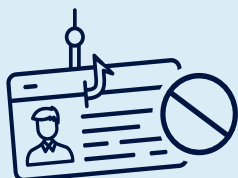


Cybersäkerhetstips

Tips och vägledning för en tryggare digital närvaro. Tipsen riktar sig till personer som exponeras särskilt mycket i offentligheten och därför kan löpa högre risk för cyberangrepp.

Vem pratar du med?



Nätfiske (Phishing)

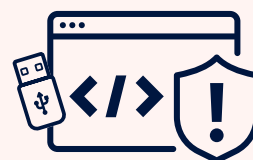
Nätfiske är en vanlig metod som hotaktörer använder för att lura till sig känslig information och skaffa obehörig åtkomst till system. Riktat nätfiske (spear phishing) är ofta sofistikerat och välgjort. Tänk på att vara vaksam på e-post från okända samt externa avsändare och ta för vana att titta på avsändaradressen i misstänkt e-post.

Ifall du är osäker, kontakta företaget eller organisationen genom kontaktuppgifter på dess officiella webbplats. Rapportera skyndsamt till it-ansvarig om du misstänker att du har blivit utsatt för nätfiske samt klickat på bilagor, länkar, skannat QR-koder eller uppgett känsliga uppgifter.

Social manipulation

Hotaktörer kan utge sig för att vara någon du känner för att försöka få tillgång till information. Tänk därför på att vara uppmärksam på digitala kontakter och lämna aldrig ut dina uppgifter utan att verifiera mottagaren och dess intention. Ha för vana att granska språket då det kan vara ett varningstecken på att du har blivit utsatt för riktat nätfiske.

Dina enheter



Uppdatera din enhet

Genom att uppdatera din enhet så snart en officiell uppdatering blir tillgänglig skyddar du både den och din information. Installera därför säkerhetsuppdateringar på din telefon, dator och andra enheter så fort en ny uppdatering blir tillgänglig. Både operativsystemet och applikationer behöver uppdateras, en del uppdateringar kräver en omstart för att få genomslag. Tänk på att endast använda dig av officiella uppdateringar.

Observera att äldre enheter kan sakna uppdateringar och är därför särskilt sårbara. Se till att använda dig av utrustning som har support.

Skydda din enhet

För att skydda din enhet, aktivera och använd den inbyggda säkerheten. Lämna inte din enhet obebakad. Dela inte med dig av din pinkod eller lösenord. Ladda din enhet med en betrodd laddare och sladd och undvik publika usb-uttag, eller använd avsedda skydd för dessa. Tänk efter innan du använder enheter du har fått från andra, exempelvis usb-minnen. För arbetsrelaterade uppgifter, använd inte privat utrustning. Var extra uppmärksam kring, och rapportera, avvikande funktionalitet och händelser i it-system.

Tänk på att inte surfa oskyddat. Undvik att använda öppna och publika wifi-nätverk samt privata molntjänster. Använd främst webbsidor med krypterad anslutning, du kan se att anslutningen är krypterad genom <https://> i adressfältet.

Lösenordshantering



Hotaktörer använder ofta lösenord som är enkla att gissa eller lösenord från tjänster som stulits för att prova om användare har återanvänt lösenord. Tänk på att välja unika lösenord för varje tjänst. Ett bra lösenord består av långa fraser, exempelvis en mening sammansatt av slumpmässiga ord och tecken. En lösenordshanterare ger dig stöd för att komma ihåg dina lösenord.

Multifaktorautentisering

För att stärka säkerheten, använd multifaktorautentisering. En ännu säkrare form av multifaktorautentisering inkluderar digitala certifikat lagrade på ett smartkort eller en säkerhetsnyckel ansluten till din dator eller telefon.

Sociala medier och appar



Sociala medier kan användas av hotaktörer för kartläggning. Tänk på vilken information du delar med dig av på sociala medier och tänk på vem du kommunicerar med. Undvik att acceptera förfrågningar från okända personer och konton. Du kan motringa för att bekräfta intentionen hos den som vill skapa kontakt.

Hotaktörer kan använda social manipulation för att skapa sig åtkomst till dina kommunikationsappar. Kontrollera regelbundet länkade enheter och konton. Populära kommunikationsappar, exempelvis Signal och Whatsapp, har ofta säkerhetsfunktioner inbyggda. Ta reda på vad som finns för den du använder och aktivera lämpliga funktioner. Var vaksam på notiser och meddelanden där du uppmanas att dela känslig information.

Kontakt

CERT-SE är tillgängliga dygnet runt alla dagar på året för att kunna agera och inom sitt uppdrag hjälpa verksamheter som har drabbats av it-säkerhetsincidenter. Mer om våra tjänster och kontaktuppgifter på cert.se

Hör av dig för att få stöd!

E-post: cert@cert.se

Ta också del av publikationen **Åtgärder för ett säkrare digitalt privatliv** som finns på ncsc.se