SVENSK HANDEL

RAPPORT

Handelns utsatthet för IT-relaterad brottslighet

Innehåll

Inledning

2019 polisanmäldes drygt 240 000 bedrägeribrott i Sverige. Sifforna säger dock väldigt lite om hur utsattheten ser ut hos svenska handelsföretag, eftersom den officiella kriminalstatistiken inte särredovisar hur många anmälningar som gjorts av företag respektive privatpersoner. Många väljer dessutom att inte polisanmäla, vilket innebär att mörkertalet är stort.

Den IT-relaterade brottsligheten är ett växande problem – men hur ser utsattheten egentligen ut hos svenska företag? Hur många har drabbats av IT-relaterad brottslighet och vilken typ av brott handlar det oftast om?

För att få svar på dessa frågor har Svensk Handel tillsammans med Svensk Digital Handel genomfört en enkätundersökning bland våra medlemsföretag. Syftet med undersökningen har varit:

- att få reda på vilka IT-relaterade brott handeln utsätts för i störst utsträckning.
- att utifrån dessa identifierade problemområden ta fram relevant rådgivning och konkreta tips på hur företagare kan minska risken för att drabbas.

Sammanfattning

Utsattheten är stor bland handelsföretagen

- **43 procent** av handelsföretagen har utsatts för IT-relaterad brottslighet det senaste året.
- **39 procent** är oroliga eller mycket oroliga för att drabbas av IT-relaterade brott.

Av de som drabbats har:

- **60 procent** mottagit ett falskt mejl, sms eller telefonsamtal.
- **Närmare hälften** fått en bluffaktura.
- **46 procent** fått förfalskade mejl där avsändaren ser ut att vara en kollega eller chef.
- **23 procent** utsatts för virus eller skadlig kod.

Få väljer att polisanmäla

- Endast **hälften** av de drabbade företagen har valt att anmäla brottet till Polisen.

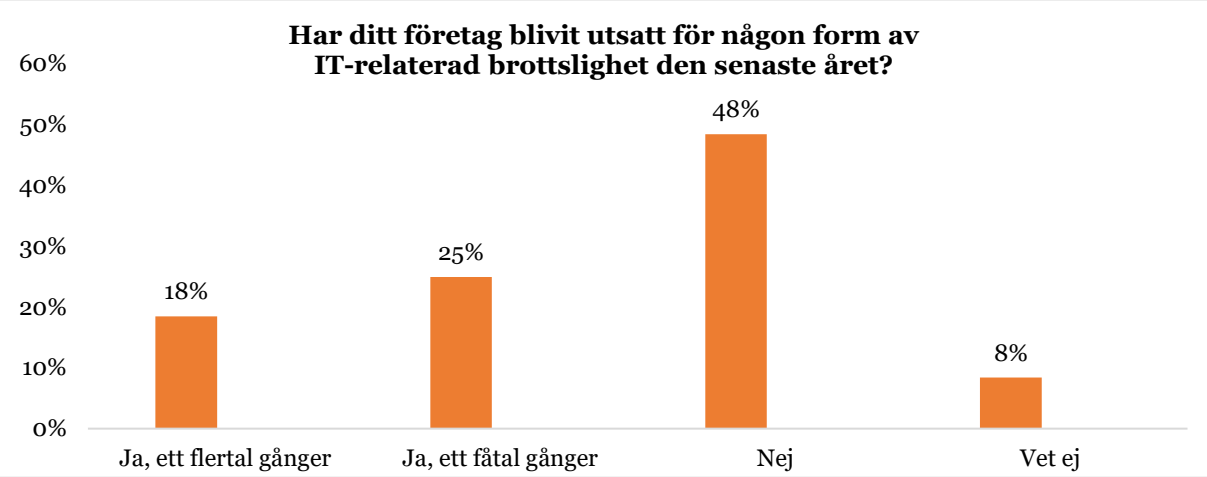
Företagen har bristande kunskap och rutiner

- Närmare **hälften** saknar kunskap om vilka åtgärder som bör vidtas för att minska risken för IT-brottslighet.
- **30 procent** saknar rutiner för hur man hanterar avvikande mejl.

Handelsföretagens utsatthet för IT-relaterad brottslighet

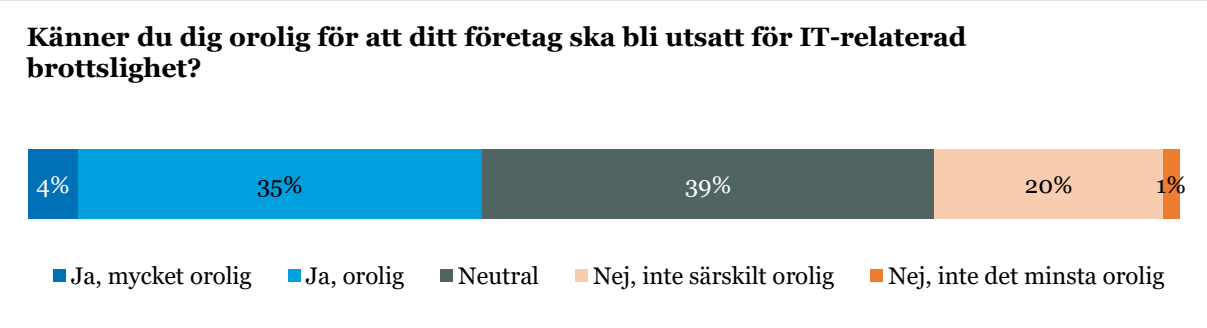
Med IT-relaterad brottslighet avses brottslighet där internet används för att utföra exempelvis ID-kapning, stjäla lösenord eller skicka falsk information (e-post/sms) i syfte att komma över information eller pengar. Även försöksbrott är inkluderade. Samtliga frågor är ställda utifrån om företaget utsatts det senaste året.

Närmare vartannat handelsföretag utsatt för IT-relaterad brottslighet det senaste året



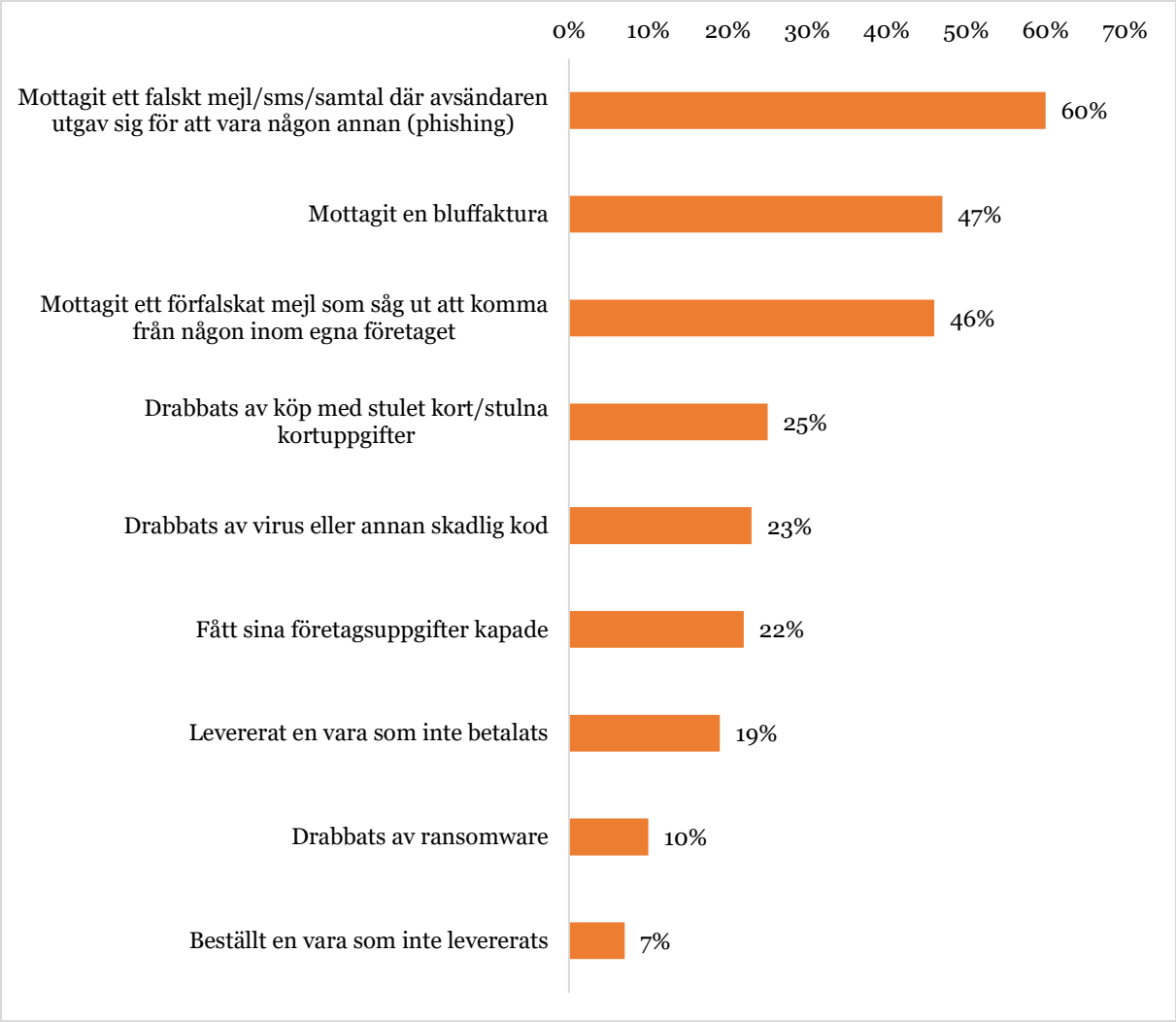
Figur 1: Andelen handelsföretag som utsatt för någon form av IT-relaterad brottslighet det senaste året

Nära hälften av företagen i undersökningen uppgav att de drabbats av IT-relaterad brottslighet det senaste året. En stor del av de drabbade uppgav dessutom att de blivit utsatta vid upprepade tillfällen. På frågan om de känner sig oroliga över att drabbas svarade 39 procent av företagen ja.



Figur 2: Andelen handelsföretag som känner oro över att utsättas för IT-relaterad brottslighet

Respondenterna vittnar om en stor mängd olika sorters IT-relaterad brottslighet som drabbar handeln. Såväl traditionella brott, däribland bluffakturor som närmare hälften av de som drabbats uppger att de mottagit, till mer avancerade angrepp, som ransomware och skadlig kod (se figur 3).



Figur 3: De vanligast förekommande IT-relaterade brotten i handeln

Phishing, smishing och vishing vanligaste brottet

Närmare **60 procent** av de som utsatts för IT-relaterad brottslighet uppger att de utsatts för ett falskt mejl, sms eller telefonsamtal där avsändaren utger sig för att vara någon annan än den de är, med avsikt att komma över information.

Phishing, eller **nätfiske** som det heter på svenska, är ett samlingsbegrepp för de olika försök till uppgiftsfiske som sker över internet. Det sker vanligen via mejl där avsändaren utger sig komma från ett väletablerat företag alternativt ser ut att komma från en myndighet. I mejlet finns en bifogad länk eller fil som mottagaren ombeds klicka på för att exempelvis verifiera inloggningsuppgifter. I de flesta fall är bedragarna ute efter kortuppgifter eller lösenord kopplade till företaget, men det kan även röra sig om att skadlig kod eller virus laddas ner till enheten.

Samma upplägg kan ta sig uttryck via sms (då kallat **smishing**) eller via telefon (**vishing**) men syftet är detsamma – att förmå mottagaren att lämna ut inloggnings- eller kortuppgifter, alternativt förmå mottagaren att ovetandes ladda ner skadlig kod eller virus till sin enhet vilket kan få förödande konsekvenser, inte minst ekonomiskt.

Som exempel kan attacken mot rederikoncernen Maersk nämnas. Sommaren 2017 drabbades Maersk av cyberattacken NotPetya. Den skadliga koden, som framförallt spreds via phishingmejl, slog ut 76 terminaler i fyra olika länder och orsakade avbrott och förseningar som varade i flera veckor. Den totala kostnaden beräknades landa på mellan 200-300 miljoner dollar.

Bluffakturor – ett konstant och ökande problem

Varannan företagare som uppgett att de utsatts för ett bedrägeribrott under 2020 har mottagit en bluffaktura. Bluffakturor är ett samlingsbegrepp för bedrägliga försäljningsmetoder via telefon, post eller e-post. Det kan börja med att en säljare tar kontakt med någon på företaget via telefon och försöker sälja in något under vilseledande omständigheter, men det kan även dyka upp fakturor utan tidigare kontakt.

Svensk Handels Varningslista har noterat en kraftig ökning av inkomna klagomål det senaste året. Varningslistan varnar för bluffakturor, företag med oseriösa försäljningsmetoder och för erbjudanden eller utskick som kan uppfattas som vilseledande. Företag som drabbas av bluffakturor kan höra av sig till Svensk Handels Varningslista för att få rådgivning, alternativt tipsa om oseriösa aktörer. Jämfört med 2019 har det skett en ökning på över 100 procent gällande inkomna klagomål till Varningslistan. Det största problemet för företagen har utan tvekan varit vilseledande försäljning av elavtal.

Snarlika tillvägagångssätt

Tillvägagångssätten har varit snarlika. Säljare ringer upp och erbjuder billigare el, inte sällan under förespeglingen att de ringer från företagets befintliga leverantör. Under samtalet skickas det över en sms-länk som man ombeds att öppna för att ta del av erbjudandet. Säljaren är vanligen mycket påstridig och stressar mottagaren av sms-länken att klicka sig vidare, vilket i slutändan resulterar i att man tackat ja till ett elavtal med det bedrägliga bolaget.

När fakturan sedan kommer är priset betydligt högre än vad man var överens om. Det är svårt att komma fram till kundtjänst för att bestrida och väldigt snabbt kommer hot om att stänga av elen om man inte betalar. Närmare 70 procent av alla klagomål till Svensk Handels Varningslista under 2020 har rört vilseledande elavtal och många företag har upplevt att det är väldigt svårt att ta sig ur dem.

Rättigheter för företagare

Juridiska personer har inte samma rättigheter som privatpersoner när det gäller ångerrätt och muntliga avtal. Som privatperson är inte muntliga avtal giltiga vid telefonförsäljning och man har som regel 14 dagars ångerrätt.

Detta gäller inte för juridiska personer vilket troligtvis är en av anledningarna till att flertalet bedragare riktar in sig på just företag. Det är dock viktigt att veta att om ett företag känner sig vilselett vid ingången av ett avtal ska fakturan inte betalas utan bestridas (läs mer under rekommendationer på sidan 14).

Närmare hälften har fått förfalskade mejl där avsändaren ser ut att vara en kollega eller chef

Det tredje vanligaste bedrägeribrottet (**46 procent**) som företagen uppgett att de utsatts för är att de mottagit ett förfalskat mejl där avsändaren utger sig för att vara någon inom

företaget. Det kan handla om att mejl med uppmaning om att ändra konto för utbetalning skickas till HR-avdelningen från vad som ser ut att vara en anställd inom företaget men i de flesta fall handlar det om så kallade VD-bedrägerier.

Ett VD-bedrägeri innebär kortfattat att en bedragare utger sig för att vara en högt uppsatt chef inom ett företag. Den falska VD:n skickar ett mejl till en annan person på företaget och ber denne göra en överföring på en stor summa pengar till ett konto. Det rör sig ofta om stora belopp som plötsligt och snabbt ska överföras. För att lyckas med detta registrerar bedragaren en liknande domänadress som dem/den han utger sig för att vara. Det kan handla om att ändra från .se till .com eller att lägga till eller ändra en bokstav i den korrekta e-postadressen. Denna typ av detaljer är svåra att upptäcka för mottagaren, varför det är viktigt att ha tydliga rutiner för vad som gäller vid transaktioner och överföringar inom företaget (läs mer under rekommendationer på sidan 15).

En av fyra utsatt för kortbedrägerier

25 procent av de drabbade handelsföretagen uppger att de utsatts för kortbedrägeri det senaste året. I undersökningsunderlaget gör vi inte skillnad på huruvida bedrägeriet skett med hjälp av ett fysiskt kort eller endast med hjälp av stulna kortuppgifter. Det rör sig om bedrägliga köp där gärningspersonen på ett eller annat sätt tillskansat sig varor eller tjänster på bekostnad av någon annan.

I majoriteten av fallen rör det sig om köp med hjälp av stulna kortuppgifter, så kallade ”**card not present-bedrägerier**”. Denna brottstyp står för omkring 40 procent av det totala antalet anmälda bedrägeribrott årligen. Förbrottet består oftast av dataintrång eller så kallad phishing där kortuppgifter stjäls för att därefter säljas på olika nätforum. När bedragaren väl har kortuppgifterna tillhands genomförs köp av varor och tjänster på nätet hos handlare vars betalningar inte stöds av 3D-secure[1].

Skadlig kod, virus och ransomware allt vanligare

Undersökningen visar att hela **23 procent** av de som drabbats av IT-relaterad brottslighet har utsatts för virus eller skadlig kod det senaste året. Vid en fråga rörande utsattheten för specifikt **ransomware** uppgav **10 procent** att de drabbats. Utpressningsvirus eller Ransomware som det ofta kallas har dessvärre blivit allt vanligare

Ransomware är en skadlig programvara som låser datorer, mobila enheter eller krypterar elektroniska filer. Om företagets enhet blir smittad märks det vanligen genom att det dyker upp ett pop-up fönster på skärmen som tydligt informerar innehavaren om att enheten infekterats. Den som ligger bakom attacken ger även instruktioner på hur aktuell lösensumma ska betalas för att återfå kontrollen över datorn.

---

[1] Den 14 september 2019 trädde det andra betaltjänstdirektivet PSD2 och dess krav på SCA (strong customer authentication) i kraft. Direktivets syfte är att skapa bättre förutsättningar för säkra och smidiga betalningar på nätet och även minska antalet bedrägliga transaktioner. SCA innebär att autentiseringen måste innehålla minst två av följande: Något man kan, exempelvis ett lösenord, något man äger, exempelvis en smartphone, något man har, exempelvis ett fingeravtryck.

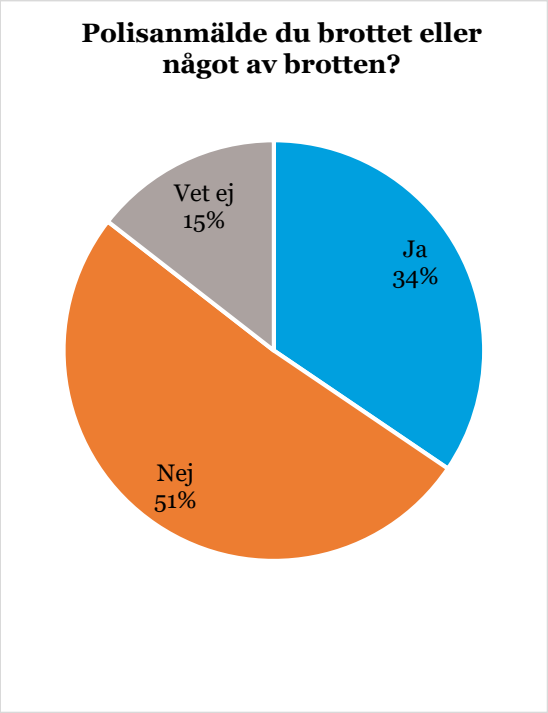
Sammanfattningsvis innebär SCA kravet att alla europeiska företag ska implementera 3D Secure vid köp som sker online. Initialt skulle implementeringen vara genomförd senast den 14 september 2019 men ett yttrande från Europeiska bankmyndigheten, EBA, den 16 oktober 2019 innebar att övergången till stark kundautentisiering för kortköp inom e-handeln sköts upp och ska vara genomförd senast den 31 december 2020.

Ransomware dyker inte bara upp på datorn utan anledning, utan skaparna av den skadliga programvaran försöker lura dig att installera programmen. Den vanligaste metoden är att skicka den skadliga koden via bluffmejl/phishing (se sid 6). Den kan också maskera sig som en falsk programuppdatering och man kan även drabbas genom att besöka smittade webbsidor.

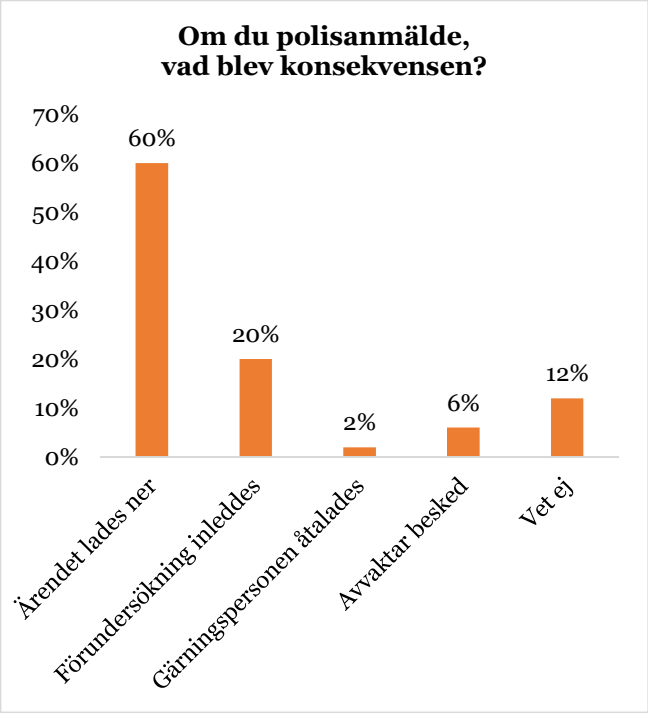
Nästan var fjärde handlare har utsatts företagskapning

22 procent av företagen uppger att de drabbats av företagskapning det senaste året. Det kan handla om att någon på falska grunder skaffat sig rätt att företräda företaget med syfte att ta ut pengar eller att köpa varor via företaget. Detta förfaringssätt är dock inte alls lika vanligt som att någon ”kapar” företaget digitalt. Det vill säga att kriminella beställer varor i företagets namn. Förfaringssättet är väldigt enkelt och det ligger på mottagaren av leveransen att kontrollera att beställaren verkligen är den som den utger sig för att vara.

Alla väljer inte att anmäla brotten till Polisen

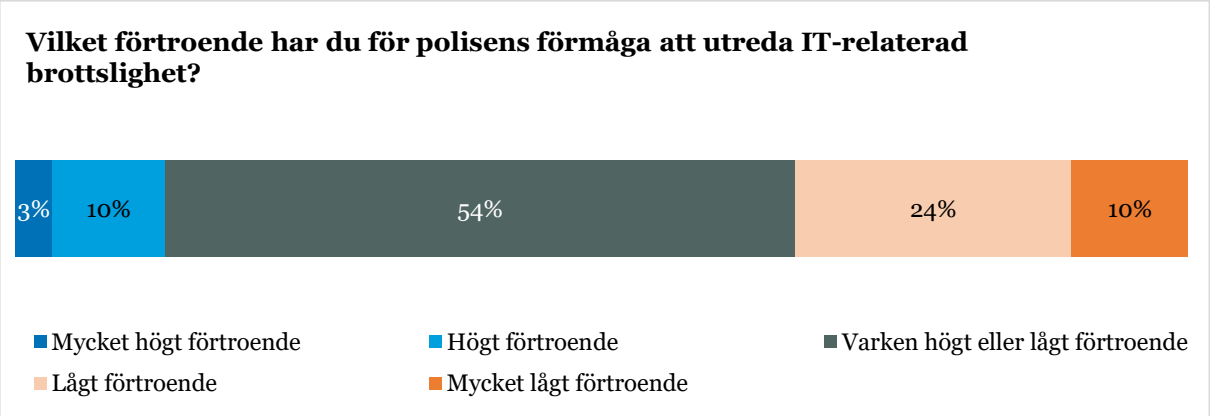


Figur 4: Andel som valde att polisanmäla brottet de utsattes för



Figur 5: Konsekvensen av polisanmälan

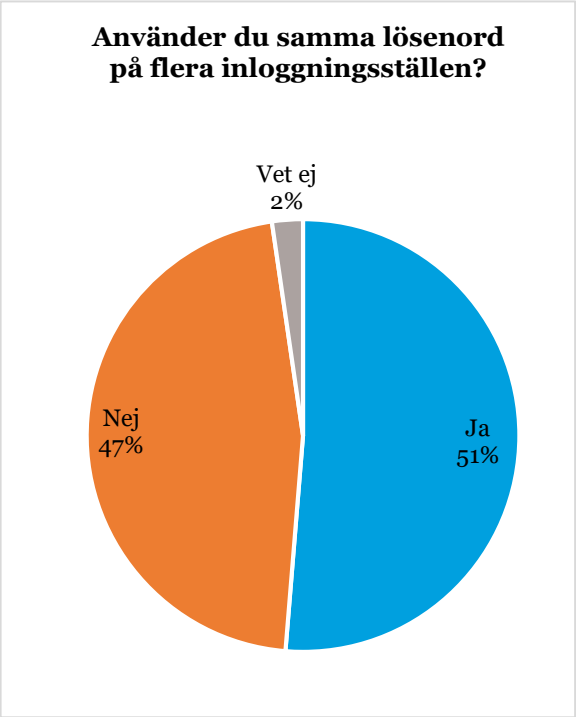
Endast en tredjedel av de drabbade företagen valde att anmäla brottet till Polisen. Av de brott som anmäldes lades 60 procent ner och i endast två procent av fallen åtalades någon för brottet. Att så få ärenden faktiskt leder till att någon åtalas för brottet påverkar sannolikt förtroendet för polisens förmåga att utreda IT-relaterade brott. Endast **13 procent** av företagen uppger att de känner högt eller mycket högt förtroende för Polisens förmåga att utreda IT-relaterade brott.



Figur 6: Handelsföretagens förtroende för polisens förmåga att utreda IT-relaterade brott

Svaga lösenord öppnar upp för angrepp

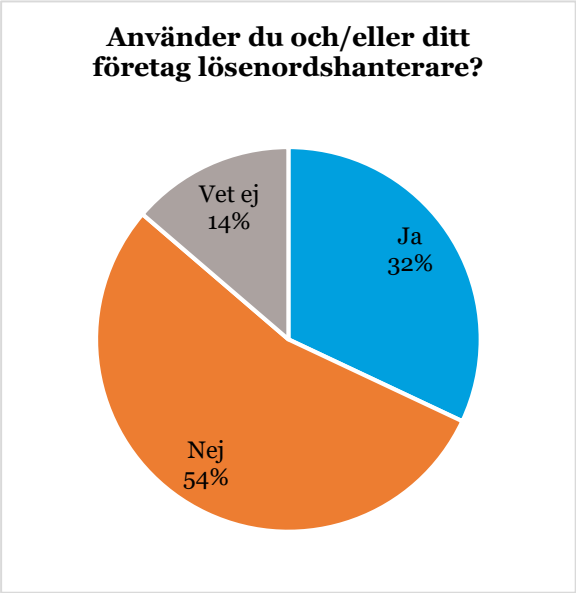
Det är mycket viktigt att använda starka lösenord för att förhindra intrång. Trots detta uppgav mer än hälften av företagen att de använder samma lösenord för flera tjänster.



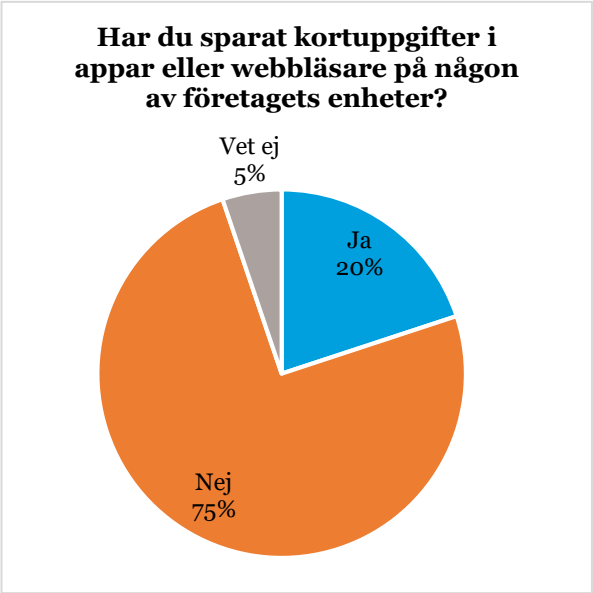
Figur 7: Nyttjandet av unika lösenord

Att använda samma lösenord för inloggning till olika tjänster bör undvikas. Om ett lösenord röjs innebär det att bedragaren får åtkomst till flera konton samtidigt. Det viktigast lösenordet är det som ger åtkomst till mejlkontot. Det är oftast dit mejl om återställning av lösenord för andra tjänster skickas.

Till de övriga tjänsterna kan såväl företag som privatpersoner med fördel använda en lösenordshanterare. En lösenordshanterare är som ett digitalt värdeskåp där användaren krypterat och säkert kan lagra sina användarnamn och lösenord till olika tjänster. Lösenordshanteraren skyddas i sin tur av ett huvudlösenord som enbart användaren känner till. Endast 32 procent av de svarande uppgav att de använde lösenordshanterare idag.

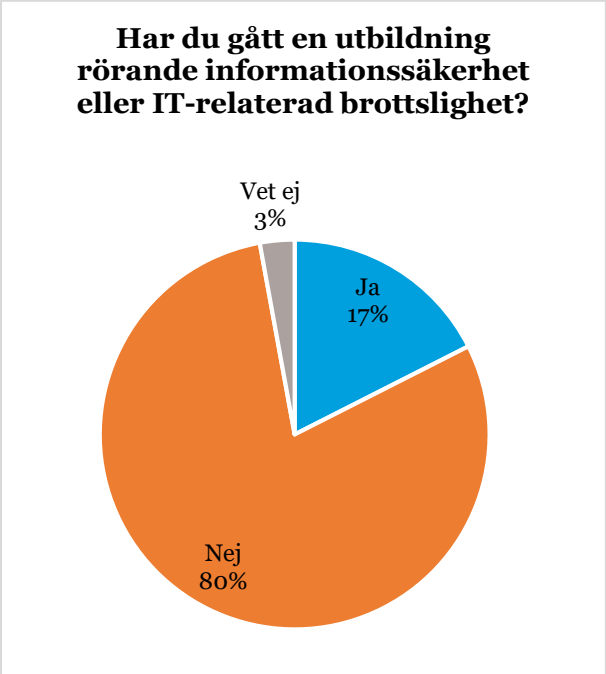


Figur 8: Nyttjandet av lösenordshanterare bland handelsföretagen

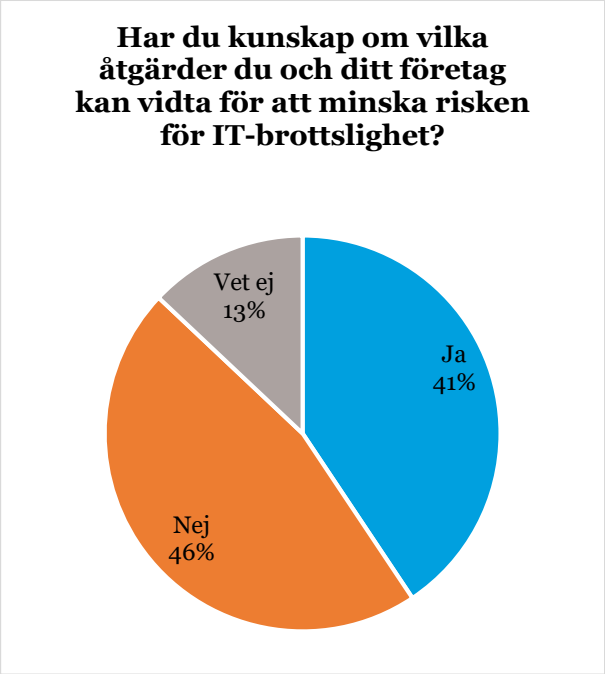


Figur 9: Lagring av kortuppgifter på företagets enheter

Kunskap och rutiner



Figur 10: IT-relaterade utbildningsinsatser på företagen rörande IT-brott

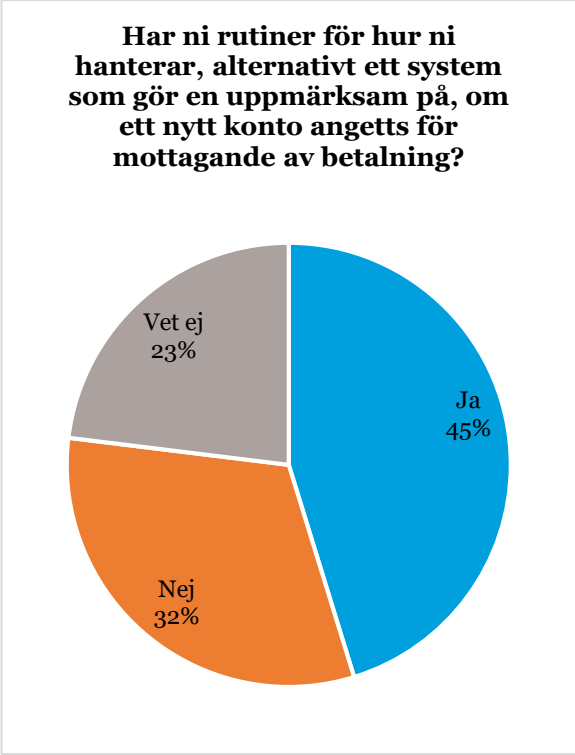


Figur 11: Brottsförebyggande kunskaper

På frågan om man som anställd gått någon utbildning rörande informationssäkerhet eller IT-relaterad brottslighet svarar **80 procent nej**. Vidare saknar närmare hälften kunskap om vilka åtgärder som bör vidtas för att minska risken för IT-brottslighet.

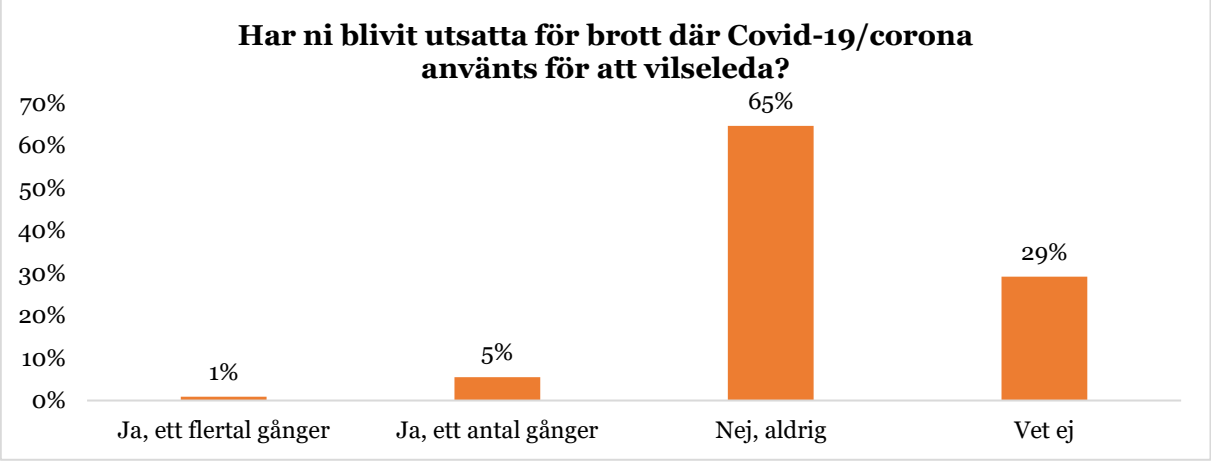
Endast hälften av företagen har ett system som gör den anställde uppmärksam på om ett nytt konto angetts för mottagande av betalning (det vill säga att det angivna kontonumret avviker från det man sedan tidigare har registrerat) och närmare 30 procent saknar rutiner för hur man hanterar avvikande mejl.

Figur 12: Handelsföretagens hantering av okända mejl



Figur 13: Handelsföretagens hantering av utbetalningar

Företagens utsatthet för bedrägerier under corona



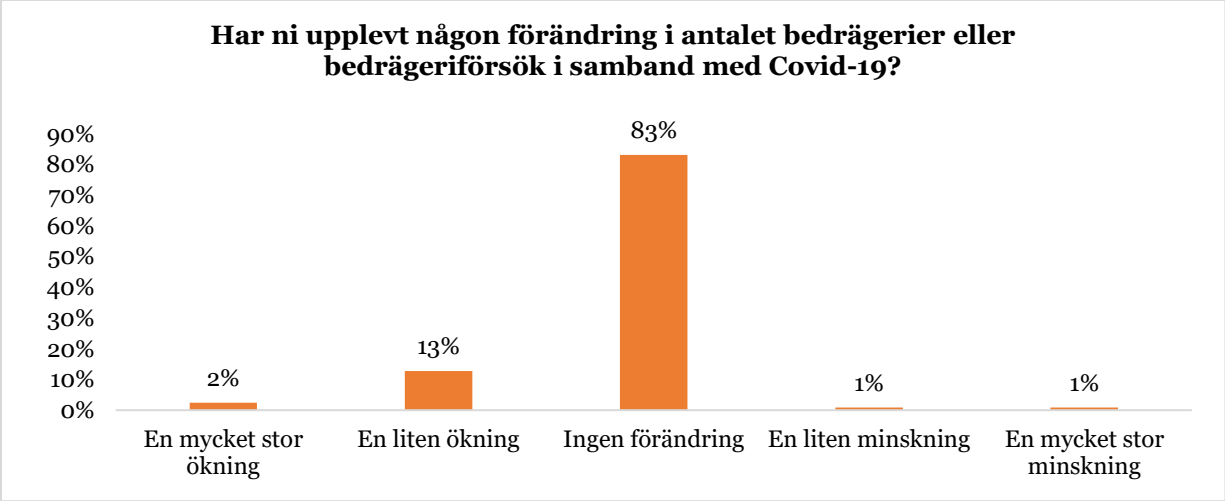
Figur 14: Utnyttjandet av Covid-19 pandemin för att vilseleda

6 procent av handelsföretagen uppger att de har utsatts för coronarelaterade bedrägerier. Resultatet ligger i linje med den information Svensk Handel kontinuerligt hämtar in gällande utsattheten för brott hos våra medlemmar.

I början av pandemin spreds det falsk information om smittan och det skapades hemsidor rörande Covid-19 som var infekterade med olika typer av skadlig kod (malware). Vissa hemsidor skapades för att stjäla lösenord och inloggningsuppgifter medan andra syftade till att infektera datorer med skadlig kod.

I början av sommaren fick Svensk Handel Säkerhetscenter in rapporter om bedragare som utnyttjade det faktum att många företag började rekommendera sina anställda att arbeta hemifrån. Bland annat skickades skräddarsydda meddelanden ut till medarbetare inom olika företag med uppdaterade ”arbeta hemma-instruktioner” som innehöll virus.

Parallellt med detta ökade antalet anmälningar rörande bluffakturor och vilseledande avtal, något som fortfarande ligger på en väldigt hög nivå.



Figur 15: Pandemins påverkan på den IT-relaterade brottsligheten

Företagen fick även en fråga rörande huruvida de har upplevt någon förändring av IT-relaterade brott i samband med pandemin. 15 procent svarade att de upplever en ökning av brott.

Sammanfattning och rekommendationer

Utsattheten för IT-relaterade brott är stor hos handelsföretagen. Nästan hälften har utsatts för ett försök eller fullbordat brott det senaste året. Samtidigt är närmare 40 procent oroliga över att drabbas.

Även om bedrägeribrottslighetens explosionsartade ökning under den senaste 10-årsperioden avstannat något är det fortfarande det vanligaste brottet i Sverige idag, och handeln är inget undantag.

Förutom att utsattheten är stor visar undersökningen även att kunskapsnivån kring vad man som företagare kan göra för att minska utsattheten brister. Det är också vanligt att det saknas tydliga rutiner kring hantering av mejl och avvikande betalningsrutiner.

Kontinuerlig utbildning inom företaget är grundläggande för att minska risken för att drabbas. IT-brottsligheten förändras hela tiden och därför måste personalen ständigt uppdateras och påminnas om vilka rutiner som gäller när exempelvis avvikande konto för utbetalning efterfrågas. Utsattheten behöver även avstigmatiseras så att man vågar berätta om man faktiskt klickat på det där mejlet. Konsekvenserna blir många gånger betydligt värre om utsattheten sker i tystnad.

Baserat på undersökningsresultaten kring handelsföretags utsatthet för IT-relaterad brottslighet presenterar Svensk Handel ett antal enkla och effektiva åtgärder för att minska risken för att drabbas av IT-relaterad brottslighet.

Så minskar du risken att drabbas av phishing, smishing och vishing

- Var misstänksam mot meddelanden från okända avsändare eller med konstigt innehåll från tillsynes kända avsändare.
- Om någon ringer upp och du är osäker på uppringarens identitet, lägg på luren eller be att få ringa tillbaka på ett nummer du själv känner till.
- Klicka aldrig på länkar och öppna aldrig filer i mejl från okända avsändare.
- Lämna aldrig ut koder, lösenord eller kontouppgifter till någon.
- Gå aldrig med på att göra banköverföringar eller "virtuella" betalningar till någon du inte känner.

Så minskar du risken att betala in felaktiga fakturor

- Om ditt företag erhåller en faktura som inte är korrekt – bestrid den. I första hand via mejl till företaget. Det räcker inte att bara ignorera den falska fakturan, du måste agera.
- Dokumentera allt: när fakturan inkommit, när och hur du bestridit den etcetera.
- Gör alltid en polisanmälan. Använd gärna Svensk Handel Säkerhetscenter (www.svenskhandel.se/sakerhetscenter/sakerhetsportalen/) eller appen Säkerhetscenter. Den är gratis och öppen för alla företagare.
- Tacka aldrig ja till något via telefon. Be att få alla papper skickade till företaget så ni har möjlighet att läsa igenom allt i lugn och ro.
- Var misstänksamma. Kontrollera nya kunder och leverantörer som kontaktar er. Ställ frågor och gör sökningar på nätet innan ni går vidare med leverans eller betalning.
- Var minst två personer som attesterar kostnader och gör inga utbetalningar under tidspress, detta minskar risken att fel begås.
- Om en säljare uppger att erbjudandet endast är giltigt idag och endast via telefon bör man rimligtvis tänka efter både en och två gånger.

Så minskar du risken att drabbas av VD-bedrägerier

- Vid misstanke bör återkoppling till VD ske via telefon.
- Upprätta rutiner som innebär möjlighet att nå beslutsfattare för extra verifiering, vid betalningar över ett visst belopp, till exempel att kunna motringa för godkännande mot en i förväg upprättad kontaktlista.
- Var observant på avsändarens mejladress. Var även uppmärksam så att domänen stämmer överens med avsändarens mejladress; .se eller .com. Det förekommer rättstavat namn men att domänen är fel.
- Istället för att klicka på ”Svara”, använd ”Vidarebefordra-funktionen” och skriv in eller välj e-postadressen från din kontaktlista till den person som du svarar till. Då undviker du att svara till en falsk e-postadress.

- Var extra vaksam på e-post som är oväntad eller där uppgifter ska ändras mot vad det brukar vara.
- Tänk på vilken information som presenteras på företagets hemsida. Här finns underlag för bedragaren att använda, till exempel bilder och e-postadresser till en rad olika befattningshavare.

Så minskar du risken att drabbas av Skadlig kod – Ransomware

- Håll dina programvaror uppdaterade.
- Ta regelbundet säkerhetskopior på den information du inte kan vara utan.
- Installera brandvägg och antivirusprogram – och aktivera automatiska uppdateringar för både operativsystem och programvaror.
- Koppla aldrig in okända externa enheter i din dator eftersom det kan leda till att ransomware sprids från dessa enheter till din dator.
- Klicka inte på bilagor, reklam och länkar om du är osäker på avsändaren.
- Undvik att surfa på publika nätverk.
- Se över behörigheterna på företaget, alla behöver inte ha åtkomst till allt. Infekteras någon med högre behörighetsgrad (typ adminbehörighet) kan hela nätverket smittas.
- Se även till så att endast godkända applikationer får köras på företagets datorer.

Oavsett på vilket sätt du drabbas så gäller huvudregeln att inte betala. Det finns inte några garantier att problemet försvinner trots betalning och risken finns att återigen drabbas eller att den skadliga programvaran finns kvar.

Du kan besöka www.nomoreransom.org för att kontrollera om din enhet har blivit smittad av ett av de utpressningsvirus för vilka det finns gratis tillgängliga dekrypteringsverktyg.

Tips på hur du säkrar dina lösenord

- Se över vilka tjänster, appar och inloggningar som används i företaget, tänk på att oftast behöver inte alla i företaget ha åtkomst till all information.
- Ha skärmlås på alla företagets datorer, mobiltelefoner och surfplattor.
- Undvik vanliga lösenord, det vill säga enstaka ord, namn eller tangentbordskombinationer.
- Undvik även personliga referenser, ingen ska genom att läsa på lite om dig kunna gissa ditt lösenord.
- Välj ett långt lösenord, minst 12 tecken. Ett tips är att använda sig av meningar.
- Se till att ha unika lösenord för alla tjänster. Genom att ha unika lösenord säkerställer man att ett dataintrång eller slarv någonstans inte drabbar ens andra konton.
- Viktigast är ditt lösenord till mejlen. Det är via mejlkontot vi kan byta och begära nytt lösenord till alla övriga tjänster.
- Spara inte dina lösenord i webbläsaren.
- Byt bara lösenord om du misstänker att det blivit röjt. Byter man lösenord ofta tenderar de att bli svaga.

Om undersökningen

Bedrägeriundersökningen genomfördes mellan den 23 september och den 12 oktober 2020. Enkäten besvarades av totalt 428 medlemsföretag, varav 266 medlemsföretag i Svensk Handel och 162 e-handlare med Svensk Digital Handels certifiering Trygg E-handel.