

Informationssäkerhet för dig som arbetar hemma

Vad är viktigt att tänka på när du och många andra samtidigt arbetar hemifrån? När fler än vanligt arbetar utanför arbetsplatsen hanteras organisationens information på ett sätt som varken vi eller våra it-system är vana vid. Det är viktigt att informationen hanteras säkert så att vi undviker att information hamnar i orätta händer, att den förstörs eller blir felaktig. För att minska riskerna, tänk på följande:



Vilka regler gäller för distansarbete i din organisation? Ta reda på vad som gäller och följ dem så att du inte blir en säkerhetsrisk. Håll dig informerad eftersom reglerna i kristider kan förändras snabbt.



Vilka regler gäller för uppkoppling mot arbetsplatsen/organisationen? När du kopplar upp dig mot organisationens it-miljö, följ reglerna. Ditt hemmanätverk kan av olika anledningar vara osäkert och inte ge informationen tillräckligt skydd. Kräver din organisation att du använder en VPN-tjänst eller tvåfaktorsinloggning? Finns krav på att enbart koppla upp dig via mobiltelefonen och använda mobildata? Du behöver veta vad som gäller.



Om det uppstår begränsningar i antalet uppkopplade medarbetare behöver ni komma överens om hur ni kan lägga upp arbetet och prioritera det viktigaste i verksamheten. Håll dig informerad om vad som gäller och hur ni kan hjälpas åt att minska belastningen. Exempelvis kan du bli ombedd att arbeta lokalt och enbart koppla upp dig korta stunder eller vissa tider.



Om du inte har åtkomst till organisationens informationssystem, på grund av att nätverket har gått ned behöver du få råd om hur du kan spara informationen på ett säkert sätt. Spara aldrig känslig information i privata molnlösningar.



Din arbetsutrustning – dator, surfplatta eller mobiltelefon är personlig och ska inte användas för privat bruk eller av andra. Informationen där ska skyddas. Det innebär att du alltid ska logga ut och låsa datorn när du lämnar den, även hemma. Ingen annan ska ha tillgång till utrustningen eller kunna ta del av informationen. Säkerställ att du har starka lösenord.



USB-minnen ska inte användas mellan privat utrustning och din arbetsdator eftersom virus kan spridas mellan enheter.



Tänk på att skydda också viktig information som finns på papper och i anteckningar. Förvara din information säkert och tänk på att låsa utrymmen där känslig information finns.



Vid digitala arbetsmöten, bedöm risken att andra kan höra eller se informationen som förmedlas.



Minska risken för att bli utsatt för bedrägeri genom att låta bli att klicka på länkar eller bilagor från okända avsändare. Ladda heller inte ned program som kommer via e-post, sms eller olika webbsidor, särskilt när avsändaren är okänd.