Digitalt självförsvar
Grunderna

Med kärlek, från:
DFRI, Sparvnästet & Konsthall C

CRYPTO PARTY

Bra och starka lösenord

1. Börja med en nonsensmening. Välj något som är roligt eller konstigt, då blir det lättare att komma ihåg.

"*Ett ruttet äpple gör ingen sommar i Bohuslän.*"

2. Se till att meningen har små och stora bokstäver, siffror och specialtecken. Ta bort alla mellanslag.

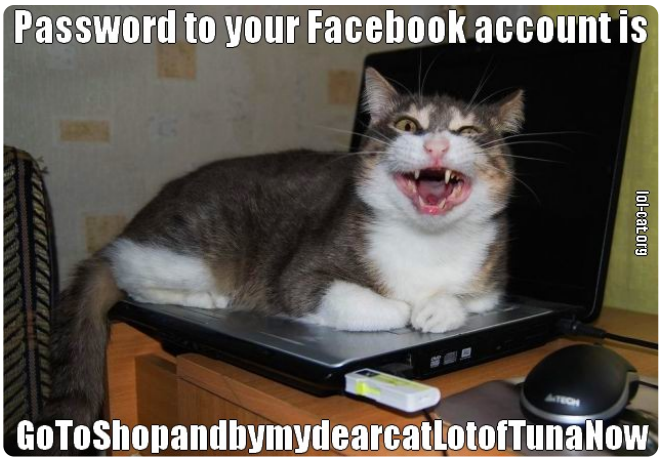
"***Ett(1)***ruttetäpplegöringensommari***B***ohuslän***.***"

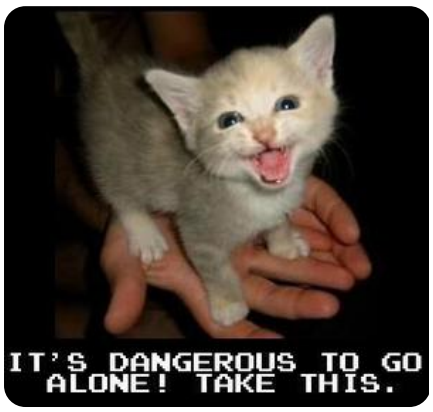
3. Behåll gärna hela meningen, men om du tycker att det är för långt att skriva kan du ta första bokstaven i varje ord.

"*E(1)rägisiB.*"

4. Anpassa lösenordet till en specifik sida. Exempel: Gunilla på Facebook.

"gf:*E(1)rägisiB.*"





Lösenordsfarorna

1. Samma lösenord på mer än ett ställe
2. Enstaka ord som finns med i en ordlista på något språk.
3. Ord stavade baklänges eller vanliga förkortningar.
4. Vanliga teckenersättningar "och" blir "&".
5. Upprepade tecken "zzzz".
6. Vanliga sekvenser "1234", "qwerty" eller "asdf".
7. Personlig information, t.ex. namn på barn.

Uppdatera dina program

Ett sätt som både brottslingar och statsmakten använder för att komma åt din dator är att utnyttja fel i program som du har installerade. Det är därför viktigt att du alltid uppdaterar dina program.

Speciellt viktigt är det att du uppdaterar:
- Ditt operativsystem, ex. Windows
- Din webläsare (Firefox eller chrome)
- Din pdf-läsare (ex. adobe)
- Din flash spelare (ex. adobe)
- Java

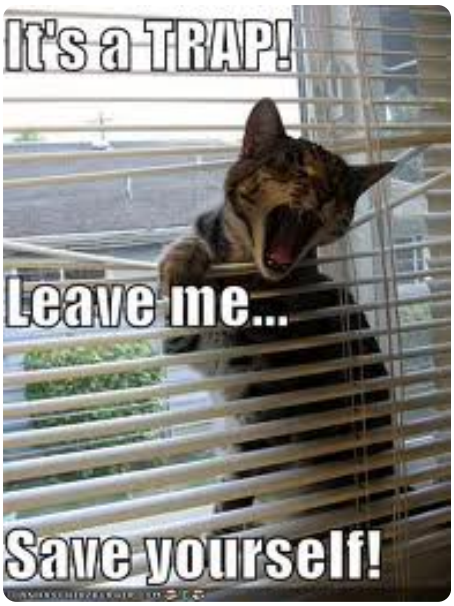
Starta om datorn minst en gång i veckan och svara ja på frågor om du vill uppdatera programmen ovan så sköter det sig oftast automatiskt.

Mail från någon du inte känner?

Var mycket vaksam!

- Klicka inte på länkar i epostmeddelandet.
- Öppna inte bifogade filer.
- Skicka aldrig något lösenord i ett mail

Inte ens om det finns bilder på söta katter!



Eposten är ditt viktigaste konto! Den kan användas för att komma åt dina andra konton genom lösenordsåterställning.

Adblock Plus

https://adblockplus.org

Installera adblock plus i din webläsare.

Gör det svårare för för reklamföretagen att kartlägga dina surfvanor.

Lås skärmen

Använd knapplås på telefonen och lås datorn när du lämnar den, även under korta perioder.

Ställ in telefon och dator så att låset slås på automatiskt efter en viss tids inaktivitet.

WiFi-surfa bland hajarna

- Använd en kabel så ofta som möjligt.
- Föredra 3G eller 4G-modem före wifi om du har möjlighet att välja.
- Öppna nätverk är *öppna* - alla kan se vad du gör.
- Dela inte ut ett *öppet* nätverk med din mobil.
- Välj **WPA** eller **WPA2**-säkerhet för din egen accesspunkt.
- Rensa bort sparade nätverk från din telefon och dator med jämna mellanrum.

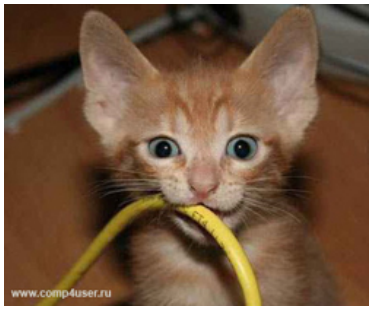
https - är superviktigt:

... när du är på öppna trådlösa nätverk
... när du skall skriva in ett lösenord på en websida
... när du kollar din mail

TIPS:
www.eff.org/https-everywhere

Viktigt! *Var inte rädd.*

Låt inte alla säkerhets-risker skrämma bort dig från teknik och Internet.



Sociala medier och du

Här är något som kan vara bra att tänka på när man är på facebook och twitter.

* Din granne läser vad du skriver
* Din hyresvärd läser vad du skriver
* Ditt ex läser vad du skriver
* Din arbetsgivare läser vad du skriver

De flesta sociala nätverk erbjuder inställningsmöjligheter för vem som skall få se vad. Hur ser dina inställningar ut?