

Current Scam Trends

- **Gift Card & Executive Impersonation**
Unexpected requests from colleagues, supervisors, or executives to purchase gift cards or provide personal information.
- **“Too Good to Be True” Deals**
Fake ads, coupons, and promotions offering steep discounts on merchandise.
- **Unsolicited Job Offers**
Roles such as “secret shopper” or “personal assistant” that often lead to financial fraud.
- **Fake Shopping Websites & Apps**
Malicious sites or mobile apps mimicking legitimate retailers to steal payment details.
- **Phony Charitable Appeals**
Social media posts or emails soliciting donations for fraudulent causes.
- **AI-Generated Phishing & Deepfake Voice Calls** *(New in 2025)*
Attackers using AI to craft convincing emails or voice messages impersonating trusted individuals.
- **QR Code Scams** *(New in 2025)*
Malicious QR codes in emails, flyers, or ads redirecting to credential-harvesting sites.
- **Account Takeover via MFA Fatigue** *(New in 2025)*
Attackers bombarding users with repeated MFA prompts to trick them into approving fraudulent access.

How to Protect Yourself

- **Recognize and Avoid Scams:**
Review [Avoiding and Reporting Scams | FTC](#).
- **Practice Safe Online Shopping:**
See tips from [‘Tis the Season to Be Skeptical - Shopping Online Securely | SANS Institute](#) and [Shop Safely This Holiday Season | CISA](#).
- **Verify Authenticity:**
Always confirm the sender’s identity, especially for messages marked as external.
- **Be Extra Cautious on Mobile:**
Mobile email clients may hide full sender addresses—double-check before responding.
- **Enable Strong Authentication:**
Use multi-factor authentication (MFA) with app-based or hardware token verification.
- **Avoid Suspicious Links & Attachments:**
Never click unsolicited links or download unknown files.
- **Check URLs Carefully:**
Compare email links to actual destination URLs before clicking.
- **Stay Informed:**
Refer to advisories at <https://security.cuny.edu> under “CUNY Issued Security Advisories.”

If You Suspect a Scam or Malware

- **Report Immediately:** Contact the college’s [Service Desk](#).
- **Notify Your Bank:** Alert your financial institution if account details may be compromised.
- **Change Passwords:** Update any exposed credentials and avoid reusing old passwords across accounts.