SANS SECURITY AWARENESS

5 tiltak som gjør hjemmekontoret sikrere

Vi vet at det å ha hjemmekontor kan være nytt for enkelte av dere. Kanskje det til og med kan være litt overveldende å tilpasse seg de nye omgivelsene. Et av våre mål er å la deg kunne jobbe så sikkert som mulig fra hjemmekontoret ditt. Under finner du fem enkle steg som hjelper deg med å sikre arbeidet ditt. Det beste med det hele er at disse stegene ikke bare hjelper deg med å sikre arbeidet ditt, men de vil også gjøre både deg og familien din mye tryggere ved at du øker cybersikkerheten i hjemmet ditt.

Deg selv: Først og fremst kan ikke teknologien alene beskytte deg. Du er selv det beste forsvaret. Angripere har lært at den enkleste måten å få det de ønsker seg på, er ved å angripe deg direkte. Dette velger de fremfor å angripe datamaskinen din eller andre enheter. Om de ønsker å få tak i passordet ditt, arbeidsinformasjon eller kontroll over datamaskinen din, vil de prøve å lure deg til å gi det til dem direkte. Dette blir ofte gjort ved å skape en følelse av at noe haster. De kan for eksempel utgi seg for å være fra Microsofts kundestøtte og fremlegge påstander om at datamaskinen din er infisert. Eller kanskje de sender deg en advarsel på e-post om en pakke som ikke kunne leveres. Kun for å lure deg til å klikke på en farlig lenke som er vedlagt i e-posten. De mest vanlige tegnene på sosialmanipuleringsbaserte angrep er bl.a.:

- Noen skaper følelsen av at noe haster veldig, ofte ved å spille på frykt, trusler, krisesituasjoner eller viktige tidsfrister. Cyberangripere er flinke til å lage overbevisende meldinger som ser ut til at de kommer fra troverdige organisasjoner som banker, regjeringen eller internasjonale organisasjoner.
- Press om å forbigå eller ignorere sikkerhetsforskrifter eller prosedyrer, eller et tilbud som er for godt til å være sant. (Dessverre, du har ikke vunnet i lotto!)

- En melding fra en venn eller kollega, men signaturen, ordlyden og tonen på meldingen høres ikke ut som vedkommende.

Til syvende og sist er det beste forsvaret mot slike angrep deg selv.

HjemmenettverkNesten: alle hjemmenettverk starter med et trådløst nettverk. Dette kalles som oftest for et Wi-Fi-nettverk. Dette er det som lar alle enhetene dine koble seg til Internett. De fleste trådløse hjemmenettverk styres av Internett-ruteren din eller et trådløst tilgangspunkt. Begge to fungerer på samme måte: De kringkaster trådløse signaler som enhetene dine kan koble seg til. Dette innebærer at det å sikre det trådløse nettverket er viktig når du skal beskytte hjemmet ditt. Vi anbefaler å gjøre det følgende for å sikre nettverket:

- Endre standardpassordet til administratorbrukeren på enheten som styrer det trådløse nettverket ditt. Administratorbrukeren er den som lar deg konfigurere innstillingene til det trådløse nettverket.
- Sørg for at kun de du stoler på, kan koble seg til det trådløse nettverket ditt. Gjør dette ved å aktivere sterk sikkerhet. Ved å aktivere dette vil et passord være nødvendig for at folk skal kunne koble seg til det trådløse nettverket. Handlinger de gjør på nett, vil nå være kryptert.
- Sørg for at passordet som brukes til å koble seg til det trådløse nettverket ditt, er et sterkt passord og at det ikke er det samme som du har brukt på administratorbrukeren. Husk på at siden enheter kan oppbevare og huske passord, trenger du kun å oppgi passordet én gang per enhet.

Vet du ikke hvordan du gjør dette? Ta kontakt med Internett-leverandøren din, klikk deg inn på nettsidene deres, sjekk dokumentasjonen som fulgte med det trådløse tilgangspunktet, eller oppsøk produsentens nettside.

Passord: Når en nettside ber deg om å opprette et passord, må du lage et sterkt passord. Jo flere tegn det består av, desto sterkere er passordet. Å bruke en passordsetning er en av de enkleste måtene å sørge for at du har et sikkert passord. En passordsetning er rett og slett et passord som består av flere forskjellige ord. Som f.eks. «*bie honning bourbon.*» Å bruke en unik passordsetning vil si at man bruker forskjellige passord på hver enhet og nettbaserte konto. På denne måten vil alle de andre kontoene og enhetene dine forbli trygge, selv

om en av passordsetningene dine kommer på avveie. Klarer du ikke å huske på alle passordsetningene dine?

Bruk et passordverktøy. Dette er et spesialisert program som trygt lagrer passordsetningene dine i et kryptert format. De har mange andre flotte funksjoner også! Bruk også totrinnsverifisering (ofte også kalt tofaktorverifisering eller multifaktorverifisering) der det lar seg gjøre. Det bruker også passordet ditt, men legger også til et ekstra steg i form av en kode som sendes til smarttelefon din, eller en app som oppretter en kode for deg. Totrinnsverifisering er kanskje det viktigste steget du kan ta for å beskytte nettbaserte kontoer, og det er mye enklere enn du kanskje tror det er.

Oppdateringer: Sørg for at datamaskiner, mobile enheter, programmer og apper kjører de nyeste utgavene av programvaren de bruker. Cyberangripere ser hele tiden etter nye svakheter de kan utnytte i programvaren som enhetene dine bruker. Finner de svakheter, bruker de spesialiserte programmer til å utnytte dem eller hacke seg inn på enhetene du bruker. Firmaene som utvikler programvaren du bruker på disse enhetene, jobber ofte iherdig med å fikse slike problemer og gir ut oppdateringer som fikser dem. Ved å sørge for at datamaskiner og mobile enheter installerer disse oppdateringene, gjør du det mye vanskeligere for andre å hacke deg. Du holder deg enkelt oppdatert ved å aktivere automatiske oppdateringer der dette lar seg gjøre. Denne regelen gjelder for nesten enhver form for teknologi som er koblet til et nettverk. Det gjelder ikke bare arbeidsmaskiner, men også TV-er som er koblet til Internett, babycaller, overvåkningskameraer, hjemmerutere, spillkonsoller og selv bilen din.

Barn/gjester: Noe du som oftest ikke trenger å tenke på når du er på kontoret ditt, er barn, gjester og andre familiemedlemmer som bruker arbeidsmaskinen din eller andre arbeidsrelaterte enheter. Sørg for at familie og venner forstår at de ikke kan bruke arbeidsmaskinene dine. Det kan hende de ved et uhell sletter eller endrer informasjon eller til og med utilsiktet infiserer enheten.