LÆR AT SPOTTE PHISHING

GUIDE TIL AT SPOTTE OG UNDGÅ PHISHING-ANGREB

www.ntd.dk

ntd.
EN IT PARTNER - TIL DET HELE

HVAD ER PHISHING?

Begrebet "phishing" bruges om den type it-kriminalitet, hvor hackere prøver at lokke dig til at udlevere fortrolige oplysninger fx via e-mail, sms eller telefonopkald.

Målet med phishing er at stjæle penge eller oplysninger fra dig fx ved at lokke dig til at trykke på et link til en hjemmeside, som ser autentisk ud. Her vil du blive bedt om at indtaste dine oplysninger, som efterfølgende vil blive sendt direkte til hackeren, som kan misbruge dem.

En anden måde at stjæle penge er at sprede skadelige vira, der låser dine filer, hvorefter en løsesum afkræves (ransomware).

KENDETEGN VED PHISHING

Der er ofte flere kendetegn i en phishing-mail eller sms, som gør det muligt for dig at spotte svindel. Her er en liste af ting, du skal være opmærksom på, hvis du har mistanke om en phishing-mail:

Afsender
En phishing-mail vil ofte ligne en officiel mail fra en person, en myndighed eller tjeneste, som du allerede har tillid til. Dette kan fx være din bank, SKAT, andre betalingsløsninger som PayPal, anden konto på et socialt medie eller en online butik, men kan også være fra en ukendt afsender.

Modtager
I princippet kan alle med en mailadresse eller mobiltelefon blive udsat for phishing. Virksomheder har i dag begge dele – det er derfor vigtigt – at du som virksomhedsejer altid er opmærksom på svindel.

KENDETEGN VED PHISHING

Der er ofte flere kendetegn i en phishing-mail eller sms, som gør det muligt for dig at spotte svindel. Her er en liste af ting, du skal være opmærksom på, hvis du har mistanke om en phishing-mail:

- **Udformning af mail, SMS, website**
  Phishing kan også gennemskues ved udseendet og formidlingen af sproget. Her skal du blandt andet være opmærksom på:
  - Fejl i dit navn
  - Stavefejl
  - Dårligt dansk
  - Manglende store bogstaver
  - Manglende anvendelse af æ, ø og å
  - Dårlig grafik

- **Formålet**
  Der er mange muligheder for phishing, og ofte kan indholdet virke truende fx ved at sætte en tidsfrist for betaling.
  I en phishing-mail vil du næsten altid blive bedt om at oplyse fortrolige oplysninger som cpr-nummer, kontonummer, kortnummer eller adgangskoder til fx NemID. Du kan fx få besked, at:
  - Aktivere din konto ved at trykke på et link
  - Oplyse din adgangskode eller uploade et billede af dit NemID, så din konto ikke bliver spærret
  - Der er et problem med din konto
  - Du har vundet en præmie
  - Du skal validere login- eller kreditkort-oplysninger

TIPS TIL AT UNDGÅ PHISHING-ANGREB

- Sæt dig grundigt ind i, hvordan du spotter fake mails, SMS'er og websites
- Spørg dig selv: Bør jeg modtage denne mail?
  - Vær især skeptisk overfor mails, der opkræver personlige- eller fortrolige oplysninger.
- Hav styr på, hvordan din bank eller andre myndigheder normalt kommunikerer med dig.
- Besvar eller åben ikke mails, som du ikke har tillid til – gør du dette, viser det afsenderen, at du er aktiv, og du vil modtage flere.
- Tryg aldrig på links i mistænkelige mails.
- Brug stærke og forskellige adgangskoder.
- Træn dine kollegaer og medarbejdere i at spotte phishing-mails.

www.ntd.dk

ntd.
EN IT PARTNER - TIL DET HELE

VIL DU VIDE MERE ELLER HAVE HJÆLP?

– Tal med os om din virksomheds IT-sikkerhed

Book et møde med os og lad os hjælpe med at sikre dig og din virksomhed INDEN, du får snavs ind i maskineriet. Ring til os på +45 5474 7575 eller send en mail til info@ntd.dk

NTD ApS
Dybendalsvænget 3 / 2630 Taastrup / +45 5474 7575
info@ntd.dk / www.ntd.dk

CVR 28111436

ntd.
EN IT PARTNER - TIL DET HELE