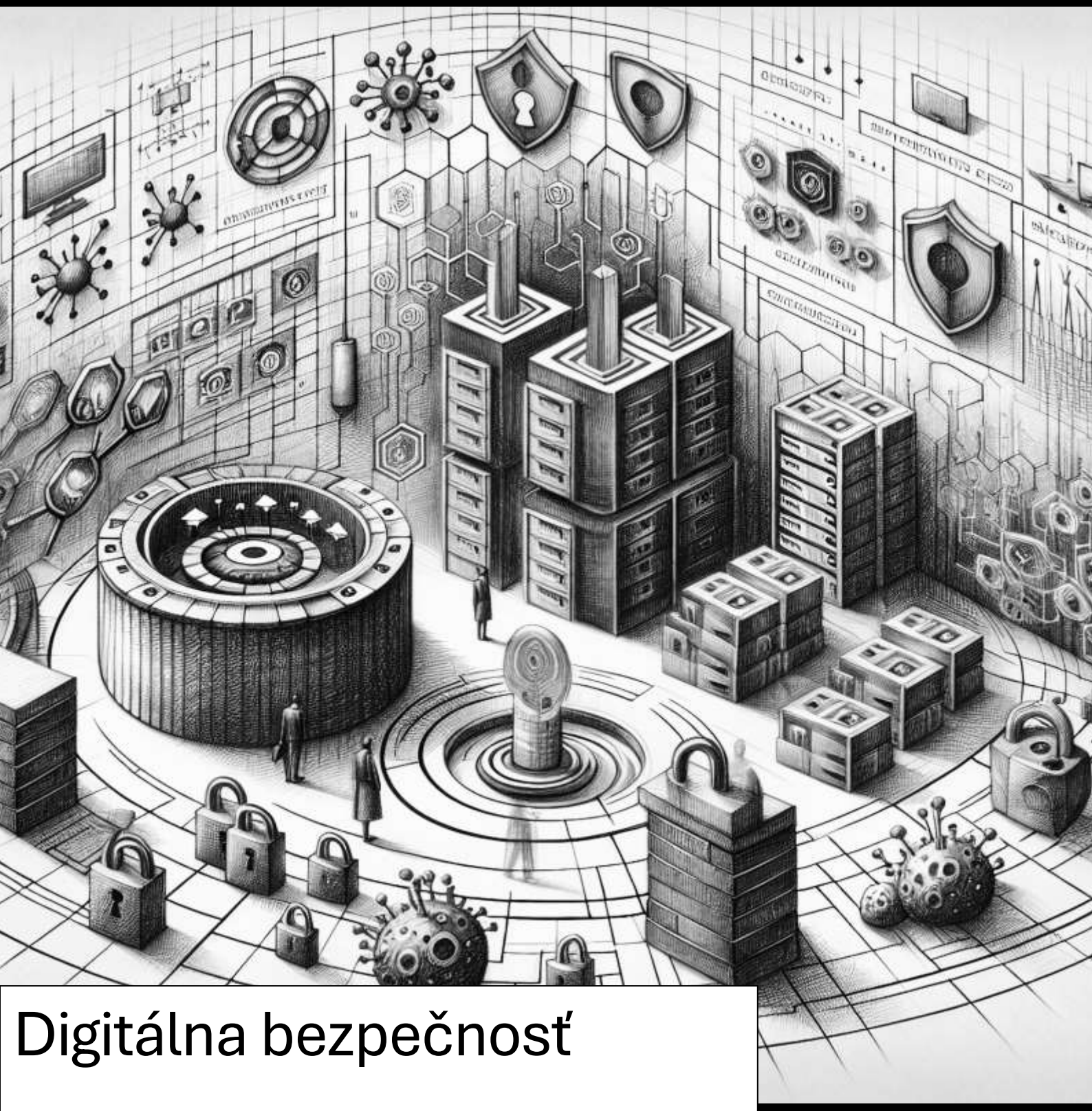

Digitálna bezpečnosť

Príručka pre novinárov

Digitálna bezpečnosť

Príručka pre novinárov

Alexandra Tóthová

Publikácia bola vytvorená na základe zdrojov pripravených počas edukačného programu Journalist Security Fellowship in Central and Southeastern Europe pod vedením Internews

Zdroj ilustračného obrázka: Stock AI-generated image ID #2475400847

Obsah

Dôležitosť digitálnej bezpečnosti 1
Heslá, správcovia hesiel, dvojfaktorové overenie 2
Správcovia hesiel 3
Vytvorenie silného hesla 3
Bezpečnostné otázky 4
Dvojstupňové overenie (2FA) 4
Phishing a ochrana proti nemu 4
Bezpečné odosielanie správ, bezpečné zdieľanie súborov a prečo je to dôležité 5
Prečo je bezpečné posielanie správ dôležité? 5
Ktorý četovací kanál na odosielanie správ je najlepší? 5
Zdieľanie súborov 6
Otváranie súborov 7
Bezpečná spolupráca s kolegami 7
Bezpečné prehliadanie internetu 8
IP adresa, VPN, prehliadač Tor 8
Chráňte svoje zariadenia 9
Zabezpečenie mobilného telefónu 10
Lokalizácia cez telefón 10
Stretnutie s citlivým zdrojom 11
Zabezpečenie PC 11
Šifrovanie 11
Papier 11
Online obťažovanie 11
Činnosti na zvládanie stresu: 12
Veci, ktoré môžete urobiť, aby ste sa ochránili: 13

Dôležitosť digitálnej bezpečnosti

Sára, novinárka pracujúca pre miestne a medzinárodné spravodajské organizácie, podáva správy o citlivých politických otázkach širokej škály, ako napríklad korupcia, zneužívanie ľudských práv, zneužívanie politickej moci a spôsoby vlády sťažujúce život určitým menšinám v jej krajine. Redakcia, pre ktorú pracuje, sa všeobecne považuje za dôveryhodný zdroj informácií. Vláda po parlamentných voľbách začala obmedzovať slobodu tlače, a prepadla redakcie a domy vybraných prominentných novinárov.

Zatiaľ čo postava Sáry je čisto fiktívna a akékoľvek podobnosti s realitou sú náhodné, počas týchto článkov bude ilustrovať dôležitosť digitálnej bezpečnosti s dôrazom na novinárov. Žurnalistika je svojou povahou mimoriadne stresujúca profesia. Zahŕňa rizikové situácie a osoby, nehovoriac o neustálom tlaku blížiacich sa termínov a klesajúcich šancoch na pracovnú stabilitu. Žurnalistika však hrá rozhodujúcu úlohu v demokratických spoločnostiach.

Slobodná, nezávislá žurnalistika, je dôležitá pre ochranu demokracie, nakoľko poskytuje informácie o miestnych, národných a medzinárodných udalostiach, ktoré ovplyvňujú životy v rôznych komunitách, a pomáhajú tak porozumieť zložitým problémom – vrátane korupcie alebo zneužívania moci, pričom vedú politické elity k zodpovednosti. Ich práca je kľúčová pre blaho spoločnosti. Kto však stráži novinárov?

V krajinách, kde sú médiá značne spolitizované, sú novinári potláčaní. Žiaľ, ide o globálny trend, ktorý sa objavuje aj na Slovensku. V súčasnej globálnej politickej klíme, je kľúčové zamerať sa na kybernetickú bezpečnosť, keďže tieto hrozby sú všadeprítomné a novinári ako skupina sú častejšie ich terčom. Tieto články sa snažia inšpirovať nielen novinárov, ale aj občiansku spoločnosť, aby prijali správnu digitálnu hygienu pre svoju bezpečnosť a ochranu pred hackermi, sledovaním alebo online obťažovaním.

Kybernetická bezpečnosť v skratke je obranou proti nepriateľským útokom spamerov, hackerov a kyberzločincov, ktorí cielia zariadenia a služby pripojené na internet. Kybernetická bezpečnosť je nápomocná aj proti zvedavým pohľadom tých, ktorí zneužívajú pozíciu moci proti kritikom. Kým samotný koncept sa môže zdať komplikovaným, dodržiavanie základných pravidiel pre zvýšenie vašej bezpečnosti a bezpečnosti vašich kolegov a okolia nemusí byť.

Ľudia nemajú radi, keď sú nútení dodržiavať bezpečnostné pravidlá, najmä ak tieto pravidlá nezapadajú presne do ich existujúcich pracovných postupov. Cieľom nasledujúcej série článkov je vysvetliť, prečo je dôležité dodržiavať určité bezpečnostné pravidlá, a tak uľahčiť ich každodenné používanie. Nedovoľte, aby snaha o dokonalosť prekážala dobrým riešeniam. Aj základné digitálne bezpečnostné opatrenia sú lepšie ako žiadne.

Sára pracuje s tímom novinárov na rôznych správach o korupcii. Nie všetci novinári v jej tíme však majú rovnakú úroveň digitálnych zručností, znalostí a postupov v oblasti bezpečnosti. Uvedomuje si, že niektorí členovia jej tímu majú tendenciu mať nedbalé postupy.

Počas vyšetrovania Sára dostane telefonát od svojho zdroja, so slovami „vláda vie, čo príde, došlo k úniku informácií“. Sára vie, že únik pochádzal zvnútra jej organizácie. Po kontrole riadenia prístupu sa dozvie, že tím dizajnérov mal prístup k celému zdieľanému Disku Google organizácie,

vrátane jej súboru s citlivými informáciami. Tím dizajnérov náhodou zdieľal súbor s nezávislým pracovníkom, ktorý tiež pracuje pre vládu.

Chyba nováčika, však? Je dôležité hovoriť o slabej digitálnej bezpečnosti, ktorá môže výrazne zabrzdiť kariéru novinára a ohrozovať postavenie kolegov a jednotlivých zdrojov. Dobré praktiky digitálnej bezpečnosti vedú k zabezpečeniu nielen vlastnej ochrany, ale aj ľudí okolo nás. Pri nábore nových členov tímu je dôležité mať na zreteli, aby prijali opatrenia digitálnej bezpečnosti, a aby ich využívanie bolo komfortné pre všetkých. V digitálnej doméne sme v bezpečí len tak, ako ten najslabší článok. Urobte malý prieskum okolo svojich kolegov, skontrolujte, či prijali bezpečnostné protokoly a či ich dodržiavajú, kto má prístup k súborom a informáciám. Pomôžete tak aj svojej osobnej bezpečnosti.

Cieľom tejto série článkov je podporiť používanie dobrej digitálnej hygieny a postupov kybernetickej bezpečnosti, v záujme ochrany pred krádežou identity, útokmi ransomware, phishingovými podvodmi, únikom údajov a peňažnými stratami. Mnohé organizácie fungujú bez prijatej oficiálnej bezpečnostnej politiky, čo tiež demonštruje, ako málo pozornosti sa venuje digitálnej bezpečnosti. Mnohí sa namiesto oficiálnej politiky spoliehajú na neoficiálne pravidlá a „dôveru“ svojich kolegov.

Je jasné, prečo to je v modernom, prevažne digitálnom svete, nedostatočné. Taktiež, je ťažké zaručiť, že všetci zamestnanci budú dodržiavať rovnaké bezpečnostné pokyny. Najbežnejšie bezpečnostné udalosti, napríklad taký phishing, môžu nových členov zaskočiť. Preto je dôležité rozprúdiť diskusiu o digitálnej bezpečnosti v každom novinárskom prostredí.

Digitálna bezpečnosť je neustály proces, nie konečný cieľ—vždy budú nové hrozby, ktoré si vyžadujú nové bezpečnostné praktiky. Koncept digitálnej bezpečnosti môže znieť komplikovane, ale osvojenie si základnej digitálnej hygieny nie je—práve to sa tieto články sa pokúsia potvrdiť a podať tému čo najjednoduchšie.

Heslá, správcovia hesiel, dvojfaktorové overenie

Sára použila rovnaké heslo pre svoj účet na Netflixe ako pre svoj pracovný e-mail. Jej účet na Netflixe unikol, čo predstavuje bezpečnostnú hrozbu pre jej tím.

V našom digitálnom živote máme množstvo rôznych online účtov, napríklad sociálne médiá, e-maily, služby zdravotnej poisťovne, účty pre nakupovanie a rôzne aplikácie na odosielanie správ, ako sú Messenger, Signal alebo WhatsApp. Keďže tieto účty často obsahujú obrovské množstvo potenciálne citlivých informácií, niektorí útočníci môžu mať veľký záujem získať k nim prístup alebo prevziať nad nimi kontrolu. Môžu dokonca chcieť zneužiť naše účty na personifikáciu, aby sa za nás vydávali. Z tohto dôvodu je nevyhnutné, aby sme udržiavali naše účty v bezpečí. Najlepším spôsobom, ako to dosiahnuť, je použitie dvojfaktorovej autentifikácie, vytváranie silných hesiel a vyhýbanie sa phishingu.

Webová stránka s názvom haveibeenpwned vie preveriť možný únik z jednotlivých účtov. Na hlavnej stránke vyhľadávania môžete zadať svoju e-mailovú adresu a zobrazia sa vám všetky úniky na ktorých sa podieľal. Toto efektívne ilustruje riziká spojené s opätovným použitím hesla na rôznych účtoch. Používanie rovnakého hesla je nebezpečná bezpečnostná praktika, pretože ak to niekto zistí heslo na jednej stránke, môže sa dostať aj na iné stránky – od e-mailu cez sociálne médiá, cez internet banking až po lekárske záznamy. Riešením, ako sa tomu vyhnúť, je všade používať jedinečné heslo.

Správcovia hesiel

Správcovia hesiel sú úžasné nástroje, ktoré pre vás vytvárajú a ukladajú jedinečné heslá. Odporúča sa ich používať čo najčastejšie. Tie v prehliadači fungujú skvele, heslá môžete tiež synchronizovať medzi rôznymi zariadeniami. Jeho cieľom je chrániť všetky vaše heslá pomocou jediného hlavného hesla. Hlavné heslo musí byť veľmi silné. Ako ďalšiu vrstvu ochrany môžete pridať aj dvojfaktorové overenie.

Správcov hesiel nie je vždy ľahké nastaviť alebo implementovať, a nemusia byť pre každého tá najlepšia voľba. Správcovia hesiel robia všetko pre to, aby zmiernili bezpečnostné problémy spojené s narušením údajov. Vytvára však jediný bod zlyhania a často je cieľom protivníkov.

Medzi odporúčaných správcov hesiel patrí 1Password (zdarma pre novinárov), eePassXC a BitWarden. Budete musieť stráviť nejaký čas, aby ste sa zoznámili s ich pokročilými funkciami, ako je napríklad automatické dopĺňanie okien webového prehliadača, ktoré môže chrániť pred niektorými útokmi, ako napríklad phishingom.

KeePassXC vám napríklad umožňuje ukladať všetky vaše heslá na vašom zariadení (a nie v cloude), zatiaľ čo 1Password vás upozorní, ak niektoré z vašich hesiel uniklo alebo bolo súčasťou narušenia bezpečnosti. Každý správca hesiel má iné nastavenia a funkcionality.

Ak sa na vás zameria silný protivník, napríklad z vlády a jeho štruktúr, je dôležité starostlivo vybrať správneho správcu hesiel a pohrať sa s nastaveniami, aby ste maximalizovali svoju bezpečnosť.

Ak váš počítač alebo telefón napadne spyware, spyware môže sledovať, ako zadávate hlavné heslo do správcu hesiel a ukradnúť vám tak všetky heslá. Preto je dôležité, aby vaše zariadenia neobsahovali škodlivý softvér. Ak máte podozrenie, že je vaše zariadenie infikované, obráťte sa na Access Now.

Ak nechcete tráviť čas správcom hesiel, existujú aj netechnické riešenia. Mať jedinečné heslo pre každú stránku, ktorú používate, a mať ho zapísané na kúsku papiera na bezpečnom mieste, je z hľadiska bezpečnosti lepšie ako opakované používanie jediného hesla na každej stránke.

Vytvorenie silného hesla

Mali by ste si zapamätať silné heslá, ktoré používate pre svoje zariadenie, šifrovanie a e-mailovú adresu.

Dobré heslo kombinuje veľké a malé písmená, čísla a špeciálne znaky. Najlepšie sú prístupové frázy pozostávajúce z viacerých náhodných slov. Ľudia však zvyčajne nie sú veľmi dobrí vo vytváraní náhodných, nepredvídateľných hesiel. Ak máte problém so zapamätaním si hesla, zamyslite sa nad tým, ako môžete skomplikovať niečo ľahko zapamätateľné. Programy na prelomenie hesiel fungujú so slovami zo slovníka, čím nepredvídateľnejšie to urobíte, tým bezpečnejšie bude. Čím viac charakterov, tým ťažšie je heslo prelomiť.

Príklad, ako si vytvoriť dobré heslo:

- heslo
- heslojeveslo
- Heslojeveslo007
- Heslojeveslo#007
- hesl@*JE*vesl@#007!

Všeobecne platí pravidlo, čím viac charakterov, znakov a čísel, tím bezpečnejšie. Kým prvú je možné prelomiť hackerským útokom viac-menej hneď, druhá (heslojeveslo) by trvala aspoň 5 sekúnd, tretia úroveň (Heslojeveslo007) podľa predpokladu 779 miliónov rokov. Posledná úroveň (hesl@*JE*vesl@#007!) je viac-menej neprelomiteľná.

Bezpečnostné otázky

"Ako sa volalo tvoje obľúbené zvieratko?" Tieto typy otázok často používajú stránky v prípade, že ste zabudli svoje heslo. Aj keď je to jednoduchý spôsob, ako sa dostať k svojmu účtu, problém môže byť v tom, že je to až príliš jednoduché. Zamyslite sa nad zadaním informácií, ktoré nie je také ľahké uhádnuť – napríklad meno a dátum narodenia zvieraťa alebo prezývku.

Dvojstupňové overenie (2FA)

Podstatou dvojfaktorového overenia je dvojstupňové overenie prístupu k vášmu účtu – silné heslo a druhý spôsob overenia. Druhý spôsob overenia je možné vykonať viacerými spôsobmi, napríklad SMS alebo e-mailovým kódom, overením doplnkovou aplikáciou alebo samostatným hardvérom vo forme bezpečnostného kľúča.

Bezpečnostný kľúč je vždy lepšou voľbou, pretože overenie SMS alebo e-mailu je možné presmerovať alebo obísť. Prostredníctvom programu Secure It Forward od Yubico môžu novinári získať bezplatné alebo lacné fyzické bezpečnostné kľúče.

Phishing a ochrana proti nemu

Typickou technikou pre útočníkov na získanie prístupu k vášmu účtu je phishing, tj. keď vám niekto pošle falošnú správu so žiadosťou, aby ste klikli na škodlivý odkaz a zadali svoje prihlasovacie údaje alebo stiahli malware. Medzi hlavné znaky phishingu môže patriť podivné fázovanie, pocit naliehavosti, podozrivá adresa URL, podozrivá e-mailová adresa odosielateľa atď.

Sára dostala phishingový e-mail, klikla naň, zadala svoje používateľské meno, heslo a kód 2FA, ktorý získala zo svojej aplikácie na overenie totožnosti. Uvedomila si, že ide o phishingovú stránku, až po zadaní svojich prihlasovacích údajov.

Phishingové útoky môžu oklamať aj skúsených bezpečnostných expertov pre ich desivú účinnosť a presvedčivosť. Odkaz, ktorý vedie k pokusu o phishing, môže vyzerať veľmi podobne ako bežne používané webové stránky, ako napríklad populárny účet sociálnych médií. Prihlasovacie údaje však nepovedú k bežnému prihláseniu, ale k uloženiu vašich údajov u útočníka.

Naučte sa rozpoznávať phishingové e-maily (chyby formátovania, odoslané z podivných adries, odkazy na nezvyčajné stránky, vyvolávanie pocitu naliehavosti), ale tiež používajte fyzické bezpečnostné kľúče a automatické dopĺňanie správcu hesiel ako ďalšiu ochranu.

Fyzické bezpečnostné kľúče sú odolné voči mnohým typom phishingu. Sofistikovaný útočník by mohol vytvoriť falošnú webovú stránku, ktorá vyzerá navlas rovnako, kde používatelia zadávajú nevedomky svoje heslá. Fyzické bezpečnostné kľúče, sú špeciálne vytvorené na zastavenie týchto útokov. Ak ste sa stali terčom, po phishingovom útoku si pre istotu zmeňte heslo.

Bezpečné odosielanie správ, bezpečné zdieľanie súborov a prečo je to dôležité

Prečo je bezpečné posielanie správ dôležité?

Sáru - novinárku, niekto kontaktoval cez Facebook Messenger s tvrdením, že má citlivé informácie z ministerstva obrany, o ktoré sa s ňou chce podeliť. Sára chce presunúť konverzáciu na bezpečnejší kanál, ktorý je end-to-end šifrovaný, aby ochránil zdroj.

End-to-end (E2E) šifrovanie znamená, že správu nie je možné počas prenosu prečítať, dokonca ani samotná spoločnosť, ktorá četový kanál prevádzkovala sa k nej nedostane tak jednoducho. Správa nebude uložená nezašifrovane ani na serveroch spoločnosti. Ak by bol hack k pripojenému účtu, ktorý bol použitý na odoslanie správy, pokiaľ neexistujú nezašifrované zálohy, nebudú mať prístup k obsahu správy. Správy však možno čítať aj inými spôsobmi, ak je telefón zaistený a odomknutý. V prípade šifrovania E2E nebudú mať orgány činné v trestnom konaní prístup k správe z kanála na odosielanie správ.

Používanie miznúcich správ vždy keď je to možné, najmä v prípade citlivých rozhovorov, pridáva ďalšiu vrstvu ochrany správy. Ak potrebujete archív správ, porozprávajte sa o alternatívnych spôsoboch ich uloženia (snímky obrazovky, ktoré sa odošlú do vašej redakcie a potom sa odstránia, písanie rukou do poznámkového bloku atď.).

Ktorý četovací kanál na odosielanie správ je najlepší?

Rôzne kanály pre odoslanie správ, nazývané aj messsengeri, pracujú s rôznymi modelmi hrozieb, preto každý z nich je trošku iný a neexistuje žiadny dokonalý nástroj. Väčšinu z nich môžete mať na rôznych prístrojoch, napr. v telefóne aj na počítači s úplnou synchronizáciou. Bezpečnostné prvky je však potrebné nastavovať individuálne na každom z prístrojov.

Signál je bezpečný kanál, ktorý sa zvyčajne odporúča. Ponúka *open source* E2E šifrovanie, nezhromažďuje žiadne metadáta a bol analyzovaný a schválený poprednými bezpečnostnými expertmi.

WhatsApp je tiež dobrou alternatívou. Aj keď poskytuje spoločnosti Meta prístup ku všetkým vašim metaúdajom, je šifrovaný E2E a bežnejší, takže je menej pravdepodobné, že pri jeho používaní vyniknete.

Obe tieto aplikácie vyžadujú napojenie na telefónne číslo, ktoré je zvyčajne registrované s osobným dokladom totožnosti. Ak novinári nechcú prezradiť svoje telefónne čísla, odporúčame im použiť Wire. Keďže je však menej bežný, môže vyniknúť a môže byť ťažké presvedčiť zdroje, aby ho používali). Signal tiež ponúka možnosť zdieľania len prezývky. Telegram je bežnejší ako Wire, ale musíte explicitne povoliť šifrované čety E2E a prehrabať sa nastaveniami, aby ste skryli svoje telefónne číslo.

V každom prípade musíte prejsť nastaveniami samotného kanálu pre posielanie správ či messengeru. Môže to zahŕňať povolenie miznutia správ, zakázanie nešifrovaných záloh v cloude a skrytie vášho profilu pred používateľmi, ktorí nie sú vo vašom zozname kontaktov.

Väčšina messengerov ponúka nejaký druh dvojfaktorovej autentifikácie, kde každý, kto si chce aktivovať svoj účet na novom zariadení, musí zadať špeciálne heslo. Heslo musí byť vždy

jedinečné. Nikdy neopakujte heslá ani nepoužívajte podobné na rôznych účtoch. Messengery môžete aj uzavrieť heslom alebo biometrickým údajom vo forme odtlačku prsta.

Povolenie dvojfaktorového overenia je vždy odporúčané všade, kde je to možné. Najlepšie sú fyzické vo forme bezpečnostného kľúča, hneď po nich nasledujú aplikácie na overovanie. Dvojfaktorová autentifikácia prostredníctvom SMS je najmenej bezpečná, ale oveľa lepšia ako nič.

Zdieľanie súborov

Počas práce na svojom investigatívnom projekte, dostane Sára telefonát od svojho zdroja so slovami „vláda vie, čo príde, došlo k úniku informácií“. Sára vie, že únik pochádzal zvnútra jej organizácie. Po kontrole riadenia prístupu sa dozvie, že tím dizajnérov mal prístup k celému zdieľanému Disku Google organizácie, vrátane jej súboru s citlivými informáciami. Tím dizajnérov náhodou zdieľal súbor s nezávislým pracovníkom, ktorý tiež pracuje aj pre vládu.

Tento typ chýb sa robí ľahšie ako sa môže zdať, preto je potrebné často kontrolovať zdieľané dokumenty a zdieľať informácie len podľa potreby. Dohodnite sa, ako má tím komunikovať, ukladať súbory a do akej miery kto k nim môže pristupovať. Uistite sa, že všetci dodržiavajú rovnaké protokoly týkajúce sa zdieľania súborov pre osobnú aj tímovú bezpečnosť.

Ak je to len trochu možné, veľmi citlivé informácie, ako napríklad totožnosť citlivých zdrojov, by sa mali zverejňovať len tým, ktorí ich skutočne potrebujú vedieť. Pri distribúcii dokumentov myslite na používanie pseudonymov a technikami možnej anonymizácie. Pri odosielaní dokumentov môžete použiť aj silné heslo (zdieľané iným kanálom, napr. miznúcou správou) pre súbory balíka Microsoft Office (Word, Excel).

Ak je to možné, nenoste súbory a dokumenty mimo pracovného prostredia (napr. preposielanie e-mailov na osobné účty, prenášanie materiálov domov na USB), pretože máte malú kontrolu nad tým, čo je nainštalované na týchto počítačoch, ak sú chránené silným heslom a majú aktuálny softvér.

Aj pri zdieľaní súborov je dôležité šifrovanie typu end-to-end. Súbory môžete bezpečne zdieľať s inými ľuďmi nasledujúcimi spôsobmi:

• Priamy prenos súborov cez Signál (podporuje až 100 MB dát)

- Využívanie programu OnionShare, ktorý bezpečne prenáša súbory cez prehliadač Tor (nie je stanovená maximálna veľkosť súboru).
- Používanie služby Tresorit Send (až 5 GB súborov)
- SecureDrop je tiež skvelý, ak chcete dostávať tipy a dokumenty anonymne, ale jeho použitie môže byť náročnejšie, pretože vyžaduje inštaláciu prehliadača Tor.
- Aplikácia s názvom Dangerzone premení potenciálne podozrivé dokumenty na bezpečné a čitateľné súbory PDF. Renomovaní programátori ho aktívne vyvíjajú, čo znamená, že je s každou verziou lepší a lepší.
- V redakcií si môžete tiež nastaviť verejné číslo signálu pre zdroje na zdieľanie súborov, vďaka čomu budú dostupné a jednoduché a E2E šifrované.

Otváranie súborov

Sára pracuje na reportovaní korupčného prípadu, ktorý sa týka dvoch krajín. V osobnom živote aj pracovne cestuje často. Dostala dokument od svojho zdroja z vládnych kruhov. Otvorí si ho, prečíta, ale keďže neobsahuje žiadne dôležité informácie, vymaže si ho. Neuvedomuje si, že dokument mal pripojený sledovač (napr. canary token), ktorý odosielateľovi oznamuje IP adresu cez ktorú si Sára dokument stiahla a cez ktorú možno určiť aj fyzickú adresu. Teraz jej zdroj vie, že pracuje na odhalení celého prípadu medzinárodnej korupcie.

Otváranie podozrivého súboru je súčasťou práce každého novinára, preto je dôležité venovať pozornosť otváraniu súboru BEZPEČNE. Najjednoduchším spôsobom dezinfekcie (odstránenie možných sledovačov a iných malware) je jednoducho do bezpečného cloudu, ako je Office 365 (online od spoločnosti Microsoft) alebo Disk Google pomocou bežného webového prehliadača. Majte na pamäti, že na to budete potrebovať účet u niektorého z týchto poskytovateľov (Gmail do určitej kapacity je bezplatný, Office 365 za poplatok).

Keď pristupujete k súboru na Disku Google alebo vo webovom vydaní Office 365, celý súbor sa otvorí a skonvertuje do formátu, ktorý váš webový prehliadač vidí na serveroch Google alebo Microsoft. Preto žiadne potenciálne škodlivé prvky v súbore neovplyvnia váš počítač, ale servery Google a Microsoft, ktoré sú vybavené na identifikáciu a odstránenie škodlivého softvéru.

Šikovne vytvorený škodlivý súbor, ako napríklad dokument balíka Office, by mohol infikovať zariadenie, či už ide o počítač alebo telefón. Z tohto dôvodu je najlepšie otvárať podozrivé súbory v telefóne alebo na Disku Google alebo v Office 365. Vyhnite sa počítačovým aplikáciám (Adobe, Word, Excel atď.), pretože potenciálny malware môže infikovať vaše zariadenie. Mnohé antivírusové softvéry dokážu podobné hrozby, ako je sledovanie, odhaliť.

Bezpečná spolupráca s kolegami

Zdieľané online dokumentov umožňuje efektívnu kolaboráciu na jednom dokumente pre celý tím. Jedna z najjednoduchších metód zdieľania súborov a spoločnej práce na dokumentoch, je prostredníctvom online služieb, ako je Disk Google alebo Office 365, pričom obe tieto služby považuje bezpečnostná komunita za bezpečné. Členovia vašej organizácie však musia dodržiavať prísne bezpečnostné konfigurácie (silné heslá, ideálne dvojstupňové overovanie). Všetci novinári, ktorí majú prístup k mimoriadne citlivým materiálom, by si mali pozrieť program rozšírenej ochrany Google (Google's Advanced Protection Programme).

Pri zdieľaných súboroch cez internet, ako je napríklad Disk Google, môžete ľahko zabudnúť na to, s kým a kedy ste zdieľali dokument. Aby ste predišli „permission creep“, čiže nežiadúceho sledovania obsahu dokumentov, nezabudnite pravidelne kontrolovať svoje súbory a zložky, alebo ich odstraňovať. Majte natrénovaný postup, ako niekomu odobrať prístup ku všetkým súborom, prihláseniam a privilégiám uverejňovania na sociálnych médiách v momente, keď opustia projekt, tím alebo organizáciu.

Bezpečné prehliadanie internetu

Na internet sme pripojení cez sieť. Keď niekto vo vašej sieti – napríklad zamestnanec telekomunikácií alebo office manažér – má prístup k nešifrovaným údajom, ktoré posielate cez sieť, môže dôjsť k sledovaniu siete. Môžu vidieť webové stránky, ktoré navštevujete (napr. www.wikipedia.org), alebo služby, ku ktorým ste pripojení (napr. Spotify), a to aj v prípadoch, keď je priame spojenie s webovou stránkou šifrované.

K sledovaniu zariadenia dochádza, keď niekto používa súbory cookie, napríklad na sledovanie vášho prehliadača alebo zariadenia. Vaša identita je zachovaná webovou stránkou, ktorú navštívite, aj keď sa pripojíte k inej sieti.

Sú situácie, keď je to naozaj užitočné, napríklad váš poskytovateľ webovej pošty rozpozná a pri používaní novej siete Wi-Fi sa nemusíte znova prihlasovať do svojho e-mailu. Problém je v tom, že vás môžu rozpoznať alebo identifikovať aj potenciálni nepriatelia a tiež reklama. Aj keď väčšina novinárov nie je ohrozená týmto druhom sledovania, je dobré mať na pamäti ochranu aj pred ním.

Pokiaľ ide o online sledovanie, môže mať dôsledky. Telekomunikačná alebo vládna agentúra môže vidieť webovú stránku, ktorú navštevujete (napríklad www.wikipedia.org), a aj to, koľko času na nej strávite, keď navštevujete túto webovú stránku, ale nie konkrétnu stránku, ktorú čítate (napr. https://sk.wikipedia.org/wiki/Konsk%C3%A1_hlava) .

Pri bezpečnom prehliadaní internetu si dajte otázku: mohlo by to potopiť vyšetrovanie, ak by telekomunikačné spoločnosti alebo vláda vedeli, aké stránky navštevujete? V závislosti od toho, pred kým sa chránime, existuje niekoľko vecí, ktoré môžeme použiť na zníženie sledovania internetu.

Sára cestuje. Po príchode na letisko ju zastaví a prehľadá hraničná polícia. Donútia ju odomknúť telefón. Všimne si, že polícia kontroluje jej kontakty, četovacie kanály a fotky. Bola na to pripravená, všetko citlivé odoslala do redakcie na bezpečný Google Drive a odstránila zo svojho zariadenia. Nevyčistila si však históriu prehliadania, kde hľadala adresu inštitúcie, do ktorej išla urobiť rozhovor.

História prehliadania ako taká sa dá použiť aj na získavanie citlivých informácií, ak je zariadenie skonfiškované. Naučte sa, ako si pravidelne mazať históriu prehliadaní a pravidelne opakujte tento úkon. Myslite nie len na históriu prehliadača, ale históriu vyhľadávaní v mobilných, ako sú napríklad Mapy Google.

Aj samotné internetové pripojenie je možné monitorovať. Pri používaní služieb Google, ako je Gmail, Disk Google, to nie je až taký problém, pretože sa zobrazuje iba pripojenie, nie presne to, čo sa deje počas pripojenia (nahrávanie súborov, odosielanie e-mailov atď.). V tomto prípade nie je potrebná virtuálna privátna sieť (virtual private network /VPN). Sú však situácie, kedy chcete svoje internetové pripojenie zamaskovať.

IP adresa, VPN, prehliadač Tor

Vašu IP adresu, pripojenie daného prístroja na internet na danej adrese, môžu vidieť webové stránky, ktoré navštívite, čo im môže umožniť určiť identitu vašej kancelárie alebo dokonca vašu geografickú polohu. Svoju IP adresu, môžete maskovať pomocou VPN.

Virtuálna privátna sieť (virtual private network /VPN) je často užitočným nástrojom, vytvára totiž odkaz, ktorý vás oddeľuje od webovej stránky, ktorú si prezeráte. To znamená, že zatiaľ čo váš

poskytovateľ VPN môže vidieť, čo prehliadate, váš telekomunikačný systém ani vláda to nemôžu priamo zobraziť. Pri používaní VPN môžete zmeniť virtuálne aj krajinu, kde prehliadate danú webstránku, čiže úspešne obchádza geo-blokáciu (napr. otvorenie Facebooku v Číne). Vyberte si spoľahlivého dodávateľa, pretože bude mať prístup k vašim metaúdajom. Nedôveryhodná sieť VPN môže byť skôr hrozbou ako pomocníkom.

Odporúčania VPN:

- TunnelBear je kanadská služba VPN.

- Mullvad je služba VPN na báze open source so sídlom vo Švédsku.

- ProtonVPN je švajčiarska služba VPN.

Prehliadač Tor je tiež fantastický anonymizačný nástroj. Smeruje váš webový prenos cez sériu ďalších počítačov, čo sťažuje každému protivníkovi sledovanie vášho prehliadania.

Mnohé webové stránky zároveň môžu blokovať pripojenia cez prehliadač Tor, či už explicitne (jednoduchým odmietnutím pripojenia) alebo implicitne (budú vás žiadať o častú verifikáciu, napríklad tak, že vás donútia neustále vyberať obrázky dopravných značiek). Ak používate prehliadač Tor, možno budete musieť upraviť niektoré svoje zvyky pri prehliadaní. Prehliadač Tor použite vtedy, keď požadujete vyššiu úroveň anonymity ako poskytujú siete VPN, napríklad pri skúmaní veľmi citlivých tém. Trh s VPN sa pravidelne mení, takže odporúčania môžu rýchlo zastarať. Prehliadač Tor sťažuje každému útočníkovi sledovanie vašej aktivity pri surfovaní presmerovaním vášho webového prenosu cez množstvo iných počítačov. Niekedy môžete pracovať na mieste, kde je určitý obsah cenzurovaný, obmedzený alebo nedostupný. Tor a VPN tiež umožňujú obísť cenzúru.

Chráňte svoje zariadenia

V pondelok ráno prichádza do redakcie, v ktorej Sára pracuje, asi 50 policajtov. Majú povolenie, ktoré sa ukáže šéfredaktorovi. Následne žiadajú všetkých novinárov, aby okamžite odišli, nechajúc všetky pracovné zariadenia, dokumenty, poznámky a pod. v kancelárií.

Je prirodzené, že kolegovia budú chcieť byť v kontakte, a tak vytvoria skupinový chat (cez Signal alebo WhatsApp). V tomto prípade môže byť dobrý nápad komunikovať prostredníctvom súkromných telefónov namiesto pracovných čísel, pretože tie by sa mi mohli spájať so zariadeniami, ktoré zostali v kancelárii.

V takýchto prípadoch všetky kroky by ste mali najskôr konzultovať s právnikom, pretože akékoľvek kroky smerom k ochrane vašich zdrojov by sa mohli považovať za manipuláciu s dôkazmi. V prípade zničenia dôkazov by z toho mohol nastať právny problém. Ak je to možné, odhláste sa na diaľku zo všetkých zariadení, ktoré sú v kancelárii, a zmeňte si heslá.

V takýchto situáciách je dôležité myslieť na osobnú bezpečnosť aj bezpečnosť a organizácie, no v neposlednom rade aj na bezpečnosť vašich zdrojov. Väčšina situácií, kedy je digitálna bezpečnosť nejakým spôsobom ohrozená, nie je taká intenzívna. Strata zariadenia, nedbalosť v prístupe k zdieľaným dokumentom, phishingové útoky, neinštalovanie silného antivírusového programu sú bežnejšie spôsoby, ako sa citlivé informácie môžu dostať do nesprávnych rúk.

Zabezpečenie mobilného telefónu

Zdroj posiela citlivé súbory Sáre cez Signal, ona si ich prezerá na svojom mobile. Je spokojná, že má informácie k dispozícii, a v piatok večer ide so svojimi priateľmi osláviť narodeniny. Na večierku stratí telefón a uvedomí si, že jej jednoduché heslo (1111) možno ľahko uhádnuť. Začína panikáriť. Čo môže urobiť?

Vo všeobecnosti sú mobilné telefóny bezpečnejšie ako notebooky a stolné počítače. V predvolenom nastavení sú takmer vždy šifrované, majú špecializovaný bezpečnostný hardvér a často môžu spúšťať aplikácie iba zo schválených zdrojov (čo spomaľuje šírenie malware).

Telefón si však musíte chrániť aj heslom. S prístupovým kódom (alebo odtlačkom prsta) nebude mať niekto, kto sa pokúša ukradnúť alebo našiel váš stratený/ukradnutý telefón, prístup k jeho obsahu. Aj keď sú biometrické heslá pohodlné, napríklad odtlačok prsta alebo rozpoznávanie tváre, nemusia byť najbezpečnejšie. Niekto vás môže prinútiť priložiť prst na telefón, aby ste ho odomkli. Číselné prístupové kódy sa považujú za bezpečnejšie, ale je potrebné, aby kombinoval rôzne čísla, ktoré nie je tak ľahké uhádnuť.

Okrem hesla, musíte aktualizovať softvér v telefóne vždy keď je nová aktualizácia dostupná. Protivníci hľadajú softvérové chyby alebo medzery, aby sa dostali do vášho telefónu bez povolenia. Keď sa nájde jedna z týchto bodov zraniteľností, program sa aktualizuje, aby napravil bezpečnostnú medzeru a znemožnil ďalší útok. V systéme Android aj iOS môžete vyhľadávať a inštalovať aktualizácie alebo zapnúť automatické aktualizácie. Keď už váš model telefónu nepodporuje aktualizácie softvéru, je čas prejsť na nový.

Aj pri najväčšom nastavení zabezpečenia môžete byť požiadaní o odomknutie telefónu – napríklad pri prekročení hraníc hraničnou políciou. Preto je dobré používať miznúce správy na kritické rozhovory, a pri prípadnej nebezpečnej situácií úplne vymazať četovacie aplikácie a mať vo zvyku pravidelne odstraňovať citlivé údaje z telefónu, ktoré už možno nepotrebujete.

Čo môže Sára urobiť vo svojej situácii? Ak je táto funkcia zapnutá, môže na diaľku vymazať celý obsah telefónu. Môže sa prihlásiť do svojich e-mailových účtov a účtov sociálnych médií cez iné zariadenie, aby si okamžite zmenila heslá, a ak je to možné, môže sa odhlásiť zo všetkých prihlásených zariadení. Ako preventívne opatrenie v budúcnosti, môže tiež uzamknúť všetky svoje aplikácie, napríklad Messenger, dodatočným heslom alebo biometrickým údajom.

Váš telefón vám môže odobrať bezpečnostná služba alebo orgány činné v trestnom konaní, napríklad počas prehľadávania. Nemyslite si, že váš telefón je po vrátení bezpečný, nakoľko sa naň mohol nainštalovať malware. Najlepším riešením by bola výmena zadržaného telefónu za nový model. Ďalšou metódou by bolo čo najskôr vykonať úplné obnovenie továrenských nastavení.

Úplné obnovenie továrenských nastavení odstráni všetky údaje z telefónu vrátane kontaktov, správ, obrázkov a všetkých ostatných údajov. Buďte na toto pripravení a použite na obnovu zálohu. Po dokončení resetovania zmeňte pre každý prípad všetky svoje heslá.

Lokalizácia cez telefón

Aby mobilná telefónna sieť prepojila konkrétny telefón s príslušnou vežou a mohla z nej odosielať a prijímať signály, musí sa telefón najskôr lokalizovať. Mali by ste predpokladať, že váš mobilný operátor vie o polohe vášho telefónu vždy, keď je zapnutý. Na miestach ako sú preplnené mestá, kde je viac mobilných veží, sa môže telefón lokalizovať presnejšie. Tiež existuje množstvo

aplikácií, ktoré dokážu sledovať vašu polohu. Pravidelne kontrolujte tieto aplikácie a udeľujte prístup k svojej polohe iba počas ich používania (napr. Google Mapy).

Stretnutie s citlivým zdrojom

Citlivé zdroje si vo všeobecnosti vyžadujú väčšiu pozornosť na ich ochranu a bezpečnosť. Môžete napr. uvažovať o pseudonymoch pri ukladaní ich kontaktu ako o forme anonymizácie.

Ďalším aspektom ktorý je potrebné mať na zreteli je lokalizácia. Vzhľadom na lokalizáciu by ste mali venovať pozornosť vášmu telefónu. Ak máte naplánované citlivé stretnutie a obávate sa, že vládna agentúra alebo telekomunikačná spoločnosť by mohli využiť údaje o polohe na zistenie, či sa nachádzate na rovnakom mieste,nevypínajte svoje telefóny tesne pred stretnutím alebo hneď, ako sa dostanete na miesto stretnutia. Oveľa rozumnejšie je pokúsiť sa napodobniť typické činnosti, ako napríklad nechať telefóny zapnuté doma alebo v práci pred stretnutím (alebo ich vypnúť niekoľko hodín vopred, ak ste typ človeka, ktorému sa batérie v telefóne neustále vybíjajú). Ktokoľvek, kto vás alebo váš zdroj sleduje, môže rýchlo zistiť, ak sa zariadenia oboch ľudí náhle prestanú pripájať k sieti.

Zabezpečenie PC

To najmenej, čo môžete urobiť, je uzamknúť počítač silným heslom a nenechať počítač bežať bez neho, keď na ňom nepracujete. Pravidelne reštartujte počítač, aby ste aktualizovali softvér. Zamknite svoje citlivé dokumenty uložené v dokumente heslom (platí aj pre dokumenty Excel a Word). Nainštalujte si dobrý antivírus.

Šifrovanie

Používanie nástrojov ako VeraCrypt alebo podobných, je užitočné pri šifrovaní dát na pevných diskoch, USB alebo externých diskoch.

Papier

Bezpečnostné praktiky by sa mali týkať aj papierových poznámkových blokov, je tiež dôležité mať na pamäti fyzické kópie dokumentov. Skryte svoje poznámky, nenechávajte ich na rovnakom mieste ako iné citlivé zariadenia, ideálne ich zamknite a pri vytváraní poznámok používajte pseudonymy, prezývky, akronymy a skratky, ktorým rozumiete len vy. Zvážte pravidelné skartovanie toho, čo nepotrebujete. Skenujte a zničte papierové dokumenty, používajte šifrovanú digitálnu zálohu. Buďte si tiež vedomí akýchkoľvek právnych dôsledkov ukladania citlivých informácií u vás doma a nie v kancelárii.

Online obťažovanie

Sára pracuje na článku o etnických menšinách a o tom, ako vládna politika vedie k väčšej marginalizácii tejto skupiny. Počas niekoľkých týždňov si Sára všimne prudký nárast komentárov na sociálnych sieťach, kde zdieľa osobné príspevky aj svoju prácu. Začnú prúdiť nenávistné a hanlivé komentáre. Všimne si, že sa na ňu zameriavajú trollovia.

Nahlási problém svojim mužským kolegom, ktorí jej povedia, aby sa tým netrápila, že to zmizne samé. Je však v strese, a má pocit, že ju členovia jej tímu nepočúvajú, alebo sa nesnažia pochopiť jej situáciu.

V prvom rade je dôležité si všimnúť, že tieto kampane trollov sa zameriavajú na mužov a ženy rozdielne, pričom ženy sú zvyčajne zasiahnuté tvrdšie, pretože je podnietená aj nenávisťou súvisiaca s pohlavím.

Ak dôjde k nehode, po príchode na miesto záchranári vyhodnotia všetky fyzické zranenia, ktoré obeť môže mať. Hoci sa online obťažovanie niekedy zdá byť obmedzené na „virtuálny" svet, musíme si byť vedomí aj dopadov na fyzickú stránku osoby, ktorá ho zažíva.

Našťastie, hovoriť o duševnom zdraví je čoraz menej tabuizované. Náš mozog reaguje podobne na fyzické aj virtuálne hrozby a keď čelí hrozbe, spúšťa kortizolom poháňanú reakciu *„boj, uteč alebo zamraz"* (FFF, Fight, Flight, Freeze). Telo rozpozná, že je čas prejsť do „režimu prežitia", spustí sa stresový cyklus. Režim prežitia vyžaduje veľa energie, preto FFF reakcia má prednosť pred všetkým ostatným v mozgu, vrátane myslenia. Náš autopilot je aktivovaný. Reagujeme rovnako na leva stojaceho pred nami, ako na online hrozbu,

Aj keď prežijeme, reakcia FFF nás vyčerpáva. Koniec ohrozenia nie je dostatočnou informáciou na to, aby telo ukončilo reakciu na ohrozenie. Zvládnutie stresora sa nerovná zvládaniu stresu. To je dôvod, prečo je *„dokončenie stresového cyklu"* kľúčovou úlohou. Nielenže musíme pochopiť cyklus ako taký, ale musíme ho tiež aplikovať na naše pravidelné praktiky duševného zdravia. Dosiahnutie záveru nášho stresového cyklu znamená oznámiť nášmu telu, že sme v bezpečí.

Čo môže Sára v jej situácií urobiť? Môže skontrolovať, či trollovia používajú rovnaký jazyk, kľúčové slová alebo dokonca hashtagy, čo naznačuje koordinovanú kampaň. Tiež si môže pozrieť najbežnejší čas odoslania, pretože opäť, môže indikovať automatizovanú a koordinovanú kampaň. Môže tiež použiť vstavané funkcie na sociálnych sieťach, ako sú blokovania a hlásenia alebo priamo kontaktovať spoločnosti sociálnych médií a nahlásiť rozsiahle obťažovanie.

V mnohých prípadoch sa trollovia chcú pozornosť a publicitu, preto ich nechajte bez reakcie, ak môžete, lebo ak uvidia, vyvolali reakciu, budú sa snažiť otravovať ďalej. Ak je to možné, radšej trollov stlmte ako blokujte – veľa ich odpovedí už neuvidíte, no oni nebudú vedieť, že sú stlmení. Blokovanie a správu trollov môžete zadať externe aj spoločnosti Trollwall. Podobne môže pomôcť aplikácia Block Party znížiť obťažovanie na Twitteri tým, že stlmí alebo zníži viditeľnosť obťažujúceho obsahu a identifikuje tých, ktorí ho šíria.

Keď potrebujete kritizovať reakciu trolla, najlepšie je urobiť snímku obrazovky jeho príspevku a okomentovať ho, než citovať alebo odpovedať na pôvodný príspevok. Týmto spôsobom môžete ostatným ukázať vyhlásenie trolla bez toho, aby ste ich upozornili alebo získali odporúčacie algoritmy na propagáciu príspevku.

Online obťažovanie, kampane trollov, očierňovacie kampane či nenávistné prejav,môžu prispieť k preťaženiu úrovne stresu, teda nervového systému a mozgu. Zvládanie stresu je preto kľúčové pravidelným uzatváraním cyklu stresu. Stres môžeme odbúrať športom, vzťahmi s ostatnými, hraním sa so psami alebo tvorbou umenia, tieto aktivity nadobúdajú väčší význam.

Činnosti na zvládanie stresu:

- Šport, pohyb tela

- Dýchacie techniky, meditácia

- Pozitívne sociálne vzťahy (priatelia, rodina, ale aj pozitívne rozhovory s neznámymi ľuďmi)

- Blízke vzťahy a náklonnosť: partner, priatelia, rodina, domáce zvieratá

- Pustite to von. Plač je v poriadku. Smiať sa je v poriadku.

- Podporovať svoju kreativitu a umenie, nájsť tam pokoj

- Duchovno, príroda, spojiť sa s niečím väčším.

Mali by sme venovať pozornosť verbálnym zločinom (nenávistné prejavy), kyberšikane, doxxingu, online obťažovaniu a akémukoľvek inému druhu online prenasledovania. Negatívne dopady takéhoto prenasledovania na telesnú a duševnú pohodu už nie sú spoločensky prijateľné. Môžu spôsobiť škodu, ktorá je rovnaká alebo väčšia ako fyzické násilie, môžu ovplyvniť viac než len bezprostredný cieľ a majú ďalekosiahle účinky na náš život. Je možné, že budú cielení aj vaši rodinní príslušníci.

Dôsledky online obťažovania môžu byť pre väčšinu ľudí ťažko pochopiteľné, takže buďte opatrní, keď hľadáte radu. Keď sa členovia rodiny alebo priatelia s dobrými úmyslami pýtajú, "nemohli by ste jednoducho odstrániť svoje účty na sociálnych sieťach?" môžu vec neúmyselne zhoršiť bagatelizovaním. Hoci takéto otázky môžu pochádzať z úprimného želania pomôcť, môžu v konečnom dôsledku minimalizovať vaše emocionálne utrpenie a prehliadať zložitosť okolností jednotlivca zamestnaného v médiách.

Z dlhodobého hľadiska je rozhodujúce vytvorenie efektívnej siete podpory. Novinári a ich organizácie by mali tráviť čas investovaním do sietí priateľov, odborníkov v oblasti duševného zdravia a odborníkov, ktorí im môžu pomôcť, ak sa situácia zhorší.

Veci, ktoré môžete urobiť, aby ste sa ochránili:

- Mať politiku *žiadne fotografie v redakcii*

- Zapnite žiadosť o kontrolu pred označením na fotografiách na sociálnych médiách

- Odstráňte staré fotografie, najmä tie, ktoré by mohli ohroziť vašu reputáciu (fotky z univerzitných večierkov atď.). Zamyslite sa nad množstvom obrázkov s vašou tvárou, a nad tým, ako sa dá AI vycvičiť na vytvorenie kompromitujúceho deepfake s využitím vašich fotografií.

- Pred zverejnením svojich osobných fotografií si premyslite, aké informácie sa zdieľajú. Nezverejňujte fotografie zo svojho okolia (nebezpečenstvo zverejnenia adresy vášho bydliska) alebo z miest, kam často cestujete (napr. miestne kúpalisko, opäť existuje nebezpečenstvo prenesenia obťažovania z internetu na fyzické obťažovanie)

- Nezverejňujte verejne fotografie členov svojej rodiny alebo priateľov, s ktorými sa často stretávate

- Poproste priateľa alebo vyhľadajte svoje meno na webe, analyzujte svoje sociálne médiá z pohľadu cudzieho človeka a zhrňte všetky informácie, ktoré tam nájdete. Pozor, počas tohto cvičenia sa môžete cítiť zraniteľne a odhaliť citlivé detaily.

- Pokračujte v uverejňovaní obsahu súvisiaceho s prácou, ale obmedzte osobný obsah. Ak úplne vypadnete z internetu, vyhrajú trollovia.