Datasäkerhet

Enter 20.04.26

Christer Levlin

Teknik

- Installera alla uppdateringar som erbjuds. Gäller för **ALLA** apparater oberoende av märke och modell.
- Om det system man använder inte längre stöds skall man skaffa nytt.
- Windows: https://endoflife.date/windows
- Android: https://endoflife.date/android
- Apple iOS: https://endoflife.date/iphone
- Apple macOS: https://endoflife.date/macos
- Gäller också eventuell router man har hemma

Virus och andra skadliga program

- Använd alltid något slag av virusskydd. Antingen sådant som finns färdigt i systemet eller “yttre”.
- Win10 / Win11 har färdigt inbyggt Microsoft Defender som är helt tillräckligt.
- **OBS!!** Man kan **INTE** samtidigt ha flere antivirusprogram aktiva. Man måste avinstallera det tidigare programmet om man vill övergå till ett annat.
- https://www.av-test.org/en/

Misstänkta e-mail och textmeddelanden

- Om man får ett e-mail eller textmeddelande som verkar “konstigt/misstänkt” kan/skall man alltid kolla avsändaren.
- Klicka **ALDRIG** på en link som ni får via ett “osäkert” e-mail eller textmeddelande.
- Säkra / osäkar websidor / textmeddelanden
- Gratis hjälpmedel på adressen https://www.f-secure.com/fi

Hur loggar jag in till Banken, Kanta....

- Man skall **ALDRIG** söka linken till nätbanken / kanta /... via Google (t.ex Aktia nätbanken) !!!
- Skriv i addressfältet in “Bank”.fi , och sök dig vidare tills du kommer till inloggningssidan. Den kan man göra till ett s.k. Bokmärke. Via bokmärket kommer man i fortsättningen direkt till rätt inloggningssida.

Bluff och bedrägeri --> nätbankskoder

- samtal från ”banken” eller någon ”myndighet”
- **INGEN** hederlig aktör frågar efter era bankkoder per telefon. Inte polisen, inte sociala myndigheter och allra minst banken.
- **INGEN** hederlig aktör skickar e-mail eller textmeddelanden med en link till en inloggningssida !!!

Bluff och bedrägeri --> kreditkort

- ett meddelande från Posten / DHL / UPS /... att ett paket är på väg men kräver någon obetald ”liten” avgift innan det kan levereras. Där finns också en link till en sida där man förväntas fylla i sina bank/kreditkortsuppgifter för att betala den ”resterande” avgiften. Fyll **INTE** i något sådant. Klicka inte ens på linken.
- Förhindra att någon gör nätköp med kortet om de på något sätt fått tag på kortuppgifterna

Beställningsfälla

- om / när man får ett erbjudande som verkar lockande skall man vara noga med den ”finstilta” texten innan man beställer. Annars kan det hända att kreditkortet börjar debiteras främmande summor regelbundet.
- Om man får ett telefonsamtal där den som ringer frågar om det är “Kalle Pettersson” i telefonen skall man INTE svara ja / kyllä. Det kan hända att den som ringer bandar samtalet och i efterskott “klipper in” ert jakande svar som svar på frågan om ni vill beställa hans produkt.

Hur kan man skydda sitt Google eller FB-konto

- Man kan definiera s.k. tvåstegsverifiering. Det betyder att varje gång man loggar in på t.ex. FB på datorn kommer det ett meddelande till telefonen att någon försöker logga in på kontot.
- Där finns två svarsalternativ av vilka man då skall klicka på “Ja,det är jag” för att komma in.
- Svara INTE på messinger meddelanden från någon “FB vän” som vill ha ert telefonnummer.

Stark identifiering

- Vanligen sker stark identifiering med hjälp av bankkoder och det gör att olika ”aktörer” försöker fiska efter dem

Alternativa metoder

- **Certifikatkort**: med kortläsare och program och dem kan man använda endast i en dator
  Med hjälp av **hightrust.id** kan man ladda kortet i en smartmobil
- **Mobilcertifikat**: kan skaffas via telefonoperatören och kostar 0 – 3€/mån. Fungerar också i äldre telefoner

Lösenord

I princip bör man ha ett lösenord för varje tjänst man använder.
Logga INTE in på andra tjänster med FB eller Google !!!

Ett starkt lösenord:

Minst 8 – 12 tecken, stora och små bokstäver, siffror och specialtecken. OBS! Inga mellanslag

Ett bra sätt är att använda “lösenfraser” t.ex “V1lleVallat0n!

Du har tappat din kod

Du har tappat din kod till
ditt lösenord,
Du gamling i nutida livet.
Så sitter du åter vid datorns
bord
Och grubblar så översig-
givet.
Vad var det för kod – var
den lång eller kort,
Var den bra eller illa
skriven?
Tänk efter nu – annars
deletas du bort
Du gamling i nutida livet.

Thorild Jonsson, Ludvika

Fritt efter Nils Ferlin

PIN-koder (Personal Identification Number)

Telefonen:

Byt SIM kortets PIN kod när ni får ett nytt.

SIM-kortet: min. 4, max 6 siffror

Bildskärmen: kan ha samma kod som SIM-kortet. Bildskärmen kan man också ofta låsa upp med fingeravtryck eller “ansiktet”.

Hur minnas alla lösenord och koder ??

Håll dom **INTE** på en massa små lappar !!!
Skaffa ett (litet) häfte att anteckna dem i. En sida för varje tjänst så det finns utrymme att skriva in det nya lösenordet / den nya koden när ni måste byta.

Frågor, kommentarer ??

Tack