Security Strategies in Web Applications and Social Networking

Chapter 4

From Personal Communication to Social Networking

Learning Objective and Key Concepts

Learning Objective

- Analyze online personal and business communications and the threats to those communications.

Key Concepts

- Different types of online personal and business communications
- Types of online attacks and the perpetrators who carry them out
- Security and privacy risks related to use of social media and social networking

Use of Internet Communications in Business

- **Passive Communication**
  - **E-mail**: Customer service, marketing, information, billing and invoices, and inquiries
  - **Message boards and forums**: Customer support, feedback on products and services, assistance with products and services, and interaction with other customers

Email

- The most convenient and effective method of personal and business communication.
- Easy to save and archive content for future reference.
- Available since the early days of online communication (1965 Mailbox), predating the World Wide Web.
- Instant messaging, **microblogging, podcasts**, and other media do threaten the popularity of e-mail.
- These technologies can augment e-mail communications but lack the versatility of e-mail to replace it entirely.
- To some members of the Y Generation, e-mail is outdated.
- Business world is relying on e-mail and its benefits.

E-mail Advantages

- **Editing -** important for professional communication where the grammar, substance, and style of a message are critical.
- **Professional layouts -** maintains a consistent layout and company branding.
- **Attachments –** easy to send many types of files. Antivirus software can check e-mail attachments for **viruses.**
- **Storage and organization -** better recordkeeping and archiving.
- **Filtering –** easy to prioritize messages, manage spam.

Rules for Personal E-mail

- Use proper spelling, grammar, and punctuation.
- Make it personal, so it doesn't look like spam.
- Attach only relevant files and files that are not too large.
- Don't write in all CAPITALS.
- Proofread the e-mail before sending.
- Don't use the Reply to All option unless a message is relevant for all recipients.
- Don't forward chain letters.
- Create a subject line that makes sense and is relevant.
- Don't overuse the Urgent and Important features.
- Filter spam messages and do not reply to them.

Rules for Business E-mail

- The e-mail system is for company purposes only.
- All e-mails are the property of the company and can be reviewed by the company at its discretion and without notice.
- Before sending any e-mail, consider that it may be read in court.
- Hardcopies of important e-mails should be kept and archived.
- **Passwords** are the responsibility of the user.
- E-mails need to be checked throughout the day to ensure customer and client requests are met.
- E-mails must be responded to within one business day.
- Non-text messages should not be received until first checked for viruses and malware.
- Do not use company e-mail to subscribe to online Web sites, newsletters, forums, or other non-work material without permission of the system administrator.

Professional E-mail Writing Tips

- In the To field, type the name of the recipient, not just the e-mail address.
- With **carbon copy (CC)** the e-mail address of each person in the CC field is visible to all other recipients. Use the blind carbon copy (BCC) option.
- The Subject field should be clear and concise to help categorize the e-mail.
- Formal business e-mail generally has three parts: the abstract, the body, and the conclusion.
  - **The abstract**—The abstract is a message overview. It lets the recipient know the purpose of the e-mail, what to expect, and the treatment of the topic.
  - **The body**—The body of the e-mail provides details and clearly describes the purpose of the e-mail. It should cover all of the topics mentioned in the overview.
  - **The conclusion**—The closing paragraph (exhortation) identifies what action the recipient needs to take or what action you (the sender) will take next. You may add an additional positive statement about continuing the company-customer relationship (feedback loop). The conclusion includes the signature block that identifies the sender, the credentials, and the company.
- **Attachments -** inform the recipient what the attachment is, its intended purpose, and whether it requires a special program to open or use.

The Key Elements of Web Pages

- The evolution of Web sites is not just about the technology but how information is displayed and presented using that technology.
- Traditional Web 1.0 sites were limited in their scope and presentation.
- The presentation of Web sites today has changed significantly based on an understanding of visitors and visitor preferences.

Eye Paths and Heat Maps

- many features for communication; images, text, headings, and colors all blend to form the message.
- placement of these features is not random.
- Web designers and marketers have developed strategies to place them on a page.
- One method is to use heat maps, which have been created based on eye-path data.
- "Eye pathing" or "eye tracking" is a method that identifies where the human eye instinctively looks on a Web page.
- Researchers have developed a chart or "heat map" that removes the guesswork of where people are looking on your page.
- ***http://www.squidoo.com/heat-map***

The Fold

- Arguably, the most critical part of a Web site is the fold. The "fold" refers to the area immediately visible before scrolling down to see more content.
- The key elements of the fold have become standard:
  - **The headline**—The headline at the top of the fold is critical.
  - **Relevant image**—Images in the fold area convey a message that reinforces the Web site.
  - **Navigation**—Navigation refers to the links to important pages, such as contact, privacy, and guarantees.
  - **Text**—The text in the fold area is brief and written for scanners.
  - **Call to action**—The call to action is specific text pinpointing what you want the reader to do next.

The Body

- The text used on Web pages does not follow the same patterns as text in books and magazines. Consider the following for Web text communication:
  - **Chunking**—This refers to the style of writing presented in chunks rather than long paragraphs.
  - **Bullet points**—Bullets are used to break up large sections of text.
  - **Body text**—The text within the fold must be succinct, brief, and strategically placed.
  - **Special effects**—Web content allows use of Flash, color, and other interactive content. These additional features enable new forms of communication.
  - **Grammar and spelling**—While you want to keep the tone and writing style at the level of your reader, you also want to ensure that you are following basic rules of English
  - **Language**—While you may choose to use slang to appeal to the reader, you need a healthy balance of professional and conversational language. Avoid highly technical terms and jargon.

Online Message Boards

- Online message boards are discussion sites grouped around particular topics.
- Today's online message boards originated from the traditional bulletin board (BBS) system.
- Many are personal, academic, or business related, and they all have rules regarding acceptable use.
- Have a clear code of conduct and distinct etiquette.

Online Forums

- An online forum is a Web application that maintains user-generated content.
- Online forums provide a central location from which users can discuss a variety of topics.
- Forums are comprised of "threads," which are a collection of posts from visitors.
- A thread is typically one discussion around a question or idea.
- Threads cascade in a tree-like structure listing posts from newest to oldest.
- There are thousands of personal and professional online forums.
- Forums are commonly used for support purposes.
- Benefits of forums:
  - **Encourage repeat visits**
  - **Enhance SEO marketing**
  - **Draw potential registered clients**
  - **Provide demographic data**
  - **Build relationships**
  - **Showcase your expertise**

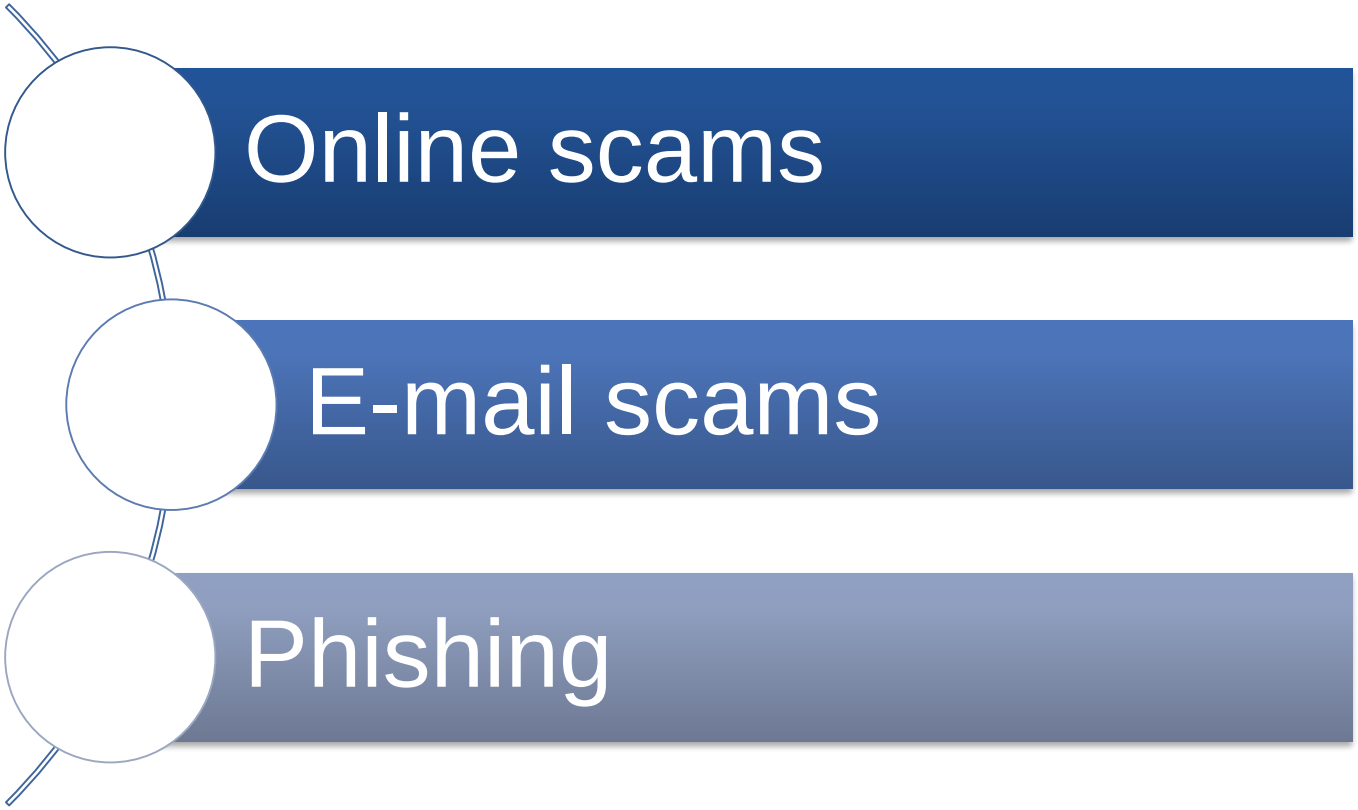
Online Virtual Community Portals

- Virtual community portals are commonplace on the Web.
- Members share a strong connection around the issues and information presented on the portal.
- Typical community portals require participation from all users and the site is very interactive (a product of Web 2.0).
- Community portals can have a dual meaning: geographic or virtual.
- Share common features, such as:
  - Home page
  - News events
  - Really Simple Syndication (RSS) feeds
  - Member directory
  - Feedback forms
  - Surveys
  - Discussion forums
  - Portal mail
  - Business directory
  - Events

Online Chat Rooms

- Online chat rooms are very popular and provide a central location for people to meet and discuss a variety of topics.
- Traditional chat rooms were text based but modern chat rooms incorporate more graphics and voice capability.
- Chat rooms are typically monitored by a moderator.
- Some chat room rules include:
  - Don't "flood" the chat room, which means constantly adding text or voice messages.
  - Limit messages to fewer than 250 characters.
  - Don't type in all, or excessive, capital letters.
  - Don't use inappropriate screen names.
  - Don't threaten other chat room users or make threats of any kind.
  - Don't hang around chat rooms without participating.
  - Let other chat room members know if you are going to be away from your computer.
  - Be friendly, polite, and considerate.

Scams



Online Scams

- Common online scams:
  - **Product offers**—Many Web sites offer products or services for free or at extreme discounts. Once credit card information is supplied, the product is not delivered and the card number is used fraudulently.
  - **Fake auctions**—Some fake auction sites never deliver the goods. Like fake product offers, the credit card information is obtained, but the product is not shipped.
  - **Online lotteries and giveaways**—Thousands of Web sites promote online lotteries and free giveaways. Although some may be legitimate, many are scams. A best practice is to review the company well before placing any confidential information on a Web site offering online lotteries and giveaways.
  - **Online contests**—Fake online contests live all over the Web. Many visitors are informed that they have won a prize and just need to enter personal information to collect.
  - **Mimic site**—Some sites mimic well-known sites to gather personal information. They may appear to be a banking site with all the company colors and logos in place, or as a well-known e-commerce site, or as sites such as PayPal. Mimic sites are often linked to fraudulent e-mail messages.
  - **Donations**—Cyber criminals take advantage of natural disasters to create illegitimate "charity" businesses supposedly helping survivors.

Protection Against Online Scams

- Be wary of unsolicited e-mail from charitable organizations, auction sites, banks, or others asking for money or personal information.
- Scan attachments to ensure they are legitimate.
- Do not click links from unsolicited e-mail as they may lead to a mimic site.
- If you receive an e-mail request from a charity you'd like to support, make sure the request is legitimate. Instead of clicking a link in the message, manually type the charity's Web address into your browser's address bar and look for how to donate.
- Keep alert on sites that try to pressure you into providing sensitive information. Phishers like to use scare tactics to create a sense of urgency.

E-mail Scams

- Some are designed to steal information, others are hoaxes, some carry **malware, m**any are simply annoying.
- Prevention:
  - In a corporate environment, **e-mail filtering software** helps detect and reject e-mail threats and spam.
  - Never submit confidential information via forms embedded within e-mail messages.
- Don’t respond to:
  - E-mail suggesting monetary windfalls
  - False giveaway e-mails
  - Charity contribution e-mail hoaxes
  - Sudden emergency e-mails
  - False virus claims and solutions
  - E-mail petitions and protests
  - E-mail chain letters
- Best defense is to monitor e-mails carefully. Do not reply to suspicious ones, do not click links, and do not open unknown attachments.

Phishing

- In a **phishing** attack, attempts are made to acquire personal, sensitive, or confidential information, often by masquerading as a trusted friend, work colleague, administrator, or legitimate Web site.
- The phisher's overall goal is to get sensitive data such as credit card numbers, username/password combinations, or bank information.
- Examples of phishing attacks include:
  - A message from an administrator asking you for your username and password
  - A Web site, such as **PayPal**, claiming you need to reenter your bank account information
  - A letter from the bank requiring personal and/or account information
  - A message from a company asking for confidential information
  - A credit card company asking for information.
- Communications from a phisher look so much like the real thing.
- User education is the best line of defense.

Preventing Phishing Attacks

- Double-check any e-mail or message asking for personal information.
- Don't click on links within e-mails that ask for your personal information. Instead, go directly to the site by typing in the Uniform Resource Locator (URL).
- Do not type personal information in a pop-up screen.
- Protect your computer with up-to-date spam filters, antivirus, and antispyware software, and a firewall.
- Only open e-mail attachments from trusted sources.

Social Engineering

- The act of manipulating people into performing actions or divulging confidential information, rather than by breaking-in or using technical hacking techniques
- Essentially a fancier, more technical way of lying

Social Engineering

- **Shoulder Surfing** - typically involves an attacker literally looking over the shoulder of the user to obtain a username and password combination. Hidden cameras may be well placed to record information.
- **Dumpster Diving** - A lot of personal information is carelessly discarded and, in the hands of the wrong people. The threat is not only to paperwork but also old hard disks. Larger corporations use disposal teams to shred and dispose of potentially sensitive data.
- **Persuasion** – The attacker pressures the user to divulge personal information. The attacker may convince the victim that the attacker is acting in the victim's or company's best interests, or that there will be serious consequences if information isn't handed over. The attacker may also ask for logon information to update the victim's computer or otherwise do a favor.
- **Impersonation - T**he attacker pretends to be someone else to gain the trust necessary to get personal information. It may be the network administrator, friends, security personnel, or co-workers. The best way to prevent impersonation is to verify a person's credentials.

Perpetrators

Scammer	• Swindles by means of deception or fraud
Blackmailer	• Extorts money by threatening to expose embarrassing information
Sex Offender	• Has committed a sex crime

Perpetrators

- **Scammers**—Scammers send fraudulent e-mail to gather personal information or they create false business sites to get credit card or other financial information. Scamming is commonplace on the Web and reduces confidence in online shopping.
- **Blackmailers**—Blackmailing takes many forms online. Often, blackmailers find personal information about you online then threaten to release it if demands are not met.
- **Sex offenders**—Many sex offenders use the Web to find victims. Sex offenders can use social networking sites, discussion boards, forums, chat rooms, or any other public Web space
- **Cyber stalkers**—Cyber stalking and tracing people electronically has become a huge problem online. Many people do not even know that someone is tracking them through social networking or other means.
- **Online bullies**—Bullying online is increasingly common online. Bullies hang out in public Web areas and track and harass other users. With a little personal information, bullies can trace victims' online steps and electronically harass them.

Privacy

- Loss of privacy data
- Violations of privacy

Loss of Privacy Data

- The terms "privacy" and "secrecy" are often used as synonyms because their meanings intersect.
- Privacy is the protection of individual rights to nondisclosure.
- **Secrecy**, on the other hand, provides protection from inadvertent information disclosure without regard to existing legislation.
- While privacy is a right, many consider secrecy a choice.
- Some Web sites sell information they gather about their visitors to other businesses. Those businesses may use this information in another inappropriate way.
- A company's privacy policy needs to state clearly what information the company is collecting, how the company will use it, and with whom the company will share this information.
- E-commerce consumers must be able to exercise control over how much information, if any, they divulge to a Web site.
- Consumers also should be able to review and correct any information an e-commerce company collects about them.
- Web site registrations and cookies are two sources of information that raise privacy issues.

Web Site Registrations

- Many Web sites take advantage of the ease of collecting customer information.
- Registration forms often ask for demographic data, such as age and Zip code, or marketing information.
- Web sites may use this information to keep you informed about new versions of the service or similar services or products they offer.
- The Electronic Privacy Information Center (EPIC) is a privacy research center. Ideas produced at EPIC have been enacted as privacy laws in the United States.
- With current Web browser technology, responses provided to one Web page cannot be remembered by the browsers themselves and used by another.

Cookies

- A "cookie" is a data file that some Web sites write to your hard drive. It contains information you entered on some Web pages, including your username and password combinations.
- Using the information in the cookies, Web browsers let the user bypass logon or other procedures in subsequent visits to the same Web page.
- Cookies make your access to certain Web pages more convenient.
- There are two types of cookies.
  - "Persistent cookies" remain on your hard drive until they expire or are erased.
  - "Session cookies," on the other hand, help browsers store data for the duration of the session.
- Because cookies may contain personal information, such as name, address, and credit information, cookies are a privacy threat.
- Browsers support cookies and provide various protection mechanisms to partially block or completely disallow their local storage.

Privacy Violations

- The issue of online privacy is a growing concern.
- The Electronic Communications Privacy Act of 1986 is the main law governing privacy on the Internet in the United States. Additional regulations have been added to cover issues that were not originally considered or events that occurred later.
- Industries may adopt their own standards and policies to address issues such as privacy
- Countries have different expectations for individual privacy. In Europe, collected data is expected to be used only for its intended purpose. Laws prohibit exchange of consumer data between businesses without the customer's express consent.
- Various global efforts have emerged to harmonize privacy or data protection. The Council of Europe Privacy Convention 108 is one of the first and most elaborate data-privacy laws within and between countries of the European Union.
- More standards and privacy protections are included in the European Union Privacy Directive.
- The United States does not yet have comparable legislation.

Secure Social Networking Practices

- Be cautious with personal information
- Review privacy settings
- Use strong passwords
- Check terms of use
- Use and maintain antivirus software

Negative Impact to Social Networking and Communications

- Scammers reduce confidence in doing business online.
- Blackmailers give people a reason to withhold personal information online.
- Sex offenders search social sites for unknowing victims.
- Cyberstalkers utilize social networking sites to stalk their victims.

Negative Impact to Social Networking and Communications

- Phishing attacks are on the rise on social networking sites.
- Web (online) and e-mail scams such as fake auctions, lotteries, and giveaways make it difficult for many people to trust.
- Impersonation of another person is a common threat to users of social networking sites.

Implications for Business

Summary

- Different types of online personal and business communications
- Types of online attacks and the perpetrators who carry them out
- Security and privacy risks related to use of social media and social networking