Sfaturi pentru a vă proteja online

Accesul online vă ajută să rămâneţi conectat cu familia şi prietenii, vă ţine la curent cu noutăţile, vă oferă acces la învăţare online şi multe altele. Dar este întotdeauna o idee bună să ţineţi cont de securitate şi există o mulţime de lucruri pe care le puteţi face pentru a vă proteja.

1. Fiţi conştienţi de informaţiile pe care le partajaţi

Când completaţi un profil pentru un cont, daţi doar **informaţiile necesare** şi pe care vă simţiţi confortabil să le oferiţi.

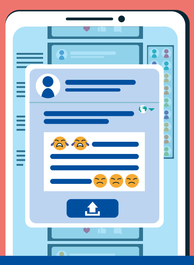
Utilizaţi **setările de confidenţialitate** şi securitate şi dezactivaţi toate funcţiile de care nu aveţi nevoie.

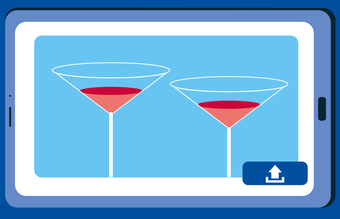
Dacă nu sunteţi sigur, reconsideraţi crearea profilului cu compania sau pe platforma respectivă.

2. Gândiţi-vă înainte de a posta

Postarea când eşti emoţional nu este întotdeauna o idee bună, ceea ce postezi online **rămâne acolo pentru totdeauna**. Chiar dacă îl ştergeţi ulterior, cineva l-ar fi putut salva sau redirecţiona.

Aşteptaţi până când sunteţi mai liniştiţi, apoi gândiţi-vă din nou, chiar doriţi să postaţi acel comentariu, acel video sau acea poză?





3. Analizaţi din timp consecinţele

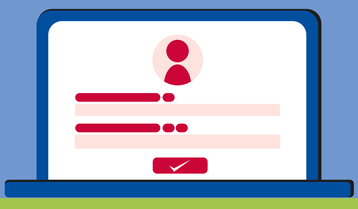
Dacă postaţi o fotografie, v-aţi gândit dacă toată lumea din fotografie este fericită să o publicaţi? Este posibil să oferiţi informaţii, cum ar fi locul în care locuiţi.

Pînă şi postarea fotografiilor din vacanţă poate atrage spărgători atunci când nu eşti acasă!

4. Pauză înainte de a juca

Înainte de a lua parte la un joc distractiv vestit pe reţelele de socializare, ia în considerare ceea ce te întreabă - numele primului tău animal de companie, numele de fată al mamei tale?

Acestea sunt aceleaşi întrebări care sunt utilizate pentru securitate, de exemplu de către bancă, astfel încât răspunsul la acestea ar putea fi furnizarea de informaţii importante hackerilor.



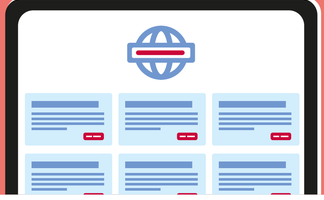
5. Asiguraţi-vă că ştiţi cu cine comunicaţi

Reţineţi că escrocii folosesc reţelele sociale, site-urile web şi vă trimit mesaje pe telefon pentru a vă fura informaţiile, banii sau identitatea.

Vă puteţi proteja fără a furniza informaţii personale, bani sau detalii despre cont, cu excepţia cazului în care puteţi verifica prin **alt mijloc de comunicare** cui i le distribuiţi.

6. Urmăriţi noutăţile despre securitatea cibernetică

Urmăriţi ştirile sau solicitaţi familiei/prietenilor să vă anunţe despre escrocheriile care sunt în circulaţie, de ex. escrocheriile de phishing, software-ul rău intenţionat, site-urile web false vă pot ajuta să rămâneţi în siguranţă online.



enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN CYBER SECURITY MONTH

#CyberSecMonth #ThinkB4UClick

I.P „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică”

Sfaturi privind asigurarea securităţii cibernetice a locuinţei

Internetul obiectelor (IoT) este reţeaua tuturor dispozitivelor din locuinţa dvs. care au conexiune la internet. S-ar putea să vă gândiţi automat la laptopul sau la televizorul inteligent, dar IoT include, de asemenea, lucruri precum console de jocuri, dispozitive de asistenţă la domiciliu, maşinile de spălat, camerele sau sistemele de alarmă a casei etc.

Deşi toate aceste dispozitive ne facilitează munca şi ne îmbunătăţesc calitatea vieţii, oricare din ele devine vulnerabil atacurilor cibernetice atât timp cât dispune de o conexiune la internet. Iată câteva sfaturi de asigurare a locuinţei dvs. în faţa eventualelor atacuri cibernetice:

1. Securizaţi toate dispozitivele

Asiguraţi-vă că toate dispozitivele au setată o parolă puternică şi activaţi opţiunea de **autentificare în doi paşi,** la dispozitivele care oferă această funcţionalitate.
(ex. parolă+TouchID, parola+SMS, FaceID+cod)

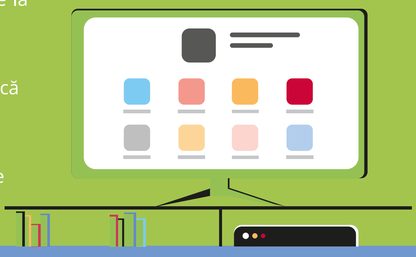
Schimbaţi **parola implicită de la router** precum şi denumirea lui. Este important să nu uitaţi că denumirile sau parola nu trebuie să includă nimic din informaţii despre casa sau familia dvs., de exemplu numele sau adresa dvs.

2. Verificaţi aplicaţiile

Descărcaţi aplicaţiile doar din **magazinele de aplicaţii oficiale** (Google Play, Apple App Store etc.). Accesând link-uri de descărcare de pe pagini nesigure pot duce la infectarea cu viruşi informatici a dispozitivelor.

Verificaţi la instalare ce **permisiuni** oferiţi aplicaţiilor, evitaţi activarea geolocaţiei, camerei, microfonului, dacă funcţiile de bază ale aplicaţiei nu ar avea nevoie nemijlocită de ele.

Revizuiţi periodic aplicaţiile şi ştergeţi-le pe cele care nu vă mai sunt necesare.

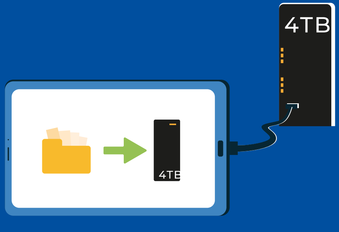


3. Revizuiţi setările de confidenţialitate pe conturile dvs. de pe reţelele de socializare

Accesaţi periodic rubrica setărilor de confidenţialitate şi **alegeţi setările** care le consideraţi cele mai potrivite.

Analizaţi bine ce **informaţii includeţi** în profilul dvs., platformele pot cere uneori şi informaţii personale sau confidenţiale, pe care nu în mod obligator ar trebui să le oferim.

4. Setaţi actualizările şi copiile de rezervă să se execute automat



IDispozitivele cu sisteme de operare sau aplicaţii învechite sunt mult mai vulnerabile la atac, de aceea având **ultimelea actualizări** sunt vitale pentru securitate. Setaţi actualizările să se execute automat atunci când sunt lansate de producător pentru a nu fi nevoia de a le descărca şi instala manual.

Asiguraţi-vă că aveţi **copii** a datelor importante pentru dvs. şi că sunt păstrate undeva offline sau in cloud. (ex. lista de contacte, poze, video).

5. Ţine-ţi informaţiile de muncă pe dispozitive separate, după posibilitate

Ideal ar fi să ţineţi informaţiile de muncă şi cele din viaţa privată pe **dispozitive separate**. Prin acestă cale veţi minimiza pierderile în cazul în care dispozitivul a fost compromis.

Dacă utilizaţi un singur dispozitiv, utilizaţi **profiluri de utilizator separate .**

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN CYBER SECURITY MONTH

#CyberSecMonth #ThinkB4UClick

I.P „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică“

Sfaturi de securizare a conturilor personale

La fel ca menţinerea uşilor încuiate pentru a ne proteja casele de spărgători, păstrarea sigură a conturilor noastre online este vitală pentru a ne proteja de infractorii cibernetici - iar parolele sunt cheia. Iată câteva sfaturi pentru a vă ajuta să vă păstraţi conturile personale în siguranţă în mediul online.

1. Setaţi parole puternice

Cu cât parola este mai complexă, cu atât mai sigură.

Creaţi parole de minim **10 caractere** care să includă combinaţii de cifre, litere majuscule şi minuscule şi simboluri speciale, dacă permite sistemul.

O cale uşoară de a stabili parole complexe este **passphrase** - o propoziţie ca de exemplu vers din cîntec sau proverb, unde folositi de exemplu doar prima/ultima litera doar vocalele/consoanele etc.

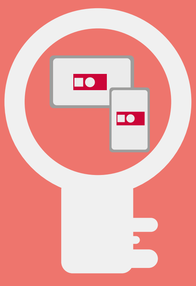
De asemenea, folosiţi parole **diferite** pentru toate conturile online.

2. Utilizaţi manageri de parole

Managerii de parole sunt aplicaţii care păstrează în siguranţă parolele pentru diverse conturi pe care le deţineţi.

Majoritatea acestor aplicaţii sunt **gratuite** şi uşor de folosit. Ele vă vor ajuta să creaţi parole puternice şi să le ţineţi în siguranţă.

Dacă nu doriţi utilizarea de aplicaţii speciale, notaţi-vă toate parolele într-un caiet şi păstraţi-l într-un loc fizic **sigur** departe de calculator.



3. Utilizaţi autentificări multi-factoriale (MFA)

Autentificările multi-factoriale (2FA) oferă un nivel suplimentar de **securitate** pentru protecţia conturilor dvs.

Este o metodă de autentificare electronică în care trebuie să prezentaţi două sau mai multe dovezi (factori) pentru a vă **confirma identitatea** şi a vă accesa contul, de exemplu **o parolă şi un cod unic** care este trimis pe telefonul dvs. mobil. Contul nu poate fi accesat fără a introduce acest cod.

4. Faceţi toate cele de mai sus!

Pentru o securitate suplimentară, utilizaţi un manager de parole care vă va crea parole puternice şi vă va permite autentificarea cu mai mulţi factori atunci când este disponibilă **pentru cea mai bună şansă** de a vă păstra conturile în siguranţă.

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN CYBER SECURITY MONTH

#CyberSecMonth #ThinkB4UClick

I.P „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică”