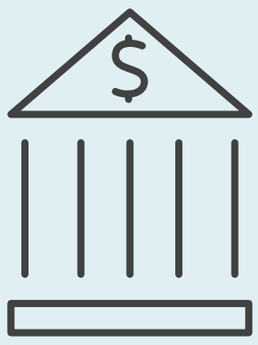
Bekjemp de tre vanligste formene for svindel

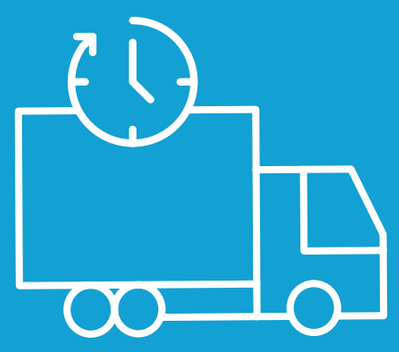
Én av to bedrifter har vært utsatt for bedrageri eller annen økonomisk kriminalitet i løpet av de siste to årene. Her forklarer vi de vanligste formene for svindel, og hvordan bedriften din kan forebygge og avsløre svindelen før skaden har skjedd.



HENVENDELSE OM BYTTE AV BANK

Eksempel:
Bedriften din mottar en e-post fra en leverandør om bytte av bank eller innbetaling til en ny konto. E-posten er tilsynelatende sendt fra leverandørens e-postsystem og virker ikke mistenkelig, men den kommer fra en svindler. Leverandørens system er hacket, og svindleren har kontroll over e-post-korrespondansen. Bedriften din betaler følgelig fakturaen til feil konto – og leverandøren får ikke pengene sine.

Løsning:
De fleste selskaper bytter bank av og til. Det i seg selv er ikke noe oppsiktsvekkende, men dersom bedriften din får en slik henvendelse, anbefaler vi å ringe kontaktperson deres hos leverandøren og få bekreftet at de har byttet bankkonto. Unngå å ringe nummeret som er oppgitt i e-posten om kontobyttet – det kan være svindleren selv som tar telefonen. Som leverandør kan du med fordel sette inn en tekst på bedriftens fakturaer, om at henvendelser om bytte av bankkonto ikke skal aksepteres uten forutgående bekreftelse fra den faste kontaktpersonen.



LEVERING TIL ANNEN ADRESSE

Eksempel:
Bedriften din har mottatt en ordre på en rekke varer. Før varene blir ekspedert, mottar ordreavdelingen eller en medarbeider i bedriften en e-post med forespørsel om levering til en annen adresse. E-posten ser ikke mistenkelig ut, siden den kommer fra kundens system, men det er et bedrageri. Kundens e-post-system er hacket, og svindleren kontrollerer korrespondansen. Bedriften din sender følgelig varene til feil adresse, og kunden mottar aldri ordren sin – og vil derfor heller ikke betale for den.

Løsning:
Det hender at kunder vil endre leveringsadresse for en ordre, men ring alltid den du vanligvis har kontakt med hos kunden. Spør hvorfor de byttet adresse, og om adressen er riktig. Denne typen svindel kan ofte fungere i bedrifter med ordreavdelinger som behandler ordrer i høyt tempo, og kanskje ikke sjekker hver enkelt ordre grundig nok.

FOR GODT TIL Å VÆRE SANT

Eksempel:
Du har lenge prøvd å slippe til som leverandør til en stor supermarkedkjede, og plutselig en dag får du napp. Bedriften mottar en e-post med en stor ordre. E-posten ser ikke mistenkelig ut, men vær på vakt. Det er svindel. Svindleren utgir seg for å være drømmekunden din, men det hele ender opp som et mareritt der dere sender et stort antall varer til en svindler, og bedriften din taper penger.

Løsning:
Hvis noe virker for godt til å være sant, er det fare for at det virkelig er nettopp det. Hvis du mottar en stor ordre fra et selskap du ikke tidligere har gjort forretninger med, må du ringe selskapet – gjerne til sentralbordet eller til en person i selskapet du kjenner. Takk for ordren og gi uttrykk for hvor glade du og kollegene dine er over den. Ordren kan være reell, eller den kan være en del av et svindelforsøk. Unngå å ringe nummeret som er oppgitt i ordren – det kan være svindleren selv som tar telefonen.