Avoiding Scams

Have you ever gotten a phone call from someone claiming to be from the IRS? Has anyone ever asked you for your social security number over the phone or asked you to send them money before they take action against you? If so, you have likely been the target of a scam.

Each semester, international students and scholars at Vanderbilt fall victim to identity theft and other scams. . It's not hard to see why – often, scams begin with a phone call from someone claiming to be from a legitimate agency, such as a bank or the Department of Homeland Security. It may be natural to think that someone claiming to be from your bank would want your SSN . . . but be careful! No bank, government agency, or other legitimate organization will ever ask for this information over the phone, unless you yourself have initiated the call. If you are ever unsure about the legitimacy of the call or threat, you can contact VUPD at any time to confirm. They are here to assist you.

Here are some very general tips to avoid being scammed:

- No **legitimate** agency will ever ask for your SSN **over the phone**, unless it is for an application or issue that you have personally called them to initiate.
- If you are shopping or banking online, make sure that the website is secure before giving out sensitive information. Look for the **lock symbol** in the browser. Don't give out sensitive information over unsecured networks.
- Keep your passwords, PINs, and other important information private. If others have access to them, they can access your data and accounts.
- **No U.S. government agency will call you to ask for money.** In fact, U.S. government agencies are likelier to contact you via **regular mail** if they have important information to send you/ask for.
- No legitimate agency will ask you to purchase Google Play Cards (or any other gift card) and provide them with the PIN.
- Some scammers will threaten to take action against you unless you give them money. They may threaten to deport you, or they may threaten to take action against you on social media. This scare tactic is part of the scam. **Never give someone money in this situation.**

If you are the victim of a scam, here are some first steps:

- If your banking or credit card information was given out, contact your bank **immediately**.
- Contact **VUPD immediately – even if it is after business hours –** and file a police report with local law enforcement. Police reports make it easier to dispute fraudulent charges that occur. If you live in Davidson County, you can complete a police report through VUPD.
- If you gave out any of your personal information (or suspect that your information has been compromised), contact the fraud units of one of the three credit reporting companies – **Experian**, **Equifax**, and **Trans Union**. They can place a fraud alert on your record, making it harder for someone to open up an account in your name. You can also request a free credit report to monitor any suspicious activities in your name. You are allowed one free report each year.
- Report the scam to the **Federal Trade Commission**.
- You can contact VUPD or the police at any time of day – including late at night.
    - VUPD: (615) 322-2745
    - Metropolitan Nashville Police Department ("Metro"): 615-862-8600

We would also recommend downloading the **VandySafe app** on your phone. This app is free and allows you to contact VUPD directly. It also includes other resources to help you stay safe on campus.

Also, contact ISSS if you have been targeted by a scam. We want to help you and make sure that you get connected to resources that can assist.