Tip 2 – Maak een sterk wachtwoord

- ***9747*** *fraudegevallen in België met internetbankieren in 2018**
  ** cijfers Febelfin*

Een egel beschermt zichzelf tegen gevaar met zijn stekels. In de digitale wereld bescherm je jezelf ook best tegen gevaren. Niet met stekels, maar voornamelijk met een sterk wachtwoord! Zonder een sterk wachtwoord ben je als een egel zonder stekels: naakt! Anderen kunnen dan toegang krijgen tot je computer en je online accounts, zoals deze op Facebook, Office 365, Skype, Smartschool, Instagram, Twitter, …, enzovoort. Daarom verzamelen we op deze pagina enkele tips om sterke wachtwoorden te maken. Aan het werk!

Wat maakt dat een wachtwoord sterk is?

1. Een sterk wachtwoord is geheim. Zeg het dus tegen niemand.
2. Gebruik geen bestaand woord als wachtwoord omdat dit makkelijk te raden is.
3. Gebruik niet je eigen naam, die van je kind, partner of hond – Sociale media kent die allemaal
4. Gebruik een combinatie van letters, cijfers, hoofdletters, kleine letters en symbolen zoals @, € of ! Vermijd letters met een accent.
5. Bij verplicht gebruik van een hoofdletter: niet enkel de eerste letter; bij verplicht gebruik van een symbool: niet louter een uitroepteken achteraan. Dat konden de hackers ook bedenken.
6. Een langer wachtwoord is een sterker wachtwoord, gebruik minstens 10 tekens.
7. Gebruik verschillende wachtwoorden. Zo kan iemand die jouw wachtwoord te weten komt niet op al jouw accounts inloggen.
8. Geen mens kan al die wachtwoorden onthouden, gebruik daarom een wachtwoordkluis.
9. Schrijf je wachtwoord niet op zodat niemand het te weten kan komen.
10. Wijzig je wachtwoord regelmatig (en zeker bij vermoeden van een lek) of combineer met tweefactorverificatie (dan hoef je je wachtwoord niet frequent te wijzigen).
11. Activeer – indien beschikbaar – de tweefactorverificatie.

Hoe zorg je voor een sterk wachtwoord?

1. **Een wachtwoordzin als basis**
   Je kan sterke wachtwoorden makkelijker onthouden met dit trucje:
   - Denk aan een zin
   - Neem van elk woord de eerste letter
   - Maak van sommige letters een hoofdletter (bijvoorbeeld de belangrijkste woorden in jouw zin of de eerste letter van een naam)
   - Behoud de cijfers en leestekens.

   En zo is de zin “Een sterk wachtwoord heeft minstens 10 verschillende tekens.” het wachtwoord esWhm10!vt geworden. MzhCe=13jo! staat voor “Mijn zus heet Charlotte en is 13 jaar oud !”

   Voorbeelden van sterke wachtwoorden:
   - EsWhm10#t.
   - MzhCe=13jo!

2. **Laat het genereren door je wachtwoordkluis**
   Als Je gebruik maakt van een wachtwoordkluis, moet je eigenlijk alleen het wachtwoord van je kluis onthouden. Alle andere wachtwoorden laat je genereren door de software, je moet ze toch niet zelf onthouden.

   Je krijgt dan bvb. wachtwoorden zoals: z1OalH5eCdoNW0kjr98i

Over tweefactorverificatie (2FA/MFA) en wachtwoordkluizen organiseren we een gratis webinar op 25 februari 2021. Schrijf je in via je contactpersoon voor informatieveiligheid.

3. **Gebruik een combinatie van een vast en variabel deel**

Een sterk wachtwoord is een lang wachtwoord en verschilt per toepassing. Kies daarom een basis voor je wachtwoord en een stuk dat verandert per toepassing. Bvb.:

Mijn basis is: Blauwe&…..9Vinvis

Dat is op zich al een sterk wachtwoord (14 karakters, hoofdletters, kleine letters, cijfers en een speciaal teken. De puntjes vervang je nu per toepassing, maar wees ook daar creatief en vermeld niet letterlijk de toepassing, want ook dat bedenken hackers zelf.

- Voor de account op Hotmail zou je kiezen: Blauwe&mail9Vinvis
- Voor je Facebook: Blauwe&smoel9Vinvis
- Voor je account op het werk Blauwe&werk9Vinvis

Daarmee heb je een sterk en lang wachtwoord, overal verschillend en toch makkelijk te onthouden.

Help, mijn wachtwoord is gekraakt!

- Verander onmiddellijk jouw oude wachtwoord door een nieuw wachtwoord. Als je hetzelfde wachtwoord gebruikt voor andere websites, dan moet je ook die wachtwoorden veranderen.
- Lukt het niet om je wachtwoord te veranderen? Vraag een nieuw wachtwoord aan de website door op “wachtwoord vergeten?” te klikken.
- Controleer en wees aandachtig voor mogelijk ongewenste gebruik of aanpassing van je gegevens van de betreffende online account