



Cofinanțat de
Uniunea Europeană



FONDUL SOCIAL EUROPEAN PLUS (FSE+)

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

Securitatea conturilor digitale la locul de muncă – parole, autentificare și acces responsabil –

Utilizarea conturilor digitale a devenit o parte firească a activității profesionale. E-mailul, platformele interne, aplicațiile de lucru, serviciile cloud, bazele de date sau instrumentele de colaborare presupun autentificarea utilizatorilor și accesarea unor informații care trebuie protejate.

De multe ori, securitatea digitală este asociată exclusiv cu departamentele IT sau cu soluții tehnice complexe. În realitate, o parte importantă a protecției unei organizații depinde și de comportamentul zilnic al angajaților. O parolă reutilizată, un cont lăsat deschis pe un dispozitiv nesupravegheat sau transmiterea necorespunzătoare a datelor de autentificare pot transforma o acțiune aparent banală într-o vulnerabilitate.

Din acest motiv, utilizarea sigură și responsabilă a conturilor profesionale reprezintă o componentă importantă a competențelor digitale necesare la locul de muncă.

Parola – prima barieră de protecție a unui cont

Parolele sunt utilizate pentru a limita accesul la conturi, aplicații și informații. Cu toate acestea, eficiența lor depinde în mare măsură de modul în care sunt create și utilizate.

Parolele foarte simple, construite din informații ușor de intuit, oferă un nivel redus de protecție. Același lucru este valabil și atunci când aceeași parolă este utilizată pentru mai multe servicii.

Dacă datele de autentificare ale unui singur cont sunt compromise, reutilizarea parolei poate permite accesarea și a altor conturi.

O practică mai sigură presupune utilizarea unor parole sau fraze de acces suficient de lungi, greu de anticipat și diferite pentru conturile importante. Atunci când organizația pune la dispoziție instrumente sau proceduri pentru gestionarea securizată a parolelor, acestea trebuie utilizate conform regulilor interne.





Conturile profesionale sunt personale, chiar dacă aparțin aceleiași organizații

În activitatea curentă poate apărea tentația de a transmite unui coleg parola unui cont pentru a rezolva mai repede o sarcină. Deși pare o soluție simplă, partajarea datelor de autentificare poate crea probleme importante.

Atunci când mai multe persoane utilizează același cont fără o procedură clară, devine dificil de stabilit cine a efectuat o anumită operațiune, cine a modificat un document sau cine a accesat anumite informații.

În plus, fiecare persoană trebuie să beneficieze, pe cât posibil și conform organizării interne, de nivelul de acces necesar responsabilităților sale, nu de acces nelimitat la toate informațiile disponibile.

Accesul responsabil înseamnă, așadar, nu doar protejarea parolei, ci și respectarea regulilor privind utilizarea conturilor și a drepturilor asociate acestora.

Autentificarea în mai mulți pași adaugă un nivel suplimentar de siguranță

O parolă poate fi compromisă în diferite moduri: poate fi divulgată accidental, interceptată printr-o tentativă de fraudă sau obținută în urma compromiterii unui serviciu.

Din acest motiv, multe aplicații utilizează autentificarea multifactor (MFA) sau autentificarea în doi pași.

Aceasta presupune confirmarea identității printr-un element suplimentar, pe lângă parolă – de exemplu, printr-o aplicație de autentificare, un cod temporar sau o altă metodă aprobată.

Avantajul este simplu: cunoașterea parolei nu mai este suficientă, de una singură, pentru accesarea contului.

Atunci când această opțiune este disponibilă sau impusă de organizație, utilizarea ei contribuie semnificativ la creșterea nivelului de securitate.

„Ține-mă minte” nu este întotdeauna cea mai bună alegere

Funcțiile prin care un dispozitiv sau un browser păstrează autentificarea activă sunt utile și economisesc timp. Totuși, contextul în care sunt folosite contează.

Pe un dispozitiv profesional individual și securizat, utilizarea unor astfel de funcții poate face parte din politica normală de lucru. Pe un calculator utilizat de mai multe persoane sau pe un dispozitiv care nu este controlat de utilizator, menținerea contului autentificat poate permite altor persoane să îl acceseze.

De aceea, este important ca angajații să știe când este sigur să păstreze o sesiune activă și când trebuie să se deconecteze.

Același principiu se aplică și blocării ecranului atunci când utilizatorul se îndepărtează de dispozitiv. Câteva minute de absență pot fi suficiente pentru ca o persoană neautorizată să



acceseze informațiile afișate.

Drepturile de acces trebuie să corespundă responsabilităților profesionale

Securitatea conturilor nu se referă doar la cine poate intra într-o aplicație, ci și la ce poate face persoana respectivă după autentificare.

Într-o organizație, nu toți angajații au nevoie să acceseze aceleași informații sau să poată modifica aceleași documente.

Unele persoane pot avea nevoie doar să consulte anumite date, în timp ce altele trebuie să le poată introduce, modifica, valida sau administra.

Limitarea accesului la ceea ce este necesar pentru realizarea sarcinilor profesionale reduce riscul modificărilor accidentale, al utilizării necorespunzătoare a informațiilor și al expunerii inutile a datelor.

Un utilizator responsabil nu încearcă să obțină acces la informații de care nu are nevoie și nu utilizează drepturile disponibile în alte scopuri decât cele profesionale pentru care au fost acordate.

Dispozitivele personale și conturile profesionale trebuie utilizate cu atenție

Munca flexibilă și accesul de la distanță au făcut posibilă utilizarea conturilor profesionale de pe mai multe dispozitive și din mai multe locații.

Această flexibilitate trebuie însă însoțită de atenție.

Atunci când politicile organizației permit accesarea conturilor profesionale de pe dispozitive personale, angajatul trebuie să respecte cerințele stabilite privind securizarea dispozitivului, actualizările, blocarea accesului și protejarea informațiilor.

De asemenea, trebuie evitată salvarea necontrolată a documentelor profesionale pe dispozitive sau în servicii personale care nu sunt aprobate pentru activitatea organizației.

Comoditatea nu trebuie să înlocuiască regulile de securitate.

Ce facem dacă suspectăm că un cont a fost compromis?

Un comportament digital responsabil presupune și capacitatea de a reacționa atunci când apare o problemă.

Semnalele pot include autentificări necunoscute, notificări privind modificarea parolei, mesaje trimise fără știrea utilizatorului, solicitări neobișnuite de confirmare sau alte activități care nu pot fi explicate.

Într-o asemenea situație, problema nu trebuie ignorată în speranța că „poate nu este nimic”.

În funcție de procedurile organizației, pot fi necesare măsuri precum:

- schimbarea imediată a parolei;



- deconectarea sesiunilor active;
- informarea persoanei sau departamentului responsabil;
- verificarea activității recente a contului;
- verificarea metodelor de recuperare și autentificare asociate;
- respectarea instrucțiunilor interne pentru gestionarea incidentelor.

Rapiditatea reacției poate limita efectele unui incident de securitate.

Securitatea digitală începe cu gesturile mici și repetate

Cele mai bune sisteme tehnice nu pot elimina complet riscurile generate de utilizarea necorespunzătoare a conturilor.

Protejarea informațiilor depinde și de câteva comportamente simple: utilizarea unor parole sigure, activarea autentificării suplimentare acolo unde este posibil, blocarea dispozitivului, evitarea partajării datelor de acces, respectarea drepturilor acordate și raportarea rapidă a activităților suspecte.

Separat, fiecare dintre aceste acțiuni poate părea minoră. Împreună, ele formează însă o cultură a responsabilității digitale la nivelul organizației.

Competența digitală nu înseamnă doar să știm să intrăm într-un cont și să folosim o aplicație. Înseamnă și să înțelegem responsabilitatea care apare odată cu accesul la instrumentele, datele și informațiile profesionale.

Competențe digitale dezvoltate prin TransformDigital – ID 336830

În cadrul proiectului TransformDigital – ID 336830, angajații din grupul țintă participă la evaluarea competențelor digitale, etapă care permite identificarea nivelului existent și a nevoilor individuale de dezvoltare. În funcție de rezultatele obținute, participanții sunt orientați către programul Competențe digitale de bază sau către programul de formare Operator introducere, validare și prelucrare date (OIVPD), contribuind astfel la dezvoltarea unor competențe digitale utile, sigure și aplicabile în activitatea profesională.

**#TransformDigital #CompetențeDigitale #SecuritateDigitală #SiguranțăOnline
#DezvoltareProfesională**

**Proiect finanțat din Fondul Social European Plus (FSE+) prin Programul Educație și Ocupare (PEO)
2021-2027 în cadrul apelului " Competențe digitale pentru piața muncii - Regiuni mai puțin dezvoltate "**