Igiena digitală - modalități de prevenire a atacurilor cibernetice

Good Digital Hygiene for Startups

https://good-start.eu/

Ce este igiena digitală?

Igiena digitală cuprinde setul de practici și protocoale care vizează menținerea securității, eficienței și integrității resurselor și operațiunilor digitale.

Practici de igienă digitală

1. **Utilizarea unor parole puternice și unice pentru fiecare cont:** Folosește parole puternice, evită reutilizarea lor și folosește un manager de parole pentru a gestiona mai ușor parolele complexe.
2. **Autentificarea multi-factor (MFA):** Activează MFA oriunde este posibil pentru a adăuga un nivel suplimentar de securitate.
3. **Actualizarea software-ului în timp util:** Asigură-te că toate sistemele de operare, aplicațiile și firmware-ul sunt actualizate pentru a beneficia de cele mai recente corecții de securitate.
4. **Copii de rezervă a datelor:** Realizează backup-uri regulate ale datelor importante și verifică periodic posibilitatea de restaurare acestor backup-uri.
5. **Criptarea datelor:** Criptează datele atât în tranzit, cât și în repaus pentru a proteja informațiile sensibile.
6. **Atenție la încercările de phishing și alte atacuri:** Fii vigilent la emailurile și mesajele suspecte și educă-te continuu asupra tacticilor noi folosite de atacatori.
7. **Utilizarea de programe antivirus și anti-malware:** Instalează și menține actualizat un software antivirus (cu funcția de scanare live activată) și anti-malware pentru a detecta și preveni amenințările.
8. **Email și dispozitive sigure:** la măsuri suplimentare pentru a-ți păstra email-ul ordonat și sigur. Un email compromis poate autoriza accesul la conturile de pe alte site-uri web, social media etc.
9. **Descărcarea soft-urillor doar din surse sigure:** NU descărca și nu instala jocuri sau software din surse suspecte, inclusiv descărcări torrent.
10. **Limitarea amprentei digitale și sociale:** Limitează informațiile pe care le distribui online, pentru a nu deveni vulnerabil în fața infractorilor cibernetici.
11. **Instruirea angajaților privind practicile de igienă digitală:** Organizează sesiuni de training regulat pentru angajați privind securitatea cibernetică și cele mai recente amenințări.
12. **Crearea unor politici și proceduri interne de gestionare a amenințărilor cibernetice:** Elaborează și menține o documentație privind politicile de securitate cibernetică și asigură-te că toți angajații le cunosc și le respectă.
13. **Crearea unui plan de răspuns la incidente:** Dezvoltă și testează un plan detaliat de răspuns la incidente pentru a gestiona eficient eventualele atacuri cibernetice.
14. **Respectarea cerințelor de reglementare și a standardelor din industrie:** Fii la curent și conform cu reglementările legale și standardele din industrie relevante pentru securitatea cibernetică.
15. **Segmentarea rețelei:** Împarte rețeaua în segmente distincte pentru a limita răspândirea eventualelor atacuri și pentru a proteja resursele critice.
16. **Monitorizarea și auditarea activităților de rețea:** Utilizează instrumente de monitorizare și audit pentru a detecta activitățile neobișnuite și pentru a răspunde prompt la posibilele incidente.
17. **Utilizarea conexiunilor sigure:** Asigură-te că toate conexiunile la rețea sunt securizate, folosind VPN-uri și protocoale de securitate, în special pentru lucrul la distanță.
18. **Controlul accesului la date și resurse:** Implementarea unui sistem de control al accesului bazat pe roluri pentru a limita accesul la date și resurse doar persoanelor autorizate.
19. **Testarea periodică a securității:** Efectuează teste de penetrare și evaluări de vulnerabilitate periodic pentru a identifica și remedia punctele slabe ale sistemelor.

Implementarea acestor practici ajută la crearea unui mediu digital mai sigur atât pentru indivizi, cât și pentru companii.