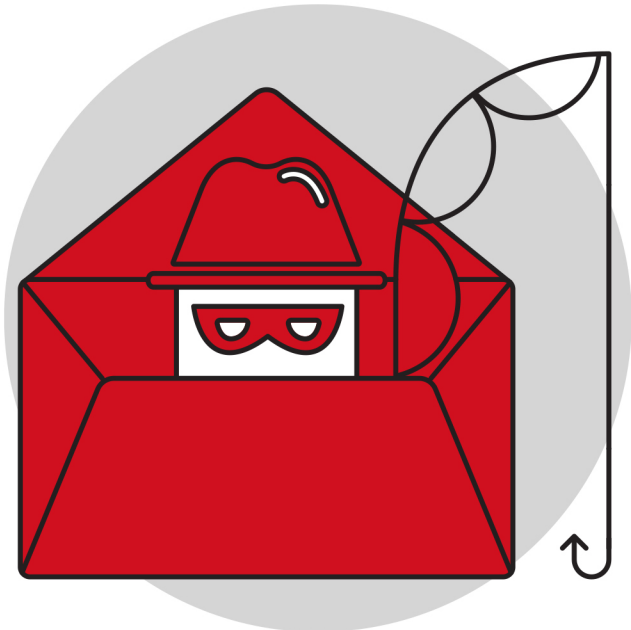
HOW TO AVOID

CYBER SCAMS



THE SCAM:

SMISHING– SCAM BY TEXT

Thieves use fake text messages to cell phones containing “urgent” messages about credit cards or bank accounts, contest prize notifications, fake survey links and messages from trusted brands. All these scams ask you to verify your identify or provide sensitive personal information.

HOW TO AVOID

- Look for noticeable grammar or spelling errors.
- Links provided in messages are slightly off (e.g., ama.zon.com vs amazon.com).
- Verify all messages you receive, even if it’s from a company you buy from often to ensure that the contact is genuine. Just like URLs and emails, phone numbers can be faked, so it’s important to double check.

THE SCAM:

PEER-TO-PEER PAYMENT APPS

Look out for application fraud with strangers signing up for apps pretending to be you and pulling money from your account. The "accidental transfer of funds" scam has hackers using stolen bank cards to transfer money to unsuspecting users. If you send the money back to the scammer to refund them, they will delete the stolen credit card from their account and add their own card in its place.

HOW TO AVOID

- Carefully review all payment requests before hitting accept.
- Ignore requests to return accidental deposits.
- Disable incoming requests on your app and only use the app to send money.
- Report any incidents immediately to the app's support team.

THE SCAM:

I.R.S. CALLS FOR YOUR S.S. NUMBER

Scammers call, email, text or reach out via social media pretending to be from the Internal Revenue Service. They request your social security number or other personal information related to taxes, stimulus checks or another claim that you owe the IRS money.

HOW TO AVOID

- Hang up on any phone calls and delete messages that ask for your S.S. number.
- Call an authorized IRS representative to verify whether the agency is trying to reach you. The IRS typically initiates contact with taxpayers through U.S. mail, so chances are, a phone call is not legitimate.

THE SCAM:

RANSOMWARE

Ransomware is malicious software that infects a computer and restricts a user's access until a ransom has been paid. This scam impacts both individuals and businesses. For individuals, the requested amount usually ranges between $200 and $400 and must be paid in a virtual currency like Bitcoin.

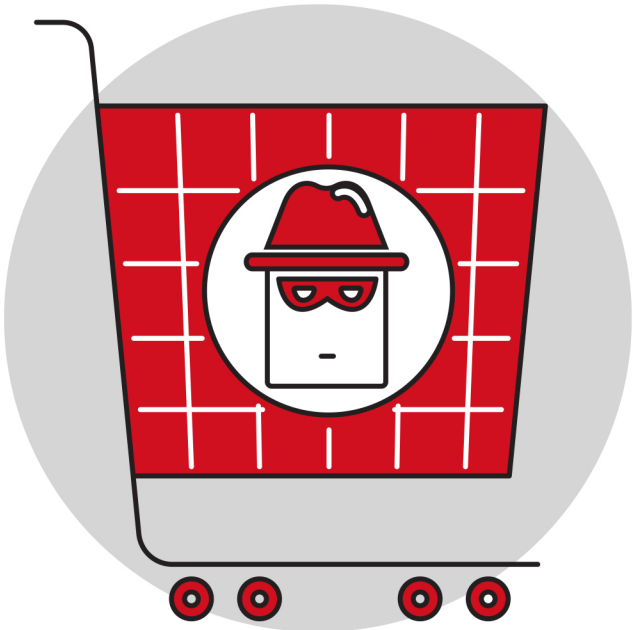
HOW TO AVOID

To avoid ransomware:

- Make sure you have updated security systems, including anti-virus software, on your devices.
- Don't click unsolicited web links in emails.

If you are a ransomware victim:

- Immediately disconnect from networks and external devices.
- Don't pay the ransom as this doesn't guarantee the release of your data.
- Contact your local FBI field office to request assistance and submit a tip online.



THE SCAM:

ONLINE SHOPPING FRAUD

In addition to phishing emails, online shoppers need to be aware of fake e-retailers with bargain basement discounts. Some deliver shoddy merchandise while others don't deliver anything at all. Some will even send email coupons with malware that infects your computer and steals your data.

HOW TO AVOID

- Look for website URLs and links with extra words or characters or that are poorly written.
- If the customer service representative uses a Yahoo or Gmail account address, it's likely fake.
- Use trusted retail websites instead of shopping with a search engine.

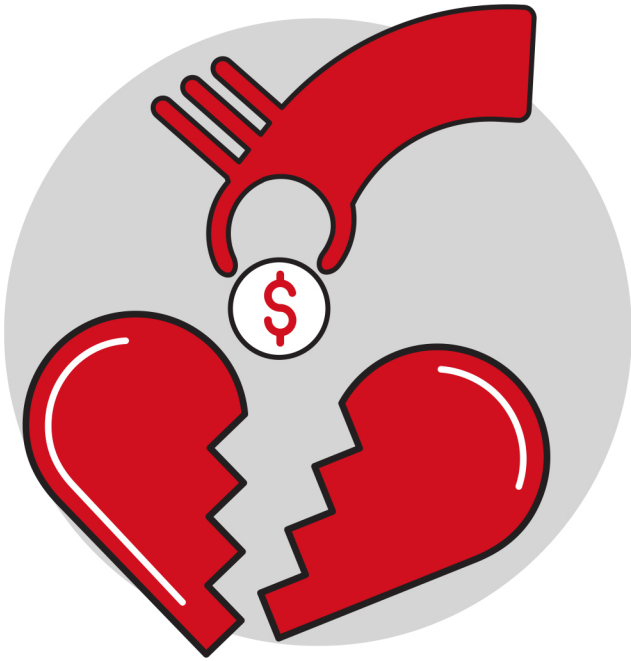
THE SCAM:

GET RICH QUICK SCHEMES

High school and college students are the main targets for schemes that promise financial aid or fake scholarships. Faux arts and literature contests that lure work submissions for a fee are also common, but students end up never seeing their work published. Acting and modeling gig scams that claim “talent scouts” are searching for the next star require upfront payment for headshots or acting lessons.

HOW TO AVOID

- Search reputable art and literature publications and websites for genuine opportunities to showcase your work.
- Walk away from any scholarship, job or contest that requires you to pay upfront.



THE SCAM:

ONLINE ROMANCE GONE WRONG

Thieves use fake text messages to cell phones containing “urgent” messages about credit cards or bank accounts, contest prize notifications, fake survey links and messages from trusted brands. All these scams ask you to verify your identify or provide sensitive personal information.

HOW TO AVOID

- Always verify people’s identities by cross-checking other sites.
- Beware of anyone who professes love too quickly or claims to be from the U.S. but is “overseas” for business or military service.
- Watch for anyone who tries to lure you off a dating site to communicate via phone or email – or worse yet, in-person.