

Digitale Veiligheidscheck ZZP & MKB

1. Wachtwoorden en inloggen

- - Gebruik je unieke wachtwoorden voor al je accounts?
- - Gebruik je een wachtwoordmanager (zoals Bitwarden)?
- - Heb je multi-factor authenticatie (MFA) ingeschakeld op e-mail, cloud en boekhouding?

2. Back-ups en dataherstel

- - Heb je een automatische back-up die buiten je apparaat wordt opgeslagen?
- - Kun je een back-up ook daadwerkelijk terugzetten (getest)?
- - Worden je mail, cloud en administratie ook geback-upt?

3. E-mail en domeinbeveiliging

- - Heb je SPF, DKIM en DMARC correct ingesteld?
- - Wordt je e-mail gecontroleerd op verdachte inlogpogingen?
- - Waarschuw je klanten voor nep-betalingsverzoeken?

4. Netwerk en apparaten

- - Is je WiFi-netwerk goed beveiligd met een sterk wachtwoord?
- - Gebruik je aparte netwerken (bijvoorbeeld voor slimme apparaten of gasten)?
- - Zijn je apparaten (laptop, NAS, printer) up-to-date en versleuteld?

5. Klantgegevens en AVG

- - Staat gevoelige klantinformatie op versleutelde apparaten of in de cloud?
- - Gebruik je aparte accounts voor privé en werk?
- - Weet je wat je moet doen bij een datalek?

6. Samenwerking en ketenveiligheid

- - Gebruik je veilige tools met MFA (zoals Teams, Dropbox, Trello)?
- - Deel je geen accounts of wachtwoorden met anderen?
- - Kun je aantonen dat je basisbeveiliging op orde is?

Digitale Veiligheidscheck – Scorekaart

Score	Situatie	Toelichting
16–18	● Topniveau	Je digitale veiligheid is uitstekend geregeld. Blijf alert en voer jaarlijks een review uit.
13–15	● Goed op orde	Je basis is stevig. Met een paar gerichte optimalisaties zit je helemaal goed.
9–12	● Verbeterpunten	Je loopt nog risico op meerdere punten. Tijd om gericht actie te ondernemen.
5–8	● Gevaarlijk gebied	Meerdere cruciale onderdelen ontbreken. Je bedrijf is op dit moment kwetsbaar.
0–4	● Direct risico	Je staat digitaal vrijwel volledig open. Onmiddellijk ingrijpen voorkomt serieuze schade.

