DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

INFORMEAZĂ-TE
PROTEJEAZĂ-TE
ACȚIONEAZĂ ÎN SIGURANȚĂ

IULIE 2026

TLP:CLEAR

Sumar executiv

Internetul reprezintă o componentă importantă a vieții academice și personale a studenților, fiind utilizat zilnic pentru activități educaționale, comunicare, tranzacții financiare și acces la informații. În același timp, utilizarea tot mai extinsă a tehnologiilor digitale este însoțită de amenințări cibernetice variate, care pot afecta securitatea conturilor, a datelor cu caracter personal și a dispozitivelor utilizatorilor.

Prezentul ghid oferă recomandări practice pentru recunoașterea, prevenirea și gestionarea principalelor riscuri întâlnite în mediul online. Sunt abordate atacurile de tip phishing, smishing și vishing, riscurile asociate rețelelor Wi-Fi publice, codurile QR utilizate în scopuri frauduloase, dezinformarea, conținutul de tip deepfake și compromiterea conturilor digitale. Documentul prezintă, de asemenea, măsuri concrete de protecție, precum utilizarea autentificării multifactor, gestionarea sigură a parolelor și aplicarea unor practici adecvate de securitate cibernetică.

Scopul materialului este de a contribui la dezvoltarea unei culturi de securitate cibernetică în cadrul comunității universitare și de a le oferi studenților informațiile necesare pentru utilizarea în siguranță a serviciilor și tehnologiilor digitale.

Ghidul a fost elaborat de studenți ai Universității Babeș-Bolyai din Cluj-Napoca, în cadrul stagiului de practică desfășurat la Directoratul Național de Securitate Cibernetică (DNSC), sub coordonarea și îndrumarea specialiștilor DNSC. Materialul reflectă colaborarea dintre mediul academic și DNSC pentru promovarea educației în domeniul securității cibernetice, creșterea nivelului de conștientizare și încurajarea unor comportamente responsabile în mediul digital.

Cuprins

1. Cum te manipulează atacatorii (ingineria socială)

Când primești un mesaj care pare trimis de o persoană cunoscută, de bancă sau de o instituție în care ai încredere, este firesc să fii mai puțin suspicios. Atacatorii profită tocmai de această încredere și încearcă să te determine să acționezi fără să verifici mai întâi solicitarea primită.

Această metodă de manipulare se numește inginerie socială. În loc să atace direct un sistem informatic, atacatorul încearcă să te convingă să îi oferi informații sensibile, să accesezi un link, să deschizi un fișier sau să efectuezi o anumită acțiune. Pentru a părea credibil, acesta poate pretinde că este un coleg, un reprezentant al băncii sau al unei instituții cunoscute.

1.1. Mecanismele psihologice: frica, urgența, curiozitatea

Atacatorii încearcă să te facă să reacționezi rapid, înainte să ai timp să verifici dacă mesajul este real. Pot folosi frica, curiozitatea, graba sau promisiunea unui câștig pentru a-ți influența decizia.

De exemplu, un mesaj care te avertizează că îți va fi suspendat contul creează un fals sentiment de urgență și te poate determina să accesezi imediat un link. Alte mesaje promit premii, reduceri sau informații „exclusive”, tocmai pentru a-ți stârni curiozitatea.

Atacatorii pot invoca și autoritatea, pretinzând că reprezintă banca, poliția, universitatea sau o altă instituție cunoscută. Scopul este să te intimideze sau să îți câștige încrederea, astfel încât să le oferi date personale, parole, coduri de autentificare ori informații bancare.

1.2. Cele mai comune capcane: phishing, smishing și vishing

Atacurile de tip phishing, smishing și vishing folosesc canale diferite de comunicare — e-mailul, mesajele SMS și apelurile telefonice —, dar urmăresc același scop: să te convingă să divulgi informații sensibile, să accesezi un link, să deschizi un fișier sau să efectuezi o plată.

În cazul unui atac de tip phishing, primești un e-mail care pare să fi fost trimis de o bancă, de o instituție publică, de universitatea ta sau de o companie cunoscută. Pentru a părea autentic, mesajul poate imita sigla, culorile și stilul comunicărilor oficiale. De obicei, conține un link sau un atașament și te îndeamnă să acționezi rapid: să îți confirmi identitatea, să îți actualizezi datele sau să previi blocarea contului.

Nu accesa linkurile din mesajele suspecte și nu deschide atașamente pe care nu le aștepți. Intră în cont folosind aplicația oficială sau scrie manual adresa site-ului în browser. Verifică adresa completă a expeditorului, nu doar numele afișat.

Smishingul este o formă de phishing transmisă prin SMS. Un exemplu frecvent este mesajul care te anunță că un colet nu poate fi livrat și îți cere să accesezi un link pentru a plăti o taxă mică. Pagina deschisă poate imita site-ul unei firme de curierat, dar scopul este obținerea datelor cardului sau a altor informații personale. Prin astfel de mesaje ți se poate cere să îți „verifici”, „actualizezi” sau „reactivezi” contul, să apelezi un număr de telefon ori să comunici un cod primit prin SMS.

Nu transmite codul PIN, parolele, datele cardului sau codurile de autentificare. Dacă mesajul pare să provină de la o firmă de curierat, de la o bancă ori de la o altă organizație, verifică solicitarea folosind datele de contact publicate pe site-ul oficial.

În cazul unui atac de tip vishing, atacatorii te contactează telefonic și pretind că reprezintă o bancă, o instituție publică sau o companie cunoscută. Pot invoca o tranzacție suspectă, o problemă tehnică ori o situație urgentă pentru a te convinge să le oferi informații confidențiale, să aprobi o autentificare sau să transferi bani. Numărul afișat pe ecran poate fi falsificat, așa că nu considera apelul legitim doar pentru că pare să provină de la o instituție cunoscută.

Nu divulga parola, codul PIN sau codurile de autentificare și nu aproba notificări de conectare pe care nu le-ai inițiat. Dacă ai suspiciuni, încheie apelul și contactează instituția folosind numărul publicat pe site-ul oficial sau, în cazul băncii, numărul înscris pe spatele cardului.

2. Riscurile din viața de zi cu zi (campus, cafenele și cumpărături)

Telefonul, laptopul și conexiunea la internet fac parte din rutina ta zilnică. Le folosești la facultate, în cafenele, pentru plăți, cumpărături sau accesarea diferitelor servicii online. Tocmai pentru că aceste activități par obișnuite, este ușor să treci cu vederea unele riscuri.

O rețea Wi-Fi publică, un cod QR lipit peste cel original sau o ofertă prea bună pot fi folosite pentru a-ți fura datele personale ori banii. În acest capitol vei afla la ce să fii atent și ce poți face pentru a evita cele mai frecvente capcane.

2.1. Conectarea la rețele Wi-Fi publice

Rețelele Wi-Fi gratuite din campusuri, cafenele, aeroporturi sau centre comerciale sunt utile atunci când nu vrei să consumi traficul de date mobile. Totuși, înainte să te conectezi, verifică denumirea exactă a rețelei. Un atacator poate crea un punct de acces cu un nume asemănător celui legitim, cum ar fi „Cafenea_X_WiFi”, pentru a te convinge să îl folosești.

O rețea falsă poate fi folosită pentru a te redirecționa către pagini frauduloase, pentru a colecta informațiile pe care le transmiți prin conexiuni neprotejate sau pentru a te convinge să instalezi o aplicație ori un certificat. Fii atent și la paginile de conectare care îți cer date personale, datele cardului sau parola unui cont pentru a-ți oferi acces la internet.

Când ai posibilitatea, folosește datele mobile sau un hotspot personal pentru activități sensibile, cum ar fi accesarea contului bancar sau efectuarea unei plăți. Dacă trebuie să folosești o rețea Wi-Fi publică, verifică adresa site-ului înainte să introduci date, dezactivează conectarea automată la rețele și nu permite partajarea fișierelor cu alte dispozitive. Prezența simbolului lacăt și a conexiunii HTTPS arată că legătura cu site-ul este criptată, dar nu garantează că site-ul este legitim.

Poți utiliza și un serviciu VPN de încredere. VPN-ul creează un tunel criptat între dispozitivul tău și serverul furnizorului VPN, reducând riscul ca traficul să fie interceptat în rețeaua locală. Totuși, nu te protejează împotriva site-urilor de phishing, a fișierelor malițioase sau a aplicațiilor compromise.

Înainte să alegi un serviciu VPN, verifică reputația furnizorului, politica de confidențialitate, actualizările oferite și modul în care sunt gestionate datele utilizatorilor. Descarcă aplicația numai din magazinul oficial al dispozitivului sau de pe site-ul furnizorului și evită aplicațiile care solicită permisiuni fără legătură cu funcționarea lor. Indiferent dacă folosești sau nu un VPN, menține sistemul de operare și aplicațiile actualizate, evită linkurile suspecte și verifică site-ul înainte să introduci parole, date personale sau informații bancare.

2.2. Capcana codurilor QR

Codurile QR îți permit să deschizi rapid un meniu, un formular sau o pagină web, dar nu îți arată direct unde vei ajunge după scanare. Tocmai de aceea, pot fi folosite și pentru a ascunde linkuri periculoase.

Un atacator poate lipi un cod QR fals peste unul legitim sau îl poate distribui pe rețelele sociale, în mesaje ori în spații publice. După scanare, poți fi redirecționat către un site de phishing, către o pagină care îți solicită date bancare sau către un site care încearcă să te convingă să instalezi o aplicație.

Înainte să deschizi linkul, verifică unde este afișat codul și dacă provine dintr-o sursă de încredere. Uită-te dacă autocolantul pare lipit peste un alt cod sau dacă există urme de înlocuire. Dacă telefonul îți afișează adresa web înainte de deschidere, verifică domeniul și eventualele greșeli de scriere.

Oprește-te dacă pagina îți cere imediat parola, datele cardului, instalarea unei aplicații sau efectuarea unei plăți. Într-o astfel de situație, verifică solicitarea folosind site-ul oficial sau datele de contact ale organizației respective.

2.3. Cum recunoști magazinele online false și ofertele „prea bune”

Magazinele online false și reclamele înșelătoare de pe rețelele sociale încearcă să îți câștige încrederea prin reduceri mari, fotografii atractive și recenzii aparent autentice. Unele site-uri copiază siglele, descrierile și imaginile unor comercianți cunoscuți, iar conturile folosite pentru promovare pot părea legitime la prima vedere.

Dacă o ofertă pare prea bună ca să fie adevărată, verifică magazinul înainte să comanzi. Caută numele comerciantului împreună cu termeni precum „recenzii”, „păreri” sau „fraudă” și compară informațiile din

mai multe surse. Uită-te cu atenție la adresa site-ului, la datele de contact, la politica de retur și la informațiile despre firma care administrează magazinul.

Un site cu aspect profesionist nu este neapărat și unul sigur. Alege metode de plată care îți oferă posibilitatea de a contesta tranzacția în cazul unei fraude. Evită transferurile bancare directe către persoane necunoscute, plățile în criptomonede și magazinele care acceptă doar metode de plată fără protecție pentru cumpărător.

Nu te lăsa grăbit de mesaje precum „stoc limitat", „ultimul produs disponibil" sau „oferta expiră în câteva minute". Aceste formulări pot fi folosite pentru a te împiedica să verifici comerciantul și să compari oferta cu alte surse. Dacă identifici un magazin sau un cont suspect, nu continua plata și raportează-l platformei pe care l-ai găsit. În cazul în care ai introdus deja datele cardului sau ai efectuat o plată, contactează imediat banca.

3. Ce vezi nu este întotdeauna real: deepfake și dezinformare

Un videoclip, o fotografie sau o înregistrare audio pot părea autentice, chiar dacă au fost modificate sau generate cu ajutorul inteligenței artificiale. Astfel de materiale sunt folosite uneori pentru a răspândi informații false, pentru a promova fraude sau pentru a compromite imaginea unei persoane.

Conținutul care provoacă teamă, furie sau surprindere este distribuit adesea înainte să fie verificat. Același lucru se întâmplă și atunci când informația confirmă ceea ce crezi deja. În acest capitol vei afla cum sunt create materialele de tip deepfake, cum poți recunoaște unele conturi false și ce verificări să faci înainte să distribui un conținut.

3.1. Cum sunt create și cum verifici materialele de tip deepfake

Materialele de tip deepfake sunt înregistrări audio, imagini sau videoclipuri generate ori modificate cu ajutorul inteligenței artificiale pentru a imita în mod convingător chipul, vocea sau gesturile unei persoane. Unele pot părea autentice la prima vedere, mai ales atunci când sunt distribuite fără informații despre sursă sau despre contextul în care au fost realizate.

Nu te baza doar pe eventualele erori de imagine sau de sunet. Pe măsură ce tehnologia evoluează, astfel de indicii devin mai greu de observat. Este mai sigur să verifici cine a publicat materialul, când a apărut și dacă informația este confirmată și de alte surse.

Tabel 1. Elemente pentru verificarea autenticității materialelor audio-video

Ce verifici	De ce este important
Sursa materialului	Verifică cine a publicat conținutul și dacă sursa este cunoscută, transparentă și credibilă.
Confirmarea din surse independente	Informațiile importante sunt, de regulă, confirmate de mai multe surse de încredere. Dacă materialul apare într-un singur loc, tratează-l cu prudență.
Contextul și data publicării	Imagini sau videoclipuri mai vechi pot fi reutilizate pentru a susține afirmații false ori pot fi prezentate într-un context diferit de cel original.
Proveniența imaginii sau a videoclipului	Folosește căutarea inversă pentru imagini sau pentru cadre extrase dintr-un videoclip, astfel încât să identifici apariții anterioare și, dacă este posibil, sursa inițială.
Coerența informațiilor prezentate	Fii atent la neconcordanțe între mișcarea buzelor și voce, schimbări nefirești ale tonului, expresii rigide sau alte elemente care nu se potrivesc. Aceste indicii nu sunt întotdeauna prezente, dar pot ridica semne de întrebare.
Mesajele care provoacă reacții puternice	Afirmațiile șocante, senzaționale sau care provoacă teamă, furie ori entuziasm trebuie verificate înainte să fie distribuite.

Materialele generate sau modificate cu ajutorul inteligenței artificiale pot fi dificil de identificat doar după aspect sau sunet. Înainte să consideri un material autentic ori să îl distribui, verifică sursa, data și contextul publicării. Caută informația și în alte surse credibile și folosește instrumente de căutare inversă atunci când ai îndoieli.

3.2. Conturi false și fraude promovate de influenceri generați cu ajutorul IA

Unele conturi folosesc imagini sau personaje generate cu ajutorul inteligenței artificiale pentru a părea autentice. Acest lucru nu înseamnă automat că un astfel de cont este fraudulos. Riscul apare atunci când persoanele din spatele lui ascund identitatea reală a contului, inventează o comunitate de urmăritori sau folosesc popularitatea aparentă pentru a promova produse și servicii înșelătoare.

Pentru a părea credibile, aceste profiluri pot publica frecvent, pot folosi comentarii automate și pot afișa un număr mare de urmăritori. După ce câștigă încrederea utilizatorilor, pot promova investiții cu profit garantat, produse „miraculoase", concursuri false sau oferte valabile pentru o perioadă foarte scurtă. Scopul poate fi obținerea banilor, a datelor personale sau a informațiilor bancare.

Tabel 2. Semne de avertizare asociate unui cont fals

Element de verificare	La ce să fii atent
Istoricul contului	Contul a fost creat recent, dar are deja foarte multe postări și o activitate care pare neobișnuit de bine organizată.
Interacțiunile	Există diferențe mari între numărul de urmăritori și nivelul real de interacțiune. Comentariile pot fi repetitive, foarte generale sau fără legătură cu postarea.
Identitatea persoanei	Nu găsești informații clare despre cine administrează contul, iar persoana prezentată nu apare în alte surse credibile.
Conținutul vizual	Imaginile pot conține elemente nefirești, diferențe între postări sau detalii greu de explicat. Aceste indicii nu dovedesc singure că un cont este fals.
Ofertele promovate	Sunt promise câștiguri rapide, rezultate garantate, reduceri foarte mari sau produse cu efecte nerealiste.
Metoda de plată	Ți se cere să plătești prin transfer direct, criptomonede sau alte metode care nu oferă protecție cumpărătorului.

Înainte să cumperi sau să trimiți date personale, verifică istoricul contului și caută informații despre el în alte surse. Poți folosi și căutarea inversă a imaginilor pentru a vedea dacă fotografiile au mai fost publicate sub alte nume. Nu te baza pe numărul de urmăritori, pe comentarii sau pe aspectul profesionist al profilului. Dacă oferta pare nerealistă, ți se cere să acționezi imediat ori plata poate fi făcută doar prin metode greu de recuperat, oprește-te și verifică înainte să continui.

3.3. Regula celor trei verificări înainte de a distribui

Înainte să distribui un material care te surprinde, te amuză sau îți provoacă o reacție puternică, oprește-te câteva secunde și fă trei verificări:

1. **Verifică sursa**. Află cine a publicat materialul și, dacă este posibil, cine este autorul inițial. Uită-te la istoricul contului sau al site-ului și verifică dacă publică informații clare și verificabile. Dacă sursa este anonimă, recent creată sau pare suspectă, nu distribui conținutul.
2. **Caută confirmări**. Verifică dacă aceeași informație apare și pe site-uri oficiale, în publicații cunoscute sau în alte surse independente. Faptul că o informație este repetată de mai multe conturi nu înseamnă automat că este adevărată, mai ales dacă toate preiau materialul din aceeași sursă.
3. **Verifică data și contextul**. Un material real poate deveni înșelător dacă este vechi, decupat sau prezentat într-un alt context. Verifică data, locul și împrejurările în care a fost publicat. Pentru imagini, poți folosi căutarea inversă, iar în cazul unui videoclip poți căuta unul dintre cadrele relevante pentru a identifica apariții mai vechi.

Pentru verificări suplimentare, poți folosi Google Images sau TinEye pentru căutarea inversă a imaginilor, precum și platforme specializate în verificarea informațiilor. Materialele de tip deepfake și conturile false pot părea foarte convingătoare. Câteva verificări simple, făcute înainte să distribui, te pot ajuta să identifici informațiile false și să nu contribui la răspândirea lor.

4. Managerii de parole și autentificarea cu doi factori

Conturile tale pot conține e-mailuri, documente, fotografii, date bancare și informații personale. Unele dintre ele, în special contul de e-mail, pot fi folosite și pentru recuperarea accesului la alte servicii. Din acest motiv, compromiterea unui singur cont poate avea efecte asupra întregii tale activități online. Două dintre cele mai eficiente măsuri pe care le poți lua sunt folosirea unei parole unice pentru fiecare cont și activarea unei metode suplimentare de verificare a identității.

4.1. De ce să folosești o parolă diferită pentru fiecare cont

Probabil ai zeci de conturi: e-mail, platforme universitare, rețele sociale, aplicații bancare sau magazine online. Folosirea aceleiași parole pentru mai multe servicii poate părea comodă, dar creează un risc important. Dacă parola utilizată pentru unul dintre servicii este compromisă, atacatorii o pot încerca automat și pe alte platforme. Astfel, un incident care afectează un singur serviciu poate conduce la compromiterea mai multor conturi.

Folosește o parolă lungă și unică pentru fiecare cont. Acordă o atenție deosebită contului de e-mail, aplicațiilor bancare și platformelor universitare. Nu crea parole noi prin modificarea unor detalii ușor de anticipat, precum adăugarea anului curent, a numelui platformei sau a unui singur caracter la sfârșitul unei parole reutilizate. Pentru a nu fi nevoit să memorezi toate parolele, poți folosi un manager de parole. Utilizarea unor parole distincte și a unui manager de parole reduce riscul ca o parolă compromisă să permită accesarea mai multor servicii.

4.2. Cum te ajută un manager de parole

Un manager de parole este o aplicație care poate genera parole lungi, unice și greu de ghicit. Acesta le stochează într-un spațiu protejat și le poate completa automat atunci când te autentifici pe site-uri sau în aplicații. În loc să memorezi toate parolele, trebuie să reții numai parola principală cu care accesezi managerul. Aceasta trebuie să fie lungă, unică și să nu fie folosită pentru niciun alt cont.

Protejează managerul de parole prin autentificare multifactor, atunci când această opțiune este disponibilă. Păstrează într-un loc sigur și informațiile necesare pentru recuperarea accesului, astfel încât să nu pierzi toate parolele dacă îți schimbi sau îți pierzi dispozitivul. Poți folosi un manager integrat în sistemul de operare sau în browser ori o aplicație dedicată. Înainte să alegi o soluție, verifică dacă:

- provine de la un furnizor de încredere și primește actualizări de securitate;
- este compatibilă cu dispozitivele și browserele pe care le folosești;
- permite sincronizarea securizată și recuperarea controlată a accesului;
- te avertizează în cazul parolelor reutilizate, slabe sau identificate în breșe de securitate.

Descarcă aplicația numai din surse oficiale și nu comunica nimănui parola principală, codurile de autentificare sau informațiile de recuperare.

4.3. De ce să activezi autentificarea cu doi factori

O parolă poate fi aflată în urma unui atac de phishing, a unei breșe de securitate sau a reutilizării sale pe mai multe platforme. Autentificarea cu doi factori — 2FA — adaugă o verificare suplimentară și reduce riscul ca parola să fie suficientă pentru accesarea contului. Autentificarea cu doi factori presupune utilizarea a doi factori distincți, de exemplu:

- ceva ce știi, precum parola;
- ceva ce deții, precum telefonul sau o cheie de securitate;
- ceva ce ești, precum amprenta sau caracteristicile faciale.

Autentificarea multifactor — MFA — folosește doi sau mai mulți factori distincți. Important nu este doar numărul etapelor parcurse, ci faptul că verificările aparțin unor categorii diferite. Atunci când serviciul permite, preferă metode rezistente la phishing, precum cheile de acces — passkeys — sau cheile de securitate. Dacă acestea nu sunt disponibile, folosește o aplicație de autentificare.

Codurile primite prin SMS oferă mai multă protecție decât utilizarea exclusivă a parolei, dar sunt mai vulnerabile decât celelalte variante. Nu aproba notificări de autentificare pe care nu le-ai inițiat și nu transmite altor persoane codurile primite sau generate de aplicație. Dacă serviciul îți oferă coduri de recuperare, păstrează-le într-un loc sigur, separat de dispozitivul folosit pentru autentificare.

Tabel 3. Sinteza măsurilor de protecție a conturilor

Subiect	Ce trebuie să reții	Recomandare principală
Parole unice	Reutilizarea unei parole poate pune în pericol mai multe conturi.	Folosește o parolă lungă și unică pentru fiecare cont.
Manager de parole	Generează și stochează parolele într-un spațiu protejat.	Alege o soluție de încredere și protejeaz-o printr-o parolă principală unică și MFA.
2FA/MFA	Solicită factori distincți pentru verificarea identității.	Preferă cheile de acces sau cheile de securitate și folosește o aplicație de autentificare atunci când acestea nu sunt disponibile.
Coduri de recuperare	Permit recuperarea contului dacă pierzi accesul la metoda principală de autentificare.	Păstrează-le într-un loc sigur și separat de dispozitivul folosit pentru autentificare.

5. Planul de urgență

Se poate întâmpla oricui. Poate ai deschis un e-mail care părea legitim, ai scanat un cod QR afișat într-un loc public sau ai introdus date pe un site care s-a dovedit ulterior a fi fals. Simpla accesare a unui link nu înseamnă automat că dispozitivul sau conturile tale au fost compromise.

Riscul depinde de ceea ce s-a întâmplat ulterior: dacă ai introdus o parolă sau date bancare, ai descărcat un fișier, ai instalat o aplicație ori ai aprobat o solicitare de autentificare sau de plată. Important este să te oprești, să verifici ce informații ai furnizat și să acționezi rapid pentru a limita eventualele consecințe.

5.1. Pașii pentru protejarea conturilor, a dispozitivului și a datelor bancare

Dacă ai introdus parola pe un site suspect, schimb-o imediat, folosind un dispozitiv în care ai încredere. Dacă ai folosit aceeași parolă și pentru alte conturi, schimb-o și pentru acestea, începând cu e-mailul, aplicațiile bancare și celelalte conturi importante. Folosește parole diferite și activează autentificarea cu doi factori ori de câte ori această opțiune este disponibilă. Verifică lista dispozitivelor și a sesiunilor conectate la conturile tale.

Deconectează dispozitivele pe care nu le recunoști sau, dacă platforma permite, închide toate sesiunile active și autentifică-te din nou folosind parola nouă. Verifică și dacă au fost modificate adresa de e-mail, numărul de telefon sau celelalte informații utilizate pentru recuperarea contului. Acordă o atenție deosebită contului de e-mail, deoarece acesta este folosit frecvent pentru recuperarea accesului la celelalte servicii. Verifică regulile de redirecționare a mesajelor, filtrele, aplicațiile conectate și activitatea recentă. Elimină orice regulă, adresă sau aplicație pe care nu o recunoști.

Dacă ai descărcat un fișier sau ai instalat o aplicație necunoscută, evită să accesezi conturi bancare sau alte servicii sensibile de pe dispozitivul respectiv. Actualizează sistemul de operare și soluția de securitate, apoi efectuează o scanare completă. Elimină fișierele sau aplicațiile identificate ca periculoase. Dacă dispozitivul continuă să se comporte neobișnuit, solicită ajutorul unei persoane cu experiență sau al unui serviciu tehnic de încredere. Dacă ai introdus datele cardului pe un site suspect, contactează imediat banca, folosind numărul publicat pe site-ul oficial sau înscris pe spatele cardului. Solicită blocarea cardului, verifică tranzacțiile recente și semnalează operațiunile pe care nu le recunoști. În funcție de situație, banca îți poate recomanda emiterea unui card nou și contestarea tranzacțiilor neautorizate.

Nu utiliza numerele de telefon, adresele sau linkurile din mesajul suspect pentru a contacta banca ori organizația a cărei identitate a fost folosită. Înainte să ștergi mesajele, e-mailurile sau celelalte elemente asociate incidentului, păstrează informațiile care pot fi utile pentru raportare: capturi de ecran, adresele site-urilor, numerele de telefon, adresele expeditorilor, data și ora comunicărilor și detaliile tranzacțiilor. Nu accesa din nou linkurile și nu le distribui altor persoane.

5.2. Cui ceri ajutorul și cum raportezi incidentul

Dacă ai identificat o tentativă de phishing, ai accesat un link suspect, ai scanat un cod QR fraudulos, ai descoperit un site fals sau crezi că un cont ori un dispozitiv a fost compromis, poți raporta situația Directoratului Național de Securitate Cibernetică (DNSC).

Canale de raportare DNSC:

- **Telefon**: 1911
- **Platforma națională de raportare a incidentelor de securitate cibernetică**: pnrisc.dnsc.ro
- **Site-ul oficial**: https://www.dnsc.ro

Dacă ai furnizat date bancare sau ai observat tranzacții pe care nu le recunoști, contactează mai întâi banca. Rapiditatea cu care semnalezi situația poate ajuta la blocarea cardului, limitarea pierderilor și analizarea tranzacțiilor.

Dacă ai pierdut bani, ai fost victima unui furt de identitate sau consideri că a fost săvârșită o infracțiune informatică, adresează-te Poliției Române. Pentru situațiile care necesită intervenție imediată, apelează 112. Urgențele nu trebuie raportate prin formularul online de petiții sau prin e-mail. Pentru situațiile care nu reprezintă urgențe, poți consulta canalele oficiale ale Poliției Române sau te poți adresa celei mai apropiate unități de poliție.

Dacă ai identificat un cont fals, o reclamă înșelătoare sau un conținut fraudulos pe Facebook, Instagram, TikTok, WhatsApp, YouTube, X ori pe o altă platformă, folosește funcția de raportare disponibilă în cadrul serviciului. Aceasta poate fi afișată sub denumirea „Raportează” sau „Report”. Blochează contul suspect și nu continua conversația.

Pentru a afla mai multe informații utile despre securitatea cibernetică, consultă materialele de conștientizare publicate de DNSC și resursele disponibile pe platforma sigurantaonline.ro. Platforma conține informații despre fraude online, fraude bancare, phishing, conținut de tip deepfake și măsurile recomandate în cazul unei fraude.

Concluzii

Securitatea cibernetică nu presupune doar tehnologii complexe sau cunoștințe avansate de informatică. De cele mai multe ori, protecția ta în mediul online depinde de câteva alegeri simple: verifică sursa înainte să accesezi un link, folosește o parolă diferită pentru fiecare cont, activează autentificarea cu doi factori și menține actualizate sistemul de operare și aplicațiile.

Nimeni nu este complet ferit de amenințările cibernetice, iar o greșeală se poate întâmpla oricui. Important este modul în care reacționezi. Dacă observi ceva suspect, oprește-te, verifică situația și acționează rapid. Cere ajutor atunci când ai nevoie și raportează incidentul prin canalele oficiale. O reacție promptă poate limita consecințele și poate contribui la protejarea altor utilizatori.

Recomandările prezentate în acest ghid te pot ajuta să recunoști tentativele de fraudă, să îți protejezi conturile și dispozitivele și să reacționezi corect în cazul unui incident. Nu trebuie să fii expert în securitate cibernetică pentru a aplica măsurile de bază, ci să adopți obiceiuri sigure și să rămâi atent la riscurile pe care le întâlnești.

Protejează-ți datele, informează-te din surse oficiale și transmite aceste recomandări prietenilor, colegilor și familiei. Un sfat oferit la momentul potrivit poate preveni o fraudă și îi poate ajuta și pe ceilalți să navigheze mai sigur în mediul digital.

Autori: Materialul a fost elaborat în cadrul stagiului de practică desfășurat la Directoratul Național de Securitate Cibernetică (DNSC) de următorii studenți ai Universității Babeș-Bolyai din Cluj-Napoca: Alexia Oprea, Denisa Ferencz, Simona Ionescu-Maniero și Sergiu Marian Oneț.

Activitatea de elaborare a materialului s-a desfășurat sub coordonarea specialiștilor DNSC.

Bibliografie

Abotezătoaei, D. (2024). *Abotezătoaei, D., & Nemoianu, I.* Preluat de pe Manipulat sau informat? Directoratul Național de Securitate Cibernetică: https://www.dnsc.ro/vezi/document/ghid-deepfake

Alecu, I. C.-C. (2021). *Ghid de securitate cibernetică. Cyberlearning*. Preluat de pe www.cyberlearning.ro/cybersecurity-guide/

Amoah, G. A.-A. (2022). *QR Code Security: Mitigating the Issue of Quishing (QR Code Phishing)*. Preluat de pe https://www.researchgate.net/publication/364593009_QR_Code_Security_Mitigating_the_Issue_of_Quishing_QR_Code_Phishing

Europol. (2022). *Public Wi-Fi Networks Can Be Exploited for #Ransomware*. Preluat de pe https://www.europol.europa.eu/sites/default/files/documents/public_wi-fi_networks.pdf

Europol. (2022). *Risks of Using Public Wi-Fi*. Preluat de pe https://www.europol.europa.eu/cms/sites/default/files/documents/infographic_-_risks_of_using_public_wi-fi.pdf

Europol. (2023). *Online Fraud Schemes: A Web of Deceit*. Preluat de pe https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight-Report_Online-fraud-schemes.pdf

Europol. (fără an). *E-mail-uri tip phishing. Directoratul Național de Securitate Cibernetică*. Preluat de pe https://www.dnsc.ro/vezi/document/scam-phishing-vishing

Glendale Community College. (fără an). Preluat de pe How to Recognize and Avoid a Phishing Scam: https://www.glendale.edu/about-gcc/faculty-and-staff/information-technology-services/_documents/how-to-recognize-and-avoid-a-phishing-scam.pdf

Pidlisna, A. A. (2024). *Fraudulent Websites: How to Avoid Becoming a Victim of Online Fraud. Vinnytsia National Technical University*. Preluat de pe https://www.researchgate.net/publication/381297842_FRAUDULENT_WEBSITES_HOW_TO_AVOID_BECOMING_A_VICTIM_OF_ONLINE_FRAUD

Sharevski, F. D. (2022). *Phishing with Malicious QR Codes. European Symposium on Usable Security — EuroUSEC 2022*. Preluat de pe https://eurousec2022.secuso.org/pre-proceedings/eurousec2022-final22.pdf