или типологија на прекршоци што се сметаат за сајбер насилство, и многу од примерите на видови на сајбер насилство се меѓусебно поврзани или се преклопуваат или се состојат од комбинација на дела. Не сите форми или случаи на сајбер насилство се подеднакво сериозни и не сите нужно бараат кривично-правно решение, но може да се решат со оценет пристап и комбинација на превентивни, едукативни, заштитни и други мерки.



Интернет вознемирување / малтретирање

Децата на кои им е дозволено да користат мобилни телефони, таблети и лаптопи со Интернет-врска многу брзо можат да научат како да ги користат ефикасно. Може дури се чини дека тие постепено стануваат неразделни од нивниот уред. Сосема е природно да користат виртуелни алатки и тие ги разбираат принципите на мрежата далеку подобро од повеќето возрасни се додека користат Интернет за корисни цели, како што се пребарување информации, учење и играње. Поголемиот дел од времето, се случува потемната страна на детската природа да биде разголена во виртуелниот свет.

Кога станува збор за малтретирање на нивните врсници, младите искористуваат апсолутно сè што Интернетот може да им понуди. Доволнен е еден истрел. Совршено спроведената социјална кампања на УНИЦЕФ, вели дека малтретирањето преку Интернет претставува една од главните причини за депресија и самоубиство кај децата на училиште. Ако имате паметен телефон, користете го мудро. Не убивај никого.

За момент, ќе научите неколку основни методи што ги користат младите агресори на Интернет. Можеби благодарение на нив, ќе можете подетално да го разгледате виртуелното однесување на вашиот ученик или дете и да забележите некои алармантни шеми.

Следење

Ситуацијата кога едно дете следи некого на Интернет подолго време, го нарушува неговиот живот и комуницира со него на начин на кој лицето се плаши од неговиот мир и безбедност, родителите многу често ја банализираат оваа рабора. Демнеење или следењето во реалниот живот бара многу напор и вклученост од угнетувачот. Сепак, следењето на Интернет поради неговата заедничка и релативна смисла, стана омилен медиум на следачи. Овој вид агресија многу често се јавува помеѓу луѓе кои се познаваат, се познавале во минатото или биле дури и во блиски односи.

Расправија преку интернет

Flaming или roasting е агресивна размена на ставови помеѓу неколку луѓе, што обично се спроведува јавно во простории за разговор или во рамките на групите за дискусија. Феноменот е само непријатен, но прилично чест. Може да има посериозни последици кога ќе се трансформира во малтретирање. Случаен разговор за спортски тимови, омилени брендови за автомобили или

компјутерски игри еволуира во низа навреди и напади, малтретирање, вознемирувањето се заснова на испраќање на агресивни, омаловажувачки, навредливи, честопати вулгарни пораки до жртвата преку електронските средства за комуникација редовно.Мобилен телефон, социјална мрежа или систем за разговор во онлајн игра се користи во вакви ситуации. Но, понекогаш се случува агресијата брзо да ескалира и да прерасне во испраќање сериозни закани кон жртвата.

Лажно претставување

Еден од главните мотиви на крадец на идентитет е да се имитира својата жртва во сајбер просторот. Користењето слаби лозинки за е-пошта или за инстант чет често го олеснува дејството на крадецот. И иако не ги објаснува мотивите на агресорите, добро е да бидете свесни за фактот дека крадец на идентитет може да предизвика многу проблеми на неговата или нејзината жртва со испраќање на дискредитативни пораки до други ученици и наставници.
Видеа или фотографии можат веднаш да бидат јавно достапни или да стигнат до луѓе кои дефинитивно не треба да имаат пристап до нив. Исто така, се случува пред материјалите да станат вирални или популарни, крадецот го уценува сопственикот, барајќи да ги исполни сопствените очекувања, како што е изложување на жртвата пред Интернет камера или плаќање на еден вид откуп.

Мултимедијални содржини – happy slapping

Тоа е само уште еден начин да се здобијат со материјали за дискредитација дури и позлобни од претходните. Целта е да се предизвика и испровоцира напад, жртвата да го направи самиот напад и притоа да биде снимена или сликана од страна на злонамерникот. Тогаш сè се одржува исто како и во другите примери на компјутерско малтретирање. Материјалот станува вирален или жртвата е уценета од заканите за нивно оцрнување при објавувањето. Оваа форма на агресивно однесување се заснова на објавување лажни информации или материјали за некои луѓе. Овие можат да бидат обични гласини за жртвите, учество во некои срамни настани. Тоа често се изменети филмови или фотографии кои сугерираат дека жртвата извршува некакви дејствија.

Социјално исклучување

Отстранување на некого намерно од список на контакти, група за дискусија или разговор предводен од група пријатели резултира во исклучување на жртвата од група врсници. Често е една од формите на релационистичко малтретирање.

Техничка агресија

Оваа форма на напад бара малку повеќе техничко знаење. Сепак, не дозволувајте да ве смири. Деновиве, децата знаат повеќе за електронските уреди отколку што може да изгледа. Техничка агресија е напад врз компјутерот што го користи жртвата, неговиот или нејзиниот компјутерски софтвер или веб-страница. Тоа вклучува испраќање компјутерски вируси или хакерски активности како што е Бомбинг напад преку пошта, што испраќа огромен број пораки на сметка на жртвата каде целта е да го наруши функционирање на е-пошта или обид за напад на компјутерот на жртвата испраќајќи одредени сомнителни линкови, фајлови или пораки.

Социјалните мрежи и видео игрите

Дигиталните медиуми и апликациите им овозможуваат на децата да комуницираат и да ја изразат својата креативност, да се поврзат со врсниците и да ги споделат своите чувства. Сепак, тие можат да бидат авенија преку која се јавува компјутерско малтретирање.

Постојат многу видови на апликации и страници достапни бесплатно кои им даваат на корисниците можност да бараат луѓе и да споделуваат или објавуваат информации за нив анонимно. Родителите можеби не се свесни за апликациите што нивните деца ги користат редовно или не се свесни за ризиците вклучени во нивната употреба.

Постојат многу начини на кои компјутерското малтретирање може да се скрие во апликациите и страниците, како што се текстови, видеа и веб-повици што исчезнуваат или не се појавуваат на дневниците за повици или текстуални пораки на уредот. Многу апликации, исто така, им овозможуваат на корисниците лесен пристап, прегледување или учество во содржина за возрасни или штетна содржина.

Прилагодувањата за приватност и локација може да ги направат поранливи на следење, мрежно малтретирање, изложеност на содржина за возрасни или други опасности.
Некои тековни популарни места и апликации за социјални медиуми вклучуваат:

- **Discord**: Апликација што им овозможува на корисниците видео разговор со други, приватна порака и придружување, креирање или учество во јавни и приватни простории за разговор. Оваа апликација често ја користат плеерите за да разговараат едни со други додека играте видео игри.
- **Facebook**: Најчесто користената страница за социјални медиуми што

е достапна на многу различни медиумски платформи.

- **Instagram**: Интернет-страница за споделување фотографии и видео што ги поврзува корисниците преку други страници за социјално вмрежување (на пример, Фејсбук).
- **Snapchat**: Апликација за пораки со фотографии што овозможува споделување слики и кратки видеа што се наменети да се избришат кратко по породувањето.
- **Telegram**: Апликација за пораки што им овозможува на корисниците да споделуваат фотографии, видеа и датотеки; остварете повици и избришете текстови или разговори од телефонот на примателот користејќи тајмер.
- **TikTok**: Апликација што им овозможува на корисниците да создаваат и споделуваат свои видеа каде што се синхронизираат, пеат, танцуваат или само зборуваат.
- **WhatsApp**: Апликација за приватни пораки што им овозможува на корисниците да пишуваат пораки, да испраќаат фотографии, видеа и информации за локацијата до нивните контакти.
- **YouTube**: Платформа за споделување видео што им овозможува на корисниците да објавуваат и споделуваат видеа.

Социјалните медиуми имаат многу придобивки кои мора да се балансираат со ризиците што ги претставуваат. Ризиците за кои треба да бидете свесни вклучуваат:
Објавената содржина може да биде неточна, штетна или невистинита.
Може да се користи за споделување штетни содржини или содржини за возрасни.

Контролите за приватност за тоа кој може да гледа или пристапува до објавениот материјал се разликуваат од апликациите, а многу корисници не се свесни како да ги користат ефективно.

Апликациите што овозможуваат видеа од корисниците во реално време „во живо“ може да се користат за да се прикаже малтретирање, насилство, самоубиство и штетни дела додека се случуваат.

Некои апликации што вклучуваат информации за локација може да се користат за добивање лични информации, како што се нечија возраст, моментална локација или местото каде што живее некој.

Апликациите што поддржуваат телефонски повици не се појавуваат во дневникот за повици, па родителите можеби не знаат со кого разговараат нивните деца.

Играњето видео игри е популарна активност, со 90 проценти

од тинејџерите кои играат игри на Интернет. Многу видео игри - без разлика дали се на компјутер, конзола за игри, мобилен телефон или таблет - им овозможуваат на корисниците да си играат со пријатели што ги познаваат лично и други што ги запознале само преку Интернет.

Иако гејмингот може да има позитивни придобивки како што се стекнување нови пријатели, дружење и учење како да стратегирате и да ги решите проблемите, тоа е исто така друго место каде се јавува сајбер-малтретирање.Анонимноста на играчите и употребата на аватари им овозможуваат на корисниците да создадат алтер-его или измислени верзии за себе, што е дел од забавата на игрите.

Но, тоа исто така им овозможува на корисниците да малтретираат, а понекогаш и да групираат со други играчи, испраќајќи или објавувајќи негативни или штетни пораки и користејќи ја играта како алатка за вознемирување. Ако некој не е толку добар во играта, другите деца можат да исмеваат или да дадат негативни забелешки што се претвораат во малтретирање, или може да го исклучат лицето од играње заедно.

Бидејќи играчите се анонимни, тие не можат нужно да одговараат за нивното однесување, а нивното вознемирување може да предизвика некои играчи да ги напуштат игрите. Некои анонимни корисници ја користат играта како средство за малтретирање странци или за добивање на нивните лични информации, како што се кориснички имиња и лозинки.

Заштита и препознавање

Родителите, наставниците и другите возрасни можеби не се свесни за сите платформи и апликации на социјалните медиуми што ги користи детето. Колку повеќе дигитални платформи користи детето, толку повеќе можности има да се изложи на потенцијално малтретирање преку Интернет.

Многу од предупредувачките знаци дека се случува малтретирање преку Интернет се случуваат околу употребата на нивниот уред од страна на детето. Бидејќи децата поминуваат многу време на своите уреди, зголемувањето или намалувањето на употребата може да биде помалку забележливо.

Важно е да се обрне внимание кога детето покажува ненадејни промени во дигиталното и социјалното однесување. Некои од предупредувачките знаци дека детето може да биде вклучено во онлајн малтретирање се:

- Забележливо, брзо зголемување или намалување на употребата на уредот, вклучително и испраќање пораки.
- Детето изложува емоционални одговори (смеа, лутина, вознемиреност) на она што се случува на нивниот уред.
- Детето го крие својот екран или уред кога другите се близу и избегнува дискусија за тоа што прават на својот уред.
- Детето почнува да ги избегнува социјалните ситуации, дури и оние во кои се уживало во минатото.
- Детето станува повлечено или депресивно или губи интерес за луѓе и активности.

Постојат работи што возрасните можат да ги направат за да спречат компјутерско малтретирање на деца кои играат игри:

- Играјте ја играта или набудувајте кога се игра играта да разбере како работи и на што е изложено дете во играта.
- Периодично проверувајте со вашето дете за тоа кој е на Интернет, играјќи ја играта со нив.
- Научете ги вашите деца за безбедно однесување на Интернет, вклучително и да не кликнете на врски од странци, да не споделувате лични информации, да не учествувате во однесување на малтретирање на други играчи и што да прават ако забележат или доживеат малтретирање.
- Воспоставете правила за тоа колку време детето може да помине играјќи видео игри.
- Наставниците, педагозите се наоѓаат во единствени позиции да ги користат своите вештини и улоги за да создадат безбедни средини со позитивни социјални норми.

Вие исто така се наоѓате на позиција каде што можете да забележите промени во однесувањето на децата во групните поставки, како група или кластери на деца се фокусираат на друго дете или други знаци дека може да се случи малтретирање преку Интернет.

Постојат работи што можете да ги направите во училницата или во другите поставувања на групата за да препознаете или спречите онлајн малтретирање.

- Ако мислите дека детето е малтретирано преку Интернет, разговарајте со него приватно за да прашате за тоа. Тие исто така може да имаат доказ на нивните дигитални уреди.
- Ако верувате дека дете е малтретирано преку Интернет, зборувајте со родител за тоа. Служете како олеснувач помеѓу детето, родителот и училиштето доколку е потребно.
- За да го разберете дигиталното однесување на децата и како се однесува онлајн малтретирањето, зголемете ја вашата дигитална свест.
- Развијте активности што поттикнуваат саморефлексија, барајќи од децата да го идентификуваат и изразат она што го мислат и чувствуваат и да ги земат предвид мислите и чувствата на другите.
- Помогнете им на децата да развијат емоционална интелигенција за да можат да научат вештини за самосвест и саморегулација и да научат како да имаат емпатија кон другите.

ДИГИТАЛЕН ОТПЕЧАТОК

Дигитален отпечаток

Дигиталните отпечатоци се записи и траги што ги оставаме зад нас додека користиме Интернет. Нашиот сопствен дигитален отпечаток може да придонесе за нашата репутација на Интернет. Може да значи дека не мора постојано да се најавуваме или да доставуваме лични детали до веб-страниците. Од друга страна, нашите дигитални отепечатоци може да им овозможат на другите да ги следат нашите постапки, како што се веб-страници што ги користиме, кои работи ги бараме и кој е во вашиот социјален круг.

Нашите дигитални отпечатоци се видливи за организации со кои немаме никаква врска и над кои често немаме контрола. Многу организации работат и зад сцената за да градат профили за нас врз основа на нашите дигитални отпечатоци. Повеќето луѓе се свесни дека кога споделуваат информации за себе на Интернет, како на пример на социјалните медиуми и кога користат услуги преку Интернет, како што се електронска пошта, размена на инстант пораки или говорни повици, тие се откажале од одредена контрола над нивната приватност.

Дали е можно некој да нè следи во виртуелниот свет на Интернетот, следејќи ги нашите дигитални отпечатоци, трагајќи по впечатоците што ги оставаме? Одговорот е „да“.

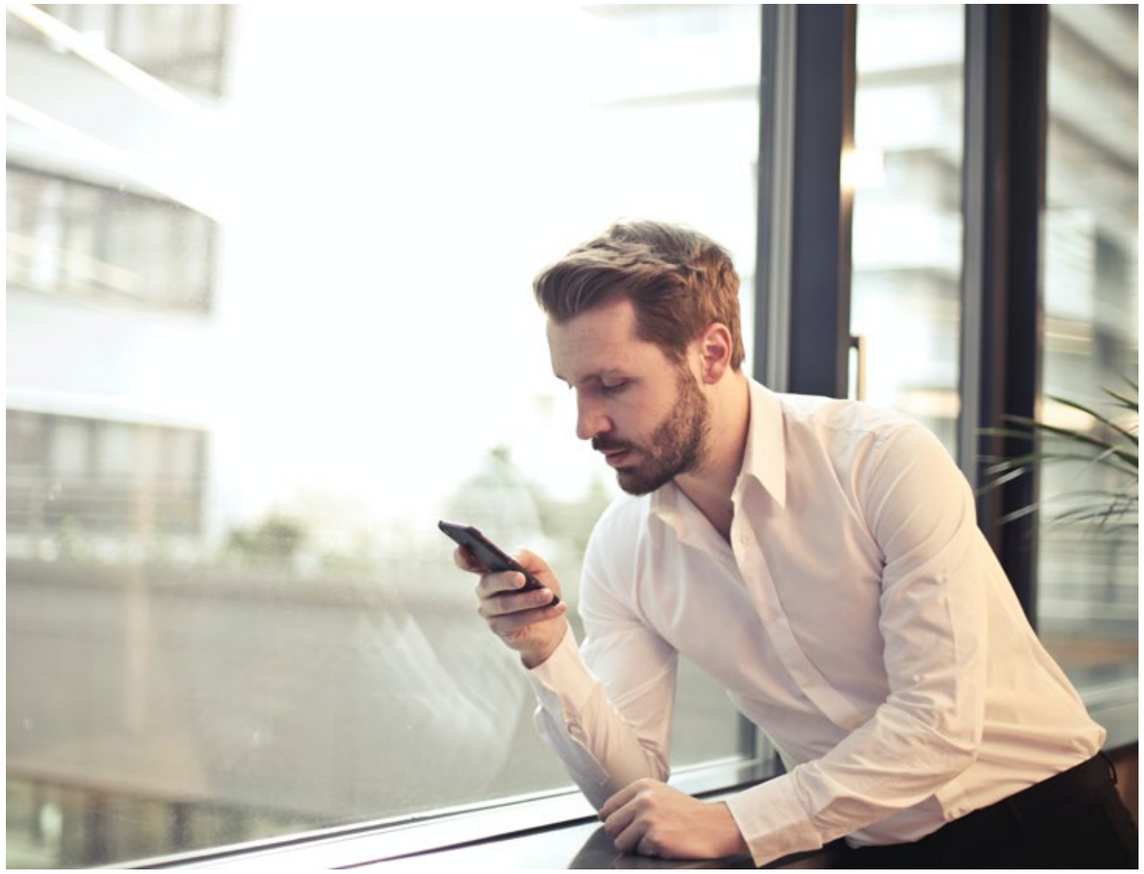
Нашите дигитални отпечатоци се поголеми отколку што можеме да претпоставуваме, и тие се користат - обично за комерцијални цели, но понекогаш и од други причини - за да не следат, да се прилагодуваат за нас и да ни прикажат релевантни реклами. Овие активности се првенствено во корист на засегнатата организација. На кратко, нашиот дигитален отпечаток е монетизиран ... но секоја директна добивка обично не доаѓа кај нас, поединецот.

Нашите посети на различни даватели на услуги генерираат податоци за нас што се собираат на секоја локација. Давателите на услуги и други трети страни разменуваат податоци за профилите на клиентите и статистичките податоци за трансакциите.

Видови на дигитални отпечатоци

Паметните телефони и таблетите имаат тенденција да остават многу различен диитален отпечаток од лаптопите и десктоп компјутерите. Современите паметни телефони работат на начини што создаваат поинтезивен отпечаток.

Апликациите се поврзуваат директно со Интернет услуги користејќи специфични интерфејси. Контролата над испраќањето на информациите до другите услуги / уреди лежи во рацете на развивачот на апликацијата и е изложена на крајниот корисник само до степенот до кој дозволува развивачот. Особено мобилните уреди, исто така, им



даваат на корисниците помала можност за анонимно поврзување.

Паметните телефони обично се свесни за локацијата. Ова им овозможува на апликациите да ги означуваат вашите активности на вашата локација. Услугите за локација честопати се овозможени стандардно или се вклучени во пакет дозволи што од корисникот се бара да ги додели кога е инсталирана апликација.

Податоците за локацијата може да се споделат експлицитно, ако апликацијата ги земе вашите податоци за локацијата и ги испраќа до Интернет-услугата, или имплицитно - на пример, ако на сликите и видеата што ги поставувате била обележани локацијата, датумот и времето кога биле земени. Се смета дека 4-6 ставки од податоците за локацијата се доволни за уникатно да се идентификува секој даден корисник.

Продавачите на паметни телефони, генерално, спроведуваат контроли за тоа дали се споделуваат податоци за локацијата и да блокираат употреба на идентификатори специфични за уредот од страна на апликациите. Ова не е нешто над кое корисникот има контрола Сепак, некои контроли врз чувствителните информации се засноваат на поставките на ниво на уредот, а други на ниво на апликација.

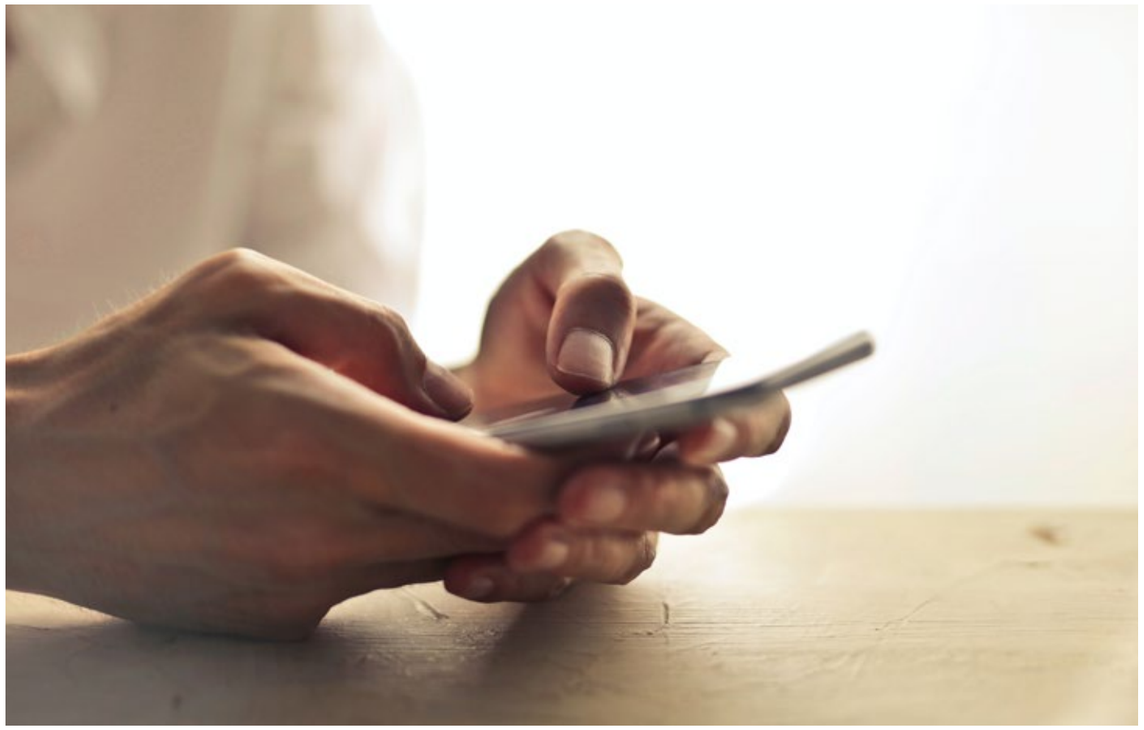
Овие можности значително се разликуваат според платформата

за паметни телефони; исто така, нивото на кое се документирани и леснотијата со која просечниот корисник може да ги открие и управува со нив.

Но, штом корисникот започне да прави означени слики или ќе и даде дозвола на новоинсталираната апликација да ги види информациите за локацијата, дозволата дадена на апликацијата ретко се прегледува.

Корисниците на десктоп компјутери и лаптопи првенствено остават стапала преку нивниот веб прелистувач. Стандардниот веб прелистувач е многу различен од апликациите што ги користат паметните телефони и таблетитеКомпаративно зрелите контроли што ги нудат прелистувачите, или дополнителни приклучоци, му овозможуваат на крајниот корисник полесно да контролира што е споделено и да расчисти идентификување на информации, како што се колачиња, што инаку може да ја намали личната приватност. Така да, десктоп компјутерите имаат предност во однос на приватноста во однос на паметните телефони.

Задачата за внимателно следење и контрола на приватноста претставува значителен режим и може да биде покомплексна отколку што очекуваат многу корисници на паметни телефони. Предизвик за сите нас, како потрошувачи и корисници, е да ја препознаеме вредноста на нашите лични информации и нашата приватност: само со прилагодување на нашите вредности и, како резултат, на нашето однесување, можеме да се надеваме дека ќе донесеме подобри, одржливи одлуки за приватноста.



Контрола врз дигиталниот отпечаток

Треба да се бориме против сопствената инерција, соочувајќи се со практичните стандарди што ја уништуваат приватноста и против заедничките, упорни напори на организациите кои имаат финансиски интерес да нè убедат да ја жртвуваме нашата приватност во интерес на нивниот профит. Веројатно имаме само ограничено време и енергија да посветиме на она што изгледа како случајна задача, додека организациите и компаниите го прават тоа како нивна работа и тие се прилично добри во тоа.

Како можеме да управувате со нашиот дигитален отпечаток? Еве неколку практики за почеток:

- Да се пребараме самите: да погледнеме што има таму. Да го пребаруваме нашето име на неколку месеци, за да бидеме запознаени со информациите до кои другите имаат пристап.
- Да ги заштитиме нашите лични податоци: Не откривајте ја својата лична адреса, телефонски број, лозинки или броеви на банкарски картички. Да размислиме за користитење на прекар наместо вашето вистинско име.
- Проверка и подесување на поставките за приватност на апликациите и сервисите што ги кориситиме.
- Да ги чуваме информациите за најавување под клуч: Никогаш да не споделуваме со никого од нашите кориснички имиња или лозинки.
- Да размислиме пред да објавиме: Никогаш да не ставаме привремена емоција на постојан интернет. Бесот е привремен; Интернет трае засекогаш. Да размислиме двапати, и да објавиме еднаш.
- Секоја фотографија што ја објавуваме може да се ископа некој ден. Да го ограничиме споделувањето сомнителни слики. Петнаесет минути хумор никогаш не вреди за цел живот потенцијално понижување.

Сега кога знаеме што е дигитален отпечаток, треба да преземеме соодветни чекори за да го одржуваме тој отпечаток. Дигиталниот свет нема да оди никаде во скоро време - затоа, треба да рзмислуваме на тоа како цел живот. Да ја искористиме платформата за да се претставиме во најдобро светло и да ги покажаме нашите најдобри квалитети. На крајот на краиштата, никогаш не знаеме кој ќе не бара во нашата новооткриена дигитална економија.

Сите мултимедијални елементи што се искористени во брошурата се под Creative Common лиценцата и се превземни од:

Ploup Design, Anna, Custom Icon Design, Sergio Sánchez López, Iconshock, Jojo Mendoza, PC Unleashed, iconic Hub, Kmg Design, kaboompics, Pexels, Glenn Carstens-Peters, Markus Winkler, Ben Sweet, Alex, Iby, Iulia Mihailov, Anete Lusina, Pixabay, Andrea Piacquadio, buffaloboy, vectoru juice, kraifreedom_studio16, rawpixel.com, fullvector, Lisa Fotios, Tyler Lastovich, Giftpundits.com, Tracy Le Blanc, Anete Lusina, Mateusz Dach, energepic.com, Omkar Patyane, fauxels, picjumbo.com, freestocks.org, RODNAE Productions, Keira Burton, Alexander Shatov, Eaters Collective, bruce mars, Markus Spiske, Lucie Liz, Alexander Kovalev, Jessica Lewis, Julia M Cameron, Tima, Miroshnichenko, geralt, Flatart, Tristan Hennrich, ThisIsEngineering, NASA, Element5 Digital, Mike, Mati Mango, Webdesigner Depot, Gakuseisean, Webalys LLC, Oliver Scholtz (and others), Icon Arts, Deleket, Susumu Yoshida, Tinti Nodarse, Iconfinder, HeungSoon, Patrick Lindenberg, Massimo Botturi.

Од следните страни:
https://www.iconfinder.com/
https://www.pexels.com/
https://pixabay.com/
https://unsplash.com/
https://www.slidescarnival.com/
https://www.freepik.com/

techsoup EUROPE

METAMORPHOSIS

Foundation for sustainable ICT solutions