Siguran rad na daljinu

SAVJETI I PREPORUKE ZA POSLOVNE SUBJEKTE

Uspostavite korporativne radne postupke (testirajte ih unaprijed ako je moguće)

Osigurajte jasne postupke o radu na daljinu, uključujući smjernice o pristupu korporativnim resursima i kome se obratiti u slučaju problema. Uspostavite jasan postupak u slučaju sigurnosnih incidenata. Primijenite dodatne mjere u vezi s dokumentacijom za srednje i više rukovodstvo radi potpisivanja, odobravanja i informiranja.

Osigurajte svoju opremu za rad na daljinu

Primijenite mjere poput šifriranja tvrdog diska, vremenskih ograničenja neaktivnosti, zaslona privatnosti, jake provjere autentičnosti i kontrole prenosivih medija i enkripcije (npr. USB pogona). Provedite postupak za onemogućavanja pristupa na daljinu izgubljenom ili ukradenom uređaju.

Siguran pristup na daljinu

Omogućite samo svojim zaposlenicima da se povežu s korporativnom mrežom putem VPN-a koji pruža tvrtka s višefaktornom autentifikacijom. Osigurajte automatski istek vremena rada na daljinu i traženje ponovne provjere autentičnosti nakon određenog razdoblja neaktivnosti.

Redovito ažurirajte operativne sustave i aplikacije uređaja

To će pomoći u smanjenju rizika od kibernetičkog kriminala u kojem se iskorištavaju ranjivosti za koje nema zakrpa.

Osigurajte svoju korporativnu komunikaciju

Provedite upotrebu multifaktorske provjere autentičnosti za pristup korporacijskim računima e-pošte. Omogućite pristup sigurnim komunikacijskim kanalima za zaposlenike radi lakog međusobnog povezivanja te komunikacije s vanjskim suradnicima.

Povećajte nadzor sigurnosti

Aktivno provjeravajte neobične aktivnosti udaljenog korisnika i povećajte razinu upozorenja za napade povezane s VPN-om.

Povećajte svijest osoblja o rizicima rada na daljinu

Educirajte zaposlenike o politici tvrtke na području rada na daljinu. Odvojite vrijeme za podizanje svijesti o kibernetičkim prijetnjama, posebno o phishingu i socijalnom inženjeringu.

Redovito se javljajte osoblju

Postavite realne ciljeve, raspored rada i mehanizme daljnjeg praćenja, budite fleksibilni gdje je to moguće i uzmite u obzir osobne okolnosti.

EUROPOL | EC3 European Cybercrime Centre

Siguran rad na daljinu

SAVJETI I PREPORUKE ZA ZAPOSLENIKE

Pristupite podacima tvrtke preko opreme tvrtke

Koristite samo uređaje i softver koji tvrtka stavlja na raspolaganje. Stvorite snažne lozinke (koristite pouzdane/odobrene upravitelje lozinki ako su dostupni), ne zapisujte ih i zaštitite ih od pogleda prilikom unošenja. Izbjegavajte mogućnosti zaobilaznih rješenja čak i ako vam se čini da pružaju upravo ono što vam je potrebno.

Stanite. Promislite. Spojite se

Prije nego što započnete rad na daljinu, upoznajte se sa službenim uređajima, pravilima i postupcima. Pazite da razumijete kako radi oprema, što se smije, a što se ne smije raditi s njom i gdje potražiti pomoć.

Siguran pristup na daljinu

Povežite se s korporativnom mrežom samo putem korporativnog VPN-a i zaštitite tokene (npr. pametne kartice) potrebne za VPN vezu.

Zaštitite svoju opremu za rad na daljinu i okruženje

Ne dozvolite članovima obitelji pristup vašim radnim uređajima. Zaključajte ih ili isključite kada nisu pod nadzorom i držite ih na sigurnom mjestu da biste spriječili gubitak, oštećenje ili krađu. Spriječite surfanje preko ramena korištenjem zaslona privatnosti i izbjegavajte usmjeravanje zaslona prema prozorima ili kamerama.

Prijava

Ako primijetite bilo kakvu neobičnu ili sumnjivu aktivnost na bilo kojem uređaju koji koristite za rad na mreži, odmah se obratite svom poslodavcu preko odgovarajućih kanala.

Budite na oprezu

Pazite na sumnjive aktivnosti i zahtjeve, posebno one financijske prirode. To bi mogla biti CEO prijevara! U slučaju sumnje, nazovite podnositelja zahtjeva radi dvostruke provjere.
Ne otvarajte poveznice ili privitke primljene u nezatraženoj e-pošti i tekstualnim porukama.

Izbjegavajte davanje osobnih podataka

Nikada ne odgovarajte osobnim podacima na poruke, čak i ako tvrde da su iz zakonitih izvora. Umjesto toga, kontaktirajte tvrtku izravno kako biste potvrdili njihov zahtjev.

Razvijajte nove rutine

Razgovarajte o planovima rada s vašim izravnim rukovodstvom i članovima tima tijekom rada na daljinu, uključujući raspodjelu zadataka, rokova i kanala komunikacije.

Upotreba privatnih uređaja

Ako je korištenje vašeg osobnog uređaja jedina opcija, a poslodavac to dopušta, provjerite jesu li operativni sustav i softver vašeg uređaja ažurirani, uključujući antivirusni/antimalware program i je li veza zaštićena putem VPN-a koji je odobrila vaša tvrtka.

Odvojite posao od slobodnog vremena

Izbjegavajte osobnu upotrebu uređaja za rad na daljinu.

EUROPOL | EC3 European Cybercrime Centre