

MĂSURI DE SIGURANȚĂ ÎN MEDIUL ONLINE

Mediul online și tehnologia sunt într-o evoluție constantă, care depășește capacitatea utilizatorului de a ține pasul cu schimbările, de a descoperi și înțelege toate riscurile și de a-și integra metodele de utilizare sigură. Nu e suficient să învățăm modul de utilizare al unui echipament, aplicații sau platforme, avem nevoie să înțelegem și care sunt termenii și condițiile de utilizare, ce este permis și ce nu este permis să facem online, felul în care suntem expuși când folosim aplicațiile și dispozitivele și cum putem fi în siguranță.

În cazul unor agresiuni în mediul online, recomandarea de a renunța la telefon, de a-și închide conturile sau de a se retrage din mediul online nu este o soluție, victima fiind cea care trebuie să suporte din nou consecințele unui comportament nepotrivit al agresorului și al modului în care acesta alege să folosească tehnologia. O astfel de măsură izolează victima de grupul de prieteni, de familie, îi afectează viața socială și profesională. Nu este o garanție că renunțarea la tehnologie va face ca abuzul să înceteze, ci poate determina agresorul să găsească noi modalități de a hărțui și să afecteze capacitatea victimei de a căuta și găsi ajutor. Schimbarea numărului de telefon, a adresei de e-mail sau conturilor sunt strategii protective, dar nu soluții, întrucât nu persoana agresată ar trebui să fie cea care să își schimbe viața pentru a se adapta hărțuirii și controlului abuziv al altcuiva. De asemenea, accesul la tehnologie și conturi poate fi util și în procesul de strângere a dovezilor și monitorizării agresorului, permițând astfel persoanei agresate să fie cu un pas înaintă.

Pentru a reduce vulnerabilitatea în mediul online și pentru a fi protejate de eventualele agresiuni, e necesară cunoașterea măsurilor de creștere a siguranței online.

PAROLELE

Parolarea reprezintă una dintre primele măsuri pe care le putem lua pentru protejarea conturilor și dispozitivelor. Anumite site-uri care cer conectarea cu cont specifică criteriile pe care trebuie să le îndeplinească o parolă pentru a fi sigură: minim 8 caractere, obligatoriu o literă mare și un caracter special.



De reținut despre parole:

- Recomandarea e de minim 16 caractere, 26 e și mai bine. Cu cât este mai lungă parola, cu atât e mai dificil de spart. De exemplu, puteți să vă verificați propria parolă pe site-ul <https://howsecureismypassword.net/>, care vă indică în cât timp un computer ar putea sparge parola utilizată.

- Puteți verifica dacă parolele sau conturile utilizate au fost implicate într-un furt de date pe <https://haveibeenpwned.com/>

- Folosiți parole diferite pentru fiecare cont sau dispozitiv

- Folosiți combinații de litere mari, litere mici, cifre și caractere speciale

- Puteți înlocui vocalele cu caractere speciale (de exemplu, a cu @)

- Puteți folosi o frază, un vers, un citat preferat

- Parolele trebuie să fie confidențiale, cunoscute doar de utilizator

- Pot fi stocate într-un password manager (Keychain pentru iOS, LastPass, Dashlane etc.), care se accesează cu o parolă unică

- Nu le salvați în browserul de internet, de exemplu Google password manager, mai ales când o altă persoană are acces la dispozitivul respectiv, întrucât poate accesa și conturile fără dificultate prin completarea automată a userului și parolei.

Să reținem că a păstra confidențialitatea asupra parolilor nu înseamnă că există ceva de ascuns, ci este despre a avea posibilitatea de a alege ce informații oferi altora despre tine, autonomie, putere și control asupra mediului online și propriei vieți.

MANAGERUL DE PAROLE / PASSWORD MANAGER

Când utilizăm conturi multiple de e-mail sau aplicații, poate fi dificil să reținem fiecare parolă, cu atât mai mult cu cât acestea ar trebui să fie unice. Pentru a păstra toate parolele în siguranță sau pentru a genera unele foarte sigure, poate fi utilizat un manager de parole. Este similar unui seif în care sunt stocate parolele, pentru accesarea căruia e necesar un cifru, reprezentat de parola unică (master password).

Managerul de parole poate fi browser-based (o aplicație care rulează direct în browserul de internet, fără să fie nevoie de descărcare pe dispozitiv, ci doar de acces la internet) sau software-based (necesită descărcare și instalare pe dispozitiv): LastPass <https://www.lastpass.com/> - browser-based sau Dashlane <https://www.dashlane.com/> - software-based. Pot fi gratuite sau cu plată.

De reținut despre managerul de parole:

- Stochează parolele într-o formă criptată, neinteligibilă
- Poate genera parole complexe, sigure

- 
- Vă reamintește când trebuie schimbate parolele
 - Vă avertizează dacă refoleșiți o parolă mai veche sau utilizată deja la un alt cont
 - O singură parolă unică - master password - trebuie reținută, cea care permite accesul la managerul de parole și permite completarea automată a datelor de logare la conturi și aplicații

AUTENTIFICAREA CU DOI FACTORI / ÎN DOI PAȘI

Autentificarea cu doi factori/în doi pași (two-factor authentication - 2FA) reprezintă o măsură suplimentară de siguranță, care dublează securizarea cu parolă și minimizează riscul ca datele sau conturile să fie compromise, chiar dacă cineva cunoaște parola acestora. Există trei modalități pentru autentificare: ceva ce știi (parola), ceva ce ai (telefon sau token bancar) și ceva ce ești (amprentă, voce, față). Autentificarea cu doi factori folosește o combinație a două dintre aceste modalități. Poate fi utilizată atât pentru e-mail, cât și pentru aplicații, de exemplu Facebook, Twitter, Instagram, WhatsApp, Telegram etc.

De reținut despre autentificarea cu doi factori:

- Autentificarea cu doi factori poate fi realizată fie prin trimiterea un cod unic prin sms, e-mail sau se dă un cod de recuperare, în funcție de opțiunea setată
- Avantajul acestei metode este că avertizează în momentul în care s-a încercat o conectare la cont de pe alt dispozitiv sau dintr-un alt browser, solicitând un cod și/sau parola de conectare pentru a confirma că utilizatorul este cel care accesează contul
- Poate oferi informații de pe ce tip de dispozitiv și din ce locație s-a încercat accesarea
- Activarea opțiunii poate fi utilă persoanelor care au părăsit partenerul agresiv pentru a se asigura că acesta nu îi accesează conturile în mod abuziv

GEOLOCALIZAREA

Geolocalizarea este una dintre modalitățile frecvente prin care o persoană oferă informații despre locul în care se află la un moment dat, fără intenție. Și asta se întâmplă pentru că atât aplicațiile, cât și browserele, au acces la locație, precum și sistemele sau aplicațiile de urmărire.

De reținut despre geolocalizare:

- Poate oferi informații agresorului despre locația în care se află victima sa
- o Din fotografiile publicate în social media care au activată localizarea, prin identificarea longitudinii și



latitudinii sau căutând imagini similare pe Google

- o Din eticheta aplicată locației atunci când fotografia este publicată în social media de către victimă sau prietenii acesteia

- o Din accesarea istoricului locațiilor în Google, în cazul în care conturile de pe telefonul mobil al victimei și cel de pe computerul de familie sunt sincronizate

- o Prin instalarea unei aplicații - fie prin acces direct la telefon, fie instalarea de la distanță (remote) prin accesarea unui link - care pot accesa atât GPS-ul telefonului, cât și listele de apeluri, conversațiile tip text, parolele, conversațiile telefonice (de exemplu Celltrack, Go&Find, Flexispy, Auto Forward etc.). Cele mai multe dintre ele sunt contra cost, dar oferă posibilitatea de utilizare gratuită pentru o perioadă de testare

- o Prin instalarea unui dispozitiv de urmărire pe mașină, în poșetă sau haine

- o Google monitorizează și contul, nu doar dispozitivul, așadar informații precum istoricul locațiilor, istoricul căutărilor pot fi accesate de agresor de pe un computer comun

- Google poate identifica poziția
 - o În funcție de adresa de IP pe care vă conectați
 - o Din activitatea anterioară, în funcție de căutarea pe internet
 - o Din locațiile etichetate
 - o De pe dispozitiv, dacă aveți activat GPS-ul pentru hărți
 - o Dacă este activat Serviciul de localizare
 - o Chiar dacă dezactivați serviciile de localizare, poziția dispozitivului tot va fi afișată, dacă este GPS-ul activat

Recomandări pentru creșterea siguranței:

- Verificați în setările telefonului ce permisiuni au aplicațiile instalate și dezactivați accesul la ceea ce nu este necesar (de exemplu, dezactivarea accesului camerei foto la locație, dezactivarea accesului Google la fotografii, telefon, locație, microfon etc.), cu mențiunea că anumite setări pot afecta funcționarea aplicațiilor - dezactivarea accesului WhatsApp la microfon afectează apelurile făcute prin intermediul acestei aplicații, dezactivarea accesului WhatsApp la fotografii împiedică transmiterea lor

- Dezactivați locația din setările telefonului. Atenție! Acest lucru ar putea afecta modul în care funcționează hărțile (Google maps, Waze)

- Eliminați etichetarea locației la camera foto, întrucât poate conține longitudinea și latitudinea locului în care a fost făcută o fotografie, conducând agresorul la victimă

- Nu folosiți geolocalizarea la niciuna dintre aplicații sau



site-uri accesate

- Nu folosiți dispozitive la care are acces altcineva, dacă nu vreți să aibă acces la informații despre locurile în care ați fost - va găsi o metodă să le vadă, dacă are un nivel mediu de cunoștințe despre internet
- Setări aplicațiile la cel mai înalt nivel de securitate
- Blocați aplicațiile și site-urile când solicită accesarea locației
- Nu sincronizați conturile de pe dispozitive
- Ștergeți istoricul din browser, inclusiv de la Google maps. Atenție! Se poate opta pentru ștergerea istoricului pe anumite perioade de timp (3 luni, 18 luni, 36 luni), dar dacă agresorul obișnuiește să verifice locațiile anterioare, ștergerea totală a istoricului îi poate trezi suspiciuni.
- Pentru mai multă siguranță, în cazul în care setările par dificil de făcut, alte două opțiuni sunt închiderea telefonului sau scoaterea bateriei de la telefon pentru a evita înregistrarea locației
- Atenție la sms-urile care par venite din partea unui cunoscut/partener, care conțin link-uri care ar trebui accesate. Se poate instala astfel o aplicație de supraveghere la distanță
- Verificați lista de aplicații instalate și dacă nu sunt cunoscute posesorului telefonului, dezinstalați-le

NAVIGAREA PE INTERNET ÎN SIGURANȚĂ

Utilizarea internetului și comportamentul în mediul online sunt două elemente care vulnerabilizează în fața agresorilor, de aceea este important să cunoașteți măsurile pentru păstrarea confidențialității și creșterea siguranței, mai ales dacă suspectați că cineva vă urmărește activitatea în mediul online.

Recomandări pentru creșterea siguranței:

- Actualizați (update) browserele
- Accesați pagini HTTPS (Hypertext Transfer Protocol Secure), care au un lacăt în fața numelui site-ului, și care asigură utilizatorul că datele sale sunt în siguranță, cum ar fi informațiile despre cardurile bancare (Atenție! în ultima perioadă, atacatorii creează pagini HTTPS pentru a păcăli utilizatorul că sunt site-uri sigure, în special cele cu vânzare de produse. O măsură de siguranță suplimentară ar fi introducerea manuală a website-ului în loc de accesarea link-ului trimis)
- Activați opțiunea "Do not track" când accesați anumite pagini (unele dintre ele întreabă)
- Folosiți Incognito mode/Navigare privată când accesați pagini Google/Safari/Internet Explorer/Mozilla pentru ca



activitatea în mediul online să nu poată fi detectată pe dispozitiv în istoricul de navigare. Cu toate acestea, dacă sunt descărcate sau marcate anumite pagini, acestea vor fi vizibile. Activarea opțiunii este diferită în funcție de sistemul de operare folosit - iOS, Android, Windows sau macOS.

- Ștergeți istoricul de navigare/history. Atenție la cazurile în care agresorul obișnuiește să verifice activitatea din mediul online, situație în care se recomandă ștergerea fiecărei căutări individual, prin apăsarea literei X care apare în dreapta site-ului căutat

- Folosiți antivirus și firewall - protejează de malware (virusi, trojani, spyware)

- Ștergeți cookie-urile

Cookie-urile sunt fișiere create de site-urile pe care le vizitați. Acestea vă ușurează experiența online salvând informații de navigare. Cu ajutorul cookie-urilor, site-urile pot:

- o să vă mențină conectat(ă);

- o să memoreze preferințele voastre pentru site-uri;

- o să vă ofere conținut relevant la nivel local.

Cookie-urile sunt folosite pentru a îmbunătăți serviciile. Dezactivarea lor depinde de sistemul de operare și browserul folosit.

- Nu salvați parolele în browser - vezi capitolul referitor la parole

- Nu apăsați pe link-uri suspecte, bannere, pop-ups care apar la navigarea pe o pagină de internet

- Nu sincronizați conturile între dispozitive, pentru că atunci agresorul poate accesa activitatea din mediul online de pe dispozitivul sincronizat cu cel al supraviețuitoarei

SIGURANȚA ÎN SOCIAL MEDIA

În această eră digitală, este de așteptat ca rețelele sociale să fie folosite de agresori pentru a amenința și hărțui. Abuzatorii își pot crea conturi false sau adrese de e-mail în acest scop, bazându-se pe faptul că nu vor fi prinși, chiar dacă există un ordin de protecție care le interzice să-și contacteze victima.

Utilizarea diferitelor platforme variază în funcție de vârstă: WhatsApp este una dintre cele mai utilizate platforme de mesagerie de persoane de toate vârstele; femeile tinere folosesc Facebook mai des decât adolescentele, care preferă Instagram. Adolescencele folosesc mult mai mult decât alte categorii de vârstă Snapchat și tot mai popularul TikTok. Nu toate aceste platforme sunt spații publice de chat deschise: WhatsApp, de exemplu, este un serviciu de



mesagerie închis, în timp ce Facebook, TikTok și Instagram permit interacțiuni deschise și prezintă un risc mai mare de hărțuire din partea unor necunoscuți.

Rețelele sociale încurajează utilizarea de noi funcții și aplicații, expunând utilizatorii la și mai multe scurgeri de date. Facebook este rețeaua socială dominantă, cu 2.9 miliarde de utilizatori în 2021.

Recomandări pentru creșterea siguranței:

Setări de securitate

- Faceți setările de securitate ale contului la cel mai înalt nivel

- Întrebați-vă cine mai are acces la contul meu? Este un cont împărțit? Cine e administrator? Cine mai poate posta pe el?

- Nu vă folosiți numele real

- Creați o adresă de e-mail separată specială pentru social media/pentru fiecare cont online

- Folosiți o parolă puternică

- Setări autentificare cu 2 factori

- Setări alerte despre conectări neautorizate

- Setări profilul pe "privat"

- Dezactivați locația

- Dezactivați "Vizibilitatea prezenței" la messenger pentru ca un agresor să nu știe când sunteți online. Și WhatsApp are această opțiune (Setări - Cont - Confidențialitate - Confirmări de citire) care, odată activată, nu mai permite expeditorului să vadă dacă mesajul a fost citit. Regula nu se aplică și conversațiilor din grupuri sau mesajelor vocale, care, chiar dacă opțiunea "Confirmare de citire" este dezactivată, vor fi bifate ca citite când destinatarul va asculta mesajul

- Limitați accesul celorlalți la datele voastre personale prin selectarea informațiilor de profil care să fie cunoscute celorlalți

- Setări profilul și etichetarea la nivel maxim de siguranță

- Activați notificarea pentru etichetare și revizuirea etichetării

- Setări postările implicit pentru "prieteni"

- Nu folosiți Facebook pentru conectarea la alte aplicații și site-uri

Comportamentul în social media

- Conținutul este în acord cu politicile platformei

- Faceți fotografii și postări doar cu acordul celorlalți care vor fi incluși

- Etichetați cu precauție persoanele, după ce le-ați obținut acordul

- Nu etichetați locația în care vă aflați



- Asigurați-vă că nu e activată locația la camera foto
- Nu dați check-in în locația în care vă aflați, pentru a permite accesul unui hărtuitor la această informație
- Nu postați fotografii care pot duce la identificarea locației și persoanelor
- Nu postați și nu trimiteți pe messenger/chat fotografii intime

Construirea comunității de prieteni din online

- Împrieteniți-vă doar cu oameni pe care îi cunoașteți în viața reală
- Verificați ce prieteni aveți în comun, verificați-le profilul și postările anterioare (dacă au cont public)
- Dacă nu sunteți sigură că profilul aparține persoanei pe care o cunoașteți în viața reală, sunați-o, verificați informația direct
- Blocați și raportați agresorii și conturile false
- Avertizați familia, prietenii despre agresori care folosesc un anumit cont pentru a se împrieteni cu ei și astfel pentru a avea acces la dumneavoastră

FUNDAȚIA SENSIBLU

CENTRUL DE CONSILIERE CASA BLU

Telefon / Fax: 021 - 311 46 36

Mobil : 0787 54 18 54

fundatia.sensiblu@adpharma.com

www.fundatiasensiblu.ro

<https://www.facebook.com/Fundatia.Sensiblu>