UNIVERSITY OF MARYLAND
University College

Learning Resource

Privacy

Introduction to Privacy

You might say that your entire life is stored somewhere online—in medical records, tax records, driver's license records, credit reports, and so on. Because so many of the records that contain identifying information about you are stored on computers, it is important that the places where these records are kept are readily accessible but still secure from unauthorized users. You have a role as well in keeping your own information secure. In this module, we will look at what constitutes personally identifiable information (PII) and the steps to ensure it is accessed only by those who have a need to see it.

Consequences of Identity Theft

A Host of Emails

Maya's friends and family started asking her about the barrage of emails she was sending to everyone. The subject lines in the e-mails were blank, and the messages contained only links to unknown websites.

Maya checked her sent messages and found that numerous messages had been sent to her friends and family from her account without her knowledge. She started to think something was wrong. She didn't know what to do.

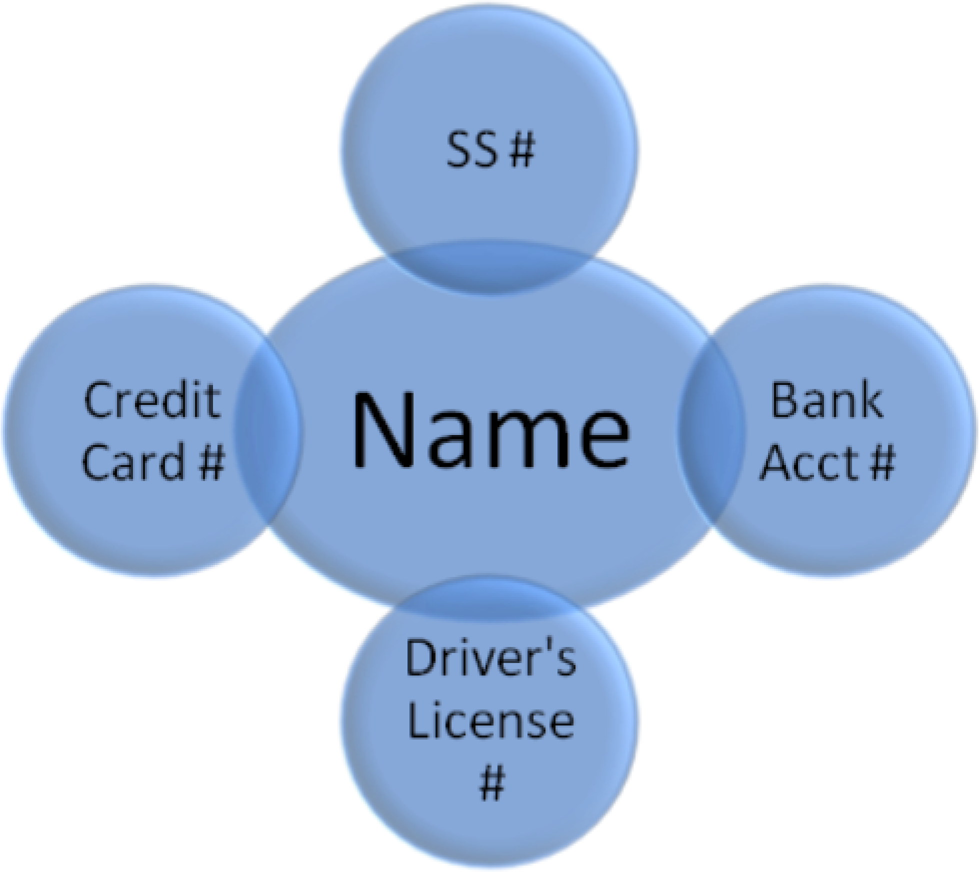
Later that day, Maya was checking Facebook and noticed that a message had been sent to all her friends on Facebook with a link to a video she had never seen before. "What is going on?" she wondered.

Finally, she got a call from her friend Alvin, who told her that he had received one of the suspicious emails, and he recognized it as a malware infection.

Many people find themselves in situations similar to Maya's. This scenario addresses some of the threats and consequences encountered in the online environment. They parallel the threats and consequences of everyday life. We all know there are bad people in the world. We learn at a young age not to take candy from strangers, not to let a stranger in the door, and not to leave valuables unattended. We lock our doors, park in well-lit areas, and avoid seedy neighborhoods at night. We learn how to be safe and avoid the threats in the world. The same goes for the online world.

Personally Identifiable Information

So, what are the threats you might encounter in the online world? Theft, particularly of your personally identifiable information (PII), tops the list of information data thieves are after. PII is any piece of information that can potentially be used to uniquely identify, contact, or locate a particular person. PII includes your full name, or first initial with your last name, linked to your social security, bank account, credit card, or driver's license number. PII is generally kept private and is often used for financial, medical, or research identification.



Personally Identifiable Information (PII)

Source: Janet Zimmer.

With this kind of information, malicious individuals and intruders can commit identity theft. Identity theft occurs when someone uses another person's PII to take on that person's identity in order to commit fraud or other crimes. Imagine the inconvenience of having to close your bank account and open a new one, or trying to convince your credit card company that you are not responsible for certain charges.

Your online user ID and password are at the top of the list of information that malicious people are after. You probably have multiple user IDs and passwords for websites you visit, various online accounts, and your email account. User IDs and passwords can provide access to additional PII or other information you would like to keep confidential. For example, you may have stored personal information in your email account profile, privacy settings, and security settings. If someone gets access to your e-mail ID and password, he or she may gain access to additional PII. Also, users sometimes include their calendars or vacation plans in email or online postings, which can make those users potential targets for home robberies.

Other than trying to access your account and personal information, malicious individuals may also be interested in compromising your computer and other connected resources, such as an iPad, smartphone, or Xbox. What do intruders do when they compromise these resources? They send spam, launch attacks on others, store files, advertise services, capture keystrokes, snoop for additional targets of value, and generally exploit whatever is available or profitable.

Why Would Someone Want to Trick You into Providing PII?

An attacker may be trying to steal your personal information for financial gain. For example, an attacker could use your bank account number, or the username and password for your online banking site, to withdraw money from your account.

Stolen PII can also be used to obtain and create personal documents, such as obtaining a birth certificate to create a driver's license, and then using the documents to get a fake passport. An attacker might steal your social security number to open a credit card in your name. For this and other reasons, it is recommended that you provide only the last four digits of your social security number to verify your identity.

Social Engineering

The "Lost" USB Drive

On the floor of a hallway in her office building, Mary finds a USB drive, also called a USB flash drive. Thinking that it must belong to one of her coworkers, she plugs the USB drive into her computer so that she can look at what is stored on it and attempt to find its owner. Two days later, Mary's computer is suspended from the network due to a malware infection. A malicious person had left the USB drive on the floor, hoping to lure someone into launching the malware that was set up to run automatically when the USB drive was plugged into a computer.

Social engineering is a technique whereby a malicious person uses deception to gain your trust and to trick you into providing information you would not freely give. Social engineering is usually associated with identity theft.

Trying to Help

For instance, if a stranger calls your cell phone to ask for your company ID and password, you would likely refuse to provide the information and hang up. But when the same person calls you and introduces himself as a staff member from the help desk, you might not hesitate to provide any information the caller is asking for, even your personally identifiable information.

Types of Social Engineering

Social engineering by e-mail. You may receive an email explaining that your Yahoo account is about to be disconnected. In order to prevent this from happening, you are prompted to provide personal information such as your user ID, password, and full name. If you respond to this phishing email with the requested information, you will have given a hacker access to your email and to PII located within your account.

Social engineering by phone. Pretending to be someone in a position of authority at a phone company or bank, a hacker calls to persuade the user to provide sensitive information.

Social engineering by dumpster diving. Also known as trashing, a hacker searches for sensitive information such as bank statements, preapproved credit cards, and student loan paperwork in the garbage. To prevent becoming a victim of dumpster diving, it is wise to shred documents with sensitive information.

Online social engineering. Hackers often try to trick users into providing sensitive information via e-mail, instant messaging, chat rooms, social networking sites, and the like. For instance, a hacker will send a fraudulent email claiming to be a banking institution, credit card company, or department store. The hacker requests that the user verify his or her user name, password, and user ID, either by responding to the email or by clicking on a link that directs the user to a legitimate-looking, but fake, website.

Reverse social engineering. A hacker poses as a technical aide to fix a computer problem that he or she actually created, or that doesn't exist at all. The user contacts this aide and is then prompted to give sensitive information to the aide in order to fix the problem. The user provides the required information and the problem seems to be solved.

Social engineering with USB drives. Hackers can also use USB drives to gain access to sensitive information kept on a computer or network. Hackers may infect one or more USB drives with a virus or Trojan horse, that, when run, will provide hackers with access to log-ins, passwords, and information on a user's computer. The hacker may then leave the infected USB unattended on the floor, in or next to a computer in an open lab, in hallways, in restrooms, or in any other area with a relatively high volume of traffic. A user who finds the USB drive may install the device in order to locate its owner, thus allowing the virus or Trojan horse to infect the computer. The hacker is then able to get PII from the infected computer and proceeds to victimize the user of that machine.

Note that social engineering, as illustrated in these examples, does not rely on technical prowess, but rather on tricking other people into deviating from normal security procedures. Being aware of some of the commonly used social engineering schemes should make you more alert and help you avoid becoming a victim.

Phishing

The most common online social engineering method is "phishing," when an attacker goes "fishing" for personal information, such as a user account name and password, a credit card number, a social security number, or some other piece of information that is considered valuable. Typically, an attacker lures victims into providing this information using fraudulent emails or websites as bait.

In this section, you will be introduced to the most common methods of phishing, some key indicators that can help you recognize phishing attempts, and strategies to protect yourself from falling victim to a phishing attack.

In a study conducted at Carnegie Mellon University in 2009, researchers found that across university departments, years of study, and gender, students aged 18 to 25 were consistently more vulnerable to phishing attacks than older participants. A complete presentation of the study results can be found at http://www.cs.cmu.edu/~jasonh/publications/soups2009-school-of-phish-final.pdf

Here is a summary of the study (Blair, Cranor, & Kumaraguru, 2009):

Some Study Findings

- In 2005, it was estimated that 73 million US adults received more than 50 phishing emails each.
- 2007 statistics estimate that 3.6 million adults lost $3.2 billion in phishing attacks.
- Financial institutions, corporations, and military communities are also victims.

Why Phishing Works

- Phishers take advantage of internet users' trust in legitimate organizations.
- Internet users may lack computer and security knowledge.
- Not all internet users use good strategies to protect themselves.

What Are Antiphishing Strategies?

- Find and take down phishing websites.
- Detect and delete phishing emails.
- Warn other users about the threat.
- Use antiphishing toolbars and web browser features.
- Train users not to fall for attacks.

Carnegie Mellon designed a training package and a laboratory experiment to determine if training helped users detect phishing emails.

Things learned from the laboratory experiment (Blair, Cranor, & Kumaraguru, 2009):

- Security notices are ineffective for training users.
- Users with embedded training make better decisions than those sent security notices.
- Participants retained knowledge after seven days.
- Training does not increase false positive errors.
- Before training, traditional-age students (18-22 years of age) are significantly more likely than staff to fall for phishing schemes.

How Would a Cyber Criminal Attempt to Phish Your Personal Information?

Email is one of the most common vehicles for phishing. You may receive an email that looks and feels legitimate—from a friend, an entity with whom you have an account (such as eBay, PayPal, or Citibank), or a business contact. The message might prompt you to verify your account number or your user ID and password, either by immediately replying to the email or by clicking a link that directs you to a fraudulent web page.

Sample Phishing Email

Recently, many Fakebank account holders received an email message from "onlineupdate@state.com" with the subject "Important Security Update." The message, shown below, claimed to be from Fakebank and prompted recipients to validate their "account ownership security" to avoid suspension by clicking on a link to a fake version of Fakebank's web log-in page. Account holders who visited the fake website and provided their user IDs and passwords gave a cyber criminal access to their online financial records.

Subject: Important Security Update
Date: Monday, 5 April 5, 2016
From: Fakebank (onlineupdate@fakebank.com)

Dear Valued User,

Your Account security validation has expired. This may be as a result of wrong or incomplete data entered during the last update.

It's strongly required that you should validate your account ownership security, to avoid service suspension.

Login to Fakebank at www.fakebank.com

We apologize for any inconveniences caused.

Security Department,
Fakebank

Protecting Yourself Against Phishing

Since protecting your PII is important in protecting yourself against identity theft, let's take a deeper look at how you can distinguish legitimate emails from phishing attempts. Keep in mind that most phishing messages have an urgency, warning you to respond immediately.

The email is most likely a phishing attempt if:

- the message is alarmist and warns you to respond immediately to verify account information or take advantage of an offer. Often there's a threat of dire consequences.
- the message does not address you by name or include other identifying information.
- the message includes long links that don't make sense or misspells the company name in a URL.
- the message includes misspellings and grammatical errors.

If you suspect you received a phish, simply delete the email. Do not respond to the email, click on an embedded link, or open the attachment. If you are not sure, verify the legitimacy of the message by contacting the supposed sender through an alternate communication channel. Don't use the contact information provided in the suspicious email; instead, use a phone number you obtain directly from a bank statement, use an existing bookmarked URL to log in to your provider's site, or use an email address that you've successfully used before.

Putting It All Together

Threats on the internet are similar in concept to threats on the highway. You are better protected when you follow traffic regulations and take certain precautions. Good safety measures include keeping your car maintained, fastening your seatbelt, stopping at stop signs and traffic lights, and avoiding potholes. To avoid theft, you keep your valuables locked away, out of sight. You lock your car.

Take the same types of security and safety measures with your computer and on the network. Keep your computer running well by updating your software and backing up your files regularly. Install antivirus software and make sure it updates daily. Avoid opening the door to untrusted sources by not opening their attachments, not clicking on their links, not installing their software, and not providing them with your sensitive data or password. Protect your personal information from theft by locking it behind strong passwords that you do not share with others. Physically lock your computing devices when unattended.

Remember, prevention is the best protection.

Visit the Federal Trade Commission's website at https://www.consumer.ftc.gov/topics/privacy-identity-online-security for resources on deterring, detecting, and defending against identity theft.

Protecting Your Privacy

Considering every possible threat to your information and resources is probably not realistic. Most of us don't have the time or resources to commit to predicting the long-term outcomes of our every action.

Rather than trying to analyze every action, it's helpful to rely on some general rules to protect your PII.

- **Keep your passwords to yourself and change them regularly.** Most cases of PII can be avoided simply by maintaining a strong password and not sharing it.
- **Use different passwords for different accounts.** Remembering multiple passwords can be a challenge, and it's often convenient to use the same password for multiple accounts, from Facebook and your bank account to your UMUC ID and Twitter accounts. The danger is that a compromise of any one of these accounts could also result in the compromise of others, if the same password is used for multiple accounts.
- **Use strong passwords**. Many of your user IDs require strong passwords to gain entry into one or more systems. In those instances when you can choose any password configuration, pick a strong password to protect your information. Changing strong passwords often is the most important thing you can do to keep your PII safe.
- **Check your credit reports annually.** Sometimes people don't learn that they are victims of identity theft until their credit rating and identity are destroyed. It's proactive to get copies of your credit reports from the credit bureaus and review them for errors. Follow up with the credit bureaus to make corrections to your reports if needed. By law, you can get one free credit report from each of the three credit bureaus every year.
- **"Google" yourself.** Enter your name in a search engine and see what data comes up. Investigate postings about yourself in the information that you find. Look for suggestions that your PII may be compromised.
- **Remember that people can be a weak link in security**. No matter how secure you make passwords and how careful you are with technology, there is always a human element to protecting your information.
- **Control physical access to your devices.** It's important not to leave laptops and other mobile devices unattended in public locations, like a coffee shop or other places with free Wi-Fi. An unattended machine is at risk, both for theft and for other security threats. When you aren't controlling physical access to your machine (by locking it in your room), don't let it out of your sight.
- **Remember to log out or lock your computer when you are finished using it.** Whether it's your email, bank account, Target shopping account, or library account, always remember to log out when you leave the website.

- **Remember to lock your computer with a password when you are finished using it.** By requiring a password to access your computer or other electronic device, you are helping to protect your information. You are also making your computer useless to a thief who cannot break password locks.

References

Blair, M. A., Cranor, L. F., & Kumaraguru, P. (2009). Results from "Help us protect the Carnegie Mellon community from identity theft" study. Retrieved from https://www.cmu.edu/iso/aware/presentation/identitytheftstudy_041009.pdf

Kumaraguru, P., Cranshaw, J., Acquisti, A., Cranor, L., Hong, J., Blair, M. A., & Pham, T. (2009). School of phish: A real-world evaluation of anti-phishing training. Retrieved from http://www.cs.cmu.edu/~jasonh/publications/soups2009-school-of-phish-final.pdf

Licenses and Attributions

All links to external sites were verified at the time of publication. UMUC is not responsible for the validity or integrity of information located at external sites.