Har du kontroll over dine digitale hjelpemidler - digitale verktøy

Det finnes ondsinnede programmer der ute som er i stand til å lure maskinen din og stjele både kredittkortinformasjon og personlige filer. Over én million mennesker rammes av nettkriminalitet *hver eneste dag*, og sannsynligvis har du selv blitt hacket mist en gang– *enten om du vet om det selv eller ikke*.Tror du at brukernavnet og passordet ditt er trygt, bare fordi du *ikke* har skrevet det ned eller fortalt det til noen andre? *Så enkelt er det ikke*

Informasjon til FSF Rygges medlemmer
November 2015
Ting og Tang - Digitale verktøy
Har du kontroll over dine digitale verktøy?

1. Innledning

I 1940-årene ble det konstruert en rekke digitale datamaskiner basert på elektroniske komponenter og i 1941 kom historiens første programmerbare maskin, Z3.
I dag blir vi svindlet og utnyttet gjennom bruk av våre forskjellige digitale verktøy. En av grunnene er manglende kunnskaper og en annen er manglende *beskyttelsesprogrammer*.
Men tilbake til 70 tallet. En dataansatt i en bank i Frankrike overførte små beløp fra andres lønnskontoer til sin egen bankkonto. Han ble millionær, avslørt og dømt for økonomisk datasnoking. Den første *hacker* i historien?
En datasnok eller hacker er en person som setter pris på den intellektuelle utfordringen ved å bryte grenser eller jobbe seg rundt begrensninger på et felt han er interessert i, primært *dataprogrammering*. Begrepet oppstod blant informatikk-studentene på Massachusetts Institute of Technology på 60 tallet.
Over én million mennesker rammes av nettkriminalitet *hver eneste dag*, og sannsynligvis har du selv blitt hacket mist en gang– *enten om du vet om det selv eller ikke*.

Punkt 11 i denne infoen viser til IKTnytt.no sin sikkerhetsguide – skrevet for deg som ønsker å lære hvordan du sikrer din PC (personlig datamaskin) , Mac (Macintosh), server (tjener), iPad (nettbrett) og iPhone (smarttelefon) mot *kyberangrep* og datainnbrudd fra *hackere*.

- Norge har fått et eget *kyberforsvar (2012)* som den fjerde forsvarsgren (tidligere, Forsvarets informasjonsinfrastruktur).

2. Hackere

Det finnes ondsinnede programmer der ute som er i stand til å lure maskinen din og stjele både kredittkortinformasjon og personlige filer. Dagens hackere defineres som datamaskinens entusiaster som bryter inn eksterne datasystemer, kombinerer kraften til Internett og spesialiserte programmeringskunnskaper og omgår avanserte sikkerhetssystemer. De ignorerer enhver stat, lover og bestemmelser de bryter i prosessen. Hackere er mer bredt definert i datamaskinen- og Internettsamfunnet som personer som: - endrer eksisterende programvare/datasystem, - programmerer skadelig programvare, - stjeler informasjon eller «planter» feilinformasjon.

Årsakene til denne virksomheten er mange. Enten for egen vinning eller på oppdrag fra andre aktører f.eks. i private selskaper eller i offentlig sektor.
http://www.ung.no/nettvett/2397_Hvordan_unngå hacking

3. Brukernavn og passord
Tror du at brukernavnet og passordet ditt er trygt, bare fordi du *ikke* har skrevet det ned eller fortalt det til noen andre? *Så enkelt er det ikke.* Det finnes dessverre en mengde måter for uvedkommende å skaffe seg tilgang til ditt *brukernavn og passord* til alle dine dataverktøy. Ref. pkt. 11.
https://sikkert.no/sikre-pc-en-din

4. Smarttelefon og nettbrett
iPhone og iPad er en av hackernes nye favoritter. Dataverktøyene inneholder ofte mye sensitiv informasjon som må/bør beskyttes, men mange tenker ikke på dette, noe som kan være svært «farlig».
https://norsis.no/2013/01/sikring-av-nettbrett-og-smarttelefoner

5. Slik hindrer du at noen misbruker Facebook - kontoen din
Mange har brent seg på ikke å logge ut fra Facebook. Dermed kan hvem som helst opptre som deg – for eksempel ved å lese igjennom alle meldingene dine eller poste en statusoppdatering, en *facerape.* Heldigvis finnes muligheten for å logge ut andre enheter som er koblet til Facebook-profilen din. Det er kjekt ikke bare når du har glemt å logge ut på datasalen, men også dersom mobiltelefonen din skulle bli stjålet og du ikke har beskyttet den med en sikkerhetskode.
Fremgangsmåten er slett ikke vanskelig, og det kan gjøres både fra PC og mobiltelefon.
http://www.dinside.no/901770/glemt-aa-logge-deg-av-facebook

6. Hvorfor er virus farlige?
Det er ikke nødvendigvis slik at virus er farlige i det hele tatt, men mange av dem er det og skaper til dels store problemer for eier og brukere av digitale verktøy. Problemene kan være alt fra å irritere brukerne gjennom å vise reklame eller ønskede politiske budskap hver gang du starter opp, til å manipulere operativsystemet (f.eks. Windows) og ta kontroll over dataverktøy og bruke de til å utføre *kriminelle* handlinger.
Vi skiller gjerne mellom ”ufarlige” og ” destruktive” virus, og det er de destruktive som ofte utgjør et problem. De mest ”vellykkede” virusene har påført verdenssamfunnet kostnader i milliardklassen.
Nylig lykkes en gruppe kriminelle å stjele 260 millioner fra bankkontoer i 26 land ved å hacke seg inn i en database med forhåndsbetalte betalingskort og tømme minibanker.
http://www.tek.no/artikler/de_farligste_datavirusene/84352
http://www.aftenposten.no/digital_old/nyheter/Slik-beskytter-du-deg-mot-virus-6611748.html

7. E- post
I mange år har det blitt advart mot svindelforsøk etter at flere e-poster som lokker med gratis gavekort har blitt sendt ut. Du må aldri åpne en e-post som starter med «Ordrebekreftelse, Godkjenning av gavekort osv.». Ikke klikk på lenken, men slett *e-posten.* Imidlertid:- ofte brukes adresseboken i e-post programmet ditt som utgangspunkt for å finne nye potensielle ofre, ganske smart, fordi dine kjente tror det er en e-post fra deg, og den åpner de vel i god tro?
http://www.nettvett.no/e-post/sikrere-e-postbruk

8. Slave-maskiner
H*ackerne* kan være ute etter å plante en *ukjent programvare* i din datamaskin, eller så kan lenken føre deg videre til *nettsider* du ellers aldri ville gått inn på, hvor det kanskje lokkes med gavekort, konkurranser, spill eller lignende. Enkelte hackere er kun ute etter å gjøre deg til ***en slave*** for å kunne stenge *en nettverksforbindelse*.

- *Eller de ønsker å «stenge» et mediehus, en skole, en politistasjon, et sykehus, osv.*

NB!
Et angrep må ikke nødvendigvis utføres via et nettverk. Det er mulig å lage programmer som ikke gjør annet enn å kopiere seg selv. Etter kort tid vil prosessoren bli overarbeidet og systemet vil stoppe.

- *Da kan du ikke bruke din PC som før eller i det hele tatt.*

FSF avd Rygge

http://www.dn.no/tekno/2014/06/18/Hacking/hacker-brukte-slaver-tjente-37-millioner-kroner

9. Historiens største hackerangrep på Internett
Et angrep som ble utført av en nederlandsk vert i et forsøk på å stoppe spredningen av en anti-spam liste fra SpamCops abonnementer. Kort tid etter ble OnNet sin egen serverpark som bl.a. IKTnytt.no benytter utsatt for et lignende angrep. *I tillegg har de fleste store bankene i verden opplevd minst ett alvorlig angrep det siste året og flere store mediehus har gått ned hele dager.*

10. Hvordan kan du beskytte deg mot hackerangrep?
Det kan du ikke, men en liste over *forebygging og responsverktøy* er gitt nedenfor. Se punkt 11 dersom du ikke er familiær med termologien i dette punktet.
Brannmurer
Brannmurer kan settes opp til å ha enkle regler slik å tillate eller nekte protokoller, porter eller IP-adresser. I tilfelle et enkelt angrep fra et lite antall uvanlige IP-adresser for eksempel, kan man sette opp en enkel regel for å slippe all innkommende trafikk fra disse hackere.

Anti-virus program

- *1 av 4 PCer har ikke et aktivt anti-virus program. Dette er skremmende.*

Når brannmuren er på plass, *er neste obligatoriske oppgave å installere et skikkelig anti*-virus program som sjekker maskinen for virus, trojanere, ormer og annen malware som du kommer over når du installerer programmer, surfer på nettet og laster ned og leser epost.

Å benytte spamfilter på private e-postadresser for å forsøke å unngå uønsket e-post **er *nytteløst.*** Benytt heller spamfiltre som bruker en statistisk metode, kalt *bayesiansk filtrering*, der programmet læres opp til å identifisere spam ved å analysere meldinger som brukeren mener er spam. Metoden er svært effektiv, men krever kontinuerlig oppfølging.
En tredje metode sjekker IP-adressene til e-postens opprinnelsessted mot kontinuerlig vedlikeholdte svartelister.
Imidlertid; - spammere blir stadig flinkere til å skjule også IP-adressen og i dag går trenden mot å sende «angrep» til PC operativsystemer (Disk Operating System, DOS) med et lovlig innhold, **men med dårlige hensikter.**
http://www.online.no/sikkerhet/virus-og-hacking.jsp

11. Litteratur - anbefalte lenker

Hva er et datavirus, og hvilke typer virus finnes?
Hva er en data orm?
Hva er en trojansk hest og hvordan bli kvitt trojanere på min maskin, nettbrett og mobil?
Hva er en bakdør?
Hva er forskjellen mellom malware, spyware, scareware, Ad-ware og root-kits?
Hva er et botnet, også kalt Zombies?
Hva er et DDoS angrep?
Hva er et "Brute Force" angrep?
Slik får andre tilgang til ditt BRUKERNAVN og PASSORD!
Ikke bruk disse passordene – følg disse passordreglene!
Sikkerhetsguide – Slik unngår du hacking og datainnbrudd
Trusselbilde i Norge: Stadig økende gap mellom trussel og sikkerhetstiltak

NB!
Punkt 11 Litteratur-anbefalte lenker viser til IKTnytt.no sin sikkerhetsguide– skrevet for deg som ønsker å lære hvordan du sikrer din PC, Mac, server, nettbrett og smarttelefon mot kyberangrep og datainnbrudd.

Endringer
FSF avd Rygge gjør oppmerksom på at det kan ha skjedd endringer i teksten siden den ble publisert på vår hjemmeside. Om du velger å gå videre og benytte deg av de opplysningene vi har lagt ut kontroller derfor med utgiver om det er kommet noen endringer.