Dediko®
Your Security is our Passion

STALDTIPS fra cyberhesten
(mest til din private brug af laptop eller telefon/tablet)

1. Tag regelmæssigt en backup af de data du ikke vil miste og gem dem på et offline medie som er låst væk. Vær sikker på at data ligger i et format som du til enhver tid kan læse og genskabe.
2. Når du browser Internettet:
    a. Brug en regelmæssigt opdateret browser (fx Google Chrome tre prikker, Hjælp, Om Google Chrome vil opdatere den automatisk)
    b. Hold dig til sider som du forventer er sikre og sørg for at der er et DNS/URL filter aktivt på din klient, fx via din anti-malware løsning
    c. Hold dig fra sider som ikke er krypterede (hængelåsen foran siden du besøger) men husk at hængelåsen kun betyder at kommunikationen mellem dig og siden er krypteret – ikke nødvendigvis at siden er sikker
    d. Pas på med hvilke add-ons du tilføjer din browser. Nogle kan være ondsindede og nogle kan spore hvad du ser og hvilke sider du besøger
    e. Gem ikke passwords i din browser men brug fx den gratis udgave fra lastpass.com til at hjælpe dig med at opbevare og huske passwords som er unikke, lange og komplekse for hver Internet service som du har en kode til.
    f. Slet din historik i browseren regelmæssigt og google hvordan du sætter din browser sikkert op – f.eks. chrome://settings/safetyCheck. Søg efter dette via Google eller på YouTube
3. Når du bruger e-mail:
    a. Tænk på at den e-mail du læser, måske ikke er fra den person du ser som afsender?!
    b. Før du klikker på et link så hold musen over linket og se om det leder til en hjemmeside som du stoler på.
    c. Se på nettet efter artikler som kan hjælpe dig med at blive god til at spotte ondsindede links – f.eks. https://gatefy.com/blog/malicious-emails-tips-recognize-them/
    d. Pas ekstremt meget på med vedhæftelser. Det gælder også almindelige dokumenter som f.eks. Word eller PowerPoint som kan indeholde ondsindede makroer. Du kan spotte det på det ikon som viser hvad dokumentet er
    e. Gem ikke personlige eller sensitive data i din e-mail

   f. Hvis du tilgår din e-mail via en Internet service – f.eks. gmail – så sørg for at den også er beskyttet med 2-faktor godkendelse via din telefon
   g. Undgå at falde for et phishinglink hvor du uforvarende kommer til at afgive dine adgangskoder, personlige data eller bliver lokket til noget som kan føre til datatab eller ransomware.
4. Når du skal bruge en adgangskode:
   a. Dine passwords SKAL være unikke og mindst 14 karakterer lange. Undgå at bruge kendte ord fra ordbogen, sekvenser af karakterer fra tastaturet. Brug LastPass til at gemme passwords. Et eksempel på et "godt" password som du kan huske kunne være tal-specialtegn-vrøvleord-specialtegn-tal (0;FnytteligFnak;0) eller hvis du kan bruges passwordhuskeren fx ("9#V*7yG?C%'T8P-)
   b. Brug ikke din arbejdsmail til at logge ind på private hjemmesider. Få f.eks. en privatmail fra gmail eller lign.
   c. Følg retningslinjer fra f.eks. CIS Password Policy Guide eller lignende sider
   d. Del aldrig dine adgangskoder med andre
5. Når du bruger sociale medier:
   a. Sørg for at adgang til dine sociale medier – f.eks. LinkedIn – er beskyttet med 2-faktor godkendelse
   b. Post aldrig noget du ikke ville sige i det offentlige rum
   c. Husk er noget først kommet på Internettet kan det være næsten umuligt at fjerne igen
   d. Hvem er du venner med? Er de hvem de giver sig ud for?
   e. Pas meget på spil og links på sociale mediesider
6. Log ind på klienten med en konto som IKKE har lokale admin rettigheder. Du kan søge efter dette på Google og YouTube. Hav en konto som HAR lokale admin rettigheder men brug den kun når det er nødvendigt.
7. Pas EKSTREMT meget på med at hente og installere software fra Internettet. Et godt tip er at du kan se om det er en udgiver du har tillid til ved at højreklikke på den fil du har hentet, vælge properties og Publisher.
8. Hold din klient regelmæssigt opdateret – i Windows er det under settings og Updates & Security. Det gælder også de tredieparts applikationer som du har på din klient
9. Sørg for at have en anti-malware funktion som er regelmæssigt opdateret. Du kan kun være sikker på at den virker hvis du har fjernet lokale admin rettigheder
10. Slå din klient firewall Du kan kun være sikker på at det virker hvis du har fjernet lokale admin rettigheder

11. Pas på med hvor du efterlader dine klienter uden opsyn. Fx i et bagagerum når du er til træning eller på et hotelværelse. Det er ikke nok at lukke låget på din laptop hvis du efterlader den uden opsyn. Så SKAL du logge ud af den.
12. Slå harddisk kryptering til (i Windows skal du lede efter "bitlocker2") og brug gerne et BIOS password.
13. Når du er på farten så pas på hvor du tilslutter dig wifi – generelt er forbindelsen via et SIM kort / telefonen mere sikker
14. Sæt aldrig et USB stick i din computer medmindre du er ejer af det og ved hvad der er på det. Slå funktionen auto-run fra
15. Lån aldrig din klient ud til andre. Du ved ikke hvad deres viden om cybersikkerhed er
16. Læs om cybersikkerhed, bliv klogere, få bedre vaner og beskyt dig selv, din familie og venner:
    a. sikkerdigital.dk
    b. https://www.varonis.com/blog/cybersecurity-statistics/