Serviciul Tehnologia Informației și Securitate Cibernetică

PRACTICI EFICIENTE DE ASIGURARE A SECURITĂȚII PE REȚELELE SOCIALE

Ghid de bune practice

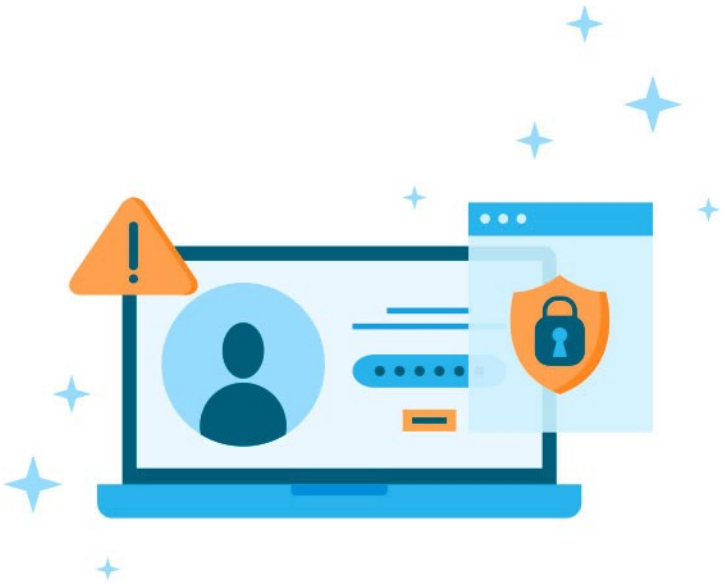
Introducere

Rețelele sociale oferă o gamă largă de oportunități pentru comunicarea cu miliarde de utilizatori din întreaga lume. Evoluția tehnologiilor și a rețelelor sociale a creat o nouă paradigmă de comunicare și interacțiune. Au devenit o parte a vieții sociale și au adus o schimbare revoluționară în modul în care folosim internetul (Facebook, Twitter și Whatsapp) în scopuri personale și profesionale.

Platformele de social media îi ajută pe utilizatori să păstreze legătura cu prietenii, să se conecteze cu clienții și să își promoveze afacerile, dar, concomitent sporesc și expunerea oamenilor și a companiilor la amenințările cibernetice.

Amenințările cibernetice pe rețelele sociale

Este important să conștientizăm că, există un set de provocări/amenințări cibernetice legate de rețelele sociale de care trebuie să ne protejăm. Fiind prezenți pe rețelele sociale devenim o potențială victimă a hackerilor/escrocilor, dar cu ușurință putem și pune în pericol alți utilizatori.

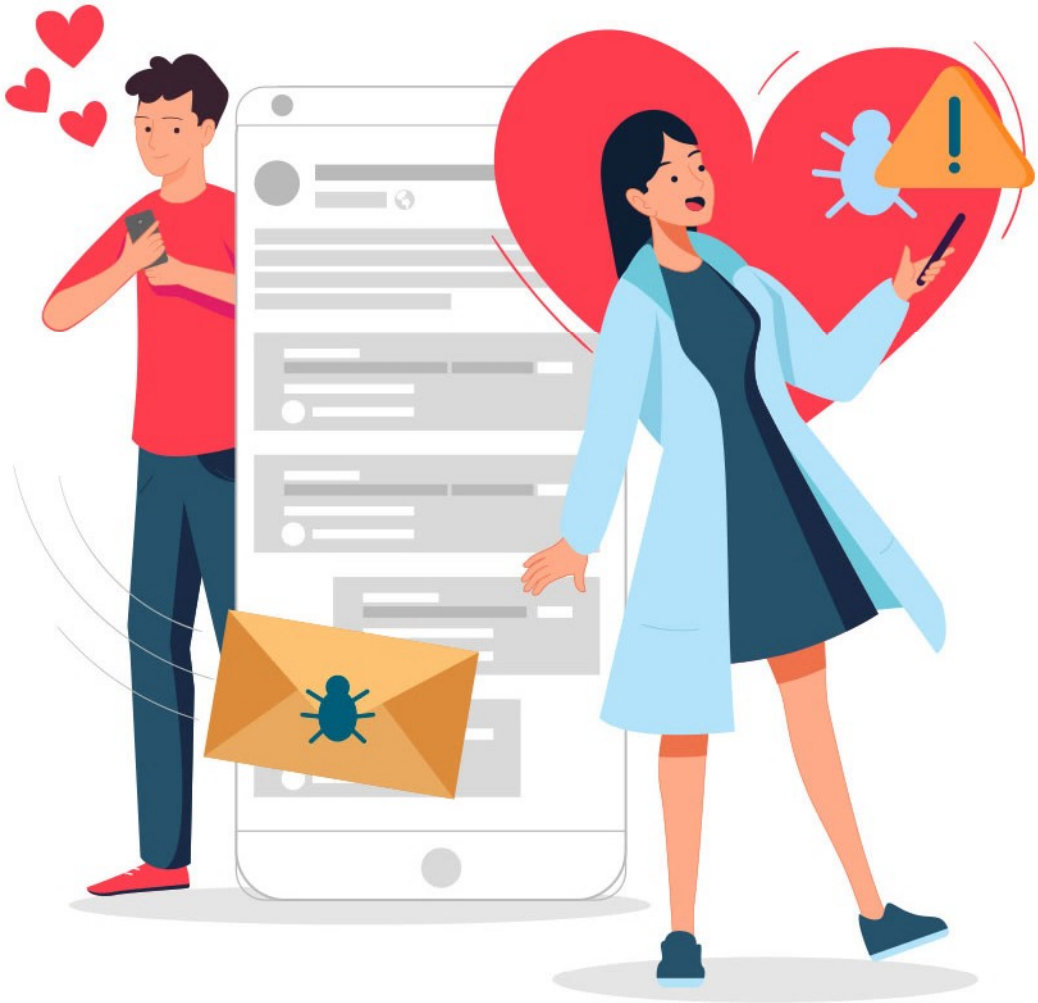


Furtul de identitate:

Utilizatorii se înregistrează pe platformele de socializare în baza informațiilor personale, ceea ce poate cauza încălcări ale confidențialității. Datele personale devin vulnerabile, deoarece hackerii și hoții de identitate le folosesc pentru a reseta parolele, a sparge conturi și a solicita bani sau pentru alte escrocherii.

Confidențialitatea datelor:

De asemenea, uneori poate provoca pierderea datelor personale sau poate instiga hackerii să folosească același lucru din motive rău intenționate. De exemplu, informațiile unui utilizator pot fi vizualizate de toată lumea dacă setarea implicită a utilizatorului este publică.



Escrocherii romantice (Romance scammers):

Escrocheriile romantice apar atunci când un infractor adoptă o identitate online falsă pentru a câștiga afecțiunea și încrederea victimei, apoi folosește iluzia unei relații romantice pentru a manipula și/sau a fura de la victimă sub diferite pretexte.

Ingineria socială se referă la tehnicile utilizate pentru a convinge o potențială victimă să divulge informații specifice sau să efectueze o anumită acțiune din motive ilegale.

Atacatorul/hackerii cercetează, colectează date despre victimă: data nașterii, familie, activitate, prieteni, locațiile vizitate, etc., ulterior, prin manipulare psihologică și abuzând de încredere obține, de la victimă, informații sensibile sau chiar încalcă politicile de securitate.

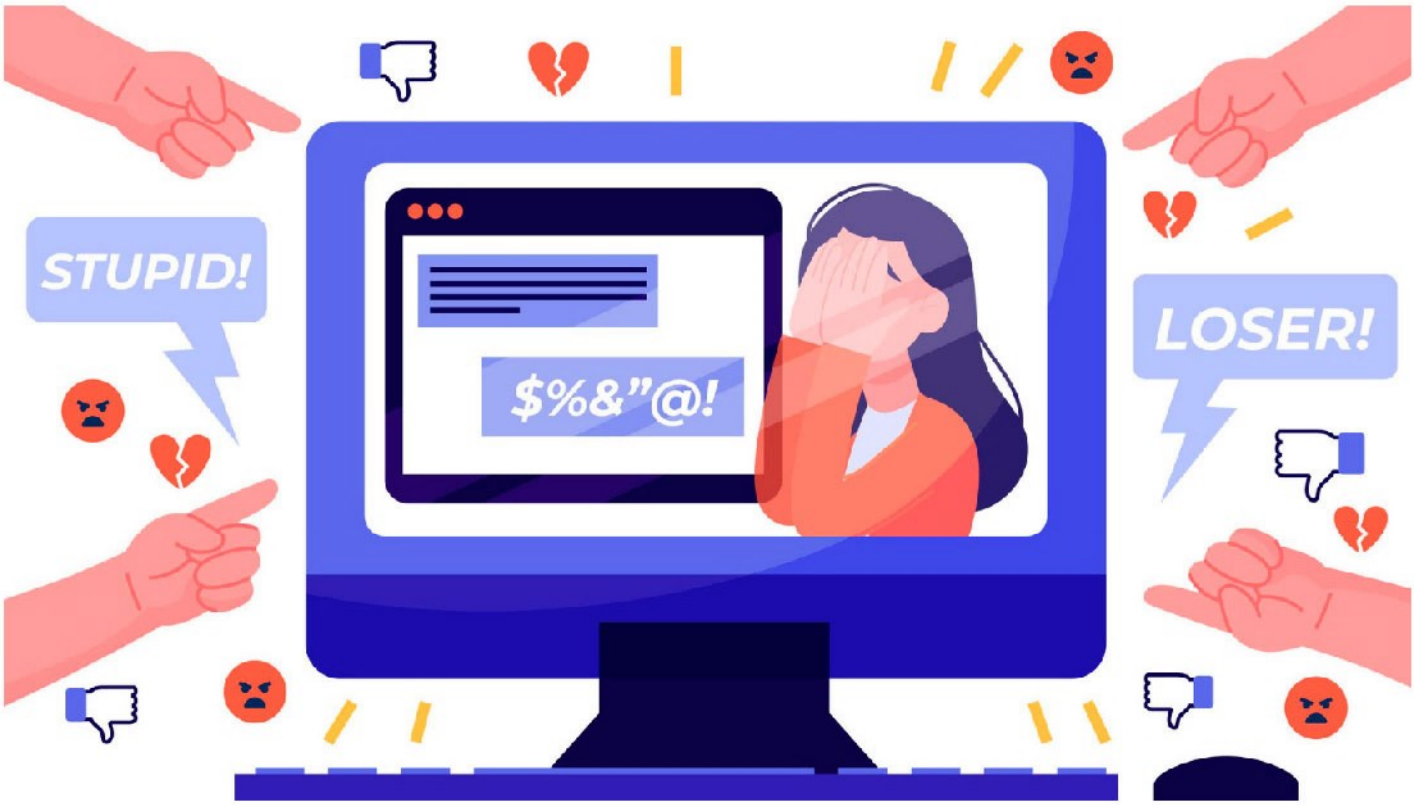
Atacurile de tip phishing sunt declanșate printr-un e-mail sau un mesaj online, în care infractorul cibernetic momește potențialele victime, încercând să le convingă să facă clic pe un link sau să deschidă un atașament, care de fapt sunt false/rău intenționate.

Dacă atacatorul folosește rețelele sociale pentru a stabili o relație cu ținta sa, va fi mult mai ușor să obțină încrederea necesară pentru a-l determina să facă clic pe linkuri rău intenționate sau să introducă informații private sensibile într-un formular online. De asemenea, infractorii cibernetici exercită presiune asupra potențialelor lor victime, creând un fals sentiment de urgență: „Acționează acum înainte de a fi prea târziu...".

Programele malware sunt viruși, troieni, spyware și ransomware, software rău intenționate promovate cu ușurință pe rețelele sociale prin intermediul reclamelor. Infractorii cibernetici le distribuie pentru a accesa dispozitivele și rețele pentru a fura date confidențiale și a prelua controlul asupra sistemelor sau provoacă o întrerupere completă a sistemului informatic, precum și pentru a crea rețele bot, criptojack. Programele malware cauzează pierderea tuturor datelor (personale, profesionale, financiare etc.).

Uzurparea identității mărcii este când un individ sau un grup încearcă să fure identitatea unei companii sau a unei mărci renumite pentru a minți victimele/angajații să furnizeze informații confidențiale și valoroase, ce pot fi folosite pentru a pirata sisteme și rețele. Uzurparea identității mărcii dăunează victimelor care cad în astfel de tactici, dar au un impact major negativ asupra reputației/numelui companiei.

Catfishing este atunci când o persoană preia informații și imagini de la un utilizator pentru a crea o identitate falsă, un cont false în Facebook, Instagram sau rețele sociale de dating, pentru a crea relații online deceptive. Din lipsă de vigilență colegii sau șefii lor acceptă prietenia unor conturi false, fără să verifice și pot dezvălui în mod deliberat date sensibile în postările lor, ceea ce poate cauza prejudicii semnificative reputației organizației.



Cyber Bullying:

Se referă la hărțuirea prin mediul digital. Poate avea loc pe rețelele de socializare, jocuri și platforme de mesagerie și are scopul de a speria, discrimina, umili, rușina, enerva, șantaja victima. Hackerii hărțuiesc victimele pe rețelele de socializare, trimițând mesaje neplăcute și lascive. Ei transformă fotografiile victimelor și le distribuie pe rețelele de socializare, pretinzând că zvonurile fac viața victimei insuportabilă.

Sextortion:

se referă la materiale foto sau video cu caracter sexual pe care utilizatorii de internet le încarcă sau le trimit unei persoane în care au încredere, dar, sunt după aceea constrânși să achite sume mari de bani pentru ca aceste materiale să nu ajungă la apropiați sau în rețea.

Terorismul cibernetic - în prezent, rețelele sociale sunt folosite și pentru a facilita promovarea, propaganda teroristă, cum ar fi: incitarea la terorism, recrutare, formarea de radicalizare și planificarea atacurilor teroriste.

Practici eficiente pentru sporirea securității cibernetice pe rețelele de socializare

Activați 2FA - Autentificarea cu doi factori este o funcție suplimentară de securitate ce, în plus față de parolă, contribuie la protejarea contului tău de Facebook. În cazul în care configurezi 2FA ți se va cere să introduci un cod de conectare pentru confirmarea tentativei de conectare ori de câte ori cineva încearcă să acceseze contul tău de Facebook de pe un browser sau dispozitiv mobil pe care nu-l recunoști. De asemenea, primești notificări ori de câte ori cineva încearcă să se conecteze la conturile tale.

Utilizează parole unice, diferite pentru fiecare cont. În cazul în care un cont ți-a fost piratat vei împiedica accesul către celelalte, iar pentru a ține evidența diferitelor parole utilizați un instrument de gestionare a acestora.

Practici eficiente pentru sporirea securității cibernetice pe rețelele de socializare

Actualizați setările de securitate pe platforme, cu regularitate. Rămâneți la curent cu opțiunile de securitate ale platformei de social media pentru a vă asigura că acestea sunt întotdeauna actuale și setate la cel mai strict nivel.

Fii atent la ce postezi dar și la ce postează alții despre tine. Nu distribui informații ce ar putea să te pună într-o situație jenantă pe tine sau pe altcineva.

Monitorizează rețelele sociale pentru a observa riscurile de securitate. Informează-te și conștientizează amenințările pe platformele de social media.

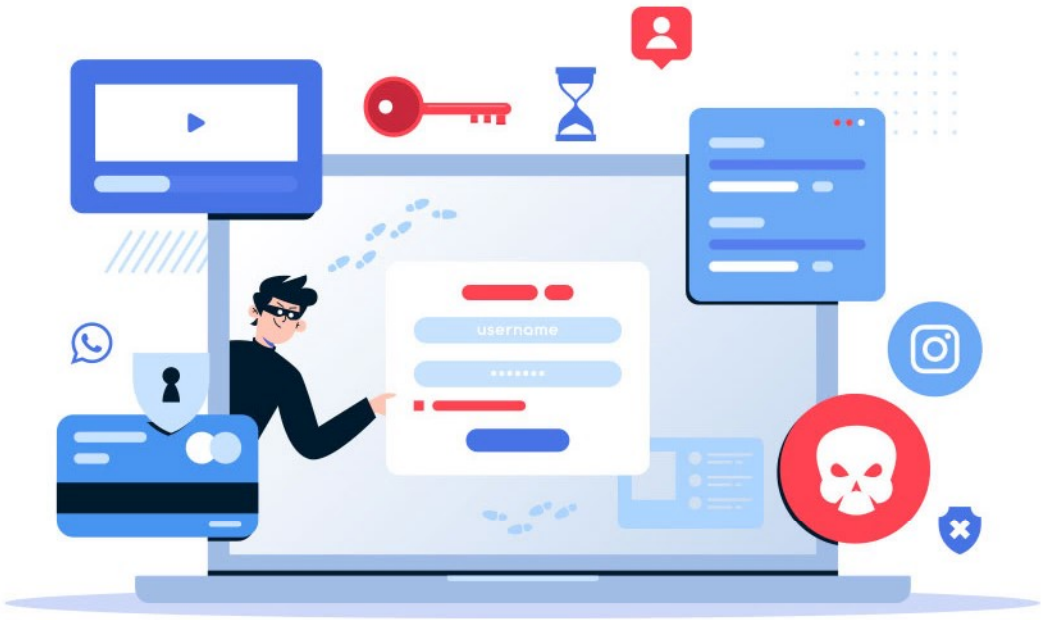
Practici eficiente pentru sporirea securității cibernetice pe rețelele de socializare

Fii atent la tentativele de falsificare ale contului tău sau tentativele de uzurpare a identității mărcii. Raportează încălcările administratorilor platformei de rețele sociale și informează-ți

Fii precaut la cererile de prietenie și mesajele venite de la persoane necunoscute sau suspecte. Uneori, acestea pot fi atacuri de tip phishing, tentative de a obține informații personale sau de a infecta dispozitivul cu malware.

Practici eficiente pentru sporirea securității cibernetice pe rețelele de socializare

Închide conturile vechi, riști ca informațiile personale distribuite pe social media să fie utilizate de altcineva în scopuri rău intenționate, fără știrea și acceptul tău.



Fii precaut la persoanele și entitățile cu care vă conectați pe platformele de socializare. Examinează cu atenție fiecare conexiune și nu te afilia cu cele suspecte.

Practici eficiente pentru sporirea securității cibernetice pe rețelele de socializare

Limitează informațiile personale distribuite pe rețele sociale (numărul de identificare personală, adresa de domiciliu, instituția bancară la care vă deserviți sau informațiile de cont bancar, etc). Rubrica „Despre mine” este opțională.

Verifică setările și actualizează aplicațiile.

Serviciul Tehnologia Informației și Securitate Cibernetică

#citește #conștientizează și fii în #SigurantaOnline

www.stisc.gov.md

Chișinău 2023