



# Vijf stappen naar veilig gebruik van wachtwoord

## Stap 1: Kies een veilig wachtwoord

Hoe kies ik een veilig wachtwoord?

### ► Gebruik lange wachtwoorden

Een sterk wachtwoord bevat tenminste 8 karakters. U kunt ook een wachtzin gebruiken, zoals bijvoorbeeld 'Dankzij e-mail gebruik ik zelden de telefoon!'. Een wachtzin met een mix van gewone letters en hoofdletters, maar ook cijfers en bijzondere leestekens, maakt een wachtzin nóg moeilijker te kraken.

### ► Gebruik geen namen of standaardwoorden

Hackers maken gebruik van standaard woordenlijsten. Deze namen worden onder andere opgezocht middels social media. Daarbij kunt u denken aan uw favoriete voetbalclub, huisdier of vakantiebestemming.

Gebruik op een tablet / smartphone nooit standaard pincodes zoals:

1234, 0000, 2580, 1111, 5555, 5683, 0852, 2222, 1212, 1998.

### ► Gebruik bijzondere tekens en cijfers

Door bijzondere tekens te gebruiken wordt het voor een hacker lastiger om een wachtwoord te kraken. U kunt allerlei leestekens gebruiken, maar bijvoorbeeld ook spaties.

### ► Wachtwoord niet 'ophogen'

Sommige diensten verplichten om een wachtwoord periodiek te wijzigen. Door simpelweg het getal in het wachtwoord op te hogen wordt het voor een hacker eenvoudig een wachtwoord te achterhalen aan de hand van een verlopen wachtwoord. Dus niet: "AppleiPhone34" naar "AppleiPhone35".

### ► Laat een wachtwoord genereren

Op het internet zijn diverse websites waar u eenvoudig een wachtwoord kunt laten genereren. Bijvoorbeeld via <https://identitysafe.norton.com/nl/password-generator>.

## Stap 2: Gebruik verschillende wachtwoorden

Gebruik nooit hetzelfde wachtwoord voor meerdere diensten. Wanneer uw wachtwoord bekend wordt bij derden dan kunnen zij dat wachtwoord uitproberen op andere websites. Op die manier krijgen onbevoegden in één klap toegang tot verschillende diensten of bijvoorbeeld uw e-mail.

## Stap 3: Houd een wachtwoord voor uzelf

Wachtwoorden zijn voor persoonlijk gebruik. Deel uw wachtwoord daarom nooit met anderen. Laat het ook niet rondslingeren op bijvoorbeeld een post-it, beeldscherm of in een bureaulade. Typ uw wachtwoord ook niet zomaar overal in wanneer daar om gevraagd wordt.

## Stap 4: Verander wachtwoorden regelmatig

Het is raadzaam om uw wachtwoord regelmatig te veranderen. Op deze wijze is het voor anderen moeilijker om het te weten te komen. Hoe vaak u het wachtwoord wijzigt kunt u zelf bepalen, maar het is verstandig dit een aantal keer per jaar te doen. Wanneer u het vermoeden hebt dat iemand uw wachtwoord heeft gezien of achterhaald, is het uiteraard nodig om het meteen te veranderen.

## Stap 5: Gebruik een wachtwoordkluis

Met allemaal verschillende wachtwoorden kan het gebeuren dat u er zoveel hebt dat het hoofd er vol van raakt en u ze dreigt te vergeten. In dat geval is wachtwoordsoftware een handig hulpmiddel.

Schouten Zekerheid maakt gebruik van de software KeePass. Deze wachtwoordkluis kan al uw wachtwoorden opslaan in één beveiligd bestand en laat wachtwoorden ook snel weer aanroepen als u ze nodig hebt. Wellicht ook handig voor uw organisatie?