Wat te doen bij een cyberincident?

Print dit uit en hang het op. Bij een incident wil je niet gaan zoeken.

M-IT SERVICES

EERST DIT, IN DEZE VOLGORDE

1 Haal het apparaat van het netwerk

Trek de netwerkkabel eruit of zet wifi uit. Zo voorkom je dat het zich verder verspreidt.

2 Zet niets uit waar bewijs op staat

Niet afsluiten en niets verwijderen. In het geheugen en de logboeken zit informatie die later nodig is.

3 Wijzig wachtwoorden

Doe dat vanaf een schoon apparaat, niet vanaf het besmette. Begin bij e-mail en beheeraccounts.

4 Meld het intern en bij je IT-partner

Laat collega's weten wat er speelt, zodat niemand op een verdachte link klikt. En bel je IT-partner.

5 Doe aangifte of meld het

Meld het bij de politie, en bij een datalek ook bij de Autoriteit Persoonsgegevens.

DOE DIT NÍET

- Niet betalen zonder advies — betalen geeft geen garantie en maakt je een aantrekkelijker doelwit.
- Niet zelf “even opschonen” — opnieuw installeren wist ook het spoor van hoe ze binnenkwamen.
- Niet wachten tot het overgaat — elk uur kan er meer data weglopen of versleuteld raken.

VUL NU IN — DAN HOEF JE STRAKS NIET TE ZOEKEN

Onze ICT-dienstverlener _____

Interne helpdesk of ICT-verantwoordelijke _____

Cyberverzekering (polisnummer + telefoon) _____

Directie of eigenaar _____

Anders _____

Twijfel je bij een stap? Bel ons — ook als je geen klant bent.

0412 744 300

www.mitservices.nl/wat-te-doen-bij-een-cyberincident