SIKKERHETSSKOLEN

Enkle tips og råd om hvordan du ferdes litt tryggere på internett

FORORD

Nettet er utrygt for dem som ikke kan beskytte seg.

Jeg er ingen sikkerhetsrådgiver. Og målet med denne siden er heller ikke å lære bort avanserte sikkerhetsteknikker – ikke av den typen som behøves av banker og militærinstallasjoner.

Målet er å hjelpe vanlige mennesker – særlig privatpersoner og småbedrifter – å ta noen enkle grep for å bli tryggere på internett.

På samme måte som airbag, sikkerhetsbelte og god forståelse av trafikkreglene gjør deg *mer* trygg, men ikke *helt* trygg, når du kjører bil, slik vil rådene i denne boken gjøre deg *mer* trygg, men ikke *helt* trygg, på nett.

Usikkerheten på nett

Så hvorfor opprette Sikkerhetsskolen siden hvis jeg ikke har noen formell kompetanse?

I årene frem mot 2017 skjedde det mye i nyhetsbildet som gjorde at jeg ble interessert i å lære hvordan jeg kunne forbedre sikkerheten på min egen digitale tilstedeværelse.

For å ta noen eksempler:

- I to store hackerangrep i 2012 og 2014 mistet Yahoo kontrollen over henholdvis 1 milliard og 500 millioner brukerkonti, inkludert passord og sikkerhetsspørsmål. (Er du blant dem, mon tro?)
- I 2014 ble Sony hacket av nord-koreanske agenter i forbindelse med filmen The Interview, og forsøkt presset til ikke å distribuere den.

- De mest kjente hendelsene i 2015 var Ashley Madison-angrepet, som

- outet 37 milioner(!) mennesker i markedet for utenomekteskapelige forhold, og Mossack Fonseca-lakkasjen (Panama-papirene, som ikke var et angrep, men likevel et stort sikkerhetsbrudd).
- I 2016 og 2017 ble viktige valg i USA og Europa hacket av russiske agenter, og det er i skrivende stund fortsatt usikkert hvilken effekt det hadde på utfallet.

» Se flere eksempler på store angrep på InformationIsBeautiful.net

I 2017 fikk dessuten internettleverandører i USA dramatisk utvidede rettigheter til å lagre og selge informasjon om sine kunder. Det er ikke et hacker-angrep, men ideen om at salg av kundenes nettvaner skal bli normen blant internettleverandører gir grunn til å være bekymret.

Vi gjør internett utrygt

Det man ofte *ikke* hører så mye om, er hvordan de store angrepene gjennomføres.

Mange av oss ser nok for seg progammerere som hamrer i vei på tastaturet og lysende grønne tegn som fyker forbi på skjermen i Matrix-stil, i en actionfylt jakt etter sikkerhetshull de kan utnytte for å få tilgang. Og slike sikkerhetshull er ekte.

Det vi ikke vet, er at det veldig ofte er vanlige mennesker som deg og meg som *er* sikkerhetshullene, og som har skylden for at disse angrepene lykkes.

Kanskje har vi ikke oppdatert programvaren på maskinen vår til siste versjon, så bakdøren står på vidt gap selv om det for lengst er blitt mulig å lukke den.

Kanskje bruker vi samme passord for å logge oss på serveren på jobben som vi brukte på Yahoo i 2014 – og som for lengst er kommet på avveie.

Kanskje får vi en tilsynelatende seriøs mail som ber oss bytte passord på Google, og vi lar oss lure til å gi brukernavn og passord til uvedkommende.

Eller kanskje vi kobler oss på gratis wifi i business loungen på en flyplass,

uten å vite at det nettverket ikke er satt opp av noen på flyplassen, men av hackere som fisker etter brukernavn og passord.

Sikkerhetsskolen blir født

Det er utrolig mange feller for oss å gå i, og jeg bestemte meg for å bruke litt tid på å lære hvordan jeg kunne unngå de mest åpenbare.

Men da jeg begynte å gjøre research ble jeg overrasket og skuffet over hvor

vanskelig det var å finne en god og rimelig komplett oversikt over enkle grep som privatpersoner og små bedrifter kan ta for å sikre seg.

Det var mange, lange artikler om enkelttemaer, men det var unødvendig vanskelig å finne ut av hva som skulle til for å ha en noenlunde komplett sikkerhetsstrategi uten gapende hull.

Derfor gjorde jeg mye research, og jeg bestemte meg for å samle de beste rådene jeg fant på ett sted.

Sikkerhetsskolen er resultatet.

For at sikkerhetsskolen skal være mest mulig enkel å bruke, finnes det viktigste innholdet på denne nettsiden, men også snart som en e-postsekvens du kan abonnere på eller som en ebok du kan laste ned.

Surf trygt!

Med vennlig hilsen

Christian K. Nordtømme

SJEKKLISTE

Blir det for mye å lese, kan du bruke dette som jukselapp.

- [ ] **Bruk en passordbehandler**
  Last ned Dashlane her
- [ ] **Lag gode, unike passord du vil huske**
- [ ] **Lær å bruke 2-faktorautentisering**
  Last ned Authy her og følg anvisningene her for å aktivere 2FA
- [ ] **Bruk *HTTPS Everywhere***
  Installere HTTPS Everywhere her
- [ ] **Bruk en god VPN**
  Last ned VyprVPN her
- [ ] **Bruk Anti-Virus & Anti-Malware**
  Last ned Sophos Home her og Malwarebytes her
- [ ] **Hold deg oppdatert**

DEL 1: HVORFOR BESKYTTE SEG?

HVEM VIL VEL HACKE MEG OG MITT?

Du er mer utsatt enn du tror.

Hvorfor skulle noen gidde å hacke meg?

Alle som er på internett har noe som kan være av interesse for en hacker. I beste fall bruker de deg bare som uvitende fotsoldat i et angrep mot mer lukrative mål, men du har nesten garantert også andre ting hackere kan være interessert i.

Det er viktig å forstå at det ikke koster hackerne nevneverdig anstrengelse å angripe deg. De angrepene vi snakker om her, er stort sett 100% automatisert.

Men hvordan skal de finne frem til lille meg blant alle som er på Internett?

Hackerne har roboter som tråler internett etter lavthengende frukt og enkle ofre. Robotene jobber utrolig raskt og har enorm kapasitet til å samle, lagre og indeksere informasjon.

Noen deler av denne prosessen krever store data-ressurser, men akkurat *det* er ganske lett tilgjengelig for hackere.

Er ikke hackerne stort sett bare vandaler og pøbler?

Det er mye penger i hacking, og derfor også mange proffe hackere som har mye å tjene på å hacke deg.

Svindlere, spammere, spioner (både bedriftsspionasje og politisk spionasje)

og selv selgere. De har ikke noe imot deg, personlig, men robotene jobber seg systematisk gjennom befolkningen, og finner deg før eller senere.

Hvem er potensielle ofre for hacking?

- Alle som har tillit, makt eller penger er åpenbare mål. Men de som har mest tillit, makt og penger har også ofte de beste sikkerhetsrutinene, så det er ofte lettere å ta dem som ikke ser seg selv som noe typisk mål.
- Alle som har ambisjoner om å få tillit, makt, eller penger. Særlig spioner vil operere med lang tidshorisont, og vil hacke hundrevis av ambisiøse mellomledere eller lovende ungdomspolitikere i dag, for å samle informasjon som kan brukes mot et knippe av dem om ti år.
- Alle som kjenner en som har tillit, makt eller penger. Din kontakt med et mer lukrativt mål/offer kan i seg selv være en brikke i et større puslespill, eller identiteten din kan stjeles og misbrukes.
- Alle som jobber for eller med et selskap som har tillit, makt eller penger. Tilgangene og tilliten du har som betrodd medarbeider og kollega kan misbrukes.
- Alle som har noe en annen ønsker seg eller kan bruke – inkludert bare en identitet og/eller statsborgerskap i et vestlig demokratisk land. Det at du er en uskyldig og forholdsvis ukjent person med en Skype-konto, en e-postadresse og kanskje en blogg, gjør deg til en perfekt brikke i et større spill. Hackere bruker roboter til å sette sammen tusenvis av uvitende ofre til en digital hær de senere kan bruke i et større angrep – et såkalt botnet, et nettverk av kaprede maskiner.

Hva har de å vinne på å hacke meg?

- Samle informasjon om deg, som kan brukes til å stjele fra deg, svindle deg, spamme deg, presse deg – nå eller senere.
- Samle informasjon om dem du kjenner og jobber med, som kan brukes til å stjele fra dem, svindle dem, spamme dem, presse dem – nå eller senere.
- Bruke din identitet til å svindle dem som stoler på deg, spamme dem som kjenner deg, eller hacke/angripe fremmede.
- Skjule seg bak deg for å få tilgang til systemer og konfidensiell

- informasjon i ditt navn

- Få tilgang til tilsynelatende ufarlig informasjon som senere kan brukes til å gjøre løgner mer troverdige – for eksempel ved å blande inn falske e-poster i en Wikileaks-dump med ekte e-poster. (Høres det kjent ut?)

Det finnes utallige grunner til å hacke deg som du ikke ser selv. Det er dessuten sannsynligvis mye lettere enn du er klar over. Det er ikke engang utenkelig at innloggingsinformasjonen din allerede er på avveie, og at den eneste grunnen til at informasjonen ikke er misbrukt (gitt at den ikke allerede er det), er at skurkene ikke har kommet til deg ennå, eller funnet ut hvordan de skal bruke deg.

ER DU PWNED?

Første oppgave: Gå til HaveIBeenPwned.com for å finne ut om du noen gang er blitt «pwned». Det vil vil være en vekker for mange.

«Pwned», med P, er internett-slang for «eid» i betydningen «utmanøvrert» eller «utkonkurrert». I denne sammenhengen betyr det at dine opplysninger blitt kompromittert.

Nettsiden HaveIBeenPwned.com har samlet informasjon fra mange av de største, kjente hacker-angrepene, som dem på LinkedIn, Dropbox og Adobe – nesten fire milliarder(!) brukerkontoer på avveie.

Når du søker på din e-postadresse, finner du ut om din informasjon er kommet på vidvanke i ett av de angrepene.

Det er viktig at du forstår at faren ikke nødvendigvis er at noen skal få tilgang til din gamle MySpace-profil. Det større problemet er om du har brukt samme kombinasjon av brukernavn og passord på en annen nettside eller app. I så fall kan du regne med noen har fått tilgang dit, også.

Gitt en liste med brukernavn eller e-postadresser med tilhørende passord, vil nemlilg hackere bruke roboter til å prøve alle disse kombinasjonene på andre nettsteder, for å se om noen på listen (du) har brukt samme brukernavn og passord på andre nettsider.

Hvis brukernavnet og passordet du brukte på MySpace eller Yahoo! en gang i tiden også fungerer på din Hotmail, Twitter, Uber eller

Dropbox-konto er det veldig stor sjanse for at andre har tilgang til alt sammen. Og om de ikke har benyttet seg av det ennå, så er det bare et spørsmål om tid.

Bare husk: HaveIBeenPwned.com har ikke 100% oversikt over alle e-postadresser som noensinne er blitt kompromittert i verden, så selv om det vil være en lettelse om du ikke dukker opp i databasen deres, er du ikke nødvendigvis trygg av den grunn.

Så hva kan du gjøre hvis du har blitt Pwned? Og hvordan kan du gjøre det enkelt å sikre deg?

Bla videre for flere anbefalinger som er enkle å følge.

DEL 2: ENKLE, GODE RÅD

BRUK EN PASSORDBEHANDLER

En passordbehandler er et nøkkelknippe for passordene dine

- Tid: Mindre enn 30 minutter
- Kostnad: 0 – 40,– pr. måned

Det mest effektive skrittet du kan ta for å sikre deg, er å sørge for at du har sterke og unike passord på hver viktige tjeneste.

Det går an å komme opp med systemer som hjelper deg opprette og huske unike passord til alle nettsider du bruker.

Men det er mye tryggere og bedre å bruke en skikkelig passordbehandler – et program for å hjelpe deg holde orden på passord, slik at det blir lett å bruke tryggere passord.

Noen bruker funksjonene som er bygget inn i nettleserene sine for dette. Disse er kronisk utrygge og mangler noen av de viktige funksjonene som hjelper deg opprette og bruke gode, sikre passord.

Jeg foretrekker selv å bruke Dashlane.

LAST NED OG PRØV DASHLANE GRATIS ➤

Dashlane er gratis for én maskin, og forholdsvis rimelig for et abonnement

som synkroniserer passordene dine mellom flere enheter (for eksempel laptop, mobil og nettbrett).

Dashlane har også en business-versjon, som kan hjelpe bedrifter å håndheve sikkerhetsrutiner. I mine øyne er det uten tvil verdt investeringen.

Det tar bare minutter å installere Dashlane og eventuelt oppgradere til betalversjonen. Deretter lar du programmet bare gå i bakgrunnen.

Dashlane vil da spørre deg om det skal huske passordene du bruker når du logger deg på nettsider, eller om det skal generere et nytt, trygt passord når du registrerer deg på en nettside der du ikke har konto fra før.

I løpet av noen dager og uker vil du har lagt all den nødvendige informasjonen inn i Dashlane uten nevneverdig innsats.

- Dashlane kan hjelpe deg ved å:
- Opprette unike, trygge passord for hver tjeneste
- Huske de passordene, samt viktige notater, kredittkortnummer og andre ting du vil holde trygt men lett tilgjengelig
- La deg dele passord trygt med andre Dashlane-brukere (også uten å dele det faktiske passordet, men kun tillate tilgang)
- Synkronisere passord og annen sikker informasjon mellom enheter (betalt)
- Logge deg inn på nettsider automatisk (på desktop) eller halvautomatisk (på mobil)
- Fortelle deg om hvert av passordene dine er trygge eller utrygge
- Advare deg når et hacker-angrep har gjort noen av passordene dine utrygge
- Automatisk endre utrygge passord

Bruk litt tid på innstillingene

Det kan være lurt å bruke noen minutter på gå gjennom innstillingene i Dashlane når du har brukt det en dag eller to, for å tilpasse det dine preferanser. For hvis ikke programmet virker slik *du* vil det skal virke, men for eksempel til stadighet foreslår å fylle ut skjemaer du ikke vil ha fylt ut, er det lett å slutte å bruke det.

LAG ET UNIKT, GODT PASSORD DU KAN HUSKE

En god huskeregel hjelper deg lage et nytt, godt passord til hver tjeneste du bruker

- Tid: 10–15 minutter
- Kostnad: kr. 0,–

Det er flere grunner til at passord alene aldri vil være helt trygge. I hvert fall ikke om du i tillegg skal kunne huske dem. Men vi kan komme opp med passord som er bedre enn det de fleste andre bruker. De fleste hackere går etter lavthengende frukt, og vil ikke bruke mange kalorier på deg om ikke robotene deres lykkes med en gang.

Et slikt forholdsvis godt passord kjennetegnes av at det:

- består av minst 8-10 tegn (gjerne mer)
- ikke utgjør et kjent ord eller navn
- inneholder en kombinasjon av store og små bokstaver, tall og spesialtegn
- er unikt for hvert enkelt nettsted

Hvordan lager du så et slikt passord som du også kan huske?

Her er en metode:

1. Ta utgangspunkt i en frase du alltid vil huske.

Det kan være tittelen på en bok eller film, en linje fra en sang eller et dikt, en gammel adresse, notene i en melodi, resultatet fra en uforglemmelig fotballkamp, eller noe helt annet.

For eksempel: *Ground Control To Major Tom* (de første ordene i David Bowies *Space Oddity*.)

2. Forkorte frasen kreativt, på en måte som kun gir mening for deg.

Det er best om du får forkortet til 5–8 tegn, tall, og både store og små bokstaver. Og det finnes nær sagt uendelig mange kreative måter å forkorte på. F.eks. kan setningen over forkortes til

GC2^Tom
(*G* for ground, *C* for control, 2 for to, *^* for major, og *Tom* for Tom)

eller med

_ctrl->MT
(_ for ground, *ctrl* for control, *->* for to, *MT* for Major Tom)

Du trenger bare én forkortelse som *du* vil huske.

Gjør passordet unikt for hver nettside

Det gjør du ved å legge til et par tegn du får fra nettsiden selv, ved å følge samme regel for hver nettside. Du kan for eksempel velge en fast bokstav i nettsidens navn og/eller antall bokstaver i navnet eller domenenavnet.

Det er lurt å bruke mer enn én variabel, for det mange nettsider som begynner på samme bokstav eller har like mange bokstaver i navnet.

For Google.com, kan vi for eksempel legge til første bokstav og antall bokstaver i navnet, og gjøre om passordet fra punkt 2 til:

G6GC2^Tom
(*G6* fordi ordet *Google* starter på G og inneholder seks bokstaver)

eller vår hemmelige variabel kan være vi kan avslutte passordet med andre bokstav i domenenavnet og antall vokaler.

_ctrl->MTo3
(*o3* fordi andre bokstav i Google er o, og navnet inneholder tre vokaler)

Det viktigste er at du gjør noe som ikke umiddelbart vil gi mening for andre, men som *du* forstår.

Det er det at kun du forstår systemet – og kanskje til og med ville synes det var flaut å forklare det til noen – som faktisk gjør det til et godt passord.

Det finnes utallige måter å gjøre det mer vanskelig å gjennomskue regelen.

Noen tips for hvordan "kryptere" forkortelsen din

Du kan bytte ut *ord* med...

- ... tegn som betyr omtrent det samme (*og* kan byttes med *&* eller *+*)
- ... bokstaver, tall eller tegn som minner om ordet (stopp = *!*, tid = *10*, elv = *11*)
- ... første eller siste bokstav i ordet

Du kan bytte ut *bokstaver* med ...

- ... tegnene like ved siden av på tastaturet eller i alfabetet (A = Q, B = N)
- ... tegn eller tall de ligner på (A = @, B = 8)
- ... tall som representerer dem på en måte (A = 1, B = 2)

Du kan bytte ut *tall* med ...

- ... bokstaveringen av tallet (3 = tre)
- ... tegnet på samme tast på tastaturet du bruker (3 = # på mitt tastatur)
- ... det dobbelte eller kvadraten av tallet (3 = 6 eller 9), eller en annen funksjon

Bruk fantasien, kombinere reglene og kom på egne regler på et hvilket som helst språk du forstår. Deretter kan du bruke samme passordregel på alle sider, og likevel få stort sett unike passord som du kan huske.

Hvis du bruker en passordbehandler i tillegg til en slik regel, trenger du heller ikke gjøre altfor det lett for deg selv å regne deg frem til passordet.

Du vil bare behøve regelen når du skal opprette nye passord eller når du ikke har tilgang til passordbehandleren din når du skal logge deg inn.

LÆR Å BRUKE TOFAKTOR-AUTENTISERING (2FA)

Tofaktor-autentisering er et vanskelig ord for et enkelt sikkerhetstiltak

- Tid: Mindre enn 30 minutter for å komme i gang
- Kostnad: Gratis

Alle som bruker nettbank i Norge kjenner til tofaktor-autentisering (også kjent som 2FA eller flerfaktorautentisering). Det betyr bare at du må bekrefte innlogging på en nettside ved hjelp av en kode du får på mobiltelefonen eller en kodebrikke (eller en annen "faktor» som er uavhengig av brukernavn og passord).

Men visste du at mange andre tjenester du bruker regelmessig – Google, Facebook, Twitter, Dropbox og mange fler – også tilbyr 2FA? De kan autentisere deg ved å sende deg en kode i en tekstmelding eller gjennom en egen app som du kan ha på telefonen eller i nettleseren din.

Det er en veldig effektiv måte å hindre andre i å logge seg på dine konti uten tillatelse, og noe av det beste du kan gjøre for å beskytte deg.

Det høres kanskje slitsomt ut å måtte bruke kode hver gang du skal logge deg på Google, men det slipper du. Som regel vil nettstedet kun kreve kode hvis det ikke kjenner igjen maskinen, nettbrettet eller telefonen du bruker.

Det tar noen minutter å konfigurere hver nettside separat, men om du bare setter det opp på de viktigste sidene – for eksempel Google og Facebook – vil du ha tatt et stort skritt mot å sikre det viktigste av din identitet online.

Last ned en app for å komme i gang

Den beste måten å komme i gang, er å laste ned en av appene for tofaktor-autentisering. Jeg bruker Authy, men Google har også sin egen Google Authenticator. Begge er gratis og begge fungerer med det som er blitt den vanlige standarden.

Logg deg deretter inn i tjenesten du ønsker å sikre (f.eks. Facebook) og gå til innstillingene dine. Oftest slår du på tofaktorautentisering på samme sted eller like ved der du endrer passord.

- Klikk her for å komme i gang med 2FA for Google
- Klikk her og scroll litt ned for å komme i gang med 2FA på Facebook
- På denne siden finner du beskrivelser (på engelsk) av hvordan du slår på tofaktor-autentisering på bl.a. Instagram, Twitter, Apple og Amazon.

For de fleste tjenester er det stort sett samme fremgangsmåte:

- Når du slår på 2FA i innstillingene får du en QR-kode. Bruk kameraet på telefonen til å scanne koden i appen. (Hvis det ikke virker, får du også en lang tallkode du kan bruke om kameraet ditt ikke virker.)
- Når koden er scannet vil en engangskode dukke opp i appen. Denne taster du inn i innstillingene for å bekrefte at du ønsker å slå på 2FA.
- Så enkelt var det.

Neste gang du logger deg på tjenesten fra enhet den ikke kjenner igjen, vil du bli bedt om sikkerhetskode. Denne finner du enkelt ved å åpne appen.

Ofte vil du også bli gitt noen sikkerhetskoder du kan bruke hvis du ikke har appen tilgjengelig. Disse må du ta vare på på et trygt sted. Jeg pleier å kopiere dem over i Dashlane, men jeg skal innrømme at det nok finnes tryggere steder som ikke er sammen med alle passordene mine.

BRUK HTTPS EVERYWHERE

HTTPS Everywhere gjør det vanskeligere å overhøre deg

- Tid: Mindre enn 3 minutter pr. nettleser
- Kostnad: Gratis

På gode, gamle internett er det lett for andre å «overhøre» deg, særlig hvis de gjør en liten innsats.

Du kjenner sikkert igjen bokstavene HTTP som ofte står i begynnelsen av en nettadresse. Kommunikasjonen med en nettside som begynner på HTTP er omtrent like lett å avlytte som telefoner i gamle tegneserier. Det er bare å koble seg på linjen på et hvilket som helst sted mellom deg og nettsiden – og det er magne slike steder – så kan man få med seg alt som sies.

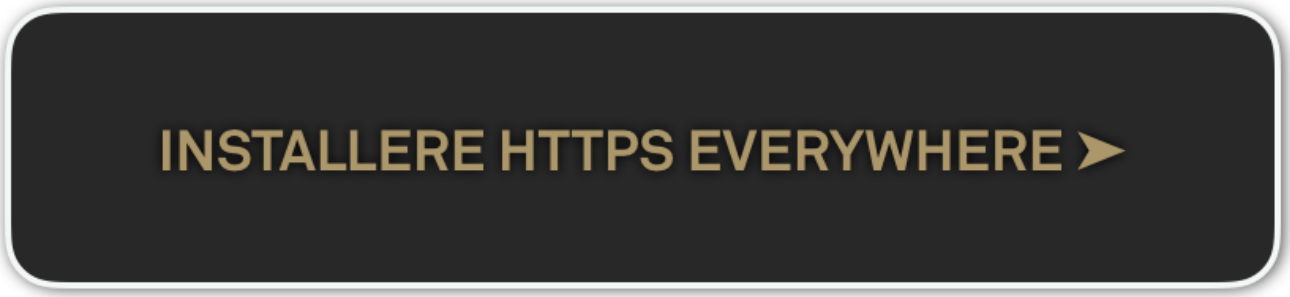
Så om du sender passord, kredittkortnummer eller annen sensitiv informasjon over en HTTP-linje, må du ikke bli overrasket om uvedkommende får tak i den informasjonen.

Mange nettsider tilbyr imidlertid HTTPS, som er en sikker versjon. All kommunikasjonen vil da bli kryptert, slik at den ikke vil gi noen mening for uvedkommende. De kan fortsatt se at du besøker f.eks. Google, men de kan ikke lenger se hva du søker. Det er det bare deg og Google som får vite.

Noen nettsider støtter bare HTTP og noen nettsider (som Google og Facebook) bruker automatisk HTTPS. Men det finnes også nettsider som tillater begge deler, uten at det er noen automatikk i det ene eller det andre.

Ettersom de aller fleste av oss vil foretrekke sikker kommunikasjon som standard, går det imidlertid an å installere en utvidelse i flere nettlesere (Chrome, Firefox, Opera og Android-enheter) som tvinger bruk av HTTPS på alle nettsteder der det er tilgjengelig.

Utvidelsen er utviklet av non-profit-organisasjonen Electronic Frontier Foundation, og kan lastes ned og installeres gratis fra deres nettsider.



BRUK EN GOD VPN

Med en god VPN kan ingen se hva du gjør på internett.

- Tid: 30 min
- Pris: ca. kr. 50/måned

HTTPS er vel og bra for å hindre andre fra å vite mye av det du gjør på Internett, men det dekker ikke alt. Fortsatt er det mange nettsteder som ikke støtter HTTPS. Og selv om nettsidene har sitt på stell, kan uvedkommende fortsatt se hvilke nettsider du besøker. Ofte er det ille nok.

Løsningen er å bruke en god VPN.

VPN står for Virtual Private Network, skjuler deg for mange av dem som ellers kan se alt du gjør på nett. For eksempel mobilselskapet ditt, internettleverandøren din, cafeen som tilbyr gratis WiFi, arbeidsgiveren din, eller folk med skumle hensikter.

I stedet for at du kobler maskinen din direkte til nettsidene du vil besøke, f.eks. YouTube, Netflix og Facebook, vil du koble deg til serveren til VPN-en, og der stopper sporet for dem som snoker. Alt spionene ser er at du er koblet til den serveren, men de kan ikke vite hvilke sider du besøker eller hva du gjør på de sidene.

Det er en bonus at mange VPN-selskaper lar deg velge mellom servere i ulike land. På den måten kan du få tilgang til innhold som ellers er geografisk begrenset. Det er mest verdifullt i udemokratiske land der myndighetene stenger, forfalsker eller overvåker ulike tjenester, men norske brukere kan ha mye glede av for eksempel å få tilgang til innholdet på amerikanske Netflix gjennom en server i USA.

Store forskjeller mellom VPN-leverandører

Hvilken VPN-leverandør du vil bruke avhenger av hva du ønsker å få til. Selskapene tilbyr VPN i ulike land med ulik lovgivning, de tilbyr ulike grader av beskyttelse, ulik kapasitet på linjene sine, ulik teknologi, og så videre.

Og du må selvsagt stole på selskapet du velger, for du må ta dem på ordet på mange ting. Det finnes flere VPN-leverandører som snur seg rundt og selger dataen dine i en eller annen form. Og hvis det var en av tingene du ville beskytte deg mot, er du ikke kommet noe lenger.

For brukere i Norge bør et av kriteriene dessuten være at leverandøren faktisk har server i Norge, slik at du kan bruke VPN-en uten å bli låst ute fra f.eks. NRK sitt innhold. Det er det ikke alle som har.

Jeg bruker nå VyprVPN fra GoldenFrog, og er strålende fornøyd med dem.

De gir god hastighet, tilbyr mange servere, har ingen loggføring, og har god brukeropplevelse, som er de viktigste tingene jeg ser etter i en god VPN. De tilbyr en gratis prøveperiode, så du risikerer ikke mye ved å prøve dem ut.

Tidligere har jeg brukt Hide.me, som også har servere mange steder i Europa og USA. Jeg var fornøyd med dem, og det var ingen viktig grunn til at jeg skiftet vekk fra dem annet enn at jeg lot abonnementet mitt utløpe.

Dessuten har jeg prøvd NordVPN. Jeg er ikke så glad i dem, blant annet fordi jeg fikk litt problemer med hastigheten da jeg prøvde dem. Men de har lang fartstid, godt rykte, og et stort nettverk med mer enn 1000 servere over hele Europa, Nord-Amerika, og store deler av Asia.

Alle tre tilbyr servere i Norge, USA og en rekke andre steder.

BRUK ANTIVIRUS OG ANTI-MALWARE

Det er ikke lenger nok med bare antivirus

• Tid: 10–15 minutter for nedlasting og installasjon (+ ukjent tid for scanning av maskinen)
• Kostnad: fra kr. 0 – ca. 1000 pr. år

Vanlige virus er ikke lenger den største trusselen, men det finnes en lang liste ulike typer "malware" som man bør beskytte seg mot av ulike grunner. Alt fra programmer som bare vil vise deg litt ekstra reklame, til programmer som spionerer på alt du gjør, og dem som låser alle filene dine og krever løsepenger.

Det er dumt å være helt ubeskyttet mot slikt, særlig når det finnes forholdsvis mange gode, gratis antivirus-programmer.

Jeg bruker gratis-programmet Sophos Home som går i bakgrunnen mens jeg jobber, og tilsynelatende gjør en god jobb med å beskytte meg.

LAST NED SOPHOS HOME GRATIS ➤

Det er imidlertid et problem at slike gratis antivirus-programmer ikke dekker opp mot alle de ulike truslene som finnes der ute.

Et par ganger, når jeg har vært ekstra paranoid, har jeg derfor også tydd

til Malwarebytes. Det er er et anti-malware-program som har en annen tilnærming til problemstillingen enn de andre på dette feltet, og som kan kjøres parallelt med et av dem. (Det er ellers ikke noen god idé å kjøre flere antivirus-programmer parallelt)

Malwarebytes har både gratis og betalversjon, som begge visstnok fanger opp ting som ikke andre plukker opp.

Jeg har imidlertid ikke hatt virus (som jeg har oppdaget) på min maskin på over 10 år, så jeg har ikke fått sendt noen av programmene gjennom syretesten.

HOLD DEG OPPDATERT

Det er viktig at du oppdaterer programvaren din

- Tid: 5–10 minutter en gang i blant
- Kostnad: kr 0,– og litt irritasjon

Det er irriterende når Apple, Adobe eller Microsoft nærmest tvinger deg til å oppgradere til siste versjon av programmet du bruker, og du oppdager at de har endret på noe du både var vant med og komfortabel med.

Endringen ødelegger arbeidsflyten fullstendig, får deg til å gjøre flere feil, og tvinger deg til å lære noe nytt.

Men uansett hvor irriterende det er, så er det viktig at du gjør det. Den viktigste grunnen til slike endringer er nemlig ikke å irritere deg, eller vise hvor flinke de er til å flytte på knapper, men å tette sikkerhetshull som er blitt kjent.

Et slikt sikkerhetshull kan være en eller annen svakhet i koden. Noe som gjør at skurker kan finne en bakvei inn i for eksempel datamaskinen eller telefonen din. Nesten all programvare har slike hull.

Og når et sikkerhetshull er blitt kjent, er det ofte bare et tidsspørsmål før hackerne har laget en robot som kan gå ut på internett, på jakt etter dem som ikke har oppdatert programvaren sin, og utnytte det sikkerhetshullet på en eller annen måte.

Men hvis du regelmessig oppdaterer programvaren på maskinen, telefonen og nettsiden din – og alle andre apparater du har som er koblet til Internett – vil du redusere sjansen for å bli offer noe slikt.

DEL 3: NOEN AV TRUSLENE

PASS DEG FOR MALWARE

Virus har gått fra å være vandalisme til sofistikert «malware».

På 80- og 90-tallet var hacking og datavirus stort sett forbundet med rampestreker og vandalisme. Og sporene etter dem var like diskret som grafitti på T-banen: Ikke bare høyst synlig, men også gjerne signert av gjerningspersonen som var sulten på anerkjennelse.

Mange har nok fortsatt det bildet på hva hackere er, men i dag er situasjonen en helt annen. Man snakker ikke bare om virus, men om såkalt malware – en mye mer omfattende gruppe uønskede programmer som i større grad handler om vinningskriminalitet enn om hærverk.

(Selve ordet er satt sammen av mal-, i betydningen dårlig, og -ware som i ordet software, eller programvare.)

Det finnes flere typer malware, og jeg kan ikke gå gjennom alle her. Men noen som er verdt å vite om:

Adware

Noen ganger brukes ordet «adware» om legitime programmer som finansierer utviklingen med annonser i stedet for vanlige salgsinntekter. I denne sammenhengen mener vi imidlertid malware-versjonen av adware.

Slike programmer installerer seg på maskinen din og viser deg uønsket reklame, gjerne i form av popup-vinduer, eller ved å erstatte annonsene på sidene du besøker med egne annonser.

Hvis maskinen din er infisert, er det likevel ikke sikkert du innser at problemet med alle annonsene du ser er på din egen maskin, og ikke bare et problem med internett.

Som oftest er adware irriterende, og det kan gå utover hastigheten på maskinen, men det er ikke spesielt farlig.

Spyware og keyloggers

Spyware er en type programmer som – som navnet sier – spionerer på deg. De «snilleste» versjonene samler bare informasjon om deg for å vise deg mer spissede annonser, og kan være kombinert med adware.

En langt skumlere versjon er keyloggers, som registrerer hvert eneste tastetrykk du gjør, og sender det tilbake til eieren sin. På den måten kan uvedkommende få tak i brukernavnene og passordene dine, samt mye annen sensitiv informasjon.

Det finnes også andre typer spyware, som ser på ulike deler av maskinen din og sender informasjon om deg «hjem» til eieren sin.

Bot

En bot – forkortelse for robot – er et lite program som plasseres på en maskin og som gjør at andre kan ta kontroll over hele eller deler av maskinen.

En hacker kan kontrollere alt fra noen hundre til flere hundre tusen slike bot-er, samlet til en hær som kalles et bot-net. Slike botnet brukes til å sende ut spam, angripe andre mål, eller simpelthen tråle internet på jakt etter flere maskiner som er lette å infisere og rekruttere til den voksende hæren av bots.

Siden det er best for eieren om bot-ene er tilgjengelig hele tiden (og ikke blir borte når folk slår av maskinen og går fra jobb) er bots mest vanlige på enheter som alltid er koblet til internet, som webservere eller på apparater med nettilgang, som webkameraer, moderne termostater og TV-er.

Ransomware

En av de skumleste typene malware er såkalt ransomware, et virus som infiserer maskinen din og krypterer filene dine.

Hvis de som står bak vet hva de gjør, er det umulig for deg å få filene tilbake i lesbar stand uten deres hjelp. Deretter blir du avkrevd løsepenger for å få tilgang til filene tilbake.

De færreste som blir rammet av et slikt agrep ser noe annet valg enn å betale.

Så hvordan kan du beskytte deg mot malware?

- Ikke åpne vedlegg du ikke forventer å få – selv om du kjenner avsenderen
- Hold programvaren din oppdatert
- Bruk et godt antimalware-program
- Ta gode sikkerhetskopier

SE OPP FOR FALSKE, TRÅDLØSE NETTVERK

Du er ekstra utsatt på offentlige trådløse nettverk

Det blir stadig lettere, og derfor også stadig vanligere, å forfalske trådløse nettverk – både wifi og mobilnettverk.

Hvem som helst kan putte en liten boks i vesken eller ryggsekken sin som utgir seg for å være mobiltårnet til Telenor, wifi-en til business class-loungen på flyplassen, eller nettverket på cafeen der du pleier å jobbe.

Ofte trenger du ikke engang koble deg på selv. Telefonen eller laptopen din kjenner igjen navnet, tror den er på kjente marker, og kobler seg til automatisk. På den måten kommer hackeren mellom deg og internett.

Om du ikke har beskyttet deg godt, kan de se alt du gjør.

Så hvordan kan du beskytte deg mot falske nettverk?

- Vær skeptisk til trådløse nettverk du ikke kjenner. (Men du behøver neppe la deg skremme fra å bruke dem.)
- Bruk HTTPS Everywhere, så kan ikke nysgjerrige spioner se hva du gjør på sidene du besøker.
- Bruk en god VPN, så kan de ikke engang se hvilke sider du besøker

IKKE LA DEG LURE AV PHISHING

Såkalt "phishing" blir stadig mer sofistikert og stadig lettere å falle for.

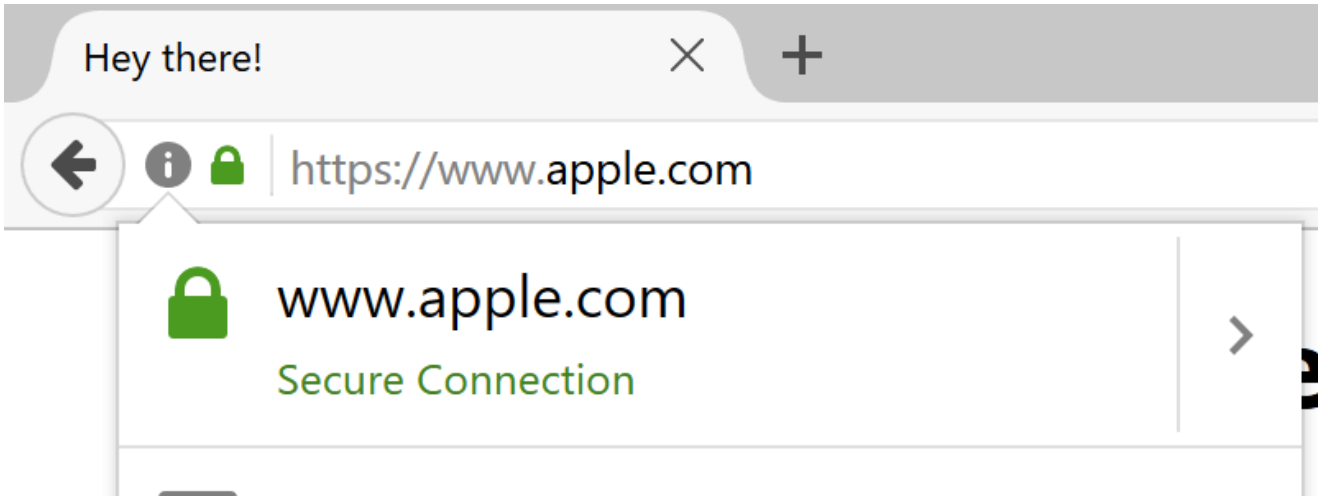
Phishing (som i det engelske ordet for å fiske, bare med "ph") er internett-lingo for å forsøke å lure folk til å oppgi brukernavn, passord, svar på sikkerhetsspørsmål eller annen sensitiv informasjon.

For eksempel kan du få en mail fra noen som utgir seg for å være noen du stoler på – banken din, Google, Facebook – og som inviterer deg til å fylle ut et skjema som ber om sensitiv informasjon. Informasjonen sendes imidlertid ikke dit du tror, men til uvedkommende, som dermed har alt de trenger for å få tilgang til din konto.

I gamle dager var phishing usofistikerte saker som var lette å gjennomskue. Dårlig språk, dårlig design, åpenbart feil nettadresse, etc.

Men angrepene er etterhvert blitt svært sofistikerte. E-posten du får kan se 100% formell ut og tiltale deg med navn. Nettsiden du kommer til kan se nøyaktig ut som innloggingssiden til Google eller Facebook.

Ved hjelp av spesialtegn og tekniske finurligheter kan angriperne på noen nettlesere til og med få lenken du klikker på og nettadressen i adresselinjen til å se helt ut som URL-en til nettsiden du trodde du skulle til. Og nettsiden bruker HTTPS, så du ser hengelåser og andre signaler du er vant til å se når du er trygg.



*Her står det faktisk ikke **www.apple.com** – les mer på **xudongz.com** (engelsk) hvis du vil lære mer.*

Så hvordan kan du unngå å bli lurt av phishing?

- Vær skeptisk til e-post du får som ber deg logge inn et sted, endre passord, eller oppgi annen sensitiv informasjon.
- Hvis du får mistanke om at noe er galt, skriv nettadressen manuelt inn i adressefeltet i nettleseren (eller bruk et bokmerke) i stedet for å klikke på en tilsendt lenke. Hvis du selv skriver inn adressen, vet du hvor du kommer. Og hvis informasjonen er viktig nok til å sende deg en mail, vil den også være viktig nok til å oppgi på selve nettsiden.
- Vær skeptisk til kundeundersøkelser, om du ikke vet du er på riktig nettside.
- Ikke delta i kjedebrev på sosiale medier som krever at du deler personlig informasjon ("10 konserter jeg har vært på", "Svar X spørsmål om meg", etc.), for ofte finnes svarene på vanlige sikkerhetsspørsmål blant informasjonen du oppgir.
- Bruk en passordbehandler. Den vil ikke la seg lure av en falsk adresse, og vil derfor ikke tilby seg å fylle inn brukernavn og passord når du er på en forfalsket side.
- Bruk tofaktor-autentisering (2FA). Selv om noen får tak i passordet ditt, vil de likevel ikke kunne logge seg inn på siden uten sikkerhetskode fra telefonen din.

SJEKKLISTE

Huker du av for alle disse punktene er du tryggere enn de fleste på nett.

- [ ] **Bruk en passordbehandler**
  Last ned Dashlane her
- [ ] **Lag gode, unike passord du huske**
- [ ] **Lær å bruke 2-faktorautentisering**
  Last ned Authy her og følge anvisningene her for å aktivere 2FA
- [ ] **Bruk *HTTPS Everywhere***
  Installere HTTPS Everywhere her
- [ ] **Bruk en god VPN**
  Last ned VyprVPN her
- [ ] **Bruk Anti-Virus & Anti-Malware**
  Last ned Sophos Home her og Malwarebytes her
- [ ] **Hold deg oppdatert**