BEWARE OF SCAMS

Scammers may contact you claiming to be an official from federal agencies such as U.S. Citizenship and Immigration Services (USCIS), Social Security Administration, or the Internal Revenue Service (IRS). We would like to remind you that US Citizenship & Immigration Services, Customs and Border Patrol, the Internal Revenue Service, and any other government organizations will contact you by U.S. mail, never by phone or email. They will also not ask for your personal information, threaten arrest/deportation, or ask for payments or fees (especially in the form of a money order or gift card.)

Typical characteristics:

- The person on the phone is aggressive; sometimes states they are from immigration or the IRS.
- They state false information, such as "there is a problem with your taxes or immigration status"
- They want you to act quickly, and tell you to stay on the phone with them.
- They demand money – often thousands of dollars
- They may threaten you
- The caller may know your school, phone number, address, and other personal information

Gather information:

- What day and time did they call you?
- Who did they say they were? (Who were they representing?)
- What exactly did they say? (What did they want you to do?)

Our advice:

- Hang up the phone and call VISA (after office hours, call: **804-505-4291**)
- Do not give money or promise to give money
- Do not meet up with the person
- Do not tell them personal or financial information
- Monitor or change information (such as bank account, credit card, online accounts, passwords, etc.) depending on the nature of the call
- If you receive anything by mail, bring it to our office and meet with an advisor

If you receive a call or document and you are unsure if it is authentic, please contact our office. If you feel you have an emergency situation and our office is closed, please contact our emergency number at **804-505-4291 OR 804-505-4131**. **Save these numbers in your phone now!**

"Red Flags" for employment scams:

- The employer offers to pay a large amount of money for very little work
- They offer to send you a check before you have begun any work, or offer you a job without ever interacting with you
- Requires you to pay a large amount of money for a "guaranteed" job or internship placement
- Requires personal information from you (social security number, bank account numbers, credit card information, copies of your passport or license, and/or other personal documents)
- Requests you to transfer or wire money from one account to another

For more information on common scams: https://www.uscis.gov/avoid-scams/common-scams

Phishing Emails:

Phishing is the number one starting point for online attackers wishing to conduct malicious activity. They are a frequent occurrence at many organizations, including ODU. At first glance, phishing emails may appear to be from legitimate sources.

- They may ask for your login ID and password
- They may provide a link to a very convincing website designed to get your login information or to transmit malware.
- They may appear to be from a known ODU associate.

*In reality, they want to gain unauthorized access to your online resources and to ODU services.

- To protect your information please:
  Follow the safe email practices found at www.odu.edu/cybersecurity
- Delete all emails that are clearly phishing attempts
- Report suspected phishing emails by forwarding them to phishing@odu.edu
- Contact the ITS Help Desk at http://www.odu.edu/ts/helpdesk if you accidently click on a suspicious link or think you might have been infected with malware
- Do NOT follow any instructions requested in a phishing email

*Remember: ODU will NEVER ask for your password by email or over the phone.