



Cofinanțat de
Uniunea Europeană



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

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

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

Titlul proiectului: eSkills – Îmbunătățirea competențelor digitale ale angajaților pentru a răspunde cerințelor pieței muncii, ID: 328355

Beneficiar: Patronatul Tinerilor Intreprinzători din România

Partener: Centrul de Consultanță și Studii Europene SRL

Material Electronic de Informare 16: Cybersecurity pentru angajați

Aprilie 2026

Fiecare angajat care folosește un calculator, un telefon de serviciu, o adresă de e-mail, o platformă online sau documente digitale are un rol important în protejarea datelor și a sistemelor companiei. De multe ori, cele mai mari vulnerabilități nu apar din cauza tehnologiei, ci din cauza lipsei de informare, a neatenției sau a unor comportamente digitale riscante.

Cybersecurity, sau securitatea cibernetică, înseamnă ansamblul măsurilor prin care informațiile, conturile, dispozitivele, aplicațiile și rețelele sunt protejate împotriva accesului neautorizat, pierderii, furtului sau compromiterii. Pentru angajați, cybersecurity nu presupune neapărat cunoștințe tehnice avansate, ci mai ales înțelegerea unor reguli simple și aplicarea lor consecventă în activitatea zilnică.



În acest context, proiectul **eSkills – Îmbunătățirea competențelor digitale ale angajaților pentru a răspunde cerințelor pieței muncii** contribuie la dezvoltarea unor competențe esențiale pentru piața muncii actuală, inclusiv prin cursuri precum **Aplicarea politicilor de securitate informatică, Protecția datelor cu caracter personal, Competențe digitale de utilizare a tehnologiei informației ca instrument de învățare și cunoaștere și Big Data, Cloud Computing și securitate cibernetică pentru companii**. Aceste programe sprijină angajații și companiile în adaptarea la cerințele digitale moderne și în reducerea riscurilor asociate utilizării tehnologiei.

1. De ce securitatea cibernetică este importantă pentru orice angajat

În activitatea profesională de zi cu zi, angajații gestionează informații diverse: date despre clienți, contracte, facturi, rapoarte, parole, documente interne, baze de date sau corespondență de serviciu. Chiar dacă unele informații par obișnuite, ele pot avea o valoare importantă pentru companie și trebuie protejate.



Un incident de securitate poate avea consecințe serioase: pierderea datelor, blocarea activității, compromiterea conturilor, afectarea imaginii companiei, pierderea încrederii clienților sau chiar sancțiuni legale în cazul expunerii datelor personale. De aceea, securitatea cibernetică trebuie privită ca parte firească a responsabilităților profesionale.



Angajatul este, de multe ori, prima linie de apărare împotriva riscurilor digitale. Un e-mail suspect identificat la timp, o parolă puternică, o atenție sporită la documentele transmise sau respectarea procedurilor interne pot preveni probleme majore.

2. Cele mai frecvente riscuri cibernetice la locul de muncă

Riscurile digitale pot apărea în multe forme, iar unele dintre ele sunt foarte greu de observat la prima vedere. Printre cele mai frecvente se află tentativele de **phishing**, prin care atacatorii trimit e-mailuri sau mesaje false pentru a obține parole, date bancare sau acces la conturi. Aceste mesaje pot părea că vin de la o instituție cunoscută, de la un furnizor, de la un coleg sau chiar de la conducerea companiei.

Un alt risc important este **utilizarea parolelor slabe sau repetate**. O parolă simplă, folosită pentru mai multe conturi, poate permite accesul rapid al persoanelor neautorizate la informații sensibile. La fel de periculoasă este transmiterea parolelor prin mesaje, salvarea lor în documente nesecurizate sau notarea lor în locuri vizibile.

Dispozitivele nesecurizate reprezintă, de asemenea, o vulnerabilitate. Un laptop fără parolă, un telefon pierdut sau un calculator lăsat deschis pot permite accesul la date confidențiale. În plus, descărcarea fișierelor din surse nesigure sau accesarea linkurilor necunoscute poate duce la infectarea sistemelor cu viruși sau programe malițioase.

Nu în ultimul rând, **gestionarea incorectă a datelor personale** poate afecta atât compania, cât și persoanele vizate. Datele clienților, angajaților sau partenerilor trebuie tratate cu responsabilitate, în conformitate cu regulile interne și cu legislația privind protecția datelor.



3. Reguli simple de cybersecurity pentru angajați

Securitatea cibernetică începe cu obiceiuri digitale corecte. Angajații nu trebuie să fie experți IT pentru a contribui la protejarea companiei, însă trebuie să respecte câteva reguli de bază.

În primul rând, fiecare cont trebuie protejat printr-o parolă puternică. O parolă sigură este suficient de lungă, nu conține informații ușor de ghicit și nu este folosită pentru mai multe conturi. Atunci când este posibil, autentificarea în doi pași ar trebui activată, deoarece oferă un nivel suplimentar de protecție.

În al doilea rând, angajații trebuie să fie atenți la e-mailurile suspecte. Un mesaj care solicită urgent date confidențiale, conține greșeli evidente, promite beneficii neobișnuite sau include linkuri necunoscute trebuie verificat cu atenție. În astfel de situații, este recomandat ca angajatul să nu acceseze linkurile și să nu descarce atașamentele înainte de confirmarea sursei.

În al treilea rând, documentele și datele trebuie gestionate responsabil. Fișierele sensibile nu trebuie trimise către persoane neautorizate, salvate pe dispozitive personale sau încărcate pe platforme nesigure. Accesul la documente trebuie acordat doar persoanelor care au nevoie reală de acele informații pentru activitatea lor.

De asemenea, angajații trebuie să blocheze calculatorul atunci când părăsesc biroul, să actualizeze aplicațiile atunci când li se solicită, să evite folosirea rețelilor Wi-Fi nesigure pentru activități profesionale și să raporteze rapid orice incident sau suspiciune.



4. Legătura dintre cybersecurity și protecția datelor personale

Securitatea cibernetică este strâns legată de protecția datelor cu caracter personal. În multe companii, angajații lucrează cu informații precum nume, adrese, numere de telefon, CNP-uri, date contractuale, date salariale sau informații despre clienți. Aceste date nu pot fi tratate superficial.

Protecția datelor înseamnă colectarea, utilizarea, stocarea și transmiterea informațiilor într-un mod responsabil și legal. Angajații trebuie să știe ce date pot utiliza, în ce scop, cui le pot transmite și cum trebuie păstrate. O greșală aparent



minoră, cum ar fi trimiterea unui document către destinatarul greșit, poate genera probleme serioase.

5. Cybersecurity și competitivitatea companiilor

O companie sigură din punct de vedere digital este o companie mai competitivă. Clienții, partenerii și furnizorii au mai multă încredere în organizațiile care protejează datele, respectă procedurile și investesc în pregătirea angajaților.

În plus, securitatea informatică reduce riscul întreruperilor de activitate. Un atac cibernetic poate bloca sistemele unei companii pentru ore, zile sau chiar săptămâni. Pentru un IMM, un astfel de incident poate însemna pierderi financiare importante. De aceea, prevenția este mult mai eficientă decât remedierea.

Angajații instruiți pot identifica riscurile mai rapid, pot evita comportamentele nesigure și pot contribui la crearea unei culturi organizaționale bazate pe responsabilitate digitală. Această cultură este esențială pentru orice companie care dorește să se digitalizeze și să se dezvolte sustenabil.

6. Rolul proiectului eSkills în dezvoltarea competențelor de securitate digitală

Proiectul eSkills sprijină angajații din regiunile Sud-Muntenia și Sud-Est în dezvoltarea competențelor digitale necesare pe piața muncii actuale. Prin evaluarea inițială a competențelor digitale și prin programele de formare oferite, participanții pot înțelege mai bine nivelul lor de pregătire și pot dobândi abilități relevante pentru activitatea profesională.

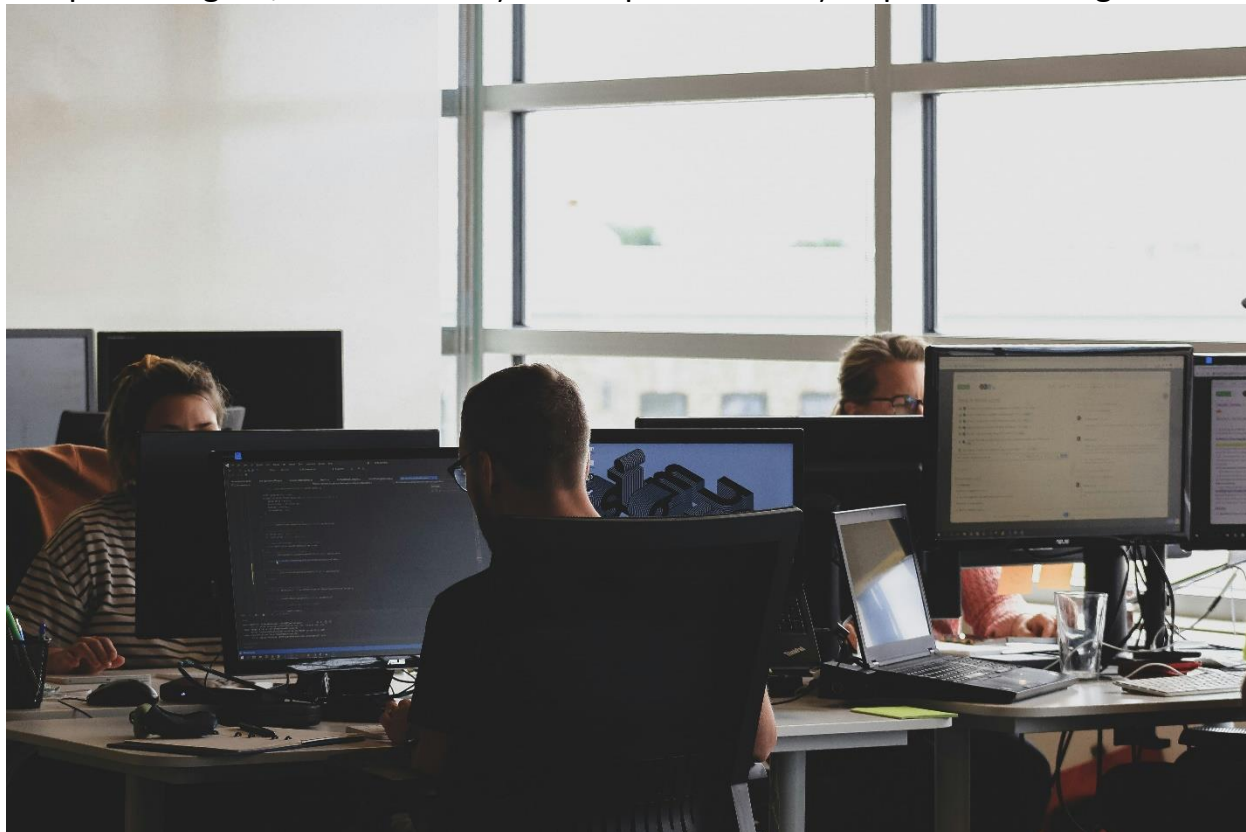
Cursurile dedicate securității informatice, protecției datelor și utilizării tehnologiei contribuie la formarea unor angajați mai atenți, mai responsabili și mai bine



Cofinanțat de
Uniunea Europeană



pregătiți pentru provocările digitale. În același timp, companiile beneficiază de echipe mai sigure, mai eficiente și mai capabile să susțină procesul de digitalizare.



Pentru a vă înscrie în proiect puteți accesa următorul link: <https://www.inscriere-eskills.ro/>

Completați formularul de la pagina respectivă, iar experții grup țintă vă vor contacta cât mai rapid cu mai multe detalii.