September 2014
Volume 9, Issue 9

Social Media Scams – Spot Them Beforehand!

Town of Wareham

From the Office of Information Management Technology

The use of social media has exploded, with 255 million active users on Twitter and more than 1.2 billon on Facebook. Unfortunately, so too have the scams and attacks that target social media. Criminals are taking advantage of the increasing number of users and the enormous amount of information exchanged.

What are Some Common Scams?

1. Information about special events (such as the Olympics), or tragedies (such as the missing Malaysian Airliner) could be used by those with malicious intent to conduct social engineering scam, particularly on social media. For example, many individuals are tempted to click on a video they see on their "newsfeed." Unfortunately, these videos may lead to a malicious website designed to infect your computer.
2. Typical scams feature notices of items that can be "free" for you or available at a very low price. If you notice an online advertisement about the newest tech gadget, at a ridiculously low cost, it is most likely a scam to trap users into clicking on the ad. Sometimes a refundable deposit is requested, other times, direct access to your Facebook account requested. These are scams intending to victimize you and your friends.

   Fake organizations claiming to be charities have mushroomed on social media sites. They often post heart-wrenching images, such as a picture of babies with serious diseases or a fire that destroyed an entire community – basically anything that will appeal to people's emotions. These posts almost always include a call-to-action, such as pleas for donations. Avoid being a victim. Investigate the legitimacy of these organizations before contributing.

What Precautions can be Taken?

- Do not post private and confidential information, such as your credit card number, password or other personal information.
- Install anti-virus software, proper firewalls, and anti-malware programs on your devices, including desktops, laptop, smartphones, tables, etc., that you use to access social networking sites.
- Inspect a link before clicking on it. If it seems suspicious, trust your instincts and don't click, even if the link has supposedly originated from someone you know and trust. It is possible that their account was compromised, and could be spreading malware without their knowledge.
- When posting images, change settings accordingly to ensure they are private and can be viewed only by people whom you trust. If you delete your account, make sure all data and pictures are removed.
- Third party applications provided by social networking sites might not have the same privacy policy or security model as the social media site. You should not allow these apps to have complete access to your account; your personal data can be stolen or misused.

- Use strong, unique passwords that only you know. Each account on social media should have varied passwords.

Exercising caution is the best defense – enjoy social media but be alert for fraudulent activities!

For More Information

Center for Internet Security Primer: Tips for Avoiding Scams Following Major Events:

https://iic.cisecurity.org/resources/documents/CISPrimer-TipsforAvoidingScamsFollowingMajorEvents_000.pdf

State of Washington, Department of Financial Institutions Social Networking Investment Scams:
http://www.dfi.wa.gov/consumers/education/investments/social-networks.htm

Norton: Top 5 Social Media Scams
http://us.norton.com/yoursecurityresource/detail.jsp?aid=social_media_scams

Panda Security: Scams on Social Networks
http://www.pandasecurity.com/mediacenter/social-media/scams-social-networks-will-surprise/

Provided By:

CENTER FOR INTERNET SECURITY | 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.