Hvem er jeg?

- Alf Høiseth
- Alder 44
- Utdannelse: Bachelor i «Drift av datasystemer» -Hist
- Har jobbet på Institutt for datateknikk og informasjonsvitenskap siden 1997
- Oppgaver: Windows drift, Server, klient, antivirus, programvare, brukerstøtte.

LIVET PÅ NETTET ER FARLIG!

Trender

- Tidligere: Mer harmløse virus og angrep. Ofte for å få prestisje i et miljø eller sverte, ramme bedrifter. Politisk motiv, Hobbybasis.

- Nå: Den økonomiske datakriminaliteten øker betraktelig. Det er blitt en industri. Mafiamiljøer er sterk innblandet. Både bedrifter og privatpersoner rammes hardt.

- Tiden det tar fra et sikkerhetshull oppdages til målrettede angrep iverksettes blir stadig kortere.

Så, hva gjør jeg? Hva trenger jeg av programmer og påpasselighet for at det skal bli bra nok?

Hva er bra nok?

Hva har jeg å tape?

- Data
- Brukernavn og passord
- Miste ansikt (spre ondsinnet kode til slekt og venner)
- Penger
- ID – tyveri

Ingen fasit !!

Utfordringer

- Ulike operativsystem.
  Windows, Mac, Linux, Android
- Flere enheter å passe på .
  Datamaskin, Nettbrett, Mobil, Hjemmenettverk, Smart TV?
- Flere brukere pr. enhet.

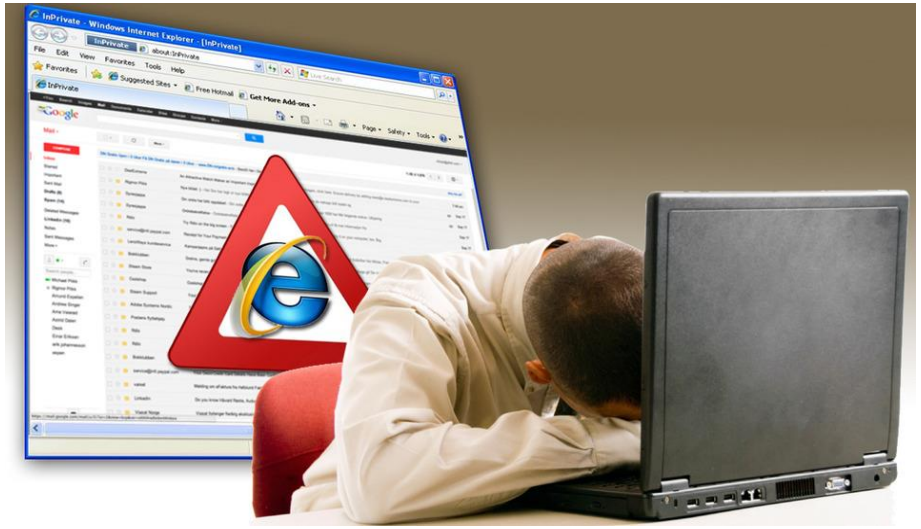
Hvilke trusler finnes?

Noen stikkord:

- Virus, ormer, trojanske hester
- Botnet
- Phishing
- Avlytting
- Spam (søppelpost)
- Spionprogramvare (spyware)
- Sikkerhetshull
- ID – tyveri

Sikkerhetshull

- «Feil» i programvare som setter datasikkerheten i fare.



Hvordan oppdager man ondsinnet programvare/kode

- For å oppdage om en har malware på datamaskinen bør man ha en form for antivirus verktøy som skanner igjennom maskinen. Dersom man ikke har slike verktøy kan det bli nesten umulig å oppdage om man har fått malware på datamaskinen.

Virus

- Ondsinnet programvare som kopierer seg selv inn i filer eller på datamaskinens oppstartssektorer.
- Virus kan kun spres dersom noen kjører en infisert fil. Det vil si at infiserte filer må overføres til mottakers maskin via CD, USB-pinne, eller via nedlasting av filer, for eksempel vedlegg i epost.

Ormer

- En orm er et program som benytter allerede eksisterende kommunikasjonsmetoder for å sende kopier av seg selv til andre datamaskiner.
- En orm kan for eksempel sende en kopi av seg selv som et vedlegg i e-post.
- Kan f.eks stjele passord.

Trojansk hest

- Ondsinnet program som utgir seg for å være noe annet enn det er, eksempelvis et legalt program eller spill. Når brukeren prøver å kjøre eller installerer dette programmet vil datamaskinen infiseres med ondsinnet kode som spyware, virus, etc.

Virus på pc

- Mange opplever å bli offer for ondartet kode i form av **virus, ormer eller trojanske hester**.
- Dersom du er en av dem som har fått din PC infisert, er det noen enkle ting du kan gjøre.

Minimer skaden

Jobb/hjemme?

- Har du tilgang til IT-avdeling eller en person med IKT kompetanse, ta kontakt med dem så fort som mulig.
- Rask rensing av maskin kan gi mindre skade på den, og kan hindre skade eller redusere problemer på andre maskiner på samme eller andre nettverk.
- Koble deg fra Internett. Dette gjør det umulig for en angriper å komme inn på PC-en din. Du hindrer også den ondartede koden i å sende dine personlige data videre eller bruke din maskin til å angripe andre maskiner.

Fjern den ondartede koden

- Har du anti-virusprogramvare installert på maskinen så oppdater denne (dersom det er mulig) og utfør et manuelt scan av hele systemet.
- Har du ikke anti-virusprogramvare, må du skaffe deg dette, enten ved å kjøpe av en lokal forhandler eller laste det ned fra Internett. (Finnes også gratis)
- Klarer ikke anti-virusprogramvaren å fjerne den ondartede programvaren, kan du bli nødt til å reinstallere operativsystemet ditt.

Reduser sannsynligheten for å bli infisert

De som blir infisert og har problemer med å fjerne ondsinnet kode, opplever at det koster tid, penger og data. Noen enkle tiltak reduserer sjansene for å bli infisert:

- **Bruk anti-virusprogramvare og vedlikehold de**. Anti-virusprogramvare kan kjøpes på nettet hos kjente leverandører og kan ofte også lastes ned gratis fra din nettbank.
- Anti-virusprogrammer kan kjenne igjen kjente virus og ormer, og beskytte deg mot disse. Det kommer stadig nye virus. Det er derfor veldig viktig å ha **automatisk oppdatering av anti-virusprogrammet**, slik at det hele tiden vet om de nyeste virusene.
- **Bytt passord om du har vært infisert.** En angriper kan ha fått kjennskap til passordene dine. Du må derfor endre alle passord, inkludert passord for nettsider som kan ha vært lagret i nettleseren din. Forsøk å lag sterke passord som er vanskelige å gjette for angripere.
- **Oppdater programvare og operativsystem.** De fleste programmer inneholder feil som kan utnyttes av angripere. Pass alltid på å installere alle sikkerhetsoppdateringer, slik at angripere ikke kan utnytte kjente feil i programmene du kjører. Mange operativsystemer og andre programmer tilbyr å gjøre oppdateringen automatisk, slik at du selv slipper å følge med på når det kommer nye oppdateringer. Dersom dette finnes for ditt operativsystem og dine programmer, bør du slå på dette.
- **Installer eller slå på brannmur.** Brannmurer kan stoppe noen typer infeksjoner ved å hindre at uønsket trafikk når frem til maskinen din. Noen operativsystemer inneholder en brannmur, men du må selv forsikre deg om at den er slått på.
- **Følg god skikk og bruk for bruk av Internett og e-post.** Ta noen enkle forholdsregler når du bruker e-post og surfer på Internett, slik at du reduserer risikoen for at det du gjør vil føre til en infeksjon. som gir tips til hvordan man kan
- **Sikkerhetskopier dine data jevnlig.** Som en forholdsregel bør du alltid ha sikkerhetskopi av filer du ikke vil miste, for eksempel på CD, DVD eller ekstern harddisk. Da slipper du å miste viktige data dersom du skulle være så uheldig å bli infisert igjen.

Sikkerhetsverktøy

- De fleste Operativsystem har gode mekanismer for beskyttelse. Brannmur og automatisk oppdatering. Bruk dem!
- Antivirusprogram. Kjøpe eller gratis?

  Gratis er ok, men ingen brukerstøtte.
- Noen ressurser

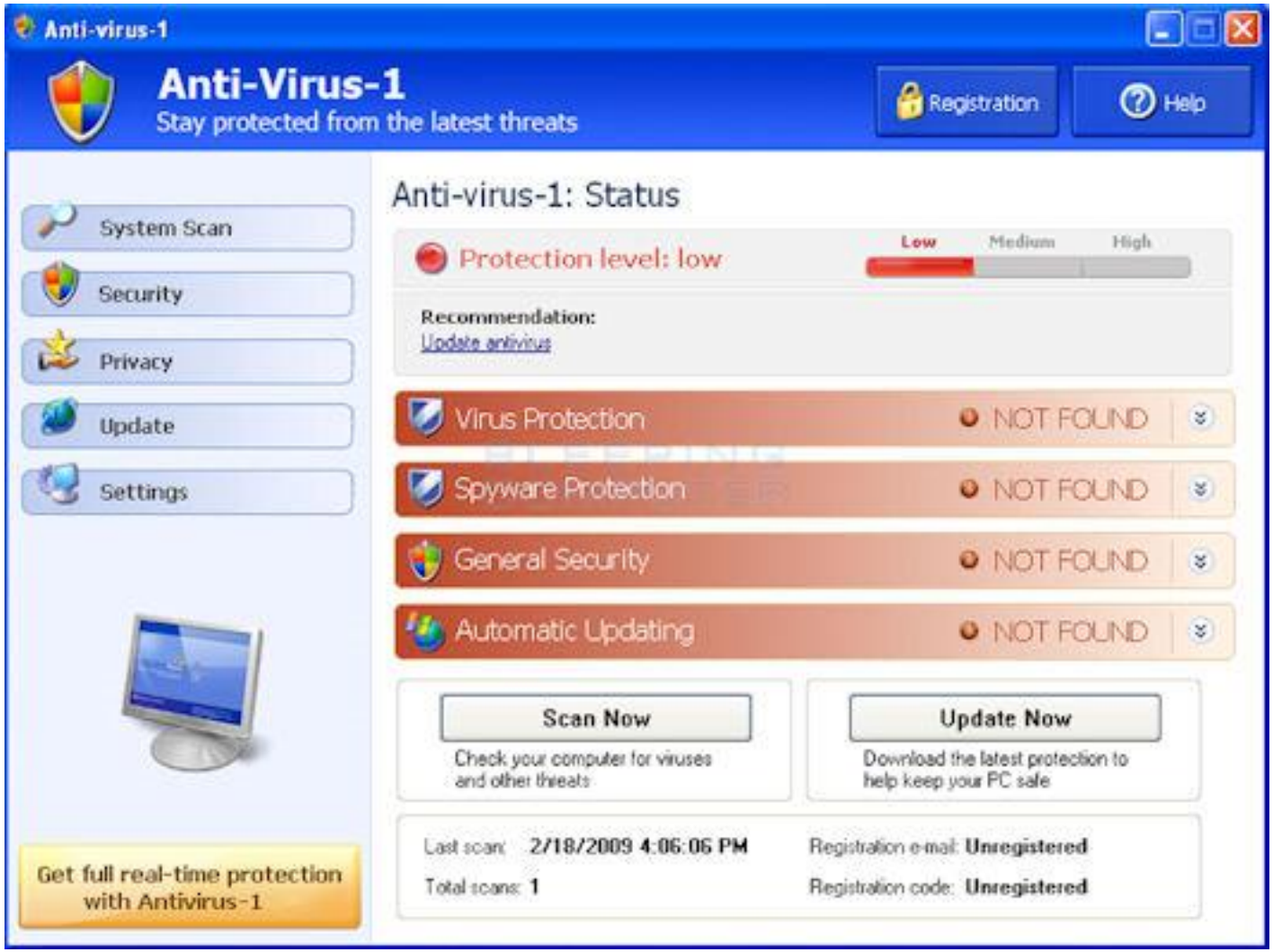
Nettsider som tilbyr gratis online scanning-tjenester:

- Trend Micro Housecall
- Norton Security Scan
- Panda Active Scan
- Bitdefender
- McAfee
- F-Secure

Spionprogramvare

- Spionprogramvare og Adware er begreper som ofte brukes om hverandre. Dette er programmer som i hovedsak brukes av reklamebransjen slik at du blir eksponert for uønsket reklame.

- Maskinen blir ofte treg og man kan få rare feilmeldinger og POPUP vinduer med reklame.


Anti-virus-1
Anti-Virus-1
Stay protected from the latest threats
Registration
Help
System Scan
Security
Privacy
Update
Settings
Anti-virus-1: Status
Protection level: low
Low
Medium
High
Recommendation:
Update antivirus
Virus Protection
NOT FOUND
Spyware Protection
NOT FOUND
General Security
NOT FOUND
Automatic Updating
NOT FOUND
Scan Now
Check your computer for viruses and other threats
Update Now
Download the latest protection to help keep your PC safe
Last scan: 2/18/2009 4:06:06 PM
Total scans: 1
Registration e-mail: Unregistered
Registration code: Unregistered
Get full real-time protection with Antivirus-1

Tiltak mot spionprogramvare

- **Ikke klikk på lenker inni pop-up-vinduer.** Fordi pop-up-vinduer ofte er relatert til spionprogramvare, kan det hende at et klikk på slike vinduer fører til at spionprogramvare installeres på datamaskinen din. For å lukke et slikt vindu må du bruke hurtigtasten [Alt]+[F4] i stedet for å trykke på en knapp i vinduet.
- **Velg "Nei" når du får uventede spørsmål om et eller annet.** Vær varsom med uventede dialogbokser som spør om du ønsker å kjøre et gitt program eller gjøre noe annet du ikke selv har valgt å gjøre. Velg alltid "Nei" eller "Cancel", eller lukk dialogboksen ved å trykke på krysset øverst i høyre hjørne av selve vinduet.
- **Vær varsom med gratis nedlastbar programvare.** Ikke last ned programmer som du ikke stoler på
- **Ikke følg lenker i e-post som later til å tilby programmer mot spionprogramvare.** Akkurat som e-postvirus, kan det hende at lenkene har en annen hensikt, nemlig å installere akkurat den typen spionprogramvare som de hevder å skulle beskytte mot.

Phishing – Fisking
Elektronisk informasjonssvindel

Fristelser – trusler – følelser

Ved phishingangrep kontaktes offeret som regel via en e-post, hvor avsenderen fremstår som en reell virksomhet, for eksempel en bank. Offeret lures videre til å klikke seg inn på en falsk nettside for å "logge seg inn" eller oppgi annen sensitiv informasjon, som konto- eller kredittkortnummer. Dette misbrukes siden av bakmennene.

From: Danske Bank <krlarx@dnksa.com>
To: alfhois@gmail.com
Cc:
Subject: Uvanlig pï¿½loggingsaktivitet !

Uvanlig påloggingsaktivitet

Vi oppdaget noe uvanlig om en nylig å logge på din konto. For å bidra til å beskytte deg, vi trenger en ekstra sikkerhetsutfordring.

Logg på detaljer:
Land/Region: Ukjent
IP adresse: 130.76.220.118
Dato: 15/04/2014 05:22 AM

Hvis dette var du, kan du trygt ignorere denne e-posten.

Hvis du ikke er sikker på at dette var du, en ondsinnet bruker kan ha passordet.
Kan du se den nyeste aktiviteten og vi vil hjelpe deg med å iverksette korrigerende tiltak.

klikk her

Til å avstå fra eller endre der du mottar security-meldingen, klikk her.

Takket være,

Forholdsregler Phishing

- Send aldri personlig eller finansiell informasjon via e-post
- Klikk ikke på lenker i e-post, men kopier heller adressen manuelt
- Vurder avsender og nettsider nøye, før du oppgir informasjon
- Sjekk om adressen er feilstavet eller slutter på .com istedenfor .no, etc.
- Forsikre deg om at nettbanker o.l. krypterer sidene (se etter: https://)
- Bruk e-postfilter, brannmur og antivirus

Trådløst nett (Wi-Fi) Avlytting

Eksterne nett – eks: hotell, flyplasser mm

- **Åpne nettverk.** Bruk trådløse nettverk med en viss skepsis. Alle rundt deg kan se dataene du sender, det er også mulig å sette opp falske aksesspunkter for å overvåke datatrafikken. Hvis du skal sende over sensitiv informasjon på disse nettverkene, bør du sørge for at nettsiden bruker en kryptert tilkobling (https) eller du er koblet opp mot en VPN. Du er også ekstra sårbar for virus og angrep.
- **pc, telefon, nettbrett**

Spam (søppelpost)
Føre-var-prinsipper

- **Svar aldri på spam**

Det er overveiende sannsynlig at varene og tjenestene det lokkes med er svindel. Ved å svare oppnår du bare å bekrefte e-postadressen din.

- **Skru av HTML-visning**

Du bør vurdere å vise e-post som ren tekst (plain text), og dermed deaktivere HTML-visning. Da unngår du å bli rammet av såkalte web bugs som sjekker om adressen er gyldig og at du faktisk har lest e-posten.

- **Skru av bilde- og forhåndsvisning**

Ønsker du å beholde HTML-visning, kan du vurdere å deaktivere visning av billedlenker. Ved å skru av forhåndsvisning av e-post, kan du slette mistenkelige meldinger uten å åpne disse først.

Adressevern (e-post)

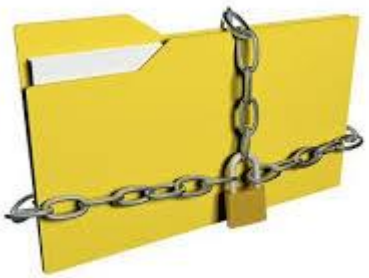
Beskytt deg mot uønsket e-post

Vær forsiktig med hvor du legger igjen e-postadressen. Havner den først i en spamliste risikerer du søppelpost i årevis fremover.

Forholdsregler

- Legg aldri ut adressen i klartekst på nettet
- Benytt eventuelt et bilde av adressen
- Vær kritisk til å oppgi adressen i skjema o.l.
- Svar aldri på spam – da bekrefter du adressen
- Opprett eventuelt en egen adresse hvor du tolererer spam

Vern om personopplysninger



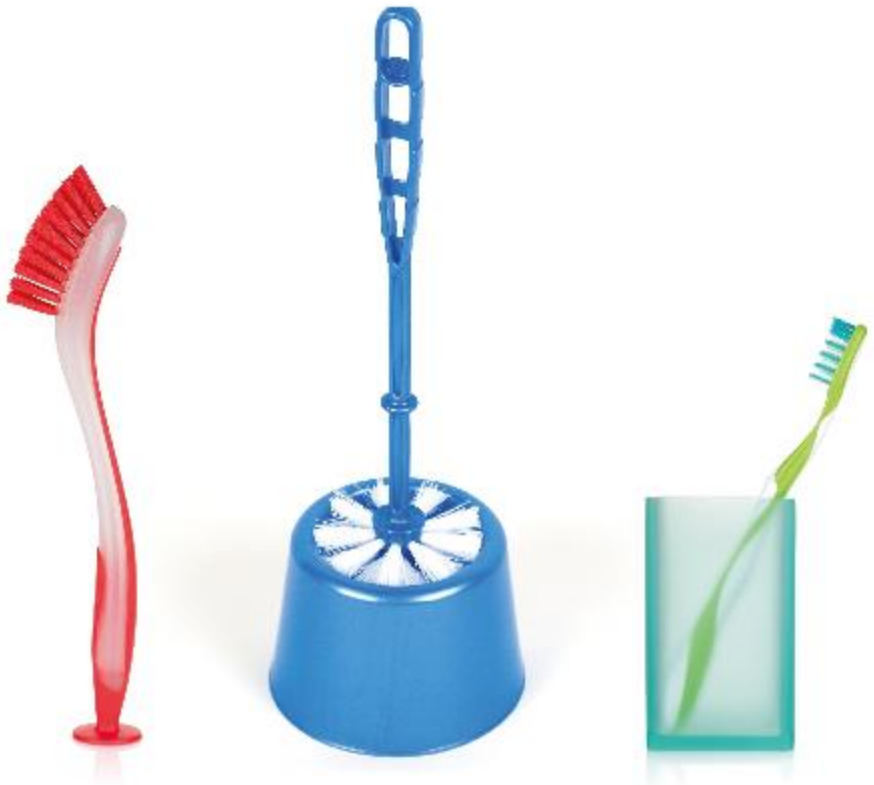
1. Handle med pålitelige virksomheter
2. Unngå å legge igjen informasjon om kredittkort
3. Ha eget kredittkort for bruk på Internett
4. Unngå bruk av debetkort
5. Bevis på at personopplysningene blir kryptert

Passordvett

- Et passord skal være lett å huske for deg og vanskelig å gjette for andre
- Benytt ulike passord for ulike tjenester
- Passordet bør være så langt som mulig
- Bytt passord med jevne mellomrom eller hvis du tror det er på avveier

STOPP. TENK. KLIKK.

Du bruker ikke samme børste overalt, hvorfor bruke samme passord?



Noen eksempler på passord

Lag forskjellige passord på forskjellige tjenester.

- Bruk et setning som du assosierer med tjenesten, men ikke direkte navnet på tjenesten. Eksempelvis trenger du passord for nettbutikk for bøker. Passordet kan da være en setning knyttet til yndlings-boka eller forfatteren din. Setningen bør ha mellomrom eller andre spesialtegn. Dette gjetter ingen og det er også vanskelig å knekke for hackere.
- «moRn, jeg heter Kari» er lett å huske, for langt til å knekkes og vanskelig å gjette. Passord som består av vanlige ord må helst være mer enn 20 tegn. Har du med blank og andre spesialtegn kan det være kortere.
- «Nthls11st» ser ut som et vrient passord å huske. Passordet er første bokstav fra hvert ord i sangstrofen «Når trollmor har lagt sine 11 små troll». Slike passord bør være mer enn 9 tegn.

Utenlands

- **Du er ekstra sårbar i et annet land**
- Du kan bli utsatt for tyveri og spionasje overalt. Sannsynligheten for slike hendelser er imidlertid større i mange andre land enn i Norge.
- **Forholdsregler**
- Legg ikke igjen datautstyr med sensitiv informasjon på hotellrommet
- Krypter sensitiv informasjon på PC, mobiltelefon og PDA
- Skru av blåtann og trådløse nettverk på bærbart datautstyr
- Bruk VPN-forbindelse eller andre sikkerhetsmekanismer
- Bruk helst datautstyr uten for mye kritisk informasjon på når du er på reise.
- Følg ellers rådene for bruk av andres PC-er og eksterne nett

Når du rammes

Dersom du tror noen kan ha fått tilgang til kontoen eller kredittkortene dine må du umiddelbart kontakte bank eller utsteder. Sjekk også kontoutskrifter og kredittkortregninger for mistenkelige belastninger.

En liten demo

- Live Hacking

- Norsk senter for informasjonssikring (NorSIS) demonstrer sårbarheten ved å ha utdatert programvare på PC.

Min konklusjon

- Antivirus hjelper, men man er ikke 100 sikret.
- Brukerens adferd den største faren for at uheldige situasjoner oppstår.
- Hvis uhellet har skjedd, eller man har mistanke?
  - Finn informasjon om problemet på nett.
  - Ta kontakt med noen som har peiling.
  - Ta nødvendige forholdsregler inntil problemet/mistanken er avverget.

NorSIS anbefaler

- Oppdater alltid alle programmer på PC-en, og sørg for å oppdatere så fort som mulig når rettelser kommer. Ikke koble til trådløse nettverk du ikke er sikker på opphavet til.
- Se etter «S»-en i adressen til nettsteder du logger deg inn på. Adressen skal starte med «HTTPS» for at den skal være sikker. Se også etter hengelåssymbolet ved adressefeltet.
- Slå på kryptering av e-posten din på mobiltelefonen, og ikke la den søke etter åpne nettverk når du beveger deg ute.
- Vær forsiktig med mobilapper du laster ned utenfor de sertifiserte app-butikkene til leverandøren.
- Tenk deg om før du klikker på lenker i e-poster og SMS-er, også fra avsendere du har tillit til.

Takk for meg og lykke til ☺

- Kilder: