Ditt månedlige nyhetsbrev om sikkerhetsbevissthet

Persontilpasset svindel

Oversikt

Cyberkriminelle kommer hele tiden på nye og kreative metoder for å lure folk. En ny form for svindel øker i popularitet – persontilpasset svindel. Cyberkriminelle finner eller kjøper informasjon om millioner av mennesker, for så å bruke informasjonen til å tilpasse angrepene etter personene de angriper. Under vil vi forklare hvordan slik svindel fungerer og gå gjennom noen eksempler. Jo mer du vet om slik svindel, jo enklere vil det være å oppdage og stoppe det.

Hvordan fungerer det?

Svindel over telefon og e-post er ikke noe nytt, cyberkriminelle har forsøkt å lure folk på denne måten i årevis. Noen kjente eksempler er «Du har vunnet i lotto» eller e-poster fra "nigerianske prinser". Men i tradisjonelle svindelforsøk som dette vet ikke de kriminelle hvem målet er. De lager bare en generell melding som de sender ut til millioner av mennesker. Og fordi disse svindelforsøkene er så generelle er de som oftest også enkle å oppdage. En persontilpasset svindel er annerledes, da gjør de kriminelle undersøkelser i forkant, og skreddersyr en melding for hver person de forsøker å svindle. De gjør dette ved å finne eller kjøpe databaser som inneholder navn, passord, telefonnummer og andre personlige detaljer. Slik informasjon er enkelt tilgjengelig fordi mange nettsider har blitt hacket, og databaser har blitt lekket. Mye er også lett tilgjengelig gjennom sosiale medier, eller i offentlige registre. De kriminelle kan så rette svindelforsøk mot alle de har informasjon om.

Vanlige knep som cyberkriminelle bruker for å lure deg til å betale dem, er frykt og utpressing. Et sånt angrep kan fungere slik: De finner eller kjøper informasjon om innlogginger og passord fra hackede nettsider. I en slik database finner de din e-postadresse og ditt passord, og sender deg en e-post (og gjør det samme med alle andre som var i databasen) med personlige detaljer om deg, inkludert passordet du brukte på den hackede nettsiden. De kriminelle hevder at passordet er "bevis" på at de har hacket PC-en eller mobilen din, som jo bare er løgn. De hevder også at mens de hacket PC-en din tok de deg også på fersken i å se på porno. De skriver så at dersom du ikke betaler utpressingssummen vil de dele bevis på denne aktiviteten med venner og familie.

Men i så å si ingen av disse tilfellene har du faktisk blitt hacket. De skriver ikke engang noe om hvem du er eller om hvilke nettsider du har besøkt. Svindlerne prøver ganske enkelt å bruke de få personlige detaljene de har om deg til å skremme deg og lure deg

til å tro at de har hacket PC-en eller mobilen din, og lure deg til å betale dem penger. Husk at skurker kan bruke disse samme teknikkene i telefonsvindel også.

Hva bør jeg gjøre?

Gjenkjenn e-poster og telefonoppringninger som dette som svindel. Det er naturlig å bli litt redd når noen har slik personlig informasjon om deg. Men husk at vedkommende lyver. Meldingen du får er en del av en automatisert, masseutsendt kampanje, ikke et målrettet forsøk på å ta deg. Det blir stadig lettere for cyberkriminelle å finne eller kjøpe slik informasjon, så forvent mer persontilpasset svindel i fremtiden. Noen tegn å se etter:

- **Når du mottar en e-post, melding eller telefonoppringning som skaper sterkt inntrykk av hastverk og dårlig tid bør du være veldig på vakt. Dersom det spilles på følelser som frykt og hastverk prøver de nok å få deg til å forhaste deg og gjøre en feil.**
- **Dersom noen krever betaling i form av kryptovaluta (som BitCoin), gavekort, eller andre betalingsformer som er vanskelig å spore er det et varseltegn.**
- **Dersom du får en e-post som virker mistenkelig kan du søke på Google for å se om noen har meldt fra om noe lignende.**

Til syvende og sist er det sunn fornuft som er ditt beste forsvar. Men vi anbefaler også at du bruker et unikt, langt passord for hver brukerkonto på nett. Dersom du ikke kan huske alle passordene dine kan du skrive dem ned på et trygt sted eller bruke et program som et passordhvelv. I tillegg bør du skru på totrinnsbekreftelse overalt hvor det er mulig.

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

Lenny Zeltser *er en cybersikkerhetsveteran. Han lager antivirusprodukter for Minerva Labs og underviser i sikkerhet ved SANS Institute. Han har også erfaring med ledelse av sikkerhetsløsninger og som konsulent. Følg ham på* zeltser.com/blog*, og på Twitter:* @lennyzeltser*.*

Ressurser

Sosial manipulering:	https://www.sans.org/u/MUU
Stop fiskingen:	https://www.sans.org/u/MUZ
Søk etter deg selv på nettet:	https://www.sans.org/u/MV4
Passordhvelv:	https://www.sans.org/u/MV9