

Sikkerhedsråd til klinikken

Brug sund fornuft, når du modtager mails

Udvis forsigtighed, og tryk aldrig på vedhæftede filer eller links i mistænkelige mails og SMS'er. Det samme gælder for afsendere, du ikke har tillid til. Det kan være svært at gennemskue, om afsenderen er reel eller ej. Hvis afsenderen er en person du kender, kan du få bekræftet mailens validitet, hvis du er i tvivl.

Forhold dig også skeptisk ved uopfordret kontakt via mail eller SMS, hvor der anmodes om koder eller personfølsomme oplysninger. Din bank eller offentlige myndigheder vil aldrig rekvirere sådanne oplysninger over mail eller SMS.

Pas godt på brugernavne og adgangskoder

Få implementeret en sikker politik for udløb- og skift af adgangskode i klinikken, og brug ikke samme adgangskode flere steder.

En god adgangskode indeholder min. 12 tegn og har en kompleks sammensætning af små- og store bogstaver, tal og specialtegn.

Antivirus

Sørg for, at I har antivirus på alle klinikkens pc'er og servere samt at disse er opdateret. For klinikker med Antivirus- eller Sikkerhedsservice (SI) Premium-aftale med EG, varetages drift og vedligehold af løsningen centralt. Disse klinikker er dog selv ansvarlige for at sikre, at EG's Endpoint Protection (F-Secure) er installeret på alle enheder. Dette er tilfældet, hvis ikonet vises nederst til højre på skærmen ved siden af uret. Klinikker uden aftale er selv ansvarlige for antivirus.

Det anbefales også, at Windows Firewall aktiveres på alle pc'er og servere. For klinikker med SI Premium varetages dette centralt af EG. Øvrige klinikker er selv ansvarlige for dette.

Spørg en IT-ansvarlig, før du downloader programmer

Download af programmer fra internettet kan udgøre en stor sikkerhedsrisiko. Derfor må der ikke installeres programmer, som den IT-ansvarlige i klinikken ikke har godkendt.

Firewall

Sørg altid for løbende at opdatere jeres firewall til nyeste firmware. For klinikker med SI Premium-aftale, Firewalls driftsaftale eller routerabonnement gennem EG, sørger EG for at vedligeholde firewallen.

Hav styr på backup og beskyt klinikkens data

Der bør dagligt tages backup af klinikkens data, så driften hurtigst muligt kan genetableres i tilfælde af nedbrud eller cyberangreb.

Er dine programmer opdateret med nyeste version?

Sørg for, at alle anvendte programmer og Windows/MAC operativsystem er opdateret med de nyeste versioner, så der ikke er sikkerhedshuller, som kan udnyttes.

Hvis klinikken har en SI Premium-aftale med EG, sørger EG for at sende opdateringer til operativsystem og understøttede programmer af F-Secure. Øvrige programmer er klinikken selv ansvarlig for at opdatere.