Ghidul #WorkingSafeOnline

bazat pe principii de securitate

Activitățile online au fost întotdeauna însoțite de provocări din perspectiva siguranței cibernetice. Începând cu măsurile de pandemie COVID -19 și limitare a mobilității, din ce în ce mai mulți cetățeni au ajuns să depindă de mijloace digitale, atât în scopuri personale, cât și profesionale - context în care siguranța online a devenit o preocupare din ce în ce mai mare.

Cu beneficii digitale vin și riscuri pe măsură, cu toate acestea, acest aspect nu ar trebui să fie un motiv de panică sau teamă în a utiliza noile tehnologii. Dimpotrivă, acesta este cel mai bun moment pentru a ne schimba comportamentul digital prin utilizarea tehnologiei cu o atitudine responsabilă - în timpul și după finalizarea pandemiei.

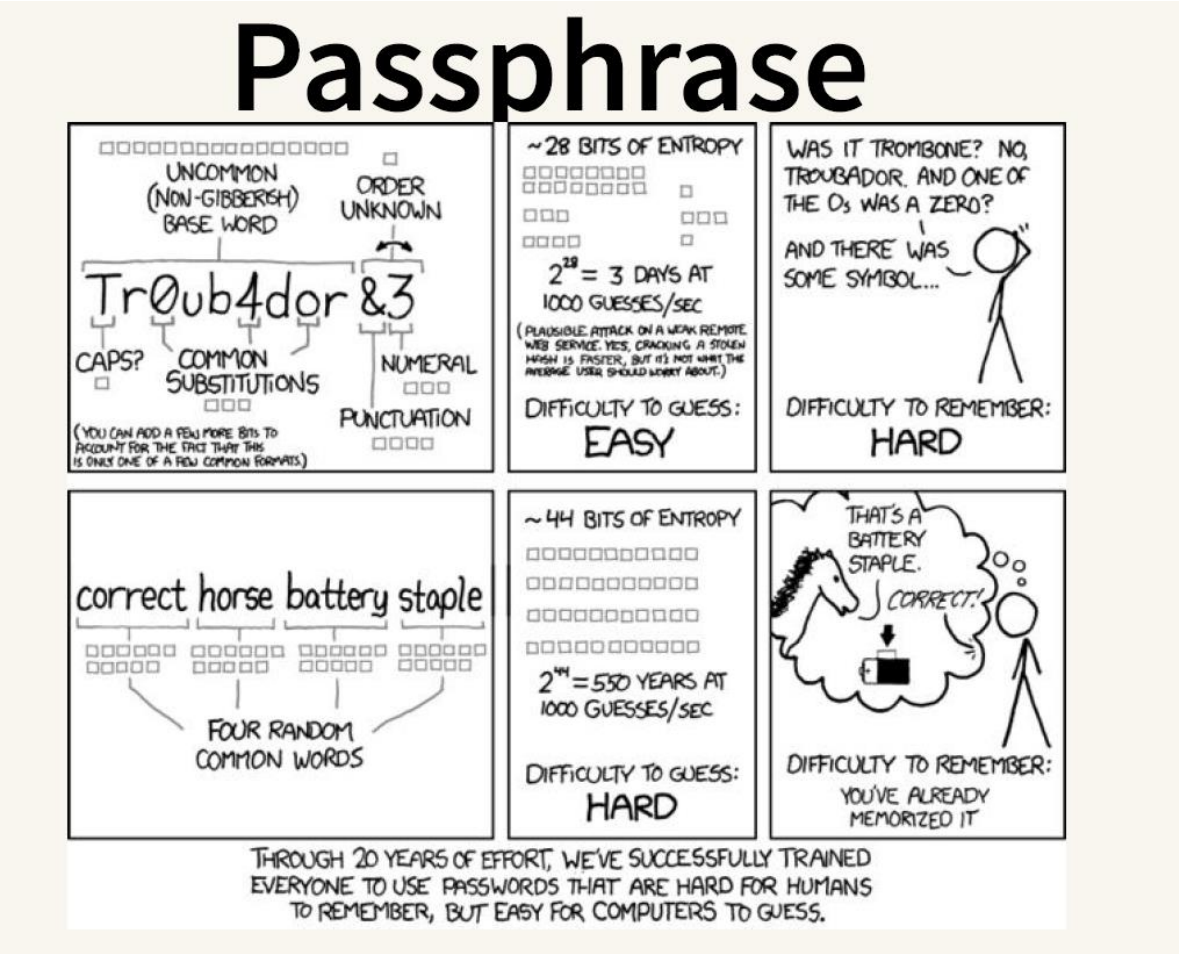
Ghidul actual este dedicat atât *persoanelor fizice* (profesori, studenți, telemuncitori, părinți sau cetățeni digitali de zi cu zi), cât și *organizațiilor* (ONG-uri, întreprinderi mici și mijlocii, freelancers).

Scopul acestui Ghid este de a veni în întâmpinarea utilizatorilor de internet și tehnologie cu o serie de bune practici care să asigure măsuri minime de siguranță pentru toată lumea. Am inclus elemente de bază și am oferit exemple care ar putea face transformarea digitală mai accesibilă pentru toți utilizatorii. Practicile și exemplele incluse în acest Ghid nu sunt însă exhaustive, întrucât în ceea ce privește securitatea și siguranța digitală sunt mult mai multe lucruri care trebuie luate în considerare.

Sperăm că acest Ghid va fi util în activitatea pe care o desfășurați și vă invităm să împărtășiți cu noi experiențele dvs. personale în lumea digitală. Nu ezitați să ne contactați dacă doriți să transmiteți feedback, recomandări sau idei noi la adresa contact@digitalcitizens.net.

Folosiți parole lungi / 2FA

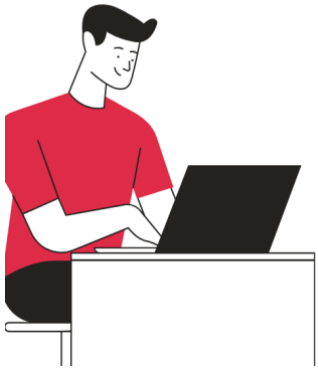
- ***Alegeți o parolă lungă*** formată din șase sau mai multe CUVINTE aleatorii (Passphrase) pentru a vă bloca computerul. Șase sau mai multe numere ca PIN - pentru a vă bloca telefonul - unde este posibil.
- Activați ***autentificarea „în doi factori" sau „în doi pași"*** pe Google, Facebook sau alte conturi online.
- ***Protejați-vă parolele*** - Nu reutilizați parolele! Utilizați un manager de parole dacă este posibil.



⇛ *Dacă sunteți interesat să aflați cât de sigură este parola dvs. o **puteți testa aici**!*

Fiți conștienți de cine are acces la datele dvs. și ce date partajați

- ***Evaluați instrumentele pe care*** le utilizați.
- Verificați-vă ***setările de confidențialitate*** în conturile de rețele sociale. Este posibil ca aceste site-uri să ofere altor utilizatori/entități mai multe informații despre dvs. decât intenționați să transmiteți.
- ***Monitorizați-*** vă conturile pentru activitatea suspectă.



⇛ *Aruncați o privire la acest proiect dacă sunteți interesați să înțelegeți și să controlați mai bine* ***urmele pe care le lăsați online*** *https://myshadow.org/*

Fiți atenți ce accesați

- Evitați click-urile pe link-uri suspecte sau atașamente de e-mail, în special de la persoane pe care nu le cunoașteți. Obiceiurile dvs. online ar putea fi dăunătoare indiferent de ce instrumente/ aplicații folosiți.
- Evitați trimiterea de ***informații sensibile*** pe site-urile web accesate prin link-uri trimise de un terț necunoscut prin e-mail/SMS. Dacă este posibil, este mai bine să introduceți manual adresa URL a site-ului web în browserul dvs., în loc să faceți click pe link, pentru a evita phishingul.
- Instalați aplicații numai din ***surse de încredere***, renunțați la descărcarea aplicațiilor piratate.

⇛ *Phishing - este încercarea frauduloasă de a obține informații sensibile, cum ar fi numele de utilizator, parolele și detaliile cardului de credit, deghizându-se ca o entitate de încredere într-o comunicare electronică.*

Faceți o copie de rezervă a datelor/backup - este una dintre cele mai bune practici care trebuie luate în considerare zilnic.

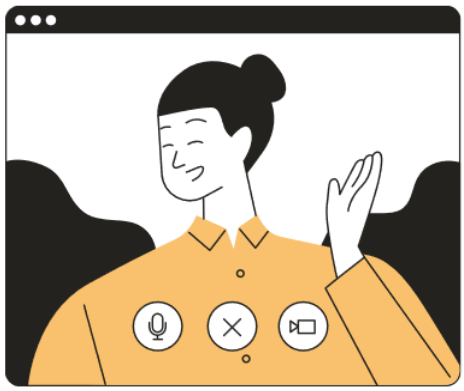
- ***Pentru computerul*** dvs. puteți utiliza stick-uri USB, hard disk-uri externe sau NAS (Network Attached Storage - folosit de obicei pentru mai multe computere în rețea).
- ***Stocare în cloud*** - puteți alege dintre o varietate de furnizori precum: iCloud, Dropbox, Google Drive și OneDrive - pentru documente, fișiere, fotografii - cu siguranță cel mai comod în zilele noastre, ușor de accesat și de partajat cu două condiții. Prima și cea mai importantă - conexiunea obligatorie la internet pentru a le putea accesa. A doua, politica de gestionare a datelor personale a platformei, trebuie să fiți atenți la acest aspect mai ales dacă stocați date sensibile. O atenție particulară trebuie acordată condițiilor de utilizare când folosiți conturi "gratuite".
- ***Smartphone*** - în funcție de sistemul de operare, de obicei, datele sunt salvate în cloud. Verificați setările pentru a decide ce date salvați și cât de des. Puteți decide să faceți backup pentru telefon manual descărcând conținutul pe computer/sau alt disc extern.
- ***Website-ul organizației*** - asigurați-vă că aveți o copie locală a site-ului dvs. web. Verificați politicile de backup cu furnizorul dvs. de găzduire - host provider și pe CMS (Sistem de gestionare a conținutului) pe care îl utilizați. De exemplu CMS WordPress are plugin-uri speciale doar pentru Backup.

⇛ *Aici puteți găsi mai multe argumente pro și contra tuturor acestor idei!*

Păstrați dispozitivul în siguranță și actualizat

- Mențineți ***actualizat sistemul de operare al*** dispozitivului utilizat, puteți activa Actualizările automate.
- Utilizați browsere web care primesc frecvent actualizări automate de securitate, ca de ex. Chrome sau Firefox.
- Asigurați-vă că aveți ***plug-in-urile*** pe care le folosiți in ***browser***, ***actualizate*** (ex. Flash, Java etc.).
- ***Criptați datele***. Majoritatea dispozitivelor sunt capabile să cripteze datele dacă activați această funcție - consultați documentația dispozitivului pentru opțiunile disponibile sau citiți mai multe despre acest subiect.

Conectați-vă in mod inteligent din afara biroului - de acasă către fișierele salvate pe server-ul din birou sau la distanță când utilizați o rețea publică, ca de exemplu în cafenea, în restaurant sau în hotel în timpul unui transfer.



- Nu utilizați niciodată internetul pe un computer care nu are un software ***antivirus*****,** antimalware și / sau firewall instalat. Dacă faceți acest lucru, există o posibilitate crescută ca un hacker să poată instala malware sau keylogger pentru a sustrage informații.
- Utilizați un ***firewall*** - Mac și Windows au firewall-uri de bază pentru desktop integrat în sistemul de operare, care vă pot ajuta să vă protejați computerul împotriva atacurilor externe. Citiți mai multe despre ce face un firewall!
- Folosiți **VPN** (rețea privată virtuală). Funcționează ca un tunel care vă protejează conexiunea. În loc să expuneți date personale celor care controlează rețeaua, le trimiteți prin intermediul unui furnizor de încredere. Dacă organizația dvs. nu are un VPN vă recomandam să citiți acest ghid și, după caz, să discutați cu un consultant IT.

⇛ ***Definiție antivirus*** *- uneori numit și* ***anti-malware****, este un software / program conceput și dezvoltat pentru a proteja calculatoarele împotriva malware-urilor precum viruși, computer worms, spyware, botnets, rootkits, keyloggers și altele similare. Programele* ***antivirus*** *scanează, detectează și elimină viruși de pe computer. Instalați programe antivirus numai dintr-o sursă cunoscută și de încredere. Mențineți actualizate definițiile virușilor, motoarele și software-ul antivirusului pentru a vă asigura că programul dvs. rămâne eficient. Iată o imagine de ansamblu actualizată!*

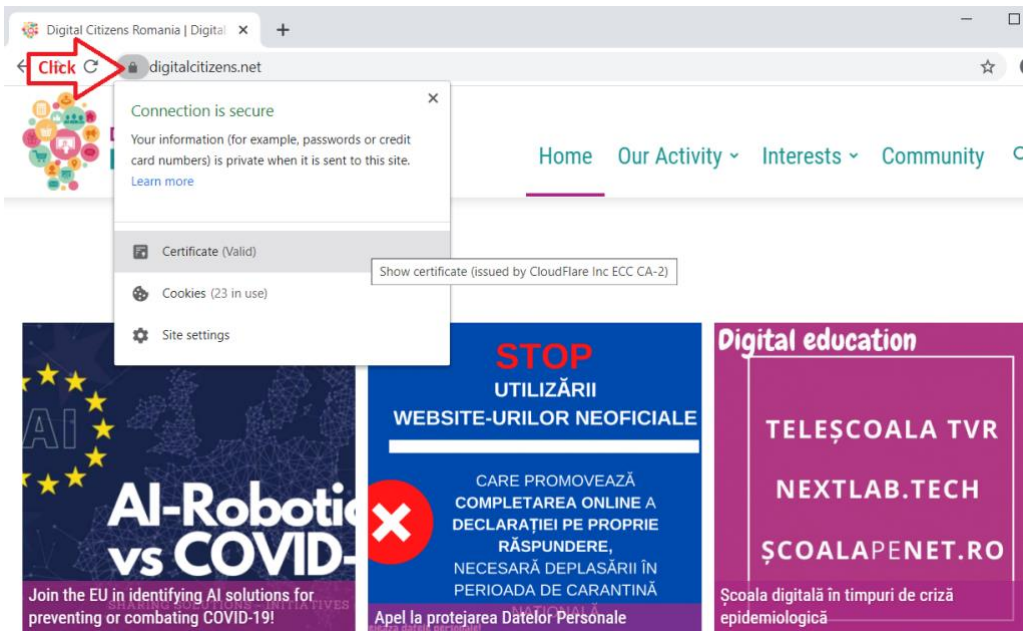
Protejați date sensibile

- Informați-vă despre definiția datelor sensibile si care sunt acestea. Dacă organizația dvs. gestionează / prelucrează date precum informații despre cardul de credit, înregistrări ale elevilor/studenților/minorilor, informații despre sănătate și orice alte informații personale, ar trebui să acordați atenție în special regulilor ***GDPR*** *- Regulamentul general privind protecția datelor, în vigoare din 25 mai 2018, care se adresează tuturor celor care interacționează cu cetățeni din statele membre ale Uniunii Europene.*

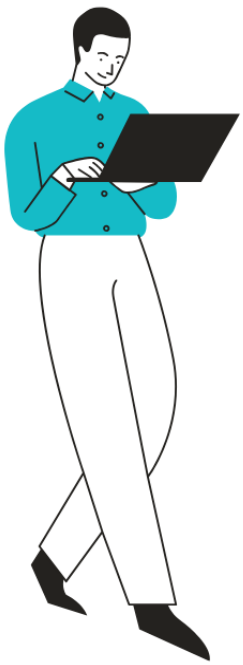
- GDPR se aplică tuturor organizațiilor - companii mari, dar și tuturor IMM-urilor și ONG-urilor, nimeni nu este scutit!
- Acordați o atenție deosebită Principiilor GDPR și drepturilor cetățenilor - instruiți-vă corect personalul și informați beneficiarii.
- Pentru mai multe exemple practice, puteți citi standardul UCB de clasificare al datelor, care include o clasificare pe niveluri de protecție a datelor și restricțiile asociate. Rețineți că exemplele incluse în link nu sunt neapărat conforme cu toate regulile GDPR.
- Desemnați o persoană din organizația dvs. să gestioneze acest tip de date.

- Nu salvați datele sensibile pe laptop, dispozitive mobile sau alte echipamente de lucru și eliminați acest tip de fișiere din sistemul dvs. atunci când nu mai sunt necesare.
- Accesați serviciile bancare sau cumpărăturile online numai pe dispozitive și rețele de încredere și deconectați-vă întotdeauna după aceste site-uri atunci când ați finalizat tranzacțiile.
- Utilizați întotdeauna criptarea atunci când stocați sau transmiteți date sensibile. Cu site-urile care necesită o autentificare, asigurați-vă că există un lacăt în bara browserului care indică o conexiune HTTPS sau prezența certificatului Secure Sockets Layer (SSL) și că adresa URL este cea corectă și nu o versiune modificată a site-ului propriu-zis.

Iată cum puteți verifica certificatul HTTPS / SSL în Chrome (alte browsere sunt similare). Atunci când conexiunea este criptată, veți găsi întotdeauna pictograma lacătului in bara de adresă a browserului:



Informați-vă despre ce trebuie făcut în cazul în care deveniți o victimă cibernetică



- Dacă primiți mesaje de avertizare despre activități suspecte sau dacă observați activități pe care dvs. nu le recunoașteți:
  - primul lucru pe care trebuie să-l faceți este să schimbați parola!
  - al doilea, controlați alte conturi conectate la profilul suspect. De exemplu, dacă vă conectați cu un cont Google pe contul universitar, trebui să verificați și acest cont în momentul în care primul cont devine suspect.
- Dacă suspectați un furt de identitate sau un alt tip de atac online, trebui să îl raportați autorităților și poliției naționale, nu ezitați să le contactați!
  - Pentru cetățenii români: folosiți CERT.ro formular de raport și contactați poliția română.
- Alertați banca dacă aveți probleme cu cardul dvs. de credit sau dacă ați trimis informații despre contul vostru de internet banking unor entități suspecte (prin SMS, telefon sau e-mail, pe site-uri de comerț electronic etc.).
- Raportați înșelătoria / frauda direct pe platforma unde ați deschis „oferta”. În cazul în care identificați publicitate falsă, folosiți instrumentele puse la dispoziție de platforme pentru a raporta frauda, în special pe Facebook și alte rețele de socializare.
- În cazul phishingului, avertizați și compania „victimă” (de exemplu, dacă observați o ofertă falsă care pretinde că provine de la o bancă sau un magazin online, dar adresa URL nu este site-ul original, ar trebui să îi informați despre situație, după ce ați alertat și CERT sau Poliția).
- În cazul pierderii sau furtului telefonului, folosiți pentru Apple Find my iPhone sau pentru Android Device Manager.

Separați viața privată de cea profesională

- Nu utilizați profilul personal de social media pentru asociația / organizația dvs. Nu este ideal să aveți clienți care se conectează pe contul dvs. privat de Facebook. În schimb, creați o pagină Facebook / Twitter / Instagram pentru organizația dvs. și faceți ca beneficiarii / utilizatorii să se conecteze cu dvs. prin intermediul acelui cont.

- Nu folosiți adresa dvs. de e-mail personală pentru activități legate de muncă.
    - Creați o adresă de e-mail profesională separată, strict pentru activitatea organizației și asigurați-vă că parola este diferită de cea a adresei dvs. de e-mail principale.
    - Asigurați-vă că aveți un cont oficial al organizației și apoi unul separat pentru fiecare membru din organizație.
    - În mod ideal, nu ar trebui să utilizați Yahoo, Gmail sau alte platforme de e-mail generice. Dacă aveți resurse, investiți într-un nume de domeniu personalizat.

Ghidul #WorkingSafeOnline - pentru a lucra în siguranță online, bazat pe principii de securitate, este creat de echipa Digital Citizens:

- Mihaela TUDORACHE - cercetare, dezvoltare de conținut, adaptare text, imagini*
- Veronica ȘTEFAN - dezvoltare de conținut, editare

Urmărește comunitatea Digital Citizens prin canalul tău media preferat

Facebook.com/DigitalCitizensRomania/
Linkedin.com/company/digital-citizens-romania
Twitter.com/DigitalRomania
Youtube.com/channel/UC_p4vd6Y9E4eivHpz8tPssgVizualizările

*Imaginile incluse în Ghidul și promovarea campaniei online au fost create folosind aplicația Canva.

Resurse utile

- Instrument pentru raportarea de criminalitate informatică online pentru toate țările Europol
- Raport (pdf) privind criminalitatea informatică și Dezinformarea în timpul COVID-19, Europol
- Agenția UE pentru Securitate Cibernetică (ENISA), Resurse pentru COVID-19
- Resurse furnizate de Asociația TechSoup pentru organizațiile non profit din toată lumea
- Resurse gratuite pentru pasionații de securitate digitală - Security Education Companion