

Eerste hulp bij digitale nood

Praktische tips om jezelf online te beschermen

In samenwerking met veiliginternetten.nl en seniorweb

KPN. Voor een beter internet

Wat doe je bij een digitale noodsituatie?

We brengen steeds meer tijd online door. We bankieren, winkelen, werken en houden contact met anderen via internet. Daarom is het goed om te weten hoe je digitaal veilig blijft en waar je op kunt letten.

Een digitale noodsituatie kan iedereen overkomen. Denk aan een klik op een verkeerde link. Een telefoontje van iemand die zich als iemand anders voordoet. Of een bericht dat echt lijkt, maar dat niet is. Het is belangrijk dat je weet waar je op moet letten en wat je kunt doen als er iets misgaat.

Bij KPN hebben we elke dag te maken met cybercriminaliteit. Elke dag werken we aan de bescherming van onze klanten tegen digitale dreigingen. Zo helpen we Nederland digitaal veilig te blijven. Maar 100 procent veilig bestaat helaas niet. Daarom is het belangrijk dat ook jij weet hoe je veilig online blijft.

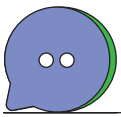
Dit boekje helpt je veiliger online te zijn. Niet alleen als er iets misgaat, maar het hele jaar door. Met praktische tips, duidelijke uitleg en vooral: wat je zelf kunt doen.

Voor dit boekje werkten we samen met veiliginternetten.nl en SeniorWeb, betrouwbare bronnen voor informatie over veilig internetten. Wil je meer weten? Kijk dan op: **kpn.com/superveilig**, **kpn.com/beterinternet** of **veiliginternetten.nl**. We helpen je graag.

In dit boekje lees je onder andere



Hoe je **sterke wachtwoorden** maakt en veilig gebruikt.



Hoe je **oplichting** herkent waarbij iemand zich voordoet als je **bank** of een **bekende**.



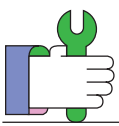
Hoe je **phishing** herkent en wat je moet doen als je toch op een **verkeerde link** klikt.



Wat je kunt doen als je account, telefoon of **persoonlijke gegevens** zijn gelekt.



Waar je terechtkunt voor hulp bij een **digitale noodsituatie**.



Welke **digitale controles** je regelmatig kunt doen om veilig online te blijven.

Kortom

Blijf rustig, blijf alert en wees voorbereid. Digitaal veilig zijn begint met weten wat je kunt doen. **Samen houden we Nederland digitaal verbonden én veilig.**

3 belangrijke stappen

Digitale veiligheid begint vóórdat er iets misgaat. Bescherm jezelf, herken verdachte situaties en weet wat je moet doen als het toch misgaat.

1.



Voorkomen
Maak het criminelen zo moeilijk mogelijk.

2.



Herkennen
Leer verdachte situaties op tijd herkennen.

3.



Handelen
Weet wat je moet doen als het misgaat.

Stap 1.

Voorkomen



Bescherm je accounts

Een groot deel van je digitale leven zit achter een wachtwoord. Denk aan je e-mail, sociale media, webwinkels en apps. Het is daarom belangrijk om je accounts goed te beschermen.

Voor elk account een ander wachtwoord
Gebruik je hetzelfde wachtwoord voor verschillende accounts? Dan kan een crimineel die jouw wachtwoord heeft ook proberen daarmee in te loggen op andere plekken. Gebruik daarom voor elk account een ander wachtwoord. Kies een lang wachtwoord dat niet makkelijk te raden is.

Gebruik een wachtwoordzin
Een wachtwoordzin is een wachtwoord dat bestaat uit meerdere woorden. Kies een lange zin die jij makkelijk onthoudt, maar een ander niet kan raden. Gebruik geen naam of andere persoonlijke informatie.

Voorbeeld
MijnFietsHeeft2LekkeB@nden!

Belangrijk
Gebruik voor ieder account een andere wachtwoordzin. Zorg ervoor dat in de wachtwoordzin minimaal één hoofdletter, één cijfer en één speciaal teken (bijvoorbeeld !@#$) bevat. Dat is vaak verplicht! Gebruik het voorbeeld hierboven niet als echt wachtwoord.

Inloggen in twee stappen
Je gebruikt dan naast je wachtwoord een extra controle, bijvoorbeeld een code of melding op je telefoon. Dit heet tweestapsverificatie. Zo kan iemand met alleen je wachtwoord niet zomaar inloggen.

Wat is 2FA?

2FA (tweestapsverificatie) is een extra beveiliging voor je account. Naast je wachtwoord gebruik je een tweede manier om te bewijzen dat jij het bent.

Dit kan bijvoorbeeld met:

- Een code uit een verificatie-app
- Een melding op je telefoon die je goedkeurt
- Een code per sms

Zo blijft je account beter beschermd, ook als iemand je wachtwoord weet.

2FA instellen

- Ga naar Instellingen > Beveiliging van je account
- Kies 2FA of tweestapsverificatie
- Kies de gewenste manier van verificatie
- Volg de stappen op het scherm en rond de controle af
- Bewaar eventuele herstelcodes op een veilige plek, bijvoorbeeld in een wachtwoordmanager

Tip: deel een verificatiecode of herstelcode nooit met iemand anders.

Ruim je accounts op

Hoe meer online accounts je hebt, hoe meer gegevens er op verschillende plekken worden opgeslagen. Oude accounts kunnen daardoor een onnodig risico vormen bij een datalek.

Zo houd je het veilig:

- Verwijder accounts die je niet meer gebruikt
- Meld je af voor nieuwsbrieven die je niet meer leest
- Controleer bij belangrijke accounts je wachtwoord en beveiligingsinstellingen
- Deel online alleen de gegevens die echt nodig zijn

Tip: een account dat je niet gebruikt, kan je beter verwijderen.

Winkel als gast

Een account aanmaken bij iedere webshop is meestal niet nodig. Kies, als het kan, voor ‘Bestellen als gast’. Je deelt dan alleen de gegevens die nodig zijn om je bestelling te bezorgen en te betalen. Je hoeft geen extra wachtwoord aan te maken.

Tip: maak alleen een account aan als je het echt nodig hebt.

4 maatregelen voor je apparaten en bestanden

Op je telefoon, tablet en computer staan persoonlijke gegevens, foto's en belangrijke bestanden. Met een paar eenvoudige maatregelen kan je die beter beschermen.



Installeer updates
Updates maken je apparaat veiliger. Installeer ze op tijd of zet automatisch bijwerken aan.

Bescherm je apparaat tegen malware
Gebruik een virusscanner en bescherming tegen schadelijke websites. KPN biedt hiervoor F-Secure en Veilig Browsen.

Maak regelmatig een back-up
Een back-up is een extra kopie van belangrijke bestanden, zoals foto's en documenten. Bewaar die bijvoorbeeld in de cloud en controleer af en toe of de back-up werkt.

Bescherm je e-mail extra goed
Via je e-mail kan je vaak wachtwoorden van andere accounts opnieuw instellen. Gebruik daarom een uniek wachtwoord en zet inloggen in twee stappen aan.

Stap 2.

Herkennen



Herken de alarmsignalen

Een bericht lijkt van je bank te komen. Een familielid appt dat er dringend geld nodig is. Criminelen proberen je op allerlei manieren te misleiden. Soms willen ze dat je geld overmaakt. Dit is online oplichting. Soms proberen ze persoonlijke gegevens te krijgen, zoals je wachtwoord of inlogcode. Dit wordt phishing genoemd. Dat kan via e-mail, sms of WhatsApp, maar ook via sociale media, QR-codes of de telefoon.

Er is haast

Criminelen proberen vaak te zorgen dat je snel reageert.
Bijvoorbeeld met berichten als:

- 'Betaal vandaag nog.'
- 'Je account wordt geblokkeerd.'
- 'Klik direct op deze link.'
- 'Ik heb dringend geld nodig.'

Door de haast heb je minder tijd om na te denken.

Iemand vraagt om gegevens of geld

Geef niet zomaar je wachtwoord, pincode, inlogcode of betaalgegevens. Vraagt een bekende onverwacht om geld? Bel die persoon dan zelf op het nummer dat je al kent. Spreek eventueel met familie of vrienden een codewoord af. Zo kan je makkelijker controleren of je echt met die persoon te maken hebt.

Belangrijk

Een bank, de politie of een officiële instantie vraagt je nooit om je pincode of inlogcode door te geven. Krijg je onverwacht een verzoek om geld over te maken of op een link te klikken? Doe dit dan niet zomaar. Ga zelf naar de officiële website of app om te controleren of het bericht klopt.

Echt of nep?

Valse berichten kunnen er heel echt uitzien. Criminelen kunnen met AI ook tekst, beeld en geluid namaken. Zelfs de stem van iemand die je kent kan nagemaakt worden. Alleen kijken of een bericht netjes is geschreven, is daarom niet genoeg.

Kijk goed naar de afzender
Kijk bij een e-mailadres vooral goed naar het deel achter de @.
Let op vreemde toevoegingen, spelfouten of extra letters. Twijfel je?
Klik dan nergens op, maar zoek zelf de officiële website of app van de organisatie op. Meer tips vind je op **veiliginternetten.nl**.

Pas op met links en bijlagen
Een link kan je naar een nagemaakte website brengen. Daar proberen criminelen bijvoorbeeld je wachtwoord of betaalgegevens te krijgen. Of er wordt malware op je computer geplaatst. Open ook niet zomaar een bijlage die je niet verwacht.

Stel jezelf de vraag: klopt het verhaal wel?
Een bericht kan er betrouwbaar uitzien en toch niet kloppen. Let daarom vooral op wat iemand van je vraagt. Moet je plotseling betalen? Je wachtwoord invullen? Een code doorgeven? Of heel snel iets doen? Is een verhaal niet te mooi om waar te zijn? Neem dan eerst de tijd om het bericht te controleren.

Zie je iets wat je niet herkent?
Soms merk je pas dat er iets mis is als iemand al probeert je account of gegevens te gebruiken. Let bijvoorbeeld op:

- Een melding van een inlogpoging die niet van jou is
- Een inlogcode waar je niet om hebt gevraagd
- Een bericht om je wachtwoord opnieuw in te stellen
- Geld dat van je rekening af is gegaan zonder dat je weet waarom

Om te onthouden

- Laat je niet onder druk zetten om snel iets te doen
- Deel nooit je inloggegevens, pincode of andere persoonlijke gegevens
- Controleer de afzender. Twijfel je? Neem contact op met de organisatie of persoon via contactgegevens die je vertrouwt.
- Klik niet zomaar op links en open geen onverwachte bijlagen
- Zie je iets wat je niet herkent? Verander dan meteen je wachtwoord.



Stap 3.

Handelen

Is er toch iets misgegaan? Geen paniek

Hoe sneller je in actie komt, hoe kleiner de schade blijft.
Hieronder lees je wat je kan doen in verschillende situaties.

Situatie 1:

Ik heb op een verdachte link geklikt

Heb je op een verdachte link geklikt of een bijlage geopend? Doe dan dit:

- [ ] **Sluit de website of het bestand**
  Vul geen gegevens in en klik nergens meer op.
- [ ] **Heb je iets gedownload of geopend?**
  Scan je apparaat dan met een beveiligingsprogramma, zoals een virusscanner.
- [ ] **Let op vreemde meldingen**
  Gedraagt je apparaat zich anders of zie je iets wat je niet vertrouwt? Vraag hulp bij het controleren van je apparaat.
- [ ] **Heb je ook gegevens ingevuld?**
  Ga dan naar situatie 2.



Situatie 2:

Ik heb gegevens ingevuld op een valse pagina

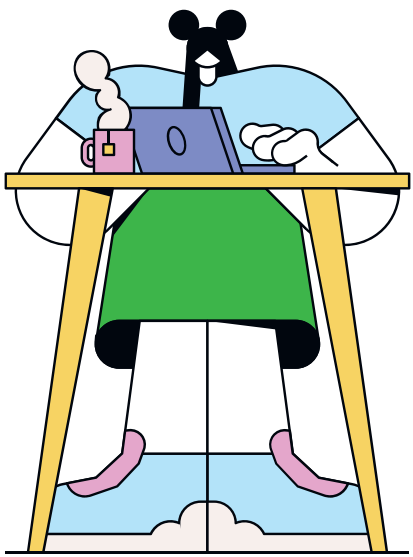
Wacht dan niet af en neem de volgende stappen.

- [ ] **Heb je een wachtwoord ingevuld?**
  Verander het meteen. Gebruik je hetzelfde wachtwoord voor iets anders? Verander het daar dan ook, begin met je e-mailaccount.

- [ ] **Heb je betaalgegevens of pincode ingevuld?**
  Neem direct contact op met je bank, controleer je rekening op betalingen die je niet herkent.

- [ ] **Heb je persoonlijke gegevens ingevuld?**
  Let extra op verdachte berichten en telefoontjes.
  Criminelen kunnen je gegevens gebruiken om je opnieuw te misleiden.

- [ ] **Bewaar bewijs**
  Bewaar het verdachte bericht of maak een screenshot.



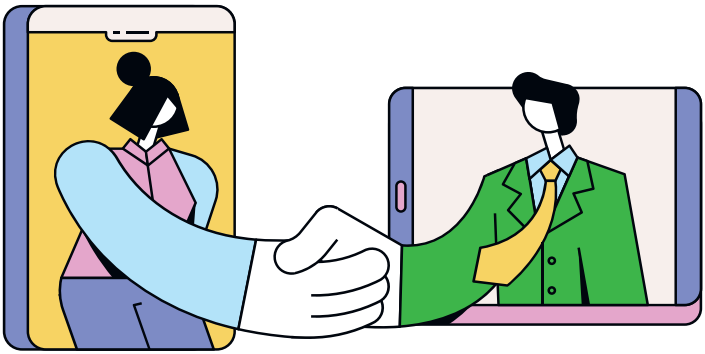


Situatie 3:

Ik heb geld overgemaakt

Heb je geld overgemaakt en denk je daarna dat je bent opgelicht? Of zie je een betaling of afschrijving die je niet herkent? Kom dan meteen in actie.

- [ ] **Bel je bank**
  Vertel wat er is gebeurd en volg de aanwijzingen van de bank.
- [ ] **Doe aangifte**
  Ga naar politie.nl of naar een politiebureau.
- [ ] **Meld de fraude**
  Ga naar fraudehelpdesk.nl.
- [ ] **Bewaar bewijs**
  Bewaar berichten, betaalverzoeken en andere informatie.
- [ ] **Controleer je rekening**
  Let op andere betalingen of afschrijvingen die je niet herkent.



Situatie 4:

Mijn gegevens zijn gestolen of gelekt

Krijg je bericht dat jouw gegevens bij een datalek betrokken zijn? Controleer wat er is gelekt en kom zo nodig in actie.

- [ ] **Controleer welke gegevens zijn gelekt**
  Controleer welke gegevens zijn gelekt. Je kan je e-mailadres ook controleren via Check je hack of Have I Been Pwned.

- [ ] **Wachtwoord gelekt?**
  Verander het meteen. Gebruikte je hetzelfde wachtwoord ergens anders? Verander het daar ook.

- [ ] **Blijf alert**
  Let extra op onverwachte berichten, telefoontjes, inlogpogingen en betalingen die je niet herkent.

- [ ] **Wordt er geld gevraagd?**
  Betaal niet. Je hebt geen garantie dat je gegevens daarna niet alsnog worden verspreid.

Situatie 5:

Iemand gebruikt mijn identiteit

Zijn je gegevens gelekt? Dat betekent niet automatisch dat iemand jouw identiteit kan misbruiken. Voor bijvoorbeeld een lening, bankrekening of telefoonabonnement zijn extra controles nodig.

Zie je wél misbruik. Doe dan dit:

- [ ] **Bewaar bewijs**
  Bewaar berichten, e-mails, rekeningen en andere informatie.

- [ ] **Waarschuw de betrokken organisatie**
  Is er iets op jouw naam besteld of aangevraagd?
  Neem contact op met die organisatie.

- [ ] **Meld identiteitsfraude**
  Meld daadwerkelijk misbruik bij het Centraal Meldpunt Identiteitsfraude (CMI). Bij een strafbaar feit kan je ook aangifte doen bij de politie.



Situatie 6:

Ik kan niet meer bij mijn account of bestanden

Lukt het opeens niet meer om in te loggen? Dan kan iemand je wachtwoord hebben veranderd. Ook kunnen criminelen bestanden op je computer blokkeren.

Kan je niet meer inloggen?
Controleer ook of je nog bij je e-mail kan. Ga daarna naar:

Wachtwoord vergeten of **Account herstellen**

Kan je niet meer bij je bestanden?
Zijn je bestanden geblokkeerd en wordt er geld gevraagd om ze weer vrij te geven? Betaal niet! Probeer de malware van je apparaat te verwijderen. Op veiliginternetten.nl vind je tips over wat je kan doen.

Heb je een back-up?
Dan heb je nog een kopie van je belangrijke bestanden.



Situatie 7:

Telefoon gestolen? Kom snel in actie

Wat kun je direct doen?

- [ ] **Vergrendel je telefoon op afstand**
  Hoe? Kijk op veiliginternetten.nl.
- [ ] **Blokkeer je simkaart**
  Via je provider.
- [ ] **Verander belangrijke wachtwoorden**
  Begin bij die van je e-mail.
- [ ] **Meld de diefstal**
  Meld je altijd bij de politie.
- [ ] **Neem contact op met je bank**
  Dit hoeft alleen als je een bank- of betaalapps op je telefoon gebruikte.
- [ ] **Wis je telefoon**
  Je kunt je telefoon op afstand wissen als je verwacht dat je deze niet terugkrijgt.
- [ ] **Controleer je bankrekening**
  Let op verdachte betalingen of berichten.

IMEI-nummer

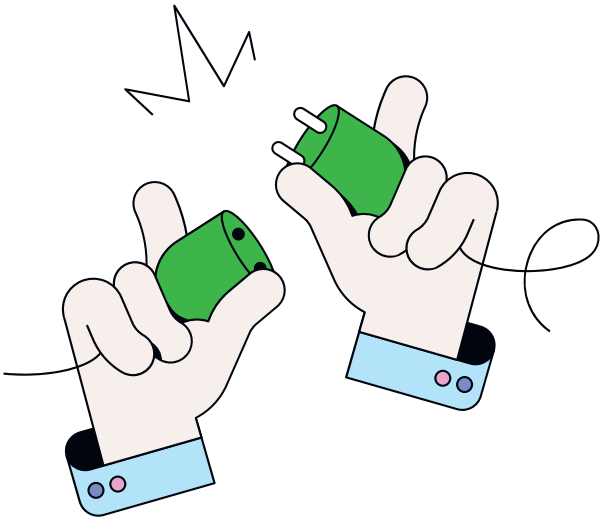
Een IMEI-nummer is het unieke identificatienummer van je telefoon. De politie of je provider kan dit nummer gebruiken als je telefoon gestolen is. Je vindt het nummer op de doos, in de instellingen of door *#06# in te toetsen in de telefoon-app.

Handig om vooraf te regelen

- Gebruik een sterke toegangscode
- Zet ‘Zoek mijn iPhone’ of ‘Vind mijn apparaat’ aan
- Maak regelmatig een back-up
- Bewaar je IMEI-nummer op een veilige plek
- Zet waar mogelijk tweestapsverificatie aan
- Zorg dat je telefoon vindbaar blijft

Meer uitleg over hoe je deze maatregelen kan nemen.

Ga naar veiliginternetten.nl.



Situatie 8:

Wat als de stroom uitvalt?

Bij een grote of langdurige stroomstoring kunnen internet, tv en telefonie uitvallen. Ook mobiel bellen en internet kunnen na verloop van tijd niet meer werken. Bereid je daarom voor.

- [ ] **Contactgegevens**
  Bewaar belangrijke nummers en adressen op papier.
- [ ] **Back-up**
  Maak een kopie van belangrijke bestanden.
- [ ] **Updates**
  Hou je apparaten up-to-date.
- [ ] **Powerbank**
  Zorg dat die opgeladen is.
- [ ] **Noodradio**
  Leg een radio op batterijen klaar.
- [ ] **Afspraken**
  Spreek af hoe je contact houdt als bellen niet lukt.

Situatie 9:

Online lastiggevallen?

Word je via sociale media, e-mail of chats lastiggevallen?
Of blijft iemand contact zoeken terwijl je dat niet wilt?
Doe dan dit:

- [ ] **Bewaar bewijs**
  Maak screenshots en bewaar berichten, foto's en andere informatie.

- [ ] **Controleer je privacy-instellingen**
  Bekijk wie je berichten, foto's en locatie kan zien.
  Deel deze informatie liever alleen met mensen die je kent.

- [ ] **Vraag hulp**
  Blijft iemand je lastigvallen of voel je je bedreigd? Zoek dan hulp.



Wat kan je nu doen?

Maak van online veiligheid een vaste gewoonte.

Heb je dit al geregeld?

- [ ] **Ik gebruik voor mijn belangrijkste accounts verschillende wachtwoorden**
- [ ] **Ik heb inloggen in twee stappen ingesteld**
- [ ] **Mijn apparaten krijgen automatisch updates**
- [ ] **Ik maak regelmatig een back-up**
- [ ] **Ik controleer mijn privacy-instellingen**
- [ ] **Ik denk na over welke persoonlijke gegevens ik online deel**

Waar kan ik terecht voor hulp?

Acuut gevaar?
Bel 112

Online lastiggevallen of misbruikt?
offlimits.nl

Fraude of oplichting?
fraudehelpdesk.nl
of 088-7867372

Tips om veilig online te blijven?
veiliginternetten.nl / kpn.com/superveilig

Hulp nodig in de digitale wereld?
seniorweb.nl of 030-2769965

Online opgelicht of een ander strafbaar feit?
Doe aangifte bij de Politie op een politiebureau of kijk op politie.nl

Meer hulp en informatie
mediawijsheid.nl / slachtofferhulp.nl / 113.nl / kindertelefoon.nl / rutgers.nl

Blijf rustig, blijf alert en wees voorbereid.
Digitaal veilig zijn begint met weten wat je kunt doen.
Zo houden we samen Nederland digitaal verbonden én veilig.

Voor meer informatie of vragen kan je altijd contact opnemen met KPN. Kijk voor meer informatie op kpn.com of ga langs bij één van onze winkels.

Meer weten over veilig internetten?

kpn.com/superveilig

kpn.com/beterinternet

veiliginternetten.nl

KPN. Voor een beter internet