GERMANNA COMMUNITY COLLEGE
POLICE DEPARTMENT

Craig L. Branch
Chief of Police

Bulletin# 17-003

OFFICIAL USE ONLY

CRIME ALERT BULLETIN

Potential Hurricane Harvey Phishing Scam Alert

Date: 08/29/17

The college police department received noticed from the Virginia State Fusion Center and US Department of Homeland Security's US Computer Emergency Readiness Team asking us to warn the college community to be on alert for potential Hurricane Harvey phishing scams. Please remain vigilant for malicious cyber activity seeking to capitalize on interest in Hurricane Harvey. We are also asking community members to exercise caution in handling any email with subject line, attachments, or hyperlinks related to Hurricane Harvey, even if it appears to originate from a trusted source.

It is heartbreaking to see people lose their lives, homes, and businesses to the ongoing flooding in Texas. However, it is also despicable when scammers exploit such tragedies to appeal to our sense of generosity and patriotism. In addition, if you receive a call that seems suspicious, you should disconnect immediately and notify law enforcement. If you are looking for a way to give, the College Police urges you to be cautious of potential charity scams. Do some research to ensure that your donation will go to a reputable organization that will use the money as promised.

Consider these tips when asked to give:

- **Be alert for charities that seem to have sprung up overnight in connection with current events.** Check out the charity with the Better Business Bureau's (BBB) Wise Giving Alliance, Charity Navigator, Charity Watch, or GuideStar.
- **When texting to donate, confirm the number with the source before you donate.** The charge will show up on your mobile phone bill, but donations are not immediate.
- **Other key Virginia Resources include;** Virginia Department of Agriculture and Consumer Services
- Office of Charitable and Regulatory Programs, Commonwealth of Virginia Campaign, and Commonwealth of Virginia Office of the Attorney General-Consumer Protection Section.

The college police department can also assist you with filing a complaint through the Internet Crime Complaint Center www.IC3.gov. If you believe you have been a victim of a scam, please contact the College Police Emergency Communications Dispatch center at (540) 891-3079 or your local law enforcement agency. If you have concerns with suspicious e-mails, please contact the College IT helpdesk. See attached alert notice from DHS.

As a reminder, if you see or hear of any suspicious person or activity in or around the college, please notify the College Police Dispatch Center immediately at extension **2911 from any college VoIP phone** or **540-727-2911 from a cell phone**.

This crime alert bulletin is being distributed as required by the Jeanne Clery Act of 1998
U.S. Code of Federal Regulations Title 34, Chapter IV, Section 668.46 (e)

OFFICIAL USE ONLY

Homeland Security

US-CERT United States Computer Emergency Readiness Team

National Cyber Awareness System:

Potential Hurricane Harvey Phishing Scams

08/28/2017 02:40 PM EDT

Original release date: August 28, 2017

US-CERT warns users to remain vigilant for malicious cyber activity seeking to capitalize on interest in Hurricane Harvey. Users are advised to exercise caution in handling any email with subject line, attachments, or hyperlinks related to Hurricane Harvey, even if it appears to originate from a trusted source. Fraudulent emails will often contain links or attachments that direct users to phishing or malware-infected websites. Emails requesting donations from duplicitous charitable organizations commonly appear after major natural disasters.

US-CERT encourages users and administrators to use caution when encountering these types of email messages and take the following preventative measures to protect themselves from phishing scams and malware campaigns:

- Do not follow unsolicited web links in email messages.
- Use caution when opening email attachments. Refer to the US-CERT Tip Using Caution with Email Attachments for more information on safely handling email attachments.
- Keep antivirus and other computer software up-to-date.
- Refer to the Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.
- Review the Federal Trade Commission information on Charity Scams.
- Verify the legitimacy of any email solicitation by contacting the organization directly through a trusted contact number. You can find trusted contact information for many charities on the BBB National Charity Report Index.