Staying Safe Online

Burrendah Primary
Independent Public School

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.

Contents:

Staying Safe on Social Network Sites

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). 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 customised applications that appear to be innocent while infecting your computer 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).

- 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). 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. You can customise your settings to restrict access to only certain people. However, there is a risk that even this private information could be exposed, so don't post anything that you wouldn't want the public to see. Also, be cautious when deciding which applications to enable, and check your settings to see what information the applications will be able to access.

- Use strong passwords - Protect your account with passwords that cannot easily be guessed (see Choosing and Protecting Passwords). 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). 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.

- Use and maintain anti-virus software - Anti-virus software recognizes most known viruses and protects your computer against them, so you may be able to detect and remove the virus before it can do any damage (see Understanding Anti-Virus Software). 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 Government Sites list at end of document).

Avoiding Social Engineering and Phishing Attacks

What is a social engineering attack?

To launch a social engineering attack, an attacker uses human interaction (social skills) to obtain or compromise information about an organization/person or their 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/person'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/family 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 web sites to solicit personal, often financial, information. Attackers 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.

How do you avoid being a victim?

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about personal or other information. If an unknown individual claims to be from a legitimate organisation, try to verify his or her identity directly with the company.
- Do not provide personal information or information about yourself or your organisation, 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 web site's security (see Protecting Your Privacy).
- Pay attention to the URL of a web site. Malicious web sites 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).
- Unknown email authors. If you are unsure whether an email request is legitimate, try to verify it by contacting the company/sender directly. Do not use contact information provided on a web site 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/phishing_archive.html).
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic (see Understanding Anti-Virus Software, and Reducing Spam).

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

If you believe you might have revealed sensitive information about your organisation, report it to the appropriate people within the organisation, 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.

Guidelines for Publishing Information Online

Why is it important to remember that the internet is public?

Because the internet is so accessible and contains a wealth of information, it has become a popular resource for communicating, for researching topics, and for finding information about people. It may seem less intimidating than actually interacting with other people because there is a sense of anonymity. However, you are not really anonymous when you are online, and it is just as easy for people to find information about you as it is for you to find information about them.
Unfortunately, many people have become so familiar and comfortable with the internet that they may adopt practices that make them vulnerable. For example, although people are typically wary of sharing personal information with strangers they meet on the street, they may not hesitate to post that same information online. Once it is online, it can be accessed by a world of strangers, and you have no idea what they might do with that information.

Remember that the internet is a public resource. Avoid putting anything online that you don't want the public to see or that you may want to retract.

What guidelines can you follow when publishing information on the internet?

- View the internet as a novel, not a diary - Make sure you are comfortable with anyone seeing the information you put online. Expect that people you have never met will find your page; even if you are keeping an online journal or blog, write it with the expectation that it is available for public consumption. Some sites may use passwords or other security restrictions to protect the information, but these methods are not usually used for most web sites. If you want the information to be private or restricted to a small, select group of people, the internet is probably not the best forum.

- Be careful what you advertise - In the past, it was difficult to find information about people other than their phone numbers or address. Now, an increasing amount of personal information is available online, especially because people are creating personal web pages with information about themselves. When deciding how much information to reveal, realise that you are broadcasting it to the world. Supplying your email address may increase the amount of spam you receive (see Reducing Spam). Providing details about your hobbies, your job, your family and friends, and your past may give attackers enough information to perform a successful social engineering attack (see Avoiding Social Engineering and Phishing Attacks).

- Realise that you can't take it back - Once you publish something online, it is available to other people and to search engines. You can change or remove information after something has been published, but it is possible that someone has already seen the original version. Even if you try to remove the page(s) from the internet, someone may have saved a copy of the page or used excerpts in another source. Some search engines "cache" copies of web pages so that they open faster; these cached copies may be available after a web page has been deleted or altered. Some web browsers may also maintain a cache of the web pages a user has visited, so the original version may be stored in a temporary file on the user's computer. Think about these implications before publishing information—once something is out there, you can't guarantee that you can completely remove it.

As a general practice, let your common sense guide your decisions about what to post online. Before you publish something on the internet, determine what value it provides and consider the implications of having the information available to the public. Identity theft is an increasing problem, and the more information an attacker can gather about you, the easier it is to pretend to be you. Behave online the way you would behave in your daily life, especially when it involves taking precautions to protect yourself.

Using Instant Messaging and Chat Rooms Safely

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 and a number of different technologies might be supported

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).

- 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.

Choosing and Protecting Passwords

Why do you need a password?

Think about the number of personal identification numbers (PINs), passwords, or passphrases you use every day: getting money from the ATM or using your debit card in a store, logging on to your computer or email, signing in to an online bank account or shopping cart...the list seems to just keep getting longer. Keeping track of all of the number, letter, and word combinations may be frustrating at

times, and maybe you've wondered if all of the fuss is worth it. After all, what attacker cares about your personal email account, right? Or why would someone bother with your practically empty bank account when there are others with much more money? Often, an attack is not specifically about your account but about using the access to your information to launch a larger attack. And while having someone gain access to your personal email might not seem like much more than an inconvenience and threat to your privacy, think of the implications of an attacker gaining access to your bank account number or your medical records.

One of the best ways to protect information or physical property is to ensure that only authorized people have access to it. Verifying that someone is the person they claim to be is the next step, and this authentication process is even more important, and more difficult, in the cyber world. Passwords are the most common means of authentication, but if you don't choose good passwords or keep them confidential, they're almost as ineffective as not having any password at all. Many systems and services have been successfully broken into due to the use of insecure and inadequate passwords, and some viruses and worms have exploited systems by guessing weak passwords.

How do you choose a good password?

Most people use passwords that are based on personal information and are easy to remember. However, that also makes it easier for an attacker to guess or "crack" them. Consider a four-digit PIN number. Is yours a combination of the month, day, or year of your birthday? Or your address or phone number? Think about how easily it is to find this information out about somebody. What about your email password—is it a word that can be found in the dictionary? If so, it may be susceptible to "dictionary" attacks, which attempt to guess passwords based on words in the dictionary.

Although intentionally misspelling a word ("daytt" instead of "date") may offer some protection against dictionary attacks, an even better method is to rely on a series of words and use memory techniques, or mnemonics, to help you remember how to decode it. For example, instead of the password "hoops," use "IITpbb" for "[I] [l]ike [T]o [p]lay [b]asket[b]all." Using both lowercase and capital letters adds another layer of obscurity. Your best defense, though, is to use a combination of numbers, special characters, and both lowercase and capital letters. Change the same example we used above to "II!2pBb." and see how much more complicated it has become just by adding numbers and special characters.

Longer passwords are more secure than shorter ones because there are more characters to guess, so consider using passphrases when you can. For example, "This passwd is 4 my email!" would be a strong password because it has many characters and includes lowercase and capital letters, numbers, and special characters. You may need to try different variations of a passphrase—many applications limit the length of passwords, and some do not accept spaces. Avoid common phrases, famous quotations, and song lyrics.

Don't assume that now that you've developed a strong password you should use it for every system or program you log into. If an attacker does guess it, he would have access to all of your accounts. You should use these techniques to develop unique passwords for each of your accounts.

Here is a review of tactics to use when choosing a password:

- Don't use passwords that are based on personal information that can be easily access or guessed.
- Don't use words that can be found in any dictionary of any language.
- Develop a mnemonic for remembering complex passwords.
- Use both lowercase and capital letters.
- Use a combination of letters, numbers, and special characters.
- Use passphrases when you can.
- Use different passwords on different systems.

How can you protect your password?

Now that you've chosen a password that's difficult to guess, you have to make sure not to leave it someplace for people to find. Writing it down and leaving it in your desk, next to your computer, or, worse, taped to your computer, is just making it easy for someone who has physical access to your computer or office. Don't tell anyone your passwords, and watch for attackers trying to trick you through phone calls or email messages requesting that you reveal your passwords (see Avoiding Social Engineering and Phishing Attacks).

Many programs offer the option of "remembering" your password, but these programs have varying degrees of security protecting that information. Some programs, such as email clients, store the information in clear text in a file on your computer. This means that anyone with access to your computer can discover all of your passwords and can gain access to your information. For this reason, always remember to log out when you are using a public computer (at the library, an internet cafe, or even a shared computer at your office).

Other programs, such as Apple's Keychain and Palm's Secure Desktop, use strong encryption to protect the information. These types of programs may be viable options for managing your passwords if you find you have too many to remember.

There's no guarantee that these techniques will prevent an attacker from learning your password, but they will make it more difficult.

Reducing Spam

What is spam?

Spam is the electronic version of "junk mail." The term spam refers to unsolicited, often unwanted, email messages. Spam does not necessarily contain viruses—valid messages from legitimate sources could fall into this category.

How can you reduce the amount of spam?

There are some steps you can take to significantly reduce the amount of spam you receive:

- Don't give your email address out arbitrarily - Email addresses have become so common that a space for them is often included on any form that asks for your address—even comment cards at restaurants. It seems harmless, so many people write them in the space provided without realising what could happen to that information. For example, companies often enter the addresses into a database so that they can keep track of their customers and the customers' preferences. Sometimes these lists are sold to or shared with other companies, and suddenly you are receiving email that you didn't request.

- Check privacy policies - Before submitting your email address online, look for a privacy policy. Most reputable sites will have a link to their privacy policy from any form where you're asked to submit personal data. You should read this policy before submitting your email address or any other personal information so that you know what the owners of the site plan to do with the information.

- Be aware of options selected by default - When you sign up for some online accounts or services, there may be a section that provides you with the option to receive email about other products and services. Sometimes there are options selected by default, so if you do not deselect them, you could begin to receive email from organisations that use those lists as well.

- Use filters - Many email programs offer filtering capabilities that allow you to block certain addresses or to only allow email from addresses on your contact list. Some ISPs offer spam "tagging" or filtering services, but legitimate messages misclassified as spam might be dropped before reaching your inbox. However, many ISPs that offer filtering services also provide options for tagging suspected spam messages so the end user can more easily identify them. This can be useful in conjunction with filtering capabilities provided by many email programs.

- Don't follow links in spam messages - Some spam relies on generators that try variations of email addresses at certain domains. If you click a link within an email message or reply to a certain address, you are just confirming that your email address is valid. Unwanted messages that offer an "unsubscribe" option are particularly tempting, but this is often just a method for collecting valid addresses that are then sent other spam.

- Disable the automatic downloading of graphics in HTML mail - Many spammers send HTML mail with a linked graphic file that is then used to track who opens the mail message—when your mail client downloads the graphic from their web server, they know you've opened the message. Disabling HTML mail entirely and viewing messages in plain text also prevents this problem.

- Consider opening an additional email account - Many domains offer free email accounts. If you frequently submit your email address (for online shopping, signing up for services, or including it on something like a comment card), you may want to have a secondary email account to protect your primary email account from any spam that could be generated. You should also use a secondary account when posting to online bulletin boards, chat rooms, public mailing lists, or USENET so that you can get rid of when it starts filling up with spam.

- Don't spam other people - Be a responsible and considerate user. Some people consider email forwards a type of spam, so be selective with the messages you redistribute. Don't forward every message to everyone in your address book, and if someone asks that you not forward messages to them, respect their request.

Understanding Anti-Virus Software

What does anti-virus software do?

Anti-virus software can identify and block many viruses before they can infect your computer. Once you install anti-virus software, it is important to keep it up to date. Although details may vary between packages, anti-virus software scans files or your computer's memory for certain patterns that may indicate an infection. The patterns it looks for are based on the signatures, or definitions, of known viruses. Virus authors are continually releasing new and updated viruses, so it is important that you have the latest definitions installed on your computer.

Once you have installed an anti-virus package, you should scan your entire computer periodically.

- Automatic scans - Depending what software you choose, you may be able to configure it to automatically scan specific files or directories and prompt you at set intervals to perform complete scans.

- Manual scans - It is also a good idea to manually scan files you receive from an outside source before opening them. This includes saving and scanning email attachments or web downloads rather than selecting the option to open them directly from the source scanning media, including CDs and DVDs, for viruses before opening any of the files.

What happens if the software finds a virus?

Each package has its own method of response when it locates a virus, and the response may differ according to whether the software locates the virus during an automatic or a manual scan. Sometimes the software will produce a dialog box alerting you that it has found a virus and asking whether you want it to "clean" the file (to remove the virus). In other cases, the software may attempt to remove the virus without asking you first. When you select an anti-virus package, familiarise yourself with its features so you know what to expect.

Which software should you use?

There are many vendors who produce anti-virus software, and deciding which one to choose can be confusing. All anti-virus software performs the same function, so your decision may be driven by recommendations, particular features, availability, or price.
Installing any anti-virus software, regardless of which package you choose, increases your level of protection. Be careful, though, of email messages claiming to include anti-virus software. Some recent viruses arrive as an email supposedly from your ISP's technical support department, containing an attachment that claims to be anti-virus software. However, the attachment itself is in fact a virus, so you could become infected by opening it.

How do you get the current virus information?

This process may differ depending what product you choose, so find out what your anti-virus software requires. Many anti-virus packages include an option to automatically receive updated virus definitions. Because new information is added frequently, it is a good idea to take advantage of this option. Resist believing email chain letters that claim that a well-known anti-virus vendor has recently detected the "worst virus in history" that will destroy your computer's hard drive. These emails are usually hoaxes.

You can confirm virus information through your anti-virus vendor or through resources offered by other anti-virus vendors.

While installing anti-virus software is one of the easiest and most effective ways to protect your computer, they have their limitations. Because they rely on virus signatures, anti-virus software can only detect viruses that have signatures installed on your computer, so it is important to keep these signatures definitions up to date. You will still be susceptible to viruses that circulate before the anti-virus vendors add new signatures, so continue to be cautious when using the internet.

Web sites that can assist in keeping your children safe online:

Cyber [Smart:]
http://www.cybersmart.gov.au/

Cyber Safe Kids
http://www.cybersafekids.com.au/

Budd:e Cyber Security Education - Primary
https://budd-e.staysmartonline.gov.au/primary/main.php

National Cyber Security Alliance
http://www.staysafeonline.org

Complied by I Nicholls
Systems Administrator
Leeming Senior High School
March 2010