telenor företag

Nya tider kräver cybersäkra företag

En säkerhetsguide för små- och medelstora företag

Telenor Företag

Alla företag har rätt att känna sig cybersäkra

Cybersäkerheten har blivit en mer prioriterad fråga – både för mindre och större företag. Varje år blir cyberbrottslingarnas metoder mer raffinerade vilket tvingar oss att ständigt utveckla våra skydd för att skapa en solid beredskap.

Kunskapen om vilken skada en hackerattack kan göra är också stor inom näringslivet. En majoritet av företagen bedömer att verksamheten skulle påverkas negativt vid en attack som pågår i minst fem dagar, visar Telenors undersökning. Knappt var femte företag skulle därför kunna tänka sig att betala lösensumma för att få tillbaka kritisk data och system.

Det här visar att allt fler företag har tvingats gå från insikten att ”det där drabbar inte oss” till steget att ta fram en plan för sin cybersäkerhet. I den här guiden tipsar vår säkerhetsexpert Marcus Lundblad om hur du ska skaffa beredskap innan attacken – och hur du bör agera om det värsta inträffar.

Samtidigt som cyberattackerna ökar, ökar också antalet bedrägerier på nätet. Även här ser vi en rad nya metoder som för en ovan kan vara svåra att upptäcka. Därför går vi här även igenom några vanliga bedrägerimetoder och hur du kan skydda dig mot dessa.

Vi på Telenor tycker att alla företag har rätt att känna sig trygga. Därför har vi tagit fram tjänsten Surfa Säkert Företag som vänder sig främst till mindre- och medelstora organisationer. Med tjänsten, som innehåller allt från virus-skydd till surf- och bankskydd, kan du känna dig trygg med att alla företagets enheter har det skydd som krävs för att kunna jobba säkert.

Undersökning:

Endast 4 av 10 svenska företag är förberedda för en hackerattack

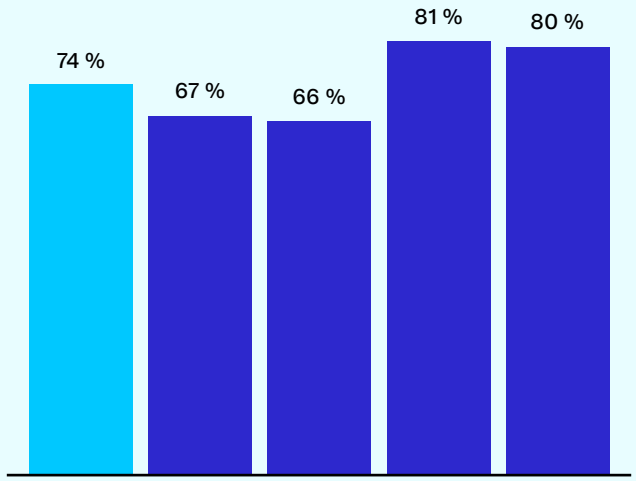
Cybersäkerhetsfrågan blir alltmer aktuell – även för små- och medelstora företag. En majoritet av de anställda har också koll på företagets cybersäkerhet – men endast 4 av 10 företag anser att man är tillräckligt förberedd på en hackerattack, visar en Telenor-undersökning från 2023[1].

Dataintrång, virusattacker, överbelastningsattacker och bedrägerier via e-post. Det är cyberbrotten som svenska mindre- och medelstora organisationer oroar sig för just nu. 9 av 10 företag tycker också att frågan om cybersäkerhet är viktig eller har blivit ännu viktigare det senaste året, visar en undersökning Nepa genomfört på uppdrag av Telenor.

Kännedomen om företagets eget skydd är också stor. Hela 8 av 10 medarbetare säger att man har koll på cybersäkerhetsarbetet. Desto mer oroande är att endast 4 av 10 företag i undersökningen anser att man är väl förberedd för digitala hot. Störst osäkerhet upplever de minsta företagen (upp till 4 anställda). I den kategorin är det knappt en fjärdedel av företagen som känner sig trygga.

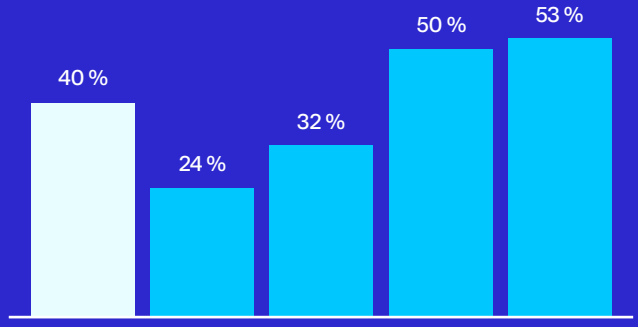
En majoritet (56 procent) av företagen uppger också att en hackerattack skulle kunna orsaka en affärskritisk skada med till exempel pausad verksamhet under en period. Knappt var femte företag skulle också kunna betala en lösensumma för att återfå kontrollen till kritisk data och system.

Drygt 7 av 10 säger att företaget har hög kännedom kring cybersäkerhet



Q: Generellt sett, hur stor kännedom skulle du säga det är kring cybersäkerhet i den verksamhet där du arbetar?

Men endast 40 procent anser att deras företag är väl förberett



Q: I vilken utsträckning anser du att ditt företag är förberett för digitala hot?

1: Telenors säkerhetsundersökning, 2023

Här är de vanligaste cyberbrotten – och så skyddar du ditt företag

Hotbilden mot företag och organisationer har förändrats. Medierna rapporterar nästan dagligen om företag som har drabbats av cyberattacker eller bedrägerier, vilket gör att ämnet är mer aktuellt än någonsin. Men hur går de vanliga cyberbrotten till egentligen? Och hur kan företag skydda sig?

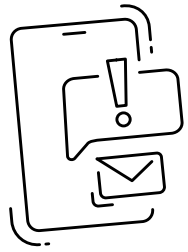
När Telenor ställde frågan till svenska mindre och medelstora organisationer (0-249 anställda) visade det sig att det vanligaste cyberbrottet som flest hade blivit utsatta för var bedrägeriförsök via e-post, 59 procent hade drabbats av detta. Näst vanligast var virusattacker (44 procent). Efter det bedrägeriförsök via SMS (40 procent), social manipulering (32 procent), dataintrång (31 procent), överbelastningsattacker (31 procent), befogenhets-bedrägeri (30 procent) och ransomware/utpressning (26 procent).

Det finns med andra ord många olika typer av cyberbrott som kan drabba ett företag. Tillvägagångssätten skiljer sig också, precis som förövarens syfte med attacken.

I vissa fall kan angriparen vara ute efter känslig information, alternativt vilja stjäla data för att sedan kunna kräva en lösensumma från företaget som angripits, så kallad Ransomware. I andra fall kan syftet vara ett regelrätt sabotage där angriparen endast är ute efter att såra det drabbade företagets verksamhet.

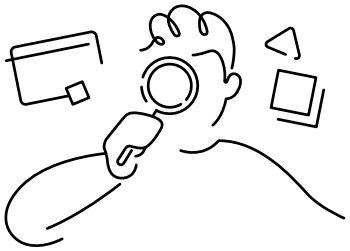
Här är de vanligaste cyberbrotten riktade mot små och medelstora företag och vad dessa innebär:

Bedrägeri via e-post eller SMS (phishing/smishing)



Virusattacker

Social manipulering



Bedrägeri via e-post eller SMS (phishing/smishing)

Vad är det?

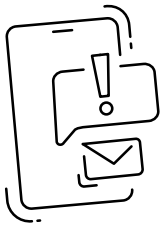
Bedrägeriformen phishing, även kallat nätfiske, har nog de flesta hört talas om och kanske även har egen erfarenhet av. Metoden innebär att förövaren fiskar efter privat information, så som bankkortsuppgifter eller annan företagskritisk information, genom att till exempel få dig att klicka på en länk i ett mejl.

Vid smishing däremot, görs bedrägeriförsöket i stället via ett SMS till din mobiltelefon. Metoden, vars namn är en kombination av SMS och phishing, har de senaste åren blivit alltmer vanlig. Många är idag medvetna om riskerna med att klicka på en länk i ett mejl med okänd avsändare, när det kommer till våra mobiltelefoner tenderar vi dock att vara mer oförsiktiga. Detta gör bluff-sms, eller smishing, till ett extra stort hot för både företag och privatpersoner.

Hur skyddar man sig?

Det bästa sättet att skydda sig mot den här typen av bedrägerier är att alltid tänka till en gång extra innan du klickar på en länk. Felstavningar, brådskande uppmaningar eller erbjudanden som verkar för bra för att vara sanna bör ses som varningstecken.

Och om du skulle drabbas – polisanmäl och se till att varna andra, kollegor eller vänner i din omgivning. Det är så vi kan få stopp på den här typen av brott.



Virusattacker

Vad är det?

Virusattacker, eller riktade attacker, innebär antingen att cyberbrottslingar är ute efter att smitta så många datorer som möjligt med skadligt virus, alternativt att man är ute efter att smitta nätverket hos ett enda företag eller en enda organisation som är målet för attacken.

Vilka har störst risk att drabbas?

Den här typen av attacker är ofta riktade mot ett företag som hanterar eller lagrar information som kan utnyttjas av brottslingen, exempelvis värdefull information om kunder, kunddatabaser, ekonomisk information eller teknisk data.

Hur skyddar man sig?

Ett sätt att skydda sig mot den här typen av attacker är att vara noga med att uppdatera sina program regelbundet. Ett annat är att skaffa ett så kallat VPN, det vill säga ett privat nätverk som krypterar informationen som delas i nätverket. VPN-anslutning både underlättar kommunikation mellan medarbetare som arbetar från olika platser samtidigt som det minimerar riskerna vid en eventuell attack.

Social manipulering

Vad är det?

Bedrägeri genom social manipulation, så kallad social engineering, är metoder för att manipulera personer eller företag till att utföra olika handlingar, ofta med syftet att komma åt företagets pengar. Det kan exempelvis röra sig om en person som utger sig för att komma från en myndighet eller en bank och som på olika sätt vill lura till sig uppgifter för att komma åt ett bankkonto, så kallat befogenhetsbedrägeri.

Hur går det till?

Metoden utnyttjar ofta människors förtroende för auktoriteter eller känslan av att vara utvald då det kan få oss att lämna ut information som vi vet att vi egentligen borde skydda.

Hur skyddar man sig bäst?

Ett bra sätt att skydda sig mot detta är att ha tydliga riktlinjer för vilka uppgifter man lämnar ut till en extern part. Känner du dig det minsta osäker: Ta kontakt med myndigheten eller banken för att undersöka om informationen går att lita på.

Om det är försent och du redan har drabbats, polisanmäl händelsen och kontakta din bank så att du får hjälp att skydda ditt konto och kan stoppa eventuella överföringar från ditt konto.

Har ditt företag utsatts för digitala attacker?

Telenors undersökning från 2023 visar att digitala attacker och cyberbrott är vanligare än vad man kan tro. Undersökningen visar exempelvis att nästan sex av tio av de tillfrågade respondenterna har utsatts för bedrägeriförsök via e-post.

40 %	Bedrägeriförsök via SMS	32 %	Social manipulering
59 %	Bedrägeriförsök via e-post	31 %	Överbelastningsattacker
26 %	Ransomware/utpressning	44 %	Virusattacker
30 %	Befogenhetsbedrägeri	31 %	Annat dataintrång

Q: Har företaget du arbetar för utsatts för någon av följande digitala attacker under de senaste 12 månaderna?

Säkerhetsordlistan:

Här har vi samlat några vanliga begrepp och ord som kan vara bra att känna till för att öka din nätsäkerhet.

Befogenhetsbedrägeri

En typ av bedrägeri där bedragaren utger sig för att vara polis, banktjänsteman eller annan auktoritet. Om offret inte genomskådar lögnen kan personen till exempel luras att lämna ifrån sig inloggningsuppgifter eller att använda e-legitimiation som ger bedragaren tillgång till personens bankuppgifter eller annan känslig information. Befogenhetsbedrägeri är en form av social manipulering.

Romansbedrägerier

Ett bedrägeri där någon använder en fejkad profil för att imitera en person, till exempel via dejtingappar. Syftet är att lura av offret pengar eller känslig information.

Cracker

En person som hackar företag eller individer på ett olagligt sätt för att orsaka skador eller tjäna pengar.

Etisk hackare

En person som hackar lagligt på uppdrag av systemägaren. Den etiska hackerns främsta uppgift är att hitta sårbarheter i systemet för att göra det mer motståndskraftigt för skadliga hackare.

Hacker

En person med teknisk förmåga som använder sin kompetens till att lösa problem, hitta genvägar eller säkerhetsluckor inom ett visst område. Ofta förknippat med datorprogrammering.

Hacktivist

En hackare som agerar på egen hand eller i grupp. Syftet är ofta att främja ett politiskt eller ideologiskt budskap.

Id-kapning

Ett bedrägeri där dina personuppgifter olovligen används för att till exempel ansöka om lån, teckna avtal eller köpa produkter.

Phishing

Ett samlingsbegrepp för olika typer av social manipulation. Phishing betyder att bedragaren ”fiskar” efter känslig information (som inloggnings-uppgifter eller betalkortsinformation). Bedragaren kan till exempel försöka få tillgång till ditt Bank-ID.

Ransomware

En typ av skadlig kod som låser eller krypterar din dator så att du blockeras från att använda den. Målet med viruset är att offret ska betala en lösensumma (ransom) för att återfå informationen eller programvaran.

Smishing

Samma sak som phishing, men här sker det via en länk i ett sms som du luras klicka på. Precis som phishing handlar det om att ”fiska” efter personlig- eller företagskritisk information.

Trojan

Är ett program som tar sig in via till exempel en bifogad bilaga i ett e-postmeddelande och som sedan ligger dold på datorn. Används för att samla in uppgifter om datorns ägare eller som en del av ett botnät där man går till angrepp mot tredje part.

Vd-bedrägeri

En ny typ av bedrägeri som innebär att bedragare utger sig för att vara ett företags vd. 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.

Vishing

Samma typ av bedrägeri som phishing och smishing, men bedrägeriet sker via telefon där bedragarna ringer och utger sig för att komma från ett seriöst företag eller myndighet. Ordet är en kombination av de engelska termerna voice och phishing.

Säkerhetsexpertens råd:

Så skyddar du ditt företag mot cyberangrepp

Alla vet att det är viktigt – trots det slarvar många företag. Cyberhotet var tidigare en fråga för de största företagen, men gäller numera alla. Här kommer Marcus Lundblad, säkerhetsexpert på Telenor, med sina bästa råd till företag som vill ta tag i sitt säkerhetsarbete.

Förr riktade de cyberkriminella ofta in sig på specifika företag. Nu spelar det mindre roll vilken bransch du verkar i eller storleken på ditt bolag. Alla som inte skyddar sig kommer bli hackade.

– Det handlar snarare om när ditt företag blir drabbat och i vilken utsträckning som det kommer ske. Det här är inte längre en fråga som bara gäller vissa specifika företag, säger Marcus Lundblad, säkerhetsexpert Telenor.

Trots en dyster utveckling finns det en rad åtgärder som ett företag kan göra för att skydda sig. Marcus Lundblad rekommenderar alla företag att börja med att inventera och kartlägga sina risker i befintliga processer och system.

I ett litet- eller medelstort företag är det dessutom viktigt att se till att alla involveras. Alla på företaget bör vara medvetna om vilka risker som finns – och veta hur man hanterar dem.

Den mänskliga faktorn är fortfarande en stor risk. Genom medarbetare som klickar på länkar, ger ut information eller öppnar ett infekterat mail kan hackare enkelt ta sig in i företagets system, säger Marcus Lundblad.

Ett råd för att göra det enkelt för medarbetarna att göra rätt är att komma överens om vilka verktyg ni ska använda – och hålla dessa uppdaterade. Därför är det en bra idé att kontinuerligt ställa frågan inåt organisationen om alla har programmen de behöver. Det minimerar risken att medarbetarna hittar egna lösningar.

Avslutningsvis har Marcus Lundblad ett råd till alla företag som vill jobba proaktivt. Se till att ha en plan för hur ni agerar om det värsta skulle inträffa. Vem tar ansvar för vad? Vem ringer ni? Finns det backup på den data som är mest affärskritisk? Glöm inte bort att öva på era rutiner och utvärdera dessa regelbundet.

Marcus Lundblad
Säkerhetsexpert på Telenor Sverige

Fem råd från säkerhets-experten Marcus Lundblad:

1. Skydda information som är affärskritisk	Se till att användare bara kommer åt bestämda resurser efter en godkännandeprocess och att deras tillgång tas bort igen direkt när uppdraget är slutfört.
2. Använd tvåfaktorsautentisering	Tvåfaktorsautentisering för tillgång till IT-system innebär att du ska uppge ”något du vet” till exempel ditt lösenord och ”något du äger” till exempel din mobiltelefon. När du skrivit ditt lösenord skickas en verifikationskod till dig via SMS och gör det i princip omöjligt för en motståndare att nå företagskritisk information.
3. Var tydlig med vilka IT-system och verktyg som är godkända	Det minskar användarnas benägenhet att använda andra digitala tjänster, så kallad Shadow IT, som kan öka risken för informationsläckor.
4. Gör de anställda till säkerhetsambassadörer	Se till att ha en process för att inhämta risker från hela företaget som sedan hanteras på ledningsnivå. Allt ska upp på bordet och alla bör känna sig delaktiga.
5. Ta fram en plan för vad som sker vid en cyberattack	Identifiera företagskritiska aktiviteter och öva inför en cyberattack. Rollbaserade Table-top-övningar är både roligt och ett kreativt sätt att identifiera problem i befintliga processer.

Skaffa Surfa Säkert Företag:

5 verktyg som ingår i tjänsten

Alla företag ska känna sig säkra. Därför har Telenor tagit fram tjänsten Surfa Säkert Företag som hjälper mindre företag med cybersäkerheten. I tjänsten ingår bland annat surfskydd, bankskydd och virusskydd – till alla företagets enheter.

Vad är Surfa Säkert Företag?

Surfa Säkert Företag är en app som Telenor utvecklat tillsammans med säkerhetsföretaget F-Secure. Den ger ett komplett cyberskydd med realtidsöversikt av dina känsligaste uppgifter. Här är några av verktygen som ingår i tjänsten:

Surf- och bankskydd

Med Mobilt VPN är du skyddad från skadliga och farliga webbsidor. Med ett extra bankskydd skyddar du också dina och företags pengar när du går in på en webbplats för säkra bankärenden.

ID-bevakning dygnet runt

För ökad trygghet kan du i realtid bevaka dina viktigaste och känsligaste uppgifter i realtid – dygnet runt.

Ett skydd för alla enheter

Förenkla det digitala livet för medarbetarna genom att enkelt installera samma skydd på alla enheter. Det ger en trygghet att ni jobbar säkert i hela företaget.

Lösenordshanterare

Genom att lagra dina lösenord är de tillgängliga från valfri enhet med en praktisk lösenordshanterare.

Virusskydd till mobil, surfplatta och dator

Skydda dina enheter mot virus, ransomware och andra skade-program med prisbelönt teknik.

Läs mer om Surfa Säkert här:

Surfa Säkert

telenor företag

Vill du veta mer?

Läs mer om Telenors erbjudande och vad vi kan göra för er på:
telenor.se/foretag/