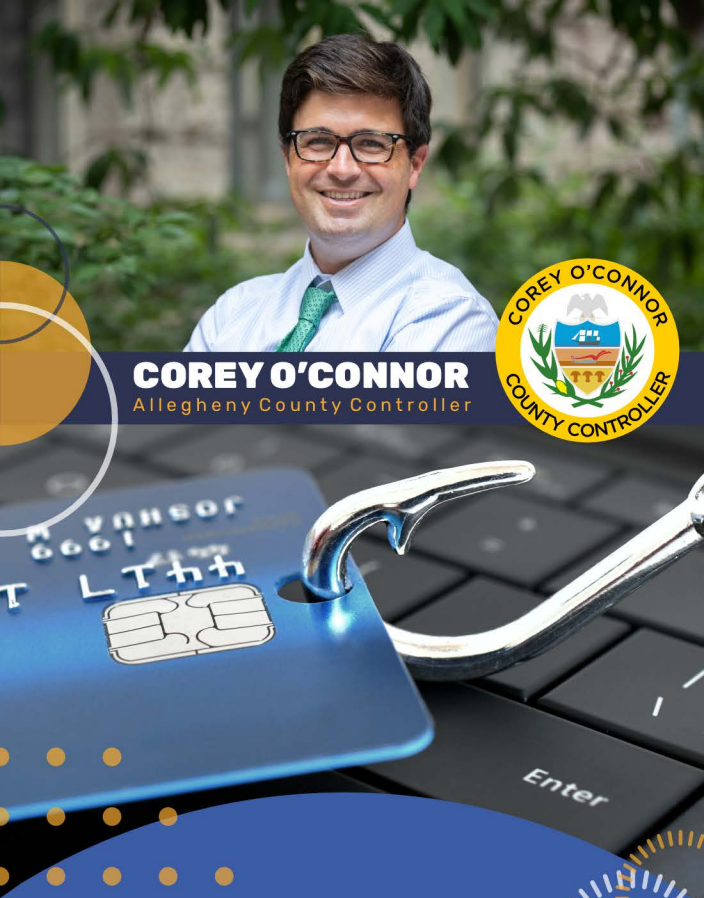



# Protect Yourself from Frauds & Scams

412.350.4660

@alleghenycontroller

alleghenycontroller.com

@AC_controller

436 Grant Street
Courthouse, Ste 104
Pittsburgh, PA 15219

controller@alleghenycounty.us

# Phishing

Such scams usually appear as emails from reputable companies or financial institutions. Scammers can also pose as government agencies. An email usually warns you of an urgent problem. You will be directed to a phone number or website to address the issue. Scammers often ask for personal information, such as Social Security Numbers, account numbers, passwords, birthplace, mother's maiden name, etc.

## Prevention...

- Typically, the text in the subject line or the body of the email will be a variety of fonts and numbers to make up words, such as using a 1 for the letter "l" or a zero for the letter "o."
- The sender's email address may be similar to an organization email, but changed in some capacity (e.g., usage of .net instead of .com).
  - Furthermore, less clever scammers will use a basic public email provider (e.g., walmartsupport@gmail.com).
- When redirecting you to a website that claims to allow you to remedy the situation, the imitation website URL will not reflect your actual URL (e.g., your account is with Citizens Bank - https://www.citizensbank.com, but the forwarding URL is https://verifyacces.ml/?x.
- Most times, the URL will not be secure (i.e., the URL will begin with HTTP instead of HTTPS). This can also be verified through a padlock icon in your browser toolbar. However, this can be replicated.
- Many times, scammers will use an organization or financial institution that you have no affiliation with, or with which you have closed an account in the past.
- Never provide account information to a website listed in an email or text message. Instead, go through your normal routine, whether it be through an app or the typical website you use to log in to your account.
- Review your account statements regularly to ensure that all charges are correct.

## If you become victimized...

- If you believe that you have been scammed, immediately contact the financial institution to which you have provided access.
- If the information provided to the scammer is sensitive information, also contact one or all of the major credit bureaus (Equifax, Experian, TransUnion) to report the fraud.
- Report suspicious contact to the Federal Trade Commission and your local law enforcement agency.

# COMMONLY USED SCAM TACTICS

## Charity

Criminals will act as representatives of a charity organization looking to obtain a donation. In most cases, individuals claiming to be from an organization have no affiliation with the group and will empty your bank account as soon as they have access to your account information.

## Goods/Services


Criminals will pose as a reputable business showcasing a product of interest. However, they have no intention of providing that product, or, in some cases, any product at all. Once they obtain your financial information, they can use it for themselves or simply never provide you the product that you believed that you bought.

## Government

Scammers will pose as government officials, from IRS agents to police officers, claiming that, due to some circumstances, you will be sued or that a warrant was issued for your arrest. Usually, they require payment to be paid prior to the end of the phone call and will request the payment be made in an obscure form, such as digital wallet, gift card, or prepaid credit card.

Write down as much information as the scammer is willing to provide, but do not give them any financial or personal information. Upon receiving as much information as possible, contact the agency that the caller claimed to be representing to see if the claims are valid.

## Grandparent

Criminals will pose as a relative, typically a child or grandchild, stating that they need immediate funds due to a situation that they are in. Again, take down as much information as possible and then contact your relative directly to assess the situation.

## Inheritance/Sweepstakes

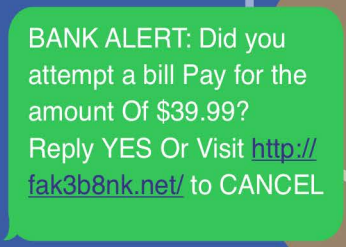
The caller will claim that you have won a lottery/sweepstakes or will be inheriting funds from a distant relative. However, in order to claim your prize/inheritance, you must pay a fee and taxes as a service. This is a scam, and you should never provide financial or personal information on the phone unless you are fully aware with whom you are speaking.

## Tech Support

A pop-up may appear on your screen claiming that your computer has acquired a virus. In most cases, a website link or phone number will accompany the message, claiming that they can assist you in removing the virus. This is a scam.

## Text

These types of scams can happen in a variety of ways. Scammers may claim to be a bank and request that you confirm a recent transaction. If you respond, they know that the number that they have contacted is a good number for them to reach out to in the future regarding the bogus payment issue. However, they usually provide a link to log in to your account and assess the situation. Although it appears to be the login page for your bank when you visit the link , it is an imitation site that will obtain your user information upon input and empty your bank account. Never respond if the claim seems suspicious. Instead, contact your local banking office for further clarification.




## SCAM PREVENTION TIPS

- Block unknown callers/unwanted calls.
- Never provide financial or personal information in response to an unexpected request.
- Resist pressure to act immediately.
- If they request payment via gift card or prepaid card, it's a scam.
- Talk about the situation with a trusted friend or relative.

# IDENTITY PROTECTION

## Create Strong Passwords

- Use passwords that are not specific to you (i.e., children's names, pet's name).
- Use upper and lowercase letters, numbers, and special characters.

## Know the Information You Share

- Many scammers will harvest public information on social media, as well as from web searches, so that when they contact you, they seem as if they are a verified representative of a business/organization.
- Review your Privacy Settings on social media accounts so that personal information is not available to the public.

## Protect Your Smartphone

- Use a long password for your phone.
- Facial recognition and/or fingerprint verification are best, if possible.
- Set up your phone via the device providers cloud service to erase all data if the device is lost or stolen.

# ELDERLY TIPS

## Changes

If you feel that your math skills or memory are depleting in any capacity, always make sure that you are open with family members so that they can protect you from a scam. Many scammers will prey on sick and/or vulnerable victims.

## Finances

Be open about your bills and spending with trusted family members, as they may uncover a scam of which you were not aware.

## Workers

Make sure that you are using trusted workers, such as contractors, electricians, plumbers, etc., when requesting work be done at your home. Review the information about the business, the representative, and the service quote with trusted family members to ensure you are not being taken advantage of by the business.

If possible, have a trusted family member with you when talking to a worker on the phone or for an at-home visit.

# WHAT TO DO IF YOU ARE THE VICTIM OF A SCAM

## If you paid money...

The moment you realize you have been scammed, contact the financial institution in which you made the payment (i.e., bank, credit card, gift card, wire transfer, etc).

Additionally, contact your local police department to file a report.

## If you provided personal information...

Many scammers try to obtain social security numbers. If you have provided yours, visit identitytheft.gov and take the appropriate steps to monitor your credit.

## If you provided a username and password...

Try to obtain access to your account as soon as possible and change your password to a new, strong password without any resemblance of the last password.

If you cannot access your account, contact the company or institution.

## If the scammer has access to your device...

- Turn off your device and disconnect from the internet.
- If you have a backup, restore it from a previous state.
- If you do not have a backup, you may have to wipe the entire system, but consult with a reliable technician first.
- Contact any financial institution that you have saved username(s)/password(s) on the device.

**For the most up to date information regarding scams, visit the Federal Trade Commission's website, https://consumer.ftc.gov/scams. In addition to information, you can also file a report regarding your situation.**