Digital Security
Progress. Protected.

REDLINE/META

Nothing has been detected

Great news! No threats were detected! However, it's still important to take necessary precautions and stay alert. Below are some steps we recommend.

Step 1: Keep your software up-to-date

Ensure all your programs, including your operating system (e.g., Windows or macOS), browser, and security software, have the latest versions. This is easy to maintain by enabling automatic updates.

Step 2: Install antivirus and anti-malware software

Ensure you have reliable antivirus protection, like ESET or another trusted provider. This software will automatically search for threats and alert you if something goes wrong. It can immediately respond if anything suspicious occurs.

Step 3: Use strong passwords

Avoid simple and short passwords. Choose passphrases that are safer and easier to remember. Use different passwords for each account. A password manager can help you easily generate strong passwords.

Step 4: Enable two-factor authentication (2FA)

Two-factor authentication (2FA) adds an extra layer of security to your accounts. Even if someone knows your password, they would also need your phone or a special code to log in.

Stap 5: Use a firewall and VPN

Consider enabling a firewall (like an invisible wall that keeps out bad elements) and use a VPN if you often use public Wi-Fi (like in cafes or schools). This encrypts and secures your internet connection.

Lees meer over Infostealers