Myndigheten för
samhällsskydd
och beredskap

Informationssäkerhet för småföretag

Praktiska råd och rekommendationer

Informationssäkerhet för småföretag

Praktiska råd och rekommendationer

Kjell Kalmelid

Informationssäkerhet för småföretag

Myndigheten för samhällsskydd och beredskap (MSB)

Kontakt: Carl Önne, carl.onne@msb.se

Foto: Shutterstock
Produktion: Advant Produktionsbyrå

Publikationsnummer: MSB1138 - november 2017
ISBN: 978-91-7383-781-1

Innehåll

Bakgrund

Om den här skriften

I den här skriften har vi sammanställt grundläggande praktiska råd och rekommendationer om informationssäkerhet för att göra dig bättre rustad att möta it- och internetrelaterade risker. Råden riktar sig till dig som ska starta eller redan driver ett företag med färre än tio anställda.

Skriften är indelad i tre huvudavsnitt:

- Skydda din dator och mobiltelefon
- Skydda din affärsinformation
- Skydda ditt företag

Vad är informationssäkerhet?

Informationssäkerhet är åtgärder som hindrar att information kommer i fel händer, förvanskas eller förstörs. Det kan till exempel handla om att skydda känsliga uppgifter, att se till att du alltid kan komma åt den information du behöver för att verksamheten ska fungera eller om att hålla dina affärsmöjligheter för dig själv. Att tänka medvetet på informationssäkerheten är alltså ett sätt för dig att slå vakt om både din tid och det kapital du har investerat i ditt företag.

Digitaliseringen har förändrat informationslandskapet

Den pågående digitala utvecklingen har förändrat närapå alla delar av samhället. Det finns nu mängder av olika digitala tjänster för att hantera, lagra och överföra information. Detta skapar både risker och möjligheter som du behöver känna till för att få goda förutsättningar att växa och utvecklas.

Håll alltid isär dina två roller

Innan du börjar läsa skriften får du här det första och viktigaste rådet för att öka ditt företags informationssäkerhet: håll isär dina roller som företagare och privatperson.

Som småföretagare växlar du förmodligen mellan att vara privatperson och företagare både under arbetstid och på fritiden. Kanske ringer det till exempel en kund, följt av ett samtal med en anhörig eller vän. Men du är aldrig företagare och privatperson samtidigt.

Som företagare är du skyldig att hålla isär företagets kassa och pengarna i din privata plånbok. På samma sätt bör du hantera din affärsinformation. Blanda aldrig affärsinformation med privat information! Om du alltid följer dessa rekommendationer lägger du en bra grund för ditt företags informationssäkerhet.

REKOMMENDATIONER

- Håll isär dina roller som företagare och privatperson.
- Håll affärsinformationen skild ifrån din privata information på datorn.
- Om möjligt, investera i en särskild jobbdator, som du inte använder för privata ändamål.

Skydda din dator och mobiltelefon

För att du ska kunna använda internet utan att drabbas av tråkigheter behöver du skydda din dator och mobiltelefon. Du bör också tänka på hur du själv agerar när du använder internet.

Installera säkerhetsuppdateringar

Tillverkaren av din dator och mobil uppmanar dig regelbundet att installera nya säkerhetsuppdateringar. Dessa bör du alltid installera. Säkerhetsuppdateringarna innehåller viktiga förbättringar av säkerheten som hjälper till att skydda din dator och mobil från datorvirus.

REKOMMENDATIONER

- Installera endast de programvaror som är absolut nödvändiga för din verksamhet.
- Installera aldrig piratkopierad programvara på din dator.
- Uppdatera datorn, programvarorna, mobilen och apparna med tillverkarnas senaste säkerhetsuppdateringar, löpande i den takt de kommer.
- Acceptera alltid automatiska uppdateringar från tillverkaren av din dator och mobil. Kontrollera att funktionen för automatiska uppdateringar är aktiverad.
- Installera endast appar från officiella appbutiker såsom Google Play och Apple App Store på mobilen.

Skapa starka lösenord

För att ingen annan ska kunna komma åt dina konton för e-post, molntjänster och sociala nätverk måste dina lösenord vara starka. Många leverantörer har egna regler för hur du ska konstruera lösenorden, men om du har möjlighet att helt fritt bestämma lösenordet bör du alltid välja ett med hög säkerhet.

REKOMMENDATIONER

- Använd aldrig samma lösenord för olika inloggningar, och byt regelbundet lösenord för de viktigaste tjänsterna.
- Skapa ett starkt lösenord genom att sätta ihop tre slumpmässiga ord tillsammans med siffror, specialtecken samt stora och små bokstäver. Lösenordet bör vara minst 12 tecken långt.
- Välj aldrig ett lösenord som kan kopplas till dig, exempelvis bilens registreringsskylt eller barnens personnummer.
- Använd inte vanliga ord som ”sommar” eller vanliga bokstavskombinationer som ”qwerty” (tecken i en följd på tangentbordet).
- Använd en lösenordshanterare, alltså en programvara eller tjänst som skapar och lagrar komplicerade lösenord. Då får du alltid till unika och svårgissade lösenord, samtidigt som du enkelt själv kan komma åt lösenorden.

Skydda din dator mot virus

Datorvirus, som exempelvis utpressningsvirus, kan orsaka stora problem för ditt företag. Därför är det av yttersta vikt att du skyddar din dator och mobil från att smittas. Datorns och mobilens inbyggda säkerhetsfunktioner ger ett grundläggande skydd, men skyddet är tyvärr inte tillräckligt. Den vanligaste orsaken till att drabbas av datorvirus är fortfarande att klicka på länkar och bifogade filer i e-post från okända eller oväntade avsändare.

REKOMMENDATIONER

- Klicka aldrig på länkar som du får i e-post från okända eller oväntade avsändare.
- Öppna inte bifogade filer som du får i e-post från okända eller oväntade avsändare.
- Om du är osäker på vem avsändaren är, låt bli att klicka på länkar och öppna inte bifogade filer.
- Installera antivirusprogram på din dator och mobiltelefon.

Skydda din affärsinformation

Använd e-tjänster

En e-tjänst är en elektronisk tjänst som du kan använda för att göra ärenden med dator eller mobiltelefon. E-tjänster är säkrare än pappershantering, så när det finns en e-tjänst för att sköta kontakter med myndigheter och andra företag bör du använda den.

Med e-tjänsten Mina meddelanden kan du till exempel ta emot, läsa och samla din myndighetspost i en säker digital brevlåda. Inga obehöriga kan läsa dina meddelanden eftersom inloggning sker med e-legitimation som exempelvis BankID. Tjänsten är helt gratis.

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

REKOMMENDATIONER

- Använd e-tjänster när det finns. Det är säkrare än att skicka information på papper.
- Skaffa dig en säker digital brevlåda med e-tjänsten *Mina meddelanden*.
- Besök **verksamt.se** regelbundet. E-tjänsterna utökas och förbättras med jämna mellanrum.

Affärskritisk information

Affärskritisk information är sådan information som du alltid måste ha tillgänglig och som du inte har råd att förlora. Ett exempel är din bokföring och den räkenskapsinformation som hör till den. Även annan information kan vara mer eller mindre kritisk för företagets fortlevnad, som exempelvis kundregister.

Molntjänster

Att använda molntjänster kan underlätta för dig som företagare, men innan du använder dem är det viktigt att du först gör en överlagd bedömning av för- och nackdelarna.

Om du sparar säkerhetskopior av affärkritisk information i ”molnet” förlorar du inte information om du till exempel skulle bli bestulen på din dator. För att vara helt trygg behöver du dock skydda både själva datorn och molntjänsten med starka lösenord. Ett alternativ till säkerhetskopior i molnet är att använda en extern hårddisk.

REKOMMENDATIONER

- Om du använder ett bokföringsprogram, ta reda på var dina data lagras.
- Fundera över om du förvarar affärskritisk information på ett sätt som uppfyller lagens krav, till exempel när det gäller bokföring eller personuppgifter.
- Fundera över hur länge ditt företag klarar sig utan anslutning till internet.
- Fundera över hur ditt företag påverkas om molntjänstleverantören går i konkurs eller får sina servrar hackade.
- Det finns inga rätta eller felaktiga svar på frågorna ovan, men de svar du kommer fram till avgör vilka säkerhetslösningar du bör välja för din affärskritiska information.

OBS! Om du förlorar din dator eller drabbas av utpressningsvirus, är det mycket viktigt att du får tillgång till inloggningsuppgifterna till dina molntjänster. Ta reda på hur olika molntjänstleverantörer gör för att du ska få nya inloggningsuppgifter. Skapa alltid starka lösenord till dina molntjänster om du har möjlighet.

Skydda ditt företag

Bedrägerier

Bedrägerier är något som har ökat de senaste åren. För att skydda dig mot bedrägerier är det viktigt att du har kontroll över hur du hanterar personlig information om dig själv och information om ditt företag. I det här avsnittet får du veta mer om:

- Id-kapning
- Utpressningsvirus
- Företagskapning
- Fakturabedrägerier

Om du följer rekommendationerna nedan minskar du risken att bli utsatt för bedrägerier.

Id-kapning

Att få sin identitet kapad innebär att någon använder ditt personnummer och andra identitetsuppgifter för att t.ex. försöka ta lån, teckna abonnemang eller köpa saker. Det vanligaste sättet att upptäcka att du drabbats av identitetsintrång är att du i din vanliga (eller digitala) brevlåda 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. Det kan vara svårigheter att få krediter eller du kan bli föremål för en spärr på vissa köp- eller säljsajter. Du kan också bli krävd på betalning för varor eller krediter som beställts och hämtats ut av andra.

REKOMMENDATIONER

- Skaffa dig en digital brevlåda. Då får du snabbt en indikation på om någon gör bedrägerier genom att id-kapa dig, eftersom alla ändrings-bekräftelser och liknande skickas dit.
- Kontakta din bank och fråga vilka verktyg de har för att du ska kunna skydda dig mot bankkortsbedrägerier. Bedrägerier med bankkort är den vanligaste typen av bedrägeri.
- 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 exempel kreditupplysningar, till annan adress.
- Aktivera adresslåset hos Adressändring, www.adressandring.se
- Förvara pass och ID-handlingar på ett säkert sätt

Om du drabbas

Följ de här instruktionerna om du får uppgifter om att någon obehörig har tagit kreditupplysningar i ditt namn eller om du blivit utsatt för ett bedrägeri:

- Kontakta det företag som beställt kreditprövningen på dig och berätta att det inte är du som ansökt om krediten.
- Spärra ditt personnummer med tjänsten Bedrägerispärren. Bedrägerispärren är ett samarbete mellan fem kreditupplysningsföretag och är helt kostnadsfri att använda.
- Ring din bank och kontrollera dina konton.
- Polisanmäl bedrägeriet så snart som möjligt.
- Bestrid fakturor som du inte godkänt eller när du blivit vilseledd. På så sätt undviker du inkasso, betalningsanmärkningar och efterföljande åtgärder. Du kan läsa hur du gör för att bestrida fakturor på sista sidan i den här skriften.

Utpressningsvirus

Utpressningsvirus, även kallat ransomware, låser datorer genom att kryptera filer. För att återfå kontrollen kräver gärningsmannen att du betalar en lösensumma inom en viss tid genom en online-betalningsmetod.

Om du råkar ut för utpressningsvirus bör du aldrig betala den lösensumma som krävs. Det finns inga garantier för att problemet försvinner trots att du betalar. Risken är stor att utpressarna ändå inte ger dig ”nyckeln” så att du kan låsa upp de krypterade filerna. Du har då inget annat val än att ominstallera datorn från grunden. Dokument och filer som inte är säkerhetskopierade går i så fall förlorade.

REKOMMENDATIONER

- Installera alltid de senaste säkerhetsuppdateringarna på din dator och mobiltelefon.
- Klicka aldrig på länkar som du får i e-post från okända eller oväntade avsändare.
- Öppna inte bifogade filer som du får i e-post från okända eller oväntade avsändare.
- Se till så att du alltid har säkerhetskopior av innehållet på en annan dator eller ett externt minne.

Om du drabbas

- Gör genast en polisanmälan.
- Betala inte den lösensumma som gärningsmannen kräver.
- 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 i styrelsen får de kontroll över företaget och dess tillgångar. Då kan bedragarna förskingra företagets kapital, ta krediter och beställa varor i företagets namn till nya leveransadresser.

REKOMMENDATIONER

- Använd tjänsten Mina meddelanden för att få en säker digital brevlåda. Tjänsten är gratis.
- På Bolagsverkets webbplats kan du snabbt och kostnadsfritt få information om ändringar i ditt företag.
- När Bolagsverket har tagit emot ändringar som rör ditt företag får du snabbt besked via e-post och sms.

Om du drabbas

Om du misstänker att felaktiga uppgifter är registrerade hos Bolagsverket, kontakta Bolagsverket på **0771–670 670** eller genom e-post till: **bolagsverket@bolagsverket.se**

Fakturabedrägerier

Fakturabedrägerier innebär att någon som uppträder som en säljare eller marknadsförare skapar en felaktig föreställning om att någon annan är betalningsskyldig för något. Ofta sker det genom att personen medvetet felaktigt påstår att ni har ingått ett bindande avtal, eller genom att vilseleda dig om innehållet 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, till exempel i form av fakturor eller inkassokrav.
- Erbjudanden som är utformade för att se ut som riktiga fakturor.

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 du drabbas

- Gör en polisanmälan om du får en faktura som du uppfattar som vilseledande, eller om du blir utsatt för påtryckningar att betala fakturan.
- 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 nämligen bestrida. Det innebär att motparten får veta att du motsätter dig betalningen och varför du gör det. Du bör bestrida fakturan snarast möjligt.
- Läs mer om hur du bestrider bluffakturor på: **www.bestrid.nu**
- Polisanmäl fakturabedrägeriet på telefon: **114 14** eller genom att besöka en polisstation.

Få hjälp med att driva ditt företag

Anlita en auktoriserad redovisningskonsult

Överväg att anlita en auktoriserad redovisningskonsult för att få hjälp med att hantera ekonomin i ditt företag. Redovisningskonsulter jobbar dagligen med informationssäkerhet i olika avseenden. De är till exempel experter på att hantera din räkenskapsinformation på ett säkert sätt och i enlighet med kraven i bokföringslagen.

Sök på ”redovisningskonsulter” eller ”auktoriserade redovisningskonsulter” på internet.

Anlita ett ombud

Ett ombud kan via Skatteverkets e-tjänster utföra vissa ärenden eller ta del av information för ditt företags eller enskilda firmas räkning. Olika typer av ombud har olika behörighet. Den som vill ha ett ombud kan använda Skatteverkets e-tjänst Ombud och behörigheter, se **www.skatteverket.se**

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 MSB1138 - november 2017 ISBN 978-91-7383-781-1