

SÅDAN SIKRER DU DIG SELV DIGITALT

Der kan ligge mange ubehagelige oplevelser på lur, hvis ikke man passer på sig selv online.

Sikkerhed på nettet kan være en svær størrelse.

Her får du politiets bedste råd:

FEM GODE RÅD TIL SIKKER FÆRDSEL PÅ NETTET

1. Udlever aldrig data

Pas godt på dine personlige oplysninger, så du ikke kan blive identificeret af folk, du ikke kender.

2. Del ikke noget privat

Tænk over, hvad du deler på nettet. Det kan være strafbart at dele visse materialer, herunder billeder.

3. Vær skeptisk

Hav en sund skepsis over for de ting, du oplever på nettet. Ikke alting er, som det ser ud til, og hvis noget virker for godt til at være sandt, så er det formentlig snyd.

SÅDAN SIKRER DU DIG SELV DIGITALT

4. Tænk selv

Tag afstand fra delekulturer, hvor andre gøres til grin eller krænkes. Det bliver

ikke mere rigtigt eller lovligt af, at andre også gør det.

5. Gå til politiet

Oplever du noget ubehageligt, så søg hjælp eller anmeld det til politiet.

Her er seks gode råd til at sikre, at dine data ikke er tilgængelige for gud og hvermand:

1. Brug falsk identitet

Det kan godt være, at indstiller din facebookprofil til at være privat. Men det ved dine venner ikke, og før du ved af det, kan dine opdateringer og private billeder være spredt over nettet under dit navn. Det gør det nemt for både arbejdsgivere og andre at finde frem til intime informationer om dig.

På samme måde kan man benytte sig af forskellige alias, når man logger på nye apps og oprette forskellige emails, der kan bruges til det private og det offentlige.

Det forhindrer også identitetstyveri.- De færreste ved det, men selv uskyldige spilapps kan registrere store mængder personlig data, og én af måderne de gør det, er, at man selv skriver sit fulde navn, når man logger ind første gang. Prøv f.eks. FakeNameGenerator.com og benyt andre mailtjenester som Guerillamail.com eller Spambox.us.

SÅDAN SIKRER DU DIG SELV DIGITALT

2. Skift browser

Hver gang du går online på f.eks. Facebook eller Google, så registreres det. Når du så søger videre på en historie på dr.dk eller køber et par sko online eller går på netbank, bliver det også registeret.

På den måde opsamles der data om dig ved hver eneste klik du foretager. Men der er en måde at snyde systemet på.-

Et godt trick er at benytte én browser til sin Facebook, en anden til sin netbank og en tredje til alt muligt andet.

Dermed sørger man for, at man ikke behøver rense ud i sine cookies hele tiden, og skal skrive sit kodeord ind i Facebook og på netbanken hele tiden.

3. Vælg andre søgemaskiner

Google er et herligt værktøj, når du skal finde noget som helst på nettet. Men Google er også en af de værste syndere, når det kommer til at tracke og gemme dine søgninger - og ifølge whistlebloweren Edward Snowden ryger disse data blandt andet direkte videre til de amerikanske efterretningstjenester.

Derfor kan det være en god idé at vælge en anden søgemaskine, når du søger på nettet. - Der findes et par gode søgemaskiner, der ikke registrerer dine søgninger. Prøv f.eks. duckduckgo.com.

4. Bloker dine data

Hvis du er nervøs for at Google, Facebook eller Twitter stadig kan opsnuse alle dine data på nettet, er der endnu en måde at sørge for at holde dem ude.- Du kan benytte et såkaldt blokeringsværktøj, der gør, at de 'tre store' ikke kan følge dig rundt på nettet. Den bedste hedder disconnect.me og er faktisk udviklet af en tidligere Google-ansat, der plejede at bruge alle sine kræfter på at tracke andre på nettet.

SÅDAN SIKRER DU DIG SELV DIGITALT

5. Skjul din IP-adresse

Hvis du vil skjule dig selv ordentligt, er det dog ikke nok bare at blokere for dine bevægelser på bestemte sites. Du må også sørge for at skifte IP-adresse engang imellem.- IP-adressen er computerens kendenavn. Den afslører hvilket land du sidder i og stort set alt om dig. Men den kan du forholdsvis nemt få et program til at sløre, så det ser ud som om du måske sidder i Frankrig eller Hong Kong i stedet. Prøv f.eks. torproject.org eller best-vpn-provider.com.

6. Krypter dine e-mails

Hvis du virkelig har noget at skjule, er der en løsning mere. Du kan køre dine emails igennem et krypteringsprogram der gør, at de bliver ulæselige af alle andre end den person, de er sendt til.- Alle store firmaer, der gør forretninger i Kina, bruger kryptering af alle deres emails, fordi de er bange for industrispionage. I dag er processen noget besværlig, men det vil formentlig ændre sig indenfor få måneder.- For et år siden var det også svært at skifte IP-adresse, men det er rigtig nemt i dag. Og kryptering vil helt sikkert blive mere brugt i fremtiden. Her kan du læse mere om, hvordan du krypterer dine emails på instructables.com eller selv prøve på comodo.com.

SÅDAN SIKRER DU DIG SELV DIGITALT

Nethandel er nemt, men du skal være på vagt

Netbutikker er nemme at bruge, når du vil shoppe hjemme fra sofaen, men det kan være svært at gennemskue, om en netbutik er sikker og pålidelig.

Køber du varer over internettet, er du faktisk godt stillet i henhold til loven. Du er nemlig bedre stillet i forhold til fortrydelsesret og muligheder for tilbagebetaling, når du handler online inden for EU, end når du handler i fysiske butikker.

Tjek webshoppen

Webshoppen skal du altid undersøge grundigt, inden du trykker køb:

- **Hvilke kontaktoplysninger har webshoppen?** Der skal både stå virksomhedens navn, en e-mail-adresse, et telefonnummer og virksomhedens fysiske postadresse.
- **Er det en dansk hjemmeside?** At virksomhedens webadresse ender på .dk er ikke en garanti for, at virksomheden ligger i Danmark. Ender webadressen på .dk, har du mulighed for at slå den op på hostmaster.dk for at finde ud af, hvor virksomheden er registreret. Ender webadressen på noget andet end .dk, kan du bruge whois.com, hvor du kan slå andre hjemmesider op.
- **Er der CVR-nummer?** Danske virksomheder har et 8-cifret CVR-nummer, når de er registreret i det Centrale Virksomhedsregister. Det er virksomhedens identifikationsnummer, som skal stå på hjemmesiden.
- **Er siden e-mærket?** E-mærket er en dansk mærkningsordning, der skal sikre forbrugerne en sikker e-handel. Virksomheder med e-mærket har forpligtet sig til at overholde gældende lovgivning og følger e-mærkets retningslinjer for blandt andet betalingsformer. E-mærket kontrollerer løbende de e-mærkede butikker.
- **Ser teksten fornuftig ud?** Hvis teksten ligner noget, der er oversat med Google Translate og er fyldt med stavefejl, kan det være tegn på, at siden ikke er sikker.
- **Er priserne realistiske?** Hvis varerne har "skæve priser" som 492,43 kroner, kan det være tegn på, at siden er oversat af en maskine. Hvis varerne er betragteligt billigere end andre steder, kan det være et tegn på, at varerne er kopivarer.

SÅDAN SIKRER DU DIG SELV DIGITALT

- **Tjek virksomheden på forbrugeranmeldessider.** Hvordan er anmeldelserne af siden? Og hvad har andre forbrugere gjort sig af erfaring med siden? Forbrugeranmeldessider, som for eksempel Trustpilot, skal tages med et gran salt, men de kan give dig en fin idé om, hvilke erfaringer andre forbrugere har gjort sig.
- **Hvor bliver varen sendt fra?** Told, skat og andre afgifter kan du risikere at skulle betale, hvis din vare ikke sendes fra et EU-land. Selv om teksten på hjemmesiden er dansk, er det ikke sikkert, at din pakke bliver afsendt fra Danmark. Derfor er det vigtigt at tjekke, hvor varerne sendes fra.

Læs betingelserne for køb

Webshoppens betingelser skal du altid læse grundigt igennem, inden du trykker køb. Du er forholdsvis godt beskyttet, når du handler online indenfor EU. Du har for eksempel 14 dages fortrydelsesret ved køb af langt de fleste varer inden for EU.

- Køber du en vare, der undtagelsesvis ikke er omfattet af fortrydelsesretten, skal netbutikken skrive det tydeligt på hjemmesiden.
- Returret, fortrydelsesret og hvem, der betaler for tilbagesendelse af varer, skal fremgå af butikkens betingelser.
- Dele af dit køb kan du kun fortryde, hvis det står i betingelserne. I så fald skal du have tilbagebetalt beløbet for den del af købet, du fortryder.
- Billige eller gratis prøvepakker på en vare kan være en fælde. Læs betingelserne grundigt, så du undgår at starte et abonnement, som du løbende betaler for.

Betal sikkert

Betalingskort, kontooverførsler eller Mobile Pay? Der findes mange forskellige måder at betale på, når du handler på nettet.

Shopper du online, så følg altid disse råd:

- **Brug altid betalingskort eller Mobile Pay.** Hvis du aldrig får din vare, eller hvis webshoppen har trukket et højere beløb end aftalt, kan banken føre dine penge tilbage for dig.
- **Betal ikke via kontooverførsel eller per efterkrav** – banken kan ikke hjælpe dig, hvis du bliver snydt!
- **Kontrollér om forbindelsen er sikker, når du betaler.** Din internetforbindelse skal være krypteret, når du overfører fortrolige oplysninger som for eksempel dit kortnummer. Forbindelsen er sikker, når der er en lille hængelås foran adressen på hjemmesiden.

SÅDAN SIKRER DU DIG SELV DIGITALT

- **Oplys aldrig dit kortnummer**, med mindre du er ved kassen og er i gang med at betale for en vare - heller ikke per mail eller telefon til en, der skal hjælpe dig!
- **Gem dokumentationen**. Tag et screenshot eller et billede af bekræftelsessiden og gem det, eller gem ordrebekræftelsen, som butikken sender til din mail.

Efter købet

Beløbet, der bliver trukket fra din konto, skal svare til det aftalte. Klag til den erhvervsdrivende, hvis der bliver trukket beløb fra din konto, som du ikke har godkendt. Klag på skrift til webshoppen, så du altid har dokumentation for din klage.

Banken skal du kontakte, hvis den erhvervsdrivende ikke accepterer din klage. Banken kan føre pengene tilbage til dig, hvis du har betalt med betalingskort eller Mobile Pay.

Er det alligevel gået galt?

Accepterer netbutikken ikke din klage, kan du for danske virksomheder klage videre til den offentlige forbrugerportal forbrug.dk. For varer købt i en EU-shop og uden for EU, er der andre klageløsninger for.

Dukker din vare aldrig op, skal du kræve pengene tilbage.

Oplever du svindel på nettet, skal du hurtigt melde netbutikken til politiet.