A HACKER'S SECURITY GUIDE // INFOGRAPHIC 07/08

BEEN HACKED? RESPONSE PROTOCOL

Account takeover, fraud, impersonation: what you do in the first hours defines how much damage you take. Follow this order.

1 **DON'T delete anything — preserve the evidence**

Don't delete or forward emails, messages, or any information about the incident. Keep everything that could serve as proof: screenshots, e-mails, conversations.

▼

2 **Report it as soon as possible**

File a report with the police department or prosecutor's office nearest you. A formal report enables the investigation and protects you if crimes are committed in your name.

▼

3 **Cut off the attacker's access**

Urgently change the compromised passwords and those of linked accounts (above all your main e-mail: everything else can be reset from there). Sign out of open sessions on all devices.

▼

4 **Contact the provider through official channels**

Use the service's form, support desk, or phone line. They'll ask for details to verify you're the owner: approximate creation date, frequent contacts, content of recent emails, folders and labels. On free services the response can take a while: be persistent.

>> WHAT NOT TO DO

[−] MISTAKES THAT MAKE EVERYTHING WORSE

- × Hiring a "hacker" to recover the account: it's illegal outside the provider's official channels, and it's usually just another scam
- × Forwarding or spreading the content of the incident
- × Waiting for the law to fix it on its own: the active role in your protection is yours

>> PREVENT TODAY TO RECOVER TOMORROW

TURN ON MFA | SET UP RECOVERY INFO | ADD A SECOND PROFILE ADMIN | BACK UP YOUR PROFILE (DOWNLOAD YOUR DATA)

THE RULE

Evidence first, report fast, new passwords now. In that order, without delay.