Brug forskellige passwords til forskellige systemer og programmer > Sørg for, at dine passwords er varierede og minimum 12 tegn

Vi har hørt det før. Passwords skal skiftes hyppigt og være forskellige for at undgå IT-kriminalitet - og det er der en grund til. IT-kriminelle bruger nemlig fortsat kendskab til passwords som metode til at få adgang til personfølsomme og kompromitterende data. En uhensigtsmæssig adfærd i forhold til passwords kan altså være en årsag til IT-kriminalitet.

IT-kriminelle får adgang til passwords på flere måder. Nogle gange handler det alene om gætterier omkring passwords, som ofte viser sig at være rigtige. Det sker især, når vi bruger vores navn, ægtefælles navn, fødselsdag og lignende – og når vi bruger det samme password på flere platforme. Havner dine brugernavne og passwords i de forkerte hænder, kan du som privatperson eller arbejdsplads risikere at ende i et længere forløb om at få data tilbage og minimere skader forbundet med dårlig IT-sikkerhed.

En anden adgang er gennem falske hjemmesider oprettet af IT-kriminelle selv. Her kan de eksempelvis opfordre til, at du opretter en profil og skriver dig op til at modtage nyhedsbreve. Herefter afprøver de dine valgte loginoplysninger på dine forskellige profiler, arbejdsrelaterede systemer og VPN-netværk. Ofte får de bid, fordi de fleste af os genbruger vores logins.

Lykkes det dem at matche loginoplysninger med klinikkens systemer, kan de opnå permanent fodfæste i klinikkens interne netværk og til dine private profiler. IT-kriminelle kan få adgang til følgende:

- Dine og klinikkens dokumenter
- Klinikkens systemer og personfølsomme data
- Din mailkonto
- Dine konti på sociale medier og cloudtjenester
- Webshops hvor betalingsoplysninger kan være gemt

Tre gode råd

- Skift passwords hver eller hver tredje måned, hvis du bruger passwords med mere end 12 tegn, og husk at bruge forskellige passwords til dine forskellige medier og netværk. På den måde bliver det sværere for IT-kriminelle at skade dig og din arbejdsplads.

- Brug passwords med ord, der ikke står i en ordbog, og som indeholder otte tegn bestående af både tal, versaler, små bogstaver og specialtegn. Brug ikke passwords med eksempelvis din egen, dine børns eller din ægtefælles fødselsdato eller navnet på din hund.

- Brug om muligt 2-faktor-validering på alle de tjenester og websites, der kræver login. Det betyder, at hver gang du skal logge ind, modtager du eksempelvis en sms med en kode, der fungerer som en ekstra godkendelse af din adgang til websitet.