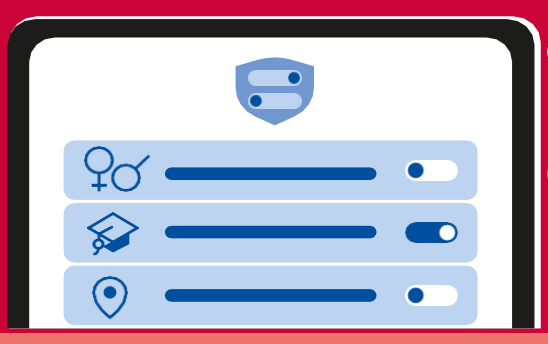
# Recomandări pentru a fi în siguranță online!

Internetul este un mediu important de comunicare și de contact cu lumea din jur: știri, cumpărături on-line, învățământ la distanță, mesagerie, etc. Dar, alegeți să fiți în siguranță on-line și țineți cont de recomandări pentru a vă proteja.



## Fiți conștienți de informațiile pecare le partajați

Atunci când creați un profil pentru un cont, oferiți doar informații pe care le acceptați să fie văzute public și sunteți sigur că nu vă vor afecta.

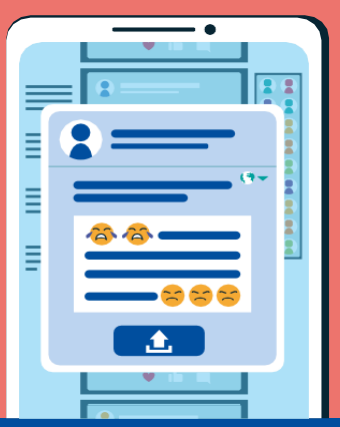
Utilizați setările de confidențialitate, securitate și dezactivați toate funcțiile de care nu aveți nevoie.

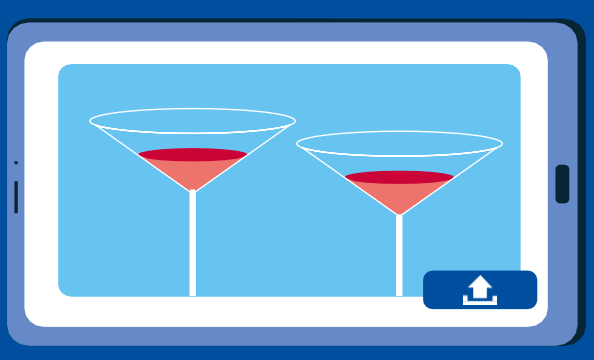
Dacă nu sunteți sigur, reconsiderați crearea profilului cu compania sau pe platforma respectivă.

## Chibzuiți înainte de a posta

Ceea ce postați online rămâne acolo pentru totdeauna. Chiar dacă ulterior, veți şterge informația, cineva va reuși să o salveze sau să o redirecționeze.

E bine să meditați/chibzuiți înainte de a distribui public un video, o fotografie sau a posta un comentariu.





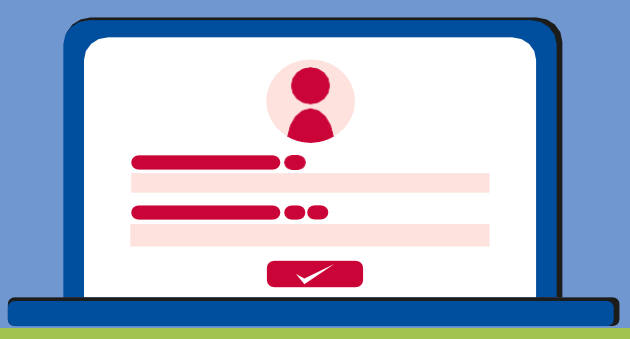
## Analizați din timp consecințele

Când intenționați să postați o fotografie, v-aţi gândit dacă toată lumea din fotografie este de acord? Sau dacă e bine să oferiți informații, despre locație?

O fotografie din vacanță poate fi un indiciu pentru infractori!

## Jocuri on-line

Dacă intenționați să participați la un joc online, folosiți un Nickname sau pseudonim și NU oferiți date personale.



## Asigurați-vă că știți cu cine comunicați

Rețineți că, și escrocii utilizează rețelele sociale, site- urile web și expediază mesaje utilizatorilor pentru a le fura datele personale, banii, etc.. Nu oferiți informații personale sau detalii despre conturile bancare, cu excepția cazului în care puteți verifica prin alt mijloc de comunicare cui i le distribuiţi.

## Urmăriți noutățile despre securitatea cibernetică

Urmăriți știrile sau solicitați familiei/prietenilor să vă anunțe despre escrocheriile care sunt în circulație, de ex. escrocheriile de phishing, software-ul rău intenționat, site-urile web falsevă pot ajuta să rămâneţi în siguranță online.

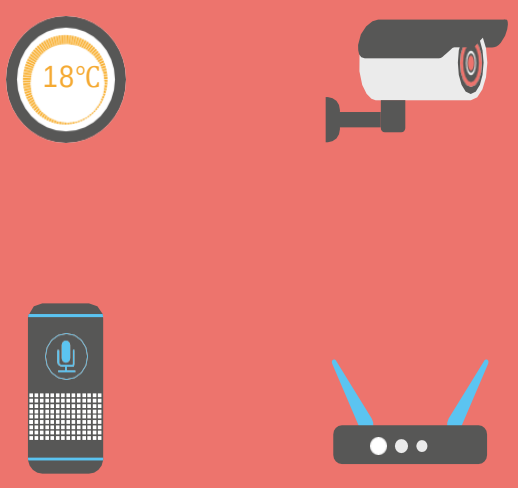
enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN CYBER SECURITY MONTH

I.P „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică”

# Recomandări pentru a fi în siguranță online!

Internetul obiectelor (IoT) este rețeaua tuturor dispozitivelor din locuința dvs., ce sunt conectate la internet: laptop, televizor, console de jocuri, dispozitive de asistență pentru domiciliu, mașini de spălat, camerele sau sistemele de alarmă a casei etc.. Toate aceste dispozitive ne îmbunătățesc calitatea vieții, dar oricare din acestea este vulnerabil atacurilor cibernetice. Țineți cont de recomandări pentru a vă proteja locuința împotriva eventualelor atacuri cibernetice:




## Securizați toate dispozitivele

Setați parole puternice și unice pentru fiecare dispozitiv şi activați opțiunea de autentificare în doi paşi, pentru dispozitivele ce oferă această funcție (ex. parolă+TouchID, parola+SMS, FaceID+cod).

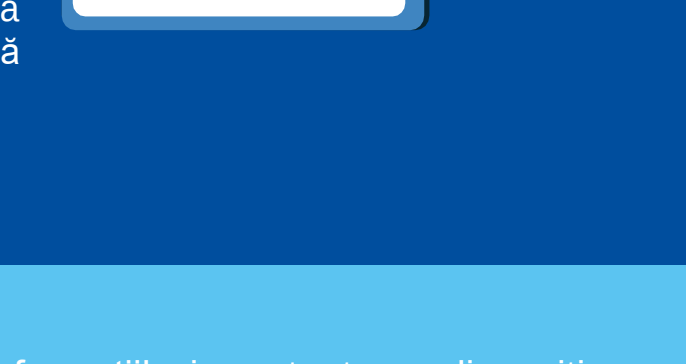
Schimbați parola implicită de la router precum și denumirea lui. Este important să nu uitaţi că denumirile sau parola nu trebuie să includă nimic din informaţii despre casa sau familia dvs.,de exemplu numele sau adresa dvs.

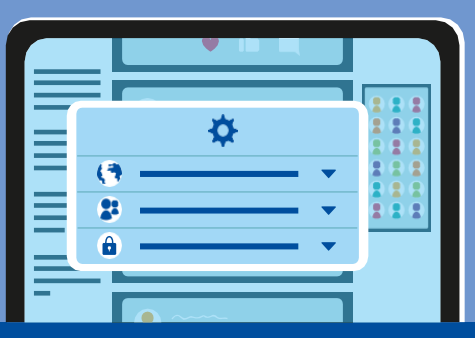
## Verificați aplicațiile

Descărcați aplicațiile doar din magazinele de aplicații oficiale (Google Play, Apple App Store etc.). Accesarea link-urilor de descărcare de pe pagini nesigure vă pot infecta dispozitivele cu viruși.

La instalare verificați ce permisiuni oferiți aplicațiilor, evitați activarea geolocaţiei, camerei, microfonului, dacă funcțiile de bază ale aplicației nu ar avea nevoie nemijlocită de ele.

Revizuiți periodic aplicațiile şi ștergeți-le pe cele carenu vă mai sunt necesare.





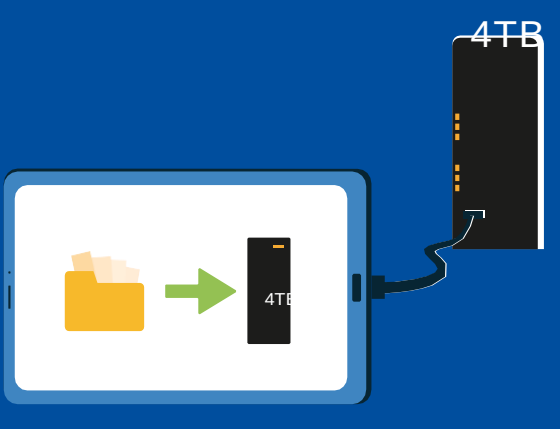
## Revizuiți setările de confidențialitate pe conturile dvs. de pe rețelele de socializare

Accesați periodic rubrica setărilor de confidențialitate și bifați setările cele mai potrivite.

Analizați ce informaţii includeți în profil, platformele pot cere uneori şi informaţii personale sau confidențiale, pe care nu în mod obligator ar trebui să le oferim.

## Alegeți setarea automată a actualizărilor și a copiilor de rezervă

IDispozitivele cu sisteme de operare sau aplicații învechite sunt mult mai vulnerabile la atac, din aceste considerente, actualizările la zi sunt vitale pentru securitate. Setarea automată a actualizărilor și păstrarea în cloud sau pe un alt dispozitiv a informațiilor (ex. lista de contacte, poze, video), vă va spori siguranța.




## Păstrați informațiile importante pe dispozitive separate

Ideal ar fi să păstrați informațiile importante pe dispozitive separate. Astfel, veți minimiza pierderile în cazul în care dispozitivul va fi compromis.

Dacă utilizați un singur dispozitiv, utilizați profiluri de utilizator separate .

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN CYBER SECURITY MONTH

#CyberSecMonth
#ThinkB4UClick

I.P „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică”

# Securizați-vă conturilor personale!

Păstrarea sigură a conturilor online este vitală pentru a ne proteja de infractorii cibernetici, iar parolele sunt cheia. Subliniem câteva recomandări, pentru a vă ajuta să aveți conturile personale on-line în siguranță.

## Setați parole puternice

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

Creați parole de minim 10 caractere care să includă combinații de cifre, litere majuscule și minuscule, simboluri speciale.

O metodă de a stabili parole complexe este passphrase/frază parolă (ex: un vers întreg, un proverb, o propoziție dintr-un text sau folosiți spre exemplu doar prima/ultima literă, doar vocale/consoane etc.

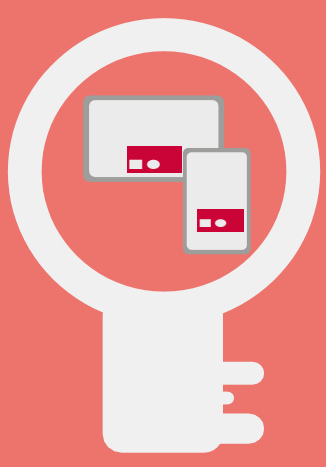
De asemenea, folosiți parole diferite pentru toate conturile online.

## Utilizați manageri de parole

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

Majoritatea acestor aplicaţii sunt gratuite şi uşor de folosit.

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

## Utilizați autentificări multi-factoriale (MFA)

Autentificările multi-factoriale (2FA) oferă un nivel suplimentar de securitate pentru protecția conturilordvs.

Este o metodă de autentificare electronică în care trebuie să prezentați 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.

#CyberSecMonth
#ThinkB4UClick

I.P „Serviciul Tehnologia Informaţiei şi Securitate Cibernetică”