2020

Staying Safe on Social Networking Sites

DHS Security Tip (ST06-003)

INCEPTUS | CAPE CORAL, FLORIDA 33904

Contents

What are social networking sites?

Social networking sites, sometimes referred to as "friend-of-a-friend" sites, build upon the concept of traditional social networks where you are connected to new people through people you already know. The purpose of some networking sites may be purely social, allowing users to establish friendships or romantic relationships, while others may focus on establishing business connections.

Although the features of social networking sites differ, they all allow you to provide information about yourself and offer some type of communication mechanism (forums, chat rooms, email, instant messages) that enables you to connect with other users. On some sites, you can browse for people based on certain criteria, while other sites require that you be "introduced" to new people through a connection you share. Many of the sites have communities or subgroups that may be based on a interest.

What security implications do these sites present?

Social networking sites rely on connections and communication, so they encourage you to provide a certain amount of personal information. When deciding how much information to reveal, people may not exercise the same amount of caution as they would when meeting someone in person because

- the internet provides a sense of anonymity
- the lack of physical interaction provides a false sense of security
- they tailor the information for their friends to read, forgetting that others may see it
- they want to offer insights to impress potential friends or associates

While most people using these sites do not pose a threat, malicious people may be drawn to them because of the accessibility and amount of personal information that's available. The more information malicious people have about you, the easier it is for them to take advantage of you. Predators may form relationships online and then convince unsuspecting individuals to meet them in person. That could lead to a dangerous situation. The personal information can also be used to conduct a social engineering attack. Using information that you provide about your location, hobbies, interests, and friends, a malicious person could impersonate a trusted friend or convince you that they have the authority to access other personal or financial data.

Additionally, because of the popularity of these sites, attackers may use them to distribute malicious code. Sites that offer applications developed by third parties are particularly susceptible. Attackers may be able to create customized applications that appear to be innocent while infecting your computer or sharing your information without your knowledge.

How can you protect yourself?

- **Limit the amount of personal information you post** - Do not post information that would make you vulnerable, such as your address or information about your schedule or routine. If your connections post information about you, make sure the combined information is not more than you would be comfortable with strangers knowing. Also be considerate when posting information, including photos, about your connections.
- **Remember that the internet is a public resource** - Only post information you are comfortable with anyone seeing. This includes information and photos in your profile and in blogs and other forums. Also, once you post information online, you can't retract it. Even if you remove the information from a site, saved or cached versions may still exist on other people's machines.
- **Be wary of strangers** - The internet makes it easy for people to misrepresent their identities and motives. Consider limiting the people who can contact you on these sites. If you interact with people you do not know, be cautious about the amount of information you reveal or agreeing to meet them in person.
- **Be skeptical** - Don't believe everything you read online. People may post false or misleading information about various topics, including their own identities. This is not necessarily done with malicious intent; it could be unintentional, an exaggeration, or a joke. Take appropriate precautions, though, and try to verify the authenticity of any information before taking any action.
- **Evaluate your settings** - Take advantage of a site's privacy settings. The default settings for some sites may allow anyone to see your profile, but you can customize your settings to restrict access to only certain people. There is still a risk that private information could be exposed despite these restrictions, so don't post anything that you wouldn't want the public to see. Sites may change their options periodically, so review your security and privacy settings regularly to make sure that your choices are still appropriate.
- **Be wary of third-party applications** - Third-party applications may provide entertainment or functionality but use caution when deciding which applications to enable. Avoid applications that seem suspicious and modify your settings to limit the amount of information the applications can access.
- **Use strong passwords** - Protect your account with passwords that cannot easily be guessed. If your password is compromised, someone else may be able to access your account and pretend to be you.
- **Check privacy policies** - Some sites may share information such as email addresses or user preferences with other companies. This may lead to an increase in spam. Also, try to locate the policy for handling referrals to make sure that you do not unintentionally sign your friends up for spam. Some sites will continue to send email messages to anyone you refer until they join.
- **Keep software, particularly your web browser, up to date** - Install software updates so that attackers cannot take advantage of known problems or vulnerabilities. Many operating systems offer automatic updates. If this option is available, you should enable it.

- **Use and maintain anti-virus software** - Anti-virus software helps protect your computer against known viruses, so you may be able to detect and remove the virus before it can do any damage. Because attackers are continually writing new viruses, it is important to keep your definitions up to date.

Children are especially susceptible to the threats that social networking sites present. Although many of these sites have age restrictions, children may misrepresent their ages so that they can join. By teaching children about Internet safety, being aware of their online habits, and guiding them to appropriate sites, parents can make sure that the children become safe and responsible users.

How can Inceptus help?

With the ever-changing threat landscape, it is difficult to keep up with the changes and threats that evolve daily. That is why you need a dedicated team that is dedicated to keeping you safe, secure and protected while doing business on the Internet. Inceptus Protection Plans are tailored security programs designed to address the gaps in your current ecosystems cyber security stance and provide the ultimate protection against hackers, malware/ransomware and downtime, all while protecting your brand & reputation.

- No matter where you have already made investments in you cyber posture Inceptus will assess your organization to identify gaps to your cyber defenses.
- A customized plan is designed to fill the gaps with plug-in cyber solutions and services to ensure that there are layers of defenses at each stage the cyber kill chain to stop even the most determined adversaries.
- Our comprehensive defense in depth strategies protect you against hackers by providing competing controls and processes between hackers and your data.
- All services are installed, hardened, managed, supported and monitored 24/7/365 by Inceptus' highly skilled analysts that follow tried and tested incident response processes and harden your ecosystem keeping you and your data stays safe.

Contact Inceptus

Inceptus
4825 Coronado Pkwy., Suite 1
Cape Coral, FL 33904
(239) 673-8130

General Questions:
info@inceptussecure.com
Support Questions:
soc@inceptussecure.com