

OUCH!

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

E-posttabber, og hvordan de kan unngås

Oversikt

E-post er fortsatt en av de mest brukte kommunikasjonskanalene, både i privat sammenheng og i yrkeslivet. Men veldig ofte kan vi være vår egen verste fiende når vi bruker e-post. Her er de fire vanligste feilene folk gjør når de sender epost, og hvordan de kan unngås.

Autofullfør

Autofullfør er en vanlig funksjonalitet som finnes i de fleste e-postklienter. Mottakerens e-postadresse blir automatisk valgt ut og fylt inn av e-postprogramvaren når du begynner å skrive navnet deres. Dermed trenger du ikke å huske e-postadressen til alle kontaktene dine, bare navnene. Problemet med autofullfør er at når du har flere kontakter med lignende navn, skal det ikke mye til at feil e-postadresse blir fylt inn av autofullfør. Du planlegger for eksempel å sende e-post med sensitiv informasjon til «Kari Nordmann», din kollega i regnskap. Istedenfor velger autofullfør e-postadressen til ditt barns fotballtrener, «Karen Nordal». Resultatet blir at du har sendt en e-post med sensitiv jobbinformasjon til en uautorisert person. For å beskytte deg mot dette, er det viktig å dobbeltsjekke navn og e-postadresse før man trykker send.

Svar alle

I tillegg til «Til:» feltet, har de fleste epostklienter også alternativet «CC:» for å velge mottaker av eposten. «CC» står for «Carbon Copy», eller blåkopi på norsk. Det vil si at folk mottar kopier og blir holdt informert. Når noen sender deg en e-post og har lagt til andre mottakere som CC, må du avgjøre om du vil svare til bare avsenderen, eller til alle som var inkludert som CC. Dersom svaret ditt er sensitivt, vil du kanskje svare kun til avsender. Husk å være forsiktig når du velger «svar», det er fort gjort å trykke feil og velge «svar alle». Hvis du trykker «svar alle» blir svaret ditt sendt til alle som er inkludert i e-posed. Når du sender sensitiv informasjon over epost må du alltid dobbeltsjekke hvem du sender til før du trykker send.

Følelser

Aldri send e-post når du er påvirket av sterke følelser. Om du gjør det, kan e-posten komme til å forårsake deg skade i fremtiden, kanskje til og med koste deg et vennskap eller en jobb. Istedenfor bør du vente et øyeblikk, og rolig organisere tankene dine. Hvis du trenger å få ut frustrasjonen din, åpne en ny e-post (forsikre deg om at det ikke er noen mottaker i «Til» feltet) og skriv nøyaktig hva du føler for å si. Kom deg så vekk fra datamaskinen, lag en kopp kaffe eller gå en tur. Når du kommer tilbake, slett det du har skrevet og begynn på nytt. Eller enda bedre, ta en telefon og ganske enkelt snakk med vedkommende, eller snakk ansikt til ansikt om mulig. Det kan være vanskelig for andre å forstå undertoner og formål ut ifra en e-post, så det du har å si fungerer kanskje bedre om du sier det på telefon eller direkte. Husk at humor (spesielt tørr humor) ikke alltid oversettes bra i emosjonelle e-poster, og at folk fort kan misforstå meldingen din.

Personvern

Til slutt bør du være klar over at e-post har få mekanismer for å beskytte personvern. E-posten din kan leses av alle som får tilgang til den, på samme måte som et brev som blir sendt i posten. E-posten din kan enkelt bli videresendt til andre, lagt ut på offentlig forum, frigitt som følge av en rettskjennelse, eller spredt dersom en e-postserver blir hacket. Hvis du har noe virkelig privat du ønsker å kommunisere burde du heller gjøre det over telefon. Det er også viktig å være klar over at e-post kan brukes som rettskraftig bevis i mange land. Til slutt, om du bruker jobbmaskinen din for å sende e-post, må du være klar over at arbeidsgiveren din sannsynligvis har rett til å overvåke og lese e-posten din, dersom den er sendt eller mottatt med jobbens resurser.

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

Keith Palmgren har jobbet i sikkerhetsindustrien i over 30 år. Keith er administrerende direktør for NetIP, inc. Han er også kursforfatter for SANS SEC301 – «Introduction to Cyber Security» - et 5 dagers SANS kurs. <https://sans.org/sec301>.



Ressurser

E-postvett: <https://www.sans.org/u/IJj>

Phishing: <https://www.sans.org/u/IJo>

Kontroller autofullfør-listen din:

[Windows](#) [Mac](#)

OUCH! utgis av SANS Security Awareness, og er distribuert under [Creative Commons BY-NC-BD 4.0 lisensen](#). Du står fritt til å distribuere dette nyhetsbrevet, eller bruke det i ditt eget bevissthetsprogram, så lenge du ikke gjør endringer på nyhetsbrevet. For oversettelser og mer informasjon, ta kontakt med oss på www.sans.org/security-awareness/ouch-newsletter. Redaksjon: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Oversatt av: NorSIS