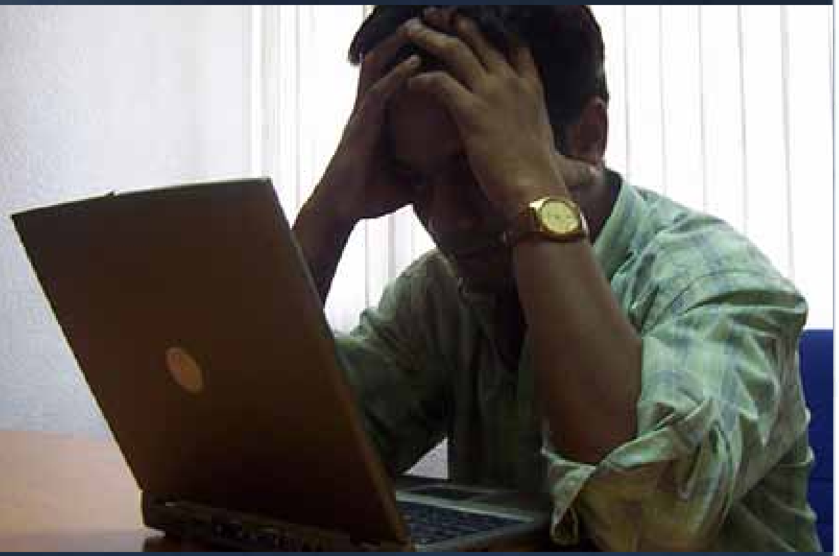
U.S. Department of Justice
Federal Bureau of Investigation

INTERNET SOCIAL NETWORKING RISKS

Internet-based social networking sites have created a revolution in social connectivity. However, con artists, 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 to trick 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. Such risks include:

- **Identity theft / Impersonation**
- **Harassment**
- **Peer pressure**
- **Loss of employment**
- **Damaged business reputation**
- **Damaged career or personal reputation**
- **Damaged data or networks**
- **Intellectual property theft / Data theft**
- **Brand hijacking**
- **Delays or interruption in production**
- **Lost revenue or income**
- **Burglary**
- **Target for spam and phishing**
- **Content alteration of websites**
- **Malware and virus dissemination**

There are many tactics people may use to trick others into providing information or granting access to that information through social networking venues. Although not exhaustive, this brochure lists some of these tactics and suggests ways to mitigate online social networking risks.

EXAMPLE ✕

You receive a message from a friend on your social networking site. The message directs you to view a video on another site. When you go to that site, a message pops up and says you need to download a newer version of software. However, the software update is really malware that, when downloaded, gives control of your computer to the creators of the malware. (In some cases, simply visiting the site will download the malware.) The malware then sends a message to all your “friends” on your social networking site directing them to the same site with the malware. The malware creators soon have multiple computers under their control (a “botnet”).

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 unknowingly perform 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. Research additional ways to prevent becoming a victim of XSS.

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. (E.g.: mimicking bank websites.)

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.

EXAMPLE

Most computer infections come from websites. Just visiting a website can expose your computer to malware even if you do not download a file or program. Often legitimate sites may be unknowingly infected.

Websites with information on popular celebrities or current sensational news items are frequently hijacked by criminals, or criminals may create such websites to lure victims to them.

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.

EXAMPLE

In March 2011, hackers sent two spear phishing emails to a small group of employees at security firm, RSA. They only needed one employee to open an infected file and launch the malware. The malware downloaded information from RSA that then helped the hackers learn how to defeat RSA’s security token. In May and June 2011, a number of defense contractors’ networks were breached via the compromised RSA token.

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.

EXAMPLE

Before the 2010 World Cup, cybercriminals offered tickets for sale or sent phishing emails claiming you won tickets to see the event.

After the death of Osama Bin Laden, a video claiming to show Bin Laden’s capture was posted on Facebook. The video was a fake. When users clicked on the link to the video, they were told to copy a JavaScript code into their browser bar which automatically sent the hoax to their friends, and gave the hackers full access to their account.

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.

Know your co-workers and clients and beware of those who impersonate a staff member or service provider to gain company or personal information.

Preventive Measures at Work:

- “Defense in Depth” – use multiple layers of security throughout the computer network.
- Identify ways you have lost data in the past and mitigate those threats. Educate employees about those threats and how to change their behavior, if necessary, to prevent future loss.
- Constantly monitor data movement on your network.
- Establish policies and procedures for intrusion detection systems on company networks.
- Establish policies about what company information can be shared on blogs or personal social web pages. Enforce the policy.
- Educate employees about how their own online behavior could impact the company.
- Provide yearly security training.
- Ask employees to report suspicious incidents as soon as possible.

Additional Preventive Measures:

- Do not store any information you want to protect on any device that connects to the Internet.
- Always use high security settings on social networking sites, and be very limited in the personal information you share. Monitor what others are posting about you on their online discussions.
- Use anti-virus and firewall software. Keep them, your browser, and operating systems patched and updated.
- Change your passwords periodically, and do not reuse old passwords. Do not use the same password for more than one system or service. For example, if someone obtains the password for your email, can they access your online banking information with the same password?
- Do not post anything that might embarrass you later or that you don’t want strangers to know.
- Verify those you correspond with. It is easy for people to fake identities over the Internet.
- Do not automatically download, or respond to content on a website or in an email. Do not click on links in email messages claiming to be from a social networking site. Instead go to the site directly to retrieve messages.
- Only install applications or software that come from trusted, well-known sites. “Free” software may come with malware. Verify what information applications will be able to access prior to enabling them. Once installed, keep it updated. If you no longer use it, delete it.
- Disable Global Positioning System (GPS) encoding. Many digital cameras encode the GPS location of a photo when it is taken. If that photo is uploaded to a site, so are the GPS coordinates, which will let people know that exact location.
- Whenever possible, encrypt communications with websites. It may be a feature social network sites allow you to enable.
- Avoid accessing your personal accounts from public computers or through public WiFi spots.
- Beware of unsolicited contacts from individuals in person, on the telephone, or on the Internet who are seeking corporate or personal data.
- Monitor your bank statements, balances, and credit reports.
- Do not share usernames, passwords, social security numbers, credit cards, bank information, salaries, computer network details, security clearances, home and office physical security and logistics, capabilities and limitations of work systems, or schedules and travel itineraries.

No legitimate service or network administrator will ask you for your password.

- Do not provide information about yourself that will allow others to answer your security questions—such as when using “I forgot my password” feature.
- Be thoughtful and limit personal information you share such as job titles, locations, hobbies, likes and dislikes, or names and details of family members, friends, and co-workers.

Educational Resources:

A number of organizations and websites provide additional details on how to protect you and your workplace from Internet social networking threats.

www.LooksTooGoodToBeTrue.com

www.OnGuardOnline.gov

www.us-cert.gov

www.ic3.gov

www.dhs.gov

www.ftc.gov

www.fbi.gov