Division of Information Security's

Monthly Security Tips Newsletter

BCB
SC Budget and Control Board

Social Media Scams: Spot Them Beforehand!

What are Some Common Scams?

- 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 scams, 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.

- 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 and 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 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/