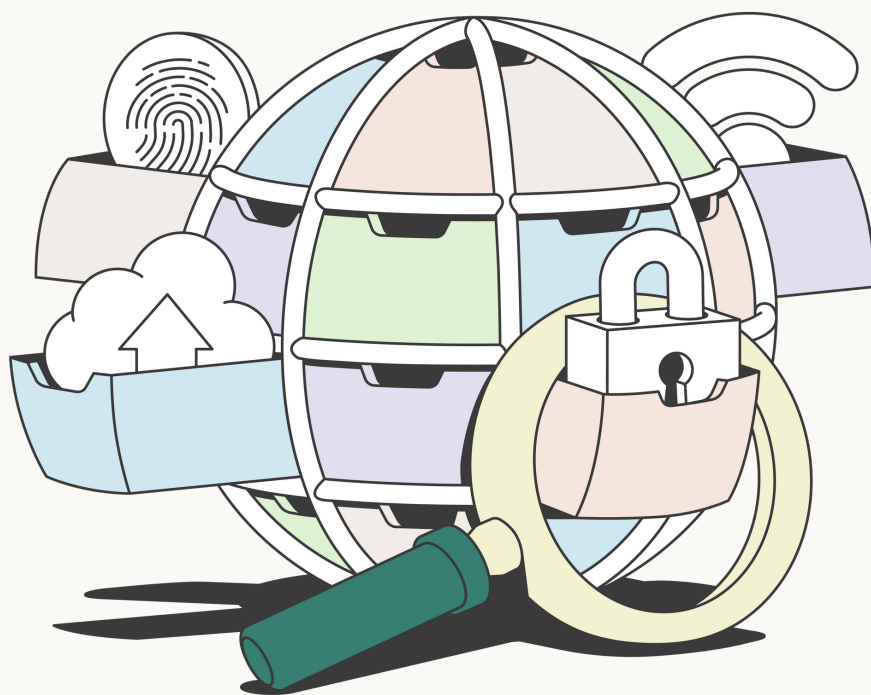




veiliginternetten.nl

5 podstawowych wskazówek dla Twojego bezpieczeństwa online



Tutaj apka, tam e-mail. Publikowanie zdjęć i filmów w mediach społecznościowych. Wideorozmowy z przyjaciółmi i rodziną. Przesyłanie pieniędzy za pośrednictwem Tikkie lub aplikacji bankowej. Logowanie się na stronach urzędów lub przychodni za pomocą DigiD. Drukowanie bezprzewodowe, sterowanie alarmem lub ogrzewaniem w domu... Internet sprawia, że codzienne życie wielu osób staje się nieco przyjemniejsze i łatwiejsze.

Ważnym jest, by dobrze zabezpieczać wszystkie swoje urządzenia i konta. Od smartfonu po drukarkę i od Instagrama po Gmail. Gdyż podobnie jak w świecie poza siecią, również w Internecie przestępcy niestety nie próżnują. Wykonując tych pięć działań, zadbasz o prawidłowe, podstawowe bezpieczeństwo w sieci. Utrudnisz w ten sposób działanie cyberprzestępcom.



veiliginternetten.nl

01 – Dbaj o stosowanie bezpiecznych haseł na wszystkich swoich urządzeniach i kontach. Oznacza to:

- Im dłuższe hasło, tym lepsze. Użyj hasła w postaci zdania.
- Używaj innego hasła dla każdego konta. Przechowuj swoje hasła w menedżerze haseł.
- Tam, gdzie to możliwe, korzystaj z logowania dwuetapowego.

03 – Używaj skanera wirusów.

- Skaner wirusów kontroluje Twoje urządzenie pod kątem jakichkolwiek problemów, takich jak wirusy, złośliwe oprogramowanie czy niebezpieczne aplikacje.

02 – Zawsze od razu aktualizuj oprogramowanie swoich urządzeń smart.

- Urządzenie smart to takie, które jest podłączone do Internetu. Może to być drukarka, niania elektroniczna czy domofon. Ale także odkurzacz automatyczny.
- Poprzez aktualizacje producenci dbają o to, by urządzenia były przez cały czas zabezpieczone. Nie zamykaj zatem okienek z prośbą o aktualizację!

04 – Regularnie wykonuj kopie zapasowe.

- W razie zhakowania możesz stracić wszystko. Dlatego też dla pewności wykonuj kopie swoich plików.

05 – Najpierw sprawdź, potem klikaj.

- Cyberprzestępcy wysyłają fałszywe linki za pośrednictwem e-maili, wiadomości tekstowych czy próśb o dokonanie zapłaty. W ten sposób próbują nakłonić Cię do udostępnienia im danych lub przekazania pieniędzy.