Det månedlige nyhedsbrev om IT-sikkerhed

E-mail brølere og hvordan du undgår dem

Oversigt

E-mail er stadig en af de primære måder, vi kommunikerer på, både i vores personlige og professionelle liv. Men, vi er ofte vores egen værste fjende når vi bruger e-mail. Her er de fire mest almindelige fejl, folk laver når de sender en e-mail og hvordan man kan undgå dem.

”Auto-Complete”

De fleste e-mailklienter har en ”Auto-Complete” funktion. Når du skriver navnet på den person, du vil sende en e-mail til, vælger din e-mailklient automatisk deres e-mailadresse for dig. På denne måde behøver du ikke at huske e-mailadressen på alle dine kontakter, du skal bare huske deres navne. Problemet opstår, når du har kontakter, der har lignende navne. Så er det meget nemt at komme til at vælge den forkerte e-mailadresse når du bruger ”auto-complete”. For eksempel, hvis du vil sende en meget følsom e-mail til Hanne Kristiansen, din kollega i regnskabsføring, men i stedet for kommer du til at vælge e-mailadressen til Hanne Kristensen, dit barns fodboldtræner. Konsekvensen er, at du ender med at sende følsom oplysninger en person, du næsten ikke kender. For at beskytte dig selv skal du altid dobbelttjekke navn og e-mailadresse når du sender følsomme oplysninger, før du klikker på send.

”Svar alle” eller ”Reply-All”

Udover “Til” (engelsk ”To”), når du opretter en e-mail, har du også “CC”. “CC” står for “Carbon Copy”, som giver dig mulighed for at sende kopier til flere personer og holde dem informeret. Når en anden sender dig en e-mail og har CC’et folk på e-mailen, skal du beslutte, om du kun vil svare afsenderen, eller om du også vil sende svar til alle, der er inkluderet i e-mailen. Hvis dit svar er følsomt, vil du højst sandsynligt kun sende svar til afsenderen. Vær dog forsigtig, når du vælger “Svar” (engelsk ”Reply”). Det er meget nemt at komme til at ramme ”Svar Alle” (engelsk “Reply-All”), hvilket betyder at du sender svar til alle i e-mailen. Endnu en gang, når du sender eller svarer på en følsom e-mail, skal du altid kontrollere, hvem du sender e-mailen til, før du trykker send.

Følelser

Send aldrig en e-mail, når du er følelsesmæssigt i ubalance. Du risikerer at e-mailen kan skade dig i fremtiden, måske endda koste dig et venskab eller et job. I stedet, skal du tage en dyb indånding, få ro på og organisere dine tanker. Hvis du stadig har brug for at komme af med din frustration, skal du åbne en ny e-mail (sørg for, at der ikke er noget navn eller e-mailadresse i feltet "TIL"). Her kan du skrive nøjagtigt, hvad du har lyst til at skrive. Rejs dig op og gå væk fra din computer, måske kan du lave en god kop kaffe eller gå en tur. Når du kommer tilbage, skal du slette beskeden og starte forfra. Eller bedre endnu tag din telefon og tal med personen, eller tag en snak ansigt til ansigt hvis det er muligt. Det kan være svært for folk at fange tonen og hensigten med en e-mail, så din besked lyder måske bedre i telefonen eller ansigt til ansigt. Husk at humor (især tør humor) ikke altid opfattes i e-mails og modtageren forstår muligvis ikke din besked. Specielt, hvis modtageren er fra en anden kultur eller I ikke taler samme sprog.

Privatliv

Endelig er dit privatliv dårligt beskyttet i e-mail. Din e-mail kan læses af enhver, der får adgang til den, som et postkort sendt med posten. Din e-mail kan nemt videresendes til andre, offentliggøres på offentlige fora, offentliggøres på grund af en retsorden eller den kan blive distribueret fordi en server er blevet hacket. Hvis du har noget virkelig privat at sige til nogen, skal du tage din telefonen og ringe til personen. Det er også vigtigt at huske, at e-mail i mange lande kan bruges som bevis i en domstol. Endelig skal du huske, at din arbejdsgiver kan have ret til at overvåge og måske endda læse din e-mail, hvis du bruger din arbejdscomputer til at sende e-mail.

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

Keith Palmgren *er sikkerhedsekspert med over 30 års erfaring i sikkerhedsbranchen. Han er administrerende direktør for NetIP, Inc. og forfatteren til fem-dages kurset "SANS SEC301 - Introduktion til Cyber Security". https://sans.org/sec301.*

Hvis du vil vide mere

Stop That Phish: https://www.sans.org/u/IJj

Social Engineering: https://www.sans.org/u/IJo

Manage Your Email's Auto-complete lists:

Windows Mac