What do your long lost childhood best friend, your college roommate, your boss and your significant other all have in common? If you are one of the hundreds of millions of people using social networks, there’s a good chance that you are linked to them through an online relationship. The information you share with your online contacts allows you to keep in touch without much effort. But who else is looking at that information? And how are they going to use it?

Online social networks are websites that allow users to build connections and relationships to other Internet users. Social networks store information remotely, rather than on a user’s personal computer. Social networking can be used to keep in touch with friends, make new contacts and find people with similar interests and ideas.

However, many people besides friends and acquaintances are interested in the information people post on social networks. Identity thieves, scam artists, debt collectors, stalkers, and corporations looking for a market advantage are using social networks to gather information about consumers. Companies that operate social networks are themselves collecting a variety of data about their users, both to personalize the services for the users and to sell to advertisers.

This fact sheet will provide information about the advantages and disadvantages of using social networks, what kind of information may be safe to post and how to protect it, as well as who is able to access different types of information posted to

1. Introduction
2. Types of Social Networks
3. What Information is Public?
   1. Information a User Shares
   2. Information Gathered Through Electronic Tracking
4. Who Can Access Information?
   1. Behavioral Advertising
   2. Third-Party Applications on Social Networks
   3. Government and Law Enforcement Use of Social Networking Sites
   4. Creditors May Use Social Networking Sites
5. Social Networking and Job Searches: Pros and Cons
   1. How Social Networks May Assist Job Seekers
   2. How Social Networks May Hinder Job Seekers
   3. How Social Networks Can Get You Fired
6. Anonymity on Social Networks
7. What Laws Protect a User’s Information Online?
8. Reading a Privacy Policy
9. Fraud on Social Networks
   1. Identity Theft
   2. Malware
   3. Social Engineering
10. Tips to Stay Safe, Private and Secure
    1. Setting Up an Account
    2. General Tips for Using Social Networks
11. Resources
these networks.

2. Types of Social Networks

There are many types of social networks available. This fact sheet examines the privacy and security implications of using a few of them. Most social networks combine elements of more than one of these types of networks, and the focus of a social network may change over time. While this fact sheet does not address every type of social network, many of the security and privacy recommendations are applicable to other types of networks.

- Personal networks. These networks allow users to create detailed online profiles and connect with other users, with an emphasis on social relationships such as friendship. For example, Facebook, Friendster and MySpace are platforms for communicating with contacts. These networks often involve users sharing information with other approved users, such as one’s gender, age, interests, educational background and employment, as well as files and links to music, photos and videos. These platforms may also share selected information with individuals and applications that are not authorized contacts.

- Status update networks. These types of social networks are designed to allow users to post short status updates in order to communicate with other users quickly. For example, Twitter focuses its services on providing instantaneous, short updates. These networks are designed to broadcast information quickly and publicly, though there may be privacy settings to restrict access to status updates.

- Location networks. With the advent of GPS-enabled cellular phones, location networks are growing in popularity. These networks are designed to broadcast one’s real-time location, either as public information or as an update viewable to authorized contacts. Many of these networks are built to interact with other social networks, so that an update made to a location network could (with proper authorization) post to one’s other social networks.

- Content-sharing networks. These networks are designed as platforms for sharing content, such as music, photographs and videos. When these websites introduce the ability to create personal profiles, establish contacts and interact with other users through comments, they become social networks as well as content hubs.

- Shared-interest networks. Some social networks are built around a common interest or geared to a specific group of people. These networks incorporate features from other types of social networks but are slanted toward a subset of individuals, such as those with similar hobbies, educational backgrounds, political affiliations, ethnic backgrounds, religious views, sexual orientations or other defining interests.

3. What Information is Public?

There are two kinds of information that can be gathered about a user from a social network: information that is shared and information gathered through electronic tracking.

Information a User Shares

Information a user shares may include:

- Photos and other media
- Age and gender
- Biographical information (education, employment history, hometown, etc.)
- Status updates (also known as posts)
- Contacts
- Interests
- Geographical location

This information becomes public in a variety of ways:

- A user may choose to post information as “public” (without restricting access via available privacy settings).
- Certain information may be publicly visible by default. In some situations, a user may be able to change the privacy settings to make the information “private” -- so that only approved users can view it. Other information must remain public; the user does not have an option to restrict access to it.
- A social network can change its privacy policy at any time without a user’s permission. (See How to Read a Privacy Policy [2]) Content that was posted with restrictive privacy settings may become visible when a privacy policy is altered.
• Approved contacts may copy and repost information – including photos – without a user’s permission, potentially bypassing privacy settings.
• Third-party applications that have been granted access may be able to view information that a user or a user’s contacts post privately.

Social networks themselves do not necessarily guarantee the security of the information that has been uploaded to a profile, even when those posts are set to be private. This was demonstrated in one May 2010 incident during which unauthorized users were able to see the private chat logs of their contacts on Facebook. While this and other similar bugs are usually quickly fixed, there is great potential for taking advantage of leaked information. (See New York Times’ Facebook Glitch Brings New Privacy Worries [3])

Information Gathered Through Electronic Tracking

Information may also be gathered from a user’s actions online using “cookies” (short strings of text stored on one’s hard drive). Some of the purposes of cookies may include:

• Tracking which websites a user has viewed.
• Storing information associated with specific websites (such as items in a shopping cart).
• Tracking movement from one website to another.
• Building a profile around a user.

In fact, a 2009 study conducted by AT&T Labs and Worcester Polytechnic Institute found that the unique identifying code assigned to users by social networks can be matched with behavior tracked by cookies. This means that advertisers and others are able to use information gleaned from social networks to build a profile of a user’s life, including linking browsing habits to one’s true identity. Read Krishnamurth and Will’s 2009 study On the Leakage of Personally Identifiable Information Via Online Social Networks [4]. Information leakage also occurs in mobile online social networks, according to Privacy Leakage in Mobile Online Networks [5], another study by Krishnamurthy and Wills.

To learn more about cookies and how to browse the Internet safely and privately, see PRC Fact Sheet 18: Privacy and the Internet [6]. To find out if or how a social network uses cookies, see the social network’s privacy policy. (See How to Read a Privacy Policy [7])

4. Who Can Access Information?

When posting information to a social network, a user probably expects authorized contacts to be able to view it. But who else can see it, and what exactly is visible?

Entities that collect personal information for legal purposes include:

• Advertisers interested in personal information so they can better target their ads to those most likely to be interested in the product
• Third-party software developers who incorporate information to personalize applications, such as an online games that interact with the social network

Entities that collect personal information for illegal purposes include:

• Identity thieves who obtain personal information either based on information a user posts or that others post about the user.
• Other online criminals, such as people planning to scam or harass individuals, or infect computers with malware (malicious software placed on a computer without the knowledge of the owner).

Behavioral Advertising

Social networks that provide their services without user fees make a profit by selling advertising. This is often done through behavioral advertising, also known as targeting.

Behavioral advertising is the term used to describe the practice of tailoring advertisements to an individual’s personal interests. This practice is appealing to marketers because targeted advertisements are more likely to result in a purchase by a viewer than comparable non-targeted advertisements. They are valuable to social networks as they can be sold at a higher price than regular ads. (See The Value of Behavioral Targeting [8] by Howard Beales, sponsored by the Network Advertising Initiative)
Social networks collect a lot of information about potential customers, which advertisers are very interested in using. In some ways, this may be useful to the user because the advertisements he or she sees may appear more relevant.

There are several concerns regarding behavioral advertising:

- Consumers may not be aware that data is associated with their profiles.
- Consumers may not be able to view the data associated with their profiles and have inaccuracies corrected.
- There are no maximum retention periods on data and no security requirements for the retention of data, leaving it susceptible to hackers and security risks.
- Information about minors may be collected and used for behavioral advertising.

Read more about behavioral advertising in PRC’s Fact Sheet 18 Privacy and the Internet - Behavioral Marketing [9].

Third-Party Applications on Social Networks

Within the context of social networking, “third-party applications” are programs that interact with a social network without actually being part of that social network. These applications take many forms but some typical and popular forms include:

- Games to play with contacts
- Online polls or quizzes
- Software that allows users to post to a social media profile via a cellular phone or web application

Some social networks allow program developers to access their platforms in order to create these applications. This makes the social network more attractive to users by facilitating the development of new and creative methods of interacting with contacts and the network.

To make these applications useful, social networks may allow developers automatic access to public information of users. In addition to public information, third-party applications may access some private information. A user may grant a third-party application access to his or her profile without realizing the extent of the permissions being granted. Users may also mistakenly assume that third-party applications are held to the same standards as the primary social network. There are also “rogue” applications which do not follow the policies and terms that govern applications. (See Consumer Reports’ Apps that bite [10])

Some facts to keep in mind when considering using third-party applications:

- They may not be covered by the social network’s privacy policy.
- They may not be guaranteed to be secure.
- Most social networks do not take responsibility for the third-party applications that interact with their sites.
- They may gain access to more information than is necessary to perform their functions.
- Sometimes applications are designed only to gather information about users
- They may contain malware designed to attack the user’s computer.
- Third-party developers may report users’ actions back to the social networking platform.
- A social network may have agreements with certain websites and applications that allow them access to public information of all users of the social network.

Third-party applications typically can access information that:

- Is considered public without explicit consent from the user.
- Is considered private when a user grants the application permission.

In some instances, once they have received permission from a primary user, the third-party applications may also gain access to the personal information of users’ contacts without those contacts granting explicit permission.

As a general rule, use caution when using third-party applications. Remember that it is difficult to control what information they are gathering, how they might use it, and who they will share it with.

Government and Law Enforcement Uses of Social Networking Sites

Freedom of Information Act (FOIA) requests filed by Electronic Frontier Foundation [11] (EFF) with assistance from University of California-Berkeley Samuelson Clinic [12] have shed light on how government agencies use social networking sites for investigations, data collection and surveillance.
While still incomplete, the documents that have been published indicate:

- Government agencies, including the U.S. Justice Department and the Internal Revenue Service (IRC), have developed training materials instructing employees on how to utilize public profile information on social networking sites during investigations.
- Facebook has been noted as having a reputation for being “cooperative with emergency requests” (See https://www.eff.org/deeplinks/2010/03/eff-posts-documents-detailing-law-enforcement[13]).
- IRS manuals specifically prohibit employees from using “fake identities” in order to “trick” users “into accepting a [government] official as a friend.” (EFF Posts Documents Detailing Law Enforcement Collection of Data From Social Media Sites[13].) However, there is no reason to believe law enforcement officers practice similar restraint about creating false profiles.

Each social network has adopted its own procedures for dealing with requests from law enforcement agencies. The degree to which these sites cooperate, or don’t cooperate, with law enforcement may not be fully explained in the privacy policy. Currently, the primary law protecting information privacy on the Internet, the Electronic Communications Privacy Act, allows government officials to access information on social networks with a subpoena. Read more about What Laws Protect a User’s Information Online[14].

View “Obtaining and Using Evidence from Social Networking Sites[15],” a Justice Department presentation obtained by EFF through FOIA request.

Additionally, information on social networking sites has been used as evidence during criminal and civil trials. This includes divorce trials, child custody battles, insurance lawsuits, criminal trials and cases brought by university police against students for inappropriate behavior or underage drinking, to name a few. Be aware that information entered as evidence in a court case could potentially become part of a public record. Read more about public records in PRC Fact Sheet 11: From Cradle to Grave: Government Records and Your Privacy[16].

The use of social networking sites by law enforcement and government agencies, coupled with the fact that information on social networking sites can be used as evidence in trials, reinforces the importance of using restraint in posting information to your profile.

Creditors May Use Social Networking Sites

Some creditors are beginning to data mine social networking sites, including Facebook and LinkedIn, in order to supplement the information gathered from traditional credit reports. By supplementing credit reports with data from social networks, creditors believe that they are obtaining a more complete picture of a potential borrower’s risk profile. Creditors claim that by including social networking data as part of credit underwriting, they can offer loans to consumers who might not qualify under traditional underwriting methods.

The use of social networking data by creditors in their underwriting decisions is largely unregulated. Consumers generally do not have any rights to dispute or correct information derived from social networks, since the information is not reported by these networks to third parties.

5. Social Networks and Job Searches: Pros and Cons

Jobseekers have increasingly turned to social networks to market themselves to potential employers, network with other professionals and search out job opportunities. However, an unprofessional social networking profile may also make a job applicant seem unsuitable by revealing too much personal or unflattering information to a potential employer. This section reviews the pros and cons of social networking for jobseekers.

This information can be applied to any situation where reputation matters, such as:

- Renting an apartment
- Beginning to date someone
- Starting or maintaining a professional relationship, for example as an independent contractor or in a managerial position
- Engaging in volunteer or electoral positions
- Applying for colleges or scholarships
- Being considered in a jury selection process

How Social Networks May Assist Jobseekers
There are a variety of ways social networks can help with the job hunt. If a job applicant initially contacts a potential employer via the Internet, a profile on a social network can help confirm that there is a real person behind an email address.

Social networks also increase networking opportunities. A job applicant can alert others to an interest in finding a job, as well as details on the desired position, by posting about this interest on a social network. Professional networks, such as LinkedIn, are designed to provide information about education, employment history and accomplishments to a large number of people. There are also professional or interest groups on a variety of networks that can increase visibility and contacts.

Potential employers can use social networks to confirm that an applicant has represented his or her interests, education level and background truthfully. They can also learn about other interests an applicant may have. Individuals who create positive, interesting and informative social networking profiles may seem like stronger candidates for certain jobs. This is especially true of, but not limited to, jobs involving outreach and communication.

How Social Networks May Hinder Jobseekers

Social networks may inadvertently reveal information jobseekers might not choose to reveal about themselves. Potential employers often use whatever information they can gather about an applicant in making a hiring decision. It is important to know what information can be seen by non-contacts and to consider what kind of conclusions might be drawn from it.

Unflattering pictures or posts could seriously affect the likelihood of getting hired. Even if one posts this information using restrictive privacy settings, there are many ways in which it may become available.

As a general rule, before posting something on a social networking profile, imagine it displayed on a billboard on the side of a highway. Would you be uncomfortable to see it there? If so, you may not want to post it at all.

While it is illegal and very hard to prove, potential employers might discriminate based on information available from profile pictures and other easily available information on one’s social networking profile. Be aware of revealing even basic information such as:

- Age
- Gender
- Race
- Disability
- Sexual orientation
- Political affiliations
- Other groups and contacts

Also, negative posts about a current job could harm an applicant’s chances of getting an offer.

The Fair Credit Reporting Act (FCRA) is a law that not only regulates credit reports but also sets national standards for employment screening and background checks. In effect, it sets limits on what information employers can get from background checks and how they can use that information (see PRC Fact Sheet 16: Employment Background Checks: A Jobseeker's Guide [17]). However, the FCRA only applies to employers using third-party screening companies. Information that an employer gathers independently, including from informal Internet searches, is not covered by the FCRA.

How Social Media Networks Can Get You Fired

Employers are increasingly monitoring what employees post on social networking sites. In fact, many companies have social media policies that limit what you can and cannot post on social networking sites about your employer.

Many companies have social media policies that limit what you can and cannot post on social networking sites about your employer. A website called Compliance Building has a database of social media policies [18] for hundreds of companies. You should ask your supervisor or human resources department what the policy is for your company.

Some states have laws that prohibit employers from disciplining an employee based on off-duty activity on social networking sites, unless the activity can be shown to damage the company in some way. In general, posts that are work-related have the potential to cause the company damage. Anti-discrimination laws prohibit employers from disciplining employees based on age, race, color, religion, national origin or gender. If you feel that you have been discriminated against, contact a lawyer. You can find
a lawyer who specializes in employment law via the National Employment Lawyers Association [19]. For more information on the laws surrounding social media in the workplace, see The Portland Press Herald: Your Business: Make Your Social Policy Clear [20]

There is no federal law that we are aware of that an employer is breaking by monitoring employees on social networking sites. In fact, employers can even hire third-party companies to monitor online employee activity for them.

The National Labor Relations Board (NLRB) has issued a number of rulings involving questions about employer social media policies. The NLRB has indicated that these cases are extremely fact-specific. It has provided the following general guidance:

- Employer policies should not be so sweeping that they prohibit the kinds of activity protected by federal labor law, such as the discussion of wages or working conditions among employees.
- An employee’s comments on social media are generally not protected if they are mere gripes not made in relation to group activity among employees.


6. Anonymity on Social Networks

Many users of social networks choose to mask their real identities. This may be done via anonymity (providing no name at all) or pseudonymity (providing a false name).

Some people who may prefer an anonymous or pseudonymous persona include, but are not limited to:

- Individuals with medical conditions who want to discuss symptoms and treatment without creating a public record of their condition
- Bloggers and activists engaging in political discourse, especially on controversial issues
- Teachers and childcare workers
- Medical professionals, including mental health professionals
- Law enforcement agents, prosecutors, parole and probation officers, judges, and other court employees
- Victims of stalking, sexual assault, and domestic violence
- Children and youth
- Jobseekers

In fact, anonymity is a useful tool for anyone who prefers to keep a strict separation between an online persona and an off-line identity. It can also be abused by individuals trying to shield their identities while engaging in illegal activities.

Typically, users who prefer to engage in social networks without divulging their true identity will create profiles using a false name as well as a false email address. If you are considering a pseudonymous profile, refer to the terms of service for the social networking site. Providing false or incomplete information violates the terms of service of some social networking sites. Users should consider using software that masks IP addresses, such as TOR [23]. Users should also remember to delete all cookies after visiting a social networking site. See PRC’s discussion of cookies in PRC Fact Sheet 18: Privacy and the Internet -- Cookies [24].

Bear in mind that it is difficult to truly separate online and off-line identities. It is possible to divulge identifying information through status updates, group memberships, photographs, friend networks and other indicators. In fact, numerous studies have shown that anonymized data can often still be linked to specific individuals.

Read more about anonymization issues:

- Arvind Narayanan and Vitaly Shmatikov’s paper, De-anonymizing Social Networks [25]
- The Electronic Frontier Foundation’s Anonymity page [26]

7. What Laws Protect a User’s Information Online?

There are currently few laws that can be interpreted as protecting information given to social networks. Most privacy laws in the United States protect specific types of information, such as medical or financial records. Some laws that do protect the privacy of information do not currently extend to casual information searches on the Internet (see FCRA, previous section) or to information revealed by the user, such as a quiz about health that provides information to drug companies. (See New York Times' Online
The Electronic Communications Privacy Act was passed in 1986, before the Internet became an essential means of communication. If information is stored on a server (such as the information on social networks), this law makes it easy for law enforcement or the government to access it via a subpoena. A variety of industry and advocacy organizations are lobbying to update this law. The proposed update would strengthen the requirements needed for governmental access to the data stored on a server by necessitating a search warrant. Information about location is also not strongly protected under ECPA. (See Digital Due Process [28])

The Children’s Online Privacy Protection Act (COPPA) requires that websites directed at children under 13 must limit their data collection and usage in certain ways. There are also limitations on the information that can be sent to advertisers (see PRC Fact Sheet 21: Children’s Online Privacy: A Resource Guide for Parents [29]). Some social networks therefore do not allow users under 13.

The California Online Privacy Act [30] (California Business and Professions Code sections 22575-22579) requires any website that collects personally identifiable information on California consumers to conspicuously post an online privacy policy. This privacy policy must describe what categories of information are collected, what categories of third-parties may be authorized to view this information, how the website owner will notify consumers about changes to the policy and the effective date of the policy. Websites without a privacy policy have 30 days within being notified of the law to comply. See a sample letter [31] to a website about the need to post a privacy policy.

Several states have enacted legislation protecting employees or job applicants from employers that require them to provide a user name or password for a social media account. For a current list of state laws and pending legislation see NCSL’s List [32]. Read the Littler Workplace Policy Institute comprehensive discussion of the history and background of social media password protection legislation and the differences between state laws at http://www.littler.com/files/press/pdf/WPI-Social-Media-Password-Protection-Privacy-May-2013.pdf [33].

8. Reading a Privacy Policy

Many people skip over the privacy policy when joining a social network. However, users can glean a lot of useful information by reviewing a privacy policy before signing up for service. A social network’s privacy policy will explain how the social network will collect and use information about people who visit the site.

Some of the information users provide to a social network is readily apparent -- such as providing a birth date in order to create a new account.

Other times, the social network may be collecting information on users “invisibly” – by tracking where users go within the social network, what links they click on and even which websites they visit after leaving the social networking site. “Invisible” tracking is often accomplished through cookies. (Read more about cookies on PRC Fact Sheet 18: Privacy and the Internet -- Cookies [6])

When reviewing a privacy policy, remember:

- Privacy policies can change – sometimes dramatically-- after a user creates an account.
- Terms of service may have information just as important as the privacy policy, so always review those as well.
- The privacy policy only covers the social network. It does not, for example, cover third-party applications that interact with the website.

Unfortunately, most privacy policies are long and difficult to understand. Here are some points to consider when reading a privacy policy:

- Start at the end. The most important portions of a privacy policy are often at the very end. For example, the end of the document typical provides contact information for a privacy contact at the company as well as the most important facts about how personally identifiable information is used. So, when pressed for time, look to the end of the document.
- Note the location and language of the privacy policy. Is it hidden away on a hard-to-find webpage or can it be found easily? Does the language seem excessively vague or incomprehensible?
- Canceling your account. If you decide to leave the social network, can you delete the account and remove all of your information? Can all data be removed entirely or will some information be maintained by the social network? Be aware
that some social networks may make it difficult or confusing to cancel an account and instead direct dissatisfied users to “deactivate” accounts.

- How long is personal information stored? Note that some information may be made ‘anonymous’ after a certain period of time, some may be deleted entirely after a certain period of time, and some may be maintained in perpetuity.

- What happens when a user dies? Does the privacy policy discuss what happens to personal information after a user dies? Will it remain online or be removed?

- Who owns the data that a user posts? Does a user lose rights to information that he or she posts? Can it be used by marketers without the user’s explicit consent? For example, can a user’s name and photos be used for advertisements?

- How can a user complain? Look for a physical address, email address, website address or phone number where users can voice concerns. Some online social networks utilize independent companies to review their privacy practices. In such cases, users who are dissatisfied by a company’s compliance to the posted privacy policy can submit complaints to the certifying company.

- How will a social network notify users about changes to the privacy policy? Will changes be posted to the homepage or will it only be posted in the privacy policy itself? Can users connect with a public profile on the social network that will inform them of changes to the privacy policy, or is there a way to receive an email if changes are made?

- Does the social network participate in seal programs? Social networks that participate in third-party seal or certification programs show some level of awareness of privacy concerns. This also gives users another place to voice concerns if any should arise. Some well-known companies include the Better Business Bureau, Verisign and Truste. However, never assume that a third-party certification means the social network will always respect users’ privacy and security.

Learn more about reading a privacy policy by visiting:

- California Office of Privacy Protection’s [How To Read a Privacy Policy](#) [7]
- Yahoo’s [Reading Privacy Policies](#) [34]

Also, try seeing what others have said about the policy. A simple Internet search could turn up thoughtful analysis of the policy, especially if the social network has been in the news.

9. Fraud on Social Networks

Criminals may use social networks to connect with potential victims. This section discusses some of the typical scams and devices used to defraud consumers on social networks. Fraud may involve more than one of the techniques described below. Some types of fraud may not be described here.

Identity Theft

Identity thieves use an individual’s personal information to pretend to be them – often for financial gain. The information users post about themselves on social networks may make it possible for an identity thief to gather enough information to steal an identity. In 2009, researchers at Carnegie University Mellon published a study showing that it is possible to predict most and sometimes all of an individual’s 9-digit Social Security number using information gleaned from social networks and online databases.

Information often targeted by identity thieves includes:

- Passwords
- Bank account information
- Credit card numbers
- Information stored on a user’s computer such as contacts
- Access to the user’s computer without his or her consent (for example, through malware)
- Social Security numbers. Remember that the key to identity theft is the Social Security number. Never provide a Social Security number through a social networking service.

Some fraud techniques to watch out for include:
Illegitimate third-party applications. These rogue applications may appear similar to other third-party applications but are designed specifically to gather information. This information may be sold to marketers but could also be useful in committing identity theft. These applications may appear as games, quizzes or questionnaires in the format of “What Kind of Famous Person Are You?” (See ABC's Online Games Can Lead to Identity Theft [36])

False connection requests. Scammers may create fake accounts on social networks and then solicit others to connect with them. These fake accounts may use the names of real people, including acquaintances, or may be entirely imaginary. Once the connection request is accepted, a scammer may be able to see restricted and private information on a user’s profile.

Learn more about protecting yourself from identity theft in general by reading PRC Fact Sheet 17: Coping with Identity Theft: Reducing the Risk of Fraud [37]. If you believe you may be the victim of identity theft, read PRC Fact Sheet 17a: Identity Theft: What to Do if It Happens to You [38].

Malware

Malware (malicious software) is a term that describes a wide range of programs that install on a user’s computer often through the use of trickery. Malware can spread quickly on a social network, infecting the computer of a user and then spreading to his or her contacts. This is because the malware may appear to come from a trusted contact, and thus users are more likely to click on links and/or download malicious programs.

Some common techniques used in spreading malware include:

- Shortened URLs, particularly on status update networks or newsfeeds. These may lead the user to download a virus or visit a website that will attempt to load malware on a user’s computer.
- Messages that appear to be from trusted contacts that encourage a user to click on a link, view a video or download a file.
- An email appearing to be from the social network itself, asking for information or requesting a user click on a link.
- Third-party applications that infect computers with malicious software and spread it to contacts.
- Fake security alerts – applications that pose as virus protection software and inform the user that his or her security software is out-of-date or a threat has been detected.

Social Engineering

There are a variety of social engineering scamming techniques which trick users into entering sensitive information. This section describes a few of the well-known techniques.

- Phishing attacks are when emails, instant messages or other messages claiming to be from a trusted source ask for information. For example, an email may appear to be from a bank and could direct a user to enter a password at a fake login page, or tell a user to call a phone number or risk having their account closed. For tips on how to spot and avoid phishing attacks, see OnGuard Online’s Phishing page [39]. Some Internet browsers have taken steps to help identify fake websites. (See GetSafe Online’s Avoid Criminal Websites [40] for these and other tips.)

- Spear phishing is a type of phishing attack that appears to be from a colleague, employer or friend and includes a link or something to download. (This is often the result of account hijacking.) These links or downloads can be malicious, such as viruses or fake websites that solicit personal information.

- Misleading solicitations. A social network might use social engineering to make people feel obligated to join. This often occurs when one person joins and (often inadvertently) provides the social network with access to his or her contact list. The social network then sends out emails to all of his or her contacts, often implying they are from the individual who joined. For example, it has been reported that Tagged.com solicits contacts of users with emails claiming the recipient has been “tagged.” These emails state: “Is <user name> your friend? Please respond or <user name> may think you said no :-( ” or “<user name> sent you photos on Tagged.” The recipient may believe this is a personal invitation from the user and feel obligated to join the network, giving out his or her information and perhaps perpetuating the solicitations.

- Hijacked accounts. A legitimate account may be taken over by an identity thief or malware for the purpose of fraud such as posting spam, sending out malware, stealing the private data of contacts or even soliciting contacts to send money. One typical scenario is when a hijacked account sends out messages stating that the account owner is overseas and in desperate straits. Contacts are urged to immediately wire money. A user may not realize his or her account has been hijacked for quite some time. An attack could also be in the form of a chat conversation.
10. Tips to Stay Safe, Private and Secure

There are many ways that information on social networks can be used for purposes other than what the user intended. Below are some practical tips to help users minimize the privacy risks when using social networks. Be aware that these tips are not 100% effective. Any time you choose to engage with social networking sites, you are taking certain risks. Common sense, caution and skepticism are some of the strongest tools you have to protect yourself.

Registering an Account

1. Use a strong password different from the passwords you use to access other sites. See PRC’s 10 Rules for Creating a Hacker-Resistant Password [41]

2. If you are asked to provide security questions, use information that others would not know about you.

3. Never provide a work-associated email to a social network, especially when signing up. Consider creating a new email address strictly to connect with your social networking profile(s).

4. Consider not using your real name, especially your last name. Be aware that this may violate the terms of service of some social networks.

5. Be sure to review the privacy policy and terms of service before signing up for an account.

6. Be sure to keep strong antivirus and spyware protection on your computer. See Fact Sheet 36: Securing Your Computer to Maintain Your Privacy [42]

7. Provide only information that is necessary or that you feel comfortable providing. When in doubt, err on the side of providing less information. Remember, you can always provide more information to a social network, but you can’t always remove information once it’s been posted.

During the registration process, social networks often solicit a new user to provide an email password so the social network can access the user’s email address book. The social network promises to connect the new user with others they may already know on the network. To be safe, don’t provide this information at all. There are some social networks that capture all of a user’s email contacts and then solicit them – often repeatedly – to join. These messages may even appear to be from the original user. If you consider providing an email address and account password to a social network, read all agreements very carefully before clicking on them.

General Tips for Using Social Networks

1. Become familiar with the privacy settings available on any social network you use. On Facebook, make sure that your default privacy setting is "Friends Only". Alternatively, use the "Custom" setting and configure the setting to achieve maximum privacy.

2. Don’t share your birthday, age, or place of birth. This information could be useful to identity thieves and to data mining companies. A research study by Carnegie Mellon University [43] found that Social Security numbers can be predicted based on publicly-available information, including your birthday, age and place of birth. The Social Security Administration began assigning randomized number series [44] on June 25, 2011. Unfortunately, the more predictable Social Security numbers will remain in effect for individuals born before June 25, 2011. If you do consider posting your birthday, age or place of birth, restrict who has access to this information using the site’s privacy settings. Also, some social networking sites allow you to show your birth month and day, but hide the year.

3. Stay aware of changes to a social network’s terms of service and privacy policy. You may be able to keep track of this by connecting to an official site profile, for example Facebook’s Site Governance [45]. Consider subscribing to an RSS feed for Tosback [46], a project of the Electronic Frontier Foundation [11] to track changes in website policies (covers some but not all social networks).

4. Be careful when you click on shortened links. Consider using a URL expander (as an application added to your browser or a website you visit) to examine short URLs before clicking on them. Example of URL expanders include LongURL, Clybs URL Expander and Long URL Please (Privacy Rights Clearinghouse does not endorse one URL expander over another.)
5. Be very cautious of pop-up windows, especially any that state your security software is out of date or that security threats
and/or viruses have been detected on your computer. Use your task manager to navigate away from these without clicking
on them, then run your spyware and virus protection software.

6. Delete cookies every time you leave a social networking site. See PRC Fact Sheet 18: Privacy and the Internet [6]

7. Remember that whatever goes on a network might eventually be seen by people not in the intended audience. Think about
whether you would want a stranger, your mother or a potential boss to see certain information or pictures. Unless they are
glowing, don’t post opinions about your company, clients, products and services. Be especially cautious about photos of
you on social networks, even if someone else placed them there. Don’t be afraid to untag photos of yourself and ask to
have content removed.

8. Don’t publicize vacation plans, especially the dates you’ll be traveling. Burglars can use this information to rob your house
while you are out of town.

9. If you use a location-aware social network, don’t make public where your home is because people will know when you are
not there. (See Please Rob Me - Raising Awareness about Oversharing [47]) In fact, you should be careful when posting
any sort of location or using geotagging features because criminals may use it to secretly track your location. For the same
reason, be careful not to share your daily routine. Posting about walking to work, where you go on your lunch break, or
when you head home is risky because it may allow a criminal to track you.

10. Be aware that your full birth date, especially the year, may be useful to identity thieves. Don’t post it, or at a minimum
restrict who has access to it.

11. Don’t post your address, phone number or email address on a social network. Remember scam artists as well as
marketing companies may be looking for this kind of information. If you do choose to post any portion of this, use privacy
settings to restrict it to approved contacts.

12. Use caution when using third-party applications. For the highest level of safety and privacy, avoid them completely. If you
consider using one, review the privacy policy and terms of service for the application.

13. If you receive a request to connect with someone and recognize the name, verify the account holder’s identity before
accepting the request. Consider calling the individual, sending an email to his or her personal account or even asking a
question only your contact would be able to answer.

14. If you receive a connection request from a stranger, the safest thing to do is to reject the request. If you decide to accept the
request, use privacy settings to limit what information is viewable to the stranger and be cautious of posting personal
information to your account, such as your current location as well as personally identifiable information.

15. Be wary of requests for money, even if they are from contacts you know and trust. If a contact’s account is compromised, a
scam artist may use his or her name and account to attempt to defraud others through bogus money requests.

16. Take additional precautions if you are the victim of stalking, harassment or domestic violence. See PRC Fact Sheet 14:
Are You Being Stalked? [48]

17. In the event that your social networking account is compromised, report it to the site immediately and alert your contacts.
You will need to change passwords, but proceed with caution because your computer security may have been
compromised. Malware, including key-logging software, may have been installed on your computer. If you use online
banking, do not log on from the computer that may have been compromised until you have ensured your computer security
is intact.

18. Prune your "friends" list on a regular basis. It’s easy to forget who you’ve friended over time, and therefore who you are
sharing information with.

19. If you are using a social networking site that offers video chatting, pay attention to the light on your computer that indicates
whether or not your webcam is in use. This will help you avoid being "caught on camera" by accident.

20. Be sure to log off from social networking sites when you no longer need to be connected. This may reduce the amount of
tracking of your web surfing and will help prevent strangers from infiltrating your account.

21. Remember that nothing that you post online is temporary. Anything you post can be cached, stored, or copied and can follow you forever.

22. Check your privacy settings often. Privacy policies and default settings may change, particularly on Facebook.

11. Resources

Nonprofit Resources

- Electronic Frontier Foundation’s “Top 12 Ways to Protect Your Online Privacy,” [www.eff.org/wp/effs-top-12-ways-protect-your-online-privacy](http://www.eff.org/wp/effs-top-12-ways-protect-your-online-privacy) [49]
- Facebook & Your Privacy (Consumer Reports, June 2012), [http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm](http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm) [52]

Government Resources

- California Department of Justice’s Privacy Enforcement and Protection Unit’s “How to Read a Privacy Policy,” [http://www.oag.ca.gov/privacy/facts/online-privacy/privacy-policy](http://www.oag.ca.gov/privacy/facts/online-privacy/privacy-policy) [2]
- California Attorney General, Privacy on the Go: Recommendations for the Mobile Ecosystem [53]
- OnGuardOnline, [www.onguardonline.gov](http://www.onguardonline.gov) [54]

Additional Resources


Privacy Rights Clearinghouse Resources

- PRC Fact Sheet 16: Employment Background Checks: A Jobseeker’s Guide [www.privacyrights.org/fs/fs16-bck.htm](http://www.privacyrights.org/fs/fs16-bck.htm) [17]
- PRC Fact Sheet 18: Privacy and the Internet: Traveling in Cyberspace Safely [www.privacyrights.org/fs/fs18-cyb.htm](http://www.privacyrights.org/fs/fs18-cyb.htm) [59]
- PRC Fact Sheet 21a: Children’s Safety on the Internet [https://www.privacyrights.org/content/childrens-safety-internet](https://www.privacyrights.org/content/childrens-safety-internet) [60] [61]
- PRC Fact Sheet 36: Securing Your Computer to Maintain Your Privacy [https://www.privacyrights.org/fs/fs36-securing-computer-privacy.htm](https://www.privacyrights.org/fs/fs36-securing-computer-privacy.htm) [42]
- Davis, Donald Carrington. "MySpace Isn’t Your Space: Expanding the Fair Credit Reporting Act to Ensure Accountability and Fairness in Employer Searches of Online Social Networking Services" [www.privacyrights.org/ar/mySpace-background-checks.htm](http://www.privacyrights.org/ar/mySpace-background-checks.htm) [62]

Special thanks to intern Sarah Pipes, candidate for a degree of Master of Science of Information


Links