Stadsbyggnadsförvaltningen
Geografisk information och visualisering

Checklista informationssäkerhet

Att skydda vår information är ett gemensamt arbete. Det handlar om att försvåra för cyberkriminella, hindra information från att nå fel personer och att se till att vi själva har tillgång till rätt information då vi behöver den. Här är en checklista med grundläggande saker som vi alla kan göra i vår vardag för att göra vår digitala miljö säkrare. Ta en titt på den ibland för att se om du kan checka av alla punkter!

Grundsäkerhet

- ☐ Har genomfört alla programvaruuppdateringar
- ☐ Inget viktigt ligger sparat lokalt på datorn
- ☐ Har bara laddat ner appar från pålitliga källor till telefonen
- ☐ Låser skärmen när jag går från datorn
- ☐ Larmar på när jag lämnar kontoret utanför öppettiderna
- ☐ Delar internet från min tjänstetelefon istället för att ansluta till publika nätverk på tåg, caféer och liknande

Lösenord

- ☐ Har valt komplexa lösenord
  Testa gärna att använda en lösenordsfras, alltså en längre mening såsom MinInfoSäkSamordn4reÄrBäst!, i stället för en kortare teckenkombination. Det är lika lätt att komma ihåg, men mycket säkrare.
- ☐ Har olika lösenord på varje ställe
  Om det känns svårt att komma ihåg alla så kan man använda en lösenordshanterare.
- ☐ Inga lösenord finns uppskrivna någonstans där någon annan kan se eller hitta dem

På internet

Var noga med att tänka efter om en hemsida verkar äkta och säker innan du skriver in ett lösenord. Ställ dig frågorna:

- ☐ Är det en sannolik webadress?
- ☐ Är anslutningen säker (börjar med https)?
- ☐ Kom jag till sidan via en länk jag har granskat och litar på?

Mail

- ☐ Är försiktig med vilka meddelanden jag öppnar
- ☐ Klickar aldrig oreflekterat på länkar i mail
- ☐ Öppnar inga okända filer

- ☐ Om jag är det minsta osäker på om ett meddelande är äkta så kontaktar jag den påstådda avsändaren via annan kanal och dubbelkollar
- ☐ Om jag tror att det är ett falskt mail så anmäler jag till supportcenter
  Vidarebefordra mailet till supportcenter så de kan analysera det. Om du har fått många misstänkta bluffmail så ska du istället ringa supportcenter.

Det finns tecken att titta efter för att bedöma om ett mail är skräppost. Ställ dig frågorna:

- ☐ Känner jag avsändaren?
- ☐ Stämmer mailadressen med avsändare och organisation? Ser den ut som en normal mailadress?
- ☐ Brukar personen skicka mail till mig vid den här tidpunkten?
- ☐ Finns det en länk eller bilaga som ser konstig ut?
  Kontrollera länkar genom att hovra över dem (på dator) eller trycka och hålla inne (på mobil)
- ☐ Trycks det på att det är bråttom att agera?
- ☐ Förekommer hot om negativa konsekvenser (t.ex. ”ditt konto spärras om du inte…”)?
- ☐ Frågas det efter känslig data (t.ex. lösenord eller bankinformation) via mail eller på en sida som länkas i mailet?
- ☐ Saknas hälsningsfras eller är den opersonlig (t.ex. ”Kära kund”)?
- ☐ Finns det stavfel och grammatiska fel?
  Texter i bluffmail är ofta översatta med ett översättningsprogram och brukar därför innehålla fel.
- ☐ Är innehållet för bra för att vara sant?

OM NÅGOT HÄNDER

Om du t.ex. tror att du har råkat lämna ut inloggningsuppgifter, klickat på en skadlig länk eller öppnat en misstänkt fil:

- ☐ Om du klickat på något misstänkt, sluta använda den berörda enheten
- ☐ Om möjligt, koppla bort enheten från internet, t.ex. stäng av routern om du är hemma
- ☐ Anmäl till supportcenter på 042-10 50 50
- ☐ Se till att vara redo att uppge stöldmärkningsnummer (står på klisterlapp på enheten) och ev. datornamn (hittas om du trycker på den röda knappen i aktivitetsfältet nere till höger)
- ☐ Ta ev. en bild på skärmen
- ☐ **Anmäl hellre en gång för mycket än en gång för lite!**