Spam

Identifiera för varje scenario om meddelandet är spam och om du bör dela information med personen. Skriv ditt svar på varje fråga i det angivna utrymmet.

Scenario 1

Du får ett e-postmeddelande från en advokat, där det står att en avlägsen släkting har sagt att du ska få en summa pengar. Det står: ”för att få pengarna ska du skicka mig ditt bankkontonummer och clearingnummer så att vi kan sätta in pengarna”.

Scenario 2

En vän skickar dig ett meddelande där det står att personen försöker leta upp ett foto som du hade visat tidigare, men personen har inte behörighet att se det. Du har inte tillgång till din dator nu för att skicka fotot till personen. Personen svarar: ”Jag kan logga in på ditt konto snabbt och ladda ner fotot. Vad har du för lösenord?”

Scenario 3

Du får ett e-postmeddelande från skolan, där det står att många elevkonton har hackats. Personen säger: ”Vi har nyligen upptäckt att många elevkonton har fått intrång. Vi beklagar detta och arbetar med att åtgärda problemet. För att återställa kontot ska du svara på det här e-postmeddelandet med ditt användarnamn och lösenord.”

Scenario 4

Du får ett e-postmeddelande från din bank där du har ett legitimt konto. I e-postmeddelandet står det att de har hackats och att du bör logga in och ändra lösenordet till ditt konto så fort som möjligt och ändra lösenord på konton som har samma lösenord.

Spam: Utbildarens kopia

Identifiera för varje scenario om meddelandet är spam och om du bör dela information med personen. Skriv ditt svar på varje fråga i det angivna utrymmet.

Scenario 1

Du får ett e-postmeddelande från en advokat, där det står att en avlägsen släkting har sagt att du ska få en summa pengar. Det står: ”för att få pengarna ska du skicka mig ditt bankkontonummer och clearingnummer så att vi kan sätta in pengarna”.

Det här e-postmeddelandet är förmodligen spam. Även om personen på rätt sätt använder din släktings namn kanske personen inte är den som han eller hon utger sig för att vara. Avsändaren skulle kunna ha fått information om din släkting på andra sätt. Att dela din bankkontoinformation är alltid riskabelt och bör ske varsamt. Skicka aldrig din information till någon såvida du inte har kontaktat personen först, och var även mycket försiktig i sådana fall. Det är exempelvis inte smart att skicka din information på e-post eftersom den är okrypterad. Det är därför många sjukhus, advokater och banker har särskilda webbplatser för att kommunicera med dig.

Scenario 2

En vän skickar dig ett meddelande där det står att personen försöker leta upp ett foto som du hade visat tidigare, men personen har inte behörighet att se det. Du har inte tillgång till din dator nu för att skicka fotot till personen. Personen svarar: ”Jag kan logga in på ditt konto snabbt och ladda ner fotot. Vad har du för lösenord?”

Även om det här inte är spam bör du inte dela dina lösenord med andra personer. När de har fått ditt lösenord kan hen stänga ute dig från ditt konto eller komma in på andra webbkonton med samma lösenord. Om en tredjepart, hackare eller åskådare ser ditt meddelande kan fler personer eventuellt komma in på ditt konto utan att du vet om det.

Scenario 3

Du får ett e-postmeddelande från skolan, där det står att många elevkonton har hackats. Personen säger: ”Vi har nyligen upptäckt att många elevkonton har utsatts för intrång. Vi beklagar detta och arbetar med att åtgärda problemet. För att återställa kontot ska du svara på det här e-postmeddelandet med ditt användarnamn och lösenord.”

Vanligtvis frågar man inte användarna om den informationen. Även om avsändaren verkar legitim bör du utgå ifrån att all e-post där du uppmanas lämna ut lösenord är spam.

Scenario 4

Du får ett e-postmeddelande från din bank där du har ett legitimt konto. I e-postmeddelandet står det att de har hackats och att du bör logga in och ändra lösenordet till ditt konto så fort som möjligt och ändra lösenord på konton som har samma lösenord.

Det som är rätt att göra är att öppna ett nytt webbläsarfönster och gå in på sidan som du brukar göra. Ett sådant meddelande (om att konton har hackats) brukar stå på företagets eller bankens kundportal. Anvisningarna på portalen ska kunna följas på ett säkert sätt. Precis som i scenario 3 kommer ingen legitim aktör begära inloggningsuppgifter av dig via e-post.