SANS SECURITY AWARENESS

OUCH!

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

Telefonsvindel

Oversikt

Når du hører ordet «cyberkriminell» ser du kanskje for deg en ond mesterskurk sittende bak en dataskjerm, mens han gjennomfører sofistikerte angrep over internett. Selv om mange av nåtidens cyberkriminelle bruker teknologi som e-post og direktemeldinger, bruker de også telefonen for å nå sine ofre. Det oppnår to store fordeler ved å bruke telefon. For det første finnes det færre sikkerhetsteknologier som kan oppdage og stoppe angrepsforsøk over telefon, enn det gjør for f.eks. e-post. For det andre er det enklere for de kriminelle å utrykke følelser over telefon, som igjen øker sannsynligheten for at de vil klare å lure ofrene sine. La oss se nærmere på hvordan vi kan oppdage og stoppe slike angrep.

Hvordan fungerer telefonsvindel?

Først og fremst må du forstå hva disse angriperne er ute etter. Som oftest vil de ha pengene dine, informasjon, eller tilgang til datamaskinen din (eller alle tre). De oppnår dette ved å lure deg til å gjøre som de vil. De kriminelle ringer folk verden rundt, og prøver å lure ofrene til å tro at de er i en situasjon hvor noe haster veldig. De prøver å skremme deg slik at du vil forhaste deg, og gjør en feil uten å innse det. Noen av de vanligste eksemplene inkluderer:

Personen som ringer utgir seg for å være fra et myndighetsorgan, og hevder at du har utestående betalinger som må betales umiddelbart over telefonen, om ikke vil det bli konsekvenser, f.eks. i form av straffeforfølgning. Dette er svindel, myndighetsorganer sender alltid betalingskrav i posten.

Personen som ringer utgir seg for å være fra Microsoft Support, og forsøker å overbevise deg om at PC-en din er infisert med virus. Når de har klart å overbevise deg vil de presse deg til å kjøpe programvare av dem eller gi dem fjerntilgang til datamaskinen. Microsoft vil aldri ringe deg om slikt.

Du får en automatisert talemelding om at bankkontoen din har blitt stengt, og at du må ringe tilbake til et oppgitt nummer for å aktivere den igjen. Når du ringer, møter du på et automatisert system som ber deg bekrefte identiteten din, og stiller deg alle mulige private spørsmål. Dette er ikke banken din, men svindlere som tar opp alt du oppgir og bruker det til identitetstyveri.

Hvordan sikre seg

Det beste forsvaret du har mot angrep og svindel over telefon er deg selv. Husk på disse rådene:

Om noen ringer deg og skaper en sterk følelse av hastverk bør du være veldig på vakt. Det er OK å stoppe opp og si «nei» når det begynner å føles merkelig, selv om alt ved samtalen kanskje virker å være OK til å begynne med.

Om du tror at en telefonoppringning er et angrepsforsøk bør du ganske enkelt legge på. Dersom du ønsker å bekrefte om oppringningen var legitim eller ikke, kan du gå til nettsiden til organisasjonen det gjelder (f.eks. banken din). Der kan du finne telefonnummeret deres og ringe dem opp direkte. Dermed er du trygg på at du faktisk snakker med den aktuelle organisasjonen på ordentlig.

Ikke stol på nummeret som står i displayet, kriminelle kan forfalske nummeret de ringer fra så det ser ut som det tilhører en legitim, norsk organisasjon.

Aldri la en som ringer deg opp ta midlertidig kontroll over PC-en din eller overtale deg til å laste ned programmer. Det kan føre til at PC-en din blir infisert med virus fra de kriminelle.

Om det kommer en oppringning fra noen du ikke personlig har kjennskap til, kan du la oppringningen gå direkte til svareren. På denne måten kan du selv gå over og undersøke ukjente oppringninger når du selv har tid. På mange telefoner kan du også benytte en «ikke forstyr»-funksjon for å gjøre dette automatisk.

Svindel og angrep over telefon er i vekst. Ditt beste forsvar for å oppdage og stoppe det er deg selv.

Norsk Versjon

NorSIS arbeider for at alle skal kunne bruke internett og IKT trygt på jobb og privat. Vi er både samarbeidspartner og pådriver overfor myndigheter og bedrifter. NorSIS er et uavhengig organ som ønsker å gjøre informasjonssikkerhet til en naturlig del av hverdagen.

Gjesteredaktør

Jen Fox *tilbyr tjenester innen sikkerhetsbevissthet, sosial manipulering, og risikoanalyse som senior sikkerhetskonsulent hos All Covered. Du finner Jen på Twitter som* @j_fox.

Ressurser

Microsoft-svindel:	https://nettvett.no/microsoft-svindel/
SMiShing – SMS-svindel:	https://nettvett.no/smishing-sms-svindel/
Sosial manipulering:	https://www.sans.org/u/Fi5