Phishing
– hvad for en fisk?

Medarbejderhåndbog om phishing

Sådan spotter du dem, der "fisker" og undgår at lande i deres net.

Mentor it
- med dig i fremtiden

Hvorfor skal jeg være opmærksom på phishing?

Phishing er den hyppigst oplevede angrebstype. I 2020 var 79% af alle, som var udsat for et cyberangreb, ramt af phishing.

Dette viser PwCs Cybercrime Survey fra 2020, som er lavet i samarbejde med blandt andet Rådet for Digital Sikkerhed, Center for Cybersikkerhed, Dansk Erhverv m.fl.

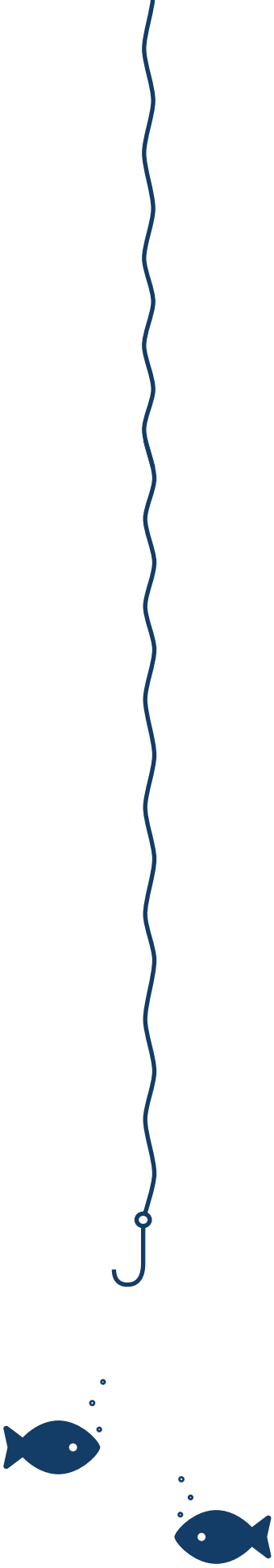
Hvad er phishing?

Phishing er forsøg på at franarre person-oplysninger. Helt enkelt: Fiske oplysninger fra dig, som kan bruges til kriminelle handlinger.

Phishing ses typisk i form af, at du modtager en e-mail fra en person eller virksomhed, du normalt har tillid til. Mailen kan opfordre til forskellige ting – en bestemt handling, et klik på et link, deling af information eller noget helt fjerde.

Men uanset hvor uskyldigt det i første omgang kan virke, må du ikke lade dig narre. Vi har samlet et par simple men vigtige anbefalinger til, hvordan du spotter fiskerne. Og ikke mindst: Hvordan du undgår at lande i deres net.

Læs dem, del dem med kollegaerne og vær bedre klædt på næste gang, et phishing-forsøg indtræffer.



Sådan spotter du banditterne

Forsøg på phishing er sjældent 100 % fejlfrit – og det er til din fordel, men det kræver, at du er opmærksom. Her følger 4 eksempler på, hvad du skal se efter, når der lander en e-mail i din indbakke:

1. Er afsenders mailadresse valid?

Hvis ikke adressen kan ses, kan du klikke på afsenders navn, og adressen vil komme frem. Her kan du blandt andet tjekke, om domænet (teksten efter @) er troværdig og i overensstemmelse med virkeligheden. @skat1234.dk er for eksempel ikke dén Skat, som typisk sender din forskudsopgørelse.

2. Er budskab, sprog og stavning troværdig?

Måden, hvorpå en e-mail er formuleret, kan ofte afsløre, om den er sand eller falsk. Sprogfejl og stavefejl var hyppigt engang, når man modtog phishingmails. Det er ikke så slemt længere, men småfejl optræder fortsat, og det kræver din opmærksomhed at spotte dem.

3. Er der links eller vedhæftede filer, du opfordres til at klikke på?

Typsik vil du blive bedt om at klikke på et link, åbne en fil eller sende noget bestemt retur til afsender. Alle tre opfordringer kan være et tegn på phishing.

4. Er mailsignaturen oprigtig?

Phishingmails har sjældent en mailsignatur, der er i overenstemmelse med, hvad du normalt oplever. Se efter, om den er mangelfuld og ulig normalen. Vær særligt ekstra opmærksom, hvis der blot er indsat: Sendt fra min iPhone.

Generelle leveråd

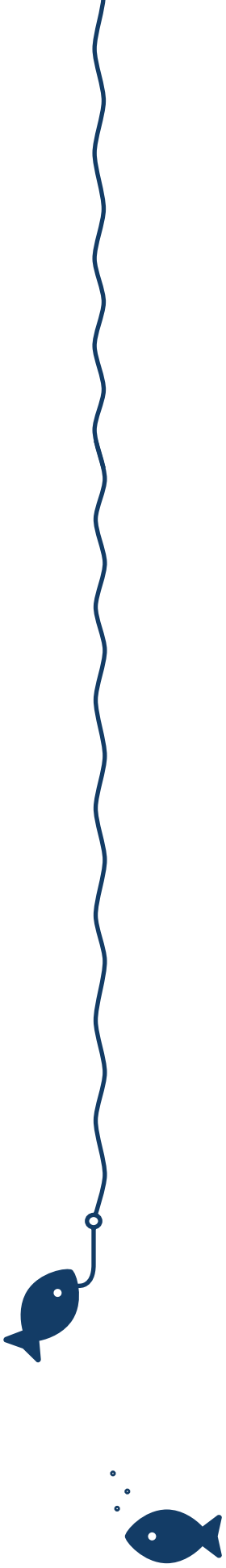
Vær altid opmærksom og eftertænksom,
når du tilgår din indbakke.

Tag dig den tid, det kræver at være påpasselig.
Det kan betale sig.

Hvad gør du, hvis du får bid?

Først og fremmest gør du ingenting. Klik ikke på noget som helst. Dernæst sørger du for at indrapportere e-mailen til din IT-ansvarlige, IT-afdeling eller IT-leverandør, så henvendelsen ikke kan skade andre. Og så sletter du e-mailen.

Nogle virksomheder har endda en phishingknap i Outlook, hvor du automatisk kan indrapportere phishing-forsøg. Er du i tvivl, om det er phishing eller ej, kan du altid få verificeret e-mailens indhold fra afsender for eksempel via telefon.



Konsekvenserne....

Hvis du ikke kender konsekvenserne ved phishing, har vi samlet et par stykker til dig:

- CEO Fraud
- Identitetstyveri
- Økonomisk svindel
- Datatab
- Nedetid

I tvivl?

Har du spørgsmål, eller du det mindste i tvivl om, hvordan du og dine kollegaer bedst navigerer i fiskesøen fuld af farlige fiskere, så sig endelig til. Vi hjælper gerne med at skabe mere sikre og trygge arbejdsrammer.

God fornøjelse!

Mentor IT Esbjerg
Mentor IT Kolding
Mentor IT København
Mentor IT Aarhus

Telefon +45 70 122 123
E-mail info@mentor-it.dk

Mentor it
- med dig i fremtiden