

Cyber criminaliteit WijsmetjeWijk Centrum

1. Bel fraude:



De telefoon gaat. Op het scherm een onbekend nummer. Als je opneemt begint er een bandje te lopen. Een stem zegt toets 1 om verder te gaan. Bijvoorbeeld; je krijgt te horen; Je Burgerservicenummer (BSN) is misbruikt bij een misdrijf, er is een arrestatiebevel tegen je uitgevaardigd, of je naam is

gevalen in rechtszaak rond drugshandel.

Wat te doen? Snel geld overmaken, zegt de stem.

De stemmen op het bandje en aan de andere kant van de telefoonlijn spreken Engels, veelal met een Indiaas accent.

“Sommige mensen raken in paniek en denken niet meer na”.

De fraudeurs achter de valse telefoontjes gaan geraffineerd te werk. Ze maken gebruik van spoofing: (gebruiken nummers van bestaande bedrijven) slachtoffers zien een ander nummer op hun telefoon. Wie dat nummer later belt komt bij particulieren, bedrijven of bij instanties terecht, die van niks weten.

Bellende oplichters nemen steeds andere vermommingen aan. Bij een van de langstlopende vormen van telefonisch bedrog belt ‘de helpdesk van Microsoft’ met de boodschap dat uw pc zich verdacht gedraagt en of u een programma wilt installeren waar- mee de helpdesk op afstand mee kan kijken: men vraagt dan, ‘Laten we eerst uw bankrekening veiligstellen. Logt u maar even in, met uw naam en pincode...’ Microsoft-fraudeurs spelen handig in op de angst voor computervirussen en hackers.

Moraal:

Hoe voorkom je dat je in de val trapt? Ga niet in op de aanwijzing om terug te bellen, zeker niet via automatisch doorschakelen (‘Druk op toets 1 in’).

Noteer het telefoonnummer dat u probeerde te bereiken en zoek op van wie het is. Bel met de servicelijn van bank, bedrijf of instantie om te checken of ze je werkelijk zoeken. Geef nooit wachtwoorden, inlogcodes, rekeningnummers of andere gevoelige informatie door.

Installeer geen onbekende software en ook geen programma’s als “**Team Viewer of Any-Desk**”, waarmee een ander uw pc kan overnemen.

Bent u er toch ingestonken? Heeft u software geïnstalleerd via een link die oplichters u hebben toegestuurd of die u via een website heeft gedownload? Zet dan de pc onmiddellijk uit.

Bel in alle gevallen uw bank en de politie op 0900-8844.

Op **Fraudehulpdesk.nl** en **Veiligbankieren.nl** staat nog meer praktische informatie. Duizenden mensen vielen al ten prooi aan criminelen die zich voordoen als de politie, Hoge Raad of Microsoft.

2. Online fraude, bank, WhatsApp, SMS:

Banken:

Nepberichten van uw bank, hetzij via whatsapp, via een E-mail, via een SMS bericht of via een brief!

WhatsApp;



U krijgt een melding van uw bank met de mededeling dat een bedrijf geld van uw rekening wil halen. De zogenaamde medewerker van de bank wil dit samen met u voorkomen. Gevraagd wordt uw gegevens **met pincode** in te vullen en het wordt voor u geregeld. Wat doet u?

E-mail;



Het Engelse woord “Phishing”, ofwel ‘hengelen’. Dat is namelijk wat de criminelen doen: hengelen naar uw gegevens. Zij sturen een bericht namens een bank, de overheid of een webwinkel. Het ziet er echt uit. Meestal gaat het om een dringend verzoek. U moet zogenaamd snel betalen of een prijs in ontvangst nemen. Door de mail zo echt mogelijk laten te lijken, proberen ze het vertrouwen van de lezer te winnen. Het slachtoffer klikt nietsvermoedend door, vult een aantal gegevens in en... beet! De criminelen krijgen wat ze zochten: inloggegevens en persoonlijke informatie.

Bijvoorbeeld; Een voorbeeld: u krijgt een e-mail die afkomstig lijkt van de ING-bank. In de e-mail wordt gevraagd om met spoed op een link te klikken. Deze e-mail komt echter niet van de bank zelf, maar van oplichters. Loop met bovenstaande punten in het achterhoofd eens door deze mail.

Herkent u hem als phishing?

Trap er niet in!

Sms-bericht;



U krijgt het volgende bericht; uw ...bankrekening is in quarantaine geplaatst en dient opnieuw te worden geverifieerd. Voorkom blokkade van uw rekening en volg de stappen in onderstaande link!

Of

U krijgt een melding van de belastingdienst; U heeft nog een openstaande schuld met kenmerk 2021SB094567 van € 350,00. Voorkom inbeslagname en betaal vandaag nog door op onderstaande link te klikken.

Sms-wedstrijd:



In het geval van Instagram-oplichting zegt de zogenaamde bekende dat hij of zij meedoet aan een sms-wedstrijd. Het slachtoffer moet even een code doorgeven die via de sms binnenkomt. Maar in werkelijkheid gaat het hier helemaal niet om een wedstrijd, maar om een betaalbevestiging. Bij een betaalplatform maakt de oplichter onder uw naam en telefoonnummer een account aan. Door de

sms-code door te geven, geeft u juist de bevestiging waar de oplichter op zit te wachten. Foute boel dus. Kap het gesprek af en blokkeer deze persoon. Laat ook aan de bekende weten dat zijn of haar naam gebruikt wordt voor dit soort oplichting, zodat anderen gewaarschuwd kunnen worden.

Whaling:



Een bijzondere vorm van phishing die extra aandacht verdient is "Whaling".

Bij deze vorm wordt u benaderd door een zogenaamd bekende, veelal iemand die zich voordoeft als zoon of dochter. Die neemt contact met u op, omdat hij of zij in nood zit en niet meer bij zijn geld kan. Trap hier niet in, maar wis het bericht en blokkeer het nummer op uw telefoon.

Wat te doen bij?



U hebt (per ongeluk) een bijlage geopend uit een nep mail:

1. Sluit het e-mailprogramma af.
2. Laat de virusscanner een uitgebreide scan van de computer uitvoeren. En laat het programma eventueel gevonden schadelijke software direct onschadelijk maken.
3. Wijzig voor de zekerheid uw (belangrijke) wachtwoorden. Zeker die van uw e-mail en de bank.
4. Wacht met internetbankieren totdat u er zeker van bent dat er geen schadelijke software op de pc aanwezig is. Twijfelt u daaraan, neem contact op met de bank voor een advies.
5. Is de mail afkomstig van een bekend bedrijf of bekende instantie, neem dan ook hiermee contact op en leg hen de situatie voor.

U hebt gegevens ingevuld op een valse website:

1. Kwam u via een mail terecht op de site? En vermoedt u dat zowel de site als e-mail nep zijn, maar u weet het niet zeker?
2. Was de mail nep en hebt u inloggegevens ingevuld? Verander direct uw wachtwoord.
3. Hebt u ook een telefoonnummer opgegeven? Als u merkt of vermoedt dat uw telefoonnummer misbruikt wordt voor (dure) sms-abonnementen, controleer dit dan op de site www.payinfo.nl

4. Hebt u een e-mailadres achtergelaten? Grote kans dat u gebombardeerd wordt met dubieuze reclamemails. Afmelden hiervoor heeft geen zin: daarmee bevestigt u dat het e-mailadres wordt gebruikt. Verplaats de e-mails naar de spam-map. Daarmee leert u uw e-mailprogramma welke e-mails spam zijn. Na een tijdje komen deze mails automatisch in de spam-map terecht.
5. Hebt u bankgegevens ingevuld? Bel direct uw bank.

U hebt geld overgemaakt naar oplichter:

Hebt u geld overgemaakt aan een partij die niet te vertrouwen is? Doe dan bij de politie aangifte van oplichting. U kunt hiervoor een afspraak maken via 0900-8844, het landelijke telefoonnummer van de politie of bij het dichtstbijzijnde politiebureau. Neem ook contact op met uw bank.

3. Babeltrucs:

Wat zijn babeltrucs?



De babeltruc. Veel ouderen zijn hier de dupe van. Maar het kan iedereen overkomen. Aan de deur, bij de pinautomaat of aan de telefoon. De dieven doen zich voor als een bankmedewerker of iemand de meterstand komt opnemen. Of als iemand die even naar het toilet moet. Met een smoes komt de dief bij u binnen om vervolgens geld of andere bezittingen te stelen. En dat wilt u natuurlijk

voorkomen!

Hoe herkent u een babeltruc?



De zogenaamde babeltruc kent tenminste drie vormen zoals hier is weergegeven.

Natuurlijk wilt u voorkomen dat u slachtoffer wordt.

We leggen u een aantal bekende voorbeelden voor van toegepaste babeltrucs. Dit doen we samen met u om te ervaren hoe u de truc kunt herkennen. Zo bent u straks extra bewust. En kunt u voorkomen dat u geld verliest of inbrekers in huis haalt.

Wat is de babeltruc?

“Babeltruc” betekent dat iemand, die u persoonlijk aanspreekt, met een smoes uw spullen of geld probeert te stelen.

Babeltruc aan de deur. Hieronder de voorbeelden:

a. “U heeft een openstaande rekening”

Een nepmedewerker van Ziggo, NUON of een andere maatschappij komt bij u aan de deur. Hij beweert dat u een openstaande rekening heeft. Soms zeggen ze dat u direct (contant) moet betalen. Soms proberen ze binnen te komen om spullen, bijvoorbeeld sieraden of geld, te stelen.

TIP: bedrijven komen nooit aan de deur om rekeningen te innen. Trap hier dus niet in.

b. “U krijgt geld terug”

Een nepmedewerker van KPN of een ander bedrijf komt bij u aan de deur. Hij beweert dat u geld terugkrijgt van het bedrijf. U hoeft alleen maar even uw bankrekeningnummer te geven...

TIP: bedrijven komen nooit aan de deur om geld terug te geven. Trap hier dus niet in.

c. “Gratis bosje bloemen”

Iemand belt aan en biedt u een bosje bloemen aan. Zogenaamd van een tuincentrum bij u in de buurt. Soms is het bosje gratis, soms wordt u gevraagd het te betalen. In beide gevallen proberen ze u af te leiden om geld te stelen.

TIP: winkels en bedrijven komen niet zomaar aan de deur om u bloemen aan te smeren. Weiger het bosje bloemen dus altijd. Ook als het gratis is.

d. “Ik ben van de thuiszorg”

Plotseling staat er iemand voor de deur die beweert van de thuiszorg te zijn. Hij of zij komt kijken of het goed gaat met u. vaak zijn ze met z'n 2-en. Zodra u ze binnenlaat, leidt de ene u af, terwijl de andere uw spullen en/of geld steelt.

Tip: thuiszorgmedewerkers komen nooit zonder afspraak bij u langs. Trap er dus niet in. U kunt eventueel om legitimatie vragen. Maar soms vervalsen ze die ook. Ga hier dus niet vanuit.

e. “Wij zijn uw nieuwe burens”

Iemand staat voor uw deur en beweert uw nieuwe burens te zijn. En of hij of zij even binnen mag komen.

TIP: laat nooit zomaar onbekenden binnen. Zeker niet als u alleen bent.

f. “Even in de meterkast kijken”

Iemand wil graag even in uw meterkast kijken, om zogenaamd de meters te controleren. Maar zodra u hem binnenlaat, ziet hij zijn kans schoon om spullen mee te nemen.

TIP: Energiebedrijven komen echt alleen op afspraak. Trap er dus niet in.

g. “Er is een gaslek”

Iemand beweert dat er een gaslekkage is in uw huis. Bijvoorbeeld door klachten van de burens. Ze willen graag uw huis even controleren op het zogenaamde gaslek.

TIP: een gaslekkage ontstaat niet zomaar. En als er een gaslek in uw huis is ruikt u dat zelf ook. Trap hier dus niet in.

h. “Ik collecteer voor het KWF”

Er staat een collectant voor uw deur. Bijvoorbeeld van KWF Kankerbestrijding. Maar u vertrouwt het niet: geef dan aan dat u nergens hebt gelezen dat er een collecte is deze week...

TIP: als u het niet vertrouwt, geef dan niet. Bel eventueel het goede doel om te vragen of zij die week collecteren. U kunt later altijd nog geld overmaken als het wel een echte collectant was.

i. “Ik ben van de Kamer van Koophandel”

Er staat een duo bij u voor de deur, zogenaamd van de Kamer van Koophandel. Ze willen graag binnenkomen om met u te praten. De ene leidt u af. De andere moet zogenaamd naar het toilet en steelt uw spullen.

TIP: de KvK staat nooit zomaar voor uw deur. Trap er dus niet in.

j. “U heeft de postcodeloterij gewonnen!”

Gefeliciteerd! U heeft de postcodeloterij gewonnen.! 2 personen komen met deze fijne boodschap, en willen graag binnenkomen. De ene leidt u af. De andere moet zogenaamd naar het toilet en steelt uw spullen.

TIP: als u niet meedoet met de postcodeloterij, klopt het verhaal van die 2 sowieso niet. En de postcodeloterij staat nooit zomaar voor uw deur. Tenzij (als u wel meedoet met de postcodeloterij, men met camera's en Caroline Tensen of Gaston voor uw deur staan.

k. "Ik kom de via Marktplaats gekochte spullen ophalen"

Degene die bij u aan de deur beweert spullen van u gekocht te hebben via Marktplaats, zal proberen bij u in huis binnen te dringen, probeert alleen maar uw spullen te stelen.

TIP: laat u niet overbluffen. Heeft u niets verkocht via Marktplaats? Dan klopt het verhaal sowieso niet. Hebt u wel iets verkocht? Vraag dan of ze specifiek kunnen vertellen wat ze dan komen ophalen.

l. "Mijn kind moet nodig naar het toilet"

Wanneer iemand met een kind aan de deur staat dat naar de wc moet, is daar natuurlijk moeilijk nee tegen te zeggen. Als iemand naar de wc gaat, loop dan nooit weg en blijf altijd in de hal staan.

TIP: Vertrouwt u het echt niet, verwijs ze dan naar een openbaar toilet.

m. "Pakketje aan de deur"

De pakketbezorger belt bij u aan en heeft een pakketje met uw adres met een voor u onbekend persoon.

Neem deze niet aan; criminelen komen het door u aangenomen later bij u ophalen met de smoes dat hun pakket verkeerd is bezorgd. De webwinkel waar het pakket is besteld stuurt u vervolgens de rekening.

Als u zeker weet dat u niets heeft besteld, neem het pakketje dan gewoon niet aan. Laat het desnoods afleveren bij een ophaalpunt. Dan kunt u later controleren of het pakketje echt voor u is. Oplichters proberen als postpakkettenbezorger uw handtekening te ontfutselen en willen uw pingegevens en pinpas stelen. Ze vragen namelijk of je ook de portokosten wilt betalen. Pin nooit aan de deur, als u daar geen specifieke afspraak voor hebt gemaakt.

TIP: Heeft u geen pakketje besteld? Neem het dan niet aan.

n. "Mag ik even naar uw computer kijken?"

Een man belt aan en vraagt of hij even uw computer mag checken. Hij concludeert al snel dat deze aan vervanging toe is. Voor een klein bedrag regelt hij dat wel even voor u... hij vraagt geld voor een nieuwe computer...

TIP: laat nooit zonder afspraak iemand zomaar binnen. Want dan klopt er iets niet. En ... geef vooral geen geld mee.

o. “Ik kom uw rookmelders controleren”

Sinds 1 juli 2022 zijn rookmelders verplicht op elke etage van uw woning. Hier zien criminelen helaas een nieuwe kans: ze bellen aan en beweren uw rookmelders te komen controleren. Ze hebben zelfs een (valse) identiteitspas. Als ze bij u binnen komen proberen ze zo veel mogelijk spullen en geld te stelen.

TIP: de overheid controleert (nog) niet op rookmelders. Mogelijk gaat dit wel gebeuren, maar dan krijgt u altijd vooraf bericht. Dus laat deze zogenaamde controleurs niet binnen.

p. “Ik heb een mooie cadeaudoos voor u”

Er komt een postbezorger bij u aan de deur, met een cadeaudoos. De bezorger ziet er zelfs uit als een werknemer van een bekend postbedrijf. Er is alleen een ‘probleem’: de verzendkosten zijn niet betaald. Ze vragen u € 1,50 te pinnen aan de deur. Als u dit doet, werkt de betaling niet. De bezorger wil u wel ‘helpen’. Maar dan wisselt hij uw pas om, waarvan hij de pincode van u heeft afgekeken. Wanneer u merkt dat uw pas omgewisseld is. Heeft de crimineel al veel geld gepind van uw rekening.

TIP: het komt eigenlijk nooit voor dat u ‘zomaar’ een cadeaudoos krijgt. Dus trap er niet in! Weiger de bezorging.

Babbeltruc aan de telefoon.

q. “Ik ben van Microsoft”

Degene aan de lijn zegt dat hij van Microsoft is. Vaak spreekt hij u in het Engels toe. Hij beweert dat er een virus op uw computer zit. Als u uw inloggegevens geeft, fikst hij het wel even voor u...U snapt het al; al uw gegevens worden gehackt.

TIP: Microsoft neemt nooit op deze manier contact met u op. Trap er dus niet in. Hang direct op.

r. “U moet direct een belastingsschuld betalen”

Deze truc richt zich meestal op ondernemers. Iemand doet zich voor als medewerker van de Belastingdienst. Die beweert dat u een belastingsschuld hebt en u moet direct betalen.

TIP: dit is absoluut nooit de werkwijze van de belastingdienst. Trap er niet in.

Babbeltrucs op straat/bij de supermarkt of langs de weg.

s. “Goedkoop gereedschap/pannenset”

Iemand heeft een ‘mooie’ deal voor u. namelijk een goedkope set gereedschap of pannen. Zo’n mooi aanbod kunt u echt niet laten schieten?

TIP: op straat aangeboden spullen zijn vaak gestolen en/of van zeer slechte kwaliteit. Sla het aanbod beleefd af.

t. “Geld voor een treinkaartje”

Iemand spreekt u aan: hij is zijn geld verloren. Of u geld voor hem heeft voor een treinkaartje. Soms komen mensen ook aan de deur met dit verhaal. Trek nooit uw portemonnee; want de crimineel probeert u af te leiden en u zo geld te ontfutselen.

TIP: het verhaal is hoogstwaarschijnlijk verzonnen. Geef niet zo meer geld als iemand daar om vraagt.

u. “Geld voor benzine”

Iemand staat stil langs de weg en trekt uw aandacht. Zijn benzine is op. Of hij een lift kan krijgen naar het volgende tankstation. Daar aangekomen blijkt hij geen geld te hebben. Kan hij dat even van u lenen?

Deze truc is extra geniepig omdat hij u in borg geeft: sieraden, telefoon of iets anders wat waardevol lijkt. Maar let op: dit is allemaal namaakspul.

TIP: wilt u iemand langs de weg helpen en herkent u iets wat hier is benoemd? Dan kunt u ervan uitgaan dat het foute boel is. Trap er dus niet in. Of vraag naar zijn legitimatie.

Tips om babbeltrucs te voorkomen



Voorkom een babbeltruc met de volgende tips:

1. Sta nooit uw pincode of andere persoonlijke gegevens af
2. Vraagt iemand uw pincode? Doe gelijk de deur dicht of hang de telefoon op
3. Kijk voordat u de deur opendoet altijd wie er aanbelt
4. Iets pakken in de huiskamer? Laat mensen altijd buiten wachten
5. Handel zoveel mogelijk af bij de deur
6. Laat nooit onbekenden in uw huis en vraag om identiteitskaart
7. Laat iemand van een bedrijf altijd een afspraak maken
8. Gebruik een raam- of deurspion, deurketting of kierstandhouder
9. Pin niet en wissel geen geld aan de deur
10. Bewaar pincode en pinpas altijd apart
11. Leg waardevolle spullen uit het zicht
12. Loop nooit met iemand mee naar buiten
13. Ben je alleen thuis? Doe de achterdeur op slot
14. Praat nooit met andere mensen over waardevolle bezittingen in huis
15. Gaat u geld pinnen? Scherm altijd de cijfers goed af met uw hand

Meld babbeltrucs bij de politie



Er wordt helaas veel misbruik gemaakt van het goede vertrouwen van ouderen. De oplichters gaan zo te werk, dat een babbeltruc iedereen kan overkomen. Denkt u dat iemand een babbeltruc bij u probeerde? Licht dan de politie gelijk in. Zo kunt u ervoor zorgen dat andere mensen niet de dupe worden van de dieven.

Waarschuw ouderen in uw omgeving

Ouderen zijn zich vaak van geen kwaad bewust. En daar maken oplichters maar al te graag gebruik van. Waarschuw ouderen in uw familie of in de buurt en vertel ze over de genoemde tips. En wat de gevolgen kunnen zijn van een babbeltruc. Zo helpt u anderen om babbeltrucs te herkennen. En belangrijker nog: te voorkomen.

4. Webshop:



We kopen allemaal wel eens, of meerdere keren, per jaar spullen via een webshop.

Er zijn webshops die de zaak oplichten, bijvoorbeeld; je bestelt wat je mooi of leuk vindt, drop dit in een winkelmandje en vul je gegevens in. Daarna gaat u afrekenen en u krijgt een bevestiging dat uw bestelling binnen een aantal dagen wordt verzonden echter; uw spullen komen niet!

De vraag is hoe kan je zien of een webshop betrouwbaar is?

- Staat er een keurmerk op de website? Bijvoorbeeld het Thuiswinkel Waarborg, Keurmerk Webshop, Trust shop of Qshop kenmerk? Ga naar de site van het betreffende keurmerk en controleer daar of de webwinkel is aangesloten.
- Als je niet eerder bij een webshop iets gekocht hebt, is het slim de naam van deze webshop in een zoekmachine in te voeren met trefwoorden als 'klacht', 'ontevreden' fraude' of 'oplichting'. Wat zijn de ervaringen van anderen? Vind je veel klachten, slechte reviews of meldingen dat spullen niet zijn ontvangen, koop dan niet van deze webshop.
- Controleer altijd of de persoonsgegevens op de website van de webshop staan. Ontbreken de persoonsgegevens? Vaak blijkt de persoon achter een website dan onvindbaar en dan heb je een probleem als het misgaat. Want wie moet je dan contacten als je geen spullen hebt ontvangen?

5. Wachtwoorden



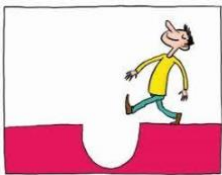
Wachtwoorden beveiligen uw gegevens. Maar u moet zelf zorgen dat ze sterk zijn en dat u ze slim bewaart en onthoudt. We bespreken de valkuilen en mogelijkheden.

Wachtwoorden

1. Veilig met een wachtwoord

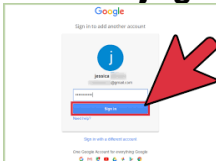
Een wachtwoord is een combinatie van cijfers, letters en leestekens waarmee u online informatie beveiligt. Het is de sleutel tot allerlei gegevens en diensten: uw e-mailaccount, een internetabonnement of internetbankieren. Zo'n wachtwoord zorgt dat alleen u dingen kunt wijzigen of aanvragen. Een sterk wachtwoord dat niemand kan raden is dus erg belangrijk.

2. Valkuilen bij wachtwoorden



Er is een aantal dingen erg belangrijk als het om wachtwoorden gaat.

3. Wijzig het standaardwachtwoord



Soms krijgt u als u een account aanmaakt een wachtwoord toegewezen. Bijvoorbeeld voor de [internetverbinding thuis](#). Het is verstandig dit wachtwoord te wijzigen, want lijsten met standaardwachtwoorden worden wel eens gestolen door hackers.

4. Kies geen makkelijk wachtwoord

Wachtwoorden moet u onthouden, daarom kiezen veel mensen een makkelijke. Denk aan een geboortedatum of eenvoudige cijferreeks. De meest gekozen beveiligingscodes zijn: 'wachtwoord', '123456', 'abc123', '11111' en '123123' en varianten daarop. Dat is niet veilig, want een computercrimineel die accounts van anderen wil hacken, probeert altijd eerst de veelgebruikte wachtwoorden.

5. Gebruik niet één wachtwoord voor alles

Het is verleidelijk om voor alles hetzelfde wachtwoord te kiezen, want dat is minder om te onthouden. Toch is het niet verstandig: mocht het bekend raken, dan kunnen andere mensen ook bij al uw accounts inbreken.

6. Laat de browser geen wachtwoorden opslaan

De meeste internetprogramma's kunnen [wachtwoorden opslaan](#). Handig, dan hoeft u het niet te onthouden. Maar het betekent ook dat iedereen die met uw computer deze sites bezoekt, meteen 'als u' wordt ingelogd. Wachtwoorden opslaan in de browser, is

alleen handig als u de enige gebruiker van de computer bent. Als er meer mensen 'm gebruiken, is het verstandig dat elke gebruiker alleen op zijn [eigen gebruikersaccount](#) werkt.

7. Sterk wachtwoord kiezen

Een sterk wachtwoord bestaat minimaal uit een reeks van 6 tot 8 letters en cijfers en minstens één leesteken. Hoe langer uw wachtwoord, hoe sterker het wachtwoord. Het is aan te raden uw wachtwoorden regelmatig te wijzigen, bijvoorbeeld elk kwartaal. De truc is om een sterk [wachtwoord te bedenken dat wél te onthouden](#) is.

8. Tweestapsverificatie: dubbel zo veilig

Een goed wachtwoord beveiligt een hoop, maar het kan nog veiliger met tweestapsverificatie: inloggen met een wachtwoord én een code die u ontvangt op een apparaat dat in uw bezit is. Dat kan een mobiele telefoon zijn of een ander apparaatje, bijvoorbeeld de Rabo Scanner van de Rabobank of met Digi-D. Is het mogelijk om [tweestapsverificatie](#) in te stellen, doe dat dan direct.

9. Beveiliging van de mobiel

Op mobiele apparaten (smartphone en tablet) en sommige nieuwe laptops zijn er veel [meer beveiligingsopties](#) dan alleen een wachtwoord. Voor mensen die visueel zijn ingesteld, is er op mobiele apparaten de optie om een patroon in te voeren in plaats van een code. En als het apparaat ervoor geschikt is, kunnen gebruikers gezichtsherkenning of een vingerafdrukscan gebruiken. Knappe jongen die dat kan namaken! Maar ook bij deze *high tech* opties blijft een wachtwoord de basis. U stelt een wachtwoord in voor het geval ze even niet werken, of iemand anders uw apparaat in geval van nood moet kunnen gebruiken.

10. Wachtwoorden opslaan



Met voor elke dienst een eigen code is de lijst met wachtwoorden lang. Te lang om te onthouden. Er zijn een paar manieren om wachtwoorden te bewaren op de pc.

De veiligste manier is met een wachtwoordmanager. Dat is een programma dat wachtwoorden onthoudt en zelfs voor u invult. U onthoudt alleen nog het hoofdwachtwoord om het programma mee te beveiligen. Een (gratis) voorbeeld daarvan is [LastPass](#).

Wie het niet fijn vindt al zijn wachtwoorden aan een derde partij te geven, kan de codes bijhouden in een Word-bestand dat u [beveiligt met een wachtwoord](#). Om de lijst te raadplegen, hoeft u dan nog maar één wachtwoord te onthouden, in plaats van allemaal. Nadeel: Crasht de computer, dan bent u alles kwijt. Zorg dus voor een goede [back-up](#).

Bronnen:

- *Seniorweb*
- *Google*