Slik avslører du en phishing e-post

10 ting du må se etter

Med et økende antall svindelforsøk initiert via e-post er det avgjørende å ta i bruk proaktive tiltak for å beskytte deg og din organisasjon. Det å være årvåken og oppmerksom nok til å oppdage phishing e-poster er et viktig steg i det å beskytte deg og dine verdier. A lære ansatte i din organisasjon til også a være oppmerksomme på faren er god investering i sikkerhet.

Her er en hurtigguide til hvordan du oppdager og håndterer phishing e-poster.

1. Ikke stol på avsendernavnet som vises

Bare fordi den ser ut til å komme fra et navn til en person du kjenner eller stoler på, betyr det ikke at dette er tilfelle. Vær helt sikker ved å dobbelt-sjekke avsenderadressen.

2. Se, men ikke klikk

Før musepekeren over ulike deler av e-posten uten å klikke. Hvis lenker i teksten ser rare ut, eller ikke henger sammen med hva e-posten handler om, ikke klikk på de! Rapporter e-posten som mistenkelig.

3. Se etter stavefeil

Angriperne bryr seg ofte mindre om rettskriving enn en normal avsender ville gjort.

4. Vurder benevningen

Er adresseringen generell eller vag? Eller er benevningen f.eks.: «Kjære kunde» eller «Kjære direktør»? Eller står det enkelt og greit «Hei, Ola Nordmann». Vurder benevningen etter hva som burde passe med hver enkelt e-post, om den er uformell eller formell.

5. Blir det spurt etter personlig informasjon?

Legitime selskaper vil ikke spørre etter personlig informasjon via en e-post.

6. Se opp for hastverk

Disse falske e-postene kan kanskje få det til å høres ut som om det er en form for krise. At direktøren ber deg gjennomføre en stor penge-overføring som haster. Stopp en halv! Sjekk alltid med avsender før slike transaksjoner gjennomføres.

7. Sjekk e-post signaturen

De aller fleste legitime avsendere vil inkludere en signaturblokk nederst i e-posten.

8. Se opp for vedlegg

Svindlerne liker å lure deg med falske vedlegg. Vedlegget kan se ekte ut ved første øyekast. Visuelt kan det se ut som et Excel- eller Word-dokument, men kan være noe helt annet. Vær sikker på at vedlegget er ekte og ikke inneholder ondsinnet kode før du klikker på det. Unngå filer som tyder på at det er kjørbare programmer eller scriptfiler (.exe, .msi, .ser, .vbs, .js, .bat bl.a.)

9. I tvil? Kontakt selskapet

Hvis du syns noe ser unormalt ut, husk: Det er bedre å være føre var enn etter snar… Mener du noe ikke stemmer og er du usikker på om e-posten du har mottatt er ekte, spør avsender.

10. Vær skeptisk

Falske e-poster har blitt utrolig sofistikerte. Selv om en e-post har bedriftens logo, korrekt språk og en tilsynelatende gyldig e-postavsender, betyr ikke dette at den er ekte. Vær skeptisk, og dersom du synes en e-post virker mistenkelig, ikke åpne den.

Smart Sikkerhet