Spam

For hvert scenario identifiserer du om meldingen er spam og om du bør dele informasjon med vedkommende. Skriv svaret på hvert spørsmål i det oppgitte feltet.

Scenario 1

Du mottar en e-post fra en advokat som informerer deg om at en fjern slektning har tilgodesett deg en pengesum. Det står «For å motta pengene må du sende meg bankkontonummer og rutingnummer, slik at jeg kan sette inn pengene.»

Scenario 2

En venn sender deg en tekstmelding og forteller deg at vedkommende prøver å finne et bilde du viste tidligere, men at vedkommende ikke har tillatelse til å se det. Du har ikke tilgang til datamaskinen din for øyeblikket, og kan ikke sende vedkommende bildet. Vennen din svarer «Jeg kan logge inn på kontoen din raskt og laste ned bildet. Hva er passordet ditt?»

Scenario 3

Du får en e-post fra skolen din som hevder at mange studentkontoer har blitt hacket. Det står «Vi har nylig oppdaget at mange studentkontoer har blitt hacket. Vi beklager dette og jobber med å løse problemet. For å tilbakestille kontoen din svarer du på denne e-posten med brukernavn og passord.»

Scenario 4

Du mottar en e-post fra banken din hvor du har en konto. I e-posten står det at banken har blitt hacket, og at du må logge inn for å endre kontopassord så snart som mulig og endre passordene på alle kontoer som deler samme passord.

Spam: Instruktørens kopi

For hvert scenario identifiserer du om meldingen er spam og om du bør dele informasjon med vedkommende. Skriv svaret på hvert spørsmål i det oppgitte feltet.

Scenario 1

Du mottar en e-post fra en advokat som informerer deg om at en fjern slektning har tilgodesett deg en pengesum. Det står «For å motta pengene må du sende meg bankkontonummer og rutingnummer, slik at jeg kan sette inn pengene.»

Denne e-posten er sannsynligvis spam. Selv om de bruker riktig navn på slektningen din, er det ikke sikkert vedkommende er den vedkommende gir seg ut for å være. Avsenderen kan ha skaffet seg informasjon om relasjonen din på andre måter. Det er alltid risikofylt å dele bankkontoinformasjonen din, og det bør gjøres med forsiktighet. Aldri send informasjonen din til noen med mindre du har kontaktet vedkommende først, og selv da må du være forsiktig. Det er for eksempel antakelig ikke en god idé å sende informasjonen din via e-post siden den ikke er kryptert. Derfor har mange sykehus, advokater og banker spesielle nettsteder til kommunikasjon med deg.

Scenario 2

En venn sender deg en tekstmelding og forteller deg at vedkommende prøver å finne et bilde du viste tidligere, men at vedkommende ikke har tillatelse til å se det. Du har ikke tilgang til datamaskinen din for øyeblikket, og kan ikke sende vedkommende bildet. Vennen din svarer «Jeg kan logge inn på kontoen din raskt og laste ned bildet. Hva er passordet ditt?»

Selv om dette ikke er spam, bør du ikke dele passordene dine med andre personer. Når de har passordet ditt, kan de muligens låse deg ut av kontoen din eller få tilgang til andre kontoer på nettet med samme passord. Hvis en tredjepart, hacker eller tilskuer ser meldingen din, kan flere personer få tilgang til kontoen din uten at du vet om det.

Scenario 3

Du får en e-post fra skolen din om at mange studentkontoer har blitt hacket. Det står «Vi har nylig oppdaget at mange studentkontoer har blitt hacket. Vi beklager dette og jobber med å løse problemet. For å tilbakestille kontoen din svarer du på denne e-posten med brukernavn og passord.»

Det er vanlig praksis å ikke spørre brukerne om denne informasjonen. Selv om avsenderen virker legitim, bør du anta at en e-post som spør etter passordet ditt, er spam.

Scenario 4

Du mottar en e-post fra banken din hvor du har en konto. I e-posten står det at banken har blitt hacket, og at du må logge inn for å endre kontopassord så snart som mulig og endre passordene på alle kontoer som deler samme passord.

Riktig handlingsforløp er å åpne et nytt nettleservindu og gå inn på nettstedet slik du vanligvis ville gjort. En avdekking av denne typen (at kontoer har blitt hacket) vil vanligvis bli nevnt på bedriftens eller bankens kundeportal. Instruksjoner på portalen skal kunne følges trygt. Som i Scenario 3 vil ingen legitime aktører be om kontoopplysninger fra deg i en e-post.