C

Cybercriminal: Meaning, Types, and How to Stay Safe

A cybercriminal is a person who commits crimes using computers, networks, or online services. Activities include account theft, online fraud, malware distribution, extortion, and unauthorized access. Criminals may work alone or specialize within a larger operation. Protecting yourself involves securing accounts, updating devi...

PUBLISHER
Gridinsoft Support

UPDATED
Oct 8, 2026

READ TIME
3 min

CONTENTS

In this guide

01 What does cybercriminal mean?
02 Common activities and roles
03 How an ordinary account becomes a target
04 Cybercriminal vs. hacker
05 Practical protection
06 What to do if you are affected

Quick answer: A cybercriminal is a person who commits crimes using computers, networks, or online services. Activities include account theft, online fraud, malware distribution, extortion, and unauthorized access. Criminals may work alone or specialize within a larger operation. Protecting yourself involves securing accounts, updating devices, independently verifying financial requests, and reporting suspicious activity promptly.

01 What does cybercriminal mean?

Some offenses depend on technology: breaking into a server or disrupting a network requires a digital target. Others use technology to scale familiar crimes, such as fraud or impersonation. A cybercriminal does not need to write sophisticated malware. Someone who operates a fake shop, uses stolen credentials, or knowingly sells unauthorized access can participate without developing the underlying tools.

The label describes criminal conduct, not a particular appearance, nationality, age, or technical skill. Whether conduct constitutes an offense depends on the facts and applicable law. Security investigations should focus on observable actions and evidence rather than stereotypes about who an attacker might be.

02 Common activities and roles

- **Fraud operators:** impersonate suppliers, support teams, employers, or financial services to obtain money or information.
- **Credential thieves:** use phishing, information stealers, or reused passwords to take over accounts.
- **Initial access brokers:** sell access to already compromised systems to other criminals.
- **Malware operators and affiliates:** develop or deploy ransomware, spyware, or botnet software.
- **Infrastructure providers:** supply hosting, delivery services, or other resources for criminal campaigns.

- **Cash-out participants:** move proceeds through accounts or other payment channels. Suspicious jobs asking you to receive and forward money deserve scrutiny.

03 How an ordinary account becomes a target

Consider an illustrative invoice scam. A criminal obtains a supplier's email password, reads recent conversations, and sends revised bank details inside an existing thread. The message comes from a real account and may contain accurate project information. The decisive warning is an unexpected payment change, not necessarily a spelling mistake or unfamiliar sender.

Other campaigns are opportunistic. Automated systems try leaked credentials against many services or search for unpatched internet-facing software. A small business or individual can be affected without being personally selected. Reducing routine exposure is useful even when there is no evidence of a targeted campaign.

04 Cybercriminal vs. hacker

Hacker is a broader term that can include authorized security researchers and people who explore technology. Permission and behavior matter. A researcher testing within agreed scope is different from someone stealing data or demanding money after unauthorized access. A claim of research does not itself establish permission.

05 Practical protection

1. Use unique passwords and enable multifactor authentication, preferably phishing-resistant methods where supported.
2. Secure the email account and recovery methods used to reset your other accounts.
3. Install updates and remove unused remote-access software and browser extensions.
4. Confirm bank-detail and payment changes through a known contact method obtained independently.
5. Keep recoverable backups and test that important files can be restored.

6. Review sign-in notifications, account sessions, and unexpected changes to forwarding or recovery settings.

06 What to do if you are affected

Record the relevant messages, URLs, timestamps, transaction references, and account changes. Recover compromised accounts through their official process from a trusted device, revoke unknown sessions, and check recovery settings. If money was transferred, contact the payment provider immediately using a verified channel. Report the incident to the platform and the appropriate local police or national cybercrime reporting service. Do not send more money to someone promising guaranteed recovery.

Further reading: Europol on cyber-attacks and online fraud schemes. Related glossary: email attacks.

NEED MORE HELP?

We are here when the guide is not enough.

Visit the Gridinsoft Support Center for current product guidance or submit a support request with the details of your case.

Open this guide online at support.gridinsoft.com