

Bekæmp de tre mest almindelige former for fraud

Hver anden virksomhed har været udsat for bedrageri eller økonomisk kriminalitet inden for de seneste to år. Vi forklarer her de mest almindelige former for fraud, og hvordan din virksomhed kan modarbejde og afsløre bedrageriet, før skaden sker.



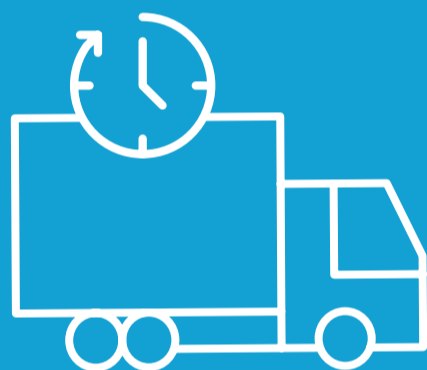
HENVENDELSE OM BANKSKIFTE

Eksempel:

Din virksomhed modtager en e-mail om bankskifte eller om indbetaling på en ny konto fra en leverandør. E-mailen er tilsyneladende sendt fra leverandørens e-mailsystem og ser ikke mistænkelig ud. Men det kommer fra en svindler. Leverandørens system er hacket, og svindleren har kontrol over e-mailkorrespondancen. Din virksomhed betaler altså fakturaen til den forkerte konto – og leverandøren får ikke sine penge.

Løsning:

De fleste virksomheder skifter bank en gang imellem. Det er ikke i sig selv opsigtsvækkende. Men hvis din virksomhed modtager sådan en henvendelse, anbefaler vi, at din virksomhed ringer til jeres kontaktperson hos leverandøren og får verificeret, at virksomheden skifter bankkonto. Ring ikke blot til det telefonnummer, der oplyses i e-mailen om bankskiftet – det kan være svindleren selv, der besvarer det opkald. Som leverandør kan man med fordel indsætte en tekst på virksomhedens fakturaer, hvor der står, at henvendelser om bankkontoskifte ikke skal accepteres uden forudgående bekræftelse hos den faste kontaktperson.



LEVERING TIL ANDEN ADRESSE

Eksempel:

Din virksomhed har modtaget en ordre på et antal varer. Inden afsendelse af varerne modtager ordreafdelingen eller en anden person i virksomheden en e-mail med ønske om levering til en anden adresse. E-mailen ser ikke mistænkelig ud, fordi den kommer fra kundens system. Men det er bedrageri. Kundens e-mail-system er hacket, og svindleren styrer korrespondancen. Din virksomhed sender altså varerne til den forkerte adresse, og din kunde modtager aldrig sin ordre – og vil derfor heller ikke betale for den.

Løsning:

Ændring af leveringsadresse kan forekomme, men ring altid til den person, du plejer at tale med hos kunden. Spørg, hvorfor man ændrer adresse, og om adressen er korrekt. Denne type svindel kan ofte ske, hvis man har en ordreafdeling, der i højt tempo behandler ordrer og måske ikke har et øje på hver bestilling.



FOR GODT TIL AT VÆRE SANDT

Eksempel:

Du har længe prøvet på at komme ind som leverandør i den store supermarkeds kæde, og pludselig en dag, så lykkes det. En e-mail havner i din virksomheds indbakke med en bestilling på en stor ordre. E-mailen ser ikke mistænkelig ud, men vær på vagt. Det er fraud. Svindleren udgiver sig for at være din drømmekunde, men det hele ender som et mareridt, hvor et stort antal varer bliver sendt til en svindler, og din virksomhed taber penge.

Løsning:

Hvis det ser for godt ud til at være sandt, så er der en risiko for, at det også er det. Hvis du modtager en stor ordre fra en virksomhed, du ikke tidligere har arbejdet med, så ring til virksomheden. Gerne på hovednummeret. Eller til en, du kender. Sig tak for ordren, og giv udtryk for, hvor stor glæde ordren vækker i din virksomhed. Måske er ordren god nok, måske er den ikke. Ring ikke blot til det telefonnummer, der oplyses i ordren – det kan være svindleren selv, der besvarer det opkald.