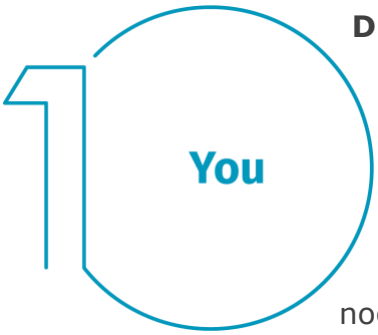
De 5 bedste trin til at arbejde sikkert hjemmefra

Vi ved godt, at det kan være helt nyt og måske lidt overvældende at arbejde hjemmefra, mens du skal vænne dig til dine nye omgivelser. Et af vores mål er at gøre dig i stand til at arbejde så sikkert hjemmefra som muligt. Herunder kan du se fem tips til, hvordan du arbejder sikkert hjemmefra. Det bedste er, at disse tips ikke kun hjælper dig med at sikre dit arbejde, men at de også vil gøre dig og din familie meget sikrere, når I cybersikrer jeres hjem.



Dig: Først fremmest skal du vide, at teknologien alene ikke kan beskytte dig – du er det bedste forsvar. Angriberne har lært, at den letteste måde at nå deres mål på er ved at gå efter dig snarere end din computer eller andre enheder. Hvis de vil have dit kodeord, dine arbejdsdata eller kontrol over din computer, vil de forsøge at snyde dig til at give det til dem, ofte ved at få dig til at gøre noget hurtigt. De kan for eksempel finde på at ringe til dig og udgive sig for at være fra Microsofts tekniske support og påstå, at din computer er inficeret af virus. Eller måske sender de en advarsel via e-mail om, at en pakke ikke kunne afleveres, og snyder dig til at klikke på et ondsindet link. De mest almindelige tegn på social engineering-angreb omfatter:

- Nogen forsøger at skabe en følelse af, at noget haster, ofte gennem frygt, trusler, en krise eller en vigtig tidsfrist. Cyberangribere er gode til at lave overbevisende beskeder, der synes at komme fra troværdige virksomheder som banker, regeringsafdelinger eller internationale organisationer.
- Pres for at omgå eller tilsidesætte sikkerhedspolitikker eller -procedurer og tilbud, der er for gode til at være rigtige (nej, du har ikke vundet i lotteriet!).
- En besked fra en ven eller kollega, som du kender, men signaturen, ordlyden eller tonen i beskeden lyder ikke som dem.

I sidste ende er du det bedste forsvar mod disse angreb.

Hjemmenetværk: Næsten alle hjemmenetværk har et trådløst (Wi-Fi) netværk. Det forbinder dine enheder trådløst til internettet. De fleste trådløse hjemmenetværk er styret af din internetrouter eller et separat, dedikeret trådløst adgangspunkt. De fungerer begge på samme måde: Ved at udsende trådløse signaler, som hjemmeenhederne tilslutter til. Det betyder, at sikring af dit trådløse netværk er afgørende for dit hjems cybersikkerhed. Vi anbefaler følgende fremgangsmåde:

- Skift administrator-standardkodeordet for den enhed, der styrer dit trådløse netværk. Din administratorkonto lader dig konfigurere indstillingerne for dit trådløse netværk.
- Sørg for, at det kun er personer, du har tillid til, som har forbindelse til dit trådløse netværk. Det kan du gøre ved at bruge stærk sikkerhed. Det kræver, at folk skal indtaste et kodeord for at tilslutte til dit trådløse netværk, så deres onlineaktiviteter bliver krypteret, når de har forbindelse.
- Sørg for, at det kodeord, folk bruger ved tilslutning til dit trådløse netværk, er stærkt og ikke det samme som administratorkodeordet. Husk, at du kun skal indtaste kodeordet én gang for hver af dine enheder, da de gemmer og husker det.

Er du usikker på, hvordan du skal følge disse trin? Spørg din internetudbyder, tjek deres hjemmeside, læs dokumentationen, der følger med dit trådløse adgangspunkt, eller kig på forhandlerens webside.

Adgangskoder: Når en side beder dig om at oprette et kodeord: Lav et stærkt kodeord; jo flere tegn, det indeholder, jo stærkere er det. Kodeordssætninger er en af de simpleste metoder til at lave et stærkt kodeord. En kodeordssætning er bare et kodeord, der består af flere ord, som for eksempel "*bi honning bourbon.*" Med unikke kodeordssætninger menes der, at du skal bruge forskellige sætninger til alle dine enheder og onlinekonti. Sådan undgår du at, alle dine konti og enheder bliver inficeret, hvis en af dem kompromitteres. Kan du ikke huske alle dine kodeordssætninger?

Så brug en kodeordsadministrator, som er et specialiseret program, der gemmer alle dine kodeordssætninger i krypteret format (og som også indeholder mange andre smarte funktioner). Endelig skal du også aktivere tofaktorgodkendelse

(også kaldet totrinsbekræftelse eller multifaktorgodkendelse), hvis muligt. Denne metode bruger din kode, men tilføjer et ekstra trin, for eksempel en kode sendt til din smartphone eller en app, der genererer koden for dig. Tofaktorgodkendelse er nok det vigtigste trin, når du skal beskytte dine onlinekonti, og det er meget lettere, end du sikkert tror.

Opdateringer: Sørg for, at alle dine computere, mobile enheder, programmer og apps kører den nyeste version af deres software. Cyberangribere søger konstant nye sårbarheder i den software, dine enheder bruger. Når de opdager svagheder, bruger de særlige programmer for at udnytte dem og hacke de enheder, du bruger. Imens arbejder de firmaer, der har udviklet softwaren, hårdt på at fjerne svaghederne ved at udgive opdateringer. Ved at sikre, at dine computere og mobile enheder installerer disse opdateringer hurtigt, kan du gøre det meget sværere for angribere at hacke dig. Aktivér automatiske opdateringer for at sikre dine enheder bedst muligt. Denne regel gælder for næsten al teknologi, der er forbundet til et netværk – både dine arbejdsenheder og internettilsluttede fjernsyn, babyalarmer, sikkerhedskameraer, hjemmeroutere, spillekonsoller eller din bil.

Børn / Gæster: På kontoret behøver du sikkert ikke at bekymre dig om børn, gæster eller familiemedlemmer, der bruger din arbejdscomputer eller andre arbejdsenheder. Sørg for, at familie og venner forstår, at de ikke kan bruge dine arbejdsenheder, da de kan komme til at slette eller modificere oplysninger eller, værre endnu, komme til at inficere enheden.