5 STÆRKE TIPS TIL SIKKER WEBSURFING

Med internettet er det blevet nemmere at holde kontakten med både venner, familie, børn og børnebørn, men der er også mange mulige trusler på internettet, som kan koste dig din opsparing eller dine mest dyrebare minder og feriebilleder. Men med de tips og tricks, du finder i guiden her, krydret med lidt sund fornuft kan du heldigvis gøre meget for, at hackerne ikke får fat i dine personlige oplysninger.

1. Køb sikkert online

Internethandlen buldrer frem, og hvis du også foretrækker at købe fødselsdags- og julegaverne til børnene og børnebørnene på nettet, bør du tage nogle forholdsregler, inden du finder dankortet frem. Allerførst kan du installere en særlig browser som f.eks. en Safepay-browser, som du bruger, hver gang du handler online. Safepay-browseren krypterer alle dine informationer, så f.eks. hackere ikke får adgang til dine betalingskort og personlige informationer. Se mere om Safepay-browser på **chilisecurity.dk**

Andre gode råd er:

- Du bør kun shoppe på sikre sider – Er der en hængelås og "https" foran hjemmesideadressen, 

så er det en sikker side at shoppe på.
- Har webshoppen e-mærke? Så lever den op til den gældende danske lov og kontrolleres løbende af e-mærkets jurister.
- Pas på med kopisider. Mange svindlere er blevet gode til at kopiere populære webshops, så hold derfor øje med hjemmesideadressen, og om der er mange stavefejl på siden.
- Vær kritisk i forbindelse med voldsomt gode tilbud – er det realistisk, at de dyre Nike sko kan sælges så billigt?
- Søg på nettet efter webshoppens navn – hvad står der om shoppen f.eks. på diverse anmeldelsessider?
- Læs salgs- og leveringsbetingelser – så er du sikker på, hvad du siger ja til, inden du køber.
- Brug altid betalingskort eller MobilePay – så kan banken hjælpe med at tilbageføre pengene, hvis du ikke modtager varerne, du har betalt for.

2. Vær kreativ med kodeordet

Vidste du, at et af de mest benyttede kodeord i 2018 er 123456?
Det gør du nu, og hvis du har samme kodeord, så er der god grund til at få det skiftet ud med det samme.

Når du skal lave et kodeord, er det ikke nok at vælge din fødselsdato og navnet på dit kæledyr – det er informationer som hackere hurtigt kan gætte eller finde frem til. I stedet for bør du blande bogstaver, tal og specialtegn med hinanden. Du kan eksempelvis bruge 3 i stedet for e eller 4 i stedet for a. Og for at få et stærkt kodeord kan du bruge specialtegn som eksempelvis udråbs- og spørgsmålstegn. For at gøre det lettere at huske din kode, kan du bruge en sætning, ret rim, titlen på din yndlingsbog eller en linje fra en sang. Det kunne f.eks. være "En snegl på vejen er tegn på regn i Spanien" 1@pvrTp"iS

Derudover er det en god ide, at du udskifter kodeordene nogle gange om året, og at du ikke bruger autologins på din mail eller Facebook. Derved undgår du, at du glemmer kodeordet og at hackerne får adgang til alle dine vigtige dokumenter, hvis du får stjålet din computer.

5 tips til det gode kodeord

1. Det skal være nemt at huske, så du ikke behøver skrive det ned.
2. Det skal være langt og gerne mindst 8 tegn.
3. Brug både tal, store og små bogstaver og specialtegn.
4. Brug ikke det samme kodeord til mail og sociale medier.
5. Skift kodeordet ofte.

3. Gem minderne på en sikker online harddisk

Det er en god ide, at du har en god backup af din harddisk i tilfælde af et hackerangreb. På den måde undgår du at miste billeder og videoer fra alle familiefesterne og ferierne. Du kan gemme en sikkerhedskopi på en ekstern harddisk, men er den koblet til din computer, risikerer du også, at den bliver hacket eller inficeret af virus.

Som yderligere sikkerhed kan du benytte dig af en online harddisk. Det er en harddisk, som du kan tilgå fra din computer eller smartphone, men som ikke er direkte forbundet med dit netværk. I stedet er online harddisken sikkert opbevaret på et datacenter, og den vil derfor ikke vil blive inficeret, hvis din computer får virus.

4. Vær kritisk, når du downloader apps

Det er ikke kun din computer, som er sårbar overfor hackerangreb. Smartphones er blevet et slaraffenland for hackere. Derfor bør du være ekstra vaks, når du downloader nye apps til din telefon.

Det er ikke unormalt, at apps beder om tilladelse til at læse dine mails og SMS'er, eller vil have adgang til kameraet og mikrofonen. Det er dog oftest sikre apps fra Google, Facebook og lignende, som sender disse forespørgsler. Det sker dog, at lyssky apps får tilegnet sig samme adgang, hvis du ikke får læst det med småt. Kast derfor altid et kritisk blik på apps, og sig nej til forespørgsler, som du ikke er helt tryg ved.

Derfor:
- Læs brugeranmeldelser af appen, inden du downloader den. Har den fået dårlige anmeldelser?
- Lav en hurtig søgning på Google og se, hvad der står skrevet om appen.
- Afvis anmodninger om adgang til beskeder og mikrofon, hvis du ikke har tillid til app'en.

5. Er du kommet galt afsted

Hvis uheldet er ude, og du er blevet hacket, er det vigtigt, at du handler hurtigt. På den måde undgår du, at hackerne får tømt din bankkonto eller stjæler dine personlige oplysninger.

Gør derfor følgende:
- Kontakt banken og få spærret alle dine kreditkort.
- Ring til NemID's kundesupport og få deaktiveret dit nøglekort.
- Ændr adgangskoderne til din e-mail, sociale medier og din router.
- Scan din computer for virus.

For at forhindre at det sker (igen), kan du også undersøge, om der er en sikkerhedspakke med til dit internet og hvordan du får den aktiveret. En sikkerhedspakke vil typisk indeholde bl.a. antivirus, firewall og mange andre funktioner, der beskytter dig og dine kære mod hackerne.

Se mere om sikkert internet hos Eniig på eniig.dk/fiber