Utpressing ….

Dette er det sikkert blitt skrevet om før i denne spalten, men en god ting kan ikke gjentas for ofte: Dersom du får e-poster som sier at du må betale et stort antall Bitcoins eller Euro til en eller annen konto, så vær veldig skeptisk!

Det er klart at dersom du har kjøpt noe på nettet eller venter på en e-faktura med samme beløpet, så er det nok i orden – men undersøk allikevel for å være sikker!

Det går i bølger. I sommer så var det en bølge av e-poster som påsto at de hadde fått tak i din e-post adresse OG PASSORDET ditt og at de ville bruke dette til å sende ut informasjon om deg, at du hadde vært innom pornografisider på nettet blant annet. Eller hadde kjøpt noen tilsvarende «tjenester» en eller annen gang. Så for å unngå at de sendte ut denne informasjonen om deg så måtte du betale en masse penger. Og igjen her for to uker siden så begynte en ny bølge av disse e-postene. Altså utpressing eller «Sextortion» (sex extortion) på utenlandsk. Oppfinnsomheten er uendelig.

Forrige hovedrunde for et år siden var at du fikk en e-post om at alle filene og bildene dine var nå kryptert med en hemmelig kode som du bare kunne få dersom du betalte. Denne var faktisk ganske guffen og jeg må innrømme at jeg gikk fem-på: jeg åpnet en e-post som så ut som at den kom fra Postverket og – pang – så var det gjort. Denne e-posten installerte en såkalt Trojaner på min maskin og alle filene ble hemmelig kryptert, men hvis jeg betalte da, 1000 euro til en konto, så ville alt bli bra igjen. Det gjorde jeg ikke. Jeg hadde egen back-up av mesteparten av det som ble borte, heldigvis. Denne typen virus kalles «Ransomware» (gisselprogram) fordi den tar alle filene og bildene dine som gisler for å utpresse deg.

Men hvordan får de tak i e-post adressen din og passordet? Eller er det blank løgn? E-post adressen er kanskje ikke så veldig vanskelig å finne. Og ofte ser det ut til at disse e-postene kommer fra «deg» som avsender. Et lite Google-søk kan fremskaffe mye. Og mange selskaper og foreninger legger ut e-postene til sine medlemmer og ansatte. (- dette burde de slutte med, spør du meg) Men passordet da? Det skulle jo være godt beskyttet overalt? Tja …. Det viser seg at mange e-post tjenere ligger noen hestehoder bak de mest oppfinnsomme «hackerne». Det gjelder særlig tjenerne til firmaer og foreninger – mens de store: online (Telenor), Google (gmail), Microsoft (hotmail, etc.), Yahoo er bedre beskyttet. Vi skrev tidligere om «gratis WiFi» på kaffebarer og hoteller, som eksempel. Der har alle stort sett et felles passord for å logge seg på. Og, ja, lese e-posten sin. Der kan andre i lokalet plukke opp både e-posten og passordet ditt hvis de vil og vet hvordan. (det er OK å lese aviser på disse barene, men hold deg unna e-posten din!) Det er også avdekket at noen (mindre) e-post tjenere kanskje har noen utro folk som selger lister med e-poster og passord til både firmaer og hackere. Straffene for denne type virksomhet er blitt ganske så alvorlige etter hvert – særlig i USA. Det er fengsel som gjelder.

Men i 99% av tilfellene så er det blank løgn: de har kanskje e-posten din, men IKKE passordet. Så for alle e-poster i den kategorien vi har omtalt her: **HIV DEM!** Og ikke åpne.

Når vi nå går inn i julen så er det liten grunn til å ødelegge høytiden ved å være paranoid - følg noen enkle regler, så er vi ganske trygge med e-postene våre:

- Ikke les eller skriv e-poster på steder der det er gratis WiFi med felles passord (eller uten passord)
- Lag deg et passord som ikke er så lett å gjette seg frem til
- Ikke spre passordet ditt til andre
- Ikke bruk samme passord overalt – i alle fall der hvor det er penger involvert (banken, aksjer)
- Bruk gjerne to-nivå autentisering (2FA) sammen med mobilen din

Det er mange steder som «maser» om passordet ditt, hvordan det skal bygges opp med antall tegn, store og små bokstaver, tall, andre tegn osv.). For oss stakkarer er jo dette en pest og en plage! Nå er det laget en verdensomspennende liste over de mest brukte: 123456, password, 123456789, 12345678, 12345, 111111, 1234567, sunshine, qwerty, iloveyou, princess, admin, welcome, 666666, abc123, football osv. Med dagens datakraft er det en smal sak å prøve ut et stort antall passord for å bryte seg inn på kort tid. Som du ser, bare med tall dominerer og så på engelsk. *Kjør på norsk!* – det er tross alt bare 5 millioner av oss. Husk at hacking er en internasjonal bransje.

To-nivå (eller to-faktor) autentisering blir mer og mer benyttet. Det er å anbefale – i alle fall i utlandet. Den mest brukte metoden er ved hjelp av mobilen din. Du får der en ny kode på sms hver gang du logger inn og som du da bruker (til å logge deg inn) i tillegg til passordet. Problemet kan være at du må ha mobilen din i nærheten og den må være ladet opp! Det finnes også andre metoder, med for eksempel kodebrikke eller fingeravtrykk gjenkjenning på mobilen, men de er mye mindre i bruk.

Så ikke fortvil! Hiv alt som du er usikker på hva er – og særlig de som truer deg med et eller annet og vil ha penger. De største hackerne sender ut 100 millionvis av disse e-postene (også på lokalt målføre) og dersom bare 0,0001 % av mottakerne biter på så blir det mye penger av det!

Med dette vil vi ønsker alle våre lesere:

En Riktig God Jul og

Et Godt Nytt År!

- Og uten utpressings e-poster!

Tore Langemyr Larsen, Seniornett Norge