CYBERSIKKERHET FOR
SMÅ VIRKSOMHETER

NorSIS

PHISHING / FALSKE E-POSTER

Du mottar en e-post som ser ut som om den er fra noen du kjenner.

Den ser ut til å være fra en av bedriftens leverandører, og den ber deg om å klikke på en lenke for å oppdatere bedriftskontoen din. Burde du trykke på den? Kanskje den ser ut til å være fra sjefen din, og spør etter nettverkspassordet? Bør du svare? I begge tilfeller – sannsynligvis ikke. Dette kan være phishing-forsøk.

HVORDAN PHISHING FUNGERER

Du mottar en e-post eller SMS

Den ser ut til å være fra noen du kjenner, og den ber deg trykke på en lenke, eller gi fra deg passordet, bankinformasjon, eller annen sensitive informasjon.

nettvett.no/er-lenken-trygg/

Den ser ekte ut

Det er enkelt å forfalske logoer og lage falske e-postadresser. Svindlere bruker kjente bedriftsnavn og later som om de er noen du kjenner.

nettvett.no/falske-e-poster/

Det haster

Meldingen presser deg til å handle raskt – ellers vil det få alvorlige konsekvenser.

Hva skjer videre

Dersom du klikker på en lenke, kan svindlerne installere skadevare eller annen programvare som kan låse deg ut fra datamaskinen, og spre seg til resten av nettverket. Hvis du bruker samme passord, har svindlerne nå tilgang til alle disse kontoene.

nettvett.no/virus/

HVA DU KAN GJØRE

Før du klikker på en lenke eller deler noe av din sensitive informasjon:

Søk den opp

Søk opp nettsiden eller telefonnummeret til bedriften eller personen som står bak meldingen/e-posten. Vær sikker på at det er den faktiske virksomheten, og at du ikke er i gang med å laste ned skadevare eller snakker med en svindler.

Snakk med noen

Å snakke med en kollega kan hjelpe deg å finne ut om forespørselen er ekte eller om det er et phishing-forsøk.

Ring noen om du er usikker

Ta opp telefonen og ring den relevante leverandøren, kollegaen eller klienten som har sendt e-posten. Få bekreftet at det virkelig er vedkommende som har sendt deg forespørselen. Bruk kontaktinformasjon du vet stemmer, ikke den du fikk oppgitt i e-posten.

nettvett.no/id-tyveri/

CYBERSIKKERHET FOR
SMÅ VIRKSOMHETER

NorSIS

HVORDAN BESKYTTE VIRKSOMHETEN

Sikkerhetskopier filene dine

Sikkerhetskopier filene dine jevnlig, og pass på at sikkerhetskopiene oppbevares et annet sted. På den måten, kan du gjenopprette informasjonen din selv om hackere har fått tilgang til maskinen og nettverket ditt. Gjør sikkerhetskopiering til en del av din faste rutine.

nettvett.no/sikkerhetskopiering/

Hold sikkerheten oppdatert

Alltid installer de nyeste oppdateringene. På mobile enheter, kan det hende at du må oppdatere manuelt.

nettvett.no/oppdateringer/

Lær opp dine ansatte

Informer om hvordan de kan unngå phishing-svindel og vis dem noen av de vanligste måtene en angriper kan infisere datamaskiner og andre enheter på. Inkluder dette i virksomhetens faste opplæringsprogram.

nettvett.no/falske-e-poster/

Distribuer et sikkerhetsnett

Bruk tekniske tiltak for å unngå phishing-e-poster i å nå virksomhetens innbokser i utgangspunktet.

nettvett.no/dmarc/

dmarc.no

OM DU BLIR RAMMET AV PHISHING-ANGREP

Varsle andre

Snakk med dine kollegaer og del dine erfaringer. Phishing-angrep rammer ofte mer enn én person i en bedrift.

Begrens skaden

Bytt umiddelbart ut passord som har blitt kompromittert, og koble infiserte enheter fra nettverket.

nettvett.no/2-trinns-bekreftelse/

Følg prosedyre

Har bedriften en beredskapsplan, følg de prosedyrene som er beskrevet for slike hendelser. Dette kan f.eks. inkludere å varsle bestemte funksjoner i organisasjonen (IT og/eller sikkerhet).

Gi beskjed til kundene

Dersom informasjon har kommet på avveie, varsle kunder og leverandører som kan ha blitt berørt – de kan også utsettes for ID-tyveri.

nettvett.no/id-tyveri/

Rapporter

Varsle din egen ledelse. Om virksomheten har en sikkerhetsleverandør, må denne også varsles. Vurder å anmelde hendelsen til politiet. Husk også å varsle den virksomheten som er blitt etterlignet i phishing-forsøket.

NorSIS

E-POST-AUTENTISERING

E-post-autentiseringsteknologi gjør det mye vanskeligere for en svindler å sende falske e-poster som ser ut som om de kommer fra din bedrift.

Denne teknologien tillater en mottakende e-postserver å verifisere at en e-post kommer fra din bedrift, og blokkerer e-poster fra svindlere – eller sender dem til en karantene-mappe, og varsler deg om dem.

HVA DU BØR VITE

Noen IT-leverandører lar deg sette opp din virksomhets e-post med ditt eget domenenavn (som du kan se på som nettsidenavnet ditt). Domenenavnet ditt kan for eksempel se ut som dette: dinbedrift.no, og e-postadressen din kan se ut som dette: navn@dinbedrift.no. Uten e-postautentisering, kan svindlere bruke samme domenenavn for å sende ut e-poster fra andre e-postservere, som ser ut som om de kommer fra din virksomhet. Dersom din e-post bruker bedriftens domenenavn, pass på at IT-leverandøren tilbyr disse tre e-postautentiseringsverktøyene:

Sender Policy Framework (SPF)

Forteller andre servere hvilke servere har tillatelse til å sende e-poster med ditt domenenavn. Om du f.eks. sender en e-post fra navn@dinbedrift.no, kan den mottakende serveren bekrefte at serveren denne e-posten ble sendt fra, er i en godkjent liste. Om den er det, går e-posten gjennom. Hvis den ikke finner en match, blir e-posten flagget som mistenkelig.

Domain Keys Identified Mail (DKIM)

Setter en digital signatur på en utgående e-post, sånn at servere kan bekrefte at en e-post fra ditt domene faktisk ble sendt fra dine servere, og ikke har blitt endret på underveis.

Domain-based Message Authentication, Reporting & Conformance (DMARC)

SPF og DKIM verifiserer adressen serveren bruker. DMARC verifiserer at denne adressen matcher «fra-adressen» du ser i toppen av e-posten. Den lar deg fortelle andre servere hva de skal gjøre om de mottar en e-post som ser ut til å komme fra ditt domene, men som virker mistenkelig (basert på SPF eller DKIM). Du kan la andre servere avvise e-posten, flagge den som spam, eller ikke gjøre noe. Du kan også sette opp DMARC slik at du får et varsel når dette skjer.

nettvett.no/dmarc

dmarc.no

Det krever litt ekspertise å konfigurere disse verktøyene slik at de fungerer som man vil, og ikke blokkerer legitime e-poster. Pass på at din IT-leverandør kan sette dem opp for deg, dersom du ikke selv har denne kompetansen. Dersom de ikke kan tilby dette, bør du vurdere å bruke en annen leverandør.