Digital Security
Progress. Protected.

REDLINE/META

Er is niets gedetecteerd

Fijn dat er niets gedetecteerd is! Los van dat feit is het belangrijk om de nodige voorzorgsmaatregelen te nemen en alert te blijven. In onderstaand stappenplan delen wij ons advies.

Stap 1: Houd je software up-to-date

Zorg ervoor dat al je programma's, zoals je besturingssysteem (bijv. Windows of macOS), je browser, en je beveiligingssoftware altijd de nieuwste versies hebben. Dit kun je makkelijk doen door automatische updates aan te zetten.

Stap 2: Installeer antivirus en anti-malware software

Zorg dat je een goede antivirus-oplossing hebt, zoals die van ESET of een andere betrouwbare leverancier. Deze gaat automatisch op zoek naar dreigingen en waarschuwt als er iets misgaat. Zo'n programma kan meteen ingrijpen als er iets verdachts gebeurt.

Stap 3: Gebruik sterke wachtwoorden

Gebruik geen eenvoudige en korte wachtwoorden. Kies voor wachtzinnen die veiliger en makkelijker te onthouden zijn. Gebruik ook verschillende wachtwoorden voor elk account. Een wachtwoordmanager kan je helpen om makkelijk sterke wachtwoorden te genereren.

Stap 4: Zet tweefactorauthenticatie (2FA) aan

Tweefactorauthenticatie (2FA) is een extra beveiliging voor je accounts. Zelfs als iemand je wachtwoord weet, hebben ze ook nog je telefoon of een speciale code nodig om in te loggen.

Stap 5: Gebruik een firewall en VPN

Overweeg om een firewall aan te zetten (dit is als een soort onzichtbare muur die slechte dingen buiten houdt) en gebruik een VPN als je vaak openbare wifi gebruikt (zoals in een café of op school). Hiermee wordt je internetverbinding versleuteld en veiliger.

Lees meer over Infostealers