

FOUND ONLINE

As a professional security and investigative group, we assist those in the high profile market with a good deal of day-to-day exposure in protecting their privacy by removing their personal information, such as addresses, family members, and associates.

A good deal of the information found in online databases is generated by us and our eagerness to keep our lives simple. Try the following offline example to see just how much information is generated and spread by you during the average day.

Offline Exercise

For three days, keep a journal of all the times you share your name, address, phone number, credit card number, how often you drive a car through an a tollbooth with E-ZPass, use a grocery store coupon card, pay your bills, or answer unsolicited email. In addition, record how many credit card offers come in the mail, as well as how many telemarketing phone calls you receive. After only three days, you'll begin to notice that you hand out your information everywhere. It is on your credit card statements, loans, liens, and deeds to your homes, in addition to automobiles and other large assets. If people you do not know call your home with offers and your shredder needs cleaning out once a week, it's time to consider minimization of information.

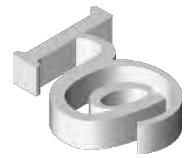
After this exercise, you might think that complete removal of yourself from the online world would seem insurmountable. Paying charges with a credit card, driving quickly through tollbooths, owning a home with a telephone, and other day-to-day “stuff” are convenient and practical.

Oddly enough, this information has always been available. It just required investigative experience and/or a serious commitment to locate these types of details through county court houses, administrative offices, and other public record venues. Since the World Wide Web, though, at least 100 U.S.-based public record companies have popped up for anyone to use. These companies will locate individuals and share intimate details about where they live, who lives with them, their age, and so on, for anyone who searches on them.

Where Do Companies Get My Name?

Organizations use information from a variety of sources for a variety of reasons. You are familiar with some of them—such as businesses wanting to send you an offer, companies wanting to better understand their marketplace or to develop new products and improve customer service. In other cases, companies use information to protect you and themselves from risks related to identity fraud.

Most companies rent or buy lists of individuals who they believe are likely to be interested in their products or services. They will use these lists to market to you either offline or online. These lists come from a variety of sources, including public records, telephone directories, and from companies who



exchange or rent their customer file for marketing purposes to other organizations who have a legitimate need for the information. The rental or exchange of customer files has been a common practice for decades and does not pose a security risk to you. The exchange usually involves only the basic contact information and very general information about your purchases. These lists are used to send mail to you, call you, e-mail you, or text you about special promotions or offers. This enables a company to more effectively reach out to individuals who are not yet customers, but who might have an interest in or need for their product or service.

It is also a very common practice for a business or organization to create a marketing file of names, addresses, and other information related to their customers' purchases. This information may include household characteristics obtained from surveys you fill out or from general communication with you.

Marketing, however, is just one use for information about you. Early detection and prevention of fraud by verifying your identity is a second use that offers significant benefits to both you and businesses. Being able to correctly recognize a customer, especially when transacting business over the phone, on the Internet, or via a mobile device, helps reduce the chances you will become a victim of identity fraud.

There are also other uses of personal information you may not have considered, such as courts tracing parents who fail to meet child support obligations, investigators conducting background checks for the purposes of compliance and anti-fraud initiatives, law enforcement agencies apprehending criminals, attorneys searching for missing heirs, or family members looking for lost relatives, to name just a few. All of these provide significant benefits to society as a whole and are permitted or, in some cases, required by various laws such as background screening for child care centers and school bus drivers.

What Kind of Information Is Available?

There is a variety of information available to businesses and organizations. Most of the information is non-sensitive, but some of it is sensitive.

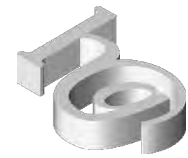
Public Records

Collected primarily from state and federal government sources, information about you may come from public records, including property deeds, marriage and professional licenses, and birth and death records.

Information is also available from court proceedings, voter registration files, driver's license records, and motor vehicle registrations. Various federal and state laws place restrictions on the use of some of these sources.

Publicly Available Information

Some information is considered in the public domain, meaning anyone has access to it. This type of information includes telephone directory listings, professional registries, classified ads, information posted in chat rooms, on blogs, and in public sections or designated as public on social network sites. Publicly available information is not always regulated by law, but responsible providers self-regulate its use through industry codes of conduct.



Customer Information

This is information that is collected when you provide information about yourself to an organization when you inquire about a product, make a donation, make a purchase, register a product warranty, or receive a service. This information includes details you provide about how to contact you and a record of your interactions with the company or organization. This information is regulated in some cases by law and in other cases by industry practice. In addition to this, responsible organizations develop their own policies to assure appropriate use of the information.

Self-reported Information

Information you voluntarily provide on a survey or questionnaire is considered self-reported. When this type of information is collected, you should be informed of the intended uses and your options for said use. Both law and industry practices limit the use of this information.

Passively Collected Information

The Internet and other technologies, like mobile devices with location tracking features and interactive televisions, may collect information about you or your device without you having to take any action. In fact, in many cases you may not be aware any collection is taking place. Some of this collection is necessary to provide you a service such as recording the number of times you go through the express lane of a tollbooth so you can be charged for the toll or when you've had a car wreck and need help locating your car to send emergency assistance. It can also be used to provide you relevant advertising such as offering you a discount on a specialty coffee from a coffee shop you are near, or to provide online advertising tailored to interests that have been identified based on other Web sites you have recently visited or keywords you have recently used in a search. Both law and industry practices limit the use of this information.

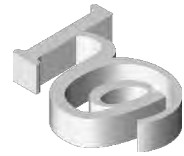
Sensitive Information

Some information, if used inappropriately, can have more serious consequences. This includes your Social Security number, driver's license number, medical records, wage and salary information, tax reports, your credit report, and information that personally identifies your children.

Sensitive information should be kept confidential and is usually not provided to other organizations unless you give specific permission or unless it is permitted, or required, under state or federal law. In order to develop credit reports, credit reporting agencies gather information from banks and other financial institutions with which you have a relationship. The Federal Trade Commission closely regulates the use of this information as directed by the Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA).

In order to assure you will be a responsible employee, tenant, or insured individual, employers, landlords, and insurance companies may ask your permission to do a background check on you. This involves verifying the information you provided on your application with the source of the data.

Background checks can also involve obtaining a credit report if your financial situation is pertinent to the employer or landlord. The Federal Trade Commission closely regulates these uses of this information as directed by the Fair Credit Reporting Act (FCRA).



How Can I Protect My Privacy?

Despite the over-abundance of information shared and sold today on the Web, there are a number of measures provided for protecting your information. It is important for you to learn about these protections and how to exercise the options that are offered to you. The following highlighted segments will give you a start on protecting your personal privacy:

Read the Privacy Policy

Reputable companies (such as financial institutions and credit card issuers) will tell you what information they collect and maintain, how it is being used, and when it is being shared with other parties. This is usually done in the form of a "Privacy Policy." You can view the privacy policy of most companies on their Web site or by contacting the company and asking for a copy. *Companies who do not post or provide a privacy policy should be given extra scrutiny.*

Act on Choices

Most companies will give you some choices regarding the use and dissemination of your personal information. Some of these choices are buried in the small print of Web sites or mailers, so you will have to look for them. If the company provides information about you to third parties for their marketing uses, you should be given a chance to "opt-out." This means you can request the company not provide information about you to third parties for marketing purposes. *Look for the annual statement from your credit card company that discusses your opt out options and act on them.*

Monitor the Accuracy

Organizations should maintain appropriate procedures that ensure the information they use about you for important or substantive decisions is accurate. You should be able to access such information if you feel it may not be accurate and have erroneous information corrected, updated, or removed. Retrieving your credit report on a regular basis and verifying the details there is a great way to monitor your private information.

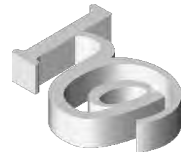
Obtain copies of and review credit reports from the three major credit reporting agencies

To order a free annual report from one, or all, of the national consumer reporting companies, visit www.annualcreditreport.com, call toll-free 877-322-8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The form can be printed from <http://ftc.gov/credit>.

Please note that annualcreditreport.com is a government recommended credit reporting service. They will ask you for personal identifiers, which might seem intrusive, but is necessary in order for you to apply for your credit reports.

Removing Information Found Online

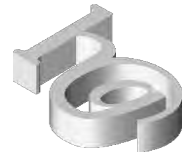
One you realize there is an abundance of information on you available to even that most casual searcher it is time to start opting out of these company resources.



A few tips and sites to follow, which will help you control, even in a small way, what is readily available to the casual searcher on the World Wide Web:

Steps

1. A very effective and helpful start is to contact your credit card companies and request to be removed from the third party marketing list. It's an offering they send out every year, as required by the FCRA; however, it is easily missed within legal jargon and interest rate updates.
2. Register with donotcall.gov to remove yourself from popular telemarketing lists.
3. Stop oversharing information online in social networks and blogs.
4. Visit Web sites which follow and locate your information, then follow the removal procedures. Some will ask you to verify your contact information, which is uncomfortable, but necessary, in order to get yourself removed.



Data Vendors for Public Records

The following vendors are the market share leaders in the public records business.

Accurint

Web Site	http://www.accurint.com
Privacy Policy	http://www.accurint.com/privacy.html
Opt-Out	Partial
Action	Visit http://www.lexisnexis.com/privacy/for-consumers/opt-out-of-lexisnexis.aspx
Affiliation	LexisNexis

Acxiom

Web Site	http://www.acxiom.com/Pages/Home.aspx
Privacy Policy	http://www.acxiom.com/about_us/privacy/privacy_policies/Pages/PrivacyPolicies.aspx
Opt-Out	Yes
Action	Visit Acxiom Web site for details on how to remove your data from Acxiom or e-mail privacy@acxiom.com or check their Privacy Statement. Be warned, it won't be easy to get it done without giving them more personal information first. The Opt-Out for consumer information can be located here: http://www.acxiom.com/about_us/privacy/consumer_information/opt_out_request_form/Pages/Opt-OutRequestForm.aspx
Affiliation	Google, Yahoo, Whowhere and Lycos.

Choicepoint

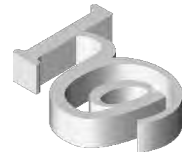
Web Site	http://www.lexisnexis.com/risk/
Privacy Policy	http://www.privacyatchoicepoint.com/
Opt-Out	Partial
Action	Visit http://www.privacyatchoicepoint.com/optout_ext.html
Affiliation	LexisNexis

Google

Web Site	http://www.google.com
Privacy Policy	http://www.google.com/intl/en/privacy.html
Opt-Out	Partial
Action	Visit http://www.google.com/support/webmasters/bin/answer.py?hl=en&answer=164734 and http://www.google.com/support/webmasters/bin/answer.py?hl=en&answer=164133 personal information

Infospace

Web Site	http://search.infospace.com/inspace/ws/index
Privacy Policy	http://support.infospace.com/privacy
Opt-Out	Yes
Action	Visit http://search.infospace.com/inspace/ws/contactUs to edit, update, or remove your personal information.



Intelius

Web Site	http://www.intelius.com
Privacy Policy	http://www.intelius.com/privacy.php
Opt-Out	Yes
Action	In order to opt out of your public information being viewable on the Intelius Web site, we need to verify your identity and require faxed proof of identity. Proof of identity can be a state issued ID card or driver's license. If you are faxing a copy of your driver's license, cross out the photo and the driver's license number. We only need to see the name, address, and date of birth. Please fax to 425-974-6194 and allow 4 to 6 weeks to process your request.
Affiliation	Anywho.com, Address.com, Infospace.com, 99lists.com, Peoplefinder.com, Peoplelookup.com, Phonebook.com, thepublicrecords.com, Zabasearch.com, backgroundcheckgateway.com,

Lexis Nexis

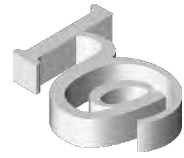
Web Site	http://www.lexisnexis.com
Privacy Policy	http://www.lexisnexis.com/privacy
Opt-Out	Partial
Action	Visit http://www.lexisnexis.com/privacy/for-consumers/opt-out-of-lexisnexis.aspx
Affiliation	Accurint.com, IRBSearch.com, Choicepoint.com

MyLife.com

Web Site	http://www.mylife.com
Privacy Policy	http://www1.mylife.com/privacy-policy
Opt-Out	Yes
Action	If you would like to remove your public listing from Mylife, return to your public profile using the Member Directory, and click the "Is This You?" link. Then click the following link: "If you like to opt out of this service, click here." An electronic form will prompt you to verify personal information, contact information, and 2 former addresses. Please fill out the form completely and select "submit form." Once your request is received, it may take up to 10 business days for your public profile to be removed from our database and Member Directory listings.
Affiliation	addressbook.com, myaddressbook.com, reunion.com, highschoolalumni.com, whoislookingforyou.com, whoissearchingforyou.com, whosesearchingforyou.com, whosesearchingforyou.com, goodcontacts.com

pipl

Web Site	http://www.pipl.com
Privacy Policy	http://www.pipl.com/privacy
Opt-Out	No
Action	Contact Mylife Customer Care toll-free at 888-704-1900
Affiliation	MyLife.com



Spokeo

Web Site	http://www.spokeo.com
Privacy Policy	http://www.spokeo.com/privacy
Opt-Out	Yes
Action	Visit http://www.spokeo.com/privacy and read the privacy policy section, "Content Removal from Spokeo Searches"

US Search

Web Site	http://www.ussearch.com/consumer/index.jsp
Privacy Policy	http://www.ussearch.com/consumer/commerce/about/privacy.jsp?adID=10002101
Opt-Out	Yes
Action	Visit http://www.ussearch.com/consumer/ala/landing.do?did=538

ZabaSearch

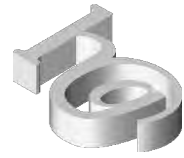
Web Site	http://www.zabasearch.com
Privacy Policy	http://www.zabasearch.com/privacy.php
Opt-Out	Yes
Action	Visit http://www.zabasearch.com/block_records

Zoom Info

Web Site	http://www.zoominfo.com
Privacy Policy	http://www.zoominfo.com/Privacy.aspx
Opt-Out	Yes
Action	Claim your account, and then remove or redact the details.

Keep Your Information Offline

1. Have all of your postal mail sent to a Post Office Box, and have packages delivered to your office.
2. Un-list and un-publish your landline phone numbers; check with your mobile service company to find out if they sell their subscribers information, and how to opt-out of that list.
3. Never put your name, number, or information on any form or application without checking to see what the policy is.
4. Mail a written request to all your credit cards and banks requesting your information be removed.
5. Do not fill out any warranty cards, but save them with original sales receipt.
6. Do not subscribe, under your own name, for any magazine subscriptions.
7. Stop sharing information in unnecessary scenarios like social networks.



Facebook Confessions, Thwarting the Cyber-Bully and Preventing Online Identity Theft

How a good thing turned into your own reality show.

The attraction of reconnecting with old friends, networking with colleagues and clients, even finding long-lost loves, can now all occur in a social network from a desktop computer (or laptop or cell phone or personal digital assistant), on a global scale. No real effort and, most importantly, no real talent (programming skills or otherwise) are necessary. With plug-and-play Web 2.0 applications (second generation Web sites such as Facebook, Wikipedia and Myspace) , you simply fill in the blanks, answer a few questions, and you are now participating in, and part of, a global network.

In the past, when Web sites were developed and maintained by a select few, those unique participants were the only authors of what happened on the Web. Today, anyone and their grandmother can start sharing their thoughts and photos online through easily accessible social networks. And they do.

But with ease-of-use often comes lack of control. While people are reuniting, connecting, and sharing in the light of online social networks, the dark side is online as well—fomenting a world of their own in which pedophiles are viewing the MySpace pages of children, gangs are creating Facebook profiles, and criminals are trolling for target homes to rob as owners announce in their social networks, “We’re going on vacation for a week!”

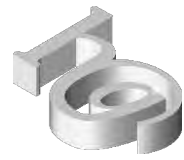
What was once a medium for the few is now an open market for any and all users—good, bad, indifferent, and sometimes downright ugly.

Everyday Joes and Janes—millions of them—once content to surf the Web and e-mail their friends as their primary Internet activities, are now using social tools like Facebook and Twitter to keep everyone apprised of their day-to-day lives, often in the most minute detail.

The technology is reaching a younger demographic. Teenagers, and younger “tweenagers,” are easily and readily adapting to the technology. And for them, there is no division between their real lives and their online lives. Their physical-world lives are also their online lives—with no holding back. The younger users will say and do pretty much anything online, and often do. On the other hand, adults and seniors are also participating in online social networks, but, unlike the younger set, these more mature folk, who grew up in an era of discretion and modesty, are not as open in their online social network postings. In general, younger people will join social networks openly; adults will generally still use caution before sharing their lives online.

Facebook Confessions

People on the social network Facebook have a lot of contact with one another—and those people actually care about what is said. These shifts can initially be unsettling for the first-time Facebook user. In the physical world, good or bad news would be shared over the telephone or spoken in person to a few close friends. You wouldn’t stand on a mountaintop and announce to the world that you just



finished a load of laundry or that you were staying home with a sick child that day. Never mind the mountaintop, you wouldn't even walk into your local grocery store and do that. Doing so would seem awkward and inappropriate. And, yet, in online social networks such as Facebook or Twitter, it feels like the social norm to mention these details. In fact, it is almost a social obligation to do so.

And that's where things get sticky. In an environment of such relatively uninhibited, open communication, it isn't long before overzealous opinions, little bits of rage, drunken rants, and other embarrassing entries get posted. The user could be upset, deranged, or overjoyed, and his or her natural reaction is to share the emotion—and often that sharing takes place on their social network. Friends don't let friends drive drunk, right? I say, not only take the keys away from that person, but also the keyboards!

Sharing your thoughts and activities online in and of itself is not necessarily a problem. The problem comes when users forget that everyone in their social network is reading their post. So when you post something in frustration with your boss, co-worker, spouse, or friend, remember that the boss, co-worker, spouse, or friend—and all their networked friends (and all of *their* networked friends) —may also be reading your posts.

Want examples? Visit <http://youopenbook.org> and search the following phrases: “hate my boss,” “cheated on my husband,” or any other such confessional phrase to search public Facebook postings using Facebook's own search service.

Having second thoughts now about using Facebook? It is possible to take part in Facebook and still maintain a semblance of privacy. To accomplish that, keep some of the following things in mind when posting to Facebook.

What Not to Do in Facebook:

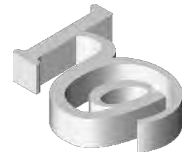
1. Do not write in a fury

If you are angry, inebriated, or simply have a big secret that you are itching to share, that is the time to step away from the keyboard. What you think is hysterical or outlandish now, might only serve to embarrass you, the poster, later.

2. Do not ignore Facebook's privacy controls

Your Facebook profile can be customized. Do it. Limit access to only your friends, friends of friends, or only yourself. Do not enter contact information, such as your phone number and address. Restrict access to your photos, birth date, religious views, and family information, among other things. Give only certain people, or groups of people, access to items such as photos or block specific people from seeing them.

3. Do not post your child's name in a photo caption



Don't use a child's name in photo tags or captions. If someone else does, delete the name's tag by clicking on "Remove Tag." If your child isn't on Facebook and someone includes his or her name in a caption, ask that person to remove the name. Do not share online the details of your child's life. Soccer practice is likely on a regular schedule, which can be easily tracked by a predator reading Facebook profiles.

4. Do not mention when you'll be away from home

When you tell your friends through Facebook that you are not going to be home, you are inviting criminals who are trolling Facebook profiles—especially unsecured profiles—to your house.

5. Do not use a weak password

Avoid using simple names or words that can be found in a dictionary as a password. Even with numerals tacked on the end of the word, these are not secure passwords. Instead, use a knuckle-breaker password, one that requires upper and lower case letters, in combination with numerals and symbols. A secure password should have a minimum of eight characters.

6. Do not put your birthday in your profile

Your birth date is an ideal target for identity thieves, who could then use the date to obtain more information about you, potentially gaining access to your bank or credit card accounts. If you've already entered your birth date in Facebook, go to your profile page and click on the Info tab, then on "Edit Information." Under the Basic Information section, choose to show only the month and day—or, better yet, no birth date at all.

7. Do not let search engines find you

To help prevent strangers from accessing your Facebook page, go to the Search section of Facebook's privacy controls and select Only Friends for Facebook search results. Be sure the box for public search results is not checked.

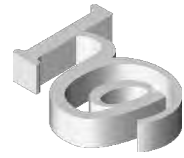
8. Do not ignore your privacy settings

Facebook changes its Terms of Service regularly. You must check your profile through the tabs "Choose Your Privacy Settings," then "Basic Directory Information," then choose "Preview my Profile."

9. Do not permit your children to be on Facebook

Facebook limits its members to ages 13 and over, but children younger than 13 do use it. If you have a young child or teenager on Facebook, then become one of their online Friends—it is your best chance to provide parental oversight of what is going on in their account. Use your e-mail address as the contact for their account so that you receive their notifications and can monitor their activities.

10. Do not Friend your employer



Sure it seems like a great idea to Friend your boss—that is, until you decide to rant about how much you hate working overtime, or you post photos of your day at the beach (um, the same day you called into work sick).

Cyber-bullying, Harassment, and Stalking

What happens when the online rants and ravings in social networks are directed towards a specific individual in a cruel or demeaning fashion?

Unfortunately, these types of posts are getting more prevalent, and it's shocking how harsh and off-color some of them can be. But the real problem comes when one or more individuals start making attacks against a specific person. Some individuals post horrendous lies or attacks online, with no restraint or remorse, against another person.

In the physical world, I can face off with an individual and say horrible things to him or her directly, or even to others, about that individual. In the physical world, this is called slander. When slanderous statements are made online in social networks, or through text messages and e-mails, they are, by definition, stored in an electronic medium, which then turns slander into libelous action. Cyber-bullying, harassment, and stalking are all measures of libelous activity.

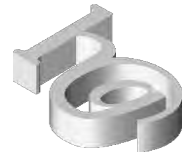
Whether called bullying or harassment or stalking, the end result is an attack on the person, defaming their name on the Web. Entire Web sites and blogs (Web logs) have been devoted to defamation campaigns against an individual. These cowardly posts, written with an agenda to defame the targeted individual, are often done in anonymous fashion, making it difficult to discern the actual offender.

Attempts to locate the online poster can be made with some success. The effort requires time and expertise—two things most online users are short on, and so the average victim is left with an unknown harasser. Adding insult to injury, most defamation posts do not cross the line far enough legally to merit law enforcement attention.

On the other hand, most victims usually have a sense of who the culprit is and might find alternatives, like using an intermediary to halt the activity. Students are told to let the teachers and administrators know if posts about themselves start appearing.

Beyond all that, there are ways to thwart and/or prevent online cyber-bullying yourself. For example:

- Run your name through Google on a regular basis to monitor where your name is being mentioned online.
- Secure your online space. One way is to set your Facebook account to private. When you allow anyone in, you are essentially giving anyone—including cyber-bullies—open access to your data.
- When you do come across a cyber-bully's online posting, resist the temptation to retort. Antagonizing a bully will only give the bully what he wants: attention. If you ignore him or her, he or she will most likely move along to another (more vocal) target.



- If someone is posting inappropriate comments on a social network service, report the abusive behavior to the social network's account security (for example, the Report link in Facebook).

Preventing Identity Theft Online

Identity theft—the theft of your personal identifiers and their unauthorized use in fraudulent activities—predates the Internet. Identity thieves are savvy enough to know that the well-protected profile is not worth pursuing. Identity theft is a crime for the lazy; such thieves would rather go after the low-hanging fruit—swiping a credit card receipt off a diner's table, for example—than strain for the hard-to-reach, well-protected profiles.

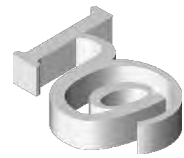
Ironically, we fear losing our identity to theft in the online financial services we use—our credit card and bank accounts—and yet give no thought to the personal information lying open in our social network profiles. The established online financial and commerce systems are some of the most trusted sites available, using multi-layered encryption software to protect your financial transactions. Of course, no one system is absolutely impenetrable, but why should a cyber thief try to steal a credit card when the Internet offers up so much more easily-attainable information?

Today, an identity thief need only turn to the personal profiles posted in social network sites, like Facebook and LinkedIn, to capture key information about a targeted individual. A full name (even maiden name), date of birth, and current home location gleaned from an open social network account are sufficient data points for a thief to start creating a fraudulent profile. In fact, LinkedIn, the working professional's social network workhorse, holds a veritable goldmine of personal information for identity thieves. Consider this: LinkedIn requires its users to post schools attended and jobs held with corresponding dates. Now layer on the personal details gleaned from linked colleagues and friends in the network and you can rather easily crib together a good list of controlled answers for most challenge questions—those security questions used to prompt for a forgotten password.

It's not impossible to lose access to your own Web-based e-mail account simply because an identity thief was able to hijack the account by answering the security challenge question after pulling the information off open-source search engines, or from one or more unprotected social network profiles.

So how does one go about preventing online identity theft? In addition to the guidelines stated earlier in this article for thwarting cyber-bullying, additional online security tips include:

- Monitor your name online. Set up a Google Alert (google.com/alert) and a Tracklet (tracklet.com) on your own name. If anything is said about you—either in a social network or elsewhere online—these services will send you a notification.
- Tweak your memorable word, in a memorable way, of course, that answers your challenge question. For example, if your first dog's name was Java, use the word "coffee" as a challenge answer, and memorize that tweaked word. Or pick one obtuse word, like "rollerblade," to answer every challenge question and, again, memorize that obtuse word.



- If someone you haven't communicated with in ages tries to contact you in a social network, ask him/her your own challenge question: "Hey, do you remember Jorge Beale getting stuck at the top of ropes in gym class?" The question can be honest or made-up. Pay more attention to the answer—does it seem authentic?
- Don't publish your life story on social networks. Be discreet online; your full name and general vicinity of where you reside are sufficient identifying information. Combining information from LinkedIn with information from Zabasearch.com lets a thief quickly locate your home address.
- Request to have your personal information removed from online identifying databases such as Intelius.com.

The Internet started as a communications network among a community of mostly academics. The evolved Internet technologies of today's Web 2.0 applications brought the Internet to the general public—the Average Joes and Janes, who have happily become active, engaged Internet users.

With the Internet now open to anyone, everyone is online. And just as there are good and not-so-good people in the physical world, there are also good and not-so-good people in the online world. With ubiquity and facility come threats and need for caution. Should you find yourself discovering the Internet's dark side of identity theft, don't pack up, shut down, and remove yourself wholesale from the online world. Instead, alter or completely delete your pertinent information (i.e., date of birth, hometown name, identifying photos, etc.) from your online profile. After completing that, leave the site active for a period of two to four weeks, to allow information-crawling search engines to capture and archive your now updated, reduced profile. After a month's time, then delete your social network profile. Actions such as these will help ward off much of the potential online threat of identity theft.

If you use a social network infrequently—for example, as a place to view your extended family's vacation photos—then offer up only non-essential information when creating an account on the service. If you do so, plus use the service's provided security tools and precautions, there should be no harm, no foul, to be concerned about. There should be nothing stored online that you need to be concerned about, nothing for anyone to bully you for, or steal from you.

Respect Web 2.0 applications. If you would not feel comfortable having your online activity broadcast through your local grocery store's public address system, while simultaneously having a giant, neon arrow pointing directly at you, then there's a good chance that your online activity has no business being online.