OUCH! | Juli, 2018

SANS SECURITY AWARENESS

OUCH!

Det månedlige nyhedsbrev om IT-sikkerhed

Telefonsvindel

Oversigt

Når du tænker på IT-kriminelle tænker du sandsynligvis på en ond "mastermind", der sidder bag en computer, og lancerer sofistikerede angreb over internettet. Mange af nutidens IT-kriminelle bruger teknologier som e-mail eller instant messaging, men de bruger også telefonopkald til at narre deres ofre. Der er to fordele ved at bruge en telefon. For det første er der i modsætning til e-mail færre sikkerhedsteknologier, der overvåger telefonopkald og kan opdage og stoppe et angreb. For det andet er det meget lettere for de IT-kriminelle at formidle følelser over telefonen, hvilket gør det mere sandsynligt, at de kan narre deres ofre. Lad os lære dig at se og stoppe disse angreb.

Hvordan virker et angreb over telefonen?

For det første skal du forstå, hvad disse it-kriminelle er efter. De vil normalt have dine penge, oplysninger eller adgang til din computer (eller alle tre). De gør det ved at narre dig til at gøre, hvad de vil have. De ringer rundt til folk i hele verden og fortæller om situationer, der lyder til at være meget presserende. De ønsker at skræmme dig så de kan få dig ud af balance og dermed ikke kan tænke klart. Herefter skynder de på dig og får dig til at lave fejl. Nogle af de mest almindelige eksempler er:

Opkalderen udgiver sig for at være fra SKAT, og fortæller at du har ubetalte skatter. De forklarer, at hvis du ikke betaler dine skatter med det samme, vil du komme i fængsel og herefter presser de dig til at betale dine restskatter med dit kreditkort over telefonen. Dette er et fupnummer!

Opkalderen lader som om, at han er Microsoft Tech Support, og forklarer, at din computer er inficeret. Når du er overbevist om, at du er smittet, presser de dig til at købe deres software eller til give dem fjernadgang til din computer. Microsoft ringer aldrig hjem til dig.

Du får en automatiseret telefonopkald om, at din bankkonto er blevet annulleret, og at du skal ringe et nummer tilbage for at genaktivere det. Når du ringer, får du fat i et automatiseret system, der beder dig om at bekræfte din identitet og beder dig om alle slags private oplysninger. Dette er i virkeligheden ikke din bank, men svindlere der registrerer alle dine oplysninger for at bruge dem til identitetssvindel.

Sådan beskytter dig selv

Det bedste forsvar du har, er dig selv. Vær opmærksom på disse ting.

Når der er en, der ringer til dig og skaber en enorm følelse af uopsættelighed og du presses til at gøre noget, være ekstremt mistænkelig. Telefonsamtalen kan virke OK i starten, men senere føles underligt. Det er OK at stoppe og sige "nej".

Hvis du mener, at et telefonopkald er et angreb, skal du lægge på. Hvis du vil bekræfte, om telefonopkaldet var legitimt, skal du gå til organisationens hjemmeside (f.eks. din bank) og få kundesupportens telefonnummer og ringe direkte til dem. På den måde sikrer du, at du taler med den virkelige organisation.

Hav ikke tillid til "Vis Nummer", svindlerne vil ofte forfalske telefonnummeret, så det ser ud til, at det kommer fra en rigtig organisation eller har samme hovednummer, som din arbejdsplads.

Giv aldrig opkalderen midlertidig kontrol over din computer og lad dig ikke narre til at downloade software. Det er sådan, svindlere kan inficere din computer.

Hvis et telefonopkald kommer fra en person, du ikke kender personligt, skal du lade opkaldet gå til din voicemail. På denne måde kan du gennemgå ukendte opkald stille og roligt. På mange telefoner kan du aktivere dette som standard med funktionen "Forstyr ikke".

Svindel og angreb over telefonen er stigende. Du er det bedste forsvar, som du har til at opdage og stoppe dem.

WelcomeSecurity samarbejder med netop din virksomhed om at identificere de IT sikkerhedsmæssige risici, som truer din virksomhed. Ved at analysere og teste jeres processer, teknologi og ikke mindst jeres medarbejder vil vi fastslå de mest effektive måder at minimere disse risici. Du kan finde os på https://www.welcomesecurity.net.

Gæsteredaktør

Jen Fox *er senior sikkerhedskonsulent ved "All Covered" og arbejder med sikkerhedsbevidsthedstræning, social engineering og risikovurdering. Find Jen på Twitter som @j_fox.*

Hvis du vil vide mere

"Consumer Information about Identity, Privacy, & Online Security":
https://www.consumer.ftc.gov/topics/privacy-identity-online-security
"Report a Phone Scam" (in the US): https://www.ftccomplaintassistant.gov/#crnt
Social Engineering: https://www.sans.org/u/Fi5