VD stödet
praktiska råd som fungerar

Alla kan bli lurade om det vill sig illa

Du har säkert både hört och läst att bedrägerier mot företag och privatpersoner ökar i en allt snabbare takt. Mörkertalet är dock stort eftersom många av olika orsaker inte anmäler begångna brott. Anledning kan vara att man skäms och känner sig dum för att man låtit sig luras.

Metoderna har blivit alltmer sofistikerade. Offentliga uppgifter finns en knapptryckning bort såsom adresser, ekonomi, fordon, familj, nyckelbefattningar och mycket mer. I det fördolda säljs och köps även annan information som någon på olika sätt kommit över, bankuppgifter, kortuppgifter, log-in, lösenord, mail, och sökhistorik m.m. Har man kunskap om hur ni arbetar, vem som gör vad, hur beslut fattas, faktura- och betalningsrutiner, vilka personer som tar de ekonomiska besluten och hur penningtransaktioner går till blir det lättare att utgöra sig för att vara anställd, kund eller leverantör för att genomföra sitt bedrägeri. Några metoder som bedragarna använder för att samla information är **1) Phishing** där bedragarna via mejl eller olika chattjänster försöker lura dig att öppna ett dokument, besöka en webbplats eller ladda ner en fil. Syftet är att infektera enheten med skadlig kod och/eller komma över behörigheter. **2) Vishing**, bedragare kontaktar dig på telefon och utger sig vara någon annan, till exempel banken. Ofta påstår bedragaren att det är bråttom för att stressa dig och att du inte ska tänka igenom situationen. **3) Smishing**, du får falska sms med länkar till sidor där du till exempel uppmanas att uppge personliga koder alternativt ringa ett falskt telefonnummer.

Olika vägar till dina pengar

Det finns många tillvägagångssätt en bedragare kan använda. Ta kontakt med en person och förmår hen att begå eller låta bli att begå en handling genom att utnyttja en förtroenderelation. Vilseleda en person att investera i något som inte existerar, inte har något värde, har lägre värde än utlovat eller är väldigt svårt att värdera. Utger sig för att ha befogenheter, t ex för att vara ekonomichef på det utsatta företaget, eller banktjänsteman på den utsattes bank och därigenom förmå den kontaktade till handling, t.ex. Vd-bedrägeri och Vishing. Gärningspersonen köper olovligen en vara/tjänst eller tar ett lån eller liknande med någon annans identitet. Lurar ett företag att betala en faktura för en vara eller en tjänst som personen/företaget inte har beställt. Använder någon annans fysiska bankkort, betalkort eller kreditkort för att olovligen genomföra köp eller utan fysiskt kort där enbart kortdata används vid transaktionen

.

Vad kan du göra för att skydda dig – några förslag

Se till att det finns skriftliga instruktioner för hur fakturor attesteras och betalas. Id handlingar förvaras på säker plats. Byt lösenord, glöm inte routrarna. Var kritisk mot fakturor, bestrid direkt om något är fel. Med Bolagsverkets app och en digital brevlåda håller du enkelt koll på ditt företag var du än är. Läs kontoutdragen, följ dina transaktioner och kontakta omedelbart banken om något inte stämmer. Skaffa ett ”shopping-kort” kopplat till konto med mindre summa. Spärra kort för utlands- och köp on-line om det är möjligt. Tänk på vilken typ av information som hamnar i soporna. Spärra obehörig adressändring på Skatteverkets hemsida. Varningslistan som Svensk Handel ligger bakom kan vara ett bra verktyg för att undvika bluffakturor och oseriösa företag. https://www.svenskhandel.se/sakerhetscenter/varningslistan

jan.marcusson-stahl@vdstodet.se
VD-STÖDET AB
Telephone +46 8 6270010
Dokumentmall: T0006-2
Karlavägen 18
114 31 Stockholm SWEDEN
www.vdstodet.se
info@vdstodet.se