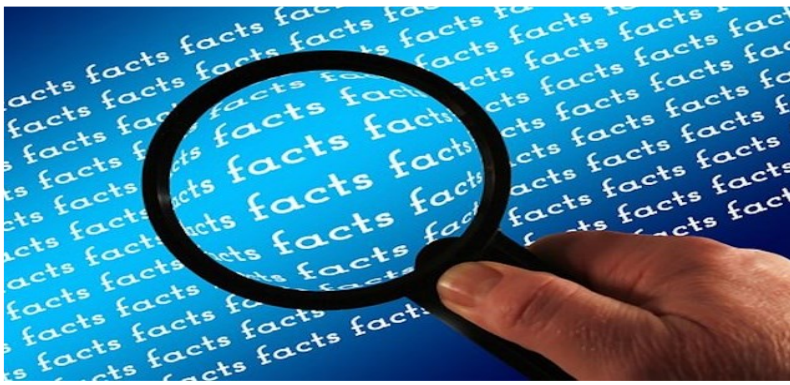
CYBER Sikkerhedstjek

12 spørgsmål du SKAL kunne svare JA til !



BACKUP

Tager vi backup **hver** dag?

Kan vi gå en **dag,** en **uge** og en **måned** tilbage, hvis vores backup skal indlæses?

Er vores backup beskyttet, så der **KUN** er adgang til den, når den er i brug?

Undgå altid at der er adgang til NAS bokse i netværket, hvis de anvendes til backup!

BESKYTTELSE AF DIT NETVÆRK

Anvender vi en firewall, som beskytter os mod uautoriseret adgang?

Anvender vi opdateret antivirus-beskyttelse på alle vores pc'ere og servere?

Har vi et opdateret spamfilter, som filtrerer uønskede mails fra?

DIN ANVENDELSE AF IT

Anvender vi alle **stærke** password?

Dvs. min. 8 karakterer, store og små bogstaver, specialtegn og tal som ikke er i rækkefølge!

Kommunikerer vi **ALTID** kritiske ændringer så som bank- og betalingsoplysninger ud til vores kunder på anden vis end blot ved at sende en e-mail?

..og ved vores kunder det?

Ved kritiske e-mails som når vi sender en PDF-faktura, anvender vi **ALDRIG** "Besvar" på en eksisterende mail, men opretter **ALTID** en ny e-mail?

Hvis vi modtager en mail, som vi er tvivl om er ægte, så er vi ikke i tvivl! – så sletter vi den!

OM ENVISTA FORENSICS

ENVISTA Forensics A/S er en del af en global virksomhed med speciale i årsagsundersøgelser inden for en række tekniske områder herunder CYBER hændelser.

NÅR DU ARBEJDER UDEFRA

Når vi logger på vores system udefra er **ALLE** vores forbindelser sikret udover blot anvendelse af brugernavn og password?

Envista anbefaler kraftigt , at der altid anvendes VPN eller tilsvarende sikkerhed!

BRUG AF EKSTERNE SYSTEMER

Anvender vi **ALTID** 2-faktor godkendelse, hvor det kan lade sig gøre?

Facebook, Gmail, MS 365, Google Adwords osv..

VORES ERFARING | DIN SIKKERHED

Vores globale CYBER Team har gennem mange år undersøgt tusinder af CYBER skader. Størstedelen kunne være undgået eller begrænset, hvis disse 12 spørgsmål havde været opfyldt!

ENVISTA FORENSICS

ENVISTAFORENSICS.COM