

Spam

Til hvert scenarie skal du identificere, om beskeden er spam, og om du bør dele oplysninger med personen. Skriv dit svar på hvert spørgsmål på den tomme plads.

Situation 1

Du modtager en e-mail fra en advokat om, at en fjern slægtning har angivet dig som arving til en sum penge. Beskeden lyder: "For at modtage pengene skal du sende mig dit bankkontonummer og dit routingnummer, så vi kan foretage overførslen".

Situation 2

En ven sender dig en tekstbesked om, at han/hun forsøger at se et billede, du tidligere har vist, men at han/hun ikke har tilladelse til at se det. Du har for øjeblikket ikke adgang til din computer, så du kan sende billedet til vedkommende. Vedkommende svarer: "Jeg kan logge på din konto og downloade billedet – hvad er din adgangskode?"

Situation 3

Du modtager en e-mail fra din skole med besked om, at mange elevkonti er blevet hacket. De skriver: "Vi har for nyligt registreret, at mange elevkonti er blevet hacket. Vi beklager og arbejder på at løse problemet. Besvar denne e-mail med dit brugernavn og din adgangskode for at få nulstillet din konto".

Situation 4

Du modtager en e-mail fra din bank, hvor du har en legitim konto. I e-mailen står der, at banken er blevet hacket, og at du hurtigst muligt skal logge på for at ændre din kontoadgangskode og ændre adgangskoderne til alle andre konti, hvortil du bruger den samme adgangskode.

Spam: Underviserkopi

Til hvert scenarie skal du identificere, om beskeden er spam, og om du bør dele oplysninger med personen. Skriv dit svar på hvert spørgsmål på den tomme plads.

Situation 1

Du modtager en e-mail fra en advokat om, at en fjern slægtning har angivet dig som arving til en sum penge. Beskeden lyder: "For at modtage pengene skal du sende mig dit bankkontonummer og dit routingnummer, så vi kan foretage overførslen".

Denne e-mail er formentlig spam. Selvom din slægtnings navn er angivet korrekt, er afsenderen formentlig ikke korrekt. Afsender kan have fundet oplysningerne om dig på andre måder. Der er altid en risiko forbundet med at dele sine bankkontooplysninger, og du skal være yderst forsigtig med at gøre det. Du skal aldrig sende oplysninger til andre, medmindre du har kontaktet vedkommende første, og du skal alligevel være meget forsigtig. Det er f.eks. ikke en god ide at sende dine oplysninger via e-mail, da det ikke er krypteret. Det er grunden til, at mange hospitaler, advokater og banker har særlige websites til kommunikation med dig.

Situation 2

En ven sender dig en tekstbesked om, at han/hun forsøger at se et billede, du tidligere har vist, men at han/hun ikke har tilladelse til at se det. Du har for øjeblikket ikke adgang til din computer, så du kan sende billedet til vedkommende. Vedkommende svarer: "Jeg kan logge på din konto og downloade billedet – hvad er din adgangskode?"

Selvom det ikke er spam, skal du ikke dele dine adgangskoder med andre. Når de har din adgangskode, kan de låse dig ude fra din egen konto eller få adgang til andre onlinekonti, hvortil du bruger samme adgangskode. Desuden kan der ske det, at hvis en tredjepart, en hacker eller en anden ser din besked, kan flere personer få adgang til din konto, uden at du ved det.

Situation 3

Du modtager en e-mail fra din skole med besked om, at mange elevkonti er blevet hacket. De skriver: "Vi har for nyligt registreret, at mange elevkonti er blevet hacket. Vi beklager og arbejder på at løse problemet. Besvar denne e-mail med dit brugernavn og din adgangskode for at få nulstillet din konto".

Det er normal praksis, at man ikke beder folk om disse oplysninger. Selvom afsenderen ser rigtig nok ud, skal du gå ud fra, at alle e-mails, der beder om din adgangskode, er spam.

Situation 4

Du modtager en e-mail fra din bank, hvor du har en legitim konto. I e-mailen står der, at banken er blevet hacket, og at du hurtigst muligt skal logge på for at ændre din kontoadgangskode og ændre adgangskoderne til alle andre konti, hvortil du bruger den samme adgangskode.

Den korrekte fremgangsmåde er at åbne et nyt browservindue og åbne websitet på normal vis. En offentliggørelse af denne type (om at konti er blevet hacket) vil normalt være nævnt på virksomhedens eller bankens kundeportal. Man kan følge instruktionerne på portalen uden at være nervøs. Som i scenarie 3 vil ingen legitim person kræve at få oplyst dine kontoplysninger via e-mail.