# Beskyt din netbank og offentlige hjemmesider, hvor du bruger Nem-ID koder

## Hackere kan snige sig uden om nemID

Netbanks kunder følte sig sikre, fordi NemID-koder er lavet, så de kun kan bruges en enkel gang. Men angreb har bevist, at hackere kan snige sig uden om nemID ved at bruge real-tids-malware og angribe, mens offeret selv er på sin netbank.

Den type af malware hedder ***phishing***. Det betyder i almindelig tale, at hackere installerer et skadeligt software (malware) på folks computere og via det følger brugerens aktiviteter og opsnapper (fisker) offerets adgangskoder. På den måde hopper de med på vognen og lige med ind på offerets bankkonti uden kontoindehaverens viden.

## Sådan kommer de ind

Hackernes vej til for eksempel din computer er gennem links, der fører til hjemmesider, der er lavet af kriminelle med det ene formål at undersøge computere for usikre indgange og såbarheder. Når de har fundet sikkerhedshullerne, bliver malwaren installeret - og så kan de gå igang med at finde alle de interessante oplysninger, som de kan misbruge. *Kriminelle kan også lokke dig til at give dem adgang via emails med en inficeret fil, som du kan blive fristet til at klikke på*. Mange kriminelle bruger også sårbarheder i computerens styresystem til at inficere computere.

Bare to timer efter installingeren af det skadelige software kan de have første offer på krogen, så det kan gå rigtig stærkt.

## Tag malware alvorligt

Malware er en sammentrækning af ordet 'malicious software', altså skadeligt software. Malware og virus rammer både Mac- og Windowsbrugere. Macs styresystem har før været bedre til at stå imod, men Mac rapporterer efterhånden om flere og flere supportopkald fra folk, der har fået malware-inficering på deres apple-produkter.

Malware findes alle steder på nettet, lige fra pornosider til falske shoppingsider, der er udviklet med det ene formål at inficere med malware, uden at brugerne aner uråd. *men hackerne går sjældent efter sikkerhedsopdaterede computere*; de går efter dem med sikkerhedshuller. Ligesom det ville være tåbeligt for en tyv at bruge tid på at finde et hus at bryde ind i, hvis nøglen alligevel hænger med en adresse vedhæftet på en opslagstavle hos den lokale brugs. Så let er det nemlig at få adgang til en computer, der ikke er sikret mod angreb.

## Fem måder at (forsøge at) undgå hacking af NemID på

Man kan undre sig over, hvordan det skadelige software er kommet ind på computeren til at starte med. Det er oftest fordi, offeret ikke har haft anti-malware installeret på sin pc. I

de nyligt omtalte NemID-sager havde de hackede bankkunder heller ikke anti-malware med realitdsbeskyttelse installeret. Realtidsbeskyttelse er en udvidet version af almindelige anti-malware programmer. Den er særligt vigtig, fordi den fanger hackerforsøget i samme øjeblik, det sker, og giver øjeblikkelig advarsel om dette. Den blokerer samtidg for angrebet og giver karantæne til den malware, der er igang med at tvinge sig adgang.

- ***Hav altid en Firewall installeret***. Sørg for, at den som alt andet sikkerheds-software er opdateret regelmæssigt. Den kan sættes til at opdatere automatisk, hvilket er anbefalelsesværdigt. En Firewall sørger for at blokere kriminielle, der prøver at få adgang til din computer - men det er langt fra nok at have blot en Firewall.

- ***Anti-virus arbejder effektivt sammen med anti-malware***. Den giver dig besked om virusinficering og mulighed for at fjerne og blokere den. Anti-malware og anti-virus er ikke det samme. Anti-virus fjerner som oftest ikke malware, men derfor er det vigtigt at have begge dele alligevel.

- ***Det kan på det kraftigste tilrådes at du laver sikre koder***. Det vil sige, at dine kodeord skal være så unikke, at de ikke sådan lige er til at cracke. Lad være at bruge dit kæledyrs navn eller dit eget efterfulgt af det årstal, du er født. Det er for nemt for de ubudne gæster at afsløre. Netop fordi det er den vigtigste oplysning til dine mest personlige informationer, bør du heller aldrig give det til nogen. Husk at din valgte kode til Nem-ID er fælles for alle offentlige netsider og din netbank.

- ***Pauseskærme, eksterne værktøjslinier, spil og andre underholdende indslag og programmer på nettet kan slæbe meget malware med sig, så pas på hvad du downloader***. Der kan ligge skjulte koder, som kan bruges til at skaffe kriminielle adgang til personfølsomme oplysninger. *Tjek dine programmer og se, hvad du egentlig har brug for og afinstaller resten.* Det kan måske have den sidegevinst, at det øger din computers hastighed.

***Husk sygdomme kan undgås ved god forebyggelse***