



Finanțat de
Uniunea Europeană



Fondul Social European Plus (FSE+)

Programul Educație și Ocupare (PEO) 2021-2027

Cod apel: PEO/79/PEO_P9/OP4/ES04.7/PEO_A36

Prioritate: P09 „Consolidarea participării populației în procesul de învățare pe tot parcursul vieții pentru facilitarea tranzițiilor și a mobilității”

Obiectiv specific: ES04.7. „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 (FSE+)”

Titlul proiectului: “ACCES la formare și cariera în București-Ilfov”

Cod SMIS: 317726

Dezvoltarea competențelor și a locurilor de muncă digitale. Securitate cibernetică la locul de muncă

Într-o eră digitală caracterizată de conectivitate continuă și volume mari de date, securitatea cibernetică la locul de muncă a devenit o prioritate esențială pentru organizații și angajați deopotrivă. Acest articol se concentrează pe importanța conștientizării riscurilor online și pe cunoașterea măsurilor de protecție a datelor personale și a informațiilor confidențiale.

1. Conștientizarea riscurilor online

Riscurile cibernetice sunt omniprezente și pot afecta grav activitățile zilnice ale unei companii. De la atacuri de tip phishing și ransomware la breșe de securitate cauzate de neglijența angajaților, amenințările sunt diverse și evoluează rapid.

Principalele riscuri online:

- **Phishing:** Mesaje sau emailuri frauduloase care încearcă să obțină informații confidențiale, cum ar fi parole sau date bancare.
- **Malware:** Software malițios, precum viruși sau troieni, care pot infecta dispozitivele utilizatorilor.
- **Acces neautorizat:** Breșe cauzate de parole slabe sau lipsa de autentificare cu doi factori.
- **Inginerie socială:** Manipulări psihologice menite să determine angajații să dezvăluie informații sensibile.

Lipsa conștientizării acestor riscuri poate conduce la pierderi financiare, daune reputaționale și compromiterea datelor confidențiale.

2. Măsuri de protecție a datelor personale și a informațiilor confidențiale

Odată ce riscurile sunt conștientizate, este esențial să fie implementate măsuri eficiente de protecție. Organizarea unei infrastructuri digitale sigure și educarea angajaților sunt pași fundamentali pentru reducerea vulnerabilităților cibernetice.

Cele mai importante măsuri de protecție:





Finanțat de
Uniunea Europeană



Fondul Social European Plus (FSE+)

Programul Educație și Ocupare (PEO) 2021-2027

Cod apel: PEO/79/PEO_P9/OP4/ES04.7/PEO_A36

Prioritate: P09 „Consolidarea participării populației în procesul de învățare pe tot parcursul vieții pentru facilitarea tranzițiilor și a mobilității”

Obiectiv specific: ES04.7. „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 (FSE+)”

Titlul proiectului: “ACCES la formare și cariera în București-Ilfov”

Cod SMIS: 317726

- **Utilizarea parolelor complexe:** Parolele trebuie să includă litere mari și mici, cifre și caractere speciale, iar schimbarea lor periodică este recomandată.
- **Activarea autentificării cu doi factori (2FA):** Aceasta adaugă un strat suplimentar de securitate, reducând riscul accesului neautorizat.
- **Criptarea datelor:** Datele sensibile ar trebui criptate pentru a preveni accesul neautorizat în caz de breșe.
- **Backup regulat:** Crearea unor copii de rezervă pentru date critice și stocarea lor în locații sigure.
- **Educația angajaților:** Organizarea de sesiuni de formare pentru a învăța echipele cum să recunoască amenințările cibernetice.

Rolul politicilor interne:

- Crearea unor politici clare privind utilizarea echipamentelor și accesul la rețeaua organizației.
- Monitorizarea activității online pentru a detecta comportamente suspecte sau breșe de securitate.
- Restricționarea accesului la informații sensibile pe baza principiului nevoii de a cunoaște (need-to-know).

3. Cultura securității cibernetice la locul de muncă

Dezvoltarea unei culturi organizaționale axate pe securitate cibernetică poate preveni numeroase incidente. Aceasta presupune implicarea tuturor angajaților, de la nivel operativ până la conducere, în adoptarea unor bune practici.

Cum poate fi promovată securitatea cibernetică?

- **Exemple din leadership:** Conducerea trebuie să adopte și să promoveze un comportament responsabil în mediul digital.
- **Comunicare constantă:** Informarea periodică a angajaților despre noi amenințări și soluții de securitate.
- **Raportarea incidentelor:** Crearea unui sistem simplu și accesibil pentru raportarea incidentelor cibernetice, astfel încât acestea să fie gestionate rapid.

Concluzie





Finanțat de
Uniunea Europeană



Fondul Social European Plus (FSE+)

Programul Educație și Ocupare (PEO) 2021-2027

Cod apel: PEO/79/PEO_P9/OP4/ES04.7/PEO_A36

Prioritate: P09 „Consolidarea participării populației în procesul de învățare pe tot parcursul vieții pentru facilitarea tranzițiilor și a mobilității”

Obiectiv specific: ES04.7. „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 (FSE+)”

Titlul proiectului: “ACCES la formare și cariera în București-Ilfov”

Cod SMIS: 317726

Securitatea cibernetică la locul de muncă nu mai poate fi considerată un subiect secundar, ci o prioritate strategică. Conștientizarea riscurilor online, implementarea măsurilor de protecție și promovarea unei culturi a securității sunt pași critici pentru protejarea datelor personale și confidențiale. Într-o lume digitală în continuă evoluție, angajații și organizațiile care investesc în securitate cibernetică vor avea un avantaj competitiv semnificativ și vor putea naviga cu succes printre provocările erei digitale.

Întocmit, *Gina NEACȘU* - Expert conștientizare, recrutare și monitorizare GT1

