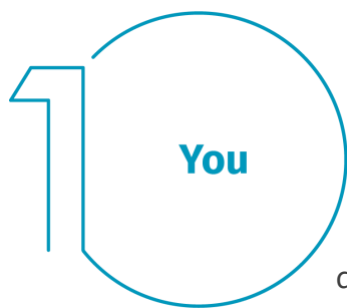


5 bästa stegen för att arbeta säkert hemma

Vi är medvetna om att alla kanske inte har arbetat hemifrån tidigare, och att det kan vara överväldigande att anpassa sig till en ny miljö. Ett av våra mål är därför att se till att ditt arbete hemifrån blir så säkert som möjligt. Nedan följer fem enkla steg för att arbeta säkert. Det bästa av allt är att alla dessa steg inte bara hjälper dig att arbeta säkert, utan att det även hjälper dig att skapa ett cybersäkert hem vilket leder till en betydligt säkrare tillvaro för dig och din familj.



Du: Först och främst, teknik i sig kan inte ge dig fullständigt skydd – du är det bästa försvaret. Angripare har lärt sig att det enklaste sättet att komma åt det de vill ha är att ha dig som måltavla, istället för din dator eller andra enheter. Om de vill komma åt ditt lösenord, dina arbetsdata eller styra din dator, försöker de lura dig till att lämna ut dessa uppgifter, ofta genom att skapa en brådskande känsla.

Exempelvis kan de ringa dig och låtsas vara Microsofts tekniska support eller hävda att din dator är infekterad. De kan även skicka ett e-postmeddelande till dig med en varning som säger att paketet inte kunde skickas och på så sätt lura dig till att klicka på en skadlig länk. De vanligaste tecknen på ett socialt manipulationsangrepp omfattar:

- Någon skapar en stark brådskande känsla, ofta genom rädsla, hot, en kris eller en viktig deadline. Cyberangripare är bra på att skapa övertygande meddelanden som verkar komma från betrodda organisationer, till exempel banker, myndigheter eller internationella organisationer.
- Pressa dig till att kringgå eller ignorera säkerhetspolicyer eller förfaranden, eller erbjuda något som är för bra för att vara sant (nej, du vann inte på lotto!)
- Ett meddelande från en vän eller kollega där signaturen, tonen eller formuleringen inte låter som dem.

I slutändan är du det bästa försvaret mot dessa angrepp.

2 Home Network

Hemnätverk: Nästan alla hemnätverk börjar med ett trådlöst nätverk (som ofta kallas Wi-Fi). Detta är det som gör det möjligt att ansluta dina enheter till internet. De flesta trådlösa hemnätverken kontrolleras av din internetrouter eller en separat, tillägnad trådlös åtkomstpunkt. Båda fungerar på samma sätt: genom att sända trådlösa signaler som enheter i hemmet ansluter till. Detta innebär att det är viktigt att säkra ditt trådlösa nätverk för att skydda ditt hem. Vi rekommenderar följande steg för att säkra det:

- Ändra det fabriksinställda administratörslösenordet för enheten som styr ditt trådlösa nätverk. Administratörskontot är det som låter dig konfigurera inställningarna för ditt trådlösa nätverk.
- Se till att endast personer som du litar på kan ansluta till ditt trådlösa nätverk. Gör detta genom att aktivera stark säkerhet. Genom att aktivera detta behöver personer ett lösenord för att kunna ansluta till ditt trådlösa nätverk, och när de är anslutna är deras onlineaktiviteter krypterade.
- Se till att lösenordet som personer använder för att ansluta till ditt trådlösa nätverk är ett starkt lösenord och att det skiljer sig från administratörslösenordet. Kom ihåg att du bara behöver ange lösenordet en gång för var och en av dina enheter, då de lagrar och kommer ihåg lösenordet.

Vet du inte hur man utför dessa steg? Be din internetleverantör om hjälp, kolla in deras webbplats, läs dokumentationen som medföljer din trådlösa åtkomstpunkt eller läs på återförsäljarens webbplats.

3 Passwords

Lösenord: När en webbplats ber dig att skapa ett lösenord: skapa ett starkt lösenord, ju fler tecken det har, desto starkare är det. Att använda en lösenordsfras är ett av de enklaste sätten att se till att du har starka lösenord. En lösenordsfras är ingenting annat än ett lösenord som består av flera ord, såsom "*bi honung whiskey*." Att använda en unik lösenordsfras innebär att du använder olika fraser för alla enheter eller onlinekonton. På så sätt är alla dina övriga konton och enheter fortfarande säkra om ett av dem komprometteras. Kan du inte komma ihåg alla dina lösenordsfraser?

Använd en lösenordshanterare, vilket är ett specialiserat program som säkert lagrar alla dina lösenordsfraser i ett krypterat format (och dessutom har flera andra bra funktioner!). Avslutningsvis, aktivera tvåstegsverifiering (som även

kallas tvåfaktorsautentisering eller multifaktorautentisering) när du har möjlighet. Den använder ditt lösenord, men lägger dessutom till ett andra steg, som t.ex. en kod som skickas till din smartphone eller en app som genererar koden för dig. Tvåstegsverifiering är antagligen den viktigaste åtgärden som du kan vidta för att skydda dina onlinekonton och är betydligt enklare än du kan tro.



Uppdateringar: Se till att var och en av dina datorer, mobila enheter, program och appar har den senaste versionen av dess programvara. Cyberangripare letar ständigt efter nya sårbarheter i programvaran som dina enheter använder. När de upptäcker sårbarheter, använder de särskilda program för att utnyttja dem och hacka enheterna som du använder. Samtidigt arbetar företagen som skapade programvaran för dessa enheter hårt med att fixa problemen genom att lansera uppdateringar. Genom att se till att dina datorer och mobila enheter omgående installerar dessa uppdateringar, gör du det svårare för någon att hacka dig. Det är bara att aktivera automatiska uppdateringar när sådana finns. Denna regel gäller nästan för all teknik som är ansluten till ett nätverk, alltså inte bara dina enheter för jobbet utan också internetanslutna TV-apparater, babymonitorer, säkerhetskameror, hemrouters, spelkonsoler eller till och med din bil.



Barn/Gäster: Något du sannolikt inte behöver oroa dig för på jobbet är att barn, gäster eller andra familjemedlemmar använder din laptop eller andra enheter avsedda för arbetet. Se till att din familj och dina vänner förstår att de inte får använda dina arbetsenheter, då de oavsiktligt kan radera eller modifiera information, eller ännu värre, oavsiktligt infektera enheten.