Myndigheten för samhällsskydd och beredskap

# Alla kan bidra till Sveriges cybersäkerhet. Du också!

## TÄNK SÄKERT

# Så skyddar du ditt företag

Det är lätt hänt att värdefull information hamnar i fel händer. Det tråkiga är att konsekvenserna kan bli allvarliga. Genom att tänka på hur du och dina medarbetare agerar på nätet och genom enkla åtgärder och rutiner så förbättras säkerheten avsevärt.

## Checklista för att skydda dig mot nätfiske

Här följer tips kring vad du och dina medarbetare kan tänka på innan ni klickar på en bifogad fil eller länk.

INNAN du klickar på en länk eller öppnar en bilaga, ställ följande frågor till dig själv:

- ☐ Är det oväntat att jag får ett mejl från den personen/avsändaren vid den här tidpunkten?
- ☐ Är det en faktura eller ett dokument i mejlet som jag inte har förväntat mig?
- ☐ Uppmanas jag agera snabbt, är det bråttom, ett tidsbegränsat erbjudande eller för bra för att vara sant?
- ☐ Tycker jag att språket, tonfallet, enstaka ordval avviker från hur avsändaren brukar skriva eller finns det enstaka stavfel?
- ☐ Uppmanas jag att lämna ifrån mig lösenord eller kort- eller kontonummer?
- ☐ Ser den bifogade bilagan eller länken konstig ut? Ser den ut att komma från en känd aktör?

Om du svarar **ja** på någon av ovanstående frågor bör du kontrollera avsändaren. Kontakta dem via andra kanaler och kontrollera om de verkligen har försökt att kontakta dig.

## Checklista för att skydda dig mot skadlig kod och ransomware

Här följer tips kring hur du och dina medarbetare kan förebygga att någon obehörig gör företagets information otillgänglig.

Ett exempel på skadlig kod är **utpressningsvirus, ransomware**. Det är en programvara som låser datorer och mobila enheter eller krypterar filer. För att återfå kontrollen begär avsändaren att du betalar en lösensumma.

Minska risken att drabbas:

- ☐ Klicka inte på länkar eller öppna bilagor i mejl och sms innan du granskat det noga. Följ checklistan ”Skydda dig mot nätfiske”.
- ☐ Uppdatera dina programvaror så fort du uppmanas säkerhetsuppdatera.
- ☐ När digitala enheter, såsom telefoner eller datorer, är för gamla för att få säkerhetsuppdateringar, byt ut dem eller koppla ner dem från internet.
- ☐ Installera antivirusprogram på dina digitala enheter.
- ☐ Säkerhetskopiera ofta. Följ checklistan ”Säkerhetskopiera din information”.
- ☐ Installera endast program eller appar på datorer eller telefoner som kommer från en säker källa.
- ☐ Var vaksam när du besöker webbplatser där du inte är helt säker på vem som står bakom informationen.
- ☐ Följ inga uppmaningar från personer du inte känner igen, inte heller på sociala medier.
- ☐ Var uppmärksam på att det verkligen är personen du känner som är bakom en förfrågan. Är du osäker kontakta personen på annat sätt och fråga.

Om företaget drabbats:

- ☐ Begränsa och minimera skadan av ett pågående angrepp genom att stänga av uppkopplingen mot internet, ”dra ut sladden”.
- ☐ Betala aldrig någon lösensumma. Att betala är ingen garanti för att företaget får tillbaka informationen igen, tvärtom ökar det risken avsevärt att företaget blir angripen igen.
- ☐ Polisanmäl händelsen.
- ☐ Ta hjälp av de resurser som finns tillgängliga hos organisationen nomoreransom.org
- ☐ Kontakta CERT-SE för att få råd och stöd i att hantera it-incidenten och förebygga att den händer igen. CERT-SE kan även agera för att varna andra som har eller riskerar att drabbas av liknande angrepp.

## Checklista för att säkra dina lösenord

Här nedan följer tips på vad du och dina medarbetare kan göra för att förebygga att någon obehörig kan få tillgång till företagets information och olika användarkonton.

- ☐ Se över vilka tjänster, inloggningar och appar som används i företaget.
- ☐ Oftast behöver inte alla i företaget ha åtkomst till all information. Därför är det viktigt att begränsa behörigheterna.
- ☐ Använd unika lösenord för olika tjänster, framför allt de viktigaste tjänsterna.
- ☐ Använd långa lösenord, gärna en lösenordsfras som är lätt att minnas med många tecken och stor teckenvariation.

- ☐ Lämna aldrig ut personliga lösenord. Se till att medarbetare använder starka lösenord till egna personliga inloggningar (konton).
- ☐ Använd om möjligt lösenordshanterare som hjälper er att skapa och hantera starka lösenord.
- ☐ Ha skärmlås på alla företagets datorer, mobiltelefoner och surfplattor.
- ☐ Aktivera flerfaktorsautentisering, även kallad tvåstegsverifiering där det går, dvs två eller flera identifieringssätt.
- ☐ Skydda administratörskonton och andra konton med höga behörigheter lite extra, de bör alltid skyddas med flerfaktorsautentisering.

## Checklista för säker användning av e-legitimation

Här följer tips om hur du kan hantera din e-legitimation på ett säkert sätt.

- ☐ Låt aldrig någon annan logga in med din e-legitimation åt dig.
- ☐ Logga aldrig in med din e-legitimation på uppmaning av någon annan. Detta gäller även om personen säger sig vara från banken, ett annat företag eller en myndighet och kan uppge detaljerade uppgifter om dig eller företaget.
- ☐ Lämna aldrig ut din e-legitimation eller koder från bankdosan till någon annan som kontaktar dig.
- ☐ Läs alltid vad du signerar i e-legitimations-appen innan du skriver under med din kod. Är du osäker kan du välja att avbryta.

## Checklista för att säkra företagets viktigaste information

Här nedan följer tips på vad du kan göra för att undvika att företagets it-utrustning används för att komma åt värdefull information eller att företaget drabbas av avbrott när information försvinner eller inte är tillgänglig.

### Trådlösa nätverk

- ☐ Har företaget ett trådlöst nätverk **(wifi)** – skydda routern med ett starkt lösenord.
- ☐ Se till att byta lösenordet i samband med installation, med ett starkt och unikt lösenord.
- ☐ Se till att även nätverket eller nätverken har starka och unika lösenord.
- ☐ Se till att routern och andra nätverksenheter får säkerhetsuppdateringar från tillverkaren eller leverantören.
- ☐ Installera ett separat nätverk för besökare som erbjuds wifi-åtkomst.
- ☐ Undvik att använda andras trådlösa nätverk (publika nätverk på exempelvis caféer och hotell). Använd istället mobilens uppkoppling.

### Säkerhetsuppdateringar

- ☐ Tacka ja till säkerhetsuppdateringar av program som är installerade på datorer eller telefoner.
- ☐ Aktivera automatiska säkerhetsuppdateringar på enheter och datorer – glöm inte wifi-routern.
- ☐ Välj leverantörer som ni känner till och litar på när ni köper it-utrustning.
- ☐ Tänk igenom vilka appar som du och dina medarbetare laddar ner och ta regelbundet bort appar som inte används.

## Checklista, tänk på detta när du säkerhetskopierar

Här följer tips om hur du och dina medarbetare kan se till att företagets viktigaste information inte går förlorad.

- ☐ Säkerhetskopiera ofta företagets information som finns på datorer och mobiler.
- ☐ Säkerhetskopiera informationen till exempelvis till en extern hårddisk, USB-minne, databas eller molnet.
- ☐ Testa säkerhetskopian med jämna mellanrum så att ni vet att filerna kan öppnas och att informationen kan återskapas.
- ☐ Gör aktiva val om vilken information som företaget bör spara i molnet eller på extern hårddisk. Fundera över vad som är viktigt att ha kontroll över själv eller vad företaget behöver ha lättillgängligt från olika platser eller enheter.
- ☐ Koppla ur säkerhetskopian från datorerna mellan kopieringarna. Annars kan även den utsättas för virus eller annan skadlig kod.
- ☐ Förvara säkerhetskopian stöld- och brandsäkert.

### Mer information

Läs mer om hur du kan skydda dig på **msb.se**

- Ring **114 14** för att komma i kontakt med polisen.
- Ring **112** vid akuta ärenden.

När vi gemensamt tar ansvar för vår säkerhet på nätet bidrar vi till att stärka hela Sveriges informations- och cybersäkerhet. Skyddar du din egen och företagets viktigaste information blir det svårare att genomföra hackerattacker och cyberangrepp.

Dessa checklistor ger dig tips på hur du som företagare med enkla åtgärder kan skydda dig och din verksamhet och förhindra att din och företagets information hamnar i fel händer.

Denna skrift är en del av en informationskampanj som MSB har fått i uppdrag av regeringen att tillsammans med Polisen genomföra. Den syftar till att öka medvetenheten och kunskapen om digitala sårbarheter och hur man som enskild person och företagare skyddar sig och sitt företag.

**TÄNK SÄKERT**

MSB Myndigheten för samhällsskydd och beredskap

Polisen


651 81 Karlstad Tel 0771-240 240 **www.msb.se**
Tryck: By Wind Produktion: Advant
Publikationsnummer MSB2415 – reviderad september 2024