Beware of Scammers
Sergeant Brian Curtis of the Mechanicsburg Police Department

Sgt. Curtis gave a presentation at First United Methodist Church on Sunday, September 27 to the adult Sunday School classes. Here is an overview of his presentation.

Most scammers use **fear** to gain control of their victim – if it seems too good to be true, most times it is!

Beware of the following:
Green Dot cards: These cards are used like a gift card (reloadable debit card) and are very hard to trace. If someone wants you to pay with a Green Dot card, that is a red flag.
https://www.moneypak.com/ProtectYourMoney.aspx.

Western Union scam: With overpayment scams, fraudsters play the role of buyer and target consumers selling a service or product. The "buyer" sends the seller a legitimate-looking check, usually drawn on a well-known bank, for an amount higher than the agreed-upon price. They contact an explanation for this overpayment and instruct the seller to deposit the check and wire back the excess funds. Weeks later, the victim learns the check is fake, but is still on the hook to pay the bank back for any money withdrawn.
https://www.westernunion.com/us/en/fraudawareness/fraud-types.html.

IRS scam: You receive a call from the 'IRS' stating that you owe money and that you will be jailed if you don't pay (again, the fear factor). You are told to buy a Green Dot card to pay off the debt. The IRS website makes this statement: "There are clear warning signs about these scams, which continue at high levels throughout the nation," said IRS Commissioner John Koskinen. "Taxpayers should remember their first contact with the IRS will not be a call from out of the blue, but through official correspondence sent through the mail. A big red flag for these scams are angry, threatening calls from people who say they are from the IRS and urging immediate payment. This is not how we operate. People should hang up immediately and contact TIGTA or the IRS."
http://www.irs.gov/uac/Newsroom/IRS-Repeats-Warning-about-Phone-Scams.

Bail scam or 'grandparents scam': A grandparent receives a frantic call from someone they believe to be their grandchild. The supposed grandchild sounds distressed and may be calling from a noisy location. The supposed grandchild claims to be involved in some type of trouble while traveling in Canada or overseas, such as being arrested or in a car accident or needing emergency car repairs, and asks the grandparent to immediately wire money to post bail or pay for medical treatment or car repairs. The scammer typically asks for several thousand dollars, and may even call back again several hours or days later asking for more money. He or she may claim embarrassment about the alleged trouble and ask the grandparent to keep it a secret.
http://www.michigan.gov/ag/0,4534,7-164-18156-205169--,00.html.

Computer Repair scam: The latest version of the scam begins with a phone call. Scammers can get your name and other basic information from public directories. They might even guess what computer software you're using. Once they have you on the phone, they often try to gain your trust by pretending to be associated with well-known companies or confusing you with a barrage of technical terms. They may ask you to go to your computer and perform a series of complex tasks. Sometimes, they target legitimate computer files and claim that they are viruses. Their tactics are designed to scare you into believing they can help fix your "problem." Once they've gained your trust, they may:

- ask you to give them remote access to your computer and then make changes to your settings that could leave your computer vulnerable
- try to enroll you in a worthless computer maintenance or warranty program
- ask for credit card information so they can bill you for phony services — or services you could get elsewhere for free
- trick you into installing malware that could steal sensitive data, like user names and passwords
- direct you to websites and ask you to enter your credit card number and other personal information

Regardless of the tactics they use, they have one purpose: to make money.
http://www.consumer.ftc.gov/articles/0346-tech-support-scams.

Phishing: When internet fraudsters impersonate a business to trick you into giving out your personal information, it's called phishing. Don't reply to email, text, or pop-up messages that ask for your personal or financial information. Don't click on links within them either – even if the message seems to be from an organization you trust. It isn't. Legitimate businesses don't ask you to send sensitive information through insecure channels. https://www.onguardonline.gov/phishing.

Skimmers: A credit card skimmer is a portable capture device that is attached in front of or on top of the legitimate scanner. The skimmer passively records the card data as you insert your credit card into the real scanner. When using an ATM machine or at the gas pump, inspect the card reader and make sure there isn't anything 'funny' about the reader. If it has something taped beside it or attached to it, or doesn't look like the other readers, do not use it! The scammer may be sitting in a parking area across from the bank or gas station and downloading all your information while you are using the device.
http://www.pcmag.com/article2/0,2817,2469560,00.asp.

Most of the above scams can be found on the consumer.ftc.gov website (Federal Trade Commission). It will list all of the current scams and there are quite a few! The links are also included for the websites of that particular scam.

Tips to keep you safe:

- Copy your credit cards (front and back), so if stolen, you know what cards you had and the number to call to cancel.
- Do not carry any credit cards in your wallet/purse that are not regularly used. Keep them in a safe place at home.
- It's best not to use a credit/debit card that is deducted directly from your account.
- Purchase credit card sleeves to protect against ID theft and credit card fraud. They are small, inexpensive and can be purchased at office supply stores or online.
- Always check your credit card statement and compare it to your purchases. Keep a close eye on your charges!
- Do not give out your personal information to someone until you have verified who they are.
- When you get a phone call from someone you don't know, get a phone number and verify the phone number – then call them back.
- If someone mentions 'Green Dot or Western Union' – hang up or delete.
- On your computer, **do not** check the box 'remember me' on your email or other websites. Type in your password each time!
- Do not keep a file on your computer with passwords, even worse, don't name your file 'passwords.' Keep a paper copy of your passwords in a safe place.
- **If it sounds strange, it probably is.**
- Trust your instincts!

All residents are invited to attend Crime Watch meetings on the **second Monday of each month at 7:00 PM at the Senior Citizens Center on Portland Street**. Mayor Jack Ritter and Borough resident Jack Baker currently head the program. A representative of the Police Department gives a summary of criminal activity in the Borough each meeting and various guest speakers address a variety of topics for discussion.