



**RED FLAG
WEEKLY**

FREE GUIDE

TOP 5 CYBER THREATS MOST PEOPLE IGNORE

Learn how scammers target your data, and the simple steps that keep you safe. Plain English. No tech skills needed.

HOW TO USE THIS GUIDE

Each threat has three parts: what it looks like, the red flags to spot, and what to do. Read one a day. Share it with someone you love.

THREAT 1 OF 5

FAKE DELIVERY & TOLL TEXTS

A text says your package is stuck or you owe a small toll. It links to a site that looks official and asks for a few dollars.

RED FLAGS TO SPOT

- Comes from a random 10-digit number or an email address
- Tiny, oddly specific amount with a late-fee threat
- Link ends in odd endings like .top, .xyz or .info

WHAT TO DO

- Don't tap the link. Open the carrier's or toll agency's app yourself
- Forward the text to 7726 (SPAM), then delete it
- Paste any link into the scanner at redflagweekly.com/scanner

THREAT 2 OF 5

BANK ALERT PANIC

An email, text or call says your account is locked or a big charge just went through. It pushes you to act right now.

RED FLAGS TO SPOT

- Sender address doesn't match the bank's real website
- Countdown pressure: "24 hours or your account closes"
- Asks for your PIN, full SSN, or a one-time code

WHAT TO DO

- Hang up or close the message. Call the number on the back of your card
- Never read a one-time code to anyone. Your bank will never ask
- Turn on alerts in your real banking app

THREAT 3 OF 5

FAKE INVOICES & TECH SUPPORT

A "renewal" bill for hundreds of dollars from Geek Squad, Norton, PayPal or Amazon. Call to cancel and they ask to connect to your computer.

RED FLAGS TO SPOT

- Bill comes from a free Gmail or Outlook address
- A charge you never made, with a phone number to call
- They want remote access or gift-card payment

WHAT TO DO

- Log in to the real account yourself to check charges
- Never let a stranger control your computer
- If you already did: disconnect from the internet and call your bank

THREAT 4 OF 5

QR CODE TRAPS ("QUISHING")

Fake QR stickers on parking meters, posters or letters send you to a lookalike payment page.

RED FLAGS TO SPOT

- Sticker placed over the original code
- The web address shown doesn't match the business
- Asks for card details just to "verify"

WHAT TO DO

- Pay with the official app or at the machine
- Preview the link before opening it
- Report tampered stickers to the business or city

THREAT 5 OF 5

AI VOICE CLONES

A call that sounds exactly like your child, grandchild or boss. They're in trouble and need money now, and say "don't tell anyone."

RED FLAGS TO SPOT

- **Extreme emergency plus secrecy**
- **Payment by wire, crypto or gift cards**
- **Caller avoids questions only the real person would know**

WHAT TO DO

- Hang up and call the person back on their known number
- Set a family code word today
- Never send money while someone is pressuring you on the line

STAY AHEAD EVERY WEEK

Scammers change tactics every week. Red Flag Weekly sends a short Red-Yellow-Green alert to your inbox so you know what to watch for, in plain English.

Already subscribed? Watch your inbox every week. Know someone who'd fall for one of these? Send them to redflagweekly.com.