Five scams you should be aware of

and how to protect yourself from them

1 QR Code Scams

Description of this scam:

QR code scams involve malicious actors using fraudulent QR codes to direct victims to phishing websites, install malware, or steal sensitive information. QR codes can be easily printed on stickers and placed over legitimate ones in public places, such as restaurants, parking meters, or advertisements, making them appear authentic.

Example scenarios for this scam:

* Fake restaurant menus redirecting you to phishing websites.
* Fraudulent parking payment QR codes stealing credit card details.
* Codes in emails or text messages claiming to offer discounts, rewards, or urgent actions.

What to watch out for:

* QR codes in unexpected places, such as stickers over existing codes.
* Links that request login credentials, payment information, or other sensitive data.
* Codes that direct you to poorly designed or suspicious websites.
* Scenarios where the QR code is the only available option for completing an action.

Steps to prevent becoming a victim:

1. Inspect QR Codes Carefully:

* Look for signs of tampering, such as stickers placed over other codes.
* Verify the source of the code before scanning, especially in public spaces.

2. Use a Secure QR Code Reader:

* Install a trusted QR code scanner app with built-in security features to alert you of malicious links.

3. Check URLs Before Proceeding:

* After scanning, review the URL the code directs you to before taking any further action.
* Avoid clicking links with misspelled domains, unexpected extensions, or suspicious formats.

4. Manually Enter URLs When Possible:

* If a QR code links to a website, type the URL manually instead of scanning.

5. Avoid Sharing Sensitive Data:

* Never provide personal or financial information on a website accessed via a QR code unless you are confident of its legitimacy.

6. Stay Updated:

* Learn about the latest QR code scam techniques and share this knowledge with others.

7. Verify with the Source:

* If a business or service asks you to scan a QR code, confirm with them directly that it is legitimate.

General Safety Tip

Treat QR codes with the same level of caution as you would links in unsolicited emails or texts. Scammers rely on convenience to bypass your usual security measures. By staying vigilant and using these preventive steps, you can avoid

[Follow this link to learn more.]

2 Lost Pet Scams

Description of this scam:

The "lost pet" scam preys on individuals desperately trying to find their missing pets. Scammers respond to lost pet ads (online or in public spaces) claiming they have found the missing animal. They often request payment upfront for "transportation fees," "boarding," "medical or surgery fees", or a "reward" and then disappear once payment is sent.

Example scenarios for this scam:

* A scammer claims to have traveled far and requires money for transportation or shipping.
* Someone insists your pet is being held at a veterinary clinic or animal shelter that requires payment upfront.
* A fraudulent responder pretends to be a 'good Samaritan', but refuses to meet in person.

What to watch out for:

* Callers or texters who refuse to provide evidence, such as a photo of the pet.
* Urgent demands for payment before returning the pet.
* Requests for payment via untraceable methods like gift cards, wire transfers, or cryptocurrency.
* Claims that the pet is injured and requires immediate funds for surgery or treatment.

General Safety Tip

When dealing with a lost pet situation, act cautiously and do not let emotions cloud your judgment. Scammers exploit emotional vulnerabilities, so staying alert and following these steps can help protect you and increase the likelihood of finding your pet safely.

[Follow this link to learn more.]

Steps to prevent becoming a victim:

1. Request Proof:

* Ask for photos or specific details about the pet to confirm the person has your pet.
* Be cautious if they avoid answering direct questions about the pet's distinguishing features.

2. Verify Their Identity:

* Arrange to meet in a safe, public location to confirm the return of your pet before making any payments.
* Bring someone with you and let others know where you are going.

3. Avoid Upfront Payments:

* Never send money without concrete proof or returning the pet.
* If a reward is offered, only provide it upon safely receiving your pet.

4. Report Suspicious Activity:

* Notify local authorities or animal control if you suspect a scam.
* Inform the platform or site where the lost pet ad was posted about the fraudulent response.

5. Use Secure Communication Channels:

* Provide a temporary phone number or email when posting lost pet ads to protect your primary contact information.

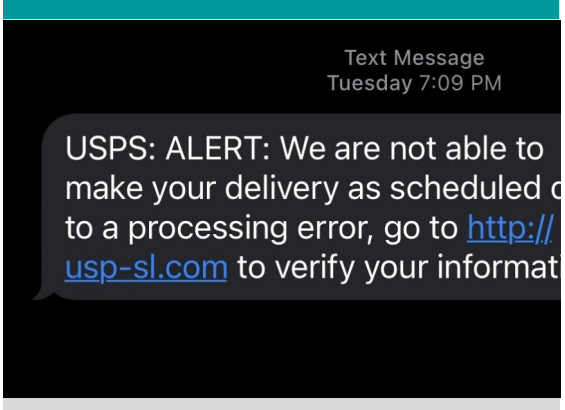
6. Check for Fake Stories:

* Be wary of overly emotional or elaborate stories about how they found your pet, especially if they seem designed to create urgency.

Never share your PIN number

NEVER give your PIN number to anyone!
No legitimate company, or company employee, will ever ask you to provide your PIN number. This includes fraud departments of financial institutions, credit card companies, and retailers.

3 "Delayed Package" Text Scams



Description of this scam:

Scammers send text messages claiming a package delivery issue due to an incomplete address, urging recipients to update their information via a provided link. These links lead to fraudulent sites aiming to steal personal and financial data.

Warning Signs:

* Texts from unknown numbers about undelivered packages.
* Links that do not correspond to official delivery service websites.
* Urgent language pressuring immediate action.

Preventive Measures:

- **Do Not Click on Unverified Links:** Access delivery information directly through official carrier websites or apps.
- **Verify Sender Information:** Cross-check tracking numbers and delivery statuses using official channels.
- **Be Cautious with Personal Information:** Avoid providing sensitive data through unsolicited messages.
- **Do Not Click on Unverified Links:** Access delivery information directly through official carrier websites or apps.

[Follow this link to learn more.]

4 Malicious Ads in Search Results

Description of this scam:

Scammers are placing deceptive ads that appear at the top of search engine results. These ads lead to fraudulent websites designed to steal personal information or install malware on users' devices. This tactic, known as "malvertising," has seen a significant increase, with a 42% rise in incidents in the U.S. during fall 2023.

Warning Signs:

* Ads that seem too good to be true, offering unrealistic deals or promotions. Links that do not correspond to official delivery service websites.
* URLs that mimic legitimate websites but have slight misspellings or unusual domains.
* Websites that request sensitive information unexpectedly.

Preventive Measures:

- **Verify URLs:** Double-check web addresses for accuracy before clicking.
- **Use Ad Blockers:** Employ reputable ad-blocking software to reduce exposure to malicious ads.
- **Update Security Software :** Keep antivirus and anti-malware programs current.
- **Be Skeptical of Unsolicited Offers:** Avoid clicking on ads that promise unrealistic benefits.

[Follow this link to learn more.]

Verify phone numbers before you call.

NEVER call a customer service or fraud department number that has been provided to you in an unsolicited text, email message, or phone call. Look up the number yourself and call the number you know to be legitimate.

5 Netflix Phishing Scams

Description of this scam:

Cybercriminals are sending fraudulent text messages claiming issues with Netflix accounts, prompting users to click on links to resolve payment problems. These links lead to fake websites that harvest login credentials and payment information. This scam has been detected in 23 countries.

Warning Signs:

* Unsolicited messages about account issues requiring immediate action.
* Links directing to non-official websites.
* Requests for personal or financial information through text messages.

Preventive Measures:

- **Avoid clicking on suspicious links:** Do not engage with unexpected messages containing links.
- **Verify through official channels:** Contact Netflix directly using official contact methods to confirm account status.
- **Enable two-factor authentication:** Add an extra layer of security to your account.
- **Educate yourself on phishing tactics:** Stay informed about common phishing strategies.

[Follow this link to learn more.]