Tip 9 – Zeg nee tegen USB

USB-sticks zijn gegevensdragers die zowel in het privé- als beroepsleven gemakkelijk in gebruik zijn. Ze zijn zeer mobiel en ze kunnen worden aangesloten op alle computers waartoe je toegang hebt.

Maar net als alle andere gegevensdragers zijn ze evenwel kwetsbaar. De stick van iemand anders kan jouw computer besmetten. En als iemand anders jouw USB-stick heeft, kan hij er de gegevens afhalen. Door jouw USB-stick in een ander toestel te steken, kan ook je eigen USB-stick (en vervolgens jouw computer) besmet geraken.

Het is dus nuttig enkele voorzorgsmaatregelen in acht te nemen wanneer je toch een USB gebruikt. De juiste reflex:

- Beschouw elke stick die iemand je uitleent of die je vindt als verdacht.
- Scan een vreemde USB-stick steeds op virussen.
- Gebruik een gebruikersaccount op je computer, geen administratoraccount. Hierdoor wordt de besmetting beperkt tot de sessie van de gebruiker en wordt niet het volledige toestel (en netwerk) aangetast.
- Update je antivirusprogramma regelmatig.

Als je toch een USB gebruikt, vergeet dan zeker niet om de gegevens op de USB te beschermen!

- Beveilig je USB-stick met een wachtwoord en versleuteling zodat deze onbruikbaar is voor andere/externe personen mocht de USB-stick verloren geraken of kwaadwillig worden gestolen. Dit kan je in Windows 10 doen via het programma "***Bitlocker To Go***". In bijlage vind je een handleiding hoe je de beveiliging kan instellen en gebruiken.
- Breng gevoelige gegevens onder in een archief (bijvoorbeeld zip) met een paswoord.
  Er bestaat software om paswoorden van archieven te kraken. Om dit te vermijden, gebruik je best een paswoord dat voldoet aan de standaarden van de wachtwoordpolicy binnen jouw bestuur.

Er zijn alternatieven om bestanden op een veilige manier uit te wisselen. Vraag hiernaar bij de ICT dienst!