Cyber Directorate
U.S. Army Criminal Investigation Division

Cybercrime Prevention Flyer

CPF 00020-2022-CID361 **1 July 2022**

Test Your Scam Knowledge

Each year, scammers target thousands of Americans in cyber-enabled scams. Recent Federal Trade Commission and Internet Crime Complaint Center reports separately show that victims were defrauded for approximately $5.8 billion and $6.9 billion last year.

Scam tactics evolve over time, but the basic elements remain the same. The best defense to combating scammers is being able to identify a scam. Take a minute and test your knowledge on these scam flags and definitions.

Charity	**Credit Card**	**Employment**	**Government**
Housing/Rental	**Investment**	**Non-delivery**	**Phishing**
Romance	**Smishing**	**Subscription**	**Tech Support**

1. ___________________ is a form of fraud in which the scammer represents themselves to be a real business or person in an email or other electronic message to gain private information.
2. ___________________ scammers use deception to steal money from people who believe they are supporting legitimate causes.
3. ___________________ scams usually begin on an online dating site or through social media contact.
4. Disguised as originating from a streaming service or a phone/internet/cable provider requesting payment detail updates, messages in ___________________ scams instead contain malicious links to steal the user's personal information.
5. ___________________ is very similar to phishing via email, except the message is received on a smartphone as a Short Message Service (SMS) message, also known as a text.
6. A common tactic of ___________________ scams is to send a job applicant a check to purchase equipment online, and then request a refund of remaining funds.
7. ___________________ fraudsters pose as telemarketers or financial advisors and promise victims high returns if they entrust them with an initial down payment.
8. Preying on the target's limited technical knowledge, ___________________ scams solicit payment for computer repair services for nonexistent problems.
9. Criminals advertise fantastic deals to target homebuyers and renters in ___________________ scams.
10. ________________ imposters pose as the Social Security Administration, the IRS, or Medicare to target victims.
11. The promise of an approved line of credit with no credit check in exchange for an upfront fee is a hallmark of __________________ scams.
12. In a __________________ scam, a buyer makes an online purchase, but never receives the goods or service. The seller may end all communication or continue to request additional funds for customs or shipping costs.

The answers are available at the bottom of the next page.

Report a crime to U.S. Army Criminal Investigation Division

Cyber Directorate
27130 Telegraph Road
Quantico, Virginia 22134

Email

Cyber Directorate Web Page

CID LOOKOUT
ON POINT FOR THE ARMY

Distribution:
This document is authorized for the widest release without restriction.

"Do What Has To Be Done"

How to Prevent from Becoming a Victim

Charity: Always research a charity before donating. The Internal Revenue Service's Tax Exempt Organization Search Tool can help verify an organization's legitimacy.

Credit Card: If established companies would not issue you credit, do not believe it would be that easy through another source. Research the issuer and never pay an upfront fee for a credit card.

Employment: Research the job offered and find the ad directly on the company's website. Being asked to deposit a check or transfer funds for training or some other reason is a red flag.

Government: A real government agency will never request gift cards, a wire transfer, or cryptocurrency as a means of payment.

Housing/Rental: These scams target both buyers and renters. Be suspicious if the owner or agent requires a signed lease or fee before seeing the property. One of the biggest red flags is insisting payment via a wire transfer or cryptocurrency.

Investment Never rush into an investment opportunity. If a customer is rushed or told not to discuss the investment with others, they are being scammed.

Non-delivery: When possible, make online purchases using a credit card. In case of an issue, credit card charges can be disputed to recover the funds.

Phishing/Smishing: Remember that companies, financial institutions, government organizations and online shopping sites will not contact you via email or text message to ask for your username, password, or personally identifiable information.

Romance: Check photos an online love interest sends for inconsistencies. Do a reverse image search of the person's profile picture to see if it's associated with another name or with details that don't match up.

Subscription: Do not click the link in a renewal message. Go to the service's website directly to check your account and make updates if necessary.

Tech Support: If you get a phone call you did not expect from someone who says there is a problem with your computer, hang up. Legitimate tech companies will not contact you by phone, email, or text message to tell you there is a problem with your computer.

Resources:

Common Scams and Crimes

Internet Crime Complaint Center (IC3)

Online Safety

Federal Trade Commission

Answer Key: 1. Phishing 2. Charity 3. Romance 4. Subscription 5. Smishing 6. Employment 7. Investment

8. Tech Support 9. Housing/Rental 10. Government 11. Credit Card 12. Non-delivery

To receive future Cyber Directorate Cybercrime Prevention Flyers, send an email to: Subscribe CPF

Disclaimer: The appearance of hyperlinks in this Cybercrime Prevention Flyer, along with the views and opinions of authors, products or services contained therein do not constitute endorsement by CID. These sites are used solely for authorized activities and information that support the organization s mission. CID does not exercise any editorial control over the information you may find at these link locations.