



Plain-English Glossary

Every term Lumaset's free courses and guides use, explained simply, in one place.

A Lumaset Foundation reference • For every free course and guide

Who it's for: anyone who hits an unfamiliar word in a Lumaset lesson or guide. **Plain language, no jargon defining jargon.**

WHAT'S INSIDE THIS GUIDE

- 1 Scam tactics
- 2 Money & payment scams
- 3 Account & device security
- 4 Recovery & credit



Who we are

Lumaset Foundation is a nonprofit that helps everyday people stay safe and confident online. We make clear, plain-language lessons about spotting scams and using technology, and we keep everything 100% free, with no account and no catch. We are a registered 501(c)(3) charity based in Fort Wayne, Indiana.

Why we made this guide

Every Lumaset course and guide is written in plain language, but a few terms come up again and again across lessons. This is the one place to look any of them up, in the same plain language.

Jump to what you need:

Page 3 — Scam tactics (phishing, spoofing, deepfakes, and more)

Page 5 — Money & payment scams

Page 6 — Account & device security

Page 8 — Recovery & credit

Scam Tactics

Deepfake

A fake video, photo, or voice recording made with AI to look or sound like a real person saying or doing something they never did. Increasingly used in scams, including fake “family emergency” calls.

Phishing

A fake email or message designed to trick you into clicking a bad link or entering your login details on a fake site. The most common way accounts get hacked.

Pig Butchering

A long-con scam where a stranger builds a fake friendship or romance over weeks before introducing a fraudulent investment or trading app. See our free guide, [Fake Investment Offers & the Romance-to-Investment Trap](#).

Romance Scam

When someone builds a fake romantic relationship online, often over months, before asking for money, gift cards, or an “investment.”

Smishing

Phishing sent by text message (SMS) instead of email. Fake package, toll, or bank alerts are common examples.

Spoofing

When a scammer fakes the caller ID, email address, or sender name to make a message look like it's from your bank, a family member, or a real company.

Vishing

Phishing done by phone call (“voice phishing”). Fake bank fraud departments and fake tech support are common examples.

Money & Payment Scams

Chargeback

When your bank or card company reverses a payment and returns your money, usually because a charge was fraudulent or a purchase was never delivered.

Escrow

A neutral third party (often a freelance platform) that holds a client's payment until agreed-upon work is delivered, then releases it. Protects both the freelancer and the client.

Gift Card Scam

When a scammer instructs a victim to buy gift cards and read them the card numbers, which lets the scammer drain the value instantly, with no way to reverse it.

Wire Transfer

A direct bank-to-bank money transfer that lands almost instantly and generally cannot be reversed once sent, which is why scammers frequently request it.

Account & Device Security

Malware

Short for “malicious software.” Any program designed to damage, spy on, or take control of your device without your permission, often installed by clicking a bad link or attachment.

Passkey

A newer, more secure way to log in using your device's fingerprint or face scan instead of typing a password. Cannot be phished the way a typed password can.

Password Manager

A free tool (often built into your phone or browser) that creates and remembers a different strong password for every account, so you only have to remember one.

Ransomware

Malware that locks your files or device and demands payment to unlock them. Reputable sources (FBI, CISA) advise never paying, and backing up files regularly so this can't hold you hostage.

Spyware

Software secretly installed on a device to monitor what someone does, sometimes used by scammers, sometimes misused in unhealthy relationships. If you suspect it, a trusted tech helper or your device's official reset can remove it.

Two-Factor Authentication (2FA)

A second login step (a text code, an app, or a fingerprint) beyond your password. The single most effective everyday step against hacked accounts.

VPN (Virtual Private Network)

A tool that encrypts your internet connection, most useful on public Wi-Fi. Not required for everyday safety, but a helpful extra layer when traveling or using shared networks.

Recovery & Credit

Credit Freeze

A free lock you can put on your credit report so no one, including you, can open new credit in your name until you unlock it. The strongest protection after identity theft.

Data Breach

When a company's systems are hacked and personal information (like emails or passwords) is stolen. If a service you use is breached, change that password everywhere you reused it.

Fraud Alert

A free, lighter-weight flag on your credit report (compared to a credit freeze) that tells lenders to verify your identity extra carefully before opening new credit.

Keep learning, free.

This glossary is a companion to every free Lumoset course and guide. Whenever a lesson uses one of these words, it means exactly what's written here.

- **No account. No cost. No catch.** Ever.
- Start anytime at lumoset.org.
- Know someone who could use this? Please share it.

Help us reach one more person. Lumoset is a donor-funded 501(c)(3) nonprofit. If this helped you, you can help us teach someone else, free, at lumoset.org. Every gift keeps every lesson free.

Lend a hand. We are volunteer-powered. If you would like to help write, teach, translate, or share our free lessons, see lumoset.org.

For librarians, senior centers, and Area Agencies on Aging: please print and share this guide freely with the people you serve. That is exactly what it is for.

Did this help? Tell us at lumoset.org. Your story helps us reach more people, and shapes what we teach next.