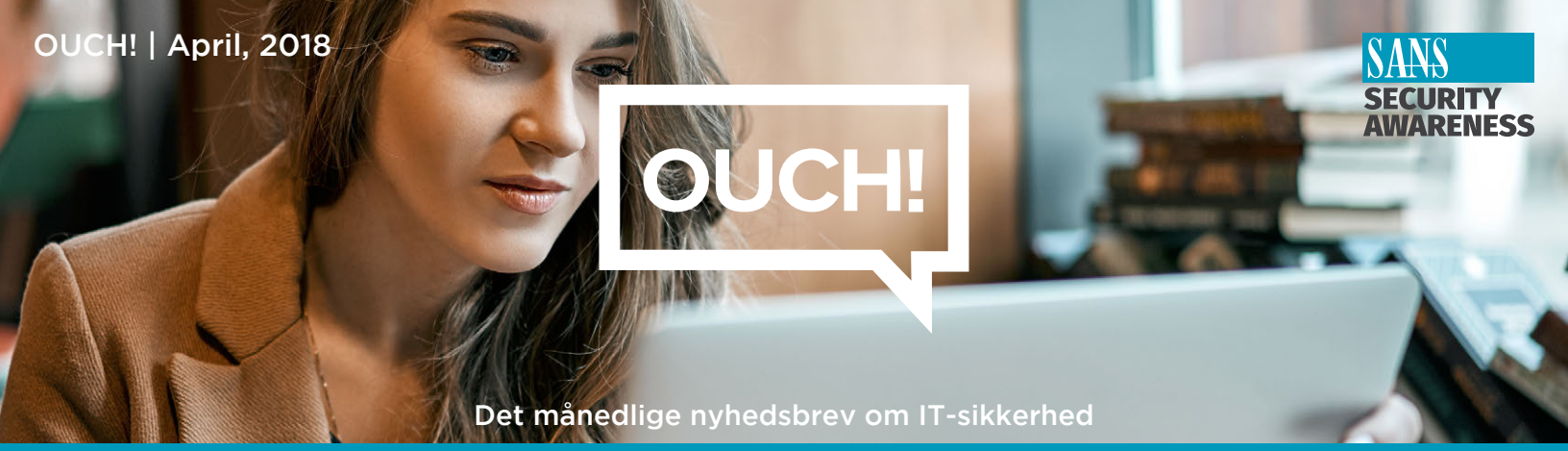

SANS SECURITY AWARENESS

OUCH!

Det månedlige nyhedsbrev om IT-sikkerhed

Stop den "Phish"

Oversigt

E-mail og messaging-tjenester (såsom Skype, Twitter eller Snapchat) er de primære måder, vi kommunikerer på. Vi bruger ikke kun disse teknologier hver dag til arbejde, men også til at holde kontakten med venner og familie. Da så mange mennesker rundt omkring i verden er afhængige af disse teknologier, er de blevet en af de primære mål for IT-kriminelle. De benytter sig af en metode der kaldes phishing. Lær, hvad phishing er, og hvordan du kan få øje på og stoppe disse angreb, uanset om du er på arbejde eller hjemme.

Hvad er phishing?

Phishing er en type angreb, der bruger e-mail eller en besked-systemer til at narre dig til at gøre noget, du ikke bør gøre, såsom at klikke på et ondsindet link, dele dit kodeord eller åbne en inficeret vedhæftning fra en e-mail. De IT-kriminelle arbejder hårdt for at gøre disse meddelelser overbevisende og tager udgangspunkt i følelsesmæssige udløsere, såsom at det haster eller spiller på din nysgerrighed. De kan få dem til at se ud som om de stammer fra nogen eller noget du kender, såsom en ven eller en virksomhed som du ofte bruger. Måske tilføjer de endda logoet fra din bank eller forfalsker e-mailadressen, så meddelelsen ser mere legitim ud. IT-kriminelle sender så disse beskeder til millioner af mennesker. De ved ikke, hvem der hopper på den, alt hvad de ved er, jo flere de sender, desto flere mennesker vil blive snydt.

Beskyt dig selv

I næsten alle tilfælde er åbning og læsning af en mail eller besked fint. For at et phishing-angreb skal virker, skal de kriminelle få dig til at gøre noget. Heldigvis er der spor på, at en besked er et angreb, her er de mest almindelige:

- En enorm følelse af hastværk, at det kræver "øjeblikkelig handling" ellers vil noget dårligt ske, som at true med at lukke en konto eller sende dig til fængsel. Den IT-kriminelle ønsker at du skynder dig og derfor gør en fejltagelse.
- At presse dig til at omgå eller ignorere politikker eller procedurer på arbejdspladsen.
- En stor følelse af nysgerrighed eller at det er for godt til at være sandt (nej, du vandt ikke lotteriet).
- En generel hilsen som "Kære kunde". De fleste virksomheder eller venner, der kontakter dig, kender dit navn

- Anmodning om meget følsomme oplysninger, f.eks. dit kreditkortnummer eller kodeord eller andre oplysninger, som den legitime afsender allerede bør vide.
- Meddelelsen siger, at den kommer fra en officiel organisation, men har dårlig grammatik, stavning eller bruger en personlig e-mail-adresse så som @ gmail.com.
- Beskeden kommer fra en officiel e-mail (f.eks. din chef), men har en svar-til-adresse, der går til en persons personlige e-mail-konto.
- Du modtager en besked fra en person, du kender, men tonen eller ordlyden lyder bare ikke som ham eller hende. Hvis du er mistænkelig, skal du ringe til afsenderen for at kontrollere, at de har sendt den. Det er nemt for en IT-kriminel at oprette en besked, der ser ud til at være fra en ven eller kollega.

I sidste ende er sund fornuft dit bedste forsvar. Hvis en e-mail eller en meddelelse virker underlig, mistænkelig eller for god til at være sand, kan det være et phishing-angreb.

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

Tonia Dudley har udviklet og kørt Security Awareness (sikkerhedsbevidstheds) programmer siden 2011, som omfatter opbygning af et prisvindende phishing-uddannelsesprogram. Du kan finde hende på www.linkedin.com/in/toniadudley.

Ressourcer

Social Engineering (oversat til dansk):	https://www.sans.org/u/Cb1
Helping Others Secure Themselves (oversat til dansk):	https://www.sans.org/u/Cb6
Email Do's and Don'ts (oversat til dansk):	https://www.sans.org/u/Cbg
CEO Fraud (oversat til dansk):	https://www.sans.org/u/Cbl
OUCH! Translations and Archives:	https://www.sans.org/u/Cbq

Licensinformation