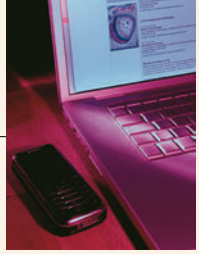

Svindelforsøk mot bedrifter og organisasjoner

Det har over tid vært flere svindelforsøk hvor NTFs ansatte og lokalforeninger er blitt bedt om å betale en faktura eller overføre penger til en konto i utlandet. Vi oppfordrer alle om å være ekstra oppmerksomme på slike henvendelser. Det er viktig at lokalforeningene har rutiner for utbetaling slik at man sikrer seg mot slike svindelforsøk.

Denne artikkelen bygger på informasjon som kan finnes på nettsiden Nettvett.no, der finner du også mer detaljert informasjon og flere tips om hva du kan gjøre for å sikre deg. På Nettvett.no finner du også informasjon og hjelp om blant annet bruk av e-post, chat og sosiale medier, spam, virus, deling av filer på internett, nettbank, og beskyttelse mot angrep utenfra.

Direktørsvindel

Direktørsvindel, eller CEO-fraud kan defineres som svindel utført ved hjelp av e-post eller SMS fra personer som utgir seg for å være i ledelsen i bedriften.

Målet med direktørsvindel er å lure en økonomimedarbeider til å betale en faktura eller overføre penger til en konto, vanligvis i utlandet. Svindlere bruker litt ulike fremgangsmåter. Svindleren spiller på at ofrene er travle og at overføringen/betalingen av penger må skje raskt.

Svindlerne blir stadig grundigere i sine forberedelser. Navn på nøkkelpersoner i bedriften blir identifisert. I tillegg blir det etablert domene med bedriftens navn for å kunne opprette epostadresser som ligner på de bedriften faktisk har.

Svindleren sender en e-post eller SMS som tilsynelatende kommer fra en

Direktørsvindel? OBS! OBS!

- Er det en e-post eller SMS hvor du blir bedt om å overføre penger uten videre dialog og at dette haster, kan dette være et svindelforsøk
- Les e-posten nøye og se etter unormale elementer. Dette kan eksempelvis være manipulert fra-felt og svar-felt, bruk av .com i stedet for .no.
- Formuleres e-posten med en fremtoning i retning av tillitt, trussel eller fristelser så er dette kjente tegn på svindelforsøk
- Se godt på og kontroller betalingsinformasjon og/eller faktura mot tidligere transaksjoner

Råd til virksomheter

- Les alltid e-post hvor det anmodes om overføring av penger to ganger
- Ledelsen bør informere sine økonomimedarbeidere på forhånd hvis de vet at det kan være aktuelt med raske pengeoverføringer i tiden som kommer
- Hvis du som økonomimedarbeider mottar e-post fra sjefen om å overføre penger, så send sjefen en SMS hvor du ber om at overføringen bekreftes

direktør i selskapet til en økonomimedarbeider. «Direktøren» ber om en større overføring til et gitt kontonummer, eller varsler om at en slik overføring er nødvendig i påvente av videre kommunikasjon. Det kan også bli vedlagt en falsk faktura ved e-posten. Hvis økonomimedarbeideren svarer på henvendelsen, blir svaret sendt til svindlerens epostadresse og ikke til direktørens epostadresse som står i avsenderfeltet. E-postene er dyktig formulert på norsk, og signert slik «direktøren» vanligvis gjør.

Svindlerne baserer disse bedrageriene på at den ansatte vil være behjelpelig og metoden kan blant annet være å gi den ansatte et inntrykk av at han eller hun er med på noe som er viktig for bedriften. Noen ganger kan direktørens navn være nok til å oppnå denne følelsen, mens andre ganger vil «direktøren» love belønning i form av bonus eller forfremmelse. Det har også vært tilfeller der «direktøren» kan ty til trusler om den ansatte ikke følger instruksjoner.

I mange tilfeller er det derimot tidspress og stress svindlerne baserer angrepet sitt på. Svindlerne kan derfor sende en e-post sent fredag ettermiddag hvor leder ber om at en faktura må betales umiddelbart. Lederen vil i tillegg være utilgjengelig på telefon på grunn en konferanse eller flyreise.

Denne typen svindel er et økende problem i Norge og rammer også organisasjoner som NTF. Det er viktig at NTFs medlemmer og lokalforeninger har rutiner for å sjekke slike krav om hasteutbetalinger.

Du kan lese mer om direktørsvindel på Nettvett.no.

E-postsvindel med løsepengevirus

Svindelkampanjer der det sendes ut mengder med falske e-poster eller SMSer blir stadig mer vanlig. I mange tilfeller har disse som formål å spre løsepengevirus (også kjent som "ransomware»). Løsepengevirus krypterer filene på offerets datamaskin, og krever løsepenger for å dekryptere dem.

Vi anbefaler ingen å betale løsepengene dersom de blir rammet av løsepengevirus. Det vil nemlig bidra til å gjøre bruk av løsepengevirus enda mer lukrativt for cyberkriminelle, og den negative trenden vil dermed fortsette.

Du kan lese mer om løsepengevirus på Nettvett.no.

Phishing og falske innloggingsider

Phishing, ofte kalt nettfiske på norsk, er det å lure til seg sensitiv informasjon, som passord eller bankkortinformasjon, over internett. I mange tilfeller gjøres det ved at cyberkriminelle forsøker å lure ofre inn på falske innloggingssider.

Dette er nettsider som er satt opp av cyberkriminelle, som ser ut som de ekte innloggingssidene til f.eks. Facebook, LinkedIn, nettbanken din eller e-postleverandøren din. Om man prøver å logge seg inn på disse sidene, vil imidlertid brukernavn og passord havne hos de kriminelle.

Falske innloggingsider kan ofte avsløres på URL-lenken, vær obs på at lenken du ser i en e-post eller i en SMS ikke nødvendigvis er den du faktisk havner på. I dette eksempelet er den øverste lenken ekte, gjenkjennbar ved at domenet er dnb.no, mens på lenken under er domenet egentlig det fiktive domenet eeseewebhost.net.

Lenker til disse falske sidene får man gjerne i en SMS eller e-post som utgir

For å unngå løsepengevirus

- Hold datamaskinens operativsystem og programvare oppdatert.
- Bruk antivirusprogram og hold det oppdatert.
- Ta sikkerhetskopi jevnlig av de filene som er viktig å ta vare på.
- Vær oppmerksom på at løsepengevirus også kan spre seg til disker og andre enheter som er tilkoblet datamaskinen.

Hvis uhellet er ute

- Det finnes ulike typer løsepengevirus; for øyeblikket finnes det ikke løsninger for alle typer. Forsøk å finne ut hvilken variant av løsepengevirus som har infisert datamaskinen og om det finnes kjente metoder for å fjerne det.

Forholdsregler mot phising

- Send aldri personlig eller finansiell informasjon via e-post
- Sjekk hvor lenken tar deg. Ved å holde musepekeren over lenken kommer webadressen opp.
- Sjekk om adressen er feilstavet eller slutter på .com istedenfor .no, etc.
- Prøv å ikke klikke på lenker i e-post, men kopier heller adressen manuelt. Dersom linken viser til en nettside, skriv adressen heller direkte inn i nettleseren.
- Vurder avsender og nettsider nøye, før du oppgir informasjon
- Forsikre deg om at nettbanker o.l. krypterer sidene (se etter: https:// og hengelåsen)
- Hold operativsystem og programmer oppdatert.
- Benytt oppdatert antivirus.

Hvis du rammes

- Dersom du tror noen kan ha fått tilgang til kontoen eller kredittkortene dine må du umiddelbart kontakte bank eller utsteder. Sjekk også kontoutskrifter og kredittkortregninger for mistenkelige belastninger.

seg for å være fra en pålitelig avsender. Om den falske siden er innlogging for nettbanken din, kommer lenken for eksempel i en SMS som ser ut til å være fra banken din, der det bes om at du følger lenken, logger inn, og bekrefter litt informasjon.

Beskyttelse i årvåkne ansatte og gode rutiner

Årvåkne ansatte i virksomheter og årvåkne tillitsvalgte med økonomiansvar i organisasjoner som NTF er den beste beskyttelsen mot former for forsøk på økonomisk svindel som er nevnt her. Gjør gjerne dette til et tema på neste møte med ansatte eller i lokalforeningen.

Gode rutiner for utbetalinger, og hva som skal gjelde av eventuelle unntak fra rutinene er også viktig – og ikke minst at rutinene følges.

Dag Kielland Nilsen
Advokat i NTF