PUBLIC SAFETY ADVISORY

Johns Hopkins Security is providing the following information for all Johns Hopkins employees and students:

Recently, federal and local law enforcement officials have noted increased reports of the following three scams. Further, some criminals have taken advantage of confusion surrounding the U.S. federal government shutdown to impersonate federal officials. Below, you will find information on how each of these fraud schemes works and how you should respond if you become a target.

1. IRS Scam

The scam: An individual claiming to be from the U.S. Internal Revenue Service calls and claims that you owe back taxes. You are also told that if you fail to respond by a certain time, you will be arrested, and that if you are in the United States on a visa, you will be deported. The caller typically asks for a wire transfer or pre-paid debit card to pay the alleged back taxes.

What you should know: U.S. government agencies do not make phone calls or send emails to inform people they are delinquent, they will not threaten people with imprisonment or deportation, and they do not accept wire transfers or pre-paid debit cards as a way of payment for any legitimate debt you may owe the U.S. government. You should ignore such calls or emails.


2. Kidnapping Scams

The scam: An individual or group uses various open sources, such as social media accounts, to compile information about you and your family. Typically, criminals will use this personal information in one of two ways. First, they may call you at either a work or a personal telephone number claiming to have kidnapped a family member—typically a child. During the call, someone may be heard in the background calling for help; the caller will claim that it is the kidnapped family member. In the second version of the scam, the individual committing the scam will try to convince you to go into hiding and cut off all contact with your family, and will then tell your family that you have been kidnapped and ask them to pay a ransom.
What you should know: At a moment of anxiety and stress, recipients of such calls may believe the background voice sounds like the allegedly kidnapped family member. Should you receive such a call, remain on the line to gather as much information as possible (see below for useful information) and use another phone line to call Johns Hopkins Security or your local police department. If you must hang up to call security or the police, do so immediately. Do not agree to meet or wire money and do not agree to any other demands. Wait for the arrival of the security team or police and provide them with as much information as possible.


3. DEA Scam

The scam: An individual claiming to be from the U.S. Drug Enforcement Administration attempts to persuade drug prescribers to provide personal information and/or a DEA registration number over the phone or by email.

What you should know: Government officials will not call or email requesting any type of personal information. Should you receive such a call or email, do not respond. Contact Johns Hopkins Security and provide details.

More information: https://www.consumer-action.org/alerts/articles/dea_calling_no_its_a_scam_hitting_doctors_and_consumers

These are a small sample of the many fraud schemes or scams that criminals use to collect money from unsuspecting individuals. Please be cautious when dealing with unsolicited emails and phone calls. If you are not sure about the authenticity of a contact you have received, do not respond; instead, immediately contact your campus security office.

When reporting such an issue, it is helpful to provide as much information as you can, such as:

- An incoming phone number;
- The nature of the call, including specific requests or demands;
- Any potentially identifying characteristics of the caller;
- An original email or social media post, if the communication was received through one of those channels;
- Information on the email address or social media account from which such a communication was received; and
- The content and originating number of a text message, if the communication was received by text.

If you have any questions, do not hesitate to contact Johns Hopkins Security.