Millennials and financial fraud: Protecting yourself in a digital world

Fear of fraud is universal. Today, 77% of Americans are concerned about fraud and identity theft when managing finances online, according to 2025 research from Edward Jones and Morning Consult. Even more striking: 26% of Americans have personally experienced financial fraud.

While fraud is often associated with the elderly, millennials are among the hardest hit. Over one-fourth (28.6%) of millennials reported experiencing financial loss due to scams — more than any other generation, per 2024 research from PYMNTS Intelligence.

Here are common scams targeting millennials:

• *Cryptocurrency* – Promises of guaranteed profits or zero risk are red flags. Watch for Ponzi schemes and fake crypto launches.

• *Payment apps* – Watch for scammers impersonating someone you know or spoofing app emails to steal credentials.

• *Online shopping* – Beware of fake sites or ads selling trendy items at unrealistic prices.

• *Student loan forgiveness* – Scammers who offer debt relief for a fee just want your info or money.

• *Government* – IRS calls or texts about an unclaimed refund or an unpaid tax bill are scams. The IRS only contacts taxpayers in writing by U.S. mail.

• *Job and gig* – Avoid unusually high-paying online jobs requiring upfront purchases.

• *Romance* – Requests for money in online relationships are a major warning sign.

Stay vigilant. Learning to spot fraud matters. Be suspicious of these warning signs: unexpected windfalls, like contests you didn't enter; pressure to pay immediately or upfront; requests for payment via gift cards, wire transfers or crypto; or receiving a check and being asked to wire part of it back.

Also look out for spelling and grammar errors in emails and texts, fake social media profiles, requests to access your computer to "fix a problem" and unsolicited contact, especially from a bank, government agency or tech support.

Protect yourself. Some practices can help you stay safe. Use strong, unique passwords and different ones for different accounts. Use multifactor authentication (MFA) wherever possible; it can block unauthorized access. And before entering personal or financial information on a website, make sure the URL starts with https:// and shows a padlock icon. This means it's a secure site.

If you think you've been scammed, don't beat yourself up. Scammers are professionals who exploit human psychology. Anyone can fall victim. Here's what to do:

Act quickly. Contact your bank or payment company immediately to try to stop any payments in progress. Change your passwords and usernames right away if they may have been compromised. Run an antivirus scan on devices that might be affected.

Report the crime. File a report with the Federal Trade Commission at reportfraud.ftc.gov. For online fraud, also file a complaint with the FBI's Internet Crime Complaint Center (ic3.gov). These agencies can provide resources and connect you with law enforcement.

Protect yourself going forward. Monitor your credit reports regularly and consider freezing your credit with the credit agencies. Learn more ways to protect yourself at consumer.ftc.gov.

The digital world offers incredible convenience but also opportunities for criminals. Stay alert and know how to respond to help protect yourself and your financial future.

This article was written by Edward Jones for use by your local Edward Jones Financial Advisor. Edward Jones, Member SIPC.

499 words