8 tips för att undvika bedrägerier i ditt företag

WHISTLEBLOWER PARTNERS

Företagsbedrägerier är ett stort och växande problem i takt med att ökad globalisering, digitalisering och ökad komplexitet inom många områden har ökat risken.

Bedrägerier inom företag är ett större problem än vad många inser. Ett företag kan förlora upp till fem procent av sin årliga omsättning på grund av interna bedrägerier. Detta framgår av internationella studier. Danska företag upplever också en kraftig ökning av ekonomisk cyberbrottslighet, där anställda luras att betala ut pengar till externa brottslingar.

Det är uppenbart att kontroll är otroligt viktigt, men även om till exempel revisionsverktyg kan vara till stor hjälp är lösningen inte fullt så enkel. Lika viktigt är en god arbetskultur där de anställda uppmuntras och påverkas till att göra rätt val så att de inte gör medvetna eller omedvetna misstag som kan bli kostsamma för företaget.

Sedan covid-19-epidemin drabbade oss har hemarbete blivit det nya normala och trenden kommer sannolikt att fortsätta. Detta har också skapat nya risker för företagen.

Här är några punkter att vara uppmärksam på när det gäller företagsbedrägerier:

1. **Ökad kontroll och medvetenhet om förfarandena i företaget**

Färre personer på kontoret kan innebära att rutinerna lättas internt för att få vardagen att flyta smidigt. Lösenord kan delas mellan kollegor och det finns en risk för att samma person kan godkänna fakturor, ändra uppgifter om borgenärer och godkänna betalningar.
Detta ger goda möjligheter till ekonomiska bedrägerier där bedragaren kan dölja sina spår. Om det sker i liten skala under en längre tid kan bedrägeriet bli ganska stort innan det – kanske – upptäcks.
Företagen bör därför inte lätta på de interna rutinerna, även om de anställda i allt större utsträckning arbetar individuellt hemifrån, och bör ständigt ”reglera” kontrollverksamheten i enlighet med riskerna.

2. **Hög medvetenhet om dataintrång, nätfiske och andra it-bedrägerier**

Kriminella försöker allt oftare lura företag att lämna ut personliga koder eller information via telefonsamtal (vishing), sms (smishing) eller e-post (phishing). Bedragaren utger sig ofta för att komma från till exempel företagets bank eller affärspartner, offentliga myndigheter, NemID eller Nets.
Vissa företag får sina e-postsystem hackade direkt, andra använder sig av nätfiske, där ett klick på en länk eller fil i ett falskt e-postmeddelande kan ge tillgång till företagets IT-system.
Det är mycket viktigt att inpränta hos de anställda att de ska vara skeptiska till oönskad kontakt eller e-postmeddelanden som ser ovanliga eller konstiga ut, och de anställda ska få inpräntat att

de aldrig ska lämna ut personlig information eller koder. I tveksamma fall bör enskilda anställda alltid kontakta företagets IT-avdelning – hellre en gång för mycket än inte alls.

3. Undvik vd-bedrägerier

Vd-bedrägerier inträffar när en anställd luras att betala en falsk faktura eller göra en obehörig överföring från företagets konto till ett konto som ägs av bedragaren. Bedragaren utger sig för att vara en högt uppsatt person i företaget.
Det är viktigt att införa rutiner i företaget för betalning av räkningar och överföringar av medel, och att alla förfrågningar som inte är normala följs upp med en kontroll, oavsett hur brådskande överföringen är enligt mejlet. Ett telefonsamtal till vd:n kan ofta avslöja hela bedrägeriet och rädda företaget från stora förluster.

4. Undvik fakturabedrägerier

Vid fakturabedrägerier låtsas bedragaren representera ett företags kund eller leverantör och ber att framtida fakturor ska betalas till ett nytt bankkonto – som tillhör bedragaren.
Det är viktigt att se till att den berörda personalen är informerad och medveten om denna typ av bedrägerier och hur man undviker dem. Det är därför viktigt att be personal med ansvar för betalning av fakturor att alltid kontrollera om det finns några oegentligheter, att fastställa fasta rutiner för hantering av manuella betalningar och att kontrollera att betalningsuppmaningar är legitima.
Det är fördelaktigt att använda ett automatiserat betalningssystem för att minimera antalet manuella betalningar.

5. Var uppmärksam på bedrägerier när du ändrar bankuppgifter

Det är viktigt att vara medveten om att denna typ av bedrägerier med ändring av bankuppgifter existerar och att denna kunskap delas med de funktioner inom företaget som kan vara potentiella offer för sådana ändringar av bankuppgifter.
Om företaget får ett e-postmeddelande om en ändring av bankuppgifter ska leverantören alltid kontaktas för att få bekräftat av företagets normala kontaktperson att ändringen av kontot är korrekt.

6. Undvik momsbedrägerier

Det finns en betydande risk för att företag utsätts för momsbedrägerier vid handel i samband med momskaruseller. Momskaruseller kännetecknas av handel med varor och tjänster över nationsgränserna. Vanligtvis sker handeln med varorna genom en bulvan som inte deklarerar eller redovisar moms när varorna säljs vidare. Varorna säljs sedan via en eller flera mellanhänder innan de skickas ut ur Danmark igen och så fortsätter karusellen.

Dessa mellanhänder kan vara äkta danska företag. Detta innebär att danska företag lätt kan hamna i en fälla som kan leda till ekonomiska förluster, till exempel i form av förlorade momsavdrag, föråldrade varor, dåligt rykte eller illojal konkurrens inom branschen. I vissa fall kan en hel marknad undermineras innan bedrägeriet upptäcks.
Om det finns minsta lilla tvivel om leverantören eller de varor som företaget köper bör du undvika affären. Det rekommenderas också att man alltid kontrollerar om de företag som företaget handlar med är momsregistrerade. Företaget gör detta genom att söka på leverantörens momsregistreringsnummer.
På SKAT's webbplats finns också ett antal särskilda punkter som man bör vara uppmärksam på vid köp och försäljning av varor.

7. **Se upp med skrivare**

Företagets skrivare kan utgöra en betydande säkerhetsrisk för företaget om man inte är försiktig.
Utvecklingen inom skrivartekniken, inklusive det faktum att skrivare innehåller samma hårdvarukomponenter som en dator, t.ex. enhet, kontrollpanel och tangentbord, innebär att företag bör skydda skrivare mot angrepp på samma sätt som en dator. Detta förbises ofta, även om företag i allmänhet är mycket medvetna om cyberhotet.

8. **Kontakta banken och anmäl bedrägerier eller försök till bedrägerier till polisen**

Om bedrägeriet har utförts via företagets bank ska banken alltid kontaktas för möjligheten att återkräva beloppet. Kontakta också alltid polisen vid ett bedrägeri eller försök till bedrägeri, även om du inte hann falla offer för bedrägeriet. Kom ihåg att spara dokumentationen och inkludera den i polisanmälan.