Digitalt Selvforsvar: Tips & Tricks

Husk at få en fysisk nøgleviser til mitID

Hvis du mister din smartphone, eller den går i stykker – og du ikke har mitID-appen installeret på en tablet – har du store problemer. Du kan ikke tilgå det offentlige, din netbank, forsikringsselskab, forsyningsselskab osv.

Derfor: Gå til **mitid.dk** og bestil en nøgleviser. Den er gratis – og kommer til din folkeregisteradresse inden for nogle få dage.

Email-håndtering

Det kan være et problem, at din mailboks bliver et stort rod-sammen af vigtige mails og diverse nyhedsbreve, der alle bliver sendt til din mailadresse

Hvis du bruger mailprogrammer som Gmail eller Outlook, kan du imidlertid tilføje et + til din mailadresse, når du skriver dig om til et nyhedsbrev eller bruger den til tilmelding til en ny tjeneste etc. Fx kimelmose+onlineshop@gmail.com .

Mailen kommer til dig, men du kan nemt sætte mailprogrammet til at sortere alle mails til kimelmose+onlineshop@gmail.com og placere den i en mappe, så den ikke ligger og forstyrrer overblikket i indbakken.

Det betyder dog stadigvæk, at de gratis tjenester – Gmail og Outlook – registrerer, hvad mails til dig handler om, emner, længde, hvorfra m.m. Så de får et meget præcist billede af, hvad du interesserer dig for – og kan bruge det i annoncer andetsteds på nettet.

Er du træt af det, kan du prøve andre mailtjenester som et supplement – fx til mere private og fortrolige mails. Det kunne være en af følgende – alle tre nemme at bruge, også på smartphones:

- Protonmail.com
- Tutanota.com
- Startmail.com

De er gratis i en basis-udgave, men ved at betale et lille beløb per måned får du mere lagerplads og flere funktioner. Absolut anbefalelsesværdigt – og billigere end én fadøl på værtshus per måned.

Søgning

Det er en hverdags beskæftigelse at søge informationer på nettet – og det er samtidig dér, at techgiganterne og annoncørerne henter en del viden om os, og hvad vi går op i. De registrerer, hvad vi søger på – og sørger også for, at vi næste gang får søgeresultater, som passer til vores interesser. Det gælder Googles søgemaskine og Microsofts Bing.

Heldigvis er der en del søgemaskiner, som blokerer for alle hjemmesidernes forsøg på at spore os videre rundt på nettet (via små programstumper placeret i browseren) og som lader os søge anonymt efter information.
Følgende er brugervenlige og leverer gode søgeresultater:

- Duckduckgo.com
- Startpage.com
- Search.brave.com
- Qwant.com

Disse fire søgemaskiner fungerer også godt til smartphone.

Browsere

Browserne er vores vindue ud til World Wide Web – og de mest brugte er Chrome (63 %), Safari (20 %) og Edge (5 %). Her er det værd at huske, at Chrome og Edge registrerer, hvilke sider vi besøger, og hvad de handler om – og browseren blokerer generelt ikke for megen sporing. Især Google lever af at levere data om kunderne til annoncefirmaer.

Opfordringen er derfor at sprede sin tilgang til nettet over flere forskellige browsere – og jævnligt bruge browsere, som ikke sporer og registrerer brugernes færden.

Igen er der mange browsere på markedet. Eksperter er enige om, at de følgende browsere er respekterer brugerens privatliv:

- Brave: Brave.com
- Firefox: Mozilla.com/firefox
- Opera: Opera.com

Disse tre browsere fungerer også godt til smartphone.

Adgangskoder - hold styr på dem

Vi er tilknyttet masser af tjenester med brugernavne og adgangskoder – og det er et problem for de fleste at holde styr på, hvilke adgangskoder der bliver brugt hvor.

Af magelighed risikerer vi at bruge den samme adgangskode flere steder – eller blot med en lille ændring i koden per tjeneste.

Det gør det *for* nemt for it-kriminelle at få hacke sig ind på vores konti.

Derfor er det en god idé at benytte en tjeneste til at holde styr på adgangskoderne. De bliver kaldt **password managers** – og er opbygget ved, at dine brugernavne og adgangskoder bliver gemt bag i en hårdt krypteret digital bankboks, som der skal enorme computerkræfter over år til at bryde ind i.

Du skal så huske én hovedadgangskode – det kan være en længere sætning ”jEggårOfteover23åenefterVand”, som låser op for de andre adgangskoder.

Afhængigt af password manager så der ofte flere funktioner, der fx holder øje med, om du bruger samme adgangskode flere sted – og siger til, om der er registreret sikkerhedslækager hos nogle af de steder, hvor du har en konto.

Følgende tjenester har et godt ry for sikkerhed og brugervenlighed:

- 1password.com
- Bitward.com
- Zohovault.com
- Dashlane.com

De fleste password managers koster et mindre beløb per måned at bruge – fx hvis du skal have adgang via mobilen.

Overvågning af sikkerhedsbrud

Sidder du og tænker: ”Gad vide om mit brugernavn – fx mailadresse – optræder i et datalæk?”

Det kan du se, hvis du går ind på hjemmesiden: **Haveibeenpwned.com**.

De sikkerhedseksperter, der driver sitet, har samlet webadresser, brugernavn, navne, adresser m.m fra kendte datalæk og hackersites (hackere elsker at prale eller sælger data). Data er lagt ind i en database, hvor man så kan søge på sit brugernavn – ofte mailadresse – og se, om der har været et datalæk.

Er der det, kan man ændre sit password.

To-faktor login er bedst

Vi kender alle såkaldt to-faktor fra først nemID og nu mitID: du logger på en tjeneste med brugernavn og adgangskode – og så skal du et tredje sted (et papkort eller via en godkender-app) finde en talkode, som du taster ind, før du bliver lukket ind.

Det er mere bøvlet, men bliver din mail, erhvervskonto til hjemmesiden eller sociale medier som Facebook hacket, er det meget træls.

Derfor slå to-faktor til på dine vigtigste konti, hvis muligheden eksisterer.

August 2023 *kimelmose@pm.me*