4–Digitale veiligheid

- Maak digitale veiligheid onderdeel van uw Integraal Plan Veiligheidszorg (IPV; zie VBMK Kennisbank):
  1 – Breng alle risico's in kaart
  2 – Leg vast wat u kunt doen om schade te voorkomen, en wat u kunt doen om schade te beperken als zich toch een ongeluk voordoet.
  3 – Houd alle documenten bij elkaar, op een veilige plek, en houd ze actueel
  4 – Voer de maatregelen uit; informeer en instrueer medewerkers
- Maak een Digitale Calamiteitenkaart en deel het met alle medewerkers: wat te doen bij risico's en calamiteiten?
- Houd overzicht over uw accounts. Noteer op een veilige plek van elk account: wie hebben toegang tot het account? Inlognaam en wachtwoord.
- Wijzig wachtwoorden regelmatig; en in elk geval als een accountbeheerder niet meer voor uw organisatie werkt.
- Check of uw emailadres en telefoonnummer voorkomen in gehackte bestanden. Bijv via de website 'Have I been Pwned?'
- Accounts zijn vaak gekoppeld aan een e-mailadres en een mobiel telefoonnummer, vooral bij tweestaps-verificatie. Let er dan op dat het account bereikbaar blijft voor degenen die ermee moeten werken. Zorg voor een reserve-toegang tot het account, zodat het niet op slot kan raken.
- Hef ongebruikte accounts op.
- Check alle veiligheids- en privacy-instellingen van het account en stel ze bewust in.
- Check vanaf welke apparaten kan worden ingelogd en de veiligheid daarvan: hebben andere gebruikers toegang tot het apparaat, het account, de inloggegevens? Zit er een virusscanner op? Is alle software up-to-date? Wordt alleen beveiligde wifi gebruikt?
- Check of de aanbieder van het account gebonden is aan de AVG (Engels: General Data Protection Regulation, GDPR). De GDPR geldt voor alle bedrijven en organisaties die in Europa gevestigd zijn.
- Kiest u voor een betaald account: kunt u later probleemloos overstappen op de onbetaalde versie?
- Adressen en betaalgegevens downloaden vanuit het account: bewaar ze volgens AVG-richtlijnen
- Publiceer liever geen privé-contactgegevens online. Toch een privé e-mailadres plaatsen: vervang het apenstaartje @ door [at]. Bijvoorbeeld: j.de.molenaar[at]gmail.com. Het helpt spam en phising te voorkomen. Bots (automatische computerprogramma's) speuren namelijk websites af naar geldige e-mailadressen.

Phising
Oplichter 'vissen' naar contactgegevens, bankgegevens of inloggegevens. In een e-mail of sms vragen ze u op op een link te klikken

Hack
Het account is overgenomen en niet meer toegankelijk voor u.

Datalek
Soms komen persoonsgegevens in handen van anderen terecht (datalek) of bestaat het risico daarop (veiligheidslek). Gaat het om grote hoeveelheden gegevens, om gevoelige informatie, of kunnen de betrokkenen schade oplopen: u bent verplicht het lek binnen 72 uur te melden bij de Autoriteit Persoonsgegevens (AP) en/of bij de betrokkenen.