Gode råd generelt:

- Hold din computer og programmer opdateret.
- Hold din computer opdateret med antivirus og firewall.
- Kontroller et link hvis du er i tvivl.→ 

- Vær skeptisk over for alle mails du modtager (også fra dem du kender. Svar evt. på mailen).
- Vælg ”offentligt netværk” når du kobler på wifi.
- Undgå offentlig wifi (f.eks. lufthavn, hotel, café osv.).
- Undgå at bruge din ”officielle” mail til det hele → 

- Gør dig selv til bruger på computeren (ikke admin).

Ransomware:

- Betal aldrig løsesummen
- Hold alt opdateret (også APP´s)
- Sørg for at have en offline backup (f.eks. ekstern harddisk)
- Hav ikke ”kompromitterende” eller belastende data liggende på online maskiner.
- Sørg for der også er backup på dine data i skyen
- Lad ikke data ”samle støv” → læg dem på en backup

Mobiltelefon:

- Vær skeptisk hvis din telefon går på 2G (Edge).
- Slå Bluetooth, GPS og WIFI fra når du ikke bruger det.
- Pas på phishing via SMS/MMS, Sociale medier osv. → Kontroller link.
- Installer antivirus på din enhed.
- Vær skeptisk når du henter APP´s.
- Begræns dine APP´s adgang til mikrofon, kamera, lokaliteter, billeder, kontakter osv. (Læs betingelserne).
- Brug kun din egen lader til mobilen.

Sociale medier:

- Vær kritisk mht. de informationer du lægger op.
  - Kan det tåle at stå på en plakat et offentligt sted?
  - Alt du lægger op bliver der for evigt og er ikke længere dit.
- Begræns de personlige informationer du deler.
- Hop ikke på ”clickbaits”
- Skil dit arbejdsliv fra dit privatliv
- Anvend sikkerhedsindstillinger (begræns din profil).
- Accepter kun venner du kender i virkeligheden.
- Vær skeptisk når du møder en på nettet.
- ”Google” dig selv, eller få en anden til det. Reager på det du ikke er bekendt med.

USB nøgler:

- Anvend aldrig USB enheder du ikke kender.
- Finder du et USB så få en IT kyndig til at undersøge det. Eller smid det ud.
- Krypter dine USB enheder (f.eks. BITLOCKER).
- Anvend aldrig billig USB enheder fra f.eks. Kina og lignende.
- Anvend aldrig billige USB ledninger (f.eks. til ladning)

Password

- Minimum 12 karakterer (Gerne 15)
- Brug ikke kendte/personlige ord
- Skift det jævnligt (max. 180 dage)
- Brug forskellig password til hver tjeneste/login
- Brug ”Two-Factor Authentication” ved login.

Social Engineering:

- Vær skeptisk i mærkelige situationer (f.eks. opkald)
- Er du i tvivl om rigtigheden, valider informationen fra andet sted
- Oplys aldrig personlige oplysninger på alm. mail eller telefon
- Makuler personfølsom affald
- Intet er gratis, så vær skeptisk hvis en ydelse præsenteres som gratis.

Internet of Things (IoT):

- Skift altid standard password
- Anvend ikke billigt udstyr købt på f.eks. ebay m.m.
- Segmenter smart TV, køleskab osv. fra resten af dit netværk
- Tag internet stikket ud af udstyret når det ikke anvendes

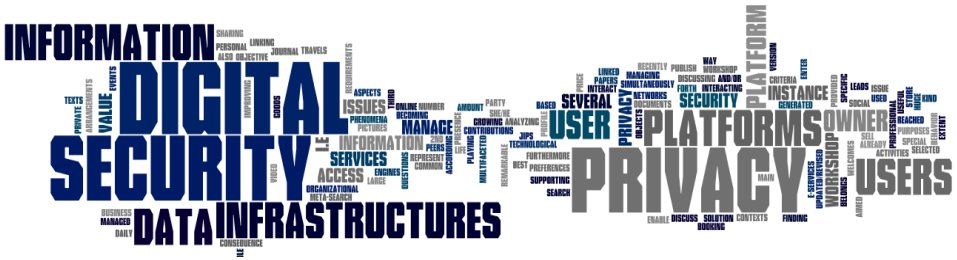
Browsing på internettet:

- Lad aldrig browseren huske dine koder
- Brug ikke den samme browser til alt
  - Explorer = Generel surfing
  - Firefox = Sociale medier, indkøb, hvor der skal logges ind.
  - Chrome = Netbank, aktier m.m.
- Tilføj en ADD-Blocker i browseren (FireFox & Chrome)
- Besøg kun sider du har tillid til (HTTPS).

OPSUMMERING

(De 6 gode råd)

1. Opdater altid din computer og programmer. ALTID!
2. Brug ikke USB udstyr du ikke kender.
3. Klik ikke på nogen links eller filer → Er du i tvivl, er du ikke i tvivl.
4. Lav password på mindst 12 karaktere, uden de er personlige og brug 2-factor.
5. Hav en offline backup af dine vigtige filer (f.eks. på ekst. Harddisk).
6. Brug ikke offentligt WiFi (bus, tog, hotel, lufthavn osv.).



CYBERTRUSLEN

Hvad kan du gøre?

December 2017

Få tiltag du som privatperson kan gøre, for at mindske risikoen for et hackerangreb eller anden kompromittering på internettet.

Udarbejdet af
Martin Kaasgaard
cyber@AWAR3N3SS.dk