

SEPTEMBER 2026

Build Your Scams Preparedness Plan



September is **National Preparedness Month**, a campaign that encourages families to prepare for natural and man-made disasters. Unfortunately, the aftermath of disasters is also when scammers try to make an unavoidable tragedy even worse. Ensure your preparedness plan includes ways to combat scams so that, in the wake of a disaster, you can stop fraud before it happens.

[CLICK HERE TO LEARN MORE](#)



Beware of Disaster Assistance Scams

After a natural disaster, scammers often move in just as quickly as officials. Be cautious of anyone claiming to represent the Federal Emergency Management Agency (FEMA) who asks for payment or personal information to process assistance. FEMA never charges application fees. Fake contractors may also knock on your door and demand payment upfront, pressure you to sign contracts or offer deals that seem too good to be true. Learn how to verify recovery officials below.

[CLICK HERE TO LEARN MORE](#)

Don't Fall for Tech Support Scams

Have you ever gotten a message that your computer has been infected with a virus? Criminals prey on your fear and pretend to represent a technology company or IT support service. Their goal is to convince you that your computer, smartphone or online account has a serious problem that requires immediate attention. Follow these tips to protect your personal information:

- Be skeptical of unsolicited calls, emails, texts and pop-up messages, especially if they claim your device has a problem.
- Never give remote access to someone who contacted you unexpectedly.
- Only seek technical support through a company's official website or customer service channels. Go to the physical store if you can.
- Keep your operating system, browser and software updated.
- Use long, unique passwords for every account and store them in a password manager app. You can compare top rated free apps [here](#).
- Enable multifactor authentication whenever it's available.

[CLICK HERE TO LEARN MORE](#)

Digital Security Check: Protect Online Accounts

Your online accounts contain valuable information, making them a prime target for scammers. One of the easiest ways to protect yourself is by updating your passwords. Long and unique passwords are the most secure, but even strong passwords will benefit from enabling multifactor authentication (MFA). Turn on MFA for any account that offers it, especially your financial accounts.

[CLICK HERE TO LEARN MORE](#)



Upcoming Events

Join us for an upcoming event and learn how to protect yourself from the latest scams. If your company or organization would like to schedule a presentation with one of our scam experts, click on "Request A Speaker" on our website.

[CLICK HERE FOR FULL CALENDAR](#)

Latest Scams in the News

- [Baptist Health warns patients of MyChart phishing scam](#)
- [Fayette Co. Sheriff's Office issues scam warning](#)
- [Glasgow police, multiple agencies, make arrest in financial scam with thousands of dollars stolen from victim](#)
- [Beware of back-to-school scams](#)
- [Jury duty and crypto scams back in Kentucky, KSP says](#)
- [Warren County Sheriff's Office warning of persistent arrest warrant scam](#)