Internet Safety Policy

Quaker Digital Academy Internet Safety Policy

QDA has designated the following articles to educate students and staff members about appropriate online behavior on social networking sites, chat rooms, electronic communications, cyberbullying awareness, and the dangers of disclosing personally identifiable information online.

The following articles were produced by the United States Computer Emergency Readiness Team and are being provided for noncommercial purposes to QDA students for educational purposes. For additional information on US-CERT, please visit: www.us-cert.gov

Table of Contents

Security Tip (ST06-003)

Staying Safe on Social Network Sites

Original Release date: March 29, 2006 | Last revised: January 26, 2011

The popularity of social networking sites continues to increase, especially among teenagers and young adults. The nature of these sites introduces security risks, so you should take certain precautions.

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 messenger) 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 particular 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 the majority of 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 (see Avoiding Social Engineering and Phishing Attacks for more information). 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 (see Guidelines for Publishing Information Online for more information).
- **Be wary of strangers** - The internet makes it easy for people to misrepresent their identities and motives (see Using Instant Messaging and Chat Rooms Safely for more information). Consider limiting the people who are allowed to 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 (see Choosing and Protecting Passwords for more information). 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 (see Reducing Spam for more information). 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 (see Understanding Patches for more information). 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 (see Understanding Anti-Virus Software for more information). 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 (see Keeping Children Safe Online for more information).

Related information

- Socializing Securely: Using Social Networking Services

Author: Mindi McDowell

Security Tip (ST04-011)

Using Instant Messaging and Chat Rooms Safely

Original release date: June 16, 2004 | Last revised: September 23, 2009

Although they offer a convenient way to communicate with other people, there are dangers associated with tools that allow real-time communication.

What are the differences between some of the tools used for real-time communication?

- Instant messaging (IM) - Commonly used for recreation, instant messaging is also becoming more widely used within corporations for communication between employees. IM, regardless of the specific software you choose, provides an interface for individuals to communicate one-on-one.
- Chat rooms - Whether public or private, chat rooms are forums for particular groups of people to interact. Many chat rooms are based upon a shared characteristic; for example, there are chat rooms for people of particular age groups or interests. Although most IM clients support "chats" among multiple users, IM is traditionally one-to-one while chats are traditionally many-to-many.
- Bots - A "chat robot," or "bot," is software that can interact with users through chat mechanisms, whether in IM or chat rooms. In some cases, users may be able to obtain current weather reports, stock status, or movie listings. In these instances, users are often aware that they are not interacting with an actual human. However, some users may be fooled by more sophisticated bots into thinking the responses they are receiving are from another person.

There are many software packages that incorporate one or more of these capabilities. A number of different technologies might be supported, including IM, Internet Relay Chat (IRC), or Jabber.

What are the dangers?

- Identities can be elusive or ambiguous - Not only is it sometimes difficult to identify whether the "person" you are talking to is human, but human nature and behavior isn't predictable. People may lie about their identity, accounts may be compromised, users may forget to log out, or an account may be shared by multiple people. All of these things make it difficult to know who you're really talking to during a conversation.
- Users are especially susceptible to certain types of attack - Trying to convince someone to run a program or click on a link is a common attack method, but it can be especially effective through IM and chat rooms. In a setting where a user feels comfortable with the "person" he or she is talking to, a malicious piece of software or an attacker has a better chance of convincing someone to fall into the trap (see Avoiding Social Engineering and Phishing Attacks for more information).
- You don't know who else might be seeing the conversation - Online interactions are easily saved, and if you're using a free commercial service the exchanges may be archived on a server. You have no control over what happens to those logs. You also don't know if there's someone looking over the shoulder of the person you're talking to, or if an attacker might be "sniffing" your conversation.
- The software you're using may contain vulnerabilities - Like any other software, chat software may have vulnerabilities that attackers can exploit.

- Default security settings may be inappropriate - The default security settings in chat software tend to be relatively permissive to make it more open and "usable," and this can make you more susceptible to attacks.

How can you use these tools safely?

- **Evaluate your security settings** - Check the default settings in your software and adjust them if they are too permissive. Make sure to disable automatic downloads. Some chat software offers the ability to limit interactions to only certain users, and you may want to take advantage of these restrictions.
- **Be conscious of what information you reveal** - Be wary of revealing personal information unless you know who you are really talking to. You should also be careful about discussing anything you or your employer might consider sensitive business information over public IM or chat services (even if you are talking to someone you know in a one-to-one conversation).
- **Try to verify the identity of the person you are talking to, if it matters** - In some forums and situations, the identity of the "person" you are talking to may not matter. However, if you need to have a degree of trust in that person, either because you are sharing certain types of information or being asked to take some action like following a link or running a program, make sure the "person" you are talking to is actually that person.
- **Don't believe everything you read** - The information or advice you receive in a chat room or by IM may be false or, worse, malicious. Try to verify the information or instructions from outside sources before taking any action.
- **Keep software up to date** - This includes the chat software, your browser, your operating system, your mail client, and, especially, your anti-virus software (see Understanding Patches and Understanding Anti-Virus Software for more information).

Authors: Mindi McDowell, Allen Householder

Security Tip (ST04-014)

Avoiding Social Engineering and Phishing Attacks

Original release date: July 28, 2004 | Last revised: October 22, 2009

> Do not give sensitive information to anyone unless you are sure that they are indeed who they claim to be and that they should have access to the information.

What is a social engineering attack?

In a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization or its computer systems. An attacker may seem unassuming and respectable, possibly claiming to be a new employee, repair person, or researcher and even offering credentials to support that identity. However, by asking questions, he or she may be able to piece together enough information to infiltrate an organization's network. If an attacker is not able to gather enough information from one source, he or she may contact another source within the same organization and rely on the information from the first source to add to his or her credibility.

What is a phishing attack?

Phishing is a form of social engineering. Phishing attacks use email or malicious websites to solicit personal information by posing as a trustworthy organization. For example, an attacker may send email seemingly from a reputable credit card company or financial institution that requests account information, often suggesting that there is a problem. When users respond with the requested information, attackers can use it to gain access to the accounts.

Phishing attacks may also appear to come from other types of organizations, such as charities. Attackers often take advantage of current events and certain times of the year, such as

- natural disasters (e.g., Hurricane Katrina, Indonesian tsunami)
- epidemics and health scares (e.g., H1N1)
- economic concerns (e.g., IRS scams)
- major political elections
- holidays

How do you avoid being a victim?

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.

- Don't send sensitive information over the Internet before checking a website's security (see Protecting Your Privacy for more information).
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic (see Understanding Firewalls, Understanding Anti-Virus Software, and Reducing Spam for more information).
- Take advantage of any anti-phishing features offered by your email client and web browser.

What do you do if you think you are a victim?

- If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including network administrators. They can be alert for any suspicious or unusual activity.
- If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.
- Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account, and do not use that password in the future.
- Watch for other signs of identity theft (see Preventing and Responding to Identity Theft for more information).
- Consider reporting the attack to the police, and file a report with the Federal Trade Commission (http://www.ftc.gov/).

Author: Mindi McDowell

Security Tip (ST06-005)

Dealing with Cyberbullies

Original Release date: May 31, 2006 | Last revised: June 1, 2011

Bullies are taking advantage of technology to intimidate and harass their victims. Dealing with cyberbullying can be difficult, but there are steps you can take.

What is cyberbullying?

Cyberbullying refers to practice of using technology to harass, or bully, someone else. Bullies used to be restricted to methods such as physical intimidation, postal mail, or the telephone. Now, developments in electronic media offer forums such as email, instant messaging, web pages, and digital photos to add to the arsenal. Computers, cell phones, and PDAs are current tools that are being used to conduct an old practice.

Forms of cyberbullying can range in severity from cruel or embarrassing rumors to threats, harassment, or stalking. It can affect any age group; however, teenagers and young adults are common victims, and cyberbullying is a growing problem in schools.

Why has cyberbullying become such a problem?

The relative anonymity of the internet is appealing for bullies because it enhances the intimidation and makes tracing the activity more difficult. Some bullies also find it easier to be more vicious because there is no personal contact. Unfortunately, the internet and email can also increase the visibility of the activity. Information or pictures posted online or forwarded in mass emails can reach a larger audience faster than more traditional methods, causing more damage to the victims. And because of the amount of personal information available online, bullies may be able to arbitrarily choose their victims.

Cyberbullying may also indicate a tendency toward more serious behavior. While bullying has always been an unfortunate reality, most bullies grow out of it. Cyberbullying has not existed long enough to have solid research, but there is evidence that it may be an early warning for more violent behavior.

How can you protect yourself or your children?

- **Teach your children good online habits** - Explain the risks of technology, and teach children how to be responsible online (see Keeping Children Safe Online for more information). Reduce their risk of becoming cyberbullies by setting guidelines for and monitoring their use of the internet and other electronic media (cell phones, PDAs, etc.).
- **Keep lines of communication open** - Regularly talk to your children about their online activities so that they feel comfortable telling you if they are being victimized.
- **Watch for warning signs** - If you notice changes in your child's behavior, try to identify the cause as soon as possible. If cyberbullying is involved, acting early can limit the damage.
- **Limit availability of personal information** - Limiting the number of people who have access to contact information or details about interests, habits, or employment reduces exposure to bullies that you or your child do not know. This may limit the risk of becoming a victim and may make it easier to identify the bully if

you or your child are victimized.

- **Avoid escalating the situation** - Responding with hostility is likely to provoke a bully and escalate the situation. Depending on the circumstances, consider ignoring the issue. Often, bullies thrive on the reaction of their victims. Other options include subtle actions. For example, you may be able to block the messages on social networking sites or stop unwanted emails by changing the email address. If you continue to get messages at the new email address, you may have a stronger case for legal action.
- **Document the activity** - Keep a record of any online activity (emails, web pages, instant messages, etc.), including relevant dates and times. In addition to archiving an electronic version, consider printing a copy.
- **Report cyberbullying to the appropriate authorities** - If you or your child are being harassed or threatened, report the activity. Many schools have instituted bullying programs, so school officials may have established policies for dealing with activity that involves students. If necessary, contact your local law enforcement. Law enforcement agencies have different policies, but your local police department or FBI branch are good starting points. Unfortunately, there is a distinction between free speech and punishable offenses, but the legal implications should be decided by the law enforcement officials and the prosecutors.

Additional information

The following organizations offer additional information about this topic:

- National Crime Prevention Council - http://www.ncpc.org/cyberbullying
- StopBullying.gov - http://www.stopbullying.gov/

Author: Mindi McDowell

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Socializing Securely: Using Social Networking Services

Mindi McDowell and Damon Morda

Social Networking Serves Many Purposes

Social networking is a way for people to connect and share information with each other online. Millions of people worldwide regularly access these types of services from mobile devices, applications, and websites. According to statistics published by some of the most well-known social networking services, there are more than 500 million active users on Facebook[1], 175 million registered users on Twitter[2], more than 100 million users on MySpace[3], and more than 80 million members on LinkedIn[4].

People may use social networking services for different reasons: to network with new contacts, reconnect with former friends, maintain current relationships, build or promote a business or project, participate in discussions about a certain topic, or just have fun meeting and interacting with other users. Some services, such as Facebook and Twitter, have a broad range of users, while others cater to specific interests. For example, LinkedIn has positioned itself as a professional networking site—profiles include resume information, and groups are created to share questions and ideas with peers in similar fields. On the other hand, MySpace is known for its emphasis on music and other entertainment. There are also social networking services that have been designed specifically to reconnect former classmates.

Sharing Information Presents Risks

When you share information online, you need to understand the potential risks, and you need to be wary of what you share and with whom.

Attacks and Unintended Information Disclosure

Attackers may use social networking services to spread malicious code, compromise users' computers, or access personal information about a user's identity, location, contact information,

[1] Facebook Factsheet (http://www.facebook.com/press/info.php?factsheet) (accessed January 3, 2011)

[2] About Twitter (http://twitter.com/about) (accessed January 3, 2011)

[3] MySpace Fact Sheet (http://www.myspace.com/pressroom/fact-sheet/) (accessed January 3, 2011)

[4] LinkedIn: About Us (http://press.linkedin.com/about) (accessed January 3, 2011)

and personal or professional relationships. You may also unintentionally reveal information to unauthorized individuals by performing certain actions. The following are some common threats to social networking services.

- **Viruses** – The popularity of social networking services makes them ideal targets for attackers who want to have the most impact with the least effort. By creating a virus and embedding it in a website or a third-party application, an attacker can potentially infect millions of computers just by relying on users to share the malicious links with their contacts.

- **Tools** – Attackers may use tools that allow them to take control of a user's account. The attacker could then access the user's private data and the data for any contacts that share their information with that user. An attacker with access to an account could also pose as that user and post malicious content.

- **Social engineering attacks** – Attackers may send an email or post a comment that appears to originate from a trusted social networking service or user. The message may contain a malicious URL or a request for personal information. If you follow the instructions, you may disclose sensitive information or compromise the security of your system.

- **Identity theft** – Attackers may be able to gather enough personal information from social networking services to assume your identity or the identity of one of your contacts. Even a few personal details may provide attackers with enough information to guess answers to security or password reminder questions for email, credit card, or bank accounts.

- **Third-party applications** – Some social networking services may allow you to add third-party applications, including games and quizzes, that provide additional functionality. Be careful using these applications—even if an application does not contain malicious code, it might access information in your profile without your knowledge. This information could then be used in a variety of ways, such as tailoring advertisements, performing market research, sending spam email, or accessing your contacts.

Professional and Personal Implications

You may risk professional opportunities, personal relationships, and safety by posting certain types of information on social networking services.

- **Business data** – Posting sensitive information intended only for internal company use on a social networking service can have serious consequences. Disclosing information about customers, intellectual property, human resource issues, mergers and acquisitions, or other company activities could result in liability or bad publicity, or could reveal information that is useful to competitors.

- **Professional reputation** – Inappropriate photos or content on a social networking service may threaten a user's educational and career prospects. Colleges and universities may

conduct online searches about potential students during the application process. Many companies also perform online searches of job candidates during the interview process. Information that suggests that a person might be unreliable, untrustworthy, or unprofessional could threaten the candidate's application. There have also been many instances of people losing their jobs for content posted to these services. Although the legality of some of these terminations is still being debated[5], posting certain comments may affect your credibility and professional reputation.

- **Personal relationships** – Because users can upload comments from any computer or smart phone that has internet access, they may impulsively post a comment that they later regret. According to a survey conducted by Retrevo, "32 percent of people who post on a social networking site regret they shared information so openly."[6] Even if comments and photos are retracted, it may be too late to undo the damage. Once information is online, there is no way to control who sees it, where it is redistributed, or what websites save it into their cache.

- **Personal safety** – You may compromise your personal security and safety by posting certain types of information on social networking services. For example, revealing that you will be away from home, especially if your address is posted in your profile, increases the risk that your home will be burglarized. You may also risk the safety of your children by posting photos and personal details. For example, if malicious individuals are able to collect enough information, such as the child's name, school, activities, or details about the parents, they might be able to lure a child into a dangerous situation.

An important element to remember about social networking services is that users may post information about other people. Without even realizing it, you may put someone else at risk by posting a comment or photo that could compromise that person's privacy or security. Sometimes, posting negative content about someone else is intentional. Social networking services have become channels for conducting cyberbullying[7], a growing problem that can lead to significant psychological trauma.

Proceed with Caution

Social networking services are useful and enjoyable, but it is important to take proactive steps to protect your computer, your personal information, and your company data. By protecting yourself, you also help to protect the people you are connected to on these services.

---

[5] "Company Accused of Firing Over Facebook Post" (http://www.nytimes.com/2010/11/09/business/09facebook.html)

[6] "Report: One in Three Regret Posting Personal Information on Social Networking Sites" (http://www.dailytech.com/Report+One+in+Three+Regret+Posting+Personal+Information+on+Social+Networking+Sites/article18401.htm)

[7] "Dealing with Cyberbullies" (http://www.us-cert.gov/cas/tips/ST06-005.html)

Implement Security Measures

Taking general security precautions will reduce the risk of compromise.

1. Use strong passwords[8], and use a unique password for each service.

2. Keep anti-virus software[9] up to date.

3. Install software updates[10] in a timely manner, particularly updates that affect web browsers.

Follow Good Practices

Social networking services offer unique risks, and you can minimize these risks by adopting good security practices.

1. **Use strong privacy and security settings** – Take advantage of the security options provided by social networking services. When choosing appropriate options, err on the side of privacy to better protect your information. These services may change their options periodically, so regularly evaluate your security and privacy settings, looking for changes and ensuring that your selections are still appropriate. Also periodically review the services' privacy policies to see if there are any changes.

2. **Avoid suspicious third-party applications** – Choose third-party applications wisely. Look for applications developed by vendors you trust, and avoid applications that seem suspicious. Limit the amount of information third-party applications can access.

3. **Treat everything as public** – The best way to protect yourself is to limit the amount of personal information you post to these services. This recommendation applies not only to information in your user profile, but also to any comments or photos you post. It is important that you consider information that you post about yourself and about others, particularly children.

4. **Share only with people you know** – Although many users seek to establish as many contacts on these services as possible, consider sharing personal information only with people you know. If you expand your contacts beyond people you are sure you can trust, check the service's settings to see if you can group your contacts and assign different levels of access based on your comfort level. Attackers may adopt different identities to try to convince users to add them as contacts, so try to confirm that contacts are who they claim to be before giving them access to your information.

Regardless of how restrictive you make your security settings, they may not offer complete privacy. An attacker or application may take advantage of software vulnerabilities, or another user may repost your information. When using social networking services, be responsible and

---

[8] "Choosing and Protecting Passwords" (http://www.us-cert.gov/cas/tips/ST04-002.html)

[9] "Understanding Anti-Virus Software" (http://www.us-cert.gov/cas/tips/ST04-005.html)

[10] "Understanding Patches" (http://www.us-cert.gov/cas/tips/ST04-006.html)

always consider the risks. Operate as if all of the content is public, and only post information you would be comfortable sharing with other people.

Additional Resources

US-CERT Resources:

- "Staying Safe on Social Network Sites" (http://www.us-cert.gov/cas/tips/ST06-003.html)
- "Guidelines for Publishing Information Online" (http://www.us-cert.gov/cas/tips/ST05-013.html)

Other Resources

- "Seven Deadly Sins of Social Networking Security" (http://www.csoonline.com/article/496314/seven-deadly-sins-of-social-networking-security)
- "Social Networking and Security Risks" (http://www.gfi.com/whitepapers/Social_Networking_and_Security_Risks.pdf)
- "Risks and Benefits of More Open Social Networking" (http://www.epa.gov/oei/symposium/2010/gotta.pdf)