BYGGA EN SÄKER ORGANISATION FÖR DISTANSARBETE

En tredjedel av IT-beslutfattarna medger att deras organisationer har drabbats av datainträng med anledning av distansarbete. Hur ser du till att dina företagsdata förblir skyddade i dessa tider när allt inte är som vanligt?

01.

Säkerställ din policy för arbete på distans

Det är **3,5 gånger** mer sannolikt att ett nätverk på hemmakontoret infekteras av skadlig programvara än ett företagsnätverk[1]

Cyberbrottslingar vet om du är en **hemanvändare eller** en företagsanvändare som arbetar hemifrån

Skydda dina medarbetare med en policy för **säkert arbete på distans** och undvik potentiell datafördrivet eller utpressning med dina egna filer

02.

Var extra vaksam på nätfiskeattacker

Covid-19-relaterat nätfiske via e-postmeddelanden representerar den största typen av **angrepp**[1]

Bedrägerier ökade med över **400 %** i Storbritannien under februari och mars[4]. Offren förlorade sammanlagt över 1,6 miljoner pund[5]

Se till att dina medarbetare vet hur de **kontrollerar vem det är som har skickat** ett e-postmeddelande innan de öppnar det. De bör även tänka efter innan de klickar på okända länkar

03.

Glöm inte bort säkerheten för enheter hemma

Dina medarbetare använder den skrivare eller scanner som de har hemma

De enheterna har förmodligen **inte de vanliga säkerhetsfunktioner** som företagets nätverksutrustning tillhandahåller

När över **25 %** av alla enheter har en eller flera tjänster exponerade på internet[6] är de mer sårbara för angrepp

För att skydda företagskritiska data bör du säkerställa att dina medarbetare har ett privat nätverk som endast kan nås med ett **säkert**, ovanligt lösenord

04.

Och konfidentiellt pappersarbete

Säkerställ att medarbetare som arbetar på distans behandlar företagets information med samma försiktighet som sina egna viktiga papper, vilket innebär att förstöra eller på ett **säkert sätt förvara allt konfidentiellt** tills de återvänder till kontoret

05.

Den bästa policyn är att ha en

Att arbeta hemifrån **innebär inte att** företagets policyer kan ignoreras

Påminn medarbetarna om att endast använda program, nätverk och molnplatser **som tillhandahålls av företaget**

Alla kostnadsfria molnsamarbeten och lagringsverktyg som de kan använda kanske **inte är säkra** om de inte först har granskats av dig

Om någon medarbetare arbetar på distans måste du säkerställa att personen tydligt förstår hur man upprätthåller samma företagssäkerhet oavsett om man arbetar på kontoret eller hemma i soffan.

Kontakta Canon för att lära dig att inte bara överleva, utan till och med blomstra i dessa tider när allt inte är som vanligt.

Canon

See the bigger picture

[1] https://www.techradar.com/news/malware-attacks-on-home-networks-are-35-times-more-common
[2] https://www.techradar.com/news/malware-attacks-on-home-networks-are-35-times-more-common
[3] https://www.techradar.com/news/malware-attacks-on-home-networks-are-35-times-more-common
[4] https://www.cybersecuritydive.com/news/phishing-attacks-increase-400-percent-during-coronavirus-crisis/580.html
[5] https://www.cybersecuritydive.com/news/phishing-attacks-increase-400-percent-during-coronavirus-crisis/580.html
[6] https://www.techradar.com/news/malware-attacks-on-home-networks-are-35-times-more-common