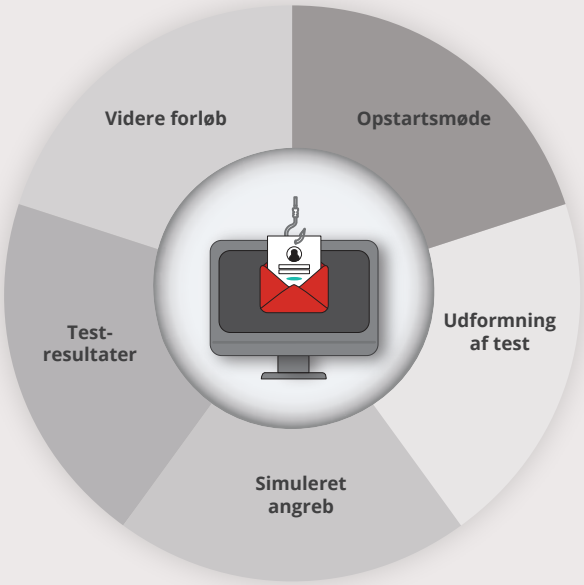
REVISIONSHUSET
TAL & TANKER



Phishing angreb

Kan medarbejderne modstå et phishing angreb?

HVORFOR

Virksomhedens ansatte repræsenterer den største kontaktflade til omverdenen, og er typisk også den største risiko, hvad angår phishing angreb.

Samtidig bliver angriberne, som udfører phishing, dygtigere og bliver dermed tiltagende sværere at gennemskue. Det er derfor vigtigt, at man som organisation ved, hvor it-fornuftige ens medarbejdere er.

Derfor er det ekstremt vigtigt, med jævne mellemrum at vurdere jeres sårbarhed over for et sådant angreb og sørge for at jeres medarbejdere ved, hvordan de skal forholde sig, hvis de bliver angrebet.

HVAD

Vi udfører Phishing testen i samarbejde med jer. Herudover oplyser vi jeres medarbejdere om mulige trusler samt uddanner dem i, hvordan de bør forholde sig, hvis de bliver forsøgt angrebet.

Det simulerede phishing angreb udformes således, at en e-mail sendes ud til de brugere i organisationen, som skal omfattes af testen.

E-mailen består typisk af en tekst og et link, som designes i samarbejde med jer. Fx: ”Din pakke fra PostNord er på vej. Klik på track and trace-linket for at se mere om din pakke.”

HVORDAN

Der afholdes et opstartsmøde med relevante personer - typisk fra IT, HR eller fra ledelsen hvis dette ønskes.

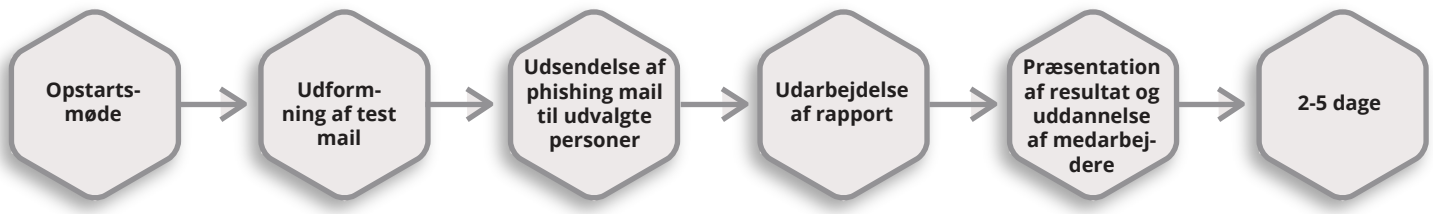
Opstartsmødet:

- Kort præsentation af, hvordan testen kommer til at forløbe
- Udformning af test mail
- Ønsker til indhold i den efterfølgende rapport
- Liste over personer som skal deltage i testen

Testresultatet:

- Hvor mange og evt. hvem åbnede mailen
- Hvor mange og evt. hvem klikkede på linket
- Hvor mange og evt. hvem forsøgte at logge ind med brugernavn og password

Procesforløb:



KONTAKT: Telefon: 86811033 | E-mail: itsikkerhed@talogtanker.dk