OUCH! | Oktober 2017

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...



# Å hjelpe andre med å sikre seg selv

## Oversikt

Mange av oss er komfortable med teknologi, også med hvordan man bruker det trygt og sikkert. Imidlertid kan det være at venner og familie ikke er like komfortable med dette. Det kan faktisk være at de er forvirret av, eller til og med redd for teknologien. Dette gjør dem veldig sårbare for nåtidens cybertrusler. Cybersikkerhet trenger ikke være skummelt, det er faktisk ganske enkelt når du har forstått det grunnleggende. Så de trenger sannsynligvis bare en guide som deg for å hjelpe dem med å forstå det grunnleggende.


**Gjesteredaktør**

Randy Marchany (Twitter: **@randymarchany**) er CISO ved Virginia Tech og en sertifisert instruktør ved SANS-instituttet.


## Fem enkle steg

Her er fem enkle steg du kan bruke for å hjelpe andre med å overkomme teknologifrykten, og få det meste ut av nåtidens teknologi på en sikker måte. Se ressurs-seksjonen på slutten av nyhetsbrevet for mer informasjon om hvert punkt.

1. **Sosial manipulering**: Sosial manipulering er en vanlig teknikk brukt av cyberkriminelle for å lure folk til å gjøre ting de ikke burde, som å avsløre passord, infisere datamaskinene sine, eller oppgi sensitiv informasjon. Dette er ikke nytt, svindlere har eksistert i tusenvis av år. Den eneste forskjellen nå, er at de samme teknikkene brukes over nettet. Du kan hjelpe andre ved å fortelle dem om de vanligste kjennetegnene for forsøk på sosial manipulering, som når noen forsøker å skape en sterk følelse av hastverk, når noe er for godt til å være sant, eller når en cyberkriminell utgir seg for å være noen du kjenner, men det høres ikke ut som dem. Del eksempler på sosial manipulering med hverandre, som phishing-e-post eller de beryktede telefonene med «Microsoft-svindel». Om ikke annet burde du sørge for at familiemedlemmene dine vet at de aldri må gi passordet sitt til noen, eller tillate fjerntilgang til datamaskinen deres.
2. **Passord**: Sterke passord er nøkkelen til å beskytte både enheter og brukerkontoer på nett. Gå gjennom prosessen med å lage sterke passord sammen med dine familiemedlemmer. Vi foreslår passord-setninger fordi de er enklest å skrive og å huske. Passord-setninger er ikke mer enn passord satt sammen av flere ord. Hjelp dem i tillegg med å installere og bruke passordhvelv. Det er viktig å bruke unike passord for hver enhet og brukerkonto. Hvis et passordhvelv blir for overveldende kan du heller lære dem å skrive ned passordene, for så å oppbevare dem på et sikkert sted. For viktige

## Å hjelpe andre med å sikre seg selv

brukerkontoer kan du hjelpe dem med å slå på to-trinns verifisering (også kalt to-faktor autentisering). To-trinns verifisering er en av de mest effektive tiltakene du kan gjøre for å sikre enhver brukerkonto.

3. **Oppdatering**: Å holde systemer oppdaterte er et nøkkelgrep enhver kan gjøre for å sikre sine enheter. Dette gjelder ikke kun for datamaskiner og mobiler, men også for alt som er koblet til internett, som for eksempel spillkonsoller, termometere, eller til og med lys eller høyttalere. Den enkleste måten å være sikker på at alle enheter er oppdatert på, er ved å aktivere automatisk oppdatering der det er en mulighet.
4. **Antivirus**: Alle kan gjøre feil. Noen ganger klikker vi, eller installerer ting vi muligens ikke skulle, som kan føre til infeksjon på enheten. Antivirus er laget for å beskytte oss fra disse feilgrepene. Selv om antivirus ikke kan stoppe all skadevare så hjelper den med å oppdage og stoppe de mest vanlige angrepene. Derfor er det lurt å forsikre seg om at alle PC-ene har antivirus installert og at det er oppdatert og aktivert. I tillegg inneholder mange av dagens antivirus-løsninger sikkerhetsteknologi som brannmurer og beskyttelse for nettleseren.
5. **Sikkerhetskopiering**: Når alt svikter er sikkerhetskopiering den eneste måten du kan få gjenopprettet dine filer etter feilaktig sletting eller dataangrep som løspengevirus. Forsikre deg om at familie og venner har automatisk sikkerhetskopiering på plass. Som oftest er den enkleste løsningen sky-basert, disse sikkerhetskopierer filene dine hver time eller når du endrer en fil. Disse løsningene gjør det ikke bare enkelt å sikkerhetskopiere filer, men også å gjenopprette dem.

*Hjelp andre med å få det meste ut av teknologien ved å dele disse fem enkle stegene med dem.*

## Sikre barna på besøk hos andre

Om du er komfortabel med teknologi har du sannsynligvis ikke bare sikret deg selv, men har også hjulpet barna dine med å sikre seg. Men når barna besøker slektninger som ikke er like komfortable med teknologi, som besteforeldre, kan det være at disse slektningene ikke er like bevisste på hvordan de skal sikre barna på nettet, eller dine forventninger til dette. Her er noen grep du kan ta for å hjelpe med å beskytte barn når de besøker andre, spesielt familie.

- **Regler**. Sørg for at andre kjenner til eventuelle regler eller forventninger du har til barnas sikkerhet. Er det for eksempel regler for hvor lenge barna kan være på nett, hvem de kan snakke med, og hvilke spill de kan eller ikke kan

## Å hjelpe andre med å sikre seg selv

spille? Stol på oss når vi sier at du ikke kan stole på at barna vil fortelle om slike regler til andre familiemedlemmer. En idé er å lage et «regelark» som du kan dele ut til familiemedlemmer barna besøker ofte.

- **Kontroll**: Om barn forstår teknologi bedre enn de som har ansvar for dem, kan de komme til å utnytte dette. For eksempel kan barn be om eller tilegne seg administrator-rettigheter på besteforeldres datamaskiner, for så å gjøre hva de vil, som å installere det ene spillet du kanskje ikke vil at de skal spille. Sørg for at familiemedlemmene vet at de ikke skal gi barna flere rettigheter enn det de har i utgangspunktet.

Til slutt, foreslå for folk at de abonnerer på opplæringsresurser som OUCH!-nyhetsbrevet, slik at de kan fortsette å lære på egenhånd. Dette nyhetsbrevet utgis gratis hver måned i over 20 språk. Registrer deg som mottaker på https://securingthehuman.sans.org/ouch.

## Lær mer

Abonner på det månedlige OUCH!-nyhetsbrevet om sikkerhetsbevissthet, se gjennom OUCH!-arkiver, og lær mer om SANS sine løsninger for sikkerhetsbevissthet ved å gå inn på securingthehuman.sans.org/ouch/archives.

## Norsk Versjon

NorSIS arbeider for at alle skal kunne bruke internett og IKT trygt på jobb og privat. Vi er både samarbeidspartner og pådriver overfor myndigheter og bedrifter. NorSIS er et uavhengig organ som ønsker å gjøre informasjonssikkerhet til en naturlig del av hverdagen.

## Ressurser

| | |
|---|---|
| Sosial manipulering: | https://securingthehuman.sans.org/ouch/2017#january2017 |
| Passordsetninger: | https://securingthehuman.sans.org/ouch/2017#april2017 |
| Passordhvelv: | https://securingthehuman.sans.org/ouch/2017#september2017 |
| To-trinns pålogging: | https://securingthehuman.sans.org/ouch/2015#september2015 |
| Sikkerhetskopiering og gjenoppretting: | https://securingthehuman.sans.org/ouch/2017#august2017 |
| Barnas trygghet på nett: | https://securingthehuman.sans.org/ouch/2017#may2017 |



Redaksjon: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Oversatt av: NorSIS