GEORGE MASON UNIVERSITY

Security Liaisons Newsletter

You are key to Internet safety and security at Mason

Information Technology Services | Security Office — itsoinfo@gmu.edu | AUGUST 2017

Identifying, Reporting Common Scams

Overview

The Federal Trade Commission (FTC) recently issued an alert on scammers posing as FTC officials who contact individuals and claim they have won prizes from a charity contest. The scammers ask for money to cover taxes or insurance costs associated with the prize.

While this is a new malicious campaign, criminals use these basic tactics time and time again with slightly different wording to take advantage of unsuspecting individuals. It may seem like a day doesn't go by without criminals contacting you online or by phone seeking money and/or personal information. Since this is so commonplace, it is worth exploring how to identify these schemes, and how to go about reporting them in the event that criminals target you.

Identifying a Scam

Two common financial schemes involve coercing individuals into paying money to prevent a negative outcome, such as a tax audit, a police investigation, or asking the individual to pay a fee upfront to claim a prize. A third type of scam seeks individuals' personally identifiable information (PII), such as Social Security numbers and birth dates, to commit identity theft. Individuals providing information to criminals may suffer financial losses, as well as negative impacts to their credit. It is important that you know how to spot these scams so you can easily ignore them.

It's most likely a scam if you:

- Have to pay money to claim a "prize" or "winnings"
- Are asked for money to stop or prevent a police, FBI, or other federal investigation
- Have to provide your bank account number and information
- Are specifically asked to purchase any form of a prepaid gift card to be used as payment
- Are approached with no prior contact to give out your date of birth, social security number, password, username or other personal sensitive information online or over the phone
- Are approached online or by phone in an unprovoked manner and asked for payment or personal information by someone claiming to be a government employee on official business

One final thing to be aware of is that criminals create convincing emails that may look like official communication from Mason, your bank, credit card issuer, or a retailer. These emails often include a link to a very convincing, yet fraudulent website that will ask you to log in with your username and password.

If you provide your credentials, the criminal can then use them to gain access to your legitimate account. From there, they can steal your personal information or generate fraudulent transactions. If you ever receive an email asking you to click a link to log in and update your account or change your information, be safe and use your browser to directly type in the legitimate website address for that account in order to complete this request. By doing this, you will always be sure you are on the right website.

Criminals constantly target individuals by email, false advertisements, and phone calls to bring these types of scams to fruition. Being wary of any communication that meets any of the above criteria will go a long way in keeping your information and money safe!

Reporting Scams

Finally, it is very important that targets of online or phone scams report this to the proper authorities. Although it can be a bit embarrassing to have been hit by such a crime, reporting is the only way to direct investigators and regulators to pursue the criminals behind the scam or identity theft. Aside from reporting the scam to law enforcement, it is important to work with your bank, credit card issuer, or the business where your account was compromised to take the necessary steps in preventing further financial loss.

If you are the target of a financial scam, report it to the FTC. If this scam was via email or over the Internet, also file a complaint with the FBI's Internet Crime Complaint Center.

Targets of identity theft can also file a report to the FTC and receive a recovery plan detailing how to move forward based on the type of scam committed.

Worth repeating

One final thing to be aware of is that criminals create convincing emails that may look like official communication from Mason, your bank, credit card issuer, or a retailer. These emails often include a link to a very convincing, yet fraudulent website that will ask you to log in with your username and password.

CYBER SECURITY AWARENESS: "OUR SHARED RESPONSIBILITY"
www.msisac.org | www.staysafeonline.org | www.nascio.org | www.dhs.gov

The information provided in the monthly newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall information security posture. Mason's IT Security Office brings you these tips produced by the Virginia Information Technologies Agency (http://www.vita.virginia.gov/security/), in coordination with: www.msisac.org and http://www.us-cert.gov/