PROJECT 2

Your Online Brand

OBJECTIVES

- Manage your online brand
- Distinguish between appropriate and compromising online content
- Protect your personal privacy
- Secure your online information to avoid identity theft

Introduction

The information you choose to convey to the world about yourself during a job search is no longer limited to what's included on your résumé. What you voluntarily post about yourself on the Internet—part of your online brand—is a natural extension of the image you present to the public.

Ranked among the top Web sites people visit regularly, social networks such as Facebook, LinkedIn, and China's Renren have become some of the Internet's fastest-growing entities. Starting from nothing in 2003, they have become the daily points of connection, communication, and community for hundreds of millions of people around the world. Personal data, photos, videos, messages, and more fill personal pages as people document their lives online. Blogs and wikis also have found a home as more people choose to digitally express themselves on the Internet.

With around-the-clock access to this personal information, questions related to both appropriateness and privacy have started to surface. Although you might post photos and comments online to keep your friends and family informed, companies have used these same postings as a rich source of information, giving them a more complete picture of who you are and how you are likely to behave as an employee. The line between what is considered private information and what is considered fair game by employers has become blurred. Knowing how to best manage your online brand has never been more important or relevant.

STARTING DATA FILES

Tech_02.docx
Revise_02.docx
Create_02.docx
VideoCritique_Worksheet_02.docx

Encore Consulting: Video Episode 2

In the Project 1 Encore Video Episodes 1a and 1b, you watched four student candidates—Matthew, Jill, Sophie, and Tony—going through on-campus interviews with Candace Johnson and Gerry West, the recruiters from Encore. The candidates exhibited varying states of preparedness, which you critiqued for use in your own career preparation activities.

Our story picks up here in Episode 2 with Candace coming back to the office to review interview results from a number of colleges. Watch Candace's introduction on the video that accompanies this text, and then read what happened back at the office in the section below.

Scenario—Encore corporate headquarters, Candace Johnson's office

Candace: "Over the past couple of weeks, I've interviewed dozens of students at several schools in the region, as has my colleague, Gerry. Now, I'm back in the office to determine who will get called for a second interview here at our office. Some of the candidates were well prepared, which definitely gives them an advantage. But there's some homework I need to do before we extend offers for visits."

Candace and her assistant, Fermina, begin poring over the interview notes and résumés collected during the recruiting run. Fifteen students were interviewed. Candace creates a quick summary of her observations from the first few.

Candace: "Let's review Sophie Aguilar's résumé and interview. Her appearance was the first sign she might not be a good fit for our firm. She was slightly disheveled and wore excessive jewelry—although her suit was OK, if a bit bright in color. I wonder if she looked in the mirror before she left the house! Can you imagine what one of our clients would think? She needs to exude professionalism and competence. And wrong as it may seem, she will be judged on her appearance—which will initially affect how much the client will respect her work. She also didn't seem to have done any research or have any idea of the type of work we do—not a good sign."

"Now, as for Matthew Brady, it's clear his mother is controlling his actions. Although I'm supportive of being close to family, he's an adult who now needs to take charge of his own affairs. We've had enough situations involving parents calling Human Resources when they don't think their child has received a fair raise or promotion, or been given a decent job assignment. In addition, he gave some signals by his answers that he isn't interested in a long-term career with Encore. What did he say? Oh, yes: *'A job like this could be a good place to start for a year or two before I move on to something else.'* With a short-term attitude, he'd not likely pay attention to details or fully engage in the continuing education we require. He *was* dressed well, though, but I suspect that was mom's doing and not his own. We need people who can think and act for themselves."

"Now, as for Jill Tanner, she made a good first impression on me. Her résumé was impeccable, and it was clear from the questions she asked that she had done her homework on Encore. She looked me in the eye and had a good firm handshake, too, which will impress our clients. The only thing we'll need to work on is her definition of professional attire. Although her suit was nice, the skirt was too short and the open-toe, strappy heels are not appropriate for the work world. We've seen this before, though, with college students. With a little side discussion about professional attire, she should be just fine. I'd like to invite her in for a second interview to meet the rest of our team, so they can provide their evaluation of her as a potential colleague. They trust me to check out the education and work experience qualifications—all the items on the résumé—so they're going to look for personality fit and interests, and whether they could spend an hour in the car with her while driving to the client location. This will be our chance to sell her on Encore as the best place to start her career at the same time. After all, we do much of our work in groups; so if she meets with their approval and she likes what she sees, we could be extending an offer within a couple weeks."

"Gerry has forwarded information on a student named Tony Bonacci that he interviewed last week. Let's see...his recruiting summary indicates the following: pleasant demeanor

and good handshake, a bit quiet or shy, well-dressed, shoes polished, clean fingernails, and neatly cut hair. And a portfolio with Excel spreadsheet assignment projects! Good, good...strong résumé with several teamwork experiences and even some leadership. Gerry doesn't say whether he sent a thank you note, but everything else looks favorable."

As Candace finishes reviewing the rest of the résumés and interview notes, Fermina hands her the day's mail. She also gives Candace the results of her informal, online checks of each candidate.

Candace: "Here's a nice thank you note from Sophie. It is handwritten, which is fine, and well written. I also see an e-mail follow-up note from her, asking when her office visit and second interview will be since she's really busy this semester and might not have time if we wait too long. Hmmm...."

"I see I've also received a handwritten thank you note from Matthew. But it looks like mom's handwriting."

"I don't see anything yet from Jill, though. That's a bit disappointing, since she was on the right track up to this point. It would have moved her to the top of the candidate second interview list if she had followed up, but the fact that she didn't will not completely ruin her chances."

"As for the online search results, it would appear that none of the candidates bothered to clean up their social network pages. It's OK to have a personal life, but I'd rather not see our employees posting pictures of themselves drinking, or scantily clad. If a client saw these images, it might compromise the integrity of the employee and give the client a reason to question that employee's judgment in a professional situation. In fact, we had an incident last year with one of our consultants that put us in a sticky situation and we ended up having to terminate her employment. We don't need that headache again!"

After finishing her review, Candace says, "OK, that's what I needed to make my final recommendations for second interviews."

Social Networks, Blogs, Wiki Postings, and Your Career

KEY POINT

Use Web 2.0 resources to develop and reinforce a positive online brand.

With the rapid growth of social networks on the Internet, the line between your personal life and public life is sometimes difficult to distinguish. A **social network** is a Web site that allows individuals to connect with others. Users can post photo, video, audio, and text content about themselves on custom-created digital pages, and then create a network of friends linked through each other's pages. Blogs and wikis also are rich sources of information, posted by individuals who wish to use the Internet as their soapbox or simply to exercise their First Amendment rights to free speech. A **blog** is an online journal, usually written in chronological order by an individual. A **wiki** is a collaborative Web site that permits multiple users to edit or add content.

It may not seem fair that total strangers can (and do) look at what you have posted on a social network page, blog, or wiki and use it to judge you. Yet the very public nature of the Internet makes it easy to do. In fact, nearly eight out of 10 employers perform online searches to see what else they can learn about the people who have applied to work for them, according to the business social networking site ExecuNet. Surveys conducted by CareerBuilder.com and the National Association of Colleges and Employers have yielded similar results. Yet 60% of Internet users are not concerned about what others find, according to the Pew Internet Project, and most don't take steps to control what's out there. In fact, nearly 75% of users have only looked once or twice for their digital presence.

More than half of the companies surveyed by CareerBuilder.com eliminated a candidate because of information they found posted online. The information included questionable or inappropriate postings and photos, poor communication skills, links to criminal behavior, and lies about qualifications. And it's not limited to just a few social network sites. Employers also use Google, WebMii, and companies that specialize in background checks to search for job candidates. They may even take a look at YouTube.

An employer cannot ask questions about a person's social life during an interview, but there is no law prohibiting the discovery of his or her interests from online sources. The *bottom line: If you do not want a potential employer to learn more than you want to reveal, remove any content you deem off-limits from all public online sources, or at least make your pages private or only available on password-protected sites. Keep in mind, however, this content may still be accessed if the background check is thorough, so* there's not a 100% guarantee of confidentiality or privacy. Figure 2-1 lists a few personal items to consider keeping off the Web.

Figure 2-1 Information that shouldn't be posted online

Age or birth date	Political affiliation
Race	Sexual orientation
Religion	Social activities and photos that may be viewed negatively
Unprofessional screen names	Personal correspondence or postings intended only for friends and family

What online sites contain personal information, photos, or videos about you that may make a potential employer question your fit with the company? Consider the links to friends' pages and postings as well.

_____

_____

_____

_____

What items from Figure 2-1 should you consider removing from online sites that you don't want potential employers or future business colleagues to see?

_____

_____

_____

_____

What, exactly, are potential employers looking for in these online searches? In addition to learning more about your demographics and your social and personal interests, they're looking for signals that you'll be a valuable contributor to their enterprise. According to a survey by ERE Media, companies are looking for a wide range of attributes, as shown in Figure 2-2.

Figure 2-2 Attributes employers look for in online searches

1. Résumé content verification: job skills, employment history, contact information
2. Presentation and communication skills
3. Integrity, intelligence, and good judgment
4. Professionalism and club/association affiliations
5. Creativity or ability to be innovative

In addition to informal online searches, many employers also rely on independent, third-party background checks to verify résumé claims and to uncover anything that may have been omitted. When such background checks are used, the Fair Credit Reporting Act (FCRA)—which regulates the collection, distribution, and use of consumer credit information—requires the employer to notify the applicant when negative information turns up, along with the name of the company that provided the information. To conduct background checks for certain information, such as driving, felony, or credit history, the applicant's written permission will be required. However, informal searches, such as a Google or WebMii search, do not fall under the requirements of the FCRA. The issue here for job applicants is that there is usually no opportunity to explain or defend the online information, or to correct it if the content contains material errors.

If you have any concerns about what your background check may reveal, consider paying the nominal fee charged by companies such as Spokeo, MyBackgroundCheck, and US Search so you can be prepared in case questions arise. Just what might show up? Anything you have been charged with—not just convictions—back to age 18 or 21, in some cases. There is no seven-year statute of limitations on what a background check can reveal; so if you have any driving violations, drug charges, or "minor in possession" citations, they could appear. If you do get questioned about your background by the recruiters, don't lie. Depending on the issue, if you are honest and direct with the company, chances are it won't be held against you in the hiring process.

Another possibility to consider is subscribing to an online service that will regularly scour the Internet on your behalf to locate information being posted about you. Such services search all social networks, professional review Web sites, blogs, online news sources, and digital media sharing sites, such as YouTube and Flickr, in addition to all publicly available Internet sites. One such company, Reputation.com, can even handle the dirty work of getting the negative or potentially damaging content removed.

Branding Yourself Online

KEY POINT

Regularly conducting online searches for your digital presence can minimize problems later on.

Does the growing use of online resources by recruiters mean you need to erase all digital evidence of your existence from the Internet? Not at all. That may send a negative signal as well. Instead, consider the content on the Internet as an extension of your résumé and manage it as your own personal marketing space.

Here are some ways to enhance what others may find when they search. First, clean up any postings you've made to social networking sites such as Facebook and MySpace, or delete (not just de-activate) any accounts you want to close. Remove any posted interests that would portray you as irresponsible or immature, including both text and photos. Consider paring back your list of friends, especially those whose online postings might contain photos of or content about you that you no longer want the public to see. You may even want to ask friends to remove photos of you that they have posted on their sites if you think the photos could be located.

Which friends do I need to ask to remove questionable images or comments about me?

_____

_____

_____

_____

Consider purchasing your own domain name through one of the Internet registrants, such as Network Solutions or Register.com. These sites show up in online searches and may prove valuable in countering any negative online content found by a potential employer. When you buy your own domain name, you can then create and post a Web site with positive content that you control. Think of it as your personal marketing space. As an alternative, create a simple Web site hosted by an Internet service provider or the free Google Sites (google.com/sites) that at least lets you control the content posted there.

Go to networksolutions.com or register.com and conduct a domain name search for your name. Is it available? How much does it cost? Does this seem like a good investment?

Do you like to write? Think about starting a blog that you can use to express your views at a site such as blogger.com, wordpress.com, or livejournal.com. Blog entries are "signed" by the author (you), so your blog should show up when an online search for your name is performed. Some recruiters are starting to use blog-searching tools such as Technorati, Blogdigger, and Daypop to review blog postings. Just make sure that the topics you discuss on any blog will be viewed favorably by a potential employer.

What about Twitter? This short-message service is increasingly being used to broadcast, or "tweet," to "followers" what you are up to, in real time and using only 140 characters. Companies are now using Twitter for business reasons, including tweets about open positions, so having a personal account is fine—but be sure your tweets, like your other online postings, tell a consistent and positive story about you. If you're interested in working for certain companies, be sure to follow them on Twitter so you get the latest news updates, including job postings, when they're sent. Who knows? Your next big job opportunity just might come to you this way.

Another way to demonstrate that you're serious about your professional career and online brand is to join a business-oriented social networking site, such as LinkedIn. Put it on your résumé, or mention it during the interview. Started in 2003, this network contains close to 100 million professionals around the world, including executives from all the Fortune 500 companies. Think of LinkedIn as a gigantic electronic address book. Corporate recruiters are starting to use this site not only to learn more about current job applicants, but also to find people who haven't applied but might be the right person for a job opening. According to LinkedIn cofounder Konstantin Guericke, well over 100,000 recruiters are registered on the site. There may be other networking sites associated with your chosen profession that you could join as well. Doing so can demonstrate that you are serious about joining the ranks of working professionals in your field. You can ask your instructors who are members to connect with you and provide recommendations, if appropriate. If you do join such a site, include keywords in your profile that describe you and will help someone find you when conducting a search. Some examples include the very words you used in your résumé.

Look at the résumé you created in Project 1. What keywords might be used to describe you in an online search?

_____

_____

_____

_____

Online Personal Privacy and Information Security

The use of online searches by corporate recruiters may be disturbing to some applicants, but the fact that an immense amount of personal information can be sourced electronically should not be a surprise to you. After all, much of that information has been openly and knowingly provided by you through Web sites, social networks, blog posts, and Twitter feeds. The challenge, as you've discovered earlier in the project, is managing the information that's available online. By remaining aware of potential uses and risks, employing common sense, and taking precautions, you can maintain a comfortable level of security and privacy. The following section discusses some laws, practices, and tools that can help.

Privacy Laws

Concerns about privacy have led to the enactment of federal and state laws regarding the storage and disclosure of personal data, as shown in Figure 2-3. There are several common threads connecting these laws. For example:

- Information collected and stored about individuals should be limited to what is necessary to carry out the function of the business or government agency collecting the data.
- Once collected, provisions should be made to restrict data access to only those employees within the organization who need such access to do their jobs.
- Personal information should be released outside the collecting organization only when the individual has agreed to its disclosure.
- When information is collected about an individual, that person should know that the data is being collected and have the chance to determine the accuracy of the data.

Figure 2-3 **Selected U.S. Laws related to privacy**

Date	Law	Purpose
2003	Fair and Accurate Credit Transactions Act of 2003 (FACT Act)	Allows consumers to put fraud alerts on their credit files if they believe they have been the victim of identity theft
2001; renewed 2006	Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act	Gives law enforcement the right to monitor people's activities, including Web and e-mail activity
1999	Gramm-Leach-Bliley Act (GLBA), also known as Financial Services Modernization Act	Protects individuals from unauthorized disclosures of financial information and requires entities to periodically report information disclosure policies to consumers
1996	National Information Infrastructure Protection Act	Penalizes theft of information across state lines, threats against networks, and computer system trespassing
1996	Health Insurance Portability and Accountability Act (HIPAA)	Regulates the disclosure of patient health information, requires providers to seek the patient's permission before sharing any medical or health-related information, and provides for the reporting of disclosed information to patients, upon request
1986	Electronic Communications Privacy Act (ECPA)	Provides the same right of privacy protection for the postal delivery service and telephone companies to the new forms of electronic communications, such as voice mail, e-mail, and cellular phones
1984	Computer Fraud and Abuse Act	Outlaws unauthorized access of federal government computers
1978	Right to Financial Privacy Act	Outlines procedures federal agencies must follow when looking at customer records in banks
1974	Privacy Act	Prohibits federal agencies from allowing information to be used for a reason other than that for which it was collected
1974	Family Educational Rights and Privacy Act (FERPA)	Gives students and parents access to school records and limits disclosure of records to unauthorized parties
1970	Fair Credit Reporting Act (FCRA)	Forbids credit reporting agencies from releasing credit information to unauthorized people and allows consumers to review their own credit records

It's important to note that although these laws provide legal protection to individuals, if you knowingly post or provide personal information for public display on Web sites such as social networks, such protection may no longer be afforded. Most Web sites now provide policy statements regarding the use of personal information. You should carefully review these statements before providing any personal information to Web sites.

Protecting Your Online Security and Privacy

KEY POINT

Actively engage in reading the privacy policies of the online resources you use.

As noted earlier, it's nearly impossible to keep personal information off the Internet. Instead, your goal should be to manage what is already available so that it can't be used in ways you never intended. In addition to using available security software and tools on your personal computer, you can also employ smart computing practices, such as limiting what you share online. Figure 2-4 outlines a few tips from the Electronic Frontier Foundation (EFF) for helping to maintain your personal privacy online.

Think for a moment about the Web sites where you may have entered personal information. Take a few minutes to read the posted privacy statements provided by each site's owner. What do their privacy policies reveal about how they use your information? If you are not comfortable with what you find, take steps now to remove the personal content.

_____

_____

_____

_____

Figure 2-4 Advice for protecting your online privacy

Only provide information that is essential.	Many Web sites ask you to complete surveys or register when you make your first purchase. If you intend to visit the site often, providing the bare minimum (required fields) may make using the sites convenient. If you are unsure of the credibility of a Web site, don't provide any information and stop using the site.
Don't reveal personal information inadvertently.	Your browser can reveal your personal details without your awareness unless you change your browser settings. In the browser's setup, options, or preferences menus, check to see whether your name and e-mail address are visible to the Web sites you visit. If you are not using the e-mail component of your browser, remove your name and e-mail address from the Account Settings for e-mail.
Mind your digital cookies.	For maximum security, you can change your browser's privacy settings to alert you to, or block all, cookies. Your security software may offer additional ways to manage the information Web sites' cookies seek.
Limit the personal information you post on the Web or share with others who may post it.	Avoid posting your home address, telephone number, e-mail address, or other personal data on any Web site that can be publicly accessed if you don't want others to gain access to it. For job seekers, a limited amount of contact information is required, such as a telephone number or e-mail address. However, there are few instances when other personal identifiers, such as those listed in Figure 2-1, are necessary.
Remain cognizant of Web security issues.	Never submit a Social Security number, a credit card number, or other financial data over a connection that is not secure. Use encryption if you must provide sensitive information. Never provide your username and password to anyone. With the proliferation of spam and phishing scams online, being vigilant about the types of financial information you reveal can minimize your risk.
Keep your primary e-mail address clean.	Consider setting up separate e-mail addresses to keep communications for your professional and personal lives separate. There are many free e-mail account providers available that make this easy to do. Use the free e-mail account for personal correspondence. If this account becomes over-run with spam or junk messages, you can simply discontinue its use and create a new one.
Read privacy policies and review security seals on Web sites.	Get in the habit of reviewing the privacy policy of the Web sites you visit frequently, especially one where you are asked to provide personal information. Check to see if the Web site backs up its privacy policy with a seal program such as TRUSTe or BBB*OnLine*, which provide a baseline of privacy standards.

Cyberstalking

KEY POINT

Avoid posting any personal information online that could be used to harass you.

Corporate recruiters, friends, family, and professional acquaintances are not the only people interested in what you post online. Individuals with less innocent intentions can use the same information sources to commit **cyberstalking**. Cyberstalking refers to the use of the Internet, e-mail, or electronic communications devices to harass another person. Women remain the most likely targets of cyberstalkers, although men and children have also been targets.

In one high-profile case in New Hampshire, a 21-year-old man murdered a 20-year-old woman and then killed himself. For days, the police did not know the motive behind the crime. However, upon confiscating his computer, they discovered he had created two Web

sites on which he expressed his loneliness and alternating love and hatred for the woman, who was a former classmate. His online journals revealed how the man had paid Internet search agencies to find the woman's Social Security number and place of employment.

Where do cyberstalkers find their victims? Online gathering places such as social networks, chat rooms, bulletin boards, newsgroups, and online auction sites are all sources. With just a mouse click, a cyberstalker can send e-mail messages to the chosen victim and can even set up time-released messages so the harassment can progress over a period of time. In late 2010, 27-year-old Mitchell W. Hill posed as Lexie Hillbrenner, an alumnus Kappa Delta sorority "sister" who contacted numerous sorority women at several colleges in Alabama, Florida, Georgia, Louisiana, and Tennessee through Facebook. Under the guise of helping to groom them for leadership positions, the stalker started by saying the contact was a normal part of sisterhood, but that they shouldn't tell anyone about their online exchanges. In subsequent chats, Hill raised the stakes by asking the women increasingly personal questions and to send inappropriate photos, and threatened to have them kicked out of the sorority if they didn't comply.

Since cyberstalkers can harass their victims from literally anywhere, it is difficult for law enforcement to identify, locate, and arrest the offenders. Hill lived in Key West but his victims were at prestigious universities across the Southeast. As of this writing, he was charged with two counts of extortion and 12 counts of video voyeurism. All 50 states and the District of Columbia have enacted laws that explicitly cover cyberstalking, and a federal anti-stalking law makes it a crime to transmit any communication containing a threat to injure another person, whether sent via telephone, e-mail, pager, or the Internet. Figure 2-5 contains some tips to help minimize your risk of becoming a cyberstalking victim and what to do if you're being stalked.

Figure 2-5 How to prevent cyberstalking and what to do if you are cyberstalked

Tips to prevent cyberstalking

1. Don't share personal information in public spaces anywhere online, nor give it to strangers, including via e-mail, social networks, or chat rooms.
2. Don't use your real name or nickname as a screen name or user ID. Pick one that is gender- and age-neutral, and avoid posting any personal information as part of any online profile.
3. Be cautious about meeting online acquaintances in person. If you choose to do so, meet in a public place and take along a friend.
4. Check the acceptable use policy for your Internet service provider to determine how it handles cyberstalking and complaints. If it fails to provide a timely and adequate response to your complaints, switch providers.
5. If you encounter an online situation that becomes uncomfortable or hostile, log off and go elsewhere online. Contact law enforcement if the situation escalates and you feel threatened in any way.

If you are being cyberstalked...

1. If you receive unwanted contact, make it clear to that person you do not want him or her to contact you again.
2. Save all communications as evidence. Do not edit or alter the contents. Keep a file with a list of all contacts you make with law enforcement and Internet system administrators as you deal with the problem.
3. Unless the communications are needed to help law enforcement catch the harasser, set up a filter to block all unwanted messages.
4. If communications persist after you have asked the person to stop contacting you, inform the harasser's Internet service provider (indicated by the domain name after the @ sign). Most providers have written policies and contacts for reporting complaints.
5. Contact your local police department and inform it of the situation in as much detail as possible. Provide any documentation you have collected to help the police understand the situation.

After reading this section, how would you rate your risk of being cyberstalked? What steps might you take to reduce this risk?

_____

_____

_____

_____

Privacy in the Workplace

KEY POINT

Ask your employer what types of monitoring, if any, it uses on employees.

Once you start a new job, you shouldn't stop managing your personal privacy. Besides using publicly available sources to learn more about you *before* offering you a position, it's quite likely that your employer will monitor you on the job *after* you start working. In a recent survey conducted by the Society for Human Resource Management and CareerJournal.com, results pointed to technology as a great enabler of on-the-job monitoring. Everything from computer and Internet use to cell phone activity and e-mails comes under the scrutiny of employers. Figure 2-6 summarizes some key findings from the survey.

Another survey in 2007 by the American Management Association and the ePolicy Institute found that two-thirds of employers monitor Web surfing to curtail inappropriate surfing. Forty-three percent monitor e-mails, and 21% have fired an employee over e-mail abuse. Nearly 75% of employers use software for the task of monitoring communications and data traffic to and from their employees. Nearly half track keyboard activity (content and keystrokes); 12% monitor blog posts and 10% watch employee use of social networking sites.

Figure 2-6 Employee privacy and monitoring survey results

Percentage of human resources professionals who agree or somewhat agree that their organizations...	have the right to:	frequently or occasionally:
Monitor employee telephone usage	87%	56%
Listen to employee telephone conversations	41%	17%
Monitor cell phone use in the workplace	76%	48%
Monitor camera cell phone use	86%	18%
Track employee computer usage	90%	70%
Monitor employee e-mail use	87%	57%
Read employee e-mails	53%	30%
Examine instant message usage	87%	31%
Track Internet use	91%	72%

There are obvious competitive and proprietary reasons for employers to be concerned about what employees are doing and sharing via technology. But companies also want to protect against hackers, viruses, and other intruders while maintaining a safe working environment. Employees believe employers monitor them to ensure they are productive, not sharing company secrets, and not applying for jobs outside the organization.

It's not just lower-level employees who are monitored, either. In 2007, Starwood CEO Steven Heyer stepped down from his post after the company's board asked him to explain a series of allegedly suggestive e-mail communications between him and a younger female employee. Personal romantic e-mail communications also were at the center of Walmart former Senior Vice President of Marketing Julie Roehm's wrongful

termination lawsuit. Initially questioned regarding the acceptance of a gift from the advertising agency that won Walmart's $580 million account (company policy prohibits its employees from accepting gifts), evidence of an inappropriate relationship between Roehm and a subordinate later surfaced in e-mails provided by the subordinate's ex-wife. In these and other cases, sophisticated software is the tool used to sift through millions of messages in search of keywords and language.

A vast majority of companies have written policies covering workplace privacy issues. A smart employee will be aware of such policies and monitoring activity to avoid the consequences of potentially damaging use.

Have you ever been monitored at work by your employer? What activities were monitored? How did it affect your behavior, if at all?

_____

_____

_____

_____

Technology Skills—Creating a LinkedIn Account

LinkedIn has grown to become one of the most popular networking sites for professionals in nearly all professions. In order to demonstrate a sincere interest in your professional career, consider establishing a LinkedIn presence while still in college so you can take full advantage of its networking opportunities when the need arises.

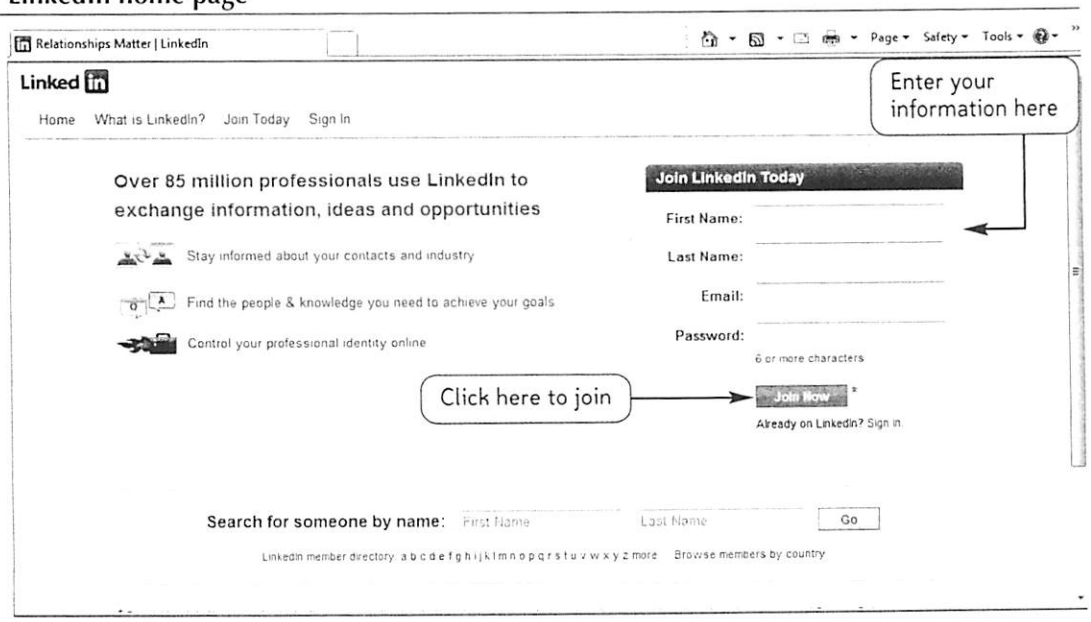
TIP

Sign up for a free e-mail account for professional use through Hotmail.com or Gmail.com before creating a LinkedIn account.

To Join LinkedIn:

1. Connect to the Internet.
2. Open a Web browser.
3. In the address box, enter **linkedin.com**. See Figure 2-7.

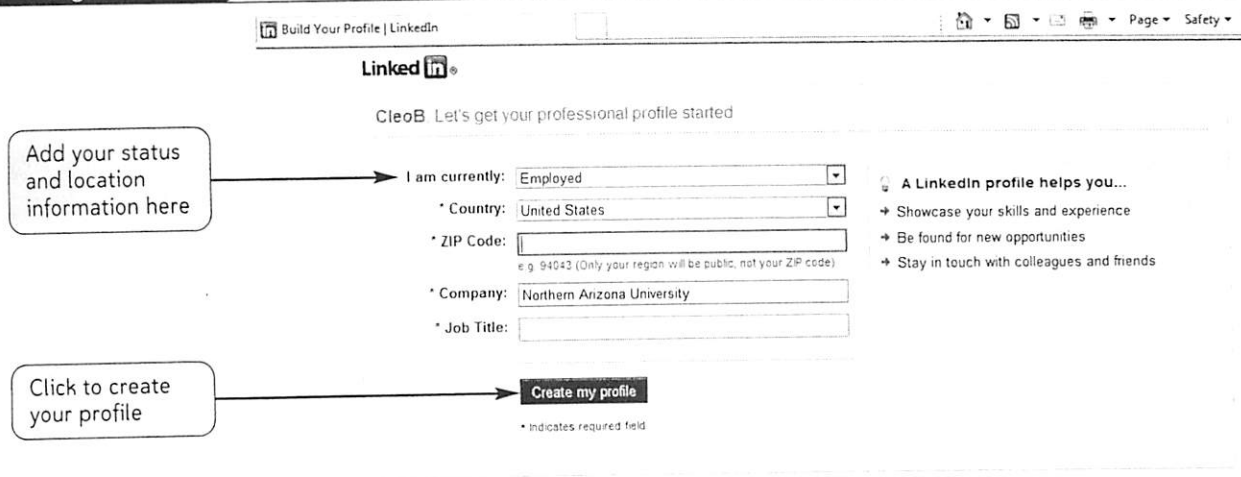
Figure 2-7 LinkedIn home page



Source: www.linkedin.com

4. Enter your first name, last name, e-mail address, and password in the Join LinkedIn Today box.
5. Click **Join Now**.
6. Complete the requested professional profile information, as shown in Figure 2-8.

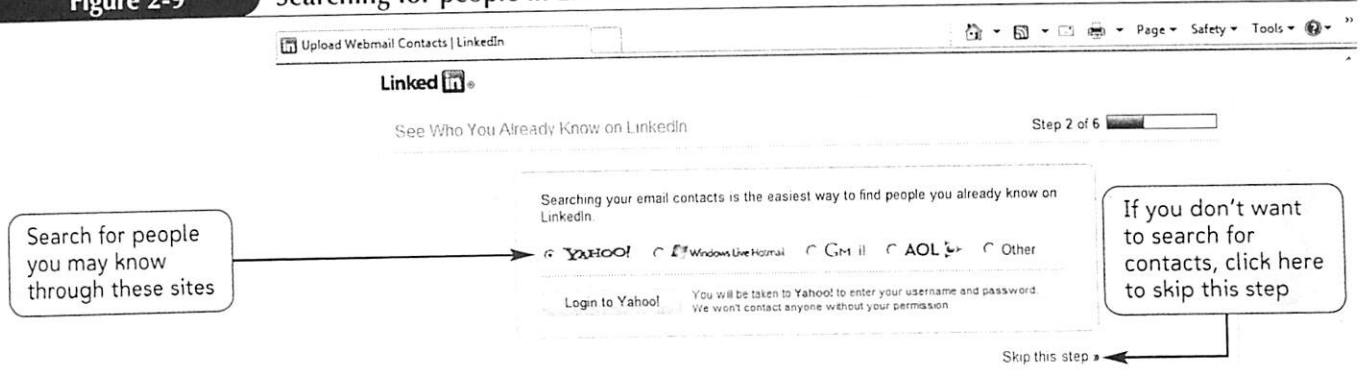
Figure 2-8 LinkedIn professional profile page



Source: www.linkedin.com

7. If you want LinkedIn to look for people you may know on LinkedIn by searching your e-mail contacts, as shown in Figure 2-9, click the service provider. Otherwise, skip this step.

Figure 2-9 Searching for people in LinkedIn



Source: www.linkedin.com

TIP

For profile pictures, headshots look more professional than full-body photos.

8. Check your e-mail inbox for a confirmation message prompting you to activate your LinkedIn account. Once activated, you can add a profile photo and additional information about yourself. Remember, this is a professional site—so limit what you post to work-related themes!

Once you've created your LinkedIn account:

1. Extend invitations to classmates with whom you want to keep in contact as a working professional.
2. If your instructor is a member, ask to join his or her professional network.
3. As with other social networks, check back periodically to make sure your information is current and accurately reflects your employment status.
4. Open **Word 2010**.
5. Launch the **Tech_02.docx** file located in the Project.02 folder included with your Data Files.
6. Save the file as **(LastName)_LinkedIn.docx**.
7. Answer the questions in the document and save it.

TIP

Use LinkedIn for professional status and work-related postings only.

PRACTICE

Personal Identity Theft Protection

Identity theft has been the top consumer fraud complaint lodged with the Federal Trade Commission since 2000, with 21% of complaints in 2009 centering on this crime. So what is identity theft? Basically, it is the theft of a person's identity through stolen identity information. In the most recent survey, the U.S. Department of Justice reports total losses in excess of $17 billion in the United States for nearly 12 million victims. The age group that was targeted the most was ages 16 to 24.

Before completing this assignment, read more on identity theft at the Federal Trade Commission's Web site, ftc.gov/idtheft.

1. Connect to the Internet and launch a Web browser.
2. Enter the URL for the Federal Trade Commission: **ftc.gov/idtheft**. This federal government agency is responsible for handling consumer complaints related to stolen identities, among other things.
3. Open a **blank document** in Word. Prepare a one-page summary of your findings related to the questions listed below.
4. Save your document as **(YourName)_IDTheft.docx**.

QUESTIONS TO ANSWER:

1. What does the FTC mean when it directs consumers to "deter, detect, and defend" against identity theft?

2. What types of fraud can be committed with stolen identity information?

3. How can you protect yourself against identity theft? List at least four practical approaches. If you use a personal social network, such as MySpace or Facebook, include one or two approaches to use in those environments.

4. How might you discover that you have been the victim of identity theft?

5. What steps should you take upon discovering that you are a victim of identity theft? List at least three actions to take.

6. List the top three things you learned from this assignment.

7. The FTC provides information on ways to increase community awareness of identity theft. If directed by your instructor, download the materials provided by the FTC and prepare a presentation that could be given to a local community group, club, or organization.

REVISE

Cleaning Up Your Online Brand

If you haven't given much thought to your online brand, now is the time to do so. Open the **Revise_02.docx** file provided with your Data Files. Follow the actions in each question, and record your results in the space provided in the document. Save the finished document as **(YourName)_OnlineBrand.docx**.

1. Perform a Google and a WebMii search on each of the following and record what the search results reveal:
   a. Your full name (including middle name)

   b. Your nicknames

   c. Your address (home and school, if different)

   d. Your phone number (home and cell)

2. Take a critical look at your blog, wiki, Twitter, and social network page postings. Have an adult relative or non-relative you respect critically evaluate the contents of these postings. Based on what he or she tells you, what needs to be removed or made private? Are there any photos, comments, typos, or grammatical errors that might give the wrong impression?

3. Once you've started work in a full-time professional position, what rules or guidelines do you think your employer might have about the use of technology and social networks? How will this affect your usage?

4. Some people don't think it's fair that employers perform background checks and online searches before making job offers, claiming that a person's private life is his or her own business and not the employer's. What's your position on this issue?

CREATE

Online Brand Protection Checklist

Take some time to create a checklist you can use to assess your personal brand protection. Use the **Create_02.docx** file if you'd like to maintain a digital copy of your list.

1. Open **Word 2010**.
2. Open the **Create_02.docx** file provided with your Project.02 Data Files and save the file as **(YourName)_Create_02.docx**.
3. Fill in the date you complete each task on the list; save and then print the document.

Figure 2-10 Online brand protection checklist

Done	Task
	Take some time to visit all the social network sites where you have posted content. Go through each one carefully and remove any content that would give your potential employer the wrong picture of who you are. If nothing else, make your pages private.
	Change any screen names or e-mail addresses that don't portray you in a professional way.
	Sign up for a new, free e-mail account for your personal correspondence.
	Google yourself. Don't stop with just your name—enter your phone numbers, addresses, and any other keywords that might be used to find you. Try other search engines as well, such as Bing, Ask.com, and Yahoo!. Now do the same thing at WebMii. If anything pops up that you don't want others to find, take steps to have the content removed, if possible.
	Try to get cached content removed from Google or other sites. Cached content is old information that doesn't immediately appear when Google returns a hit, but can be accessed by clicking on the link to cached content. Check back every few months because Google often restores archived content from backups—which means that your "removed" cached content will re-appear without your knowledge. Google posts information about how to do this under Help on its Web site.
	Sign up for a Google Alert (google.com/alerts) if you think your name might end up in the news.
	Get a free copy of your credit report at annualcreditreport.com and check it for accuracy. (Note: This is *not* the same site as the fee-based freecreditreport.com.)
	Check your browser's security settings to make sure they are set at the level you are most comfortable with.
	Investigate your current or potential employer's privacy policies with regard to employee monitoring through a Web search, company human resources policies, or the company's intranet resources.

APPLY

Case Study 1

Encore: After the Interviews As you reflect on Candace Johnson's comments at the start of this project, and what the student candidates did as part of their preparation and follow-up outside the interview setting, take a moment to write a few notes about what you plan to do in the future.

1. Open **Word 2010** and launch the **VideoCritique_Worksheet_02.docx** file located in the Project.02 folder included with your Data Files.
2. Fill in the worksheet with your answers.
3. Save, print, and submit it to your instructor.