Lås din computer, når du forlader rummet > Lad aldrig uvedkommende se dine data

IT-kriminalitet er ikke altid noget, der sker på afstand ved hackerangreb, randsomware eller malware. IT-kriminalitet kan også finde sted i klinikken, mens du er på arbejde. Det kan ske, når du forlader en arbejdscomputer tilgængelig for omgivelserne. I sådanne tilfælde kan IT-kriminelle, der eksempelvis agerer patienter, nemlig nå at installere skadelige programmer, der giver adgang til personfølsomme data.

Familie og venner, der låner en arbejdscomputer eller andre enheder, kan også utilsigtet medvirke til, at en computer eller et netværk bliver angrebet af malware, hvorefter personfølsomme eller virksomhedsrelaterede oplysninger kan havne hos de forkerte eller på nettet. Det kan eksempelvis ske, at en person låner din computer til at hente en fil fra et website, hvor der gemmer sig malware. Malware kan "gemme" sig i alle typer filer - dog typisk i filer som .exe, .zip og MS Office-filer som .doc, .xls og .ppt. Familie eller venner, der låner en arbejdscomputer, kan ligeledes komme til at slette vigtige data ved et uheld, så de mistes helt, eller så du er nødt til at få en IT-rådgiver til at genskabe dine data.

Det er altså vigtigt, at en arbejdscomputer forbliver en arbejdscomputer. Det betyder, at man altid bør låse den, når man forlader den og være meget påpasselig med at lade andre låne den.

Tre gode råd

- Forlader du din arbejdscomputer, tablet eller mobiltelefon i et rum på arbejdet eller derhjemme, skal du altid sætte den i låst tilstand.

- Udlån ikke en arbejdscomputer til familie eller venner. Dette øger risikoen for, at der kommer virus eller hackere ind på virksomhedens netværk, ligesom der ved fejl kan forsvinde vigtige data.

- Udarbejd en vejledning med IT-retningslinjer for klinikkens medarbejdere. Her kan der eksempelvis indgå retningslinjer for, hvordan ansatte skal lukke programmer ned og bruge passwords, samt hvor ofte og hvordan der bør skiftes passwords.