June 2015
Volume 10, Issue 6

Social Engineering Through The Internet

United Republic Bank
You and URB.

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

Social engineering refers to the methods attackers use to manipulate people into sharing sensitive information, or taking an action, such as downloading a file. Sometimes a social engineer is able to rely solely on information posted online or will sometimes interact with the victim to persuade the victim to share details or perform an action.

Oversharing Online

Information posted online can seem harmless, until you think about how a social engineer could use the same information. By gathering multiple pieces of information from various sources, a cyber criminal could have enough facts about you to craft a very convincing social engineering scam. Think about how these seemingly innocuous details might be valuable to the cyber criminal:

- Posting a picture of your pet might give away your pet's name, or posting a photo of your car would identify its color. Pet's name and car color are common security questions.
- Answering a "meme" can give away personally identifiable information (PII) such as your date of birth or other sensitive information, including answers to security questions.

Be careful about how much information you post and think about how the various pieces might be combined for use by a cyber criminal.

Persuasion Scams

The following three common types of persuasion methods highlight different ways social engineers target victims through the Internet.

Tech Support Call Scams

In Tech Support Call Scams the scammer, claiming to work for a well-known software or technology company cold calls victims in an attempt to convince the victim that their computer is at risk of attack, attacking another computer, or is infected with malware, and that only the caller can remediate the problem. In convincing the victim, the scammer often persuades the victim to provide remote access to the victim's computer. The scammer can then install malware or access sensitive information. In some variations the scammer persuades the victim to pay for unnecessary or fictitious antivirus software or software updates.

Romance Scams

In Romance Scams the malicious actors create fake profiles on dating websites and establish relationships with other site members. Once a sense of trust is established, the scammer fabricates an emergency and asks the victim for financial assistance. The

scammer generally claims they will repay the victim as soon as the crisis is over, however, if the victim sends money, the scammer will prolong the scam, sometimes stealing thousands of dollars from the victim.

Traveler Scams

In this scenario, also known as the "Grandparent Scam," malicious actors use information posted on social media websites by a traveling family member to trick other family members into sending money overseas. Often the scam targets the elderly, who are less likely to realize the information was originally posted online. The scammer will monitor social media websites for people traveling overseas, and then contact the family members, through the Internet or via phone, with a crisis and requesting that money be sent immediately. The scammers rely on all the information users post online about themselves and their trips, in order to convince the family member that they know the traveler and are privy to personal details, and thus should be trusted.

Easy Tips to Protect Yourself from Social Engineering

- Use discretion when posting personal information on social media. This information is a treasure-trove to scammers who will use it to feign trustworthiness.
- Before posting any information, consider: What does this information say about me? How can this information be used against me? Is this information, if combined with other information, harmful?
- Remind friends and family members to exercise the same caution. Request that they remove revealing information about you.
- Verify the identity of anyone who contacts you through different means – do not use the information they provide you.
- Do not send money to people you do not know and trust.

For More Information

- Internet Crime Complaint Center (IC3): http://www.ic3.gov/default.aspx
- Federal Bureau of Investigation's Common Fraud Schemes: http://www.fbi.gov/scams-safety/fraud/internet_fraud
- OnGuard Online: https://www.onguardonline.gov/
- Looks Too Good To Be True: http://www.lookstoogoodtobetrue.com/

Provided By:

Center for Internet Security
MULTI-STATE Information Sharing & Analysis Center

STOP | THINK | CONNECT