Helpful Information and Tips

Ferguson Township Police Department

Contacting Police

- Ferguson Township Police are available to assist you 24 hours a day, seven days a week, 365 days a year.
- When you need help or your gut tells you to report something, consider it an emergency and **call 9-1-1.**
- If you need to report a crime, suspicious vehicles or activity, car crash, an injured person or animal, someone in harm's way, or something you have witnessed, contact the police immediately. **Don't wait!**
- In an emergency, please do not use email, Facebook, or after-hours phone messages.
  For non-emergencies, call 1.800.479.0050
  Visit our web site for Online reporting or submitting an anonymous tip (Non-emergencies only)

Theft Prevention

- Each and every time you leave your apartment, lock your doors.
- Keep your doors and windows locked.
- Be a good neighbor and report suspicious people in the apartment complex.
- Keep your porch light on at night.
- Remove any packages from your porch each day. Do not have packages delivered when you are not in town. If you must have packages sent, have them delivered to the office or ask a trusted neighbor to pickup and hold them for you until your return.

Protecting Your Vehicle

- Always lock your vehicle and keep items of value out of sight, or preferably, not in your vehicle at all.This will discourage break-ins and thefts.

Protecting Yourself from Scams and Fraud

Ferguson Township Police encourage residents to be aware of common scams. Attempts to scam peopleout of their money are made throughout the year.

Scams come as phone calls, emails and most recently as text messages. Some common scams:

- Scammer claims to be a bank advising they need a moment of your time and requests private information that — if given — can allow access to your account.
- Scammer claims to be a representative of a law enforcement agency, pretending there is an arrest warrant and threatening you with incarceration if a fine is not paid. The suspect directs you to use a Green Dot MoneyPak or Apple iTunes card to pay the fine. Typically, the scammer will "spoof" his or her own phone number so that yourcaller ID will display 9-1-1 or another law enforcement agency phone number.
- Scammer convinces you to send payments for promised prizes, loans, jobs, discounted products or other financialawards upfront through a Western Union wire transfer. They also pretend to be family members in need of cash or law enforcement officers demanding payment. No one receives the cash, prizes or services they are promised.
- Scammer pretends to be the IRS advising that you owe taxes. The IRS will NOT contact you by phone. Scammers also have claimed to be the Department of Education advising students they owe money on student loans.
- Scammer calls and threatens to physically harm you if you do not send money. Scammers may also advise thatthey have a family member hostage and will injure them if you do not send money.
- When selling something online, the scammer offers to pay more than the seller requested. The scammer sendsa fake check including the extra money and asks the victim to send the extra money back. The victim loses the product and money because the check is fake.

Avoid being a victim of fraud:

Remember that you cannot trust everyone who calls or emails you. Most scammers use phone and Internet contactsfrom outside of

the United States and law enforcement does not have the jurisdiction to prosecute or retrieve your money. If it seems too good to be true, it probably is! Some ways to prevent fraud:

- Don't agree to anything over the phone. If you can see the caller's number, make a note of it. Search the Internetfor the number to determine its source.
- Never follow instructions to purchase a money or gift card for payment. Scammers will ask you to purchasea card and read the numbers over the phone. This allows them access to your funds.
- Do not give out personal information such as your Social Security number, date of birth, account numbers andsuch over the phone.
- Never click on a link in a questionable e-mail. If you want to follow up with a business or company youbelieve is attempting to reach you, use your Internet browser to search for its URL address.

Questions about the Law

If you ever feel you may be a victim of a crime or just have a question about the law, please visit theFTPD web page at **www.twp.ferguson.pa.us**. If you still have questions, please contact the FTPD at **814.237.1172** or email **police@twp.ferguson.pa.us**

Must Pay with Gift Cards (IRS, Police and iTunes / Gift Cards)

HOW THE SCAM WORKS: A customer receives a threatening voice message from a scammer pretending to be from the U.S. Internal Revenue Service. To avoid being arrested for tax evasion, the victim is told that he or she can pay the fine with iTunes gift cards or other gift cards. In a similar example, a "State Trooper" calls to say that the victim failed to show up for jury duty and there is warrant out for his or her arrest. To avoid going to jail, "bail" can be paid using "MoneyPak" as a bond until the case is cleared.
Once gift cards are purchased, the scammer will ask the victim to repeat the gift card numbers over the phone–at which time, the scammer drains the value of the gift cards. Victims who fall for the initial ploy are often told to go back to the store to buy additional gift cards.

On the surface, this scam seems really easy to spot and hard to believe but given that Americans have been swindled out of nearly $40 million from it, there is obviously more to the story. According to an article on the IRS iTunes gift cards scam, "scammers posed as U.S. Internal Revenue Service officials and left victims voicemails accusing them of tax evasion and threatening them with arrest." The callers were highly trained and very convincing.

RED FLAG: No reputable company nor the IRS or any government agency will ever demand payment via gift cards, iTunes, pre-paid credit cards or Western Union.

WHAT TO DO: If you get a phone call from someone telling you to make a payment with gift cards, hang up the phone. If you get an email from a company telling you to make a payment with gift cards, delete it. Don't be fooled. If you have any doubts that the call or email is legitimate, contact the company yourself. Don't call the number given to you on the voice message, and don't respond to the email or click any of the links inside of it. Initiate the call yourself.

Business email scams

Phishing email attacks are on the rise. A phishing email is an email you receive from someone pretending to be someone else (pretending to be a co-worker, boss or friend), asking for something in return.

The most common example of this is an email from "your supervisor" asking for you to buy a gift card for her because she is in a meeting. These are fake and you should not respond. In extreme cases, the email asks you to click a link, which then gains access to your computer and collects private information.

How to spot a phishing email?

To spot a phony email, you can generally notice it by looking at the "From" email address. Don't just look at the name. The name on the header may appear that it is coming from a trusted source but take a second look and pay particular attention to the

email address. Do you recognize the email address? It could be one character off or completely different. Is it an email address that the person usually uses to contact you? Is the request itself unusual? If there is any doubt, contact the person directly before taking additional action.

Here is an example:

On May 20, 2021, at 1:25 PM, Laura [redacted] <mayor7978@[redacted]com> wrote:

P[redacted]
I'm so tied up right now, can you purchase an iTunes gift card 4 pieces -$100 each at any near by store?
I would reimburse you when am through later today. I would have preferred to call you but can't receive or call at the moment with my line
let me know if you can purchase them now.
Thanks and I'll be awaiting ASAP
Best Regard
Laura [redacted]

You can also spot these emails by the content. Does your co-worker, boss or friend ask you to provide confidential financial information, buy gift cards, or ask for your credit card information over email.

Different from hacking, spoofing and phishing simply try to emulate as close as possible the email address of the person it is pretending to be. They simply found the emails by searching public websites and are using it to try to trick you.

Grandparent Scam

The "legal trouble" scam. Fraudsters often work in tandem for this one. The caller claims they are a grandchild who has just been arrested. This sets up their plea for grandma or grandpa to send money to post bail. Here's where they pass the phone to someone who claims they are the child's attorney. This speaker will ask for cash and likely dictate the terms of delivery.

The "medical trouble" scam. The caller claims they are a grandchild who has just been seriously injured. They tell a convincing tale about where, when, and how it all happened, leading to the big ask: that their grandparent quickly wire them thousands of dollars to pay the medical bills.

If someone contacts you or your grandparent claiming to be a grandchild or other family member desperately in need of quick money:

1. **Resist the urge to act immediately.** No matter how dramatic the story is, stop and collect information. Your most effective protection against this scam is to verify the facts before acting. This exposes the lies in the scammer's story.

2. **Verify the facts.** To make sure the caller is who they claim to be, ask a question about them that a stranger couldn't possibly answer. Further, hang up and call them member back at their own phone number. And don't stop there! Check with someone else in your family or circle of friends, to see if this story checks out. Believe it or not, grandparent scammers have often been caught by just this simple act of verification, which revealed their story was false.
3. **Stop and pause before sending cash, gift cards, or money transfers.** Even if you've collected the information, verified the story, and you think it all checks out, pause for one last moment before sending the money. Once the scammer gets the money, it's gone!

Keys to remember

1. Most organizations, including police, tax offices, courts and other government agencies, do not accept payment in the form of gift cards, Google Play, iTune, greendot cards. If you are asked to pay a bill or debt with any of the above, it's almost certain to be a scam.

2. Police, tax offices, courts, other governmental agencies and officers, power companies and large companies will not ask you to make payment in an individual's name. If someone tells you to make the payment in a person's name, it's a scam.

3. Do not believe your caller ID. Criminals can make any phone number appear on your caller ID including 911.

4. Hang up or obtain a call back number. They will pressure you not to hang up. If they give you a phone number, write it down. Use the internet or bills listing company phone numbers to verify the agency's real contact information.

5. Do not give out your personal / sensitive information (bank accounts, social security numbers, etc..) over the phone or Internet unless you are absolutely, positively sure you are speaking to a trusted individual. You call the company using a phone number you've researched!!

6. If you are unsure, get a call back number and contact family, friends, search the internet or contact the police to help vet the truthfulness of the person.

7. They use wire transfers because most overseas retailers don't require ID to receive wire transfer payment. Similarly, gift cards and iTunes, are not traceable and easily cashed by the scammer.