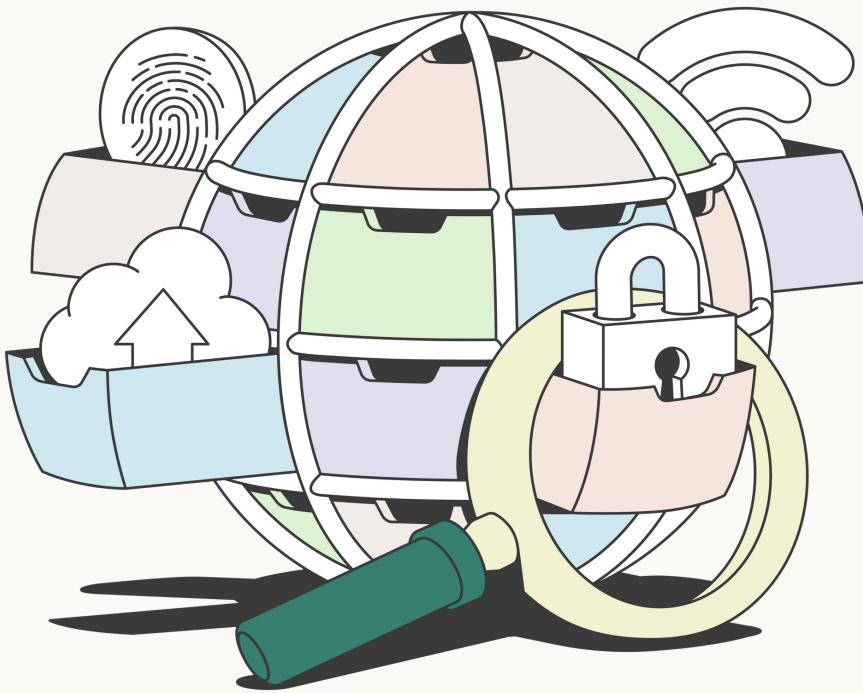




veiliginternetten.nl

5 основних порад для вашої безпеки онлайн



Купа застосунків та повідомлень. Надсилання фотографій та відеороликів через соцмережі. Відеодзвінки друзям і родичам. Переказ грошей через Tikkie чи банківський застосунок. Реєстрація в органах влади чи запис до лікаря через DigiD. Бездротовий друк, налаштування сигналізації чи опалення в будинку... Інтернет робить повсякденне життя набагато веселішим і простішим для багатьох людей.

І дуже важливо належним чином захистити всі свої пристрої та облікові записи. Це стосується всього: від смартфона до принтера, від Instagram до Gmail. Тому що так само, як і в реальному світі, злочинці, на жаль, активні також в Інтернеті. Дотримуючись цих п'яти порад, ви забезпечите свою базову безпеку онлайн. Таким чином, ви значно ускладните життя кіберзлочинцям.



veiliginternetten.nl

01 – Встановіть надійні паролі для всіх своїх пристроїв та облікових записів. Це означає:

- Чим довше, тим краще. Використовуйте ключову фразу.
- Використовуйте різні паролі для кожного облікового запису. І зберігайте свої паролі в менеджері паролів.
- За можливості використовуйте двофакторну автентифікацію.

03 – Використовуйте антивірусну програму

- Антивірус перевіряє ваш пристрій на наявність різного роду небезпек, таких як віруси, шкідливе програмне забезпечення та небезпечні застосунки.

02 – Завжди оновлюйте програмне забезпечення на своїх «розумних» пристроях

- «Розумний» пристрій — це той, що підключений до мережі Інтернет. Це можуть бути деякі принтери, радіоняні та дверні дзвінки. І навіть робот-пилосос.
- За допомогою оновлень виробники гарантують, що безпека ваших пристроїв залишатиметься на належному рівні. Тож не закривайте одразу ці спливаючі сповіщення про оновлення!

04 – Регулярно створюйте резервні копії

- Якщо вас зламають, ви можете втратити все. Тому задля впевненості робіть копії своїх файлів.

05 – Спочатку перевіряйте, а потім натискайте

- Інтернет-злочинці надсилають фальшиві посилання через електронну пошту, текстові повідомлення чи платіжні вимоги. Так вони намагаються переконати вас поділитися даними чи переказати гроші.