

# TÄNK SÄKERT

Skydda din viktigaste information.

## Så skyddar du ditt företag

Det är lätt hänt att företagets värdefulla 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 näffiske och skadlig kod

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

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

- Är det oväntat att jag får ett mejl från den personen/avsändaren vid den här tidpunkten?
- 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 enstaka stavfel?
- Uppmanas jag att lämna ifrån mig lösenord eller kort- eller kontonummer eller lösenord?
- 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 via andra kanaler. Kontakta dem och kontrollera om de verkligen har försökt att kontakta dig.



Myndigheten för  
samhällsskydd  
och beredskap



Polisen

## 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 din information och dina användarkonton.

- 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. Därför är det viktigt att begränsa behörigheterna
- Använd starka och olika lösenord för alla tjänster.
- Se till att medarbetare använder starka lösenord till egna personliga inloggningar (konton).
- Använd om möjligt lösenordshanterare.
- Ha skärmlås på alla företagets datorer, mobiltelefoner och surfplattor.

## Checklista för att säkra dina kortuppgifter

Här nedan följer tips kring vad du kan tänka på för att företagets kortuppgifter inte ska hamna i fel händer. Se till att rutinerna är kända och kan förstås av alla berörda.

- Använd bankens säkerhetslösning för företagets bankkort. Spärra för internetköp och öppna kortet när ni avser att handla på nätet.
- Lämna aldrig ut koder eller kortuppgifter till någon som efterfrågar dem i mejl, sms eller telefon.
- Gör aktiva val innan ni tillåter webbsidan eller appen ni handlar på att spara person/företagets- och kortuppgifter.
- Förvara alltid företagets kort säkert
- Spärra kortet och gör en polisanmälan om du förlorat ditt bankkort eller upptäcker att olovliga köp gjorts.



Myndigheten för  
samhällsskydd  
och beredskap



Polisen

## 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

### Säkerhetskopiering

- Säkerhetskopiera regelbundet information på datorer och mobiler, så att ingenting går förloras om något skulle hända med enheterna.
- Säkerhetskopiera till en extern hårddisk eller molnet. Kontrollera att informationen kan återläsas.
- Gör aktiva val 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 som företaget behöver ha lättillgängligt från olika platser eller enheter.

### 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, unikt lösenord.
- Se till att även nätverket eller nätverken har starka unika lösenord.
- Installera ett separat nätverk för besökare som erbjuds wifi-åtkomst.
- Undvik att använda andras trådlösa nätverk (publika nätverk på ex. caféer och hotell). Använd istället mobilens uppkoppling.



Myndigheten för  
samhällsskydd  
och beredskap



Polisen

## Säkerhetsuppdatering

- 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.

### Mer information

Läs mer om hur du kan skydda dig på [msb.se](https://msb.se)

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



Myndigheten för  
samhällsskydd  
och beredskap



Polisen