Digital Security
Progress. Protected.

REDLINE/META

An infostealer has been detected

We understand that it can be confusing to know exactly what steps to take to protect yourself. This simple document aims to guide you with practical steps.

Step 1: Run a full scan

If a quick scan has detected malware (a virus or a dangerous program), we advise you to have your entire device thoroughly checked, which is called a "full scan."

Actions to take

- Open the Redline/META scanner and select "Full System Scan."
- Allow the program to examine everything, which may take a few moments.

Step 2: Change your passwords

If you are infected, we recommend changing all your passwords. This is crucial because the malware may have viewed or stored your passwords, giving someone else access to your accounts.

Actions to take

- Change passwords for critical accounts, such as email, banking, social media, and work accounts.
- Do this on another device, such as a phone or tablet, that is not infected. You want to avoid having your new passwords stolen again.
- Avoid simple and short passwords. Choose passphrases that are safer and easier to remember. Use unique passwords for each account.

Step 3: Monitor your bank and personal accounts

The malware might have attempted to steal your bank or credit card details. It's important to check for any suspicious or unfamiliar transactions.

Actions to take

- Log into your bank account and review your recent transactions.
- Look for payments or amounts you don't recognize.
- If you see anything suspicious, call your bank immediately to report it.
- Did you enter credit card or work account login details while your device was infected? Report this to the involved companies so they can take protective measures.

Step 4: Update your device and security software

Sometimes criminals exploit "holes" in outdated software to access your device. Updating your software (like replacing a lock after losing your key) closes these holes.

Actions to take

- Update your operating system (like Windows or Mac).
- Update your security programs to ensure they are always the latest version, which enhances protection.
- 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).

Step 5: Keep Monitoring Your Accounts

Even after the malware has been removed through a full scan, stay vigilant. Sometimes data can be used even after you think everything is safe.

Actions to take

- Regularly check your email, bank, and social media for suspicious activities like strange messages or transactions.
- Use a password manager to create and store strong passwords, so you don't have to come up with new ones each time and can easily use secure passwords.

Step 6: Contact an expert

If you're unsure about the complete removal or have sensitive information (like company data), it may be wise to consult an expert who can ensure security and identify hidden issues.

Actions to take

- Search online for a reliable IT expert or company specializing in malware removal.
- Request that they check and secure your system.