



**Cofinanțat de
Uniunea Europeană**



Programul Educație și Ocupare (PEO) 2021-2027

Prioritate: P9. Consolidarea participării populației în procesul de învățare pe tot parcursul vieții pentru facilitarea tranzițiilor și a mobilității

Obiectiv specific: ESO4.7_Promovarea învățării pe tot parcursul vieții, în special a oportunităților flexibile de actualizare a competențelor și de recalificare pentru toți, ținând seama de competențele antreprenoriale și digitale, printr-o mai bună anticipare a schimbării și a cerințelor de noi competențe bazate pe nevoile pieței muncii, precum și prin facilitarea tranzițiilor profesionale și promovarea mobilității profesionale

Titlu Apel: Competențe digitale pentru piața muncii - Regiuni mai puțin dezvoltate

Titlu proiect: TransformDigital

Cod Apel: PEO/375/PEO_P9/OP4/ESO4.7/PEO_A34

Cod proiect: 336830

Ce este Phishing-ul și cum îl recunoști?

În era digitală, utilizarea internetului și a serviciilor online face parte din activitățile noastre zilnice. Totuși, odată cu dezvoltarea tehnologiei, au crescut și riscurile asociate securității cibernetice. Una dintre cele mai frecvente metode utilizate de infractorii informatici pentru a obține date personale sau financiare este phishing-ul.

Phishing-ul reprezintă o tentativă de fraudă prin care atacatorii încearcă să obțină informații confidențiale, precum parole, date bancare sau informații personale, pretinzând că sunt o persoană, instituție sau companie de încredere. De cele mai multe ori, aceste atacuri sunt realizate prin e-mailuri, mesaje text sau pagini web false care imită foarte bine site-uri oficiale.

Scopul phishing-ului este de a determina utilizatorul să ofere voluntar informații sensibile sau să acceseze linkuri periculoase care pot compromite dispozitivul sau conturile personale.

Cum recunoști un mesaj de tip phishing?

Există câteva semne care pot indica faptul că un mesaj este fraudulos:

Mesaje urgente sau alarmante

Atacatorii încearcă adesea să creeze panică sau presiune, folosind formulări precum:

- „Contul dumneavoastră va fi blocat”
- „Trebuie să confirmați imediat datele”
- „Ați câștigat un premiu”





**Cofinanțat de
Uniunea Europeană**



Adrese de e-mail suspecte

Expeditorul poate folosi adrese asemănătoare cu cele oficiale, dar care conțin litere sau simboluri diferite.

Linkuri necunoscute sau suspecte

Înainte de a accesa un link, verifică adresa reală a site-ului. Multe pagini de phishing imită aspectul unor site-uri cunoscute pentru a păcăli utilizatorii.

Greșeli gramaticale sau de exprimare

Multe mesaje de phishing conțin greșeli de ortografie, formulări neobișnuite sau traduceri automate.

Cereri de informații personale

Instituțiile serioase nu solicită parole, coduri PIN sau date bancare prin e-mail sau SMS.

Cum te protejezi?

- ✓ Nu accesa linkuri sau atașamente din mesaje suspecte
- ✓ Verifică întotdeauna adresa expeditorului
- ✓ Utilizează parole puternice și diferite pentru fiecare cont
- ✓ Activează autentificarea în doi pași
- ✓ Actualizează periodic programele antivirus și sistemul de operare
- ✓ Nu furniza date personale fără verificarea sursei

De ce este importantă educația digitală?

Dezvoltarea competențelor digitale și a cunoștințelor privind securitatea cibernetică este esențială pentru utilizarea sigură a tehnologiei. Informarea și atenția pot preveni pierderea datelor personale sau compromiterea conturilor online.

Într-un mediu digital tot mai complex, protejarea informațiilor personale trebuie să devină o prioritate pentru fiecare utilizator.

