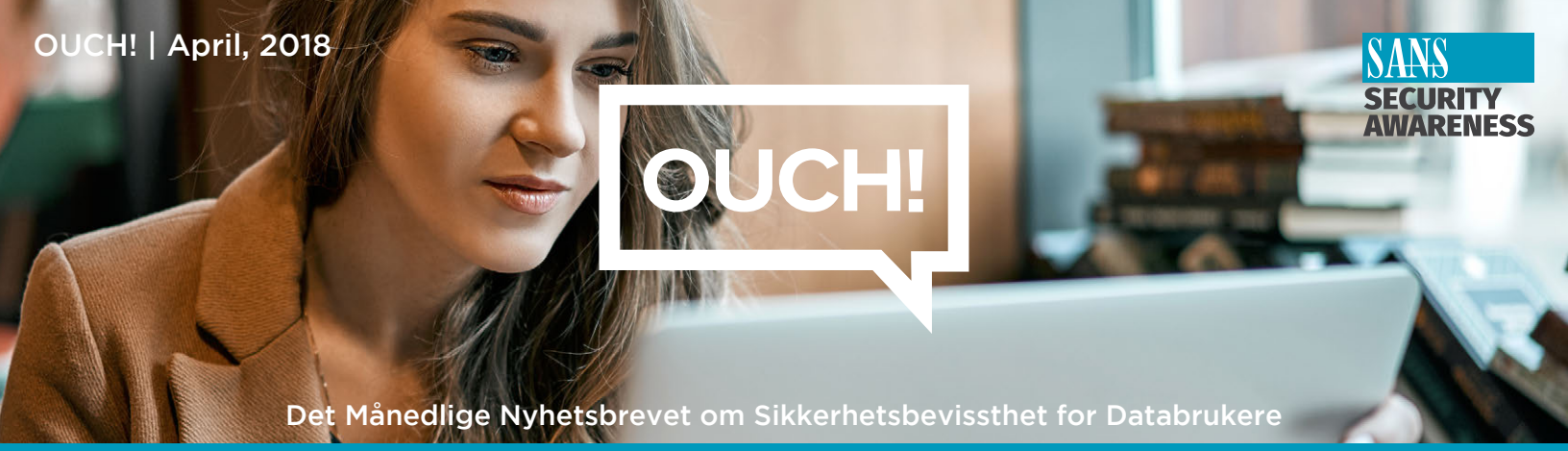

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

Stop fiskingen

Oversikt

E-post og meldingstjenester (som Skype, Twitter og Snapchat) er blant hovedmåtene vi kommuniserer på. Vi bruker slike teknologier daglig på jobben, men også for å holde kontakt med familie og venner. Siden så mange mennesker bruker og er avhengig av disse teknologiene, har de blitt en av de viktigste angrepsplattformene brukt av cyberkriminelle, en angrepsmetode kalt phishing. Lær hva phishing er, og hvordan slike angrep kan avsløres og stoppes, uavhengig av om du er på jobb eller hjemme.

Hva er phishing/nettfisking

Phishing (ofte kalt nettfisking på norsk) er en type angrep som bruker e-post eller andre meldingstjenester for å lure deg til å gjøre en bestemt handling som du ikke burde gjøre, som å klikke på en skadelig lenke, gi fra deg passordet ditt, eller åpne et infisert vedlegg. Angripere jobber hardt med å gjøre meldingene overbevisende, og med å spille på følelsene dine, som hast og nysgjerrighet. De kan få meldingene til å se ut som de kommer fra noen eller noe du er kjent med, som en venn eller en pålitelig bedrift du har erfaring med. Eller kanskje de til og med bruker logoen til banken din, eller forfalsker avsenderadressen så meldingen virker mer ekte. Angriperne sender så disse meldingene til millioner av mennesker. De vet ikke hvem som vil bite på, alt de vet er at jo flere de sender ut, jo flere vil bli rammet.

Hvordan beskytte seg

I nesten alle tilfeller er det å bare åpne og lese en e-post eller en melding helt i orden. For at et phishingangrep skal fungere, må bakmennene lykkes i å lure deg til å gjøre noe. Heldigvis finnes det avslørende spor på at en melding kan være et slikt angrep, her er de vanligste:

- En sterk følelse av hastverk, det kreves «umiddelbar handling» før noe negativt skjer, som at kontoen din blir stengt eller du havner i fengsel. Dette er tomme trusler, angriperne forsøker å stresse deg til å gjøre en feil uten at du tar deg tid til å tenke deg om.
- Legge press på deg til å omgå rutiner og prosedyrer på arbeidsplassen din.
- Forsøk på å pirre nysgjerrigheten din veldig, eller at noe er for godt til å være sant (nei, du har ikke vunnet i lotto).
- En generisk hilsen som «Kjære kunde». De fleste firmaer eller venner som kontakter deg vet hva du heter.

- Det bes om svært sensitiv informasjon, som kortnummer på bank- eller kredittkort, eller passord, eller annen informasjon som den legitime avsenderen allerede burde vite, eller ikke har behov for å be om.
- Meldingen hevder å være fra en offisiell organisasjon, men har dårlig grammatikk eller feilstavinger, eller er sendt fra en personlig e-postadresse som @gmail.com.
- Meldingen kommer fra en offisiell e-postadresse (som f.eks. sjefen din) men har en Svar-Til-adresse som går til en annens personlige e-post.
- Du får en melding fra en du kjenner, men tonen og ordleggingen virker ulikt ham eller henne. Om du blir mistenksom kan du ringe avsenderen for å få bekreftet at vedkommende faktisk sendte den. Det er enkelt for cyberkriminelle å lage en melding som virker som den kommer fra venn eller en kollega.

Til syvende og sist er sunn fornuft ditt beste forsvar. Om en e-post eller melding virker merkelig, mistenkelig, eller for god til å være sann, så kan det være et phishingangrep.

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

Jessica Barker er verdensledende i menneskesentrert cybersikkerhet. Hun er medgrunnlegger av Redacted Firm, hvor hun gir konsulenttjenester til klienter over hele verden, og hun er en velkjent foredragsholder. Følg henne på Twitter på @drjessicabarker.

Ressurser

Sosial manipulering:	https://www.sans.org/u/Cb1
Å hjelpe andre med å sikre seg selv:	https://www.sans.org/u/Cb6
E-postregler:	https://www.sans.org/u/Cbg
Direktørsvindel:	https://www.sans.org/u/Cbl
OUCH! oversettelser og arkiver:	https://www.sans.org/u/Cbq

Tillatelse

 Redaksjon: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Oversatt av: NorSIS