SOCIAL MEDIA

Lawrence J. Fennelly, CHL III, CPOI, CSSI, CSSP-I

Marianna Perry, M.S., CPP, CSSP-I

"Social Media has transformed how culture works. Digital crowds have become powerful cultural innovators."

Douglas Holt
Harvard Business Review, 2016

We are not only in the digital technology age, but we are in the age of Social Media. Our culture has been affected by this phenomenon. Many managers jump on-line before they even brush their teeth!

Social media has helped to bind groups and communities together. We have more linked-in security groups on line than we ever knew existed, and this group culture has expanded with active participants.

For the Security Cultural Community, the groups discuss issues, books, events and knowledge. They ask questions, seek answers and seek certifications. Leaders and Leadership strategies are developed. Consultants get a boost and audiences are formed. Some may call this Crowd Culture. Webinars and conferences are promoted on-line as well as presenters.

Security companies offering a wide variety of on-line whitepapers touting their latest technology and use this as a means of promoting their brand of products. Professional public relations firms are busier than ever because a new media outlet is now available to them.

We are seeing this person and that person with five million followers! Our ASIS School Safety and Security Council in less than a year old and has 3000 followers . . . and the group is becoming larger each month! But what is the ultimate goal? What are the long term objectives? Where will all of the growth come from? Moving ahead strategies will be developed taking the Social Media Culture to the next level.

Since we're talking about Social Media, we would be remiss to not mention some things about on-line safety. We all can use a few reminders on internet safety. The following information is taken from: www.fbi.gov. Internet-based social networking sites have created a revolution in social connectivity. However, conartists, criminals and other dishonest actors are exploiting this capability for nefarious purposes. There are primarily two tactics used to exploit online social networks. In practice, they are often combined:

1. Computer savvy hackers who specialize in writing and manipulating computer code to gain access or install unwanted software on your computer or phone.

2. Social or human hackers who specialize in exploiting personal connections through social networks. Social hackers, sometimes referred to as "social engineers," manipulate people through social interactions (in person, over the phone, or in writing).

Humans are a weak link in cyber security, and hackers and social manipulators know this. They try totrick people into getting past security walls. They design their actions to appear harmless and legitimate. Falling for an online scam or computer hack could be damaging for an individual victim as well as the organization the victim works for.

Vulnerability of Social Networking Sites

Social networking sites are Internet-based services that allow people to communicate and share information with a group.

Risks:

Once information is posted to a social networking site, it is no longer private. The more information you post, the more vulnerable you may become. Even when using high security settings, friends or websites may inadvertently leak your information. Personal information you share could be used to conduct attacks against you or your associates. The more information shared, the more likely someone could impersonate you and trick one of your friends into sharing personal information,downloading malware, or providing access to restricted sites.Predators, hackers, business competitors, and foreign state actors troll social networking sites looking for information or people to target for exploitation.

Information gleaned from social networking sites may be used to design a specific attack that does not come by way of the social networking site.

Tactics:

Baiting - Someone gives you a USB drive or other electronic media that is preloaded with malware in the hope you will use the device and enable them to hack your computer. Do not use any electronic storage device unless you know its origin is legitimate and safe. Scan all electronic media for viruses before use.

Click-jacking - Concealing hyperlinks beneath legitimate clickable content which, when clicked, causes a user to unknowinglyperform actions, such as downloading malware, or sending your ID to a site. Numerous click-jacking scams have employed "Like" and "Share" buttons on social networking sites. Disable scripting and iframes in whatever Internet browser you use. Research other ways to set your browser options to maximize security.

Cross-Site Scripting (XSS) - Malicious code is injected into a benign or trusted website. A Stored XSS Attack is when malicious code is permanently stored on a server; a computer is compromised when requesting the stored data. A Reflected XSS Attack is when a person is tricked into clicking on a malicious link; the injected code travels to the server then reflects the attack back to the victim's browser. The computer deems the code is from a "trusted" source.

Turn off "HTTP TRACE" support on all webservers.

Doxing - Publicly releasing a person's identifying information including full name, date of birth, address, and pictures typically retrieved from social networking site profiles.

Be careful what information you share about yourself, family, and friends (online, in print, and in person).

Elicitation - The strategic use of conversation to extract information from people without giving them the feeling they are being interrogated. Be aware of elicitation tactics and the way social engineers try to obtain personal information.

Pharming - Redirecting users from legitimate websites to fraudulent ones for the purpose of extracting confidential data. Watch out for website URLs that use variations in spelling or domain names, or use “.com” instead of “.gov”, for example. Type a website’s address rather than clicking on a link.

Phishing - Usually an email that looks like it is from a legitimate organization or person, but is not and contains a link or file with malware. Phishing attacks typically try to snag any random victim. Spear phishing attacks target a specific person or organization as their intended victim.

Do not open email or email attachments or click on links sent from people you do not know. If you receive a suspicious email from someone you know, ask them about it before opening it.

Phreaking - Gaining unauthorized access to telecommunication systems.

Do not provide secure phone numbers that provide direct access to a Private Branch Exchange or through the Public Branch Exchange to the public phone network.

Scams - Fake deals that trick people into providing money, information, or service in exchange for the deal.

If it sounds too good to be true, it is most likely a scam. Cybercriminals use popular events and news stories as bait for people to open infected email, visit infected websites, or donate money to bogus charities.

Spoofing - Deceiving computers or computer users by hiding or faking one’s identity. Email spoofing utilizes a sham email address or simulates a genuine email address. IP spoofing hides or masks a computer’s IP address.