

CHECKLISTA INFORMATIONSSÄKERHET

Brandväggar och uppdaterade operativsystem är viktiga för din informationssäkerhet, men skyddar inte mot ett riskfyllt beteende. Din digitala säkerhet handlar också om ditt beteende och din medvetenhet om risker.

- Lämna aldrig din dator obevakad. Behöver du det, så logga alltid ut eller stäng av. Ditt konto är ditt ansvar.
- Se till att din dator, surfplatta och smartphone kräver inloggning (skärmlås) som automatiskt aktiveras.
- Sprid inte ut ditt lösenord genom att skriva upp det i närheten av din dator eller annan lättillgänglig plats.
- Låna inte ut ditt konto.
- Lämna aldrig ut ditt lösenord eller dina kontouppgifter till andra.
- Klicka inte på länkar och bilder som du inte vet vad de kommer ifrån. Klicka aldrig OK utan att läsa vad du godkänner. Du kan råka installera virus eller annan skadlig programvara på din dator.
- Spara aldrig inloggningsuppgifter i din webbläsare eller i din dator.
- Ha alltid en uppdaterad version av antivirusprogram på alla dina enheter.
- Se till att alltid ha dina enheter uppdaterade med senaste versioner av programvara, operativsystem, mm.
- Hantera externa USB-minnen, minneskort och hårddiskar med försiktighet. De kan innehålla skadlig kod.
- Undvik att använda publika wifi. Enheter som är uppkopplade på samma wifi kan läsa trafiken samt du kan råka använda ett avsiktligt uppsatt falskt wifi som har till syfte att läsa din datatrafik.

Din uppkopplade vardag skapar möjligheter för kriminella och aktörer som försöker komma över information om dig och din organisation. Med bra säkerhetsrutiner och en god säkerhetskultur gör du deras försök mycket svårare.

Vad är det vi skyddar oss mot?

Det kan vara trojaner, programvara som läser av vad du skriver på tangentbordet, access till webbkamera eller något annat. Metoderna utvecklas hela tiden och blir svårare att upptäcka för användaren.

Hur går det till?

Vanligast är via ett mail med en länk eller bifogad fil men du kan också hamna på en skadlig webbsida.

Sociala medier och appar

Tänk på vilken information du lämnar ut om dig själv och din familj. Se till att äga din identitet i sociala medier även om du väljer att inte vara aktiv, särskilt om du har ett ovanligt namn eller publik roll. Det minskar risken för att någon ska utge sig för att vara du.

Tänk på:

- Vilken information lagras om dig och dina vänner? Ta del av användarvillkoren innan du installerar en ny app eller programvara. Vill du ge applikationen access till vänlistor, historik, platsdata, kamera eller din mikrofon?
- Hur publik är du? Ofta är det du själv som måste ändra inställningar för vem som ska kunna se din profil och vad du publicerar.
- Dina digitala fotspår. Det är lätt att spåra en persons intressen och vanor via sociala medier. Information som kan utnyttjas av kriminella eller andra aktörer med oärliga avsikter för att skapa kontakt med dig.
- Bilder lämnar ut information om du inte aktivt har valt att ta bort bilddata. Tänk på bildens bakgrund, personer på bilden samt bilddata kan identifieras och användas av någon annan.
- Omvärldsbevaka din identitet. Se till att regelbundet söka efter din identitet så ingen använder den utan din vetskap.
- Aktivera tvåfaktorsautentisering för dina sociala medier.
- Var aktsam vid vänförfrågningar via sociala medier, även om personen på bilden är någon du känner och flera av dina nuvarande vänner redan är vän med. Verifiera att det verkligen är rätt person bakom kontot. Risken för att det är en kapad identitet ökar om det är en publik person med viktig befattning.
- Var uppmärksam på "informationsfiske" via grupper och forum.

Falska nyheter, påståenden och inlägg i sociala medier kan avsiktligt ha publicerats för att påverka dig. Var aktsam så du inte är med och bidrar till spridningen av desinformation som kan ha publicerats för att skada Sverige.

Har du sett falska inlägg eller desinformation delas, ta en bild och rapportera på **fake@psykologisktforsvar.nu**

Vi samlar löpande information om informationspåverkan och analyserar med syfte att snabbt kunna sprida kunskap hos myndigheter och näringsliv samt som underlag för vidare analys av metoder för att möta informationspåverkan.



EARHART
BUSINESS PROTECTION AGENCY

Specialister inom risk- och krishantering i en uppkopplad virtuell verklighet.

www.bizprotectionagency.com