fiscfree themaflits

On tour in cyberspace

Sterk staaltje wachtwoordcreatie

Wist je dat '123456' en 'qwerty' twee veelgebruikte wachtwoorden zijn? Die van jou zijn ongetwijfeld beter, maar bedenk: met de naam van je kanarie of poes kom je ook niet meer weg. Over het algemeen geldt: hoe meer tekens, des te beter.

Je wachtwoorden zijn de belangrijkste beveiliging van je privégegevens. Maar het zijn er zoveel! En je vergeet die krengen steeds! Daarom hier een tip voor het maken van sterke exemplaren, die je nog kunt onthouden ook. Je begint met één sterk, eenvoudig te onthouden wachtwoord. Voor al je andere wachtwoorden voeg je steeds een specifiek deel toe.

1. Kies een zin die je gemakkelijk onthoudt – het liefst inclusief cijfers en hoofdletters – en trek die samen. Voorbeeld: 'Ik ga 300 kilometer fietsen in Zuid-Frankrijk' wordt Ig300kfiZ-F. Dit wordt het vaste deel voor al je wachtwoorden.

2. Bedenk hoe je de naam van de service waarvoor je een nieuw wachtwoord maakt, in het vaste deel verwerkt. Bijvoorbeeld: je neemt telkens de tweede en een-na-laatste letter uit de naam van de service. Voor Facebook is dat dan ao en voor Netflix ei. Nog beter is het als je deze letters bijvoorbeeld een plekje opschuift in het alfabet: ao wordt bp, ei wordt fj. Gebruik deze lettercombinaties steeds op dezelfde plaats in het vaste deel van je wachtwoord. Vooraan, bijvoorbeeld. Het wachtwoord voor Facebook wordt dan bpIg300kfiZ-F en voor Netflix fjIg300kfiZ-F. Tadaa!

Ook zin in een nieuwe pc, laptop, tablet of een 2-in-1? Via je FiscFree®-account kun je er met belastingvoordeel eentje aanschaffen. Bekijk snel wat er allemaal mogelijk is.

Laat je niet hack maken

Je hoort en leest er regelmatig over, maar 'malware', 'ransomware', wat is het nu precies?

Malware (malicious (kwaadaardige) software) is bedoeld om toegang tot je computer te krijgen door je listig via mails en links bepaalde software te laten installeren. Die software houdt bij wat je op je computer doet en kan schade aanbrengen zonder dat je het merkt.

Ransomware vergrendelt de toegang tot een computer. De eigenaar kan er pas weer in als er losgeld is betaald. Cryptoware – een vorm van ransomware – versleutelt de data in een systeem, en alleen de auteurs van de ransomware hebben de sleutel om er weer bij te kunnen. Afdingen schijnt mogelijk te zijn bij het betalen van losgeld, maar voorkomen lijkt een beter idee.

Wat kun je doen om je computer zo goed mogelijk te beschermen? Gebruik goede beveiligingssoftware en wachtwoorden, stel updates niet uit – ook al zijn ze soms superirritant – wees alert op dubieuze e-mail, en vooral: maak regelmatig back-ups.

Laptop of tablet? Aaargh!

Eigenlijk heb je een nieuwe laptop nodig, maar ook zo'n kekke tablet lonkt... Hoe maak je nu de beste keuze? Kijk eens op www.consumentenbond.nl, daar zie je alle eigenschappen, voor- en nadelen van laptops en tablets overzichtelijk op een rij. Wil je helemaal niet kiezen? Ga dan gewoon voor een 2-in-1! Daarmee heb je het beste van twee werelden en veel meer gebruiksmogelijkheden dan bij een standaard laptop of tablet alleen. Door het toetsenbord los te koppelen of het scherm 360 graden om te klappen, komt bij een 2-in-1-laptop het touchscreen vrij. Zo heb je een tablet in een handomdraai!

Ik. Wil. Ook!