Otte råd til bedre it-sikkerhed i praksis Thomas Birk Kristiansen har sammen med it-sikkerhedsekspert Jens Heyn Roed Andersen formuleret otte gode råd til praktiserende læger, der vil øge it-sikkerheden i deres praksis.

dagensmedicin.dk/praksislaege-samler-otte-raad-bedre-it-sikkerhed-praksis/

De otte råd er lavpraktiske, handlingsanvisende og kan for de flestes vedkommende udføres af lægen selv uden behov for at involvere teknikere eller systemleverandør.

1. **Administratorrettigheder**
   De fleste har administratorrettigheder til den computer, de bruger. Det betyder, at man kan installere software på den. Det er belejligt, men computere med administratorrettigheder er eftertragtede mål for hackere. Du bør derfor ikke have administratorrettigheder til den konto, du bruger til det daglige log-in. Du bør kun logge på administratorkontoen, når der skal installeres software. Og husk at logge ud igen.
2. **Opdater din computer**
   Uanset hvilket operativsystem, du bruger, bør du opdatere din computer, telefon eller tablet regelmæssigt. Når hackere finder vej ind i din computer, skyldes det ofte fejl i softwaren. Ved en opdatering udbedres disse fejl og sårbarheder, og du bør hyppigt og hurtigst muligt opdatere al software, efterhånden som den udgives. Dette gælder også Apple-produkter, som trods gængs opfattelse også får virus. Du kan indstille din computer til at opdatere automatisk.
3. **Backup**
   Mange begynder først at sikkerhedskopiere, efter at det er gået galt, og de har mistet alle deres data. Selv om sikkerhedskopiering er kedeligt, så spørg dig selv, hvordan du vil have det, hvis du mister alle dine data? Ud over at lave en aftale med en backup-leverandør, typisk via dit systemhus, bør du med jævne mellemrum kopiere data til et eksternt drev og derefter låse det inde. Et netværksdrev alene er desværre ikke nok, da mange såkaldte “ransomware”-angreb også kan kryptere disse drev.
4. **Unikke adgangskoder**
   Mange anvender det samme adgangskode til flere websites, da der i dag er brug for mange logins, og det er nemt at huske et enkelt. Men desværre er det ikke ualmindeligt, at de websteder du besøger og har tillid til, bliver hacket. Så lav forskellige unikke passwords til forskellige websites. Udtænk et simpelt system, så hvert password bliver helt unikt, og tilpasset det website, du besøger. For eksempel kan de første fire bogstaver angive websitet, efterfulgt af det samme komplekse ord hver gang. For eksempel FaceJeg3lskernengodbøf! for Facebook og TwitJeg3lskernengodbøf! for Twitter. Det er langt, komplekst og indeholder tal og specialtegn.
5. **Standard Passwords**
   Hvis klinikken har forskellige enheder, der har forbindelse til internettet, såsom internetroutere, kameraer, køleskabe, spirometre, EKG-apparater med mere bør du sikre, at standardpasswordet, som producenten leverede det med, er ændret. Hackere kender nemlig også disse og retter derfor angreb mod dem, fordi det er nemt.
6. **Brug Antivirus**
   Der er ingen undskyldninger for ikke at bruge et antivirus program, og selvom det ikke giver nogen garantier, så brug det alligevel. Der er endda mange gratis antivirusprodukter derude. Men du får ofte, hvad du betaler for.
7. **Two Factor Authentication (2FA)**
   Generelt ses flere og flere kompromitterede e-mailkonti og konti til sociale medier, da disse kan omsættes til penge. Den risiko mindskes med 2FA, og det er faktisk ganske enkelt og giver en rigtig god sikkerhed. Hvis websitet ser, at du logger på fra en ny enhed, vil sitet sende dig en sms med en engangskode, som du indtaster som en ekstra adgangskode. Det betyder, at for at hacke din konto, skal en hacker udover at kende din adgangskode også have adgang til din telefon. Det er meget besværligt. Snak med din systemleverandør, og sørg for at du anvender NemID, som netop er 2FA, hver morgen, når du logger ind i dit journalsystem.
8. **Vær forsigtig**
   Selv om du føler dig sikker, når du surfer, så husk, at der altid vil være nogen på internettet med onde hensigter, som kan finde lige præcis dig, hvis du er sårbar. Det betaler sig at være fornuftig og forsigtig. Tænk dig om to gange, før du klikker på et link eller åbner en vedhæftet fil til en e-mail – også selvom du kender afsenderen.