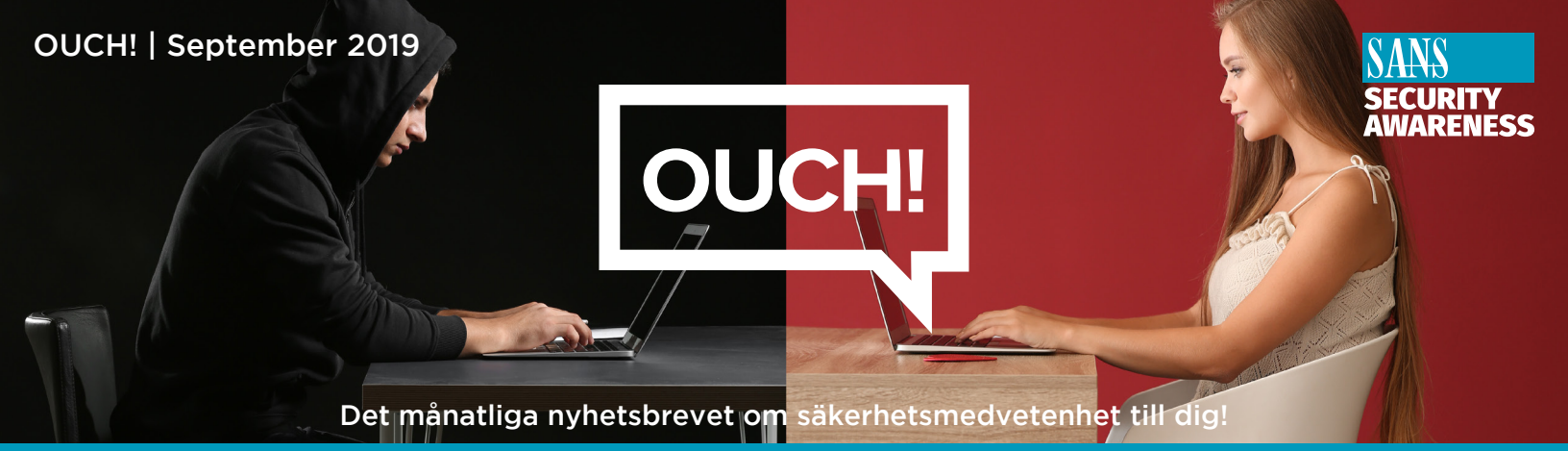
OUCH! | September 2019



Det månatliga nyhetsbrevet om säkerhetsmedvetenhet till dig!

Du kan bli lurad i sociala medier

Översikt

Många har drabbats av en nätfiskeattack via e-post på jobbet eller hemma. Dessa e-postmeddelanden verkar legitima och kan se ut att vara skickade från din bank, din chef eller din favorit online-butik. De är riktiga attacker som försöker stressa eller lura dig till att utföra en handling du inte ska göra, t.ex. öppna en infekterad e-postbilaga eller dela ditt lösenord eller överföra pengar. Utmaningen är att desto mer kunniga vi blir på att upptäcka och stoppa dessa e-postattacker desto mer kommer cyberbrottslingarna att försöka andra metoder för att kontakta och lura människor.

Försök att lura eller bedra dig kan ske över nästa alla typer av kommunikation som du använder; Skype, WhatsApp och Slack till Twitter, Facebook, Snapchat, Instagram eller spelappar. Kommunikation över dessa plattformar och kanaler kan upplevas mer informell eller pålitlig och det är just därför som angriparna använder dem för att lura andra. Dessutom har det med dagens teknik blivit mycket lättare för angripare att vara något eller någon de vill. Det är viktigt att komma ihåg att all kommunikation inte är som den verkar vara och att människor inte alltid är de som de utger sig för att vara.

Viktiga slutsatser

Här är de vanligaste ledtrådarna för att meddelandet du precis fått eller inlägget du precis läst kan vara en attack.

Brådskande: Ett meddelande som har en känsla av att vara brådskande och som kräver "omedelbar handling" innan något dåligt händer; som hot att stänga ett konto eller att du hamnar i fängelse. Angriparen vill stressa dig till att göra ett misstag.

Påtryckning: Pressa dig att kringgå eller ignorera policyer eller rutiner på jobbet.

Nyfikenhet: En stark känsla av nyfikenhet eller något som är för bra för att vara sant. Nej, du vann inte lotteriet.

Känslig: En begäran om mycket känslig information som ditt kreditkortsnummer eller lösenord eller någon annan information som du inte är bekväm att dela.

Officiella meddelanden: Meddelandet säger att det kommer från en officiell organisation, men det har dålig grammatik eller stavning. De flesta statliga organisationer använder inte sociala medier för att kommunicera direkt till dig. Ring tillbaka till organisationen om du är osäker om meddelandet är legitimt, men använd ett tillförlitligt telefonnummer som till exempel finns på deras webbsida.

Imitation: Du får ett meddelande från en vän eller en medarbetare men tonen eller formuleringen låter inte som dem. Om du är osäker kan du ringa avsändaren för att kontrollera om de skickade meddelandet. Det är enkelt för en angripare att skapa meddelanden som ser ut att komma från någon du känner. I vissa fall kan de ta över ett av din väns konto för att sedan lura dig genom att låtsas att de är din vän. Var extra uppmärksam på sms, Twitter och andra former av korta meddelanden där det är svårare att få en känsla av avsändarens personlighet.

Du är själv det bästa försvaret mot bedrägerier, lurendrejeri och liknande attacker. Om ett inlägg eller ett meddelande verkar udda eller misstänkt ska du ignorera eller ta bort det. Om det kommer från någon du känner ringer du hen för att kontrollera att de verkligen skickade meddelandet.

Visolit är nordens ledande specialist på molntjänster. Visolit har för närvarande Europas största och mest moderna driftsplattform för SMB-marknaden. Vi levererar allt från komplett IT-drift till enklare IT-tjänster som anpassas och integreras utifrån kundens existerande behov och infrastruktur. Med våra tjänster får små och medelstora företag tillgång till IT med en kvalitet och säkerhet som normalt är undantaget stora internationella företag. www.visolit.se eller följ oss på LinkedIn https://www.linkedin.com/company/visolit

Gästredaktör

Dr Jessica Barker *(@drjessicabarker) är ledande inom den mänskliga sidan av cybersäkerhet. Hon är co-CEO of Cygenta, där hon följer sin passion att öka medvetenheten om cybersäkerhet genom positiv påverkan, beteende och kultur runt om i världen. Hon är ordförande för ClubCISO och är en populär föreläsare.*

Referenser

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

Visolit