TÄNK SÄKERT

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 nätfiske 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.

MSB Myndigheten för samhällsskydd och beredskap

Polisen

Checklista för e-legitimation

Här nedan följer tips om hur ni i företaget kan hantera e-legitimationer så att ingen obehörig lurar er.

- ☐ 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 företag eller en myndighet och även om de kan uppge detaljerade uppgifter om dig, medarbetare eller företaget.
- ☐ Läs alltid vad du signerar i applikationen eller på nätet innan du skriver under. Är du osäker kan du välja att avbryta.

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.
- ☐ Oftast behöver inte alla i företaget ha åtkomst till all information. Därför är det viktigt att begränsa behörigheterna.
- ☐ Använd långa lösenord, gärna en lösenordsfras som är lätt att minnas med många tecken och stor teckenvariation.
- ☐ Använd unika lösenord för olika tjänster, framför allt de viktigaste tjänsterna.
- ☐ Lämna aldrig ut dina 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 där det går.

MSB 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.

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.

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.

MSB Myndigheten för samhällsskydd och beredskap
Polisen

Checklista för säkerhetskopiering av information

Här nedan följer tips om hur du och dina medarbetare kan se till att företagets viktiga information inte går förlorad om företaget drabbas av längre avbrott.

- ☐ Säkerhetskopiera ofta och med jämna mellanrum informationen på datorer och mobiler.
- ☐ Säkerhetskopiera till en extern hårddisk, databas eller molnet. Kontrollera 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.

MSB Myndigheten för samhällsskydd och beredskap

Polisen