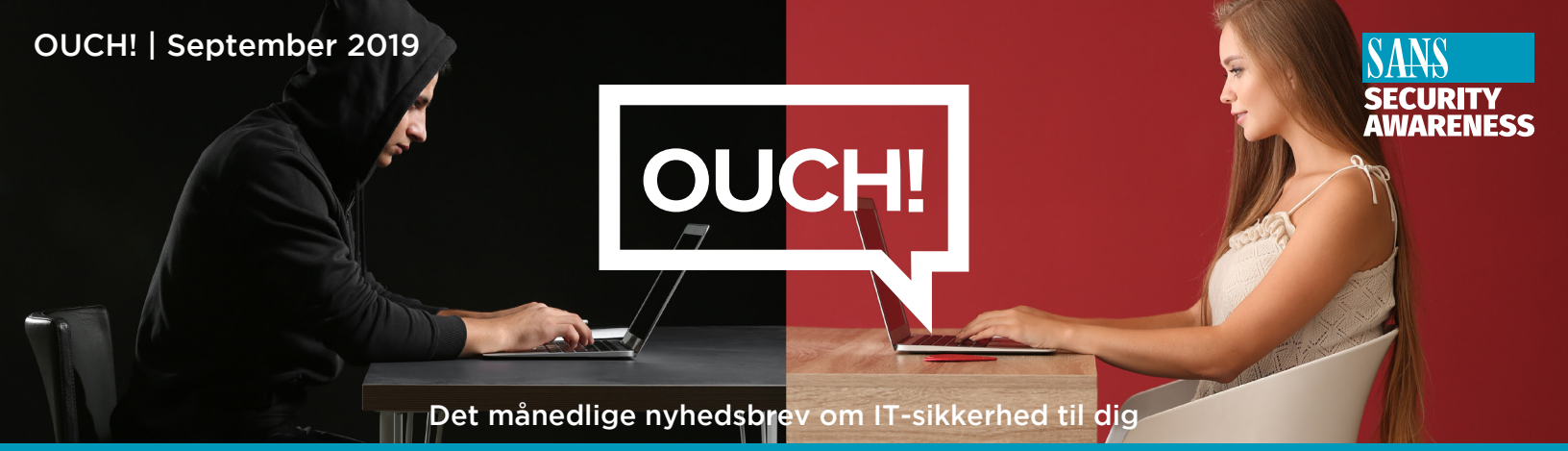
OUCH! | September 2019



Bedrag gennem sociale medier

Oversigt

Mange af os har modtaget phishing e-mail, enten på arbejdet eller hjemme. Dette er e-mails, der ser legitime ud, f.eks. fra din bank, din chef eller din foretrukne online butik. Men dette er i virkeligheden et angreb, der forsøger at narre dig til at gøre noget, du ikke bør tage, såsom at åbne en inficeret e-mail, dele din adgangskode eller overføre penge. Udfordringen er, jo bedre vi bliver til at gennemskue og stoppe disse e-mail-angreb, jo flere IT-kriminelle prøver andre metoder til at komme i kontakt med dig og svindle dig.

Forsøg på at snyde dig kan ske over næsten enhver form for kommunikation, du bruger, fra Skype, WhatsApp og Slack til Twitter, Facebook, Snapchat, Instagram eller endda gaming-apps. Kommunikation over disse platforme eller kanaler kan føles mere uformel og troværdig, og det er netop derfor, at angribere bruger dem til at narre andre. Derudover er det med nutidens teknologier blevet meget lettere for enhver svindler at foregive at være den organisation eller person, de ønsker. Det er vigtigt at huske, at enhver kommunikation, du deltager i, muligvis ikke er hvad det ser ud til at være, og at folk ikke altid er dem som de udgiver sig for at være.

Key takeaways

Her er de mest almindelige spor på, at den meddelelse, du lige har modtaget, eller det indlæg, du lige har læst, kan være et angreb.

Hast: En meddelelse, der har en følelse af hast, der kræver "øjeblikkelig handling", før der sker noget dårligt, som at true med at lukke en konto eller sende dig i fængsel. Angriberen forsøger at få dig til at vil skynde dig så du begår en fejl.

Påvirkelighed: Ved at presse dig til at omgå eller ignorere politikker eller procedurer på arbejdet.

Nysgerrighed: En stærk følelse af nysgerrighed eller noget, der er for godt til at være sandt. Nej, du vandt ikke lotteriet.

Følsomhed: En anmodning om meget følsomme oplysninger, f.eks. dit kreditkortnummer eller adgangskode, eller oplysninger, som du ikke har det godt med at dele.

Officielle meddelelser: Meddelelsen siger, at den kommer fra en officiel organisation, men har dårlig grammatik eller stavefejl. De fleste regeringsorganisationer vil ikke bruge sociale medier til officiel kommunikation direkte med dig. Hvis du ikke er sikker på, om meddelelsen er legitim, skal du ringe til organisationen, men finde deres telefonnummer et andet sted end i beskeden, f.eks. fra deres hjemmeside.

Efterligning: Du modtager en besked fra en ven eller en medarbejder, men tonen eller ordlyden er anderledes end den plejer at være. Hvis du er mistænksom, skal du ringe til afsenderen for at kontrollere, at de har sendt beskeden. Det er let for en IT-kriminel at oprette beskeder, der ser ud til at være fra nogen, du kender. I nogle tilfælde kan de overtage en af din venners konto og derefter foregive at være din ven og nå ud til dig. Vær særlig opmærksom på tekstbeskeder, Twitter og andre formater der indeholder korte meddelelser, som er vanskeligere at få en fornemmelse af afsenderens personlighed

Du er det bedste forsvar mod svindel og angreb som disse. Hvis et indlæg eller en meddelelse virker underlig eller mistænksom, skal du blot ignorere eller slette den, eller hvis det er fra en person, du personligt kender, skal du ringe til personen for at bekræfte, om de virkelig sendte det.

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

Dr Jessica Barker *(@drjessicabarker) er førende inden for den menneskelige side af IT-sikkerhed. Hun er co-CEO for Cygenta, hvor hun følger sin passion for positivt at påvirke opmærksomhed omkring IT-sikkerhed, adfærd og kultur rundt omkring i verden. Hun er formand for ClubCISO og en populær keynote speaker.*

Hvis du vil vide mere

Social Engineering:	https://www.sans.org/u/Uz6
Phone Call Scams:	https://www.sans.org/u/Uzb
Stop That Phish:	https://www.sans.org/u/Uzg
Personalized Scams:	https://www.sans.org/u/Uzl