→ Skydda din information och dina konton med starka lösenord och flerfaktorsautentisering

I många fall är det bara ett lösenord som skyddar din personliga information och din digitala identitet från obehöriga. Därför är det viktigt att använda starka lösenord och att aktivera så kallad flerfaktors-autentisering på alla tjänster och konton som erbjuder det. Flerfaktors-autentisering innebär att du behöver flera olika sätt att identifiera dig för att logga in. Det är extra vik tigt att skydda din epost och dina sociala medier ordentligt.

Ett starkt lösenord ska vara:

- Långt – minst 12 tecken, gärna längre.
- Ovanligt – det ska inte gå att gissa sig till.
- Opersonligt – det ska inte gå att koppla till dig som person.
- Unikt – det innebär att du ska ha olika lösenord för varje tjänst.

Tips! För att skapa ett starkt lösenord kan du sätta ihop fyra slumpvis valda ord och byta ut några tecken mot siffror eller specialtecken. För att komma ihåg dina lösenord kan du använda en så kallad lösenordshanterare, eller skriva ner dem på en lapp som du förvarar på ett säkert ställe.

TÄNK SÄKERT

Läs mer på internetstiftelsen.se/tanksakert

Så undviker du att bli lurad på nätet

TÄNK SÄKERT

ETT SAMARBETE MELLAN

MSB Myndigheten för samhällsskydd och beredskap · Polisen · INTERNETSTIFTELSEN

Allt mer av det vi gör i vår vardag kräver tillgång till internet. Det kan handla om bankärenden, att beställa medicin och handla varor på nätet. Internet har underlättat vardagen på många sätt, men där finns också bedragare som vill lura dig på till exempel pengar, lösenord och kortuppgifter.

Här får du lära dig mer om hur de vanligaste bedrägerierna går till och hur du kan skydda dig.

Så luras bedragarna

Du kanske har hört begreppet **nätfiske**. Det är ett samlings namn för när bedragare försöker lura dig att dela med dig av din personliga information. Bedra gare kan använda kontaktvägar såsom mejl, sms och telefon.

För att lura dig är det vanligt att bedragarna som kontaktar dig låtsas jobba på en bank, en myndighet eller ett välkänt företag eller organisation. Bedragarnas ärenden varierar, men av olika anledningar uppmanas du nästan alltid att klicka på en länk eller att öppna en bifogad fil i ett mejl. Bedragarna kan också be dig att dela koder från din bankdosa, använda din e-legitima tion eller ladda hem ett program från nätet. För att du ska följa uppmaningen försöker bedragarna stressa dig med sina påhittade ärenden och de spelar ofta på dina känslor genom att göra dig nyfiken, glad eller orolig.

Tänk på att aldrig dela personlig information som koder, lösenord eller kortuppgifter med någon som kontaktar dig. Du ska heller aldrig använda ditt bank-id eller annan e-legitimation på uppmaning av någon som kontaktar dig!

→ Undvik att klicka på länkar i mejl, sms och olika textmeddelanden

Klickar du på en länk i bedragarnas mejl och meddelanden leds du vanligtvis vidare till en falsk webbsida där du uppmanas att logga in med ditt lösen ord, knappa in ditt kortnummer eller dela annan personlig information. Det kan till exempel vara en falsk webbshop, en falsk kopia av en myndighetssida eller en falsk inloggningssida till en streamingtjänst. De falska webbsidorna ser äkta ut, men så fort du knappar in din infor mation stjäls den av bedragarna.

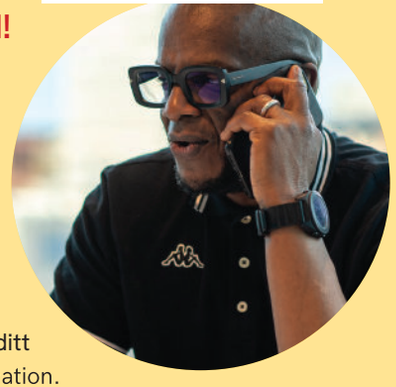
→ Undvik att öppna bifogade filer i mejl och andra textmeddelanden

Öppnar du en bifogad fil i bedragarnas mejl och meddelanden är risken stor att din dator infekteras med virus och spionprogram. Ett spionprogram registrerar sedan allt du gör och skickar din värdefulla information, till exempel dina lösenord och kortuppgifter, till bedragarna.

Skydda din dator mot virus:

- Använd ett bra antivirusprogram och aktivera din dators brandvägg.
- Uppdatera operativsystemet, appar och program direkt när det finns nya upp-dateringar.

→ Lägg på luren, våga vara bestämd!



Om någon som ringer dig ber dig om dina kortuppgif ter eller att ladda ner ett program från internet ska du lägga på luren direkt, oavsett vad ärendet gäller. Detsamma gäller om den som ringer uppmanar dig att använda din bankdosa, ditt bank-id eller annan e-legitimation.

→ Lita aldrig på avsändarnamn och uppringande nummer

Kom ihåg att du aldrig kan lita på avsändarnamn i mejl, sms och andra textmeddelanden. Det är superenkelt för bedra garna att för falska. Du kan inte heller lita på att det uppringande numret eller det nummer som visas i ett sms är äkta. För att kontrollera om mejlet, telefonsamtalet eller textmed delandet är äkta kan du kon takta den påstådda avsändaren via en kontaktväg som du själv letar upp. Svara aldrig på miss tänkta mejl, telefonsamtal och textmeddelanden.

Kom ihåg att ditt lösenord är en värdehandling:

- Dela inte dina lösenord med någon.
- Logga inte in på dina tjänster från andras datorer och mobiler. Lånade datorer och mobiler kan vara inställda på att spara dina lösenord automa-tiskt, eller vara infekterade med spionprogram.
- Byt inte lösenord i onödan. Byt bara lösenord om du vet att det är svagt eller om du miss-tänker att det blivit röjt.

→ Var kritisk mot annonser på webben och sociala medier

Annonser på nätet kontrolleras sällan av människor innan de läggs upp. Det medför att falska annonser på webben och sociala medier har bli vit ett vanligt sätt för bedragare att lura dig på pengar, kortuppgifter och lösenord, eller för att infektera din dator med virus och andra skadeprogram.

Se upp för annonser med fantastiska erbjudanden, gratisprodukter, investeringsförslag, tävlingar och olika quiz. Kom också ihåg att din dator inte har fått virus bara för att det står så i olika pop upfönster på webben. Dessa varningar är falska och syftar till att infektera din enhet med virus.