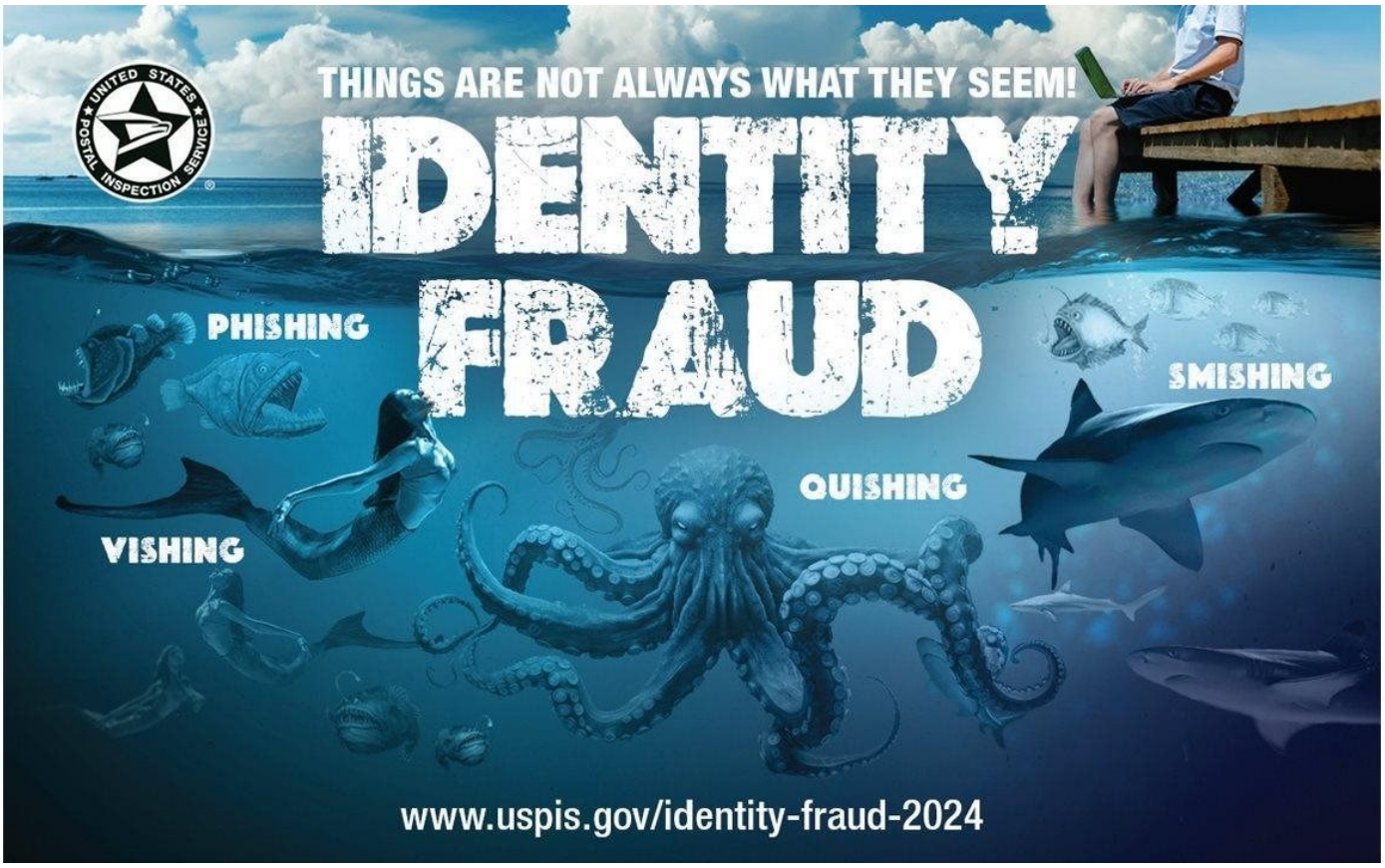
Things are not always what they seem: Beware of identity fraud



(BPT) - Scam artists are constantly changing tactics to steal your personal identifiable information (PII), including account usernames and passwords, Social Security numbers, birth dates, credit and debit card numbers, personal identification numbers (PINs) or other sensitive information. With this information, they can carry out crimes like financial fraud that can be difficult and frustrating for victims to remedy.

The United States Postal Inspection Service is working hard to stop these scammers in their tracks. You can help too, by familiarizing yourself with these identity fraud scams designed to trick you into giving up your “financial DNA” and turning over your personal identifiable information (PII) to imposters.

1. Phishing

If you ever receive an email about a package delivery or unpaid online postage charges, usually with the subject line, “Delivery Failure Notification," be careful. These phishing emails appear to be from the U.S. Postal Service but they are not and you should not interact with them. The phishing emails may contain either a spoofed or fake URL for you to follow or a file that if opened, can activate a virus, both resulting in stealing your personal information.

How can you tell if an email is NOT from USPS or the Postal Inspection Service? If the email requests “immediate action,” has poor grammar and spelling errors, asks you to confirm PII or asks for payment of any kind, you’re likely dealing with a phishing email. USPS officials would never contact consumers directly asking for payment or PII.

If you receive a phishing email:

- Treat your personal information like cash
- Don’t click on any links
- Forward USPS-related spam emails to spam@uspis.gov
- Report non-USPS spam emails to the Federal Trade Commission
- Delete the email

2. Smishing

Have you received unsolicited mobile text messages with an unfamiliar or strange web link that indicates a USPS delivery requires your response? You’re likely dealing with a smishing scam. This type of deceptive text message lures recipients into providing personal or financial information. Scammers often attempt to disguise themselves as a government agency, bank or other company to lend legitimacy to their claims.

Even if you've signed up for USPS tracking, pay close attention to the message. The Postal Service will never ask you for PII in a text message, redirect you to another site for payment, or contact you via text message, unless you initiated the request.

If you receive a smishing text message from the Postal Service:

- Don't click on the link
- Don't reply
- Forward the smishing/text message to 7726 or email spam@uspis.gov
- Report non-USPS fraud to the Federal Trade Commission
- Delete the text message
- Block spam messages
- Review your cellphone bill for suspicious charges
- Keep your security software up to date

3. Vishing

You may have enjoyed the game telephone when you were younger but calls from scammers trying to get your personal information are nothing to play with. A new twist on phishing, vishing is something you need to be aware of. Vishing is short for voice phishing and scammers will try to hook you as soon as you answer the phone.

Here's how to spot it.

Scammers call from a number that may look familiar or even appear to be from a legitimate source, like your bank or a government agency. The caller, however, is anything but legit. They may claim there's an issue with your account or a problem that requires your immediate attention. Then the scammers will ask for sensitive information like Social Security numbers, credit card details or passwords.

To protect yourself from vishing:

- Verify the identity of the caller
- Ask yourself why the caller is asking for your information
- Never give out sensitive information over the phone
- Report the call to the alleged bank, government agency or company
- Block spam callers
- Place your number on the national Do Not Call List

4. Quishing

QR codes are incredibly common nowadays. You've probably seen them on posters, food menus and TV screens. Take caution before you scan. Some QR codes may be a form of phishing known as quishing.

If you receive a message from an unfamiliar email address or text message or find a poster in a high-traffic location, don't scan it. If you do, the QR code could take you to a scammer's website (which may look legitimate) but is designed to scam you out of your PII.

If you find or receive a suspicious QR code:

- Don't scan it, especially if the message or poster urges you to act immediately
- Report the QR code to the bank, government agency or company that the scam artist is impersonating
- Block scam messages

Stay alert!

Scammers are always on the hunt for sensitive information. Protect yourself and others by using caution and reporting suspicious emails, texts, calls, voicemails and QR codes to the proper authorities. To learn more about how to protect yourself from identity fraud, visit uspis.gov/identity-fraud-2024. You can also find additional fraud prevention resources on our website at USPIS.gov.