OUCH! | Juli 2015

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

Sosiale Medier

Oversikt

Sosiale medier som Facebook, Twitter, Instagram og LinkedIn er fantastiske ressurser, som lar deg møte, samhandle og dele med mennesker over hele verden. Men med alle disse mulighetene kommer det også risikoer, ikke bare for deg men også din familie, venner og arbeidsgiver. I dette nyhetsbrevet vil vi forklare hva disse farene er og hvordan bruke disse mediene sikkert og trygt.

Gjesteredaktør

Tanya Baccam er en mangeårig sikkerhetskonsulent. Hun har vært SANS forfatter og instruktør for over et tiår, blant annet i SEC502, SEC542, SEC401, MGT414, AUD507 og mange andre kurs. Følg henne på Twitter på **@tbaccam**.

Personvern

En vanlig bekymring med sosiale medier er beskyttelsen av din personlig informasjon. Potensielle farer inkluderer:

- **Påvirker din fremtid**: Noen virksomheter søker gjennom sosiale medier som en del av bakgrunnssjekker. Flaue eller avslørende bilder eller innlegg, uansett hvor gamle, kan forhindre deg fra å bli ansatt eller forfremmet. I tillegg gjør mange universitet lignede sjekker for nye studentsøknader. Personvernsinnstillinger kan ikke beskytte deg når disse virksomhetene spør deg om å «Like» eller bli med på deres sider eller visse innlegg kan bli arkivert på flere nettsider.
- **Angrep mot deg**: Cyberangripere kan analysere dine innlegg og bruke disse for å skaffe seg tilgang til din eller din virksomhets informasjon. For eksempel, de kan bruke informasjonen du deler til å gjette seg frem til svaret på sikkerhetsspørsmålet ditt til å tilbakestille dine passord på nettet, lage målrettede e-postangrep (såkalt «spearphishing»), eller ringe noen i din virksomhet og utgi seg for å være deg. I tillegg kan disse angrepene smitte over til den fysiske verdenen, som for eksempel å identifisere hvor du jobber eller bor.
- **Skade arbeidsgiver ved et uhell**: Kriminelle eller konkurrenter kan bruke enhver sensitiv informasjon du legger ut om din virksomhet mot din arbeidsgiver. I tillegg kan dine innlegg potensielt skape et omdømmetap for virksomheten din. Sørg for å sjekke din virksomhets prosedyrer før du legger ut noe om jobben din, i tillegg så kan noen av dine innlegg på sosiale medier bli monitorert.

Den beste beskyttelsen er å begrense hva du legger ut. Ja, personvernsinnstillinger kan gi noe beskyttelse, men de er ofte forvirrende og endres hyppig uten din viten. Hva du trodde var privat kan kjapt bli offentlig av forskjellige

Sosiale Medier

grunner. I tillegg, vernet rundt dine innlegg er bare så sikker som de menneskene du deler det med. Jo flere venner eller kontakter du deler med, jo mer sannsynlig vil denne informasjonen bli offentlig. Du burde anta at alt du legger ut kan eller vil bli offentlig og en permanent del av Internettet.

Og til slutt, vær bevisst over hva dine venner legger ut om deg. Hvis de legger ut noe som du ikke er komfortabel med, be dem å fjerne det. Hvis de nekter eller ignorerer deg, ta kontakt med det aktuelle sosiale mediet og be dem om å fjerne innholdet om deg. Samtidig, være respektfull med hva du legger ut om andre.



Sosiale medier er morsomme og kraftfulle, men vær forsiktig med hva du deler og med hvem.

Sikkerhet

I tillegg til personvernsutfordringer, her er noen steg for å beskytte kontoene dine på sosiale medier og aktiviteten på nettet.

- **Pålogging**: Beskytt hver av dine kontoer med et sterkt, unikt passord og ikke del dem men noen andre. I tillegg, mange sosiale medier støtter sterkere autentisering, som to-stegs verifisering. Alltid aktiver disse sterkere autentiseringsløsningene når det er mulig. Og til slutt, ikke bruk din konto på sosiale medier til å logge deg på andre sider, hvis denne blir hacket så vil alle de andre kontoene bli sårbare.
- **Personvernsinnstillinger**: Hvis du bruker personvernsinnstillingene, sørg for å gå gjennom dem jevnlig. Sosiale medier endrer ofte personvernsinnstillingene og det er fort gjort å gjøre en feil. Det er også mange apper og tjenester lar deg «tagge» din plassering med innholdet du legger ut (såkalt «geotagging»). Jevnlige sjekk disse innstillingene hvis du ønsker å holde din plassering privat.
- **Kryptering**: Sosiale medier bruker kryptering kalt HTTPS til å sikre dine koblinger på nettet til deres side. Noen sider som Twitter og Google+ setter på dette som standard, mens andre krever at du manuelt setter på HTTPS. Sjekk din sosiale mediers kontoinnstillinger og sett på HTTPS som standard tilkobling hvis det er mulig.
- **E-post**: Vær skeptisk over e-poster som hevder å komme fra sosiale medier, da disse kan enkelt være forfalsket sendt fra cyberkriminelle. Den tryggeste måten å svare på en slik beskjed er å logge deg inn på det sosiale mediet direkte, muligens fra ett lagret bokmerke, og så lese og svare på meldinger eller varsler fra nettsiden.
- **Ondsinnede linker/svindel**: Vær varsom med mistenkelige lenker eller potensielle svindel lagt ut på sosiale medier. Skurkene bruker sosiale medier til å spre sine egne angrep. Bare fordi en melding blir lagt ut

Sosiale Medier

av en venn så må det ikke bety at meldingen faktisk er fra dem, deres konto kan ha blitt kompromittert. Hvis et familiemedlem eller en venn har lagt ut en rar melding du ikke kan få bekreftet (for eksempel at de har blitt ranet og du må sende dem penger), ring dem på mobiltelefonen eller benytt andre midler for å bekrefte at meldingen virkelig er fra dem.

- **Mobilapper**: De fleste sosiale medier tilbyr mobilapper for gi tilgang til dine kontoer på nettet. Sørg for å laste ned disse mobilappene fra pålitelige nettsider og at din mobiltelefon er beskyttet med et sterkt passord. Hvis din mobiltelefon er ulåst når du mister den, så kan hvilken som helst få tilgang til dine sosiale medier via mobiltelefonen og begynne å legge ut innlegg som deg.

Sosiale medier er en fantastisk måte å kommunisere og holde kontakten med verden. Hvis du følger rådene beskrevet her, bør du være i stand til å nyte en mye tryggere opplevelse på nettet. For å lære mer om hvordan du kan bruke sosiale medier sikkert eller rapportere om uautorisert aktivitet, sjekk ut ditt sosiale mediet sine sikkerhetssider.

Les Mer

Abonner på månedlig OUCH! nyhetsbrev om sikkerhetsbevissthet, se gjennom OUCH! arkivene og lær mer om SANS sine programmer for sikkerhetsbevissthet hos http://www.securingthehuman.org.

Norsk Versjon

NorSIS er en del av regjeringens helhetlig satsing på informasjonssikkerhet i Norge. NorSIS jobber for at informasjonssikkerhet skal bli en naturlig del av hverdagen. Les mer på www.norsis.no.

Ressurser

Passordsetninger:	http://www.securingthehuman.org/ouch/2015#april2015
To-steg verifisering:	http://www.securingthehuman.org/ouch/2013#august2013
Sikker bruk av mobilapplikasjoner:	http://www.securingthehuman.org/ouch/2015#january2015
Opplære barn i cybersikkerhet:	http://www.securingthehuman.org/ouch/2015#june2015
Facebook sikkerhet:	https://www.facebook.com/safety

Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis