

MINISTRY OF CYBER AFFAIRS

First 24 Hours



A two-page quick-start from The Investigator's Handbook.
Getting Evidence from Online Platforms, Services, Banks
and Providers

Independent publication. Ministry of Cyber Affairs is an independent news and information website. It is not a government body, police force, court, bank, service provider or recovery service, and this handbook is general information, not legal advice or an official instruction from any authority.

Free sample, Version 1.0, October 2026

Get the full handbook (more than 55,000 words, 9 chapters, glossary and templates) free at ministryofcyberaffairs.com/investigator-handbook

Please read first

Who we are. Ministry of Cyber Affairs is an independent news and information website. We are not a government body, police force, court, bank, provider or recovery service, and nothing in this handbook is an official instruction from any authority.

Not legal advice. The handbook describes processes as official sources describe them. Which legal power applies, and whether a request is sufficient, is decided by your prosecutor, legal adviser or court under the law of your country.

Contacts change. Every portal, email address, postal address and telephone number was checked on its official page on 18 October 2026. Companies and agencies change them without notice. Confirm on the official page before you serve legal process or send case material. Each entry links the page we checked.

Sources. Every chapter ends with the primary sources it relies on: official company and regulator pages, the text of laws and treaties, and published statistics. Each factual claim was rechecked by an independent reviewer against its source. If you find an error, tell us at <https://ministryofcyberaffairs.com/contact> and we will correct it and note the correction at <https://ministryofcyberaffairs.com/corrections>.

How this edition was made. AI tools helped research and draft the text. Every claim was then checked against its source and reviewed separately. See “About this handbook” for details.

Personal copy. This PDF was issued to registered readers. You may print it and share extracts within your agency with attribution. Please send colleagues to <https://ministryofcyberaffairs.com/investigator-handbook> so they receive updates.

© 2026 Ministry of Cyber Affairs. Version 1.0, October 2026.

First 24 hours: quick-start

Use this two-page checklist when a new online-fraud or threat case lands on your desk. It puts the steps in priority order: rule out danger to life, secure what you already hold, ask holders to preserve what they hold, move quickly on money, and then choose the right chapter. It describes common practice; follow your own agency's procedure and the law that applies to you.

Priority checklist

- ☐ **Step 1. Emergency test first.** Is there a significant and imminent risk to the life or safety of a person (the wording of [Article 3, paragraph 2.c, of the Second Additional Protocol to the Budapest Convention](#))? If yes, go to the emergency route of the service involved (see the [online-services directory](#)) before anything else. U.S. law lets a provider disclose to a governmental entity if it believes in good faith that an emergency involving danger of death or serious physical injury requires disclosure without delay ([18 U.S.C. 2702\(b\)\(8\) and \(c\)\(4\)](#)). The decision to disclose stays with the provider.
- ☐ **Step 2. Secure what the complainant holds.** Collect full URLs, usernames and account IDs, phone numbers, transaction references, messages and emails with their full headers. Record every date and time with its time zone. Work from copies and note how each item was obtained.
- ☐ **Step 3. Fix the integrity of each item.** Calculate a hash (for example SHA-256, defined in [FIPS 180-4](#)) and start a chain-of-custody record that shows who handled each item, where and when ([RFC 3227, section 4.1](#)).
- ☐ **Step 4. If a device is switched on, capture volatile data first.** RFC 3227 advises collecting from the most volatile to the least volatile source, starting with registers and cache, then routing tables and memory, temporary file systems and disk.
- ☐ **Step 5. Send preservation requests today.** Identify every holder (platform, host, telecom operator, bank, exchange) and ask each to preserve. See the table below for how long preservation lasts.
- ☐ **Step 6. Move on the money.** If funds left an account recently, the complainant's bank must be told at once. See "Money" below.
- ☐ **Step 7. Decide who must not be told.** Check whether the holder notifies its user when it receives legal process, and whether you can obtain a non-disclosure order. In the United States a court can order a provider not to notify any other person of a warrant, subpoena or court order for a period the court considers appropriate ([18 U.S.C. 2705\(b\)](#)).
- ☐ **Step 8. Open the case log.** Note every request sent, to whom, when and by what channel, so deadlines can be diarised.

How long does preservation last?

Instrument	Period	Source
U.S. Stored Communications Act, request by a governmental entity	90 days, extendable by one further 90 days on a renewed request	18 U.S.C. 2703(f)
Budapest Convention, domestic order (Article 16)	As long as necessary, up to a maximum of 90 days; a Party may provide for the order to be renewed	CETS 185

Instrument	Period	Source
EU European Preservation Order Certificate (EPOC-PR)	60 days, plus 30 more if extended, unless a production request follows. The Regulation applies from 18 August 2026	Regulation (EU) 2023/1543

KEY POINT. Preservation holds the data. It does not hand it over. You still need valid legal process for disclosure. Diarise the expiry date the day you send the request.

Money: act first, paperwork second

- Tell the complainant to contact the sending bank immediately and ask for a recall or reversal. The FBI's Internet Crime Complaint Center (IC3) says its Recovery Asset Team, set up in February 2018, liaises with financial institutions to help freeze funds sent to domestic accounts under fraudulent pretences ([IC3 D-FFKC process](#)).
- In India, the Ministry of Home Affairs describes the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS), launched in 2021 for immediate reporting of financial fraud, and the toll-free helpline 1930 ([PIB, 17 March 2026](#)).
- For every other country, use [Bank Fraud Help](#), [Mobile Wallet Fraud Help](#) and [E-commerce Fraud Help](#).

Decision table: what to do, and where to go next

The chapter references below are in-document links.

Your case involves	Do first	Open next
Threat to life, child safety or self-harm	Emergency test, then the provider's emergency route	Emergency template (Chapter 9) and Chapter 1
Money already sent	Bank recall request; national fraud helpline; preservation at the receiving institution	Chapter 6
An account on Google, Meta, WhatsApp, Apple, Snapchat, Microsoft or TikTok	Preservation request through the platform's official portal	Chapter 2
Any other messaging, cloud, hosting, gaming, travel or marketplace service	Find the service entry; check its emergency, preservation and user-notice lines	Chapter 3
An IP address only	Look up the holder with RDAP; ask for the source port and the exact UTC time, because networks may share one address among many customers (RFC 6302)	Chapter 5
A phone number or SIM	Identify the operator; preservation request to its legal contact	Chapter 5
Cryptocurrency	Record wallet addresses and transaction hashes; identify any exchange (VASP) involved	Chapter 7
Holder in another country	Check whether a 24/7 contact, direct request, executive agreement or mutual legal assistance applies	Chapter 4 and Chapter 1
Evidence the complainant holds (screens, files, devices)	Capture, hash and log custody before anything is changed	Chapter 8

Your case involves	Do first	Open next
You are ready to write a request	Use the preservation letter and cover sheet	Chapter 9 templates
You are not sure where to start	Secure evidence and send preservation requests, then read the process ladder	Chapter 1

Directories you will use today

- [LERS hub](#), [online services](#) and [country routes](#).
- [ISP directory](#) and [cyber agencies](#).
- [Investigators hub](#) and [Cybercrime Help](#) for the complainant.

WATCH OUT. Portals and addresses change. Confirm on the official page before you serve process. Contact only the channel a holder publishes. Never use informal or unofficial routes to obtain data.

Sources for this chapter

1. Legal Information Institute (Cornell), 18 U.S.C. 2702, Voluntary disclosure of customer communications or records (<https://www.law.cornell.edu/uscode/text/18/2702>), accessed 18 October 2026.
2. Legal Information Institute (Cornell), 18 U.S.C. 2703, Required disclosure of customer communications or records (<https://www.law.cornell.edu/uscode/text/18/2703>), accessed 18 October 2026.
3. Council of Europe, [Convention on Cybercrime \(ETS No. 185\)](#), Article 16 (<https://rm.coe.int/1680081561>), accessed 18 October 2026.
4. European Union, [Regulation \(EU\) 2023/1543 on European Production Orders and European Preservation Orders](#) (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R1543>), accessed 18 October 2026.
5. NIST, [FIPS 180-4, Secure Hash Standard](#) (<https://csrc.nist.gov/pubs/fips/180-4/upd1/final>), accessed 18 October 2026.
6. IETF, [RFC 6302, Logging Recommendations for Internet-Facing Servers](#) (<https://www.rfc-editor.org/rfc/rfc6302>), accessed 18 October 2026.
7. Legal Information Institute (Cornell), 18 U.S.C. 2705, Delayed notice (<https://www.law.cornell.edu/uscode/text/18/2705>), accessed 18 October 2026.
8. IETF, [RFC 3227, Guidelines for Evidence Collection and Archiving](#) (<https://www.rfc-editor.org/rfc/rfc3227>), accessed 18 October 2026.
9. FBI Internet Crime Complaint Center, [Domestic Financial Fraud Kill Chain \(D-FFKC\) Process](#) (<https://www.justice.gov/elderjustice/media/1364051/dl?inline>), accessed 18 October 2026.
10. Press Information Bureau, Government of India, [Indian Cyber Coordination Centre](#) (<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2241344®=3&lang=1>), 17 March 2026, accessed 18 October 2026.
11. Council of Europe, [Second Additional Protocol to the Convention on Cybercrime \(CETS No. 224\)](#), Article 3, paragraph 2.c (<https://rm.coe.int/1680a49dab>), accessed 18 October 2026.