Willi Nielsen Mobil: (+45) 2030 0104 e-mail: willi.6340@outlook.com

Smartphone / Tablet, Android, Undervisning, februar, 2016.

Sikkerhed på din Smartphone og tablet.

1. Sikkerhed på en Smartphone / tablet.

På din "normale" PC har "man" normalt installeret et anti-virus-program.

Der er en del debat om graden af sikkerhed og nødvendigheden for antivirus-beskyttelse på en tablet.
Herunder gives nogle guidelines for dette emne.

2. Begreber for sikkerhed på en tablet (og ligeledes for Smartphones).

Sikkerhed på "mobile enheder" (her defineret som Tablets og Smartphones) omfatter disse hovedemner:

a) Antivirus, Spyware, Malware
b) Phishing
c) Firewall

Ad a) Antivirus, Spyware, Malware.
På en "mobilenhed" afvikles der **ikke** programmer (programmer afvikles på en PC), men **apps** (applications).
Et **program** kan interagere med andre programmer og dermed "sprede en virus".

En app har ikke "adgang" til en anden app, og kan **derfor ikke sprede en evt. virus**.
En app

- kan ikke "selv replikere"
- kan ikke komme ud med en virus (kan ikke sprede en virus)
- kan ikke eksekvere (udføre) en såkaldt exe.fil, som er den metode, hvorved en virus spredes på en "normal" PC,

Derfor er der **ikke umiddelbart behov** for en antivirus-app på en tablet (se dog nedenfor under Windows 8.1).

Ad b) Phishing,
Kort dansk beskrivelse = "at fiske" oplysninger fra en bruger via e-mail (eller via SMS, beskeder).

Phishing er et internetfænomen, hvor svindlere forsøger at franarre godtroende internetbrugere deres brugernavn, adgangskode, kreditkort- eller netbank oplysninger.

Willi Nielsen Mobil: (+45) 2030 0104 e-mail: willi.6340@outlook.com

Det sker typisk ved at brugeren får tilsendt en e-mail eller fx en direkte besked på Twitter, hvis indhold forsøger at få brugeren til at indsende sine oplysninger pr. e-mail eller logge ind på en falsk internetside, der ligner f.eks. bankens. Mailen kan fremstå, som om den er afsendt fra et socialt medie, en auktionshjemmeside, en IT administrator eller en person fra modtagerens adressekartotek.

Phishing er altså mere en "personlig handling udført af brugeren", og **man kan derfor ikke beskytte sig med en eller anden form for "værktøj"** (anti-phishing program eller app).

Ad c) Firewall,
Formålet med en Firewall: at beskytte sin PC eller tablet eller smartphones mod "uhensigtsmæssig" trafik.

En **firewall** eller på dansk en **brandmur** er et stykke netudstyr eller software, der udvælger hvilke netværkspakker som skal have adgang fra den ene side af en firewall til den anden side efter et regelsæt.
Oftest sidder firewallen mellem

- adgang til og fra et ubeskyttet netværk som fx Internet ("den store verden")
- og et beskyttet netværk fx LAN ("din egen verden" = dit netværk i dit eget hjem).

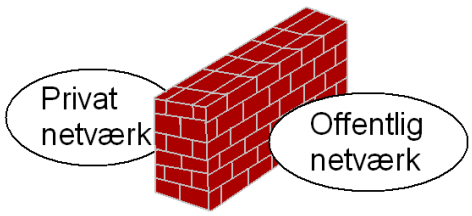
En firewall skal således hindre uautoriseret adgang til **det interne netværk**.

Firewallen er typisk "et sæt af regler" i en konfiguration af det software, som befinder sig i en router eller i en PC.

Regelsættet i en firewall **fungerer som et filter**, så den første regel, som den aktuelle trafik passer med, bliver brugt. Det betyder, at de specifikke regler skal defineres først og de generelle senere.
Et simpelt regelsæt for en personlig firewall kunne være:

- Tillad al trafik **fra** denne maskine.
- Tillad al trafik **til** denne maskine, **hvis** det er et svar på en "fra" (udgående) trafik,
- Log det, der ikke er taget stilling til og fortsæt med næste regel,
- Afvis det, der ikke er taget stilling til.

I et privat hjem er den vigtigste enhed for Firewall = din router, fordi denne router er forbindelsen mellem "det ydre" og "det indre" netværk.



Firewall kontrollerer trafikken gennem "porte",
Alle enheder har en IP-adresse (Internet protocol adresse), som er unikt "i hele verden" for den pågældende enhed. (En sandhed med tekniske modifikationer – afhængig af NAT-opsætning).

Network Address Translation (NAT) is the process where a network device, usually a firewall, assigns a public address to a computer (or group of computers) inside a private network. The main use of NAT is to limit the number of public IP addresses.

I private hjem kommer IP-adressen via routerens IP-adresse, et eksempel: 192.168.0.128

IP-adressen på din tablet (og smartphone) kan du se under Indstillinger, herunder "Om tablet", herunder "Status".

3. Afhængig af styresystem er der forskel på sikkerhed for en tablet.

Det er vigtigt at skelne mellem de forskellige styresystemer, som anvendes på en tablet:
De 3 mest udbredte:

a) Android,
b) iOS (Apple),
c) Windows 10,

ad a) Windows:
En enhed med Windows 10 kan køre **både** programmer **og** kan køre apps.
På grund af, at Windows 10 – både på en PC og en tablet - kan køre programmer, bør der aktiveres et "antivirus program"
Hvis man har en tablet med Windows 8.1 **skal man aktivere** det præinstallerede "Windows defender", der er en fast komponent af Windows styresystemet.
Windows defender er normalt aktiveret ved køb, men kan være deaktiveret, hvis der er præinstalleret et andet virus-program (f.eks. Norton, McAfee,,,).
Hvis man så senere fjerner / sletter Norton, McAfee så **skal man selv aktivere** Windows defender.

Ad b) Android
Her gælder betragtningerne ovenfor under afsnit 2.

4. Sikkerhed-apps til tablet, et udvalg.

Du kan søge på nettet med søgeord "android tablet sikkerhed", hvorved der kommer diverse gode henvisninger.

http://www.appsandroid.dk/joomla/apps/sikkerhedbackup.html
fra 2012

Herunder er udvalgt 4 sikkerheds apps, jeg kan ikke anbefale den ene frem for den anden, da det afhænger af, hvordan du selv bruger din tablet.

Hermed menes, om du bruger din tablet til at læse e-bøger, til at gå på nettet for at finde informationer, om du bruger den til "personfølsomme oplysninger" på sociale tjenester, om du bruger den til din Netbank, E-boks, Sundhed.dk, Borger.dk ,,,,

- Android-security-Avast
- Android-security-AVG
- Android-security-Ahnlab
- Android-security-Anguanjia

5. Avast-app, omtale.

Mobile Security & Antivirus - Avast

Beskrivelse:

Installer den i dag - helt **GRATIS**.

- Beskyt din Android-telefon og -tablet med den topvurderede **(4,5 stjerner!)** gratis sikkerheds-app til mobiler, med både antivirus- og antityveri-funktioner.
- Avast Mobile Security beskytter din enhed mod virusser, malware og spyware
  Den hjælper dig med at lokalisere din mistede telefon via vores web-baserede lokaliseringsfunktion.
- Ekstern låsning af din enhed og/eller sletning af hukommelsen med den avancerede Anti-Theft-komponent beskytter din data.

- Nyttige funktioner som netværksmåler, app-administrering og endda firewall (på rootede telefoner) giver dig fuld kontrol over din mobiltelefon.
- Antivirusmotor: Scanner installerede apps, indhold af hukommelseskort og nye apps automatisk ved første anvendelse.
- Kør automatiske scan, når du sover Inklusive SMS-/filscan, for komplet mobilsikkerhed.
- Brugt af millioner af mennesker og anbefalet af højtstående Android-myndigheder:
  - ★ AndroidAuthority: *"Det bedste er blevet endnu bedre... intet kommer i nærheden"*
  - ★ Android and Me: *"Den bedste anityveriløsning på markedet."*
  - ★ AndroidPolice: *"Ganske enkelt alt du har brug for, hvis din enhed mistes eller bliver stjålet."*
  - ★ Droid-Life: *"Det bliver ikke mere omfattende end dette".*

6. AVG-app, anmeldelser / omtale.
Anmeldt april 2013.

Funktioner og indstillinger:
En scanning af hele telefonen startes med et enkelt tryk på skærmen, og *AVG Antivirus* har fire overordnede elementer der indgår i en scanning:

- Apps.
- Indstillinger.
- Mediefiler på SD kortet (billed, lyd, og video filer).
- Indholdet (kontakter, bogmærker og *SMS*).

Der er mulighed for at tage backup af dine *apps* til SD kortet, samt låse de apps du bare vil beholde med en kode. Dette er lidt sejt, for så kan tyven ikke afinstallere de apps der hjælper dig med at finde ham.
Du kan også tage backup af indstillinger, bogmærker, *SMS* osv. Denne sidste funktion er i beta, og det er gendannelses-funktionen også.

Der er også indbygget task-killer, som kan slukke dine kørende programmer og frigive mere RAM (det er en anden diskussion, hvorvidt det er nødvendigt eller ej).

Hvis du får en mistænkelig *SMS*, eller du browser rundt på nettet, og finder en mistænkelig webside, så kan du rapportere det til hovedcentralen. Du kan også blokere indgående opkald og SMS`er.

Èn af de fedeste detaljer er Findr, som er en service der hjælper dig med at finde din forsvundne Android mobiltelefon. Det du gør, er at logge ind på **Droidsecurity`s webside**. Når du har logget ind med din Google konto, møder du et stort kort hvor du kan se hvor din telefon befinder sig. Udover det er der følgende muligheder enten via websiden eller SMS:

- Lost (se på kortet hvor din mobiltelefon befinder sig lige nu).
- Found (når du har generhvervet din Android).
- Lock (lås din telefon)
- Wipe (slet alle data på telefonen).
- Lost message (bestem hvad der skal stå på den låste skærm, efter du har låst den).
- Disable roaming (slå roaming fra, så det ikke kan lade sig gøre at roame).

AVG Antivirus understøtter 15 sprog hvor dansk ikke er et af dem.
Når du downloader en app fra Android market, scanner AVG Antivirus app`en, og viser et lille ikon i statusbaren efter end scanning, om scanningen er godkendt. Der er også en *widget*, der fortæller dig om telefonen er clean eller ej.

Brugervenlighed:
Når du åbner app`en bliver du mødt af et ikon, jeg bedst kan beskrive som lignende de Ritalin uno jeg får imod ADHD. Anyway, så med et enkelt tryk på skærmen går scanningen igang. Efter endt

scanning bliver du oplyst om hvor mange apps, mediefiler, kontakter, bogmærker, og SMSèr der er blevet scannet for *malware* og vira. Dette er meget hurtigt og nemt.

Når du downloader *apps*, musik eller andet, scanner *AVG Antivirus* som sagt det downloadede element. Dette foregår lige så stille i baggrunden, og du er ikke nødt til at hive statusbaren ned for at bekræfte noget som helst efter godkendt endt scanning. Det fungerer synes jeg. Da menuen er på engelsk kan det godt, for ikke så godt engelsktalende, tage lidt tid at finde ud af hvad de forskellige funktioner er til, og hvordan man konfigurerer dem.

7. Virusfighter, anmeldelser / omtale.
(Fra marts 2012)
VIRUSfighter er en anti-malware app, og må ikke forveksles med andre **Android antivirus apps** som **AVG Antivirus** og **Super security** der har flere funktioner.

Meningen er at den skal scanne din mobil for uønskede ting, og der gør den et rigtig godt job, endda uden at bruge alt for meget batteri.

Jeg er svær at imponere, når det kommer til det her med apps, men jeg er imponeret.
VIRUSfighter er virkelig nem at bruge, den er gratis, og den leverer varen. Står du og mangler en antivirus-app kan jeg kun anbefale *VIRUSfighter*.
VIRUSfighter fungerer både på Android tablets og mobiler.

En så simpel, men stadigvæk brugbar app skal have gode karakterer. Flot stykke arbejde.

8. Kommentarer til brug af Nem-ID via din tablet (eller Smartphone).
Du kan uden problemer logge på de "offentlige digitale tjenester" (borger.dk, sundhed.dk, SKAT.dk,,,) og din egen netbank via din NemID-logon proces.
For NemID er sikkerheden kontrolleret i selve bruger af "NemID" – og ikke i din tablet (eller Smartphone), så en antivirus-app vil ikke ændre på sikkerheden omkring brugen af NemID.
Siden efteråret 2014 har firmaet bag ved NemID (firmaet Nets) haft sin egen app til brug af logon til Nemid på "mobile enheder".

Lidt om sikkerheden ved brug af NemID på mobile enheder:
https://www.nemid.nu/dk-da/privat/sikkerhed/gode_raad_om_sikkerhed/pas_paa_falske_hjemmesider/index.html

9. "Gode almene råd" om beskyttelse af tablet / smartphone.
Fra "Alt om Data", marts 2013.
http://www.altomdata.dk/de-bedste-tips-til-tablet-sikkerhed-1

a) Beskyt din mobile netbank:
Mobil netbank er populær. Siden 2009 har der været en stigning på 200 % i antallet af brugere. Over en milliard mennesker vil bruge mobile enheder til at få adgang til bankydelser ved udgangen af 2017, og den største bekymring for brugere af mobil netbank er sikkerhed. Og med rette. Vi dækker vores pinkoder, når vi betjener en pengeautomat på gaden, så lad os være ligeså forsigtige online.

TIPS:

- Download din banks mobil-applikation til din tablet, så du kan være sikker på at besøge den rigtige bank hver gang, og ikke et site, som kan udnytte dine personlige data.
- Undgå at gå online på din mobile netbank fra offentlige Wi-Fi spots. Hvis du absolut skal, så sørg for, at det er et sikkert netværk og ændr din adgangskode med det samme bagefter. Sørg for at du logger ud af sitet snarere end blot at lukke browseren.
- Hvis du mister din tablet, skal du kontakte din bank omgående, så den kan holde øje med dine bankaktiviteter og afsløre eventuel svindel.

Willi Nielsen Mobil: (+45) 2030 0104 e-mail: willi.6340@outlook.com

b) Minimer dit tab:

Tablets kombinerer to af de funktioner, en tyv elsker: de er værdifulde såvel som små og transportable - og følgelig stjæles flere og flere tablets. Idet mange af os nu medbringer vores tablet overalt, er tabet af mobile enheder stigende. Det er selvfølgelig ikke kun den fysiske enhed, der går tabt, men også de værdifulde personlige data, der findes på den.

TIPS:

- Installer GPS-software, som gør det muligt for dig at spore din tablet, hvis du mister den.
- Sørg for at have din enheds serienummer ved hånden – det kan du give til myndighederne, hvis du mister den.
- Hvis du mister din tablet, bør du straks ændre dine online adgangskoder (sociale medier, bank osv.), især for applikationer, der automatisk logger dig ind.
- Fortæl din bank, at et potentielt sikkerhedsbrud har fundet sted, så de kan holde ekstra godt øje med dine konti.

c) Tjek før du tilslutter dig et trådløst netværk:

Overalt, hvor du befinder dig, fra cafeer til lufthavne, er der **nu gratis Wi-Fi** – fantastisk, når du vil online med din tablet. Faktisk er 17% af de mobile enheder, der anvender trådløse hotspots, nu tablets. Men hackere kan komme ind på usikre trådløse hotspots lige så nemt, som du kan. Dette betyder, at de potentielt kan få adgang til din tablet, og dermed få adgang dine e-mails, dine filer, dine billeder.

TIPS:

- Sørg for, at du opretter forbindelse til det rigtige Wi-Fi-hotspot. Hackere opretter ofte hotspots på cafeer med navne som "Gratis Wi-Fi" for at tillokke brugere.
- Vær opmærksom på fejl, som at en hjemmesides certifikat er "udløbet" eller "ugyldig" - dette kan betyde, at en hacker har fået adgang til Wi-Fi-netværket. Prøv at indtaste webstedets webadresse igen, og hvis du stadig ser fejlen, så forlad netværket.
- Der findes masser af offentlige Wi-Fi-hotspots, og nye vil blive ved med at dukke op. Men mange vil, i hvert fald på kort sigt, forblive åbne uden den nødvendige sikring. Offentlig Wi-Fi-sikkerhed er i sin vorden, så begynde at handle sikkert nu.

d) Beskyt dine adgangskoder:

Aktivitet på sociale medier er en del af de flestes daglige rutiner.
Sociale netværk er blevet en af de mest populære og tidskrævende online-aktivitetet – med globale brugere, der tilbringer omkring 22% af deres tid online på sociale medier.
Mens de fleste af os ville være forsigtige med at uddele vores sociale netværkspasswords til vores venner, forbliver mange af os permanent logget ind på vores tablets, og gør os dermed sårbare over for sikkerhedsbrud.

TIPS:

- Hvis du er nødt til at forblive logget på dine sociale mediekonti på din tablet, sørg da for at have et stærkt personligt identifikationsnummer (PIN) eller adgangskodelås til din tablet for at forhindre uautoriseret adgang.
- Beslut dig for, hvilke af dine netværk, der er i højrisiko, og hvilke, der er i lavrisiko, og prioritere sikkerhed herefter.
- Hvis du har et netværk, som indeholder følsomme forretningsmæssige eller personlige data, så overvej at implementere yderligere sikkerhedselementer.
- Gennemgå nøje de sociale medieapplikationer, du downloader. Sørg for, at de stammer fra en velrenommeret udgiver. Læs også app'ens fortrolighedspolitik med henblik på at kontrollere, hvor stor en del af dine data, app'en vil få adgang til, og hvad den eventuelt vil dele med en tredjepart.