CHECKLIST ALS JE OP EEN PHISHING LINK HEBT GEKLIKT.

□ Internetverbinding verbreken (wifi uit, kabel los, vliegtuigstand aan)
□ Website sluiten, niets meer aanklikken
□ Apparaat scannen met up-to-date virusscanner
□ Browsergeschiedenis, cache en cookies wissen
□ Controleren of er downloads zijn → verdachte bestanden verwijderen

Als je géén gegevens hebt ingevuld

□ Extra letten op je bankrekening en accounts
□ Apparaat nogmaals controleren met scan

Als je wél gegevens hebt ingevuld

□ Bankgegevens → direct bank bellen, rekening/pas blokkeren
□ Persoonsgegevens (BSN, DigiD, adres) → gemeente bellen, fraude melden
□ Accountgegevens (mail, sociale media, webshop, etc.):
□ Wachtwoord direct wijzigen
□ Onbekende apparaten uitloggen
□ Tweefactorauthenticatie (2FA) aanzetten
□ Contacten waarschuwen voor mogelijke nepberichten

Controle & melding

□ Bank- en creditcardtransacties controleren
□ Controleren op verdachte inlogpogingen
□ Phishing melden bij Fraudehelpdesk.nl
□ Eventueel aangifte doen bij de politie
□ Organisatie (bank/bedrijf) informeren waar de phishing namens werd verstuurd

Voor de toekomst

□ Wachtwoorden uniek en sterk maken (evt. met wachtwoordmanager)
□ 2FA instellen op belangrijke accounts
□ Regelmatig back-ups maken
□ Altijd kritisch kijken naar e-mails/links (spelfouten, rare afzender, vreemde URL)