

Tech Tuesday: Building a digital defense by knowing the top ten red flag fraud signs

May 24, 2022



TECH TUESDAY: Red Flag Fraud Signs

- Requests payment via gift cards, wire transfers, or virtual currency.
- Creates a sense of urgency or deadline to pay quickly.
- Demands secrecy from you.
- Poor grammar or misspellings.
- Payments offered in amounts higher than listed price.
- Email addresses disguised to seem legitimate.
- Unsolicited emails, texts, etc., requesting you confirm usernames and/or passwords.
- Requests to move to a new platform to communicate.
- Requests to access your personal bank account to pay you for a service.
- Unsolicited emails with links or attachments.
- Report fraud to www.ic3.gov.

 **FBI** FEDERAL BUREAU OF INVESTIGATION

Portland Field Office

Scammers never stop; they work around the clock to cash in on the latest scheme hoping to steal your money or your identity. You’ve heard many of their pitches: they pretend to be romantically interested in you, say they are a relative in trouble, or pretend to be collecting money for a charity after a natural disaster.

Soon, the cycle of fraud begins. When the FBI or another law enforcement or government agency issues a release about their scheme, they adapt and make enough changes to their pitch to convince the victims their claims are real. It’s time to crush their crime spree.

Think about it this way, “scams change, red flags don’t!” No matter what type of story you hear via email, text, phone, social media, by mail, or in person, scams change, but the below red flags don’t. Here are our top ten signs the person you are communicating with is trying to scam you. The person;

Requests payment via gift cards, wire transfers, or virtual currency.

Creates a sense of urgency or deadline to pay quickly.

Demands secrecy from you.

Poor grammar or misspellings.

Payments offered in amounts higher than listed price.

Email addresses disguised to seem legitimate.

Unsolicited emails, texts, etc., requesting you confirm usernames and/or passwords.

Requests to move to a new platform to communicate.

Requests to access your personal bank account to pay you for a service.

Unsolicited emails with links or attachments.

No matter what type of story someone is telling you, as always, if it sounds too good to be true, it probably is.

If you believe are a victim of an online scam, you should report the incident to the FBI's Internet Crime Complaint Center at www.ic3.gov or call your FBI local office.