Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- **Hva er direktørsvindel?**
- **Hvordan beskytte seg?**

Direktørsvindel

Hva er direktørsvindel?

Cyberkriminelle er luringer – de finner konstant på nye metoder for å oppnå det de ønsker. En av de mest effektive metodene deres er å rette seg direkte mot folk som deg. Cyberkriminelle har lært seg at ubevisste folk er det svakeste leddet i enhver organisasjon, men de har glemt at kunnskapsrike folk som OUCH!-lesere kan være organisasjonens beste forsvar.

Gjesteredaktør

Angela Pappas er direktør for informasjonssikkerhetstrening og bevisstgjøring ved Thomson Reuters. I denne rollen er Angela ansvarlig for ambassadørprogrammet, e-læring, og opplæring av ansatte om phishing.

Cyberkriminelle har utviklet en ny angrepsmetode kjent som direktørsvindel, eller CEO fraud og noen ganger også Business Email Compromise (BEC) på engelsk. I slike angrep gir en kriminell seg ut for å være en direktør eller en annen leder i din organisasjon. De kriminelle sender en e-post til ansatte som deg selv, i et forsøk på å få deg til å gjøre noe du ikke burde gjøre. Slike angrep er ekstremt effektive nettopp fordi de kriminelle gjør godt forarbeid. Blant annet ser de gjennom nettsiden til organisasjonen for å finne ut hvor dere holder til, hvem som er ledere, og hvilke andre organisasjoner dere samarbeider med. Så bruker de kriminelle sider som LinkedIn, Facebook og Twitter for å finne ut alt de kan om kollegene dine. Når de har gjort seg kjent med strukturen i organisasjonen, velger de seg ut spesifikke ansatte som mål. De velger ut disse målene ut ifra hva de ønsker å oppnå. Om de ønsker penger, velger de seg ut noen i regnskap eller økonomi. Ønsker de skatteinformasjon, velger de seg ut noen i HR. Om de ønsker tilgang til databasen, velger de noen i IT.

Når de har bestemt seg for hva de vil ha, og hvem de vil bruke som mål, begynner de å konstruere angrepet. Som oftest bruker de spear phishing. Phishing vil si at en angriper sender en e-post til millioner av mottakere med det formål å lure dem til å gjøre noe, for eksempel åpne et infisert vedlegg eller besøke et farlig nettsted. Spear phishing ligner phishing, men istedenfor å sende en generisk e-post til millioner av mottakere, sender de en spesiallaget e-post til et lite, bestemt antall mottakere. Disse e-postene fremstår som helt realistiske, og er vanskelige å oppdage. Ofte virker det som om de kommer fra noen du kjenner og jobber med, som en kollega, eller kanskje til og med sjefen. E-postene fremstår som realistiske kanskje

Direktørsvindel

fordi de bruker den samme sjargongen som kollegene dine, eller fordi de bruker firmaets logo eller den offisielle signaturen til en leder. Ofte skaper disse e-postene en sterk følelse av hast, det kreves at du handler umiddelbart og ikke snakker med noen. De kriminelle vil at du skal forhaste deg og gjøre en feil. Her er tre vanlige scenarier:

Direktørsvindel er et farlig angrep som kan omgå de fleste sikkerhetsrutiner. Til syvende og sist er du vårt beste forsvar.

Bankoverføring: En cyberkriminell er ute etter penger. I slike tilfeller vil de undersøke hvem som jobber i regnskap, finans, eller eventuelle andre som håndterer organisasjonens økonomi. Deretter vil de kriminelle konstruere og sende en e-post der de utgir seg for å være sjefen; i e-posten forteller de at det er en nødssituasjon, og at pengene må overføres til en hvis konto omgående.

Skattesvindel: Cyberkriminelle vil stjele informasjon om kollegene dine for å utgi seg for å være dem, og begå skattesvindel. De undersøker organisasjonen for å finne ut hvem som håndterer personlig informasjon om ansatte, for eksempel noen i administrasjon eller HR. Deretter sender de kriminelle falske e-poster der de utgir seg for å være høytstående ledere eller muligens noen fra juridisk avdeling, og krever å få tilsendt visse dokumenter øyeblikkelig.

Falsk advokat: Ikke alle tilfeller av direktørsvindel involverer kun e-post, andre metoder som telefon kan også brukes. Et slikt scenario starter gjerne med at kriminelle sender deg en e-post der de utgir seg for å være en leder, og gjør deg oppmerksom på at en advokat snart vil ringe inn om en viktig sak. Så blir du oppringt av den kriminelle, som nå utgir seg for å være advokaten. Den kriminelle skaper et sterk følelse dårlig tid ved å snakke om konfidensielle saker som haster. Følelsen av hastverk lurer deg til å handle med en gang.

Hvordan beskytte seg?

Så hva kan du gjøre for å beskytte virksomheten og deg selv? Sunn fornuft er ditt beste forsvar. Om du mottar en beskjed fra sjefen eller en kollega som ikke høres eller føles riktig, kan det være et angrepsforsøk. Noen tegn å se etter kan være blant annet at det skapes et sterkt inntrykk av dårlig tid, at en signatur ikke virker riktig, at det brukes en tone du ikke ville forventet, eller at det er brukt et annet navn i e-posten enn det navnet vedkommende vanligvis bruker for deg. I noen tilfeller

Direktørsvindel

kan det også være at angriperen bruker en e-postadresse eller et telefonnummer som du aldri har sett før, eller kanskje de bruker en e-postadresse som er veldig lik den til en kollega eller sjef, men ikke helt lik. Om du er i tvil, ring vedkommende på et telefonnummer du stoler på, eller møt dem ansikt til ansikt (ikke svar via e-post), og bekreft at de sendte e-posten. Omgå aldri sikkerhetspolicyer og sikkerhetsrutiner. Organisasjonen din har godt mulig policyer som definerer korrekt prosedyre for å godkjenne overføring av penger eller deling av konfidensiell informasjon. Forespørsler som forsøker å omgå disse policyene, uansett hva som tilsynelatende er kilden, burde ses på som mistenkelige, og må verifiseres før man foretar seg noe. Om du mottar en slik forespørsel og er usikker på hva du skal gjøre, kontakt en overordnet, help-desken, eller informasjonssikkerhets-teamet med en gang.

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/2014#november2014
Phishing:	https://securingthehuman.sans.org//ouch/2015#december2015
Hva er skadevare:	https://securingthehuman.sans.org/ouch/2016#march2016
Totrinns pålogging:	https://securingthehuman.sans.org/ouch/2015#september2015
Dagens tips:	https://www.sans.org/tip-of-the-day

OUCH! utgis av SANS Securing The Human, og er distribuert under Creative Commons BY-NC-BD 4.0 lisensen. Du står fritt til å distribuere dette nyhetsbrevet, eller bruke det i ditt eget bevissthetsprogram, så lenge du ikke gjør endringer på nyhetsbrevet. For oversettelser og mer informasjon, ta kontakt med oss på ouch@securingthehuman.org.

Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Oversatt av: NorSIS

securingthehuman.sans.org/blog /securethehuman @securethehuman securingthehuman.sans.org/gplus