NorSIS

BRUKERSTØTTESVINDEL

Du mottar en telefonsamtale, pop-up-vindu, eller e-post som forteller deg at det er et problem med datamaskinen din.

Svindlere står ofte bak disse telefonsamtalene, pop-up-vinduene, og e-postene. De bruker gjene falske telefonnummer eller e-postadresser for å få deg til å tro at dette er noen du kan stole på. De vil ha tak i pengene dine, personlig informasjon, eller skaffe tilgang til filene dine. Dette kan påvirke driften og ikke minst anseelsen til virksomheten.

nettvett.no/falske-e-poster/

nettvett.no/phishing/

nettvett.no/smishing-sms-svindel/

HVORDAN SVINDELEN FUNGERER

Svindlerne kan utgi seg for å være fra en kjent bedrift, for eksempel Microsoft, eller en lokal IT-leverandør. De bruker ulike tekniske begreper for å overbevise deg om at du har problemer med datamaskinen din. De kan for eksempel spørre deg om å åpne noen filer, eller scanne maskinen din – og deretter fortelle deg at filene eller resultatet av scannen viser at det er et problem ... til tross for at det **egentlig** ikke er det.

Svindlerne kan deretter:

Spørre deg om å gi dem kontroll til maskinen din – noe som gir dem tilgang til all informasjon lagret på den, samt nettverket den er koblet til.

Installere skadevare som gir dem tilgang til datamaskinen din, og dermed sensitive data som brukernavn og passord.

Forsøke å selge deg programvare eller reparasjonstjenester som er verdiløse eller egentlig gratis.

nettvett.no/microsoft-svindel/

nettvett.no/direktor-svindel/

Forsøke å verve deg til en verdiløs abonnementstjeneste for vedlikehold av datamaskinen din.

Spørre etter kredittkortinformasjon, så de kan fakturere deg for falske tjenester eller tjenester som egentlig er gratis.

Henvise deg til nettsider hvor du må oppgi informasjon knyttet til kredittkort eller bankkonto, eller annen personlig informasjon.

nettvett.no/sosial-manipulering/

nettvett.no/okonomisk-svindel-rettet-bedrifter/

CYBERSIKKERHET FOR
SMÅ VIRKSOMHETER

NorSIS

HVORDAN **BESKYTTE** VIRKSOMHETEN DIN

Dersom noen ringer deg og sier at det er et problem med datamaskinen din, **legg på.** En uventet samtale med en brukerstøtte er svindel – selv om nummeret er lokalt eller ser legitimt ut. Disse svindlerne bruker falsk anrops-ID for å se ut som en lokal bedrift eller en kjent virksomhet.

Om du får en pop-up-melding som sier at du må ringe brukerstøtte, ignorer den. Noen pop-up-meldinger om maskinproblemer kan være legitime, men ikke ring et nummer eller klikk på en lenke som dukker opp i en pop-up-varsel.

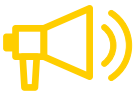
Om du er bekymret for virus eller andre trusler, ring brukerstøtte ved å bruke det kjente telefonnummeret deres, eller det du finner på nettsidene deres. Rådfør deg eventuelt med en kollega.

Aldri gi bort passordet ditt, og ikke gi fjerntilgang til din datamaskin til noen som kontakter deg uventet.

HVA DU BØR GJØRE OM DU BLIR **SVINDLET**

Dersom du har gitt bort passordet ditt, bytt det alle steder du har brukt det. Husk å bruke unike passord for hver konto/tjeneste. Du kan vurdere å bruke et passordhåndteringsprogram.

nettvett.no/passord/



Kvitt deg med skadevare. Oppdater eller last ned legitim sikkerhetsprogramvare. Scan datamaskinen din, og slett alt som programvaren sier er et problem. Om du trenger hjelp, rådfør deg med en IT-kyndig person du har tillit til.

Dersom den utsatte datamaskinen er koblet til nettverket, må du varsle IT-ansvarlig.

Om du har kjøpt tulletjenester, kontakt bank- eller kredittkortselskap for å få annullert transaksjonene. Sjekk kontoutskriften din for kostnader du ikke har godkjent. Sjekk kontoutskriftene jevnlig for å unngå at svindleren ikke trekker deg for penger månedlig.