

**Masterclass Cybercrime**

Websites:

* [www.nomoreransom.org](http://www.nomoreransom.org)
* [www.digitaltrustcenter.nl](http://www.digitaltrustcenter.nl)
* [www.fraudehelpdesk.nl](http://www.fraudehelpdesk.nl)
* [www.ccinfo.nl](http://www.ccinfo.nl)
* [www.haveibeenpwnd.com](http://www.haveibeenpwnd.com)
* [www.politie.nl/checkjehack](http://www.politie.nl/checkjehack)

**VOOR IEDER ACCOUNT EEN ANDER WACHTWOORD!**

Een wachtwoord manager kan u hierbij helpen.

\*Apple gebruikers kunnen gebruik maken van de sleutelhanger functie (standaard aanwezig in het besturingssysteem.

\*Kijk welke wachtwoordmanager het beste bij u past, vele bieden extra’s welke u wellicht niet nodig hebt.

**Enkele bekende wachtwoord managers**

* Nordpass
* Proton Pass
* Dashlane
* 1password
* Bitwarden

Probeer privé en zakelijk gescheiden te houden, voornoemde managers gebaseerd op de cloud. Offline dus lokale oplossingen bestaan er ook.

**Ransomware /gijzelsoftware**

Alle bestanden mogelijk versleuteld, geen toegang meer tot de bestanden. Voorkomen?

* Maak backups, 90 dagen +
* Controleer de werking van de backup(s)
* Antivirus + updaten!
* Update systemen
* Zorg voor een noodplan
* Wees alert met het openen van bijlages in mail.
* Monitor de systemen op afwijkend gedrag, inloggen tijdens de nacht, vanaf afwijkende IP adressen (Buitenland) (enkele voorbeelden)
* ICT dienstverlener? Vraag hoe het is geregeld aangaande bescherming en in geval van nood!

Standaard antivirus kan ransomware mogelijk niet altijd detecteren! CDR, content disarm & reconstruction is andere techniek om u te beschermen TIP: [www.bodyguard.io](http://www.bodyguard.io)