SANS SECURITY AWARENESS
NorSIS Norsk senter for informasjonssikring
OUCH! | Desember 2017
Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- Passord er ikke lenger nok
- Hva er to-trinns autentisering?
- Hvordan det fungerer

Lås din innlogging

Oversikt

Gjesteredaktør
Tiffany Schoenike er direktør for kampanjer og initiativer ved National Cyber Security Alliance (**@staysafeonline**). I 2016 jobbet hun med det hvite hus og USAs regjering og industri for å utvikle «STOP. THINK. CONNECT.™» kampanjen «Lock Down Your Login» om to-trinns autentisering.

Autentisering, eller det å bevise hvem du er, er et nøkkelbegrep når det kommer til å beskytte informasjon du har i form av e-post, sosiale medier, nettbank, og annet. Du tenker nok ikke over det, men det er tre forskjellige måter å bevise hvem man er på: Med noe du vet – som et passord, med noe du har – som førerkortet ditt, og med noe du er – som fingeravtrykket ditt. Hver og en av disse kommer med fordeler og ulemper. Den vanligste autentiseringsmetoden er med passord – noe du vet. Dessverre viser det seg i stadig større grad at passord alene ikke er sikkert nok. I dette nyhetsbrevet lærer vi deg å låse innloggingen din med noe langt bedre enn kun passord: To-trinns autentisering.

Passord er ikke lenger nok

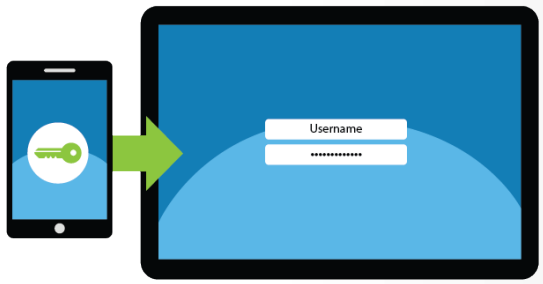
Passord beviser hvem du er basert på noe du vet. Men om noen klarer å gjette eller få tilgang til passordet ditt, kan de utgi seg for å være deg og skaffe seg tilgang til din fortrolige informasjon. Passord på avveie har blitt en av de fremste årsakene til at brukerkontoer blir hacket. Derfor blir du fortalt at du skal bruke passordsetninger som er vanskelige for andre å gjette, forskjellige passord for hver brukerkonto, og å aldri dele passord med andre. Selv om disse rådene fortsatt er gjeldende, er ikke lenger passord like effektive. Heldigvis er det en rask og enkel måte for å få deg i kontroll og sikre informasjonen din, som kalles to-trinns autentisering.

Hva er to-trinns autentisering?

To-trinns autentisering (også kalt to-faktor autentisering, multifaktor autentisering og 2FA) er langt sterkere enn å benytte

Lås din innlogging

kun passord. Den krever ikke én, men to forskjellige autentiseringsmåter for å bevise hvem du er. Et godt eksempel er bankkortet ditt. Når du skal ta ut penger fra en minibank, bruker du faktisk to-trinns autentisering. For å få tilgang til kontantene dine trenger du t ting: Bankkortet ditt (noe du har) og PIN-koden din (noe du vet). Dersom bankkortet ditt blir borte eller blir stjålet kan ikke andre ta ut penger fra deg, uten å også kjenne til PIN-koden din. En tyv må ha både bankkortet og PIN-koden for å kunne ta ut penger. To-trinns autentisering benytter seg av det samme prinsippet.



Lås din innlogging ved å bruke to-trinns autentisering når det er tilgjengelig, det er en av de viktigste tiltakene du kan gjøre for å beskytte deg selv på nettet.

Hvordan det fungerer

To-trinns autentisering er tilgjengelig på alle norske nettbanker, og det meste av e-post, sosiale medier, og mange andre sider. I tillegg tilbyr de fleste slike sider enkle steg-for-steg-instruksjoner som forklarer hvordan du aktiverer to-trinns autentisering. Når du har aktivert to-trinns autentisering kan du utvide det til å fungere slik: Først logger du deg inn på brukerkontoen med brukernavn og passord slik du pleier. Dette er den første av de to trinnene – noe du vet. Så vil du motta en unik kode, ofte i form av SMS til mobilen din. Du skriver så inn koden, dette er det andre av de to trinnene – du må ha telefonen din for å kunne motta koden. Nå er kontoen din virkelig godt låst. Selv om passordet ditt skulle bli stjålet av cyberkriminelle, vil de ikke kunne få tilgang til brukerkontoen din med mindre de også har mobiltelefonen din.

Istedenfor å motta den unike koden som tekstmelding kan du installere en spesiell autentiseringsapp på mobilen din. Denne appen genererer en unik kode for deg hver gang du trenger den for å logge inn. Fordelen med en slik app, er at den faktisk er enda sikrere enn tekstmelding, fordi koden blir generert på mobilen din istedenfor å bli sendt til den. I tillegg er det mer praktisk fordi du ikke trenger å være tilkoblet en teleoperatør for å få en kode. Appen genererer konstant nye koder som kan brukes for innlogging til dine brukerkontoer.

Lås din innlogging

Selv om to-trinns autentisering kanskje virker som det er mer tungvint i starten, vil informasjonen din være betydelig mer trygg. Ikke vent til du blir hacket, lås innloggingene dine nå ved å aktivere to-trinns autentisering på nøkkelkontoer som e-post, nettbank, og sosiale medier, og nyt sinnsroen det gir å vite at du er langt sikrere.

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

Passordsetninger:	https://securingthehuman.sans.org/ouch/2017#april2017
Oversikt over nettsteder med to-trinns autentisering:	https://twofactorauth.org
Stop|Think|Connect:	https://www.lockdownyourlogin.org
To-trinns autentisering på Google:	http://www.google.com/landing/2step/

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