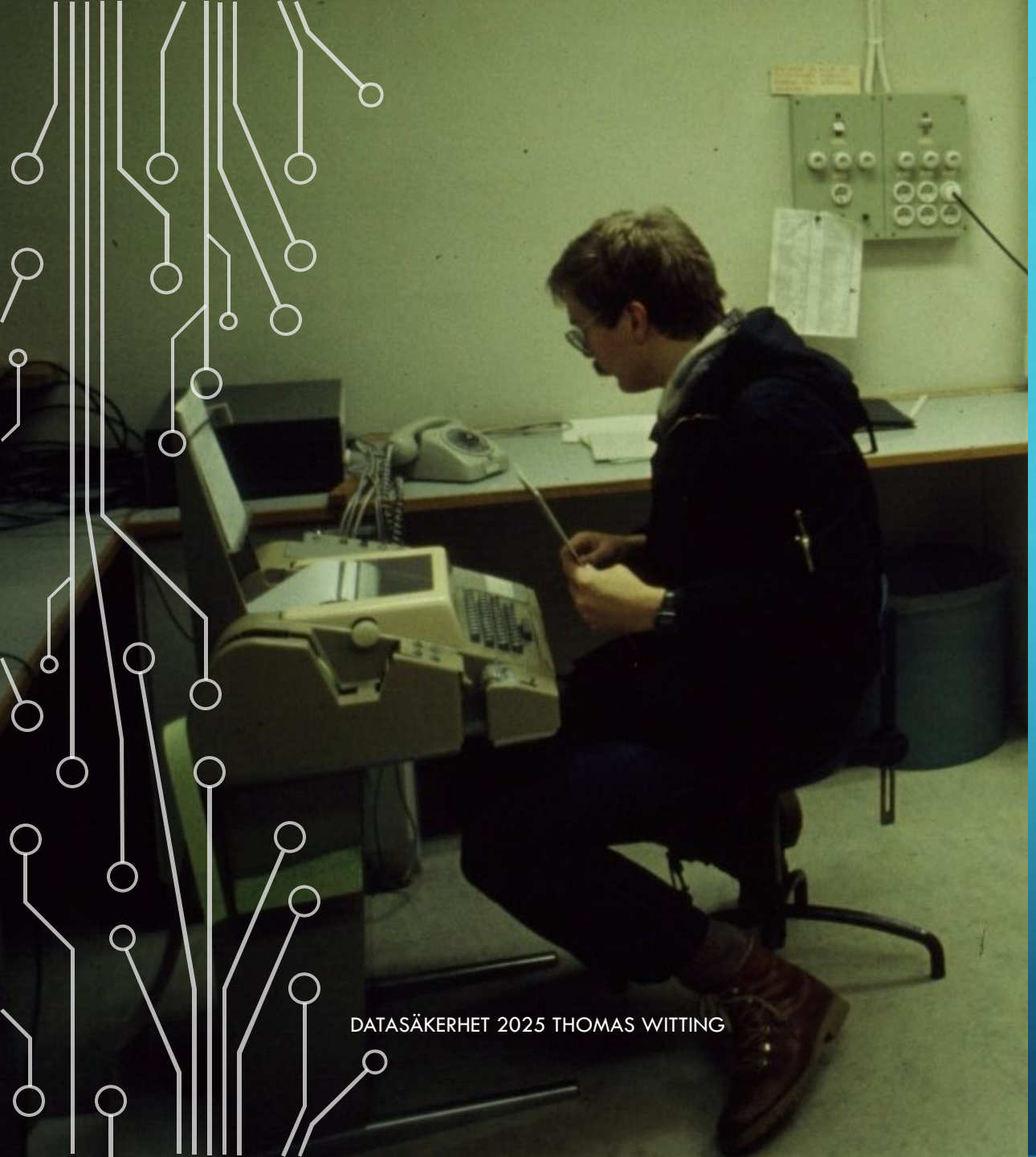
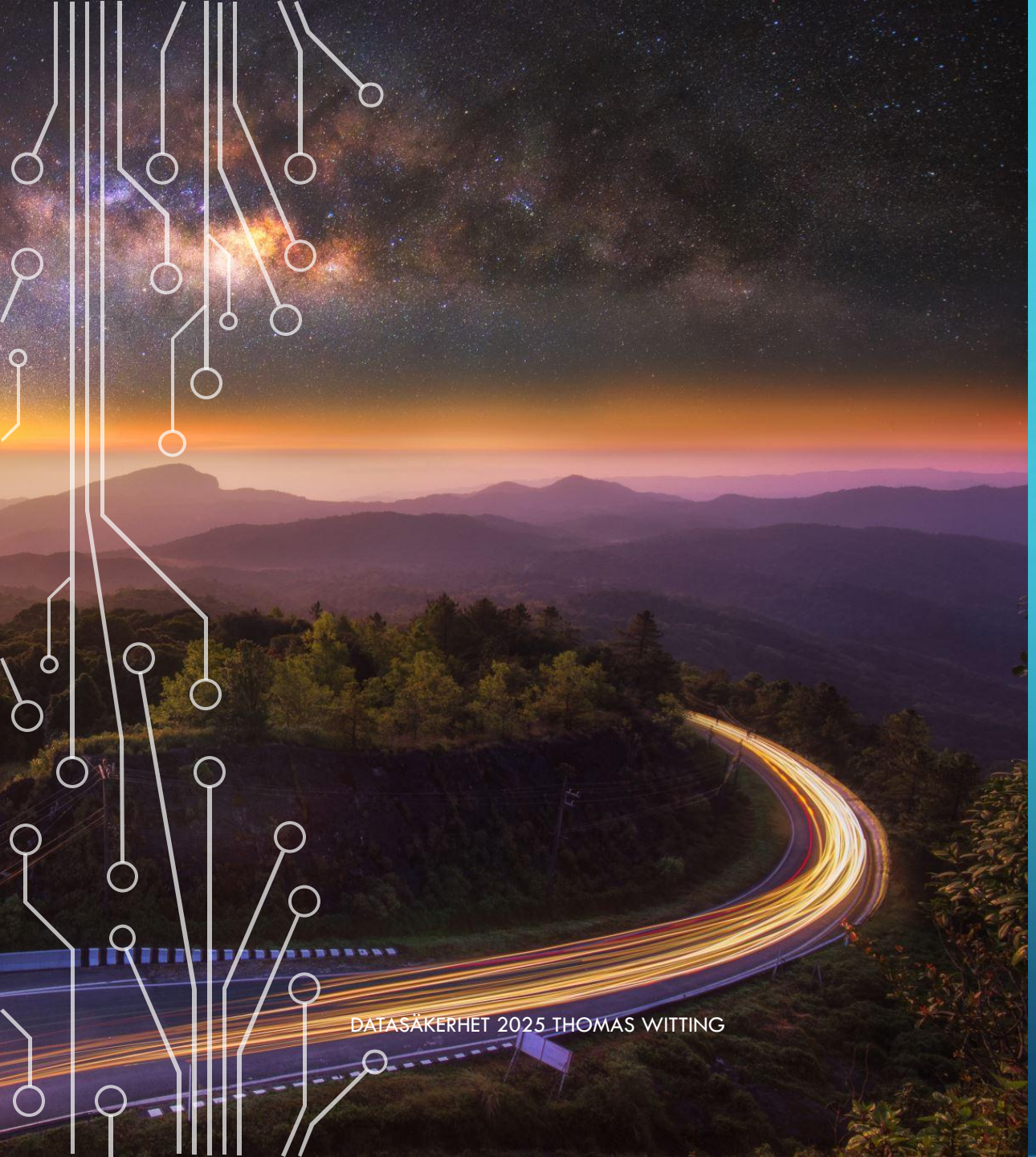
DATASÄKERHET



DATASÄKERHET 2025

- Föreläsare: Thomas Witting, FK Helsingfors Univeritet
- 34 år på LM Ericsson - senaste åren inom Cybersäkerhet för Produkter.
- Byggt datanät i flera länder och skolat folk på plats *nästan* över hela planeten



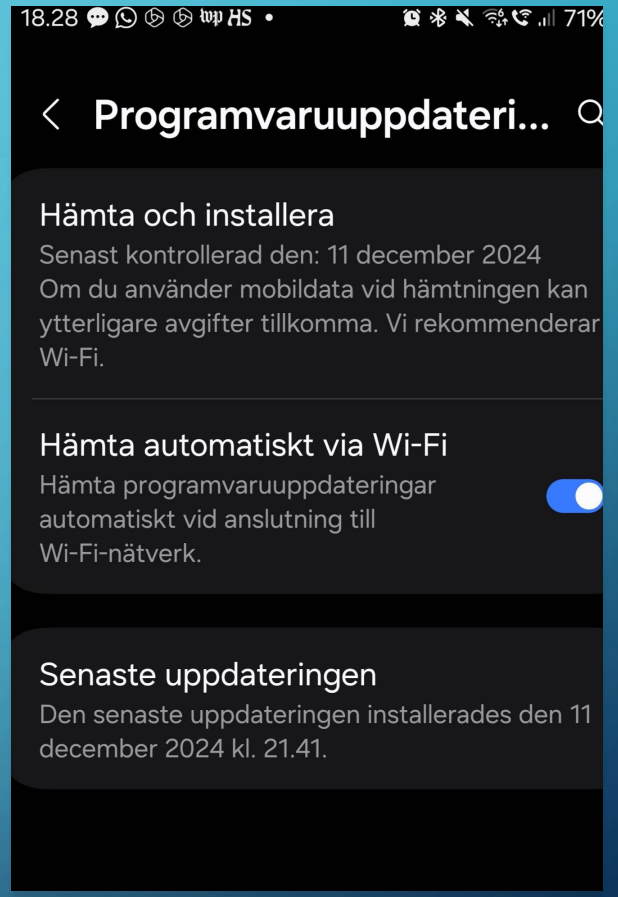
AGENDA

- Är min apparat i skick?
- Virus och hur man skyddar sig effektivt
- Andra sätt att skydda sig
- Fällor och risker –konstiga meddelanden och samtal
- Hur hantera lösenord
- Betalningar med telefon eller platta
- Frågor

ÄR MIN APPARAT I SKICK?

TEKNIKEN I MIN APPARAT ?

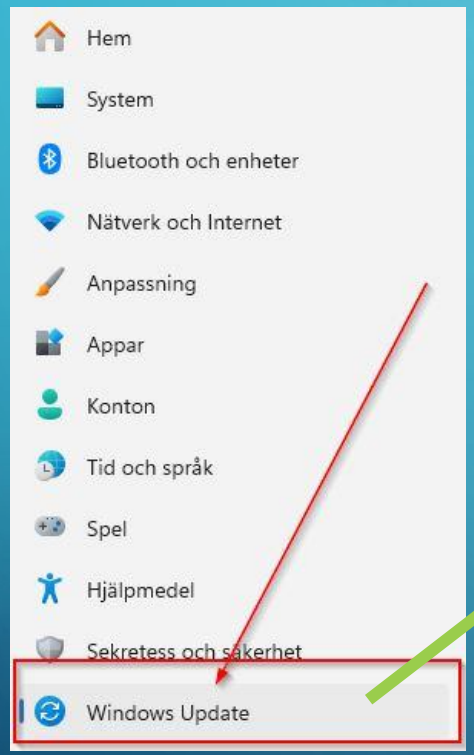
- Hur vet jag om min apparat är kurant, up-to-date, i bästa möjliga skick?
  - Det kan man kolla själv på apparaten – Programvaruuppdatering, Software Update
  - Allt som är i användning bör ha de senaste uppdateringarna.
- REKOMMENDATION: om apparaten är gammal, dvs får inte mera uppdateringar, då skaffar man en ny.



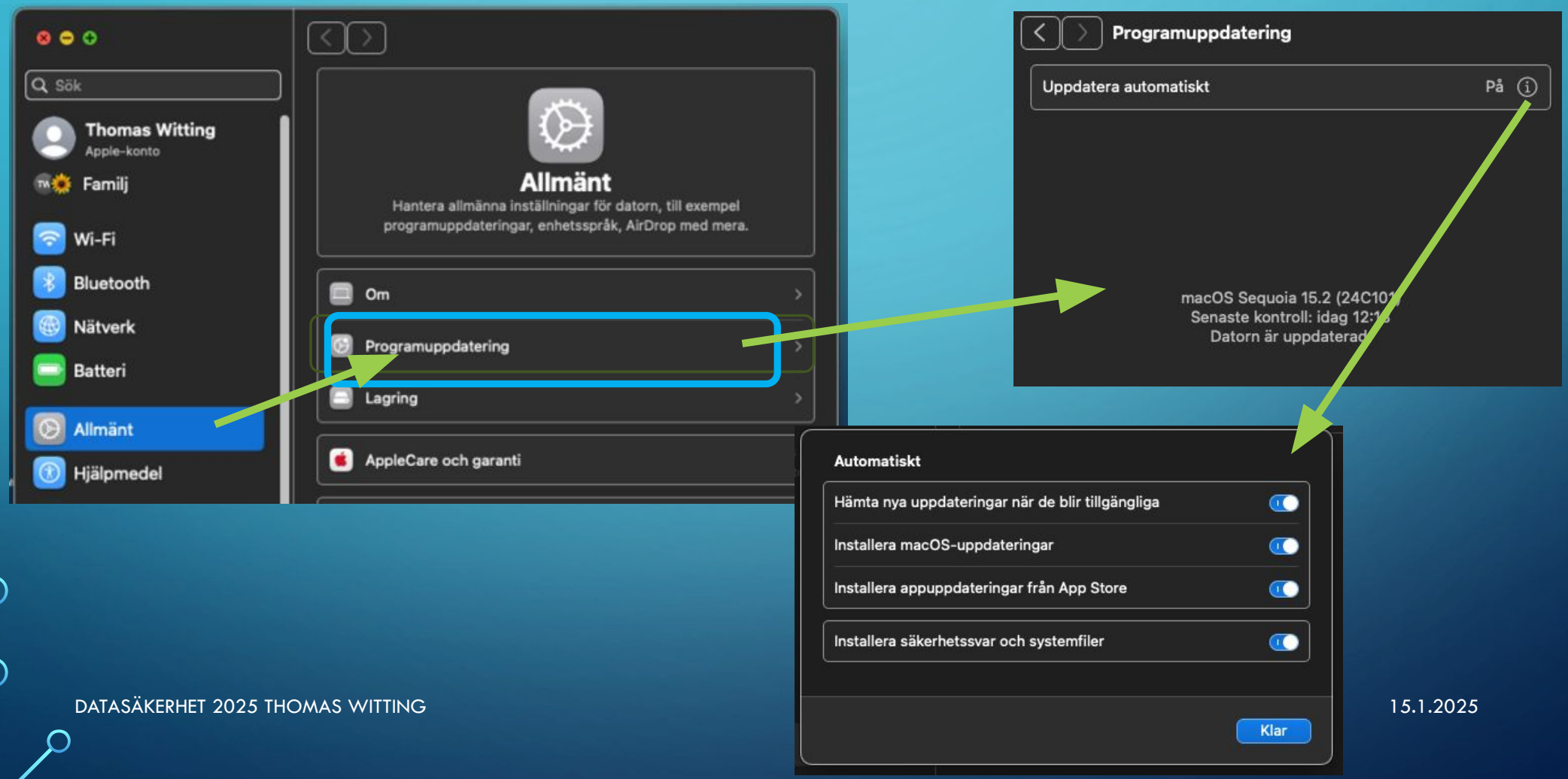
VILKA APPARATER DÅ?

- Alla apparater man använder för viktig datakommunikation, banker, skatter hälsomyndigheter och inte minst att hålla kontakt med de släkt o vänner
- Man bör kontrollera hela kedjan, t.ex. från laptopen ut till internet
  - Har datorn den senaste mjukvaran inklusive säkerhetsuppdateringarna ?
  - Hur är den kopplad till internet hemma? Via en "mokkula" eller en router? Är den uppdaterad? Vem ansvarar för det?
  - Trådlöst nät eller med kabel ?

HUR KONTROLLERA (WIN 10-11) ?



HUR KONTROLLERA (MACOS) ?

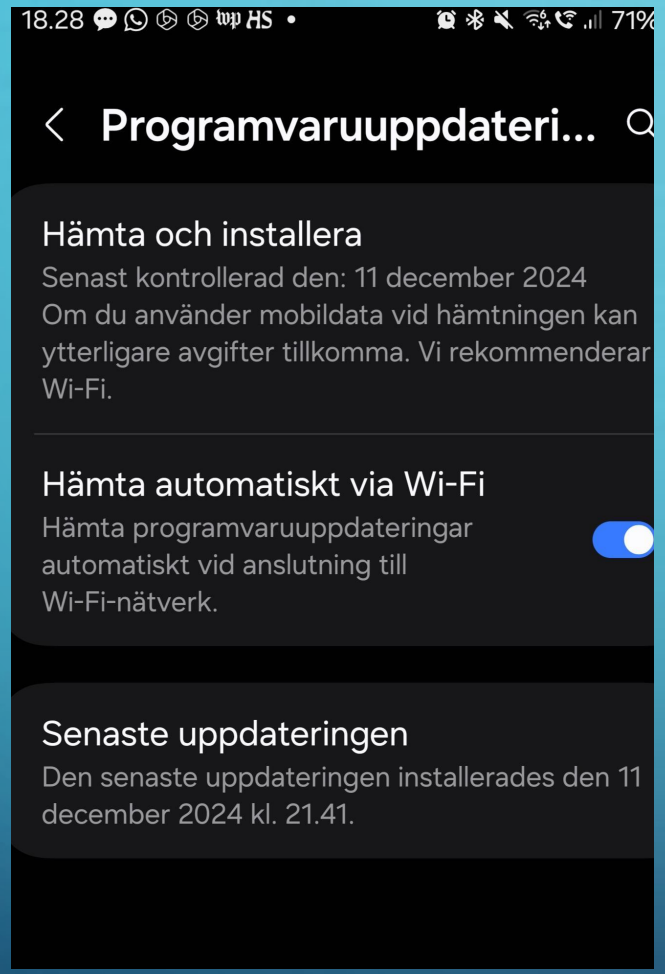


LINUX OCH CHROMEOS

Linux – helt beroende på distributionen, finns appar och man kan köra enkla kommandon direkt i en sk. terminal

ChromeOS (Flex) - behövs inte alls för en privat användare.

HUR KONTROLLERA ANDROID, IPHONE



MEN DEDÄR ANDRA APPARATERNA DÅ?

Tyvärr är det inte möjligt att ge något standardförfarande!

ANDRA SÄTT ATT KONTROLLERA

- Om man vill kontrollera mera "officiellt" kan man söka på tillverkarens sidor, eller genom att besöka https://endoflife.date websidorna för många produkter:
  - https://endoflife.date/android för Android telefoner och surplattor, Samsung, Sony etc
  - https://endoflife.date/windows för Windows bärbara och bordsdatorer
  - https://endoflife.date/iphone för iPhone Apple telefoner
  - https://endoflife.date/ipados för iPad Apple surfplattor
  - https://endoflife.date/macos för Mac bordsdatorer och Macbook (Air, Pro)

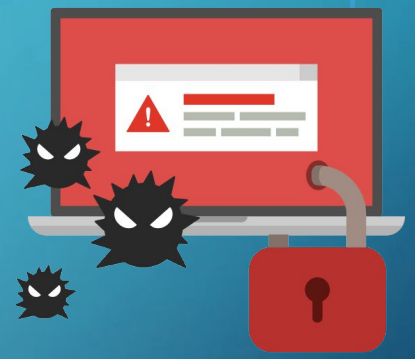
VIRUS OCH HUR MAN SKYDDAR SIG EFFEKTIVT

VIRUS – SKADLIG PROGRAMVARA I DATORER

- Även en väl uppdaterad helhet av apparater kan drabbas av illvillig mjukvara i nån form. Man skyddar en uppdaterad dator såhär:
  - Systemets egna skydd anses numera vara fullgott, förutsatt att man inte själv utsätter sig för fara.

    - **Windows**: Defender, SmartScreen, Windows Security Center, Windows Firewall
    - **MacOS**: XProtect, Gatekeeper, Malware Removal Tool (MRT)
    - Linux: Mycket beroende på varianten, men behöver i regel mindre skydd och öppna källkodsprogram finns att tillgå, men kräver en hel del arbete att sätta upp
    - ChromeOS Flex: Bästa möjliga skydd på bekostnad av att Google samlar och säljer användardata

VIRUS – ILLVILLIGA APPAR I TELEONEN



- Moderna uppdaterade telefoner är tillräckligt skyddade ifall:
  - Användaren kan hålla sig borta från skumma webbsidor och kan
  - låta bli att ladda applikationer från källor andra än de officiella applikationsbutikerna (Google Play och App Store),
  - och INTE klickar på allt som man ser i epost och textmeddelanden (SMS) utan att tänka efter
  - Dessutom använder sig av säkra webbläsare, Google Safe Browsing (Chrome) eller Safaris Säker Surfning.

ANDRA SÄTT ATT SKYDDA SIG

ÖVRIGA SKYDD OCH ATT TÄNKA PÅ

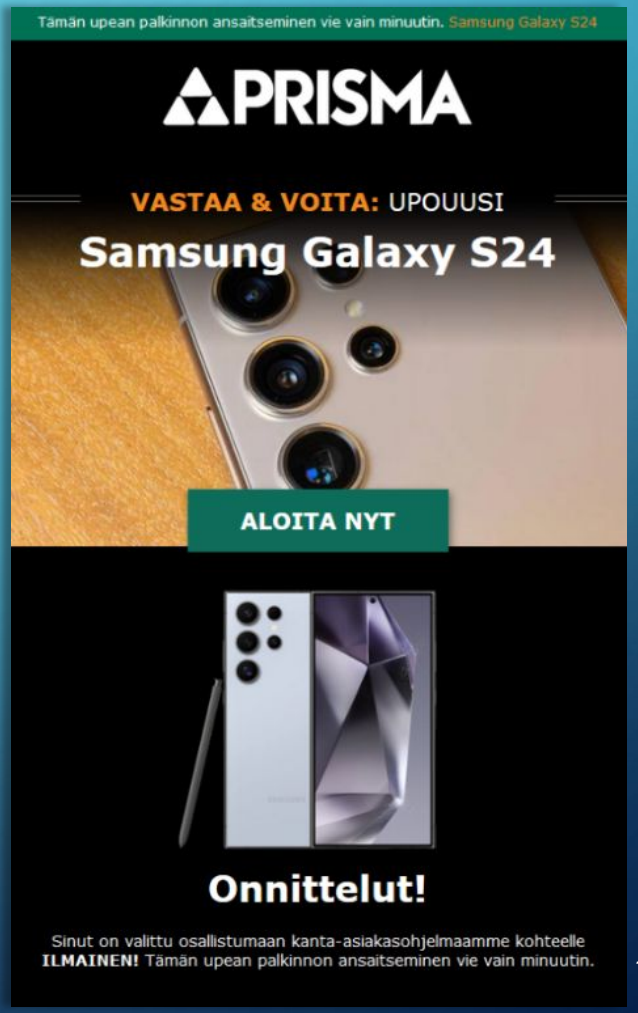
- Skärmlås, gärna med mera än 4 siffror eller bokstäver
- Biometriska lås, fingeravtryck och ansiktsigenkänning

- Behörigheter – vad får den nya appen göra, får den läsa mina kontakter osv.
- Data på min apparat kan antingen vara i klartext eller kypterat – krypterat är att föredra.
- Om jag vill ha in en applikation vad säger pålitliga källor på internet om den?

HÅRDARE SKYDD

- Om man vill, kan man skaffa ett skydd som kostar, fördelarna är:
  - Det tjatas inte om att gå från gratisversion till köpeversion
  - mångsidigt skydd utöver de sedvanliga, ofta tillgängligt till alla arkitekturer (Win, Mac, Android, iPhone osv)
  - Ofta fungerande stöd, t.o.m. över telefon.
- NOTERA:
  - Om något är bra och gratis är det du som är produkten.
  - Det kan bli problem om man kör två virusskydd samtidigt – de misstänker varandra

FÄLLOR OCH RISKER – KONSTIGA MEDDELANDEN OCH SAMTAL



SAMTAL SOM MAN INTE BESTÄLLT

- Ingen riktig myndighet eller tjänsteleverantör frågar NÅGONSIN efter bankkoder genom att ringa och be dem.
- Om samtalet börjar med typ “Är det Gunnar Godtrogensson jag talar med?” är det skäl att först fråga vem som ringer och i vilket ärende, istället för att säga “Ja” eller på annat sätt direkt bekräfta. Svara gärna alltid med “Hallo” först, de som ringer i sunt ärende vet nog att ha tålamod.

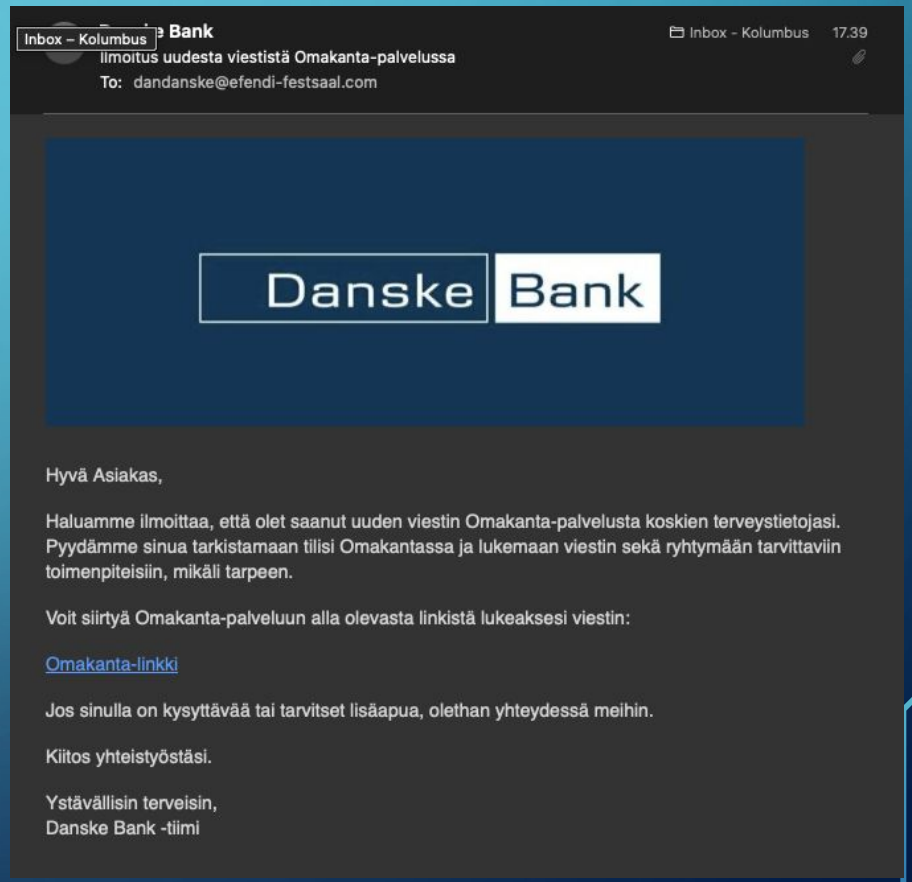
DEN STÖRSTA RISKFAKTORN: JAG SJÄLV!

- Jag kanske klickar på ett brådskande varningsmeddelande i en email från min bank, posten, Omakanta eller vero.fi ?

Posti-ilmoitus:
Pakettisi on saapunut varastollemme, eikä sitä voida lähettää väärien osoitetietojen vuoksi, täytä tarkat osoitetiedot uudelleen, lähetämme sen 24 tunnin kuluessa.

https://qrco.de/bf9a8W?sidubaradåK8rJBPTqc

Hauskaa päivää!



HUR LOGGAR JAG IN ?

- Bästa sätt är att skriva länken in i addressfältet manuellt
  - Exmpel: vero.fi , omakanta.fi, traficom.fi osv
- Gör sedan ett bokmärke av inloggningssidan

Om man söker med t.ex. Google efter en sida till vilken man vill logga in skall man inte blint lita på att det är rätt.

En del kriminella gör t.o.m. reklaminlägg som syns bredvid listningen från en sökning, de är kortlivade men klickar man på en sådan kan man bli lurad.

SE UPP FÖR BESTÄLLNINGSFÄLLOR!

- Ett email med lockande erbjudande t.ex. för tandborstar och tandkräm kan vara en beställningsfälla, dvs man tror att man köper en vara, men i själva verket går man med på en prenumeration som sen är svår att avbryta. Ofta kan dehär komma som reklam i "flödet" dvs allt som puffas ut till din telefon, dator eller surfplatta.

- Vid köp av telefon eller annan apparat trugas det service-avtal eller extra långa garantier. Helt lagligt och ok, men var mycket kritisk inför detta, eftersom de vanliga garantierna ofta är rätt långa, men service-avtalen dyra samt kan vara mycket spartanska, i allt utom priset.

EXTRA SKYDD TILL KONTON

- Många populära tjänster, som Google och Facebook, kan erbjuda extra skydd till ditt konto, dvs förutom ditt användarnamn och lösenord kan man ombes skriva in en kod som genereras av en applikation på telefonen eller surfplattan, nästan som på banken.
- Alternativt skickas ett SMS eller en email med en kod som skall knappas in, eller så ombes man svara på en fråga, typ ”Var det du?”.

Det kallas för flerstegsverifikation. Det är mycket bra att ta i bruk.

KONSTIGA MEDDELANDEN & SAMTAL

- Typiska fall:
  - En god vän som du varit vän med länge på Facebook vill bli din vän pånytt
  - Du får ett meddelande på Messenger av en vän som säger sig ha tappat ditt telefonnummer – försäkra dig med SMS att det verkligen är så
  - Ett meddelande (SMS eller WhatsApp) av någon som utger sig för att vara ditt barn som påstår att hen tappat sin telefon eller dylikt och behöver pengar för att ta sig hem.

ENKELT SKYDD MOT IMITATION

- LÖSENKOD för familjen. En lösning till att säkerställa att det verkligen är en närstående som talar/textar är att komma överens om en fråga som bara de inblandade kan veta svaret till - inget konstigt eller knepigt, men nog unikt.
- T.ex. ”Var var vi på X födelsedag?” eller t.o.m. en lösenfras eller ett enskilt lösenord, som till och med de yngsta kan hantera.

SOCIAL MANIPULATION – SOCIAL ENGINEERING

- “Social engineering” är en metod för manipulation där en person utnyttjar psykologi och mänskliga svagheter för att lura individer eller organisationer att avslöja känslig information, utföra vissa handlingar eller ge åtkomst till resurser. Det handlar ofta om att bygga förtroende eller skapa en känsla av brådska för att få offret att agera utan att tänka kritiskt.
- Det bästa skyddet mot det är sunt förnuft.
- Det ordnas tävlingar i detta t.ex. på DEFCON Las Vegas

CHECKLISTA FÖR SUSPEKTA MEDDELANDEN

Väntar jag mig ett meddelande från nån leverantör eller myndighet?

Kommer det från en avsändare som är trovärdig?

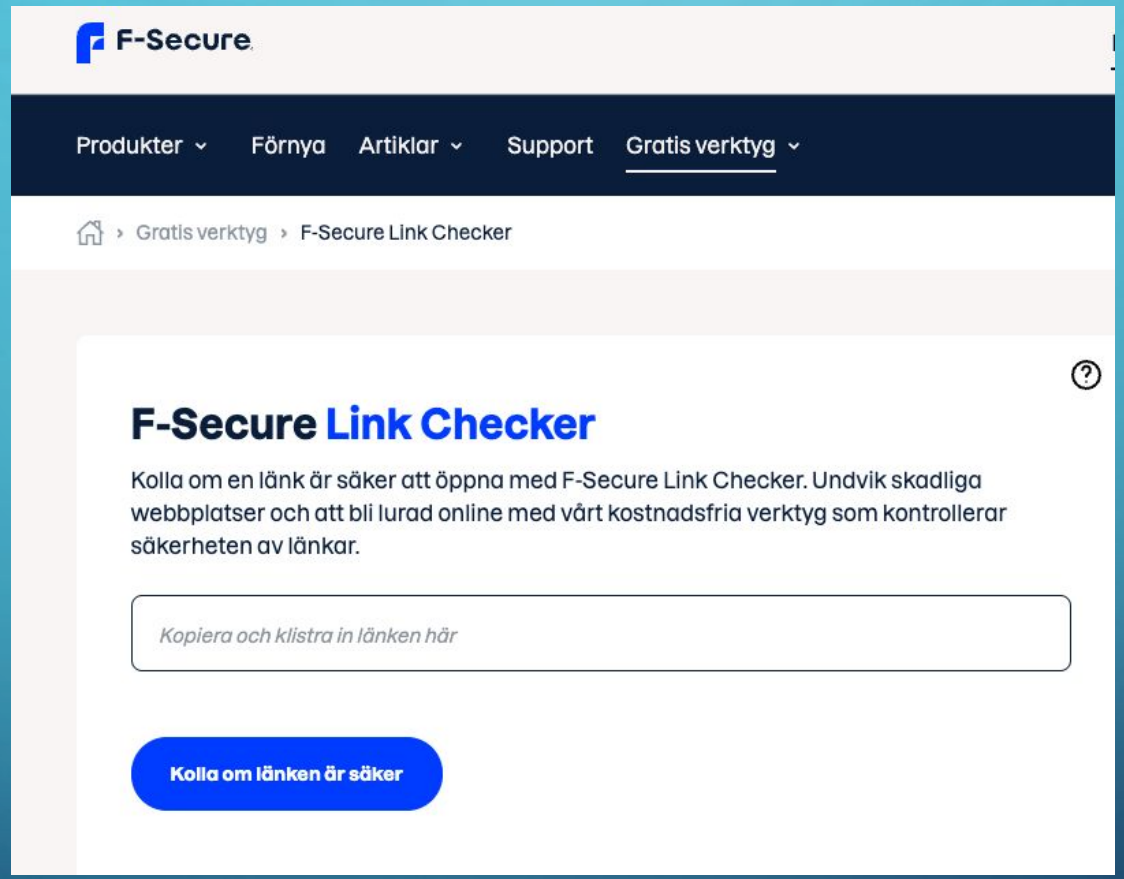
Vad vill avsändaren?

Måste jag klicka på nåt i meddelandet för att gå vidare

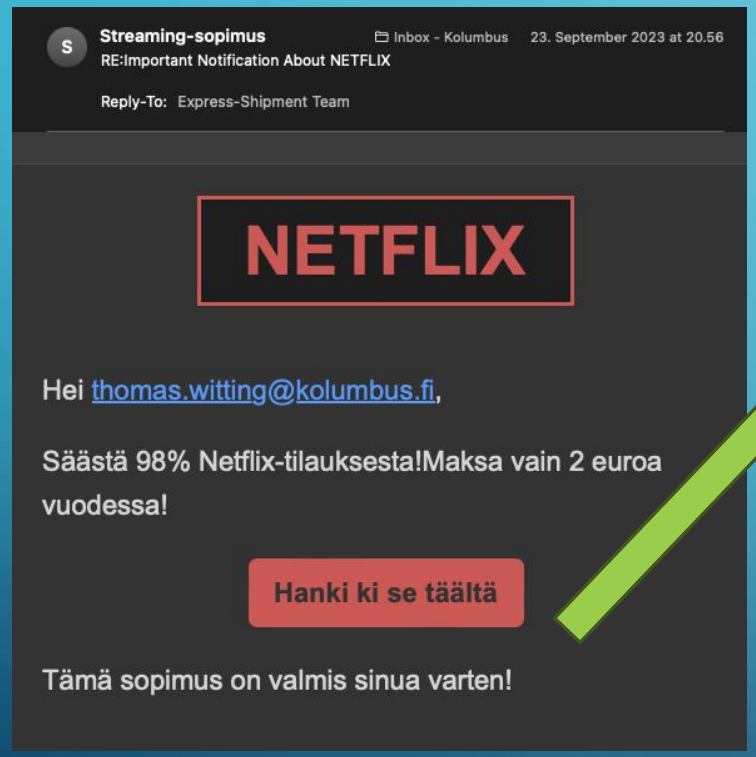
Är länken trovärdig?

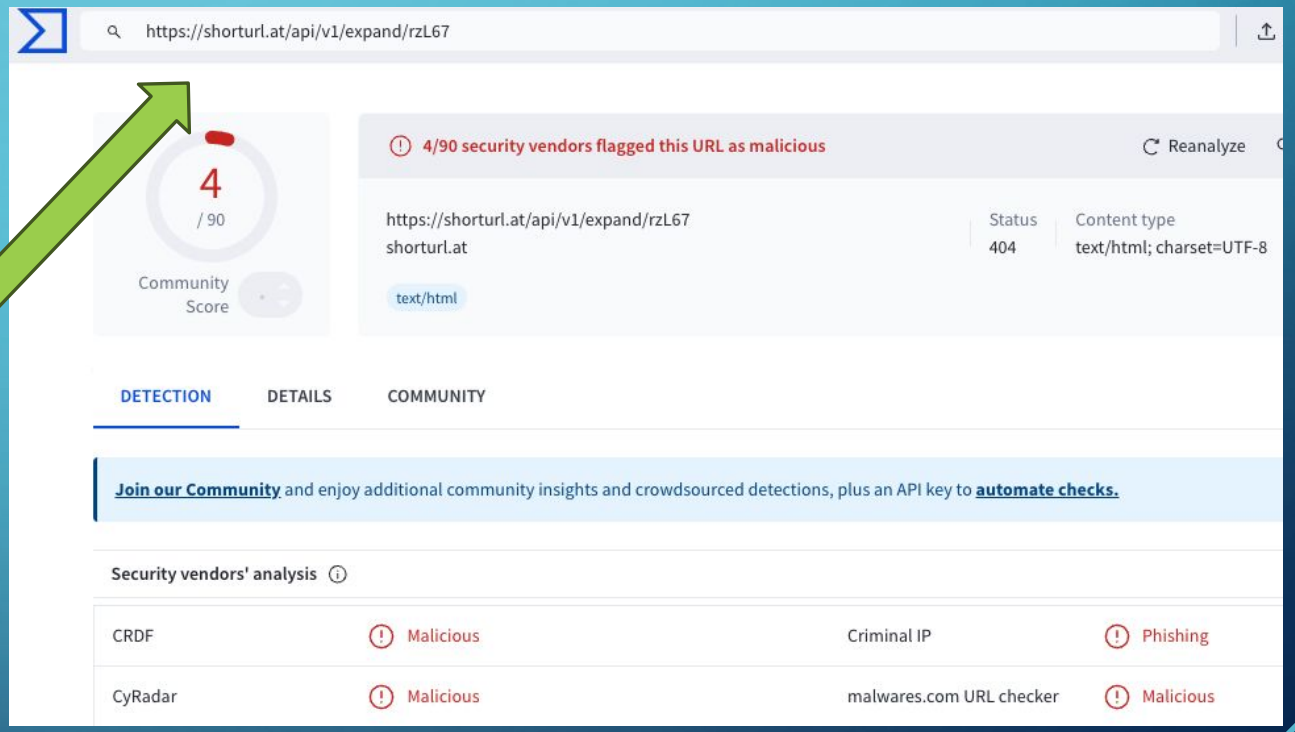
OBS! DE flesta seriösa tjänsterna skickar aldrig meddelanden där man anmodas logga in, man anvisas gå till tjänsten själv.

HJÄLPMEDEL: https://www.f-secure.com/se-sv/link-checker



EXEMPEL MED VIRUSTOTAL.COM





HUR HANTERA LÖSENORD

- ... och varför?

Om vändan att använda unika lösenord

- Förr gick det bra med ett enda bra lösenord på alla ställen, och man kunde till och med låna sin användare och lösen till andra.
- Ofta tänker man att varför skulle det inte gå bra, vissa tjänster låter dig gissa 3 – 5 gånger och sen blir det paus eller så låser sig tjänsten helt.
- Tyvärr är det inte så som det fungerar. En hacker söker sällan en enskild apparat och dess användare utan bryter sig in i system där det kan finnas hundratusentals användare och deras krypterade (hashade) lösenord. Om ett lösenord är använt på flera ställen blir det kalas!

UNIKA LÖSENORD FORTS…

- Såhär ser lösenordet “**kissekatt**” ut i hash form:
- **c0b0b4af21f28f06b2c5ee2ee95ab6658b964acc**
- i den stulna filen står min användare såhär:

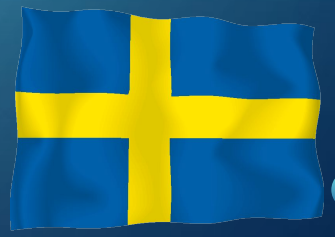
```
thomas, c0b0b4af21f28f06b2c5ee2ee95ab6658b964acc
```

- Det går inte att återfå ordet “kissekatt” genom att mixtra med hashet, det är en envägsprocess, lite som att blanda blå målfärg med gult, man får grönt, men från grönt får man inte tillbaka den exakta blå färgen och motsvarande gul
- **MEN: Man kan gissa!**

ANTAL TECKEN	ENDAST SMÅ BOKSTÄVER	MINST EN STOR BOKSTAV	MINST EN STOR BOKSTAV + EN SIFFRA	MINST EN STOR BOKSTAV + EN SIFFRA & EN SYMBOL
1	OMEDELBART	OMEDELBART	-	-
2	OMEDELBART	OMEDELBART	OMEDELBART	-
3	OMEDELBART	OMEDELBART	OMEDELBART	OMEDELBART
4	OMEDELBART	OMEDELBART	OMEDELBART	OMEDELBART
5	OMEDELBART	OMEDELBART	OMEDELBART	OMEDELBART
6	OMEDELBART	OMEDELBART	OMEDELBART	OMEDELBART
7	OMEDELBART	OMEDELBART	1 MINUT	6 MINUTER
8	OMEDELBART	22 MINUTER	1 TIMME	8 TIMMAR
9	2 MINUTER	19 TIMMAR	3 DAGAR	3 VECKOR
10	1 TIMME	1 MÅNAD	7 MÅNADER	5 ÅR
11	1 DAG	5 ÅR	41 ÅR	400 ÅR
12	3 VECKOR	300 ÅR	2000 ÅR	34 000 ÅR

1.qwerty123
2.qwerty1
3.salasana
4.123456
5.perkele
6.123456789
7.kakka123
8.paska123
9.qwerty
10.Qwerty123

1, 123456
2, qwerty123
3, qwerty1
4, 123456789
5, hejsan
6, hejhej
7, hejsan123
8, bajskorv
9, password
10, 12345678



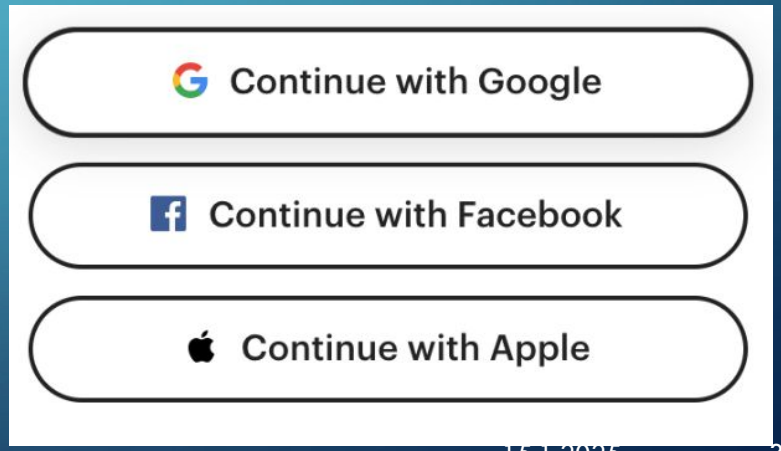
ETT BRA LÖSENORD?

- 10-12 tecken med siffror, små och stora bokstäver och specialtecken #&/%
- Hitta gärna på ett metod för att skapa lösenord, en mening eller lösryckta ord som också är lätt att skriva med knappsatsen på telefonen, längden är avgörande.
- Skriv ner dina lösenord i ett litet häfte som du förvarar noggrant eller
- ta i bruk ett lösenordsvalv om det bara går, det sparar mycket nerver.
  - Det finns både gratis och betalversioner och Windows, Mac, iPhone. iPad och Android har sådana inbyggda, men ifall man använder sig av finska F-Secure kommer det "på köpet"

FORTSÄTT MED …

- Är dethär tryggt?
- SVAR: Ja, förutsatt att:
  - Ditt Facebook, Google eller Apple konto är intakt
  - Du har flerstegsautentisering igång

Det enda som sker är att dehär tjänsterna gör en trygg autentisering av dig till den tjänst du vill logga in på.



PIN KODER OSV.

1234

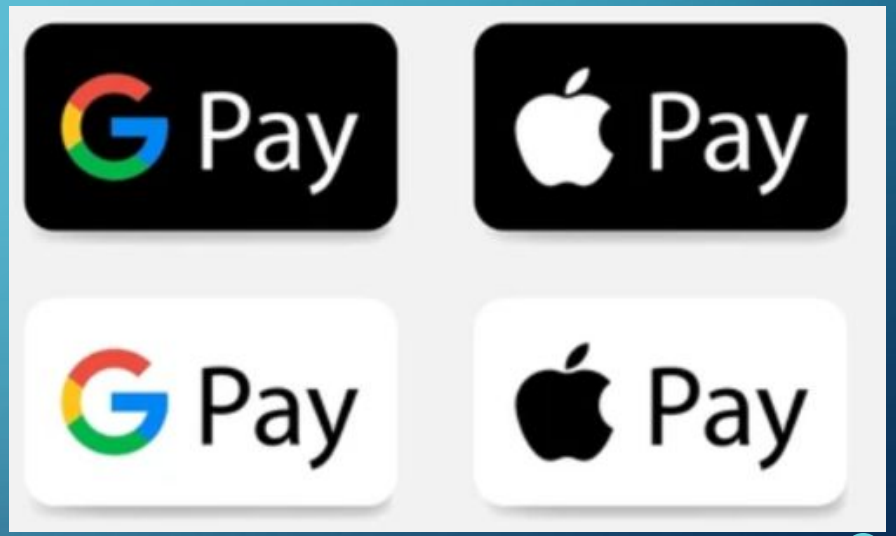
0000

- Telefonen ber vid omstart typiskt om PIN koden för SIM-kortet först, sedan
- vill den ha en PIN kod för bildskärmen
- Den senare koden kan ersättas med lösenord (bokstäver och siffror) eller helst med biometrisk autentisering i form av fingeravtryck eller ansiktsigenkänning.
- Det lönar sig att ta i bruk biometrisk indentifikation, för man kan använda det till exempel i samband med betalningar med telefon eller inloggning till banker. Vid omstart eller power off & on fungerar INTE biometrin på första - PIN behövs

BETALA MED TELEFON ELLER PEKPLATTA

BETALA MED APPLE PAY ELLER GOOGLE PAY I TELEFON - ÄR DET TRYGGT?

- SVAR: Ja, tryggast möjliga sätt för närvarande
- Varför? Jo man visar inte upp sitt kort och sätter inte in det i någon apparat som kan vara kompromitterad
- Särskilt bra kopplat med biometrisk identifikation
- Lätt att ta i bruk - NEJ!



TACK FÖR ATT NI KOM! VAR TRYGGA DÄRUTE PÅ NÄTET!

Det är tryggt att vara på nätet, bara man kommer ihåg att:

- Om det låter för bra för att vara sant är det ofta inte det!
- Om det är fint och passligt och gratis, är det du som är produkten
  - sätt inte ut hela ditt liv på sociala nätverk, det tåget gick för länge sedan!
- Försöka att inte ha bråttom, en dator väntar ofta tålmodigt
- Datorn går väldigt sällan sönder eller slutar fungera genom att du provar dig fram med sunt förnuft.

FRÅGOR , KOMMENTARER ?