MANUAL PËR SIGURINË DIGJITALE

2021

Manuali u realizua me mbështetjen e:

techsoup EUROPE

METAMORPHOSIS
Foundation for sustainable ICT solutions

Manual për sigurinë digjitale për ar-simtarët e shkollës fillore dhe të mesme

Përmbajtja

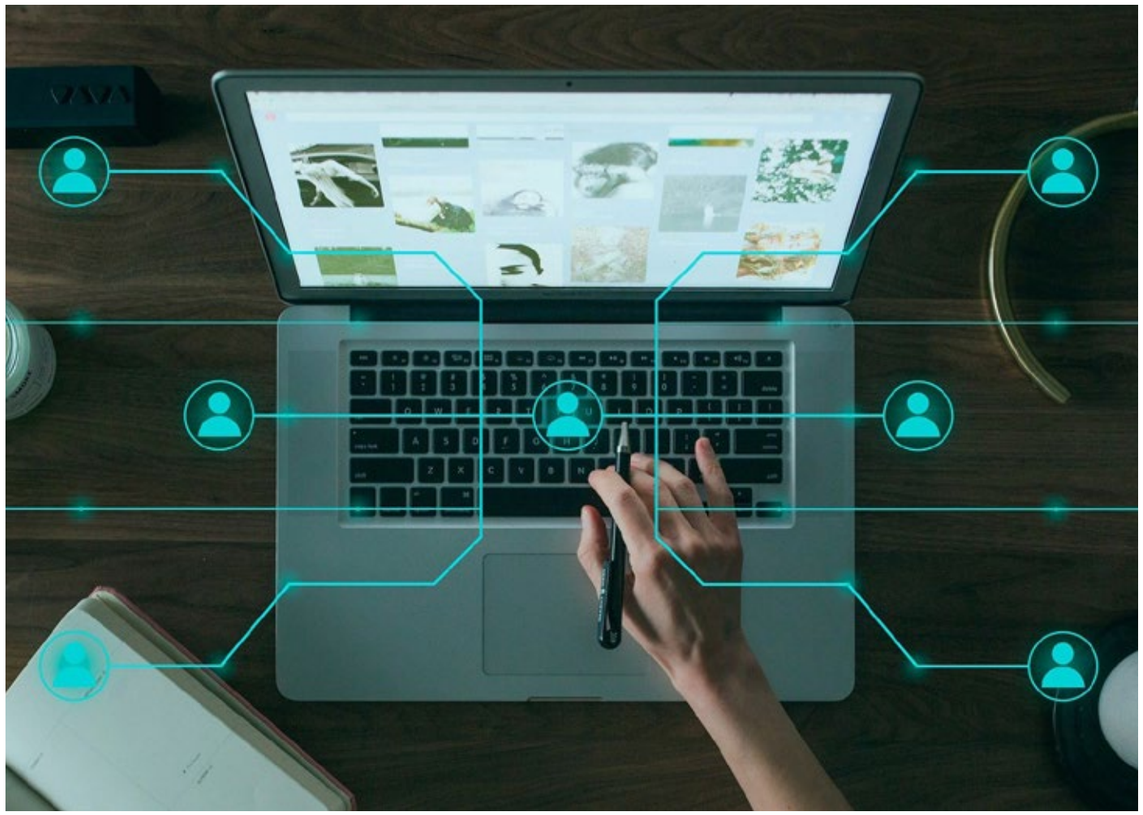
Hyrje

Ne jetojmë në një kohë kur një pjesë e madhe e jetëve tona, personale dhe profesionale, përfshihen në botën digjitale të Internetit. Ne bëjmë veprimet tona bankare, blerjet, pagimin e faturave, planifikimin shoqëror, madje edhe pjesë të punës sonë në botën digjitale. Kjo mbështetje e shtuar në internet dhe pajisjet digjitale mbart rreziqe së bashku me komoditetin që ju ofron.

SIGURIA DIGJITALE

Çfarë është siguria digjitale?

- Siguria digjitale paraqet siguri logjike dhe fizike të pajisjeve digjitale.
- Siguria e aplikacioneve të cilat i përdorim, si dhe informacionet dhe të dhënat në to.
- Siguria e rrjetit në varësi se në cilin rrjet jemi të lidhur: Të shtëpisë / Të kompanisë / Rrjet publik
- Siguria gjatë kohës në të cilën jemi të lidhur me internet
- Siguria gjatë operimit
- Edukimi i përdoruesit të fundit.



Siguria Fizike

Siguria fizike paraqet sigurinë e vetë pajisjes, si dhe qasjen fizike në të. Në thelbin e saj, siguria fizike është mbajtja e objekteve, njerëzve dhe pasurive tuaja të sigurta nga kërcënimet reale. Kjo përfshin zbulimin fizik të ndërhyrësve, mbrojtjen nga katastrofat natyrore dhe reagimin ndaj këtyre kërcënimeve.

Sulmet fizike mund të jenë ndërhyrje në një qendër të sigurt të të dhënave ose depërtim në zona të kufizuara të një ndërtese. Sulmuesit mund të vjedhin ose dëmtojnë pajisje të rëndësishme IT, të tilla si servera, laptopë, pajisje telefoni, të fitojnë qasje në terminale të rëndësishme, të vjedhin informacione përmes USB ose të dërgojnë malware në pajisjet tuaja.

Praktikat për siguri më të madhe fizike:

- • Të gjitha pajisjet digjitale duhet të kenë një lloj regjimi mbrojtjeje ose mënyre mbylljeje. Për shembull, pajisja e telefonit duhet të zhbllokohet duke futur një fjalëkalim ose PIN.

- Sa herë që largohemi nga vendi ynë i punës, pajisja jonë duhet të jetë e kyçur. Përndryshe, nëse përdorim një sistem operativ Windows, shtypja e tastit Windows dhe tastit L do të mbyllë kompjuterin tonë, në fakt do të shfaqet një ekran për t'u kyçur. Për sa kohë që nuk jemi afër hapësirës sonë ku punojmë ose pajisjeve tona, ato duhet të jenë të kyçura.

  Që nga kthimi në punë, bëni një kontroll të vogël në portat USB të pajisjes dhe nëse diçka është zhvendosur.

• Tryeza jonë e punës duhet të jetë e pastër, pa rrëmujë ose shënime ngjitëse me fjalëkalime, informacione përdoruesi ose informacione që mund të ndihmojnë të gjejnë fjalëkalimet tona. Kjo praktikë njihet gjithashtu si "Politika e pastrimit të tryezës".

• Avantazhi i pajisjeve telefoni është se ato të gjitha mbështesin një mekanizëm të përcjelljes së vendndodhjes. Kjo është e dobishme nëse është e aktivizuar, sepse kur pajisja jonë humbet ose vidhet, ne mund ta lokalizojmë dhe ta gjejmë më lehtë.

Fjalëkalimet

Një **fjalëkalim** është një sekret i memorizuar, zakonisht një varg karakteresh (shkronja, numra, karaktere speciale) që përdoren zakonisht për të verifikuar identitetin e një përdoruesi. Në ditët e sotme, shumë aplikacione, pajisje, faqe në internet dhe platforma nuk na detyrojnë të kemi një llogari dhe fjalëkalim.

Praktikat për fjalëkalime të sigurta:

• Fjalëkalimi duhet të jetë sa më i gjatë me karaktere, dmth të paktën 8 karaktere.
• Të jetë sa më kompleks që është e mundur, pra të përmbajë një kombinim të shkronjave të mëdha dhe të vogla, numrave dhe karaktereve speciale.
• Fjalëkalimi duhet të jetë diçka që nuk ka lidhje me përdoruesin, për të qenë e vështirë të qëllohet.
• Nëse aplikacioni ose shërbimi ka dy mundësi për autentikim, të dy duhet të përdoren. Për shembull, Facebook na mundëson që nga momenti kur ne do të shënojmë informacionet si emri i përdoruesit dhe fjalëkalimi, të na dërgojë kod nëpërmjet një SMS të cilin duhet ta shënojmë që të futemi ne Facebook.
• Nëse kemi një numër të madh të fjalëkalimeve dhe shërbimeve që përdorim, është e dëshirueshme që të gjithë të kenë fjalëkalime të ndryshme.
• Nëse ruajmë fjalëkalime në shfletues si Firefox ose Chrome, përdorni tiparin e Fjalëkalimit Primar / Master. Kur në çdo sesion, përndryshe duke përdorur shfletuesin, do të duhet të fusim Primar / Master (fjalëkalimin kryesor) në mënyrë që të jemi në gjendje të përdorim fjalëkalimet e ruajtura.
• Ndryshimi i rregullt i fjalëkalimeve, në një periudhë të caktuar kohe rekomandohet të ndryshoni fjalëkalimin.

Shembull për fjalëkalim të ”fortë” është kjo: **0va-e-J@KA_l0zink@**

Shfletimi Web

Çdo ditë ne vizitojmë një numër të madh faqesh në internet, të cilat i përdorim për leximin e lajmeve, kërkimin e informacionit, rrjeteve sociale dhe të tjera. Çdo faqe në internet përdor një protokoll komunikimi, është shumë e rëndësishme të dini se cilat faqe në internet përdorin një protokoll të sigurtë dhe cilat faqe janë të sigurta për tu vizituar.

HTTP mundëson komunikimin ndërmjet sistemeve të ndryshme. Zakonisht përdoret për të transferuar të dhëna nga një server në një shfletues në mënyrë që të lejojë përdoruesit të shfletojnë faqet e internetit.

Problemi me protokollet e rregullta **HTTP** është se informacioni që rrjedh nga serveri në shfletues nuk është i koduar, që do të thotë se mund të vidhet lehtësisht. Protokollet HTTPS e rregullojnë këtë duke përdorur një certifikatë SSL, e cila ndihmon në krijimin e një lidhjeje të sigurt të koduar midis serverit dhe shfletuesit, duke mbrojtur kështu informacionin potencialisht të ndjeshëm nga vjedhja pasi transmetohet midis serverit dhe shfletuesit.

HTTPS është veçanërisht i rëndësishëm për faqet e internetit ku ne fusim llogari përdoruesi, fjalëkalime dhe karta krediti.

Shtesa të tjera që mund të instalojmë në shfletues janë:

- **Bitdefender TrafficLight** - është një shtojcë që na tregon nëse faqja në të cilën ndodhemi është e sigurtë për tu vizituar apo jo.

- **Avast Online Security** - është një shtojcë ku çdo kërkim dhe shfletim na tregon lidhjet dhe nëse ato janë të sigurta për t'u vizituar para se t'i klikojmë ato.

Spam mesazhet

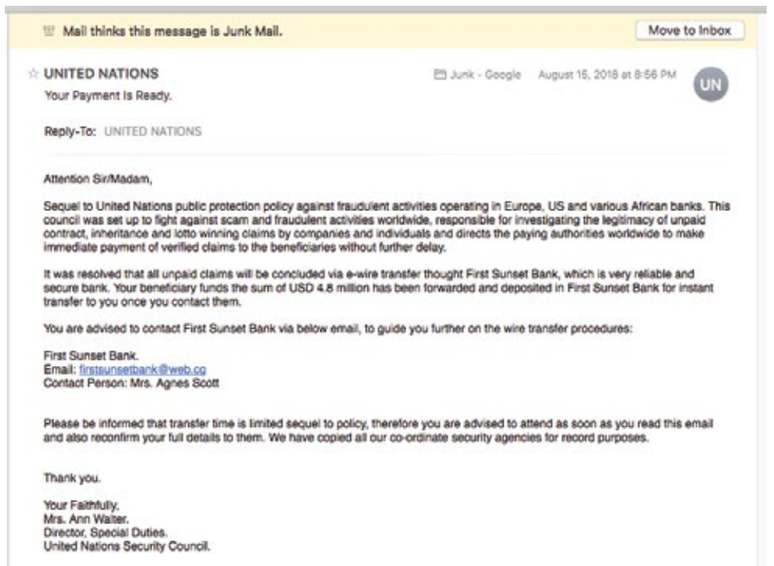
Emaili është një nga mjetet më të përdorura të komunikimit sot, kështu që është shënjestër e shumë sulmeve dhe përdoret për mashtrime të ndryshme. Çdo vit mbi 50% e numrit të përgjithshëm të postave elektronike të dërguara në Internet janë mesazhe spam.

Në shumicën e rasteve, spam mesazhet janë material reklamues, një rast i tillë në botën reale do të ishte sikur të merrnit një fletushkë në kutinë tuaj postare. Ajo fletushkë nuk paraqet problem derisa të filloni të merrni shumë spam mesazhe në baza javore ose ditore.

Por mesazhet spam nuk janë gjithmonë reklama, ato shpesh ndodhin të jenë si paralajmërime antivirusi, të cilat tregojnë se kompjuteri ynë është i infektuar me malware dhe se duhet të instalojmë antivirusin e tyre për ta pastruar. Këto mesazhe janë të pavërteta.

Një lloj tjetër i mesazhit mashtrues është se ne kemi fituar një çmim material ose monetar, ose llotari, të cilën nuk e kemi luajtur kurrë.

Disa shembuj të spam mesazheve.



Mail thinks this message is Junk Mail. Move to Inbox

UNITED NATIONS
Your Payment Is Ready.
Junk - Google August 15, 2018 at 8:56 PM

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.

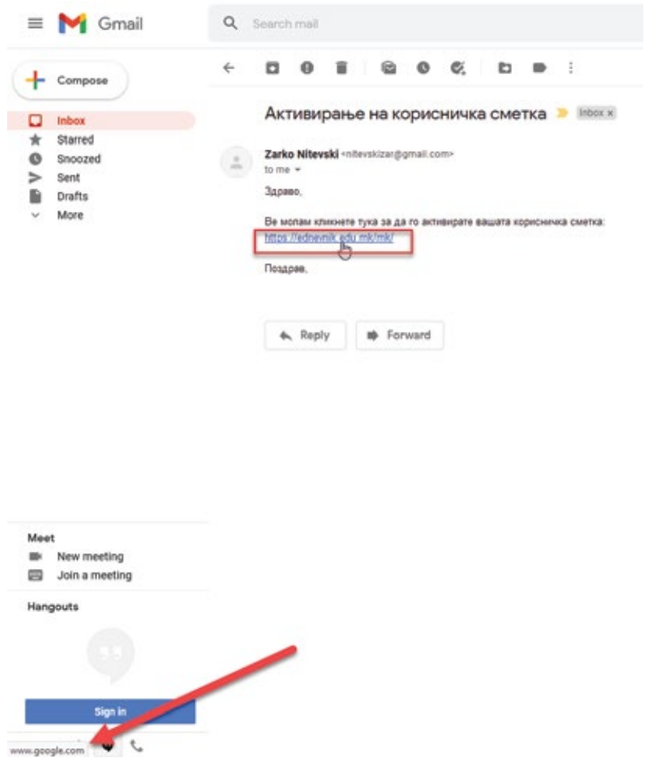
You are advised to contact First Sunset Bank via below email, to guide you further on the wire transfer procedures:

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.



Ajo që mund të shihet në shembujt është se linqet në mesazhe janë gjithmonë të dyshimta ose nuk korrespondojnë me kompaninë e përfaqësuar në mesazh. Ato shpesh dinë të kenë gabime shtypi ose gabime gramatikore në tekste. Dhe nganjëherë adresa nga e cila dërgohet mesazhi është e dyshimtë.

Praktika të cilat duhet ti dijmë:

1. Mos e publikoni postën tuaj elektronike askund
2. Nëse pajtohemi në një listë postash, duhet ta bëjmë me vetëdije.
3. Nëse pas një kohe duam të fshijmë nga një listë e caktuar postare, të dimë se ku ta bëjmë atë.

Inxhineria sociale

Në kontekstin e sigurisë, inxhinieria sociale është manipulimi psikologjik i njerëzve për të kryer veprime ose për të dhënë informacione konfidenciale. Ekzistojnë një numër mënyrash, por më e famshmja dhe e përdorura është sulmi Phishing.

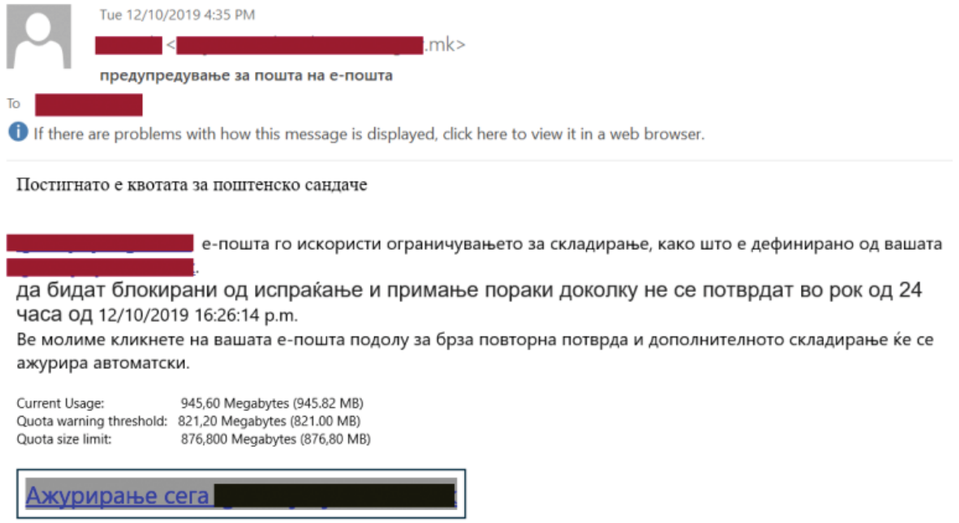
Sulmi Phishing

Mesazhet phishing janë shumë të ngjashme me spam mesazhet, pasi mesazhet e phishing kërkojnë të nxjerrin informacion ose para nga ne. Kjo ndodh kur sulmuesi, duke u paraqitur si një entitet i besueshëm, mashtron viktimën për të hapur një email ose mesazh të çastit. Marrësi pastaj mashtrohet të klikojë në një link të dyshimtë ose link me qëllim të keq, e cila mund të çojë në instalimin e malware ose ridrejtimin në një faqe ku ata duhet të futin të dhëna personale dhe të ndjeshme.

Ata zakonisht paraqiten sikur se janë nga ndonjë bankë ose institucion financiar, një fitues çmimi, një llotari ose ndonjë faqe e njohur si Facebook. Në të gjitha situatat thuhet se duhet t'u dërgojmë atyre informacione personale si emrin dhe mbiemrin, adresën e banimit, numrin e sigurimeve shoqërore, fjalëkalimin, xhirollogarinë, etj...

Ajo që është specifike në lidhje me phishing, ndryshe nga spam-i, është se ky informacion duhet të dërgohet gjithmonë në kohën më të shkurtër të mundshme, në të kundërtën do të na ndodhë diçka e keqe. Për shembull: ne do të humbasim hyrjen në postën elektronike ose llogarinë e përdoruesit, do të humbasim para dhe të tjera. Dhe të gjitha mesazhet janë shkruar në një mënyrë të tillë që duhet të reagohet shpejt dhe menjëherë dhe se është shumë e rëndësishme.

Disa shembuj të sulmeve phishing


Tue 12/10/2019 4:35 PM

[redacted] <[redacted].mk>

предупредување за пошта на е-пошта

To [redacted]

If there are problems with how this message is displayed, click here to view it in a web browser.

Постигнато е квотата за поштенско сандаче

[redacted] е-пошта го искористи ограничувањето за складирање, како што е дефинирано од вашата [redacted].

да бидат блокирани од испраќање и примање пораки доколку не се потврдат во рок од 24 часа од 12/10/2019 16:26:14 p.m.

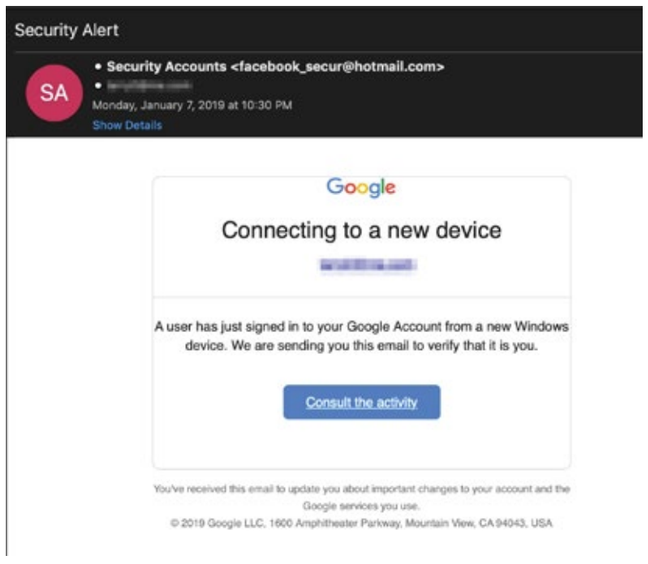
Ве молиме кликнете на вашата е-пошта подолу за брза повторна потврда и дополнителното складирање ќе се ажурира автоматски.

Current Usage: 945,60 Megabytes (945.82 MB)
Quota warning threshold: 821,20 Megabytes (821.00 MB)
Quota size limit: 876,800 Megabytes (876,80 MB)

Ажурирање сега [redacted]

Со почит,

[[-Domain-]] поддршка 2019 година.


Security Alert

• Security Accounts <facebook_secur@hotmail.com>

Monday, January 7, 2019 at 10:30 PM

Show Details

Google

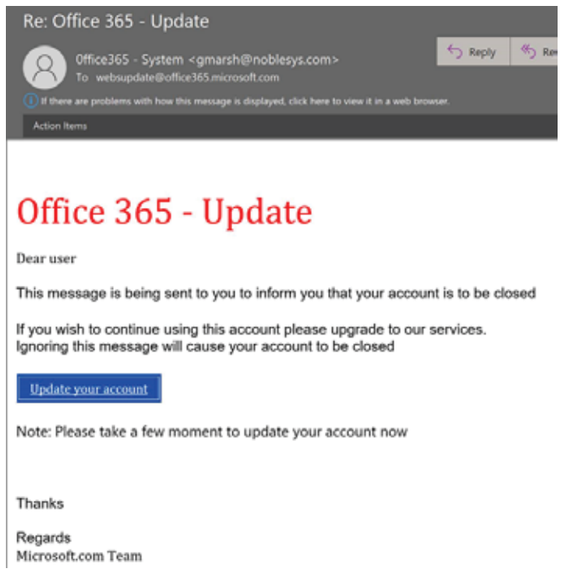
Connecting to a new device

A user has just signed in to your Google Account from a new Windows device. We are sending you this email to verify that it is you.

Consult the activity

You've received this email to update you about important changes to your account and the Google services you use.

© 2019 Google LLC, 1600 Amphitheater Parkway, Mountain View, CA 94043, USA


Re: Office 365 - Update

Office365 - System <gmarsh@noblesys.com>

To websupdate@office365.microsoft.com

Reply

If there are problems with how this message is displayed, click here to view it in a web browser.

Action Items

Office 365 - Update

Dear user

This message is being sent to you to inform you that your account is to be closed

If you wish to continue using this account please upgrade to our services.
Ignoring this message will cause your account to be closed

Update your account

Note: Please take a few moment to update your account now

Thanks

Regards
Microsoft.com Team

Nga shembujt mund të konkludojmë se të njëjtat gabime që ekzistojnë në mesazhet spam janë të pranishme edhe këtu. Si linqe të dyshimta, adresa nga e cila dërgohet mesazhi nuk korrespondon me mesazhin ose është e dyshimtë dhe ka gabime në tekste.

Softueri qëllimkeq

Malware (Softueri qëllimkeq) i referohet çdo programi me qëllim të keq që shkakton dëme në një sistem kompjuterik ose rrjet. Sulmon një kompjuter ose rrjet në formën e viruseve, krimbave, trojane, etj. Misioni i tyre shpesh është të përmbushin detyra të paligjshme të tilla si vjedhja e të dhënave, fshirja e dokumenteve konfidenciale ose shtimi i softuerit pa miratimin e përdoruesit.

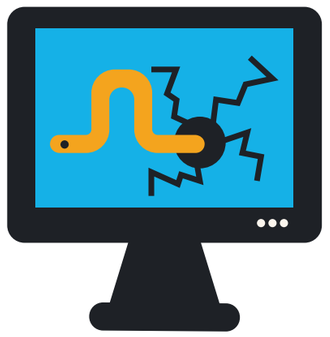
Ekzistojnë një numër programesh që bien nën softuerin qëllimkeq. Shumë shpesh ne as nuk jemi të vetëdijshëm se kemi malware (softuer qëllimkeq) derisa sistemi të fillojë të ngadalësohet ose t'i ndodhin gjëra të çuditshme.

Viruset në Kompjuter

Viruset mund të replikohen vetë, por atyre u duhet një mënyrë për t'u përhapur në një host tjetër. Dëmtimi i virusit mund të jetë aq i thjeshtë si përshembull një ikonë e re në sfondin tonë, e deri tek shkyçja e antivirusit, programi të sistemit ose fshirjen dhe shkatërrimin e dokumenteve.

Ato zakonisht transmetohen përmes të dhënave të shkarkuara nga interneti, posta elektronike ose mediave portative si **CD dhe USB.**

Krimbi Kompjuterik



Krimbat janë të ngjashëm me viruset kompjuterikë në atë që ata mund të kopjojnë dhe lëvizin lirshëm pa nevojë për ndihmë. Efektet e krimbave janë se ata përdorin burime kompjuterike të tilla si kujtesa ose fuqia e përpunimit të kompjuterit.

Softuer reklamues - AdWare

AdWare është një program reklamimi që instalohet së bashku me një aplikacion tjetër pa dijeninë e përdoruesit. Qëllimi kryesor është të shfaqni reklama pop-up që janë të bezdisshme dhe të parëndësishme për përdoruesin, si dhe të ndryshoni faqen fillestare të shfletuesit me një faqe të dyshimtë.

Softueri spiunues - Spyware

SSpyware është një lloj softueri që synon të mbledhë informacione të caktuara si fjalëkalimet, historia e shfletimit, historia e kërkimit të gjërave, kontaktet, llogaritë bankare dhe më shumë.

Mund të kuptoni nëse kompjuteri juaj ose lidhja e internetit po fillojnë të ngadalësohen.

RansomWare

Ransomware është softuer qëllimkeq që kripton të gjitha të dhënat në një kompjuter dhe kërkon një shumë të caktuar parash për të deshifruar ato të dhëna, përndryshe ato do të fshihen ose nuk do të deshifrohen kurrë. Mënyra më e zakonshme e përhapjes është përmes një sulmi phishing ose duke klikuar në linqe dhe faqe të dyshimta.

Mbrojtja

Disa praktika për mbrojtje më të mirë të pajisjeve tona:

- Duhet të kemi të instaluar softuer antivirus në të gjitha pajisjet që përdorim. Nëse përdorim sistemin operativ Windows, në thelb kemi antivirus Windows Defender i cili është nga Microsoft dhe është falas.
- Bëni një skanim të rregullt të pajisjes dhe të dhënave tona. Një herë në muaj të bëjmë një skanim të plotë të pajisjes.
- Azhurnoni rregullisht sistemin operativ.
- Azhurnoni rregullisht aplikacionet që përdorim dhe që i kemi të instaluara. Të tilla si: Microsoft Teams, Microsoft Office, Firefox, Chrome, Skype dhe të tjera.
- Të keni të instaluar në shfletuesin tuaj një bllokues AdWare të reklamave. Një sugjerim i mirë dhe falas është AdBlocker Plus (https://adblockplus.org/).

Çfarë është privatësia e internetit?

Mund të jetë një përvojë emocionuese, konfuze dhe madje pak e frikshme në botën tonë moderne digjitale. Kur i përdorim rrjetet sociale, më shumë se kurrë më parë ne ndajmë më shumë nga jeta jonë, dhe atë me një audiencë masive dhe kompani të mëdha dhe të fuqishme. Teknologjia e njohjes së fytyrës përdoret për të zhbllokuar telefonin tonë, për të vërtetuar identitetin tonë, për të lexuar shprehjet tona gjatë intervistave të punës dhe për të ndjekur lëvizjet tona në publik. Interneti i gjërave lidh shumë pajisje të përditshme me internet për ta bërë jetën tonë më të lehtë, por gjithashtu na lë të prekshëm nga pirateria dhe kontrolli.

Shpesh është e paqartë se kush mbledh informacionin tonë personal. Çfarë informacioni mbledhin ata, çfarë bëjnë me të dhënat tona, me kë ndajnë sekretet tona dhe a kemi privatësi? Privatësia jonë është e rëndësishme sepse na jep hapësirën që ne duhet ta zhvillojmë si qenie njerëzore.

Privatësia na jep lirinë për të lexuar, mësuar dhe shprehur veten pa u shqetësuar se kush mund të shohë. Kjo na jep mundësinë për t'i dhënë besimin tonë të tjerëve në mënyrë që të mund të blejmë, të shoqërohemi, të jemi intim me njëri-tjetrin dhe të krijojmë lidhje sociale që mbajnë komunitetet tona të forta, demokracinë tonë funksionuese dhe jetët tona të pasuruara. Shkurtimisht, pa intimitet nuk mund të funksionojmë si duhet si shoqëri ose si individë.

Privatësia e internetit përfshin të drejtën për informacione personale në lidhje me ruajtjen, përdorimin, sigurinë e palëve të treta dhe shfaqjen e informacionit personal përmes internetit. Privatësia e internetit është një nëngrup i privatësisë së të dhënave. Shqetësimet në lidhje me privatësinë kanë lindur që nga fillimet e rrjeteve kompjuterike.

Kërcënime për privatësi

Kontrolli mbi informacionin personal është gjithmonë tërheqës. Kush nuk do të dëshironte më shumë pushtet mbi gjërat që ndikojnë në jetët tona, por me këtë pushtet shpesh vjen dhe një detyrim i madh.

Nëse nuk e verifikojmë atë kontroll, atëherë jemi në rrezik, kompanitë mund ta marrin pasivitetin tonë si një lëshim, si një pëlqim të heshtur. Kjo na bën të duhet të rregullojmë cilësimet e privatësisë në Facebook, si dhe me Instagram, Twitter. Gjithashtu me Google, Amazon, Netflix, Snapchat, Microsoft, Siri, Cortana, Viber, Candy Crush, smart TV, fshesë robotike, Wi-Fi në makinë dhe ndonjë vegël inteligjente për fëmijët tanë. Disa aplikacione celulare kërkojnë mbi 200 leje? Mesatarja është rreth pesë.

Ekziston një shprehje e cila thotë: nëse nuk paguan për produktin, atëherë ti je produkti.

Mënyra se si teknologjitë janë të krijuara mund të ndikojë në privatësinë tonë.

E para, rrjetet sociale janë të dizajnuara në mënyrë që ne sa më shumë të shpërndajmë. E dyta, kompanitë që qëndrojnë pas rrjeteve sociale dhe përdoruesit e tjerë rrezikojnë privatësinë tuaj. E treta, është shumë e vështirë të mbrosh veten nga rreziqet e rrjeteve sociale.

Është kaq e lehtë të postoni diçka në rrjetet sociale. Kushdo që dëshiron të përdorë shërbime si Facebook, Twitter ose Snapchat mund të krijojë një llogari dhe të fillojë të ndajë fotot në sekonda. Në kuptimin e plotë të fjalës, çdo element i dizajnit të rrjeteve sociale është krijuar për të na bërë të shpërndajmë gjërat tona. Për shembull, shiriti i menusë për aplikacionin celular Facebook nuk u zhvendos në pjesën e poshtme të ekranit për estetikë, por për t'i afruar ato butona më pranë gishtave të mëdhenj.

Rrjetet sociale mund të japin një sens rreziku. Në fakt, ka disa kërcënime për t'u marrë parasysh. Së pari, shpërndarja. Së dyti, dhënia e pëlqimit. Së treti, ekspozimi i tepërt.

Me çdo shpërndarje ne zbulojmë vetëm pak më shumë për veten tonë. Efekti është i ngjashëm me nocionet tradicionale të mbikëqyrjes, ku me çdo mbikqyrje të njerëzve mësojmë diçka shtesë. Me atë që, kjo mbikëqyrje moderne na bën që ne vet të shpërndajmë ose të themi diçka

për veten tonë. Për shembull, në fillim të vitit 2016, Facebook prezantoi një seri mënyrash të reja për të bashkëvepruar me postimet. Tani përdoruesit mund të reagojnë me një emocion të dashur, qesharak, mahnitës, të trishtuar ose të zemëruar në postim. Kur mërzitemi nga ndërveprimi në aplikacion, kalojmë në aplikacione të tjera të ndryshme ose dalim plotësisht, këta quhen përdorues të bezdisur. Përdoruesit e interesuar të cilët vazhdojnë të shpërndajnë ose prodhojnë të dhëna quhen përdorues interesantë sepse me shpërndarjet e tyre, njerëz të tjerë interesohen për postimet e tyre dhe ashtu krijohet zingjiri. Le të kthehemi tek fenomeni i dhënies së pëlqimit. Merrni parasysh atë butonin e vogël me të cilin pajtohemi ose një fushë për zgjedhje që çdo përdorues klikon si pjesë e procesit të regjistrimit.

Ne biem dakord për shumë cilësime të privatësisë në tekste të gjata dhe të mëdha të quajtura Kushtet e Përdorimit. Ne gjithashtu pranojmë në mënyrë rutinore për lloje specifike të mbledhjes së të dhënave nga klikimet që bëjmë. Pajtohemi kur aplikacionet kërkojnë qasje në kamerën e telefonit tonë, vendndodhjen tonë ose kontaktet tona. Sepse kur diçka u ndodh të dhënave tona, ne nuk mund të ankohemi sepse kemi rënë dakord vetë. Ne mund të ndihemi aq të mbingarkuar nga mijëra kërkesa për qasje, leje dhe pëlqime për të përdorur të dhënat tona saqë themi vetëm po sepse jemi kaq të rraskapitur. Gjithashtu, hilet e dizajnit mund të na bëjnë të klikojmë në butone si pajtohem, para se të dimë se çfarë po bëjmë. Butonat, karakteret dhe oraret mund të manipulohen që ne të klikojmë rastësisht, ose kuptimi i rëndësisë të injorohet. Formulimet konfuze, menutë e vendosura dhe truket e tjera përdoren për të fshehur mekanizmat e pajtueshmërisë.

Miqtë e këqij janë një tjetër rrezik në rrjetet sociale. Ndonjëherë një mik është fjala e gabuar për të përshkruar rrjetin tuaj social.

TRANSFERIMI I TË DHËNAVE

Transferimi i të dhënave

Të dhënat kompjuterike janë informacione të përpunuara ose të ruajtura në një kompjuter. Ky informacion mund të jetë në formën e dokumenteve si tekst, imazhe, audio, programeve kompjuterikë me përmbajtje video ose lloje të tjerë të të dhënave.

Transferimi ose transferimi i të dhënave është çdo informacion që transmetohet nga një vend në tjetrin përmes disa metodave të komunikimit. Për shembull, ndarja e një dokumenti në Internet ose një media portative siç është një USB ose CD.

Të dhënat mund të transferohen nga kompjuterët përmes internetit duke përdorur një nga metodat e mëposhtme. Nëse duam të transferojmë ose dërgojmë të dhëna në Internet, duhet t'i ngarkojmë ato të dhëna në Internet. Nëse duam të marrim të dhëna nga interneti, atëherë themi që ato të dhëna i shkarkojmë nga interneti. Gjithashtu është mundur të shkëmbehen të dhëna me njëri-tjetrin direkt nga kompjuterët e tyre përmes internetit. Ky lloj komunikimi quhet transferimi i të dhënave peer-to-peer.

Rreziqet e transmetimit të të dhënave

Gjatë gjithë punës në kompjuter, ne punojmë me informacione dhe të dhëna. Ka një numër rreziqesh në transferimin e të dhënave, më të zakonshmet janë këto:

1. Shkarkimi ose marrja e të dhënave nga interneti

Ne duhet të sigurohemi që faqja ku shkarkojmë të dhënat është e sigurt, për shembull nëse shkarkojmë programin Microsoft Teams duhet të sigurohemi që t'i shkarkojmë nga faqja zyrtare e Microsoft. Më së miri është që çdo e dhënë e shkarkuar të skanohet nga Antivirus në kompjuterin tonë. Skanimi është veçanërisht i rëndësishëm nëse përdorni një torrent për të shkarkuar të dhëna.

2. Marrja e të dhënave përmes postës elektronike

Të dhënat më të rrezikshme të cilave mund t'i bashkangjiten malware (softuer me qëllim të keq) janë dokumentet Word (.docx), dokumentet PDF (.pdf), softueri (.exe) dhe të dhënat e ngjeshura ose të kompresuara (. Zip). Çdo dokument i postës elektronike që marrim duhet të skanohet.

3. Transferimi nga media portative

Sa herë që lidhim një disk USB ose vendosim një CD në kompjuterin tonë duhet të skanohet.

Rikthimi i të dhënat e fshira

Shpesh ndodh që ne të fshijmë disa të dhëna gabimisht ose ndonjë softuer me qëllim të keq ka fshirë të dhënat tona. Ekziston një mundësi që ne mund t'i rikthejmë (rimarrim) ato të dhëna të fshira me ndihmën e mjeteve të rikthimit të të dhënave.

Ka shumë mjete falas dhe me pagesë, një shembull i tillë është softueri Recuva (https://www.ccleaner.com/recuva). Para se të përpiqemi të rikthejmë të dhënat, së pari duhet të kuptojmë konceptin se si fshirja e të dhënave ndonjëherë mund të rikthehet dhe ndonjëherë jo. Kur fshijmë të dhëna në Windows, ne thjesht fshijmë indeksin e atyre të dhënave, dhe sistemi ynë operativ nuk mund të tregojë më ato të dhëna, por të dhënat janë akoma në hard disk. Derisa ato të dhëna nuk fshihen, dmth. ssnjë e dhënë tjetër e re nuk ruhet në të njëjtin vend, ne kemi një shans për ti rikthyer ato të dhëna të fshira ose të humbura.

DHUNA KIBERNETIKE

Dhuna kibernetike

Në praktikë, aktet e dhunës cyber mund të përfshijnë forma të ndryshme të ngacmimit, cënimit të privatësisë, abuzimit seksual dhe shfrytëzimit seksual, si dhe krimeve për varësi kundër grupeve shoqërore ose komuniteteve.

Dhuna cyber mund të përfshijë gjithashtu kërcënime të drejtpërdrejta ose dhunë fizike, si dhe forma të ndryshme të krimit në internet.

Cyber dhuna ndahet në:

- Cyberbullying dhe cyberharassment – Cyber bullizmi dhe maltretimi në internet
- Cyberstalking - Mbikëqyrja në internet
- Shkelja e privatësisë në internet dhe gjuha e urrejtjes
- Shfrytëzimi seksual dhe abuzimi seksual i fëmijëve përmes internetit
- Cyberthreats - Kërcënimet në internet dhe krimin kibernetik - Krimi kompjuterik

Cyber maltretimi është ndoshta forma më e gjerë e ngacmimit në internet dhe përfshin një rrjedhë të vazhdueshme dhe të përsëritur të sjelljes drejtuar një personi të caktuar, duke shkaktuar stres serioz emocional dhe shpesh frikë nga dëmtimi fizik.

Mbikëqyrja ose ndjekja në internet është përdorimi i internetit ose mjeteve të tjera elektronike për të ndjekur ose ngacmuar një individ, grup ose organizatë. Mund të përfshijë akuza të rreme dhe shpifje. Mund të përfshijë gjithashtu mbikëqyrje, vjedhje të identitetit, kërcënime, vandalizëm, kërkesë për seks ose mbledhje informacioni që mund të përdoret për të kërcënuar, turpëruar ose maltretuar.

Shumë forma të dhunës cyber kanë lidhje me shkeljen e privatësisë së viktimave. Kjo mund të përfshijë ndërhyrje në kompjuter për të marrë, vjedhur, zbuluar ose manipuluar të dhëna intime, hulumtime dhe transmetuar të dhëna personale ("doxing") ose veprime të tilla si mbikëqyrje / ndjekje në internet ose "revenge porn".

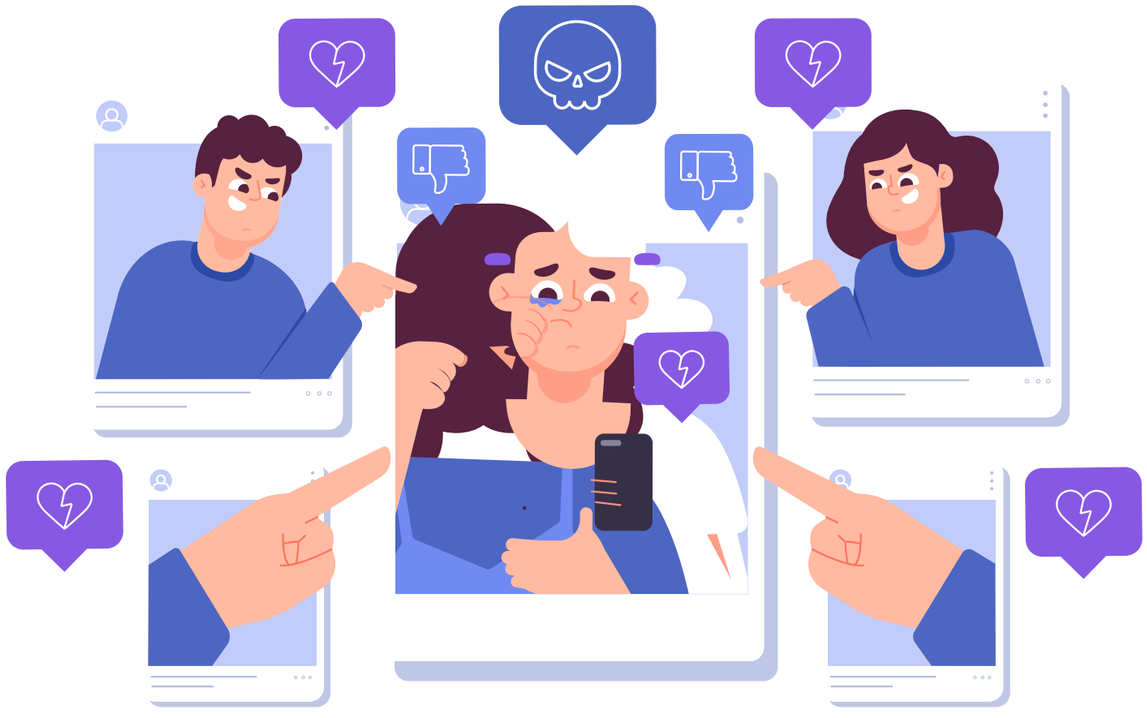
Shfrytëzimi seksual dhe abuzimi seksual i fëmijëve përmes internetit

Fëmijët duket se janë grupi kryesor i viktimave të dhunës cyber, veçanërisht në lidhje me dhunën seksuale në internet. Edhe përkundër asaj se "Shfrytëzimi seksual në internet dhe abuzimi seksual i fëmijëve" nuk janë domosdoshmërisht forma të reja dhe të theksuara të shfrytëzimit seksual dhe abuzimit seksual të fëmijëve, interneti po rrit aksesin tek fëmijët nga personat që i kërkojnë për keqpërdorim seksual dhe i shfrytëzojnë ata. Interneti lehtëson ndarjen e imazheve dhe videove të abuzimit seksual dhe kështu rrit ndikimin e dëmshëm afatgjatë të abuzimit të fëmijëve.

Kërcënimet në internet dhe krimi kompjuterik

Cyber dhuna përfshin gjithashtu kërcënime të drejtpërdrejta të dhunës ose dhunë të drejtpërdrejtë fizike. Sistemet kompjuterike mund të përdoren në lidhje me vrasje, rrëmbime, përdhunime dhe akte të tjera të dhunës seksuale ose zhvatjes. Duke pasur parasysh përkufizimin e përcaktuar më sipër, disa forma të krimit kibernetik mund të konsiderohen gjithashtu akte të ngacmimit në internet, të tilla si qasja e paligjshme në të dhënat intime personale, shkatërrimi i të dhënave, bllokimi i hyrjes në një sistem kompjuterik ose të dhëna, etj.

Ende nuk ka leksik të qëndrueshëm ose tipologji të veprave që konsiderohen dhunë cyber, dhe shumë shembuj të llojeve të ngacmimit në internet janë të ndërlidhura ose të mbivendosura ose përbëhen nga një kombinim i veprimeve. Jo të gjitha format ose rastet e ngacmimit në internet janë njësoj serioze dhe jo të gjitha kërkojnë domosdoshmërisht një zgjidhje ligjore penale, por mund të adresohen me një qasje të vlerësuar dhe një kombinim të masave parandaluese, arsimore, mbrojtëse dhe masave të tjera.



Ngacmimi në internet

Fëmijët që lejohen të përdorin telefona celularë, tableta dhe laptopë me lidhje interneti shpejt mësuan se si t'i përdorin ato në mënyrë efektive. Ata madje mund të duket se gradualisht bëhen të pandashëm nga pajisja e tyre. Është mjaft e natyrshme që ata të përdorin mjete virtuale dhe ata i kuptojnë parimet e rrjetit shumë më mirë sesa shumica e të rriturve për sa kohë që ata përdorin internetin për qëllime të dobishme të tilla si kërkimi i informacionit, mësimi dhe lojërat. Shumicën e kohës, ana e errët e natyrës së fëmijëve ndodh që të ekspozohet në botën virtuale.

Kur bëhet fjalë për të ngacmuar bashkëmoshatarët e tyre, të rinjtë po përfitojnë nga gjithçka që ofron interneti. Një e shtënë është e mjaftueshme. Fushata sociale e kryer mirë e UNICEF-it thotë se maltretimi nëpërmjet internetit është një nga shkaqet kryesore të depresionit dhe vetëvrasjes tek fëmijët nëpër shkolla. Nëse keni një smartphone, përdorni atë me mençuri. Mos vrit askënd. Për një moment, ju do të mësoni disa metoda themelore të përdorura nga agresorët e rinj në Internet. Ndoshta falë tyre, ju do të jeni në gjendje të shikoni më në detaje sjelljen virtuale të studentit ose fëmijës tuaj dhe të vini re disa sjellje alarmante.

Përndjekja

Situata kur një fëmijë ndjek dikë në internet për një kohë të gjatë, prish jetën e tij dhe komunikon me të në një mënyrë që personi të ketë frikë nga paqja dhe siguria e tij, prindërit shpesh e banalizojnë këtë gjë. Përndjekja ose ndjekja në jetën reale kërkon shumë përpjekje dhe përfshirje nga shtypësi. Sidoqoftë, ndjekja në Internet, për shkak të kuptimit të tij të përbashkët dhe relativ, është bërë një medium i preferuar i ndjekësve. Ky lloj agresioni shpesh ndodh midis njerëzve që e njohin njëri-tjetrin, kanë njohur njëri-tjetrin në të kaluarën ose madje kanë qenë në marrëdhënie të ngushta.

Përleshje nëpërmjet internetit

Flaming ose roasting është një shkëmbim agresiv i pikëpamjeve midis disa njerëzve, i cili zakonisht kryhet në publik në dhomat e bisedave ose brenda grupeve të diskutimit. Fenomeni është vetëm i pakëndshëm, por mjaft i zakonshëm. Mund të ketë pasoja më serioze kur shndërrohet në maltretim. Bisedat e rastësishme për skuadrat sportive, markat e preferuara të makinave ose lojërat kompjuterike evoluojnë në një seri fyerjesh dhe sulmesh, maltretimesh, ngacmimesh bazuar në dërgimin e mesazheve agresive, nënçmuese, ofenduese, shpesh vulgare tek viktima përmes mjeteve elektronike të komunikimit në baza të rregullta.

Një telefon celular, rrjet social ose sistem bisede në internet përdoret në situata të tilla. Por ndonjëherë agresioni përshkallëzohet shpejt dhe shndërrohet në dërgimin e kërcënimeve serioze ndaj viktimës .

Paraqitje e rremë

Një nga motivet kryesore të një vjedhësi të identitetit është të imitojë viktimën e tij në hapësirën kibernetike. Përdorimi i fjalëkalimeve të dobëta për email dhe i bisedave të menjëhershme shpesh lehtëson vjedhësin. Dhe ndërsa nuk shpjegon motivet e agresorëve, është mirë të jesh i vetëdijshëm për faktin se një vjedhës i identitetit mund t'i shkaktojë shumë telashe viktimës së tij ose të saj duke dërguar mesazhe diskredituese te studentët dhe mësuesit e tjerë.

Videot ose fotot mund të bëhen menjëherë publike ose të arritshme për njerëzit që nuk duhet patjetër të kenë qasje në to. Ndodh gjithashtu që para se materialet të bëhen virale ose të njohura, hajduti shantazhon pronarin, duke kërkuar të përmbushë pritjet e tij, të tilla si ekspozimi i viktimës në një kamerë në internet ose pagimi i një shpërblimi.

Video inqizime – happy slapping

Është thjesht një mënyrë tjetër për të marrë materiale të diskredituara edhe më të keqija sesa ato të mëparshmet. Qëllimi është të shkaktohet dhe provokojë një sulm, viktima të bëjë vetë sulmin dhe të filmohet ose fotografohet nga autori dashakeq. Atëherë gjithçka është e njëjtë si në shembujt e tjerë të ngacmimeve kompjuterike. Materiali bëhet viral ose viktima shantazhohet nga kërcënimet për interpretimin e tyre gjatë hedhjes së materialeve. Kjo formë e sjelljes agresive bazohet në postimin e informacionit ose materialeve të rreme për disa njerëz. Këto mund të jenë thashetheme të zakonshme për viktimat, pjesëmarrje në disa ngjarje të turpshme. Këto shpesh janë filma ose fotografi të modifikuara që sugjerojnë se viktima po kryen disa veprime.

Përjashtimi social

Heqja e qëllimshme e dikujt nga një listë kontakti, grup diskutimi ose bisedë e drejtuar nga një grup miqsh rezulton në përjashtimin e viktimës nga grupi i kolegëve. Shpesh është një nga format e maltretimeve relacionale.

Agresioni teknik

Kjo formë e sulmit kërkon pak më shumë njohuri teknike. Megjithatë, mos lejoni të ju qetësojë. Këto ditë, fëmijët kanë njohuri mëshumë për pa-

jisjet elektronike nga ajo se çfarë mund të duket. Agresioni teknik është një sulm ndaj kompjuterit të përdorur nga viktima, softuerit të tij ose të saj kompjuterik ose web faqe. Kjo përfshin dërgimin e viruseve kompjuterikë ose aktivitete të piraterisë të tilla si një sulm bombardues përmes postës, e cila dërgon një numër të madh të mesazheve në llogarinë e viktimës, ku qëllimi është të prish funksionimin e postës elektronike ose të përpiqen të sulmojnë kompjuterin e viktimës duke dërguar disa lidhje, skedarë ose mesazhe të dyshimta.

Rrjetet sociale dhe video lojërat

Mediumet dhe aplikacionet digjitale lejojnë fëmijët të komunikojnë dhe të shprehin kreativitetin e tyre, të lidhen me bashkëmoshatarët dhe të ndajnë ndjenjat e tyre. Sidoqoftë, ato gjithashtu mund të jenë rrugë përmes së cilës ndodh ngacmimi kompjuterik.

Ekzistojnë shumë lloje të aplikacioneve dhe faqeve në dispozicion falas që u japin përdoruesve mundësinë për të kërkuar njerëz dhe për të ndarë ose postuar informacion në lidhje me ta në mënyrë anonime. Prindërit mund të mos jenë të vetëdijshëm për aplikimet që fëmijët e tyre përdorin rregullisht ose mund të mos jenë të vetëdijshëm për rreziqet që përfshihen në përdorimin e tyre.

Ka shumë mënyra që ngacmimi kompjuterik mund të fshihet në aplikacione dhe faqe, siç janë tekstet, videot dhe thirrjet në internet që zhduken ose nuk shfaqen në regjistrat e thirrjeve ose mesazhet me tekst në pajisjen tuaj. Shumë aplikacione gjithashtu u lejojnë përdoruesve të kenë lehtësisht qasje, shikojnë ose ndajnë përmbajtje për të rritur ose me qëllim të keq.

Cilësimet e privatësisë dhe vendndodhjes mund t'i bëjnë ata më të ndjeshëm ndaj mbikëqyrjes, ngacmimit në internet, ekspozimit të përmbajtjes së të rriturve ose rreziqeve të tjera.

Disa nga faqet dhe aplikacionet aktuale të njohura të mediave sociale përfshijnë:

- **Discord**: Një aplikacion që lejon përdoruesit të bisedojnë me video me të tjerët, të dërgojnë mesazhe private dhe të bashkohen, të krijojnë ose të marrin pjesë në dhomat e bisedave publike dhe private. Ky aplikacion shpesh përdoret nga lojtarët për të folur me njëri-tjetrin gjatë kohës që luajnë lojëra video.
- **Facebook**: Faqja më e përdorur zakonisht e mediave sociale në dispozicion në shumë platforma të ndryshme mediatike.

- **Instagram**: Web faqe për shpërndarjen e fotove dhe videove që lidh përdoruesit përmes faqeve të tjera të rrjeteve sociale (për shembull, Facebook).
- **Snapchat**: Aplikacioni për mesazhe me fotografi që ju lejon të ndani fotografi dhe video të shkurtra që synojnë të fshihen menjëherë pas dorëzimit.
- **Telegram**: Aplikacioni për mesazhe që lejon përdoruesit të ndajnë foto, video dhe skedarë; bëni telefonata dhe fshini tekste ose biseda nga telefoni i marrësit duke përdorur kohëmatës.
- **TikTok**: Një aplikacion që lejon përdoruesit të krijojnë dhe të ndajnë videot e tyre ku sinkronizojnë, këndojnë, kërcejnë ose thjesht flasin.
- **WhatsApp**: Aplikacioni i mesazheve private që lejon përdoruesit të shkruajnë mesazhe, të dërgojnë foto, video dhe informacione për vendndodhjen në kontaktet e tyre.
- **YouTube**: : Platformë për ndarjen e videos që lejon përdoruesit të postojnë dhe të ndajnë video.

Mediat sociale kanë shumë përfitime që duhet të ekuilibrohen me rreziqet që ato paraqesin. Rreziqet për të qenë të vetëdijshëm përfshijnë:

Përmbajtja e publikuar mund të jetë e pasaktë, e dëmshme ose e pavërtetë.

Mund të përdoret për të ndarë përmbajtje të dëmshme ose përmbajtje për të rritur. Kontrollet e privatësisë se kush mund të shikojë ose të përdorë materialin e botuar ndryshojnë nga aplikacionet dhe shumë përdorues nuk janë të vetëdijshëm se si t'i përdorin ato në mënyrë efektive.

Aplikacionet që ofrojnë video në kohë reale nga përdoruesit mund të përdoren për të treguar ngacmim, dhunë, vetëvrasje dhe keqtrajtim teksa ndodhin.

Disa aplikacione që përfshijnë informacione për vendndodhjen mund të përdoren për të marrë informacione personale, të tilla si mosha e dikujt, vendndodhja aktuale ose vendndodhja.

Aplikimet që mbështesin thirrjet telefonike nuk shfaqen në regjistrin e telefonatave, kështu që prindërit mund të mos e dinë me kë flasin fëmijët e tyre.

Të luash video lojëra është një aktivitet i njohur, me 90 përqind të adoleshentëve që luajnë lojëra në internet. Shumë lojëra video - qoftë në kompjuter, tastierë lojërash, celular ose tablet - i lejojnë përdoruesit të luajnë me miqtë që njohin personalisht dhe të tjerët që i kanë takuar vetëm në internet.

Ndërsa lojërat e lojërave mund të kenë përfitime pozitive të tilla si krijimi i miqve të rinj, shoqërimi dhe të mësuarit se si të strategjizohen dhe zgjidhen problemet, është gjithashtu një vend tjetër ku ndodh ngacmimi në internet. Anonimiteti i lojtarëve dhe përdorimi i avatarëve i lejojnë përdoruesit të krijojnë alter-ego ose versione imagjinare të vetvetes, e cila është pjesë e argëtimit të lojërave.

Por gjithashtu lejon përdoruesit të ngacmojnë dhe nganjëherë të grupohen me lojtarë të tjerë, duke dërguar ose postuar mesazhe negative ose të dëmshme dhe duke përdorur lojën si një mjet ngacmimi. Nëse dikush nuk është aq i mirë në lojë, fëmijët e tjerë mund të tallen ose të bëjnë vërejtje negative që kthehen në ngacmim, ose ata mund ta përjashtojnë personin nga loja së bashku.

Për shkak se lojtarët janë anonimë, ata mund të mos konsiderohen domosdoshmërisht të përgjegjshëm për sjelljen e tyre dhe ngacmimi i tyre mund të bëjë që disa lojtarë të largohen nga lojërat. Disa përdorues anonimë e përdorin lojën si një mjet për të ngacmuar të huajtë ose për të marrë informacionin e tyre personal, siç janë emrat e përdoruesve dhe fjalëkalimet.

Mbrojtja dhe njohja

Prindërit, mësuesit dhe të rriturit e tjerë mund të mos jenë të vetëdijshëm për të gjitha platformat dhe aplikacionet e mediave sociale që përdor një fëmijë. Sa më shumë platforma digjitale të përdorë një fëmijë, aq më shumë mundësi ka që ai ose ajo të ekspozohet ndaj ngacmimeve të mundshme përmes internetit.

Shumë nga shenjat paralajmëruese të ngacmimit në internet ndodhin rreth një fëmije duke përdorur pajisjen e tyre. Për shkak se fëmijët kalojnë shumë kohë në pajisjet e tyre, rritja ose zvogëlimi i përdorimit mund të jetë më pak i dukshëm.

Është e rëndësishme t'i kushtohet vëmendje kur një fëmijë shfaq ndryshime të papritura në sjelljen digjitale dhe shoqërore. Disa nga shenjat paralajmëruese që një fëmijë mund të përfshihet në ngacmimin në internet janë::

- Rritja ose zvogëlimi i shpejtë i përdorimit të pajisjes, duke përfshirë mesazhet.
- Fëmija shfaq përgjigje emocionale (të qeshura, zemërimi, ankthi) ndaj asaj që po ndodh në pajisjen e tij.
- Fëmija fsheh ekranin ose pajisjen e tij kur të tjerët janë afër dhe shmang diskutimin për atë që po bëjnë në pajisjen e tij.
- Fëmija fillon të shmangë situatat shoqërore, madje edhe ato të cilat i ka shijuar në të kaluarën.
- Fëmija tërhiqet ose bie në depresion ose humbet interesin për njerëzit dhe aktivitetet.

Ka gjëra që të rriturit mund të bëjnë për të parandaluar ngacmimin kompjuterik të fëmijëve që luajnë lojëra:

- Luajeni lojën ose vëzhgojeni kur luhet loja për të kuptuar se si funksionon dhe nga çfarë ekspozohet një fëmijë në lojë.
- Kontrolloni në mënyrë periodike me fëmijën tuaj për atë që është në internet duke luajtur lojën me ta.
- Mësojini fëmijët tuaj në lidhje me sjelljen e sigurt në internet, duke përfshirë mos klikimin në lidhje nga të huajt, mos ndarjen e informacioneve personale, mospërfshirje në sjellje ngacmimi me lojtarë të tjerë dhe çfarë të bëjnë nëse ata vërejnë ose përjetojnë ngacmim
- Vendosni rregulla për sa kohë fëmija mund të kalojë duke luajtur lojëra video.

Mësuesit, pedagogët janë në pozicione unike për të përdorur aftësitë dhe rolet e tyre për të krijuar ambiente të sigurta me norma pozitive shoqërore.

Ju jeni gjithashtu në një pozicion ku mund të vëreni ndryshime në sjelljen e fëmijëve në mjediset e grupeve, të tilla si një grup ose grupe fëmijësh që përqendrohen te një fëmijë tjetër ose shenja të tjera ngacmimi mund të ndodhë në internet.

Ka gjëra që mund të bëni në klasë ose në grupe të tjera të grupeve për të identifikuar ose parandaluar ngacmimin në internet.

- Nëse mendoni se fëmija juaj po ngacmohet në internet, bisedoni me ta privatisht për ta zbuluar. Ata gjithashtu mund të kenë prova në pajisjet e tyre digjitale.
- Nëse besoni se një fëmijë është ngacmuar në internet, flisni me një prind në lidhje me të. Shërbeni si ndihmës midis fëmijës, prindit dhe shkollës nëse është e nevojshme.
- Për të kuptuar sjelljen digjitale të fëmijëve dhe si sillet ngacmimi në internet, rritni vetëdijen tuaj digjitale.
- Zhvilloni aktivitete që inkurajojnë vetë-reflektimin, duke u kërkuar fëmijëve të identifikojnë dhe shprehin ato që mendojnë dhe ndiejnë dhe të marrin parasysh mendimet dhe ndjenjat e të tjerëve.
- Ndihmoni fëmijët të zhvillojnë inteligjencë emocionale në mënyrë që ata të mësojnë aftësitë e vetë-ndërgjegjësimit dhe vetë-rregullimit dhe të mësojnë se si të bashkë ndjenjë me të tjerët.

SHTYPJE DIGJITALE

Shtypje digjitale

Gjurmët digjitale janë shënime dhe gjurmë që lëmë pas ndërsa përdorim internetin. Gjurma jonë digjitale mund të kontribuojë në reputacionin tonë në Internet. Kjo do të thotë që ne nuk duhet të hyjmë vazhdimisht ose të paraqesim detaje personale në faqet e internetit. Nga ana tjetër, gjurmët e gishtërinjve tanë digjital mund t'i lejojnë të tjerët të gjurmojnë veprimet tona, të tilla si faqet e internetit që përdorim, gjërat që kërkojmë dhe kush është në rrethin tuaj shoqëror.

Gjurmët tona digjitale janë të dukshme për organizatat me të cilat nuk kemi asnjë lidhje dhe mbi të cilat shpesh nuk kemi kontroll. Shumë organizata gjithashtu punojnë prapa skenave për të ndërtuar profile për ne bazuar në gjurmët tona digjitale. Shumica e njerëzve janë të vetëdijshëm se kur ndajnë informacione për veten e tyre në Internet, siç janë rrjetet sociale dhe përdorin shërbime të Internetit si e-mail, mesazhe të çastit ose postë zanore, ata kanë hequr dorë nga kontrolli mbi privatësinë e tyre.

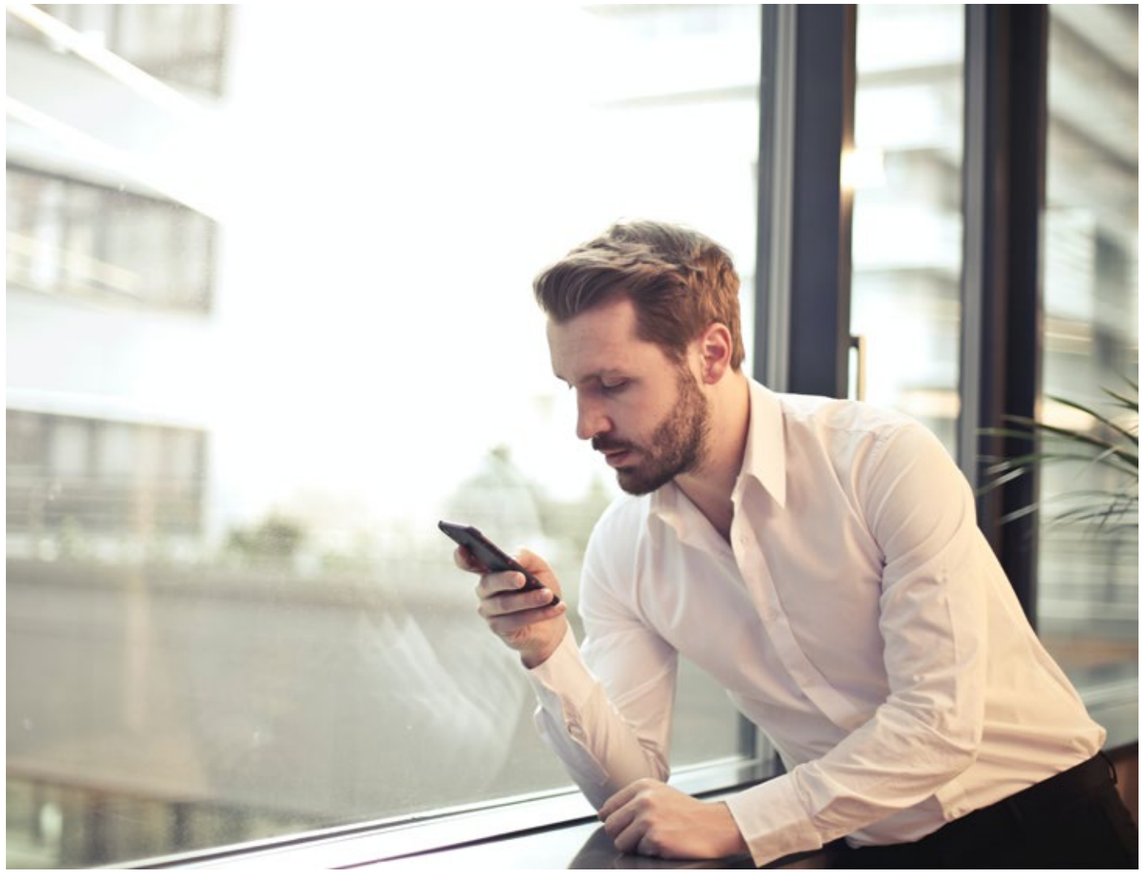
A është e mundur që dikush të na ndjekë në botën virtuale të internetit, duke gjurmët tona digjitale, duke kërkuar përshtypjet që lëmë? Përgjigja është “po”.

Gjurmët tona digjitale janë më të mëdha sesa mund të imagjinojmë dhe ato përdoren - zakonisht për qëllime komerciale, por nganjëherë për arsye të tjera - për të na gjurmuar, për të na u përshtatur dhe për të na treguar reklama përkatëse. Këto aktivitete janë kryesisht për të mirën e organizatës në fjalë. Me pak fjalë, gjurma jonë digjitale monetarizohet ... por jo çdo fitim i drejtpërdrejtë zakonisht vjen tek ne, tek individi.

Vizitat tona në ofrues të ndryshëm të shërbimeve gjenerojnë të dhëna për ne që mblidhen në secilin vend. Ofruesit e shërbimeve dhe palët e tjera të treta shkëmbejnë të dhëna të profilit të klientit dhe statistikat e transaksioneve.

Llojet e printimeve digjitale

Smartfonët dhe tabletët kanë për tendencë të lënë një gjurmë digjitale shumë më të ndryshme sesa laptopët dhe desktopët. Telefonat inteligjentë modernë funksionojnë në mënyra që krijojnë një përshtypje më intensive. Aplikacionet lidhen direkt me shërbimet e Internetit duke përdorur ndërfaqe specifike. Kontrolli mbi dërgimin e informacionit te shërbimet / pajisjet e tjera qëndron në duart e zhvilluesit të aplikacionit dhe i ekspozohet përdoruesit përfundimtar vetëm në masën e lejuar nga zhvilluesi. Veçanërisht pajisjet mobile gjithashtu u japin përdoruesve më pak akses në lidhjen anonime.



Smartfonët zakonisht janë të vetëdijshëm për vendndodhjen. Kjo i lejon aplikacionet të shënojnë aktivitetet tuaja në vendndodhjen tuaj. Shërbimet e vendndodhjes shpesh aktivizohen si parazgjedhje ose përfshihen në paketën e lejeve që kërkohet të japë përdoruesi kur instalohet një aplikacion.

Të dhënat e vendndodhjes mund të ndahen në mënyrë eksplicite nëse aplikacioni merr të dhënat tuaja të vendndodhjes dhe i dërgon ato në një shërbim të Internetit, ose në mënyrë implicite - për shembull, nëse fotografitë dhe videot që postoni tregojnë vendndodhjen, datën dhe kohën kur janë marrë. Konsiderohet se 4-6 artikuj të të dhënave të vendndodhjes janë të mjaftueshme për të identifikuar në mënyrë unike secilin përdorues të dhënë.

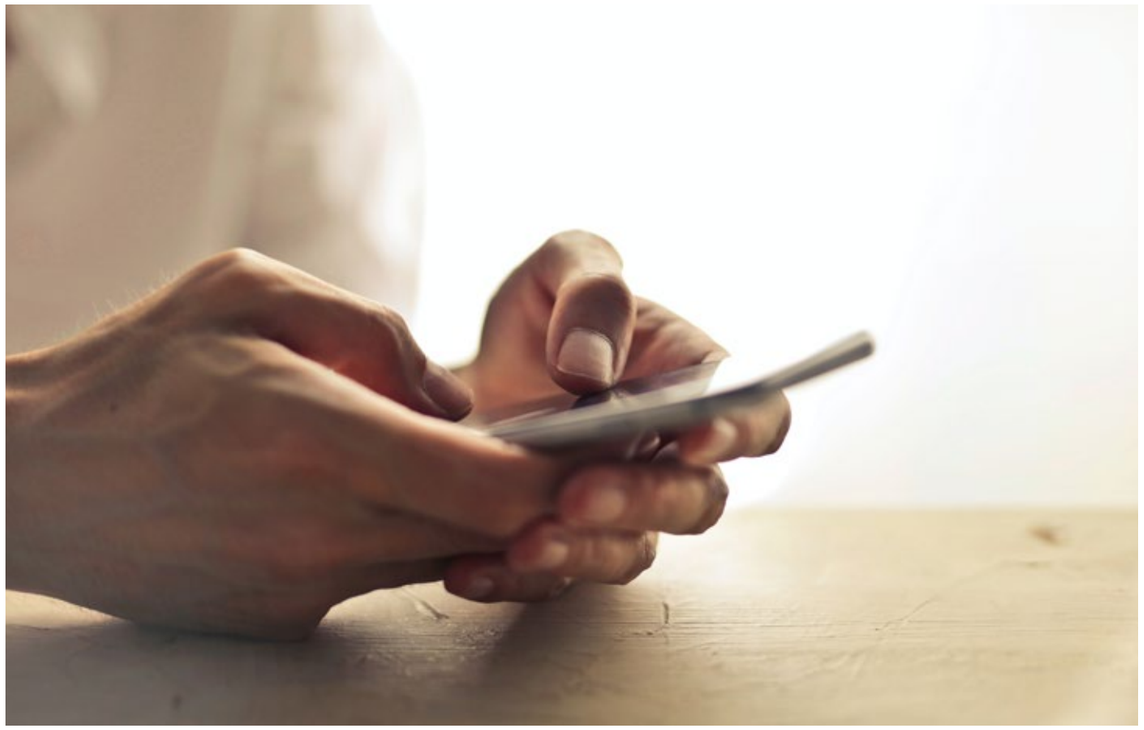
Shitësit e telefonave inteligjentë zakonisht kontrollojnë nëse të dhënat e vendndodhjes ndahen dhe bllokojnë përdorimin e identifikuesve specifikë të pajisjes nga aplikacionet. Kjo nuk është diçka mbi të cilën përdoruesi ka kontroll. Sidoqoftë, disa kontrolle mbi informacionin e ndjeshëm bazohen në cilësimet e nivelit të pajisjes, dhe të tjera në cilësimet e nivelit të aplikacionit.

Këto aftësi ndryshojnë shumë në varësi të platformës smartphone; si dhe nivelin në të cilin ato dokumentohen dhe lehtësinë me të cilën përdoruesi mesatar mund t'i zbulojë dhe menaxhojë ato.

Sidoqoftë, sapo një përdorues të fillojë të marrë imazhe të etiketuara ose t'i japë aplikacionit të sapo instaluar leje për të parë informacionin e vendndodhjes, leja e dhënë aplikacionit rishikohet rrallë.

Përdoruesit e desktopëve dhe laptopëve kryesisht i lënë gjurmët përmes shfletuesit të tyre të internetit. Shfletuesi standard i internetit është shumë i ndryshëm nga aplikacionet e përdorura në smartphone dhe tabletë. Kontrollet relativisht të pjekura të ofruara nga shfletuesit, ose shtojca shtesë, i lejojnë përdoruesit përfundimtar të kontrollojë më lehtë atë që ndahet dhe informacionin e qartë të identifikimit, të tilla si cookies, të cilat përndryshe mund të zvogëlojnë privatësinë personale. Kështu që po, desktopët kanë një avantazh ndaj privatësisë në krahasim me telefonat inteligjentë.

Detyra e monitorimit dhe kontrollit nga afër të privatësisë është një mënyrë e rëndësishme dhe mund të jetë më komplekse sesa shumë përdorues të smartphone-ve që mund të presin. Është një sfidë për të gjithë ne, si konsumatorë dhe shfrytëzues, të njohim vlerën e informacionit tonë personal dhe privatësisë sonë: vetëm duke përshtatur vlerat tona dhe, si rezultat, sjelljen tonë, mund të shpresojmë të sjellim vendime më të mira dhe të qëndrueshme për privatësinë.



Kontroll digjital i gjurmëve të gishtave

Ne duhet të luftojmë kundër inercionit tonë, duke u përballur me standarde praktike që shkatërrojnë privatësinë dhe kundër përpjekjeve të përbashkëta, të vazhdueshme të organizatave me një interes financiar për të na bindur të sakrifikojmë privatësinë tonë për hir të fitimeve të tyre. Ne ndoshta kemi vetëm kohë dhe energji të kufizuar për t'i kushtuar asaj që duket si një detyrë e rastësishme, ndërsa organizatat dhe kompanitë e bëjnë atë si punën e tyre dhe ata janë mjaft të mirë në të.

Si mund ta menaxhojmë gjurmët tona digjitale? Këtu janë disa praktika për fillim:

- Të kërkojmë në Google për vete: Le të shohim se çfarë ka atje. Le të kërkojmë emrin tonë çdo disa muaj për t'u njohur me informacionin në të cilin të tjerët kanë qasje.
- Mbrojtja e informacionit tonë personal: Mos zbuloni adresën tuaj personale, numrin e telefonit, fjalëkalimet ose numrat e kartës bankare. Merrni parasysh të përdorni një pseudonim në vend të emrit tuaj të vërtetë.
- Kontrolloni dhe caktoni cilësimet e privatësisë së aplikacioneve dhe shërbimeve që përdorim.
- Mbani informacionin kyç të hyrjes nën dry: Asnjëherë mos ndani asnjë nga emrat e përdoruesit ose fjalëkalimet tuaja.
- Le të mendojmë para se të postojmë: Asnjëherë mos vendosni emocione të përkohshme në një internet të përhershëm. Zemërimi është i përkohshëm; Interneti zgjat përgjithmonë. Para se të postojmë: Le të mendojmë dy herë, dhe të botojmë një herë.
- Çdo foto që postojmë mund të gërmohet një ditë. Kufizoni ndarjen e imazheve të dyshimta. Pesëmbëdhjetë minuta humor nuk ia vlen asnjëherë një poshtërim të mundshëm gjatë gjithë jetës.

Tani që e dimë se çfarë është gjurmë digjitale, duhet të ndërmarrim hapat e duhur për ta ruajtur atë gjurmë. Bota digjitale nuk do të shkojë askund në ndonjë kohë së shpejti - kështu që duhet të mendojmë për të si një jetë të tërë. Le të përdorim platformën për të prezantuar veten në dritën më të mirë dhe për të treguar cilësitë tona më të mira. Mbi të gjitha, ne kurrë nuk e dimë kush do të na kërkojë në ekonominë tonë digjitale të sapo gjetur.

Të gjithë artikujt multimedialë të përdorur në këtë broshurë janë të licencuar nën një licencë Creative Commons dhe shkarkohen nga:

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, Heung-Soon, Patrick Lindenberg, Massimo Botturi.

Nga faqet vijuese:
https://www.iconfinder.com/
https://www.pexels.com/
https://pixabay.com/
https://unsplash.com/
https://www.slidescarnival.com
https://freepik.com/

techsoup EUROPE

METAMORPHOSIS

Foundation for sustainable ICT solutions