

Lucrează în siguranță de acasă

RECOMANDĂRI PENTRU ANGAJATORI



Stabiliți politici și proceduri de lucru (testați-le în avans dacă este posibil)

Oferiți o politică clară în cazul telemuncii, incluzând ghiduri privind accesarea resurselor companiei, cine este persoana de contact, în caz de probleme. Stabiliți o procedură clară în caz de incidente de securitate. Aplicați măsuri suplimentare privind documentația care va necesita atenția conducerii în scopuri de semnătură, aprobare/feedback și informare.

Securizați echipamentul dedicat telemuncii



Implementați măsuri de securitate precum criptarea hard disk-ului, timpul de inactivitate, ecranele de protecție, autentificarea complexă, precum și controlul/criptarea mediilor de stocare (ex. stick USB). Implementați proceduri pentru dezactivarea de la distanță a accesului la un dispozitiv pierdut sau furat.



Acces sigur de la distanță

Permiteți doar angajaților dvs. să se conecteze la rețeaua companiei printr-o soluție de tip VPN cu autentificare multi-factor. Asigurați-vă că sesiunile la distanță se pot deconecta automat și necesită reautentificare după o anumită perioadă de inactivitate.

Actualizează frecvent sistemul de operare și aplicațiile



Astfel de măsuri scad riscul de compromitere a dispozitivelor prin vulnerabilități nerezolvate.



Securizați comunicațiile companiei

Aplicați autentificarea multi-factorială pentru a accesa conturile de e-mail ale companiei. Oferiți acces la canale sigure de comunicare între angajați, precum și unele similare pentru comunicarea cu exteriorul.

Creșteți capacitatea de monitorizare a securității



Verificați constant activitățile neobișnuite pe dispozitivele companiei și creșteți nivelul de alertă pentru atacuri legate de VPN.



Creșteți nivelul de conștientizare al angajaților în ceea ce privește riscurile de securitate ale telemuncii

Educați angajații cu privire la politica companiei în domeniul telemuncii. Alocați timp pentru a informa referitor la amenințările cibernetice, în special phishing și inginerie socială.

Faceți verificări periodice cu personalul



Stabiliți obiective, programe de lucru și mecanisme de verificare realiste, arătând flexibilitate, atunci când este posibil și ținând cont de circumstanțele personale.

Lucrează în siguranță de acasă

Recomandări

PENTRU ANGAJAȚI



Accesează datele companiei de pe echipamentele primite la serviciu

Folosiți doar dispozitive și software furnizat de companie. Creați parole puternice (folosiți un manager de parole, dacă aveți la dispoziție), nu le scrieți și protejați-le atunci când le tastați. Evitați opțiunile de lucru alternative, chiar dacă par să ofere exact ceea ce aveți nevoie.

Stop. Gândește. Conectează-te



Înainte de a începe lucrul de la distanță, familiarizați-vă cu dispozitivele, politicile și procedurile companiei. Asigurați-vă că înțelegeți modul de operare al echipamentelor, ceea ce trebuie făcut și ce nu (în cazul acestora) și unde să vă adresați.



Acces de la distanță sigur

Conectați-vă la rețeaua companiei doar prin VPN și protejați token-urile (sau cardurile inteligente) necesare pentru conexiunea VPN.

Protejează echipamentul și mediul de lucru la distanță



Nu permiteți membrilor familiei sau altor persoane să vă acceseze dispozitivele de lucru. Blocați-le sau închideți-le când sunt nesupravegheate și păstrați-le întotdeauna într-o locație sigură, pentru a preveni pierderea, deteriorarea sau furtul. Împiedicați scurgerea de date accidentală, folosind ecrane de confidențialitate și evitați orientarea ecranelor spre ferestre sau camere foto.



Raportați

Dacă observați vreo activitate neobișnuită sau suspectă pe orice dispozitiv pe care îl utilizați pentru a lucra la distanță, contactați imediat angajatorul pe canale sigure.



Fii atent!

Atenție la orice activități sau cereri suspecte, în special la cele financiare. Ar putea fi o fraudă! În cazul în care aveți dubii, apelați solicitantul pentru a verifica. Nu faceți clic pe linkurile sau fișierele atașate primite în e-mailuri și mesaje text nesolicitate.

Evitați furnizarea de informații personale



Nu răspundeți niciodată cu informații personale la mesaje, chiar dacă pretind că provin dintr-o sursă legitimă. În schimb, contactați direct compania pentru a confirma solicitarea acestora.



Dezvoltați noi rutine

Discutați planurile de lucru cu conducerea și membrii echipei, în perioada lucrului de la distanță, inclusiv distribuirea sarcinilor, a termenelor și a canalelor de comunicare.

Folosirea dispozitivelor private



Dacă utilizarea dispozitivului personal este singura opțiune de lucru și angajatorul dvs. vă permite folosirea lui, asigurați-vă că sistemul de operare și software-ul dispozitivului sunt actualizate, aveți o soluție antivirus instalată, iar conexiunea este securizată printr-un VPN aprobat de companie.



Separă activitatea pentru job de cea recreativă!

Evitați folosirea în interes personal a dispozitivelor dedicate lucrului de la distanță.