July, 2017
Volume 12, Issue 7

Identifying and Reporting Common Scams

Central Bank
11201 Clay Road
Houston, Texas 77041
832.485.2300

From the Desk of Thomas F. Duffy, Chair, MS-ISAC

On July 6, 2017 the Federal Trade Commission (FTC) 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, scammers 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 scammers 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 scammers target you.

Identifying the scam

Two common financial schemes involve coercing individuals into paying money to prevent a negative outcome, such as a tax audit or police investigation, or asking the individual to pay a fee up front to claim a prize. A third type of scam seeks individuals' personally identifiable information (PII), such as Social Security numbers and birthdates, to commit identity theft. Individuals providing information to scammers may suffer large 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 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 scammers create convincing emails that may look like official communication from 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.

Scammers 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 at www.ftc.gov/complaint. If this scam was via email or over the Internet, also file a complaint with the FBI's Internet Crime Complaint Center at www.ic3.gov/complaint.

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

MS-ISAC
Multi-State Information Sharing & Analysis Center

STOP | THINK CONNECT™

The information provided in the Monthly Security Tips 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 cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.
Disclaimer: These links are provided because they have information that may be useful. The Center for Internet Security (CIS) does not warrant the accuracy of any information contained in the links and neither endorses nor intends to promote the advertising of the resources listed herein. The opinions and statements contained in such resources are those of the author(s) and do not necessarily represent the opinions of CIS.