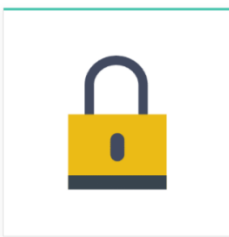


### Welke technieken gebruiken cybercriminelen?

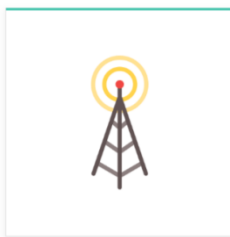
Cybercriminelen zijn mensen die het internet misbruiken om gebruikers op te lichten, hun computers te beschadigen of vertrouwelijke informatie van bedrijven of internetgebruikers te stelen. Dit zijn de middelen die ze gebruiken:



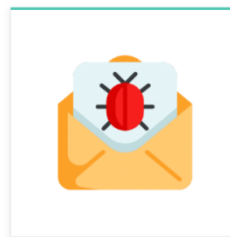
Virussen of malware installeren die de computer beschadigen



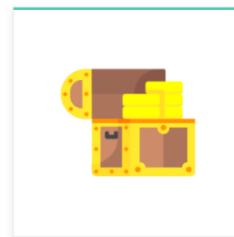
Binnendringen in onbeveiligde sites om zo persoonlijke informatie te stelen



Informatie stelen die door internetgebruikers op onbeveiligde wifi-netwerken is achtergelaten



Frauduleuze e-mails versturen



Internetgebruikers bedriegen door hen voorstellen te doen die te mooi zijn om waar te zijn



Zich voordoen als een familielid dat geld nodig heeft

### Hoe bescherm je je computer tegen aanvallen?

Installeer een **antivirusprogramma** (Windows defender, Avast enz.) en een firewall



**Werk geregeld** je programma's bij

### Welke regels moet je volgen om veilig te surfen?

1 Leer **betrouwbare** websites herkennen

The image shows a browser window with the URL `https://economie.fgov.be/nl`. Three callout boxes highlight parts of the URL: 'hangslot' points to the lock icon, 'https://' points to the protocol, and '.fgov.be' points to the domain. Below the browser window is the header of the 'economie' website, including navigation links like 'HOME', 'THEMA'S', 'NIEUWS', and 'PUBLICATIES', and a search bar.

## 2 Gebruik **veilige wachtwoorden**

Een wachtwoord is veilig als andere mensen het moeilijk kunnen achterhalen: het moet een lang woord zijn dat bestaat uit cijfers, letters en speciale tekens.

**i** In 2017 waren de meest 'gekaapte' wachtwoorden: *123456*, *wachtwoord*, *welkom*, *voetbal* enz.

3 **Meld je weer af** als je op een openbare computer hebt gewerkt en je daarbij op een account hebt aangemeld

4 Maak verbinding met een **beveiligd wifi-netwerk** om je bankzaken te doen

## Waaraan herken je frauduleuze e-mails?

---

Zo kun je frauduleuze e-mails herkennen:

- Het bericht komt van een **eigenaardig e-mailadres**
- Iemand vraagt je **geld te sturen om kosten te betalen**
- De e-mail bevat heel wat **spelfouten**
- Het bericht bevat **onrealistische dreigementen**
- Het bericht bevat een aanbieding **die te mooi is om waar te zijn**
- Iemand vraagt je om **persoonlijke gegevens op te sturen**



Markeer frauduleuze e-mails altijd als  
ONGEWENSTE E-MAIL.

Je hebt je online veiligheid grotendeels zelf in de hand! Wees voorzichtig met de persoonlijke gegevens die je op het internet achterlaat en volg altijd de bovenstaande veiligheidsregels. Zo voorkom je aanvallen van cybercriminelen.

**Leer nog meer op [123digit.be](https://123digit.be)!**