

Datele importante pe care le salvezi pe telefonul mobil sau pe tabletă pot fi accesate cu ușurință de persoane necunoscute fără prea mari cunoștințe de informatică.

Încearcă să urmărești recomandările de mai jos astfel încât să îți protejezi datele și intimitatea:

1. Parolează-ti telefonul

Aceasta este una dintre cele mai simple și banale recomandări, dar care este adesea omisă de către utilizatorii de dispozitive mobile. Utilizarea parolelor de tip pattern (trasarea unor linii pe ecran) oferă un bun nivel de siguranță, însă urmele pe care le lasă degetele pe ecran pot ajuta la aflarea parolei-pattern utilizate. O parola clasică, din cel puțin 4 cifre, este cea mai bună variantă.



2. Asigură-te că dispozitivul tău mobil se blochează automat

Dacă îți setezi o parolă la telefon, dar îl lași neblocat pentru 15 minute pe birou, e ca și cum i-ai invita pe ceilalți să-ți acceseze datele. Majoritatea telefoanelor inteligente/tabletelor îți permit să alegi un interval de timp după care dispozitivul să se blocheze automat. Folosește această opțiune pentru un interval care ți se pare convenabil, dar mai mic de 2 minute.



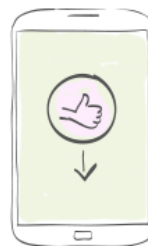
3. Instalează un software de securitate

Dispozitivul tău mobil este un echipament de calcul, un calculator și ar trebui să îl tratezi ca atare din punct de vedere al securității. Caută aplicații care te protejează în special față de amenințări de tip malware, remote data wipe, etc.



4. Descarcă aplicații doar din surse verificate

Google Play și App Store iau securitatea foarte în serios. Citește întotdeauna review-urile utilizatorilor și permisiunile aplicațiilor.



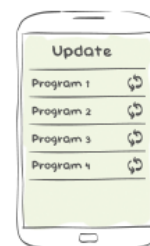
5. Întotdeauna verifică permisiunile aplicațiilor pe care le descarci

Multe aplicații solicită mai mult decât permisiunile de bază. De exemplu, poți să fii sigur că o aplicație de SMS va trimite și recepționa SMS-uri la fel cum o aplicație care te ajută să găsești cel mai bun traseu pe sosea îți va solicita poziția prin GPS. Totuși, aplicațiile care îți solicită, de exemplu, acces la lista ta de contacte sau îți solicită parola de email ar trebui tratate cu mai multă grijă.



6. Instalează update-uri

Update-urile pentru sistemele de operare deseori includ patch-uri ce repară vulnerabilități de securitate.



7. Fii atent întotdeauna la link-urile primite prin e-mail sau SMS

Ne-am obișnuit din utilizarea normală a calculatorului să tratăm cu grijă link-urile suspecte. Aceeași atenție trebuie acordată și link-urilor primite pe tablete sau pe telefoane inteligente, indiferent dacă utilizează Android sau IOS.



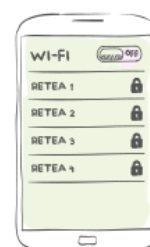
8. Criptează-ți telefonul

Chiar dacă ți-ai securizat dispozitivul mobil cu o parolă, cineva tot poate să acceseze datele de pe telefonul tău. Utilizarea criptării pentru datele de pe telefonul tău previne un astfel de furt de informații.



9. Blochează conectarea automată la wi-fi

Conectarea automată la puncte de acces Internet necriptate nu îți consumă doar bateria, ci înseamnă practic acordarea accesului oricui pe dispozitivul tău mobil.



10. Blochează conectarea automată la Bluetooth

Conectarea automată la Bluetooth lasă o ușă deschisă pentru orice persoană interesată să acceseze informații private, liste de contacte, parole stocate etc. de pe smartphone-ul tău. Pentru a evita furtul de informații, utilizează doar conexiuni Bluetooth despre care știi sigur că sunt securizate.

