itnlvision
solutions for one global market

Undgå phishing e-mails med DMARC.

Phishing e-mails er e-mails der er sendt af en ikke-autoriseret person som modtageren tror er sendt af jer.
Dette er et stadigt stigende problem, og bruges i stor grad til at stjæle persondata, bank/kreditkort oplysninger, loginoplysninger og lign.

For at bekæmpe dette, kan I sætte DMARC op på sit domænes DNS.

Du kan læse mere omkring DMARC på https://sikkerdigital.dk/myndighed/tekniske-tiltag/dmarc

For at opsætte DMARC, kræver det at I har adgang til at ændre i det der hedder en DNS (Domain Name System) for det domæne i sender mails fra.
Dette kan i de fleste tilfælde gøres i det kontrolpanel i kan logge ind i via jeres webhotel.

Dette er især vigtigt hvis i vil sende mails til @gmail.com eller @yahoo, da de har øget deres sikkerhedskrav i kampen mod phishing og derfor vil fra d. 1. februar 2024, i stigende grad afvise E-mails der ikke opfylder deres krav omkring DMARC, SPF og DKIM.

For yderligere forklaring på hvordan man håndterer en DNS og dens opsætning, kontakt jeres webhotel, da det kan variere fra webhotel til webhotel.

DMARC:

DMARC (Domain-based Message Authentication Reporting and Conformance) er en politik man sætter op på sit domænes DNS, som styrer hvordan e-mails der fejler en eller begge af SPF og DKIM, skal håndteres.

Ydermere vil der blive sendt en rapport fil til en e-mailadresse hvert døgn, hvis der har været nogle e-mails der har fejlet enten SPF eller DKIM og derved har aktiveret DMARC politikken.

Der er tre forskellige politikker som DMARC kan bruge.

- **DMARC Politik "none":**
  - Der bliver ikke foretaget nogen handling på mails der fejler SPF eller DKIM.
  - Der sendes en rapport hvert døgn, hvis der har været sendt nogle e-mails.
  - Anbefalet politik at bruge når man sætter DMARC op til at starte med.
- **DMARC Politik "quarantine":**
  - E-mails der fejler enten SPF eller DKIM verificering vil blive behandlet som en mistænkelig e-mail og markeret som SPAM.
  - Der sendes en rapport hvert døgn, hvis der har været sendt nogle e-mails.
- **DMARC Politik "reject":**
  - E-mails der fejler enten SPF eller DKIM verificering vil blive afvist af modtagerens mail-server, og derved aldrig komme frem.
  - Der sendes en rapport hvert døgn, hvis der har været sendt nogle e-mails.

Der er forskellige online værktøjer der kan bruges til at generere en DMARC Record, f.eks. https://dmarcly.com/tools/dmarc-generator

Eksempel på DMARC record på en DNS:

Type: TXT
Navn / Host: _dmarc
Værdi / Indhold: v=DMARC1; p=none; rua=mailto:dmarc-rapport@eksempel.dk; sp=none;

Nogle DNS-udbydere kræver at man "Udgiver" sine ændringer efterfølgende, så kig efter en "Udgiv" knap. Hvis der ikke er nogen, er det meget sandsynligt at det bliver udgiver automatisk.

OBS: Der KAN gå op til 48 timer før en DNS bliver færdig opdateret i hele verdenen, men vil oftest være klar inden for 60 minutter.

Send venligst en mail til rhe@itnvision.dk eller support@itnvision.dk med navnet på jeres domæne og at i har sat DKIM Record op. Så kører vi en hurtig test og verificere at det virker som forventet.