Lumoset

FREE ONLINE-SAFETY EDUCATION

The 2026 Top 5 Scams in the US

The texts, emails, and calls fooling Americans right now, and how to stop each one.

A Lumoset Foundation guide · Part of the free Stay-Safe-Online series

Who it's for: anyone who wants to spot the scams fooling people right now, and know exactly what to do. **Plain language, no jargon.** A short read you can act on, and share with someone you want to protect.

WHAT'S INSIDE THIS GUIDE

Who we are

Lumoset 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

Scams are getting harder to spot, and they are hitting more people every year. Most of them work the same way: they rush you and scare you into acting before you think. We pulled together the five scams Americans are reporting most right now, explained in plain words, so you can recognize each one and know exactly what to do. Share it with anyone you want to protect.

> **Remember: Stop, and check it yourself using a phone number or website you look up on your own, never the one they gave you.**

Jump to what you need:

The “Unpaid Toll” Text

What it is. A text says you owe a small unpaid toll, often just a few dollars, and warns of late fees, a suspended license, or legal action if you do not pay right away. It includes a link.

How it works. The link opens a page that looks like a real toll agency and asks for your card number. Fake toll texts are one of the fastest-growing scams right now. In May 2026 the FTC reported that government-impersonation scams rose about 40%, driven in part by fake “overdue toll” texts, and researchers have tracked thousands of fake toll websites in many states. New versions are written by AI, so they read cleanly.

Example. You get a text: “You have an unpaid toll of $6.99. Pay now to avoid a $50 late fee.” But you have not driven a toll road, and real agencies do not collect this way.

Red flags

- A toll bill by text, with a link.
- A tiny amount paired with a big threat.
- A web address that is not your state toll agency's real site.

Do this now

1. Do not tap the link.

2. If you use toll roads, check your balance by typing your state toll agency's real website yourself, or call the number on a past bill.

3. Delete the text. Report it by forwarding to 7726 (which flags it to your carrier) and at reportfraud.ftc.gov.

Learn it free: Get confident spotting any scam in our free course, Spot the Scam. No account needed.

The Fake Renewal Invoice (Geek Squad, Norton, PayPal, McAfee)

What it is. An email or invoice says a subscription you do not remember is about to renew for a large amount, often around $499, and gives a phone number to “cancel” or “dispute” the charge.

How it works. Because you never bought it, you call to stop the charge. The person who answers is the scammer. They offer to “help” by remotely connecting to your computer, or by getting your card or bank login to process a “refund.” Best Buy's Geek Squad was the most-reported impersonated company in 2023, with about 52,000 reports, per FTC data released in May 2024. Some fake invoices even arrive through PayPal's real system, which makes them look genuine.

Example. An email from “Geek Squad Billing” says your $499.99 plan renews tomorrow, “call to cancel.” You never had a plan. The number goes straight to the scammer.

Red flags

- A charge for something you never bought.
- Pressure to call a number in the email to cancel.
- Anyone asking to remotely access your computer, or for your card “to refund you.”

Do this now

1. Do not call the number in the email.
2. Never let a stranger connect to your computer.
3. If you are worried it might be real, log in to that account yourself the normal way, or call the number on the company's official website.
4. Report it at reportfraud.ftc.gov.

Learn it free: Spot the Scam shows you how to check any suspicious message. Always free.

The “Family Emergency” Call (Grandparent & AI-Voice Scams)

What it is. A call or message says a grandchild or loved one is in trouble, in jail, in an accident, or stranded, and needs money right now. And you must keep it secret.

How it works. Scammers can now copy a familiar voice using AI from just a few seconds of audio, so it may truly sound like your family member. The FTC has warned that scammers use cloned voices in “family emergency” calls. The panic and secrecy are the whole trick, to stop you from checking.

Example. “Grandma, it's me, I've been in a wreck and I'm in jail. Please don't tell Mom. I need bail money by gift card.” The voice sounds right, but real emergencies do not come with “pay in gift cards” and “tell no one.”

Red flags

- Urgent trouble plus a demand for secrecy.
- A request for gift cards, wire transfer, cash, or cryptocurrency.
- “Don't tell Mom and Dad.”

Do this now

1. Hang up and call the person back on the number you already have for them.
2. Check with another family member.
3. Agree on a family safe word now, so you can always confirm it is really them.
4. Report it at reportfraud.ftc.gov.

Learn it free: Spot the Scam covers AI voice tricks and the safe-word habit. Free, no account.

The Fake USPS / Package Text

What it is. A text says your package cannot be delivered until you "update your address" or pay a small fee, with a link.

How it works. The link leads to a fake USPS page that steals your card number and personal details. These work because so many of us are always waiting on a package. The FTC and USPS have both warned about fake package texts.

Example. "USPS: your package is on hold. Update your address here: [link]." You do have something coming, so it feels real. But USPS does not text links asking for payment or personal details.

Red flags

- A delivery "problem" you did not expect, asking you to click.
- A request for payment or personal details to release a package.
- A web address that is not usps.com.

Do this now

1. Do not tap the link.

2. Track any real package by typing usps.com yourself, using the tracking number from your order.

3. Delete the text. Forward scam texts to 7726.

Learn it free: Learn to check any link safely in Spot the Scam. Always free.

The “Bank Fraud Department” Call (Zelle & Gift Cards)

What it is. A call, text, or pop-up says your bank found fraud and you must “protect” your money by moving it, sharing a code, or buying gift cards.

How it works. The scammer pretends to be your bank's fraud team and creates panic so you act before you think. The key truth: a real bank will never ask you to move money to a “safe account,” read them a one-time code, or pay in gift cards.

Example. “This is the fraud department. To protect your account, move your balance to the safe account we set up, and read us the code we just texted you.” That “safe account” is the scammer's.

Red flags

- Pressure to move money, send Zelle, or buy gift cards to “keep it safe.”
- Anyone asking for a one-time passcode you got by text.
- A caller ID showing your bank's name (this can be faked).

Do this now

1. Hang up.
2. Call your bank using the number on the back of your card.
3. Never share a one-time code, and never buy gift cards for anyone who calls.
4. Report it at reportfraud.ftc.gov.

Learn it free: Spot the Scam teaches the calm, verify-first habit that beats this. Free.

If You Already Paid or Shared Information

You are not alone, and it is not your fault. These scams fool careful people every day. What matters now is acting quickly, in this order:

1. Call your bank or card company right away to stop or try to reverse the payment.

2. Change the password on any account you shared, and turn on 2-step verification.

3. If you shared personal details, get a free, step-by-step recovery plan at **IdentityTheft.gov** (a free FTC service).

4. Report it at reportfraud.ftc.gov. For an older adult, you can also call the National Elder Fraud Hotline at 833-372-8311.

> **Remember: Reporting helps investigators stop these scams and warn others. Your report matters, even if you did not lose money.**

Keep learning, free.

This guide is a start. Our free course **Spot the Scam** walks you through spotting any scam, step by step, at your own pace. We also teach free courses on setting up email, protecting your accounts, and using technology with confidence.

• **No account. No cost. No catch.** Ever.

• Start anytime at lumoset.org.

• Know someone who would find this helpful? Please share it. That is how we protect more people.

Want to build your everyday online confidence too? Get our free guide, **Lumoset's Top 5 Digital Skills to Learn in 2026**, at lumoset.org.

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.