FLORIDA INTERNATIONAL UNIVERSITY POLICE DEPARTMENT

NOTIFICATION

TIMELY WARNING BULLETIN

Date: November 1, 2019

The Florida International University Police Department (FIUPD) and the Division of Information Technology (DoIT) want you to be aware of ongoing fraudulent activity so you do not fall victim. Scammers are becoming increasingly savvy on how to defraud users and obtain their personal information. Don't become a victim! There are different ways in which these scammers can obtain your personal information.

Phishing is one of the easiest and most common forms of a cyber-attack. Typically in the form of email communication, a scammer will send an email that appears to be from a legitimate email address and will ask you to provide sensitive information or perform some action on their behalf. These emails are carefully crafted so that you open them without any suspicion.

In addition to email, there are other channels in which you can be phished like vishing, which is a form of phishing done over the phone, and smishing or SMS phishing done through text messages. Scammers will call impersonating your bank or the Internal Revenue Service (IRS) and try to obtain personal information such as your Social Security Number or bank account number. You may receive a fake order detail confirmation containing a link which would route you to a fake page designed to gather your personal information.

Ransomware, is a type of cyber-attack that uses malicious software to take control of your computer and encrypts all of your files preventing you from having access to them until a ransom payment is made. Usually, the ransomware attacks occur when users click on a link or attachment received by email.

Scammers are also using personal information obtained through online social media profiles such as Facebook or Instagram to contact family members and make them believe you or a family member has been kidnapped. The scammers demand a ransom and will state that if you do not wire the money immediately, they will harm the fake victim. These can be quite elaborate with people screaming in the background. If you were to receive this phone call stall the caller by stating you need to take notes and text the alleged kidnap victim to make sure they are safe.

Unsuspecting victims are also being offered large sums of money in exchange for cashing a winning lottery ticket or checks on behalf of scammers. They will ask you for money as a sign of good faith and provide you with a fake lottery ticket or a worthless check.

Remember you are your best defense in protecting yourself from scammers and staying educated and informed is critical. DoIT offers resources to help you become better informed on how to protect yourself. Visit https://security.fiu.edu for more information. Also, the Federal Trade Commission offers information outlining the latest scams at https://www.consumer.ftc.gov/features/scam-alerts. As always, the FIUPD is also here at 305-348-2626 to help. In the event of an emergency, please call FIUPD at 305-348-5911.

Florida International University Police Department

885 Southwest 109th Avenue, PG5 Marketplace

(305) 348-2626 | Emergency: (305) 348-5911