Various Scams

- **Retail Scams:** Cybercriminals set up fake online stores offering enticing discounts on holiday items to lure shoppers. When victims attempt to make a purchase, their payment and personal information are stolen.
    - Instead of clicking on suspicious links, manually enter the URL into your browser.
    - Verify that the website's URL starts with "https" and look for a padlock symbol to confirm the site is encrypted. Ensure the padlock symbol is genuine and properly located in the browser. Stick with retailers that you already know and trust
    - Only shop with retailers that you already know and trust.
    - Use a credit card for online purchases rather than a debit card, as credit cards offer better protection against fraudulent transactions.

- **Sweetheart/Romance:** A scammer feigns romantic interest in their victim to gain their trust, ultimately intending to steal their money.

- **Can You Hear Me Now:** The scammer will quickly ask, "Can you hear me now?" to prompt you to say "yes," making it appear as if you authorized certain purchases.

- **Kidnapping:** The scammer falsely claims to have someone you care about captive and demands a ransom.
    - Ask specific questions, try to contact the supposed victim to verify their safety, and engage the scammer in conversation to extract details they might not have.

- **Arrest:** The caller claims that the victim's loved one has been arrested and requires bond money, possibly even pretending to be a family member requesting funds for bail.
    - Determine the jurisdiction where the person is being held and contact the appropriate agency directly to verify the information.

- **COVID-19 Testing Kits:** Home shipments of COVID-19 kids and Medicare billing issues
    - Contact Medicare to report that you did not order the kits and to get instructions on where to return them
    - Reach out to the APS Hotline and file a report

- **Postage Stamps:** Fraudulent websites are selling counterfeit stamps at discounted rates, typically 20-50 cents below their face value. These sites often use the USPS logo or images of USPS vehicles to appear legitimate. Counterfeit stamps are also being promoted on social media platforms.
    - To verify the authenticity of stamps, purchase them from your local post office, the official USPS website (www.usps.com), or an authorized Postal Provider such as a grocery store, pharmacy, office supply store, or bank.

- **Jury Duty:** Scammers are calling individuals, claiming they missed jury duty and must pay a fine. Remember, government officials will never contact you by phone to demand payment for missed jury duty.

- **Amazon Impersonation Scam**: The person may receive a phone call, email, or text to notify them of an “unauthorized purchase” or “suspicious activity” on their Amazon account. They might be directed to download an app, press a number to speak with customer service, or follow a link to request a refund. These actions could give the scammer access to their Amazon account or banking details.
    - Check your Amazon account under the “orders” tab to confirm if any recent orders have been placed.
      Contact Amazon directly to verify if there have been any purchases or if they sent an email notification.

- **Overpayment:** A person sells an item through an online platform, and the buyer overpays using a counterfeit check or a digital wallet (e.g., PayPal/CashApp). The buyer then requests a refund of the excess amount, claiming it was an error. Later, the check bounces or the payment is rejected, leaving the seller without both the money and the item.

- **Gift Card:** Scammers persuade individuals to buy gift cards as payment for items. After the gift card is purchased, they request the card number, and the money is then stolen.
    - Gift cards should only be used as gifts, not for payments. Anyone requesting gift cards as payment is likely a scammer.
      Contact the company from which the gift card was purchased; they may have a method to potentially recover the funds.

- **Payroll Diversion:** The scammer uses the employee's work login credentials to email the company's HR department, requesting a change to the employee's direct deposit information or to access the HR system and make the change themselves.
      Companies should always confirm the person's identity through at least three methods before providing any password or account information.

- **Utility Disconnection:** Someone pretends to be from the utility department, insisting on immediate payment for an overdue bill and threatening to disconnect service.
    - Utility companies will not request payment by phone; official notices will be sent by mail. o Reach out to your utility company directly or log in to your online account to verify your account status.

- **Package Delivery:** An email or text appears to come from a familiar carrier, notifying the recipient of a missed package delivery. It provides a link for rescheduling the delivery, which collects personal information. There was never a package, and the victim ends up downloading malware and disclosing personal details that could lead to identity theft.

- **Pet Delivery:** A scammer uses stock images of animals and ask for payment upfront

- **Phishing:** A phishing scam that uses QR codes.

- **Tech Support:** A person receives pop-ups that say their computers security is at risk.