## *Handla säkert på nätet och IRL*

(Agera) (In Real Life)

Dina enheter är dina

- Mobiltelefon

  Pinkod, kod för öppning av telefon

- Bankkort, Kreditkort

  Pinkod för inköp,kortnummer, giltighetstid, CVC-kod

- Bank-id, Mobilt Bank-id, Bankdosa

Lämna aldrig ut information om dina enheter till 3-e part (undantag kanske för make/maka, barn, god man) framförallt ALDRIG på uppmaning av någon som kontaktat dig.

**En särskild varningsklocka ska ringa om det framhålls att det är bråttom.**

# På nätet

Vissa E-butiker erbjuder köp som verifieras med

**Verfied by Visa / MasterCard SecureCode**

Innebär att man måste komplettera kortuppgifterna med ytterligare en kod, idag oftast med Bank-id.

Generellt bör man stänga sina kort för internetköp när man klarat av sina köp, detta är olika beroende på vilken bank man har, men proceduren är enkel att genomföra.

Allmänt kan man rekommendera att inte ha alla tillgångar på ett och samma konto och låta det konto man kommer åt med sitt bankkort bara ha den buffert man behöver.

# E-post

Var rädd om E-postkontot, det kan vara inkörsport till all information på din enhet och på nätet

Använd ett separat lösenord för E-post, gärna kombinerat med 2-faktorverifiering.

Klicka inte på länkar du fått i din E-post om du inte är säker på avsändare och innehåll.

Läs NOGGRANT igenom brev du fått med erbjudanden eller förfrågningar från Postnord, Elgiganten, NetOnNet etc.

Finns det formuleringar, stavfel eller språkbruk som känns underliga?

Exempel:myndighetspost som inleds med.

Kära….

# Telefonen

Försök att hålla din kontaktlista uppdaterad
så att du kan identifiera de som ringer.

Undvik att svara på okända nummer,
är ärendet viktigt, talar uppringaren in ett meddelande eller ringer en gång till.

Slutar uppringningen efter 3 signaler är det oftast en datorstyrd uppringning från en telefonförsäljningskedja.

Vårdcentral och offentlig förvaltning ringer oftast från hemligt nummer och i de flesta fall är det som svar på ett initiativ från dig.

# *Tips för säkra lösenord*

**Lösenord ska betraktas som värdehandlingar. Välj därför lösenord med omsorg och tänk på hur du hanterar dem.**

## Lösenfraser

Som alternativ till klassiska lösenord kan man gärna använda en lösenfras. Lösenfraser är ofta enklare att komma ihåg, enklare (men längre) att skriva in, och ger samtidigt ökad säkerhet.

Lösenfraser består av ett
antal **slumpmässigt** valda ord. Förutsatt att orden verkligen väljs helt slumpmässigt behövs inga siffror, specialtecken eller liknande.

## 10 användbara tips

1. **Lösenord ska vara långa nog**. Tio tecken är en rimlig miniminivå i dagsläget, men helst ska man använda minst femton tecken.

2. **Lösenord ska innehålla olika sorters tecken**. Använd åtminstone någon siffra, specialtecken (plus, minus, snedstreck, punkt, osv) och stor bokstav. Däremot kan det vara bra att låta bli tecken som "å", "ä", "ö", med flera, som kan krångla på vissa system.
3. **Använd inte ditt användarnamn**, namn eller annan personlig information som lösenord eller ens del av lösenordet. Sådan information är alldeles för lätt att ta reda på.
4. **Undvik ord från ordlistor** och namn på andra personer, orter, länder osv. De som försöker knäcka lösenord använder långa listor med vanliga ord och namn från flera olika språk.
5. Ett bra sätt att skapa lösenord kan vara att **hitta på en ramsa** som är lätt att komma ihåg. Låt lösenordet bestå av första bokstaven i varje ord, men glöm inte att använda både stora och små bokstäver och lägg till några siffror och specialtecken. Ju barnsligare och roligare ramsa, desto lättare att komma ihåg!

6. Om du måste använda samma lösenord på flera system, tänk då på att likväl **aldrig använda samma lösenord** för säkra/viktiga system som för osäkra/oviktiga.

7. **Undvik att skriva upp lösenord**. Om du trots allt måste göra det, skriv då aldrig lösenord, användarnamn och vilket system det gäller tillsammans.
8. **Byt lösenord när det behövs**. Om du misstänker att ditt lösenord är känt av någon annan än dig själv, ska du byta lösenord direkt. Det finns egentligen ingen anledning att byta lösenord regelbundet, annat än för att byta till ett som är längre eller enklare att komma ihåg.
9. **Skicka aldrig lösenord via vanlig, okrypterad, e-post**. Det finns risk att det hamnar hos fel mottagare eller att någon snappar upp det på vägen.
10. **Ingen person ska fråga dig efter lösenord**.

## Lösenordshanterare

Lösenordshanterare underlättar användningen av starka lösenord och användningen av olika lösenord för varje tjänst. Det räcker att komma ihåg ett lösenord för att få tillgång till alla sina unika lösenord:

Det finns i huvudsak två typer av lösenordshanterare: de som lagrar lösenorden på din egen enhet, och de som lagrar lösenorden i molnet. Molntjänsterna gör det enkelt att få tillgång till alla lösenord på alla enheter man använder, medan de med lagring på den egna enheten ger en högre grad av kontroll.

## Exempel lösenordshanterare

### LastPass

LastPass är en molntjänst som finns i både gratisversion och flera betalversioner. Funktionerna i gratisversionen är tillräckliga för de allra flesta. LastPass fungerar i de flesta webbläsare och mobila enheter.

Vid användning av LastPass rekommenderar vi starkt att man aktiverar tvåstegsverifiering (*multifactor authentication*) för extra säkerhet.

LastPass ger flera alternativ för tvåstegsverifiering. Deras egen app (LastPass Authenticator) är den enklaste att använda, men den som redan använder Microsofts app (Microsoft Authenticator) eller Googles app för tvåstegsverifiering kan använda dem med LastPass också.

Välj ett huvudlösenord ("master password") som är långt och komplext.