



Myndigheten för
samhällsskydd
och beredskap

Informationssäkerhet för små företag

Rekommendationer för dig som driver
eget företag med upp till 10 anställda



Informationssäkerhet för små företag

Rekommendationer för dig som driver
eget företag med upp till 10 anställda

Informationssäkerhet för småföretag

Myndigheten för samhällsskydd och beredskap (MSB)

Foto: Shutterstock

Produktion: Advant Produktionsbyrå

Tryck: Danagård Litho

Publikationsnummer: MSB1304

ISBN: 978-91-7383-886-3

Innehåll

Bakgrund	4
Om dokumentet	4
Vad är informationssäkerhet?	4
Varför ska företagsinformation skyddas?	5
Skydda din dator och mobiltelefon	7
Agera säkert på internet och med e-post	7
Installera säkerhetsuppdateringar	8
Gör inloggningen säkrare	8
Skydda din dator mot virus	10
Skydda ditt trådlösa nätverk	11
Grundläggande it-säkerhet – norm och test	11
Skydda din företagsinformation	13
Använd e-tjänster	13
Den viktigaste informationen	14
Skydda ditt företag mot bedrägerier	17
Id-kapning	17
Utpressning	19
Företagskapning	20
Fakturabedrägerier	21

Bakgrund

Den digitala utvecklingen har förändrat nästan alla delar av samhället och påverkar också företagens hantering av sin information. Till stöd för företag finns mängder av it-utrustning, it-program och digitala tjänster för att hantera, lagra och överföra information. Detta skapar möjligheter att arbeta effektivt och kan utveckla företaget, men också risker som du som företagare behöver känna till.

Om dokumentet

I det här dokumentet har vi sammanställt rekommendationer till din hjälp att göra ditt företag bättre rustat att hantera information säkert genom att möta it- och internetrelaterade risker och använda digitaliseringen till din fördel.

Dokumentet är indelad i tre huvudavsnitt:

- Skydda din dator och mobiltelefon
- Skydda din företagsinformation
- Skydda ditt företag och dig som ägare

Vad är informationssäkerhet?

Informationssäkerhet innebär att hantera information så att:

- Endast behöriga personer får ta del av information (konfidentialitet)
- Den alltid går att lita på, inte är manipulerad eller förstörd (riktighet)
- Den alltid finns åtkomlig och användbar när den behövs (tillgänglighet)

Informationssäkerhet är att förstå de risker som finns med att hantera information och att införa de skydd, tekniska åtgärder och rutiner, som behövs.

Varför ska företagsinformation skyddas?

Det blir allt viktigare att ha tillgång till information för att företaget ska fungera utan störningar och avbrott.

Fundera över vilken information som är viktigast för att ditt företag ska fungera och vilka problem som uppstår om någon obehörig kommer åt informationen, om den är felaktig eller att ni på företaget inte kommer åt informationen längre. Att ni på företaget vet vad som är er viktigaste information är nödvändigt för att kunna skydda företagets information på ett effektivt sätt.



Skydda din dator och mobiltelefon

Datorer och mobiltelefoner behöver skyddas från de risker som kan uppstå när de används. Du minskar riskerna genom att införa tekniska skydd och genom att ha säkra arbetssätt.

Agera säkert på internet och med e-post

Hur du och dina anställda agerar på internet är avgörande för hur väl företagets information skyddas. Besök bara webbplatser du behöver för att driva företaget och undvik webbplatser med oseriöst innehåll.

Lämna bara ut bankkortsuppgifter vid köp på webbplatser hos företag som du litar på och som har säkra betalningssätt för internet-handel. Prata med din bank om det går att få kortet automatiskt stängt för köp på internet, men med möjlighet att lätt öppna funktionen vid behov.

Var uppmärksam på e-post där det finns länkar som du uppmanas klicka på eftersom det kan leda till att skadlig kod installeras på din dator. E-posten ser ofta ut att komma från seriösa avsändare som du förväntas få meddelanden från såsom myndigheter eller banker. Undvik att använda publika nät eftersom det finns risk att någon obehörig kommer åt din information. Du kan skydda dig genom att använda VPN eller genom att koppla upp dig via din mobil.

REKOMMENDATIONER

- Besök inte oseriösa webbplatser och tänk efter innan du klickar på länkar eller laddar ner filer.
- Ha bra rutiner för köp på internet.
- Tänk efter och granska kritiskt e-post innan du klickar på en länk eller öppnar en fil, även från tillsynes kända avsändare.
- Undvik att använda publika nät.

Installera säkerhetsuppdateringar

Tillverkare av datorer och mobiler skickar regelbundet ut säkerhetsuppdateringar. Dessa bör alltid installeras direkt. Säkerhetsuppdateringarna innehåller viktiga förbättringar som hjälper till att skydda utrustningen.

REKOMMENDATIONER

- Acceptera alltid automatiska uppdateringar från tillverkaren av din dator och mobil. Kontrollera att funktionen för automatiska uppdateringar är aktiverad.
- Uppdatera datorn, programvarorna, mobilen och apparna med tillverkarnas senaste säkerhetsuppdateringar direkt.

Gör inloggningen säkrare

För att ingen annan ska kunna komma åt din information behöver lösenorden för dina konton exempelvis e-post, molntjänster och andra digitala tjänster vara starka. Många leverantörer har egna regler för hur du ska konstruera lösenord, men om du har möjlighet att bestämma lösenordet, välj alltid ett starkt lösenord. Ett starkt lösenord är en kombination av olika bokstäver, tecken och siffror som är tillräckligt långt. Använd inte vanliga ord eller något som kan kopplas till dig personligen till exempel barnens namn eller personnummer.

En lösenordshanterare, en programvara eller tjänst som skapar och lagrar starka lösenord kan vara en stor hjälp om du har många lösenord att hålla reda på. I lösenordshanteraren samlar du alla dina lösenord krypterade och oläsliga. Då behöver du bara komma ihåg ett starkt lösenord, det till lösenordshanteraren.

Många tjänster erbjuder tvåfaktorsinloggning. Det betyder att du fyller i en engångskod vid inloggningen, utöver ditt lösenord. Engångskoden skickas till dig via SMS, eller skapas i en app som du installerar på mobiltelefonen.

Om du vill återställa ett lösenord för att du glömt eller tappat bort det skickas vanligtvis ett meddelande om återställning av lösenordet till din e-postadress. Det är därför viktigt att just e-postkontot skyddas med ett unikt och starkt lösenord. Ta reda på om din e-posttjänst erbjuder tvåfaktorsinloggning och använd i så fall det.

REKOMMENDATIONER

- Aktivera och använd tvåfaktorsinloggning med engångskoder om det erbjuds.
- Använd alltid olika lösenord för olika konton.
- Lämna inte ut lösenord eller koder till någon.
- Se till att alla medarbetare har en egen inloggning, konto med eget användarnamn.
- Skapa starka lösenord genom att till exempel sätta ihop tre slumpmässiga ord tillsammans med siffror, specialtecken samt stora och små bokstäver. Använd långa lösenord, minst 12 tecken.
- Använd en lösenordshanterare om du har många lösenord att hålla rätt på.

Skydda din dator mot virus

Datorvirus, som exempelvis utpressningsvirus, kan orsaka stora problem för ditt företag. Därför är det viktigt att skydda företagets dator och mobil från att smittas. Datorns och mobilens inbyggda säkerhetsfunktioner ger ett grundläggande skydd men skyddet är ofta inte tillräckligt.

Installera ett antivirusprogram som kompletterar grundskyddet mot datorvirus. Använd också en brandvägg för att minska risken att någon för dig okänd kopplar upp sig mot din it-utrustning via internet. Det finns flera olika leverantörer av skydd mot skadlig kod och många av dessa program erbjuder också brandväggsfunktion. Har du ingen egen brandvägg i ditt nätverk är det ett bra alternativ. Din internetleverantör erbjuder ofta också ett brandvägsskydd.

Var restriktiv med vilka program och appar du laddar ner till din dator eller mobiltelefon. Installera bara program och appar från välkända leverantörer. Ladda aldrig ner piratkopierade program eftersom de kan innehålla skadlig kod.

Även om du har antivirusprogram och brandvägg är det viktigt att inte klicka på länkar och bifogade filer för att uppnå ett bra skydd.

REKOMMENDATIONER

- Installera antivirusprogram på företagets datorer och mobiltelefoner.
- Installera brandvägg för att skydda datorer.
- Installera endast de programvaror som är absolut nödvändiga för företagets verksamhet och endast från leverantörer du litar på.
- Installera endast appar från officiella appbutiker såsom Google Play och Apple App Store på mobilen.
- Installera aldrig piratkopierad programvara.
- Tänk efter och granska kritiskt e-post innan du klickar på en länk eller öppnar en fil, även från tillsynes kända avsändare.

Skydda ditt trådlösa nätverk

Ett trådlöst nätverk (WiFi) gör det möjligt för er att arbeta mer flexibelt på företaget. Det krävs inte dyr utrustning men den behöver installeras så att den skyddar företagets information tillräckligt.

REKOMMENDATIONER

- Välj utrustning med brandväggsfunktion och aktivera den.
- Byt leverantörens lösenord för att administrera utrustningen till ett starkt lösenord.
- Välj att kryptera det trådlösa nätverket med WPA2.
- Om ni erbjuder era gäster tillgång till nätverk skapa ett separat nätverk för detta och begränsa det så att gästerna enbart kan nå internet.

Grundläggande it-säkerhet – norm och test

MSB ger i samarbete med Stöldskyddsföreningen, SSF, ut en norm som riktar sig främst till små och medelstora företag som är i behov av praktiska åtgärder för att skydda sin information. Normen, Basnivå – grundläggande it-säkerhet, ska fungera som ett första steg i företagets arbete att möta it-risker kopplat till informationshantering. Företag som uppfyller kraven i normen kan certifiera sig enligt basnivån. På sidan www.ssfcybersakerhet.se kan du testa företagets it-säkerhet.



Skydda din företagsinformation

Använd e-tjänster

En e-tjänst kan användas för att utföra vissa ärenden med hjälp av dator eller mobiltelefon. Många myndigheter erbjuder e-tjänster där företaget kan sköta sina myndighetskontakter. Det finns också privatägda e-tjänster där även privata bolag kan dela information.

Skaffa en säker digital brevlåda via www.minameddelanden.se. Genom en digital brevlåda kan du till exempel ta emot, läsa och samla företagets myndighetspost i en säker digital brevlåda. För enskild firma väljer man en privat digital brevlåda. Inga obehöriga kan läsa dina meddelanden eftersom inloggning sker med e-legitimation som exempelvis BankID. Tjänsten är gratis.

På webbplatsen verksamt.se samlar myndigheterna Bolagsverket, Skatteverket, Arbetsförmedlingen och Tillväxtverket information om och ger tillgång till flera e-tjänster som du har nytta av.

REKOMMENDATIONER

- Använd e-tjänster där det erbjuds.
- Använd en säker digital brevlåda.
- Besök www.verksamt.se regelbundet. E-tjänsterna utökas och förbättras med jämna mellanrum.



Den viktigaste informationen

Företagets viktigaste information är sådan information som du måste ha tillgänglig för att driva företaget. Vad som är viktig information för ditt företag vet bara ni, men det kan till exempel vara företagets bokföring, affärsinformation, kunders information, kundregister eller utvecklingsplaner. Tänk även igenom hur beroende ni är av internet för att kunna fungera och hur länge ni klarar er utan anslutning.

En enkel åtgärd för att skydda företagets information får ni när du och dina medarbetare skiljer mellan vad som är företagets information och vad som är privat information.

Är ni flera som arbetar på företaget kan det vara bra att skriva ner hur ni ska arbeta för att skydda information till exempel vilka som ska ha konton i olika it-system, hur ofta ni gör säkerhetskopiering eller rutiner för att göra köp på internet. Dessutom kan ni behöva rutiner för hur ni ska agera om ni blir av med en dator och behöver få nya inloggningsuppgifter för att få åtkomst till information i tjänster från en annan dator.

Säkerhetskopiering

Information kan gå förlorad om den bara sparas på ett ställe. Ta för vana att regelbundet ta en säkerhetskopia av den information du har på datorn. Använd en molntjänst, extern lagringstjänst eller en extern hårddisk för att lagra säkerhetskopian. Tänk på att skydda säkerhetskopian genom ett starkt lösenord till molntjänsten eller att den externa hårddisken kopplas bort direkt efter säkerhetskopieringen och förvaras inlåst.

Molntjänster

Att använda molntjänster kan underlätta för dig som företagare. Innan du använder dem är det viktigt att göra en överlagd bedömning av för- och nackdelar.

För att kunna göra den bedömningen behöver ni veta var molntjänsten eller annan lagringstjänst lagrar informationen och att leverantören uppfyller de krav som dataskyddslagen (GDPR) ställer på hantering av personuppgifter. Mer information om hur personuppgifter ska hanteras finns på www.verksamst.se och hos Datainspektionen, www.datainspektionen.se.

REKOMMENDATIONER

- Skilj på när du agerar som företagare eller medarbetare på företaget och när du är privatperson.
- Använd inte företagets dator, telefon och it-konton till exempel e-post och molntjänster för privata ändamål.
- Tillåter företaget att dator och telefon används privat är det extra viktigt att skilja privat information från företagets information.
- Dokumentera, om det behövs, rutiner som beskriver hur ni på företaget ska hantera er information säkert.
- Ta reda på var företagets viktigaste information lagras.
- Fundera över hur länge ditt företag klarar sig utan anslutning till internet.
- Ta reda på hur ni får nya inloggningsuppgifter till olika tjänster.



Skydda ditt företag mot bedrägerier

Bedrägerier är något som har ökat de senaste åren. För att skydda dig som företagare och privatperson mot bedrägerier är det viktigt att hantera personlig information om dig själv och information om ditt företag på ett sätt som minskar risken att bli utsatt för bedrägerier.

I det här avsnittet får du veta mer om:

- Id-kapning
- Utpressningsvirus
- Företagskapning
- Fakturabedrägerier

Id-kapning

Att få sin identitet kapad innebär att någon använder ditt personnummer och andra identitetsuppgifter för att till exempel ta lån, teckna abonnemang eller köpa saker. Det vanligaste sättet att upptäcka att du drabbats av identitetsintrång är att du får fakturor eller besked om kreditupplysningar som du inte känner igen.

Om du blivit utsatt för id-kapning får du lägga ned mycket tid på att försöka stoppa den fortsatta användningen av identitetsuppgifterna och lösa alla praktiska problem som uppstått. Du kan få svårigheter med att få krediter eller bli föremål för en spärr på vissa köp- eller sajter. Du kan också bli krävd på betalning för krediter och för varor som beställts och hämtats ut av andra.

REKOMMENDATIONER

- Lämna inte ut personliga uppgifter utan att vara säker på mottagarens avsikter.
- Använd en digital brevlåda även för dig som privatperson. Alla ändringsbekräftelser eller liknande får du information om i den digitala brevlådan exempelvis om någon avser att kapa din identitet och en kreditupplysning gjorts.
- Kontakta din bank och fråga vad du kan göra för att skydda dig mot bankkortsbedrägerier.
- Anmäl hos Skatteverket att du endast ska kunna göra en adressändring med hjälp av e-legitimation. Då minskar risken att någon omdirigerar din post till en annan adress och du inte upptäcker bedrägeriet.
- Aktivera adresslåset hos Adressändring, www.adressandring.se.
- Förvara pass, ID-handlingar och bankkort på ett säkert sätt.
- Lämna aldrig ut uppgifter om din e-legitimation (till exempel BankID eller bankdosa) och logga aldrig in någonstans på någon annans begäran.

Om du drabbas – gör så här

Om någon obehörig har tagit kreditupplysningar i ditt namn eller om du blivit utsatt för ett bedrägeri gör så här:

1. Kontakta det företag som beställt kreditprövningen på dig och berätta att det inte är du som ansökt om krediten.
2. Spärra ditt personnummer med tjänsten Bedrägerispärren, till exempel på www.minuc.se. Bedrägerispärren är ett samarbete mellan fem kreditupplysningsföretag.
3. Kontrollera ifall obehöriga transaktioner skett ifrån dina konton. Ring din bank om du är osäker eller behöver hjälp.
4. Polisanmäl bedrägeriet så snart som möjligt.

Utpressning

Utpressning genom utpressningsvirus, även kallat ransomware, gör informationen på din dator oåtkomlig genom att kryptera filerna. För att få tillbaka informationen i användbart format uppmanas du betala en lösensumma.

Om du råkar ut för utpressningsvirus bör du aldrig betala. Risken är stor att utpressarna ändå inte ger dig det program som behövs för att du ska kunna låsa upp de krypterade filerna.

Det enda du kan göra är att ominstallera datorn. Dokument och filer som inte är säkerhetskopierade går då förlorade.

REKOMMENDATIONER

- Installera alltid de senaste säkerhetsuppdateringarna på din dator och mobiltelefon.
- Tänk efter och granska kritiskt e-post innan du klickar på en länk eller öppnar en fil, även från tillsynes kända avsändare.
- Se till så att du regelbundet gör säkerhetskopior av innehållet i din dator.
- Ta för vana att koppla ur den externa hårddisken där du tar säkerhetskopior och låsa in det när det inte används.

Om du drabbas

1. Gör genast en polisanmälan.
2. Betala inte den lösensumma som utpressaren kräver.
3. Gör en fullständig ominstallation av datorn och lägg sedan tillbaka de filer du behöver från din senaste säkerhetskopia.

Företagskapning

Viss information om ditt företag är offentlig exempelvis uppgifter om styrelsen. Om bedragare lyckas anmäla en ändring till Bolagsverket och registrera en ny firmatecknare får de kontroll över företaget och dess tillgångar. Då kan bedragarna förskingra företagets kapital, ta krediter och beställa varor till andra leveransadresser i företagets namn.

Anmäla ombud hos Skatteverket

Ombud är någon som utför vissa arbetsuppgifter exempelvis deklarationer eller tar del av information för företagets räkning hos Skatteverket. Den som vill ta hjälp av ett ombud väljer vilken behörighet ombudet ska ha, alltså vad ombudet ska kunna göra. Se e-tjänst Ombud och behörigheter, www.skatteverket.se.

REKOMMENDATIONER

- Använd en digital brevlåda. Alla ändringsbekräftelser eller liknande får du information om i den digitala brevlådan exempelvis om firmatecknaren ändrats hos Bolagsverket.
- Var misstänksam om du inte får post du förväntar dig få eller minskad mängd post till företaget.
- Var vaksam och kontrollera dina företagsuppgifter och bankkonton regelbundet så att du snabbt upptäcker om någon obehörig har åtkomst.

Om du drabbas

Om du misstänker att felaktiga uppgifter är registrerade hos Bolagsverket, kontakta Bolagsverket, www.bolagsverket.se.



Fakturabedrägerier

Fakturabedrägerier innebär att någon på felaktiga grunder uppger att du ingått ett avtal med dem. Ofta sker det genom att en person påstår att ni har ingått ett bindande avtal eller genom att vilseleda dig om villkoren i ett avtal.

Det finns olika former av fakturabedrägerier:

- Fakturor som har föregåtts av telefonkontakt och där det påstås att ni har ingått ett avtal trots att det inte är fallet. Det kan också vara så att ni har ingått ett avtal, men inte på de villkor som påstås.
- Helt påhittade krav på ersättning till exempel i form av fakturor eller inkassokrav.
- Erbjudanden som är utformade för att se ut som riktiga fakturor från företag du har ett avtal med.

REKOMMENDATIONER

- Tänk på hur du agerar när en telefonförsäljare ringer.
- Skriv gärna en minnesanteckning om vad du och försäljaren pratat om.
- Be försäljaren upprepa vad ni kommit överens om.
- Om en av dina leverantörer ändrar faktureringsadress eller bankgiro-nummer utan att du informerats, kontakta din leverantör.

Om du drabbas

1. Gör en polisanmälan om du får ett erbjudande som ser ut som en faktura eller om du blir utsatt för påtryckningar att betala en faktura som är felaktig.
2. Betala inte fakturan om du fått den utan att du har beställt något eller om du tycker att den innehåller något annat allvarligt fel. Bluffakturor ska du bestrida. Det innebär att motparten får veta att du motsätter dig betalningen och varför du gör det. Du bör bestrida fakturan snarast möjligt.
3. Läs mer om hur du bestrider bluffakturor på www.kronofogden.se.
4. Polisanmäl bedrägeriet på Polisens e-tjänst, www.polisen.se, telefon 114 14, eller genom att besöka en polisstation.

Om MSB

MSB har i uppgift att samordna arbetet med samhällets informations- och cybersäkerhet. Arbetet berör hela samhället – från organisationer, kommuner och andra myndigheter till företag och enskilda individer. MSB stödjer förebyggande åtgärder och arbetar med att främja ett systematiskt långsiktigt arbete med samhällets informations- och cybersäkerhet på alla nivåer i samhället.

Myndigheten för samhällsskydd och beredskap (MSB)
651 81 Karlstad Tel 0771-240 240 www.msb.se
Publ.nr MSB1304 - november 2018 ISBN 978-91-7383-886-3