10 TIPS OM JE PRIVACY TE VERBETEREN

De bibliotheek doet er van alles aan om ervoor te zorgen dat jouw privacy gewaarborgd is. We nemen maatregelen om jouw gegevens zo veilig mogelijk te bewaren en zorgen ervoor dat onze apparatuur voldoet aan de veiligheidseisen. Maar er zijn natuurlijk ook zaken die jij zelf kunt doen! Tien tips om je gegevens te beschermen en jouw internetveiligheid te verbeteren

1

‘Ik heb niets te verbergen, ze mogen alles van me weten’

Fijn, maar is dat echt zo? Mag iedereen weten wat je verdient, waar je woont, wat je koopt, welke websites je bezoekt of waar je bent? Interessante informatie voor bedrijven om een goed beeld van je te krijgen en je gerichte advertenties te tonen. Hoe beter bedrijven je kennen, hoe groter de kans dat je geld uitgeeft aan hun producten. Ook al was je het niet van plan. Dus misschien is het toch beter om bepaalde informatie voor jezelf te houden!

2

Denk goed na wat je deelt over jezelf

In de privacywet staat dat bedrijven in de Europese Unie niet zomaar allerlei persoonsgegevens van je mogen verwerken. Maar toch krijg je soms de vraag om heel veel persoonlijke informatie te verstrekken. Denk goed na over welke gegevens je van jezelf invult.

3

Controleer regelmatig je privacy-instellingen

Voor veel sociale media, webshops en websites heb je een account nodig. Controleer bij het aanmaken de privacy-instellingen. Wie mag jouw berichten zien, wie mag er op reageren, wie mag je naam toevoegen aan berichten, welke gegevens mogen gebruikt worden voor reclame? Pas de standaardinstellingen aan naar je eigen wensen en controleer regelmatig of de instellingen nog steeds goed zijn. Sites en browsers veranderen de instellingen namelijk regelmatig.

4

Kies een sterk wachtwoord

Een goed wachtwoord hoeft niet ingewikkeld te zijn. Belangrijker is dat je wachtwoord lang is en per website verschilt. Gebruik bijvoorbeeld een zin of gebruik een ezelsbruggetje dat alleen voor jou logisch is. Gebruik geen gegevens die mensen op kunnen zoeken via bijvoorbeeld Facebook. Zoals jouw naam, die van je kinderen of je geboortedatum; allemaal zijn ze makkelijk te raden. Wist je dat 12345 het meest gebruikte wachtwoord is? Hoe veilig ben je dan?

5

Gebruik een wachtwoordmanager

Vind je het lastig om al die wachtwoorden te onthouden, gebruik dan een digitale kluis om je wachtwoorden in op te slaan. Een digitale kluis of wachtwoordmanager is toegankelijk via internet of via een app op je telefoon. Ze zijn uiteraard in hoge mate beveiligd en veel veiliger dan een opschrijfboekje. Kijk eens naar lastpass.com of dashlane.com

de Bibliotheek

6

Gebruik twee-factor authenticatie

Om extra veilig in te loggen bieden steeds meer websites de mogelijkheid om je account te beveiligen met een extra code. Deze code wordt, zodra je je gebruiksnaam en wachtwoord hebt ingetikt, naar je telefoon gestuurd. Bijvoorbeeld via een SMS of een appje. Deze code moet je weer intikken op de site waar je inlogt.
Je logt extra veilig in met het principe:

- iets wat je kent, een wachtwoord of pincode en
- iets wat je hebt, bijvoorbeeld je telefoon of
- iets wat je bent, bijvoorbeeld je vingerafdruk of gezichtsherkenning via de telefoon.

7

Pas op met het gebruik van openbaar Wifi

Als je ergens gebruik wilt maken van de openbare wifi, controleer het dan eerst. Kies bij voorkeur een wifipunt waar je een wachtwoord voor nodig hebt. Doe geen bankzaken of andere gevoelige zaken via een openbaar wifipunt. De kans bestaat dat een crimineel al je internetverkeer afluistert en misbruik maakt van jouw gegevens. Gebruik dan liever je mobiele data. En gebruik altijd de app van je eigen bank. Dat is veel veiliger dan bankieren via de browser.

8

Beveilig je gegevens

Om helemaal veilig te zijn kun je jouw internet-verkeer versleutelen via een Virtual Private Network (VPN). Dat is een programma of app die jouw internetverkeer versleuteld in geheimtaal. Daarmee kunnen anderen niet achterhalen wat je op het internet aan het doen bent, ook niet op een openbaar wifinetwerk. Een VPN kost geld maar het is zeer de moeite waard om te investeren in een abonnement van een paar euro per maand. Kijk eens bij NordVPN.com en Privateinternetaccess.com

9

Update en back-up

Installeer de laatste software- en beveiligings-updates op je computer, telefoon of tablet. En zorg dat je een kopie van jouw foto's, documenten en gegevens op een externe harde schijf of op internet (in de 'cloud') opslaat. Raak je je telefoon kwijt of gaat je computer stuk, dan heb je altijd nog je waardevolle gegevens op een andere plek.

10

Gebruik een zoekmachine die niets van je opslaat

Een zoekmachine als Google slaat heel veel gegevens van jou en je internetgewoontes op. Daarmee krijgt Google een goed beeld van wie jij bent en daar kunnen ze hun reclames en zoekresultaten beter op afstemmen. Ook verkopen ze jouw gegevens aan bedrijven. Twee zoekmachines die dat niet doen en alleen maar voor jou zoeken, zijn Duckduckgo.com en Startpage.com.

Succes! Heb je vragen of heb je hulp nodig, vraag het aan een medewerker in de bibliotheek!

Handige links
toolbox.bitsoffreedom.nl
veiliginternetten.nl
consumentenbond.nl/veilig-internetten

Zelf aan de slag?
Volg dan het stappenplan op data-detox.nl

Deze boeken raden we je aan:

- Je hebt wél iets te verbergen
  Maurits Martijn, Dimitri Tokmetzis
  Over het levensbelang van privacy
- Online veiligheid
  Consumentenbond, Dirkjan van Ittersum

de Bibliotheek