NAF Principles of Information Technology

Lesson 4

Staying Safe Online

Student Resources

|  |  |
| --- | --- |
| Resource | Description |
| Student Resource 4.1 | Scavenger Hunt: Cybercrime |
| Student Resource 4.2 | K-W-L Chart: Online Privacy and Ethics |
| Student Resource 4.3 | Reading: Maintaining Your Privacy and Acting Ethically Online |
| Student Resource 4.4 | Analysis: Online Profile |
| Student Resource 4.5 | Personal Guidelines: Staying Safe Online |

Student Resource 4.1

Scavenger Hunt: Cybercrime

Student Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Directions: Use the following websites and additional online resources (if necessary) to find the answers to as many of the following questions as possible. Be sure to cite where you found each answer. You have a limited amount of time, so work as quickly as you can. Questions do not have to be answered in order; you may skip around.

* “How Computer Viruses Work.” HowStuffWorks, <http://www.howstuffworks.com/virus.htm>
* Symantec Security Response, Symantec Corporation, <http://www.symantec.com/security_response/index.jsp>
* Computer Crime & Intellectual Property Section, US Department of Justice, <http://www.justice.gov/criminal/cybercrime/index.html>
* OnGuard Online, US Government, <http://www.onguardonline.gov/>

1. How can cybercriminals harm a person whose personal information they have stolen?
2. How do web bugs invade a person’s privacy?
3. What do cyberstalkers do? How do you protect yourself from them?
4. How can you avoid becoming a victim of identity theft?
5. What is phishing? What are some clues you can look for to avoid it?
6. Briefly summarize two examples of cybercrime stories.
7. What’s a bot?
8. Name three actions you should take if you believe you’ve been victimized by crimeware or   
   online fraud.
9. How does pharming work?
10. Name two ways to protect your password.

Student Resource 4.2

K-W-L Chart: Online Privacy and Ethics

Student Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_

Directions: In the first column of the chart, write what you already know about each of the three topics. In the second column, write down anything you would like to know. As you read Student Resource 4.3, Reading: Maintaining Your Privacy and Acting Ethically Online, write the important points that you learn about each topic.

| What I Know | What I Want to Know | What I Learned |
| --- | --- | --- |
| Protecting Your Identity |  |  |
| Protecting Yourself from Cyberstalking |  |  |
| Copyright Infringement and Piracy |  |  |

Student Resource 4.3

Reading: Maintaining Your Privacy and Acting Ethically Online

You’ve heard the stories: Someone goes to buy a car but can’t because someone else has been using that person’s identity to rack up bad credit. Hackers break into a large retailer’s servers and steal millions of credit card numbers. A kid makes what he thinks is a friend on a social media site, only to find out that the friend’s profile is fake—a cover for an adult with nothing but bad intentions.

The beauty of the Internet is that it opens up the world to us; the danger is that it opens up us to the world. From the theft of one’s ideas to the theft of one’s identity, the Internet can be treacherous if you don’t know how to properly protect yourself and others.

Understand the Risks

Information about you and your identity is sent around the web all the time. Some of this is legal and safe, and some of it is neither.

Legal Access to Your Information

**Make a Purchase:** Do you have an iTunes account? An Amazon account? It’s convenient to make a purchase online with a single click, but for that to happen, the company has to store a lot of personal information about you, such as your name, address, phone number, and credit card information. Even when you do not have an account set up, you are sharing this information with a company whenever you buy online.

**Company Information-Sharing:** Have you ever gotten a catalog from a company you’ve never heard of? Many companies will also share your information with other companies, either by trading it or selling it. This is why it is important to read the fine print. Companies are required to tell you what they will do with your information before you give it to them. Also, they are allowed to share your name, telephone number, address, age, and ethnicity, but not information such as your Social Security, bank account, or credit card number.

**Web Bugs:** Have you noticed how ads for something you were looking at online or even writing about in your emails suddenly appear on the side of your screen? That’s thanks to web bugs. Web bugs are used to monitor who looks at a certain web page or email. They can track when a page was viewed and the identity of the computer. Usually web bugs are invisible. Often businesses place them to track how many visitors access their site. Ad networks use web bugs to add information to a profile of what sites a person is visiting. Then they use this information to send ads that are likely to interest the person, based on the type of sites that person visits. Another use for web bugs is to track whether a recipient opened an email. Web bugs are very controversial, but—as of now—the courts have left them alone.

Illegal Access to Your Information

**Spam:** You get an email from a traveler overseas. The traveler says she has lost her wallet and her passport and she just needs you to send some money, and she will pay you back ten times over. Or you get an email from a Nigerian prince who has a large sum of money he needs help managing. If you just send him your bank account number, he will wire the money into your account, and you can help him spend it.

Both of these are examples of spam. These can often sound honest and compelling, but beware of any get-rich-quick schemes that promise to help earn you lots of money in your spare time.

**Phishing:** You receive an email that looks like it is from your bank. There has been a problem with your account, it says, and to fix it, you need to send your account number and personal identification number (PIN). Do you do it? Many people might recognize this as a trick, but the person sending it only needs one or two to respond. They are *phishing*, also called *spoofing*. The idea is that bait is thrown out with the hope that, although most people will ignore it, some will bite. Con artists send millions of emails that seem to come from websites people trust, such as their bank or credit card company. In the emails, phishers ask for personal information. If they get any, the thieves then use it to commit crimes in the victim’s name.

Phishing typically happens in the form of emails or pop-up screens that ask you to validate or update your account records. A thief can use any sensitive information that you type in to transfer money, make payments, and commit other crimes. Never forget that real companies will not ask you for personal information in an email.

**Spyware:**Spyware is software that can be installed on your computer without your knowledge. It monitors Internet usage. Spyware can also instruct your computer to perform actions. For example, it can instruct your web browser to open a web page you did not mean to visit; it can also install software, collect personal data, and send your personal information to someone else.

Identity Theft

Spam, phishing, and spyware are all tools criminals use to steal people’s identities. If a thief gets your Social Security, bank account, and credit card numbers, he or she can open and use credit card accounts in your name, take out fraudulent loans, or commit other crimes. And you wouldn’t know anything about it.

Losing money is only one of the risks of identity theft. Thieves can use your data to get a driver’s license or other ID with their photo but your name and information. They can then use that ID to get jobs and file fake income tax returns, apply for passports and visas, file insurance claims, even give your name and mailing address to police and other authorities if they are arrested.

Protect Yourself Online

It may seem like there are a lot of ways for your identity to be taken or for you to be in danger online, but there are also many kinds of protections in place.

Government Protection

The Federal Trade Commission

The Federal Trade Commission (FTC) is the government agency that regulates the Internet. It is the FTC’s job to teach everyone about the importance of online privacy and to fight online crime and unfairness. The FTC also works to protect children’s privacy when they are online.

Children’s Online Privacy Protection

Did you ever try to open an account when you were 10 or 11, only to find your parents needed to sign off too? That’s because in 1998, Congress passed the Children’s Online Privacy Protection Act (COPPA). This law requires sites to get parental permission before collecting information online from children younger than 13. Anyone who runs a website or online service that allows users younger than 13 must follow COPPA. Users must have a parent’s permission before they give personal information or create an account. Parents can review and delete any information about their children stored on any website.

The FTC takes COPPA very seriously and has even fined companies that ignore it. For example, Xanga was fined $1 million because it let children younger than 13 sign up for its service without getting their parent’s permission first.

Company Protections

Encryption

To protect sensitive user information (such as a credit card number), many commercial websites use encryption. Encryption assures users that their personal information cannot be seen by anyone other than the website being used.

Authentication

How does Netflix know it’s really you logging in to your account? Netflix uses a process called authentication.This identifies a user logging on to a network or confirms the authenticity of a transmitted message.

**Password Protection:** In private and public computer networks (including the Internet), authentication is typically done through the use of passwords. Knowledge of the password is assumed to prove that the user is who he or she claims to be.

The first time you register on a network, you are either assigned a password or asked to choose one yourself. Each time you go to that network, you must remember and use the previously declared password. Passwords are the simplest authentication model to use, and that is why password models are so common. Unfortunately, they are also a weak authentication model because passwords are guessed or stolen relatively easily.

Coming up with a password that’s both strong and easy to remember can take some creativity. You don’t want to create a password that’s so complex that you end up writing it down or reusing it for multiple services. Try using part of a phrase, song, or poem that is easy for you to remember. If you are having problems remembering your password, write down your “system” in a way that only you can understand it. Remember: never write down the password itself!

Once you have chosen a password, avoid using the “Remember This Password” feature on websites. This feature, typically used to access secure applications (such as email, calendar, and financial systems) and web browsers (such as Firefox and Internet Explorer), does not adequately protect passwords. It may be possible for malware or an unauthorized user to obtain this stored information.

**Two-Factor Authentication:** A more secure method than just a password, this type of authentication involves two separate components. For example, you might need your banking or debit card plus a PIN to gain access to your bank account.

**Tokens:** Some computer systems achieve improved security with *authentication tokens*. An authentication token is a device or image used to identify the user. Specialized token-reader hardware or software is sometimes necessary to use a specific token. Authentication tokens include biometric authentication, USB tokens, and smart cards. Some sites will send a unique code to your smartphone via text message, which you then need to enter in the web browser to complete the login.

**Smart Card:** A small plastic card (the size of a credit card) that contains a cryptographic key, a smart card is inserted into a special reader attached to the system. The system reads the key from the smart card and asks for your passphrase to unlock the key. After you enter your passphrase, the system performs a cryptographic key exchange with the central server for verification of the key. Smart cards have the unique ability to store large amounts of data, carry out their own on-card functions (for example, encryption and mutual authentication), and interact in an intelligent manner with a smart card reader.

**Biometric Authentication:** A newer technology, and type of authentication token, this requires people to use some portion of their body for authentication. It could be a fingerprint, a retina scan, iris scan, facial scan, or voice recognition. This form of authentication is currently more expensive than the others, so it is much less common. Its benefits include no passwords to remember and no cards to misplace or have stolen.

Protective Measures You Can Take

Laws and technological tools can be complicated, but there are also simple ways for you to protect yourself:

* Ignore emails and websites that make big promises. Offers that sound too good to be true usually don’t provide anything but a headache and can even prove to be dangerous.
* Never reply to phishing emails or click any links in the messages.
* Get a phishing filter. It can help protect you from web fraud and identity theft by warning you about or blocking you from reported phishing websites.
* Look for encryption.
* Choose a password that is hard to crack but easy for you to remember. A strong password includes:
  + At least eight characters.
  + At least one number.
  + At least one letter.
  + A mixture of lower- and uppercase letters.
  + At least one symbol (such as !, %, #, $, or &).
  + No simple names or words (even foreign words), simple patterns, or famous equations.
* Surf anonymously. The easiest way to make sure websites can’t gather personal information about you and your computer is to use your web browser’s anonymous browsing mode. The names may differ by browser:
  + Firefox: private browsing
  + Chrome and the Android : incognito mode
  + Internet Explore: InPrivate Browsing
  + Safari (on the iPhone and iPad): private browsing mode, plus Safari has a “Fraudulent Website Warning” if Safari believes a site is a phishing site

Protecting Yourself from Cyberstalkers

*Cyberstalking* is a kind of crime committed online by perpetrators who seek to harass victims, sometimes in the form of sexual violence or interpersonal violence. You can take the following steps to prevent cyberstalking:

* Always select a gender-neutral user name for your email address or for chat.
* Share your primary email address *only* with people you know and trust.
* *Don’t* give out personal information (such as your real name, address, or phone number) in your profiles.
* If someone bothers you in a chat room and won’t go away, put them on “block” or “ignore.”
* Do not give your password to anyone, especially if someone sends you an instant message (IM). Your service provider will never ask you for your password.
* Be very careful about putting pictures of yourself online. Some stalkers become obsessed with an image.
* Talk to a parent or an authority you trust about uncomfortable situations.

Protect Ideas

While invasions of your personal information are quite scary, they are not the only danger of an open Internet. As you know, massive amounts of information are stored online, from newspapers to blueprints for product design to research papers to someone’s personal poem on their Facebook page. Being able to see all of this information is wonderful, but it’s important to approach it ethically in order to protect the rights of those who create it.

Copyright Laws

Did you know that the articles in that online newspaper are protected by law? Even that person’s poem is! Copyright laws are a way to protect producers of information. These laws protect the use of original ideas and information. There are two basic rules to remember: 1) you must have someone’s permission before using their work, and 2) you should always give credit where credit is due.

How do copyright laws affect you? Whenever you conduct research, you must follow copyright laws.

The first rule is pretty easy to follow. Oftentimes, just the work being publicly available online counts as giving permission. In some cases—such as when you want to use a long piece of text or a graphic or photo—you might have to ask permission. To do this, contact the owner of the copyrighted materials. This is usually done through the publisher and involves a specific request form.

The second rule is where people often run into trouble. Remember this: **always cite your sources!** Use a citation each time you:

* Quote two or more words
* Paraphrase or summarize facts and ideas
* Use original images
* Use noninterchangeable computer programs such as calculation programs, data analysis programs, geographic information systems (GISs), or three-dimensional information software

Using someone else’s words, ideas, or images without asking permission is called **copyright infringement.** Using someone else’s words, ideas, or images without citation is called **plagiarism.**Copyright infringement is against the law and, of course, school and company policies. School or company plagiarism policies generally include punishments such as being expelled or fired. The person whose copyright was violated may have the option to sue the plagiarist, if the use counts as infringement.

Employee Monitoring

One way that businesses protect their confidential data is with employee monitoring. The American Management Association performed a survey on employee monitoring and found that 75% of the businesses surveyed monitored their employees.

Employee monitoring actually affects your personal information, too. It is legal for companies to monitor employees’ Internet use, read and keep emails, listen to phone calls, and even monitor keystrokes, if the employee is using the company’s resources (in other words, the company’s computer and Internet connection). However, it is smart for a company to have a written policy about this and to tell both customers and employees about any potential monitoring. In addition, businesses might view your social media entries if they are considering hiring you, to see what kind of person you are.

Piracy

You also need to be aware of copyright laws when you download music, video games, software, or movies. While it may be tempting to download your new favorite song from a site that lets you do it for free, there’s a good chance you would be engaging in another form of copyright infringement called piracy**.**Piracy is the downloading, using, selling, or buying of copyright-protected items without permission from the owner. It’s also piracy to copy a music CD, video game, or other software from a friend.

That doesn’t mean every time you download something for free you are breaking the law. Open source software like Linux and OpenOffice is legitimately free. A lot of other legitimately free software is also available from sites such as Download.com and SourceForge, while free movies are available on sites like YouTube. In each of these cases, the owner is giving people permission to download his or her materials. However, if the download is actually for sale and you download it for free without permission from the original owner—even if it is off of a friend’s computer—you are committing piracy.

Some people get involved in piracy by joining peer-to-peer (P2P) networks. These sites allow users to share all sorts of files. Though some file sharing is perfectly legal (if you have created the content of the file you are sharing), many people using P2P sites are sharing items whose copyrights they do not own. In recent years, the government has made moves to shut down these sites and punish people who use them. Sites that facilitate peer-to-peer file sharing, such as Pirate Bay and isoHunt, are being raided, sued, and shut down all the time. The popular BitTorrent system of file sharing leaves its users especially vulnerable because it is very easy to detect everyone who is using BitTorrent to share a file. Individual people who use BitTorrent for piracy have received warning notices, been disconnected from their Internet provider, and in some cases been sued.

What Can Happen When Someone Commits Piracy?

It might not seem like a big deal to you, but piracy can carry heavy penalties. At the least, people committing piracy may have their accounts permanently closed by their Internet service providers. In some cases, the government has gotten involved, charging fines and sending guilty parties to jail.

**Digital Millennium Copyright Act (DMCA):** In 1998, Congress passed a law that makes it a crime to use any technology to help get around copyright restrictions, and makes illegal any technology designed to do that. Copyright holders can sue anyone for using or distributing their material. That means violating the copyright of a software program, movie, song, or book makes you liable to be sued and prosecuted.

When people commit piracy, they often cause trouble for those around them. For example, if you were to download an illegal copy of a song or movie while at school or work, your school or employer could also get in trouble. Schools and businesses must follow the same laws that individuals do. As a result, schools that find students involved in piracy may close the students’ accounts, suspend the students, or even choose to expel them. Businesses may do the same, closing an employee’s account, placing the employee on probation, or firing the employee.

How Can I Avoid Piracy?

The best way to avoid piracy is to stay away from P2P websites. If you can’t afford to buy something, check with your local library to see whether you can borrow a copy, or see whether a friend will loan you a legally obtained copy of a CD or movie you are interested in. Another option is to use the computer of a friend who has the software you are interested in.

What Should I Do If I Suspect Piracy?

The old saying “If it seems too good to be true, it probably is” is true. If you come across a website offering free copies of the latest music, movies, or software, don’t download them! You can report piracy at several websites:

* Music: Contact the RIAA at <http://www.riaa.com/report-piracy/>.
* Movies: Contact the Motion Picture Association of America at <http://www.mpaa.org/contact-us/>.
* Software: Contact the Software and Information Industry Association (SIIA) at <http://www.siia.net/piracy/report/report.asp>.

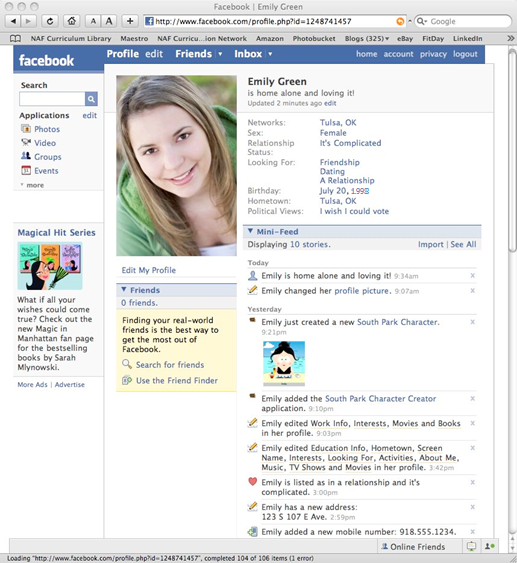
These groups take piracy very seriously, and they want your help. Some, like the SIIA, even offer rewards of up to $1 million to those who report pirates.

Student Resource 4.4

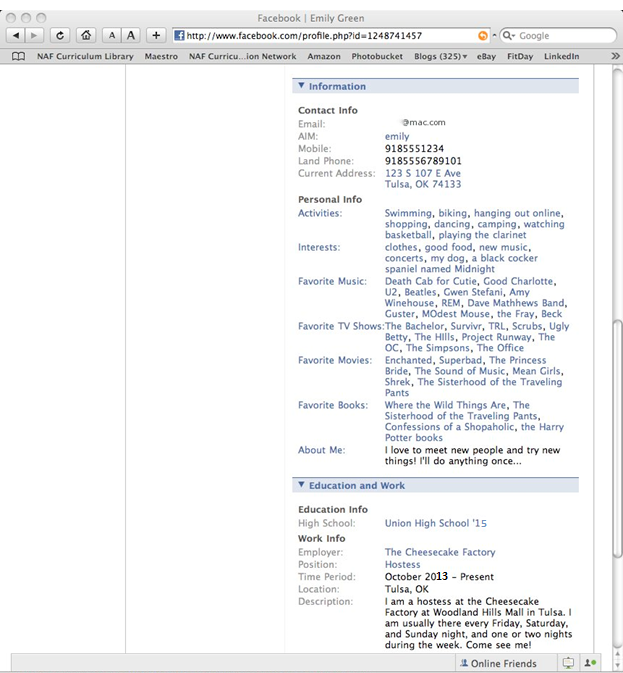
Analysis: Online Profile

Student Name:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Directions: Review the online profile on the following pages. What information is okay for this user to reveal? What should she not have revealed? Circle areas where you think the user made good choices to protect her privacy. Draw boxes around information you think the user should not have revealed about herself. Add any notes or comments you think of as you review these pages: What would you do differently? How could she have told some information about herself in a better way that would have protected her privacy more?



Your notes and comments:



Your notes and comments:

Student Resource 4.5

Personal Guidelines: Staying Safe Online

Directions: This is your chance to create guidelines for yourself for staying safe online. Read through this assignment so that you understand what your assignment should include, and then work through the Planning Your Guidelines section. Focus on the types of Internet media that you use most often. When you are ready to start writing, follow the instructions in the Structuring Your Guidelines section. Before you begin work, look at the rubric that your teacher has given you, and ask your teacher if you have any questions about the quality of good guidelines. Also, read through the example that is part of this resource and use it to help you structure your assignment.

Guiding Question

Your assignment should answer the following question:

* In light of all you have learned in this lesson, what are your personal guidelines for staying safe online?

Online Resources

You may want to consult the following Internet safety guidelines from Microsoft and the US government to help you formulate your ideas for your assignment:

* “11 Tips for Social Networking Safety.” Microsoft, <https://www.microsoft.com/en-us/safety/online-privacy/social-networking.aspx> (accessed May 17, 2016).
* “Net Cetera: Chatting with Kids about Being Online.” <https://www.onguardonline.gov/articles/pdf-0001-netcetera.pdf> (accessed April 19, 2016).

Planning Your Guidelines

1. In the space below, make a list of the important safety concerns you need to keep in mind when using the Internet.
2. For each item on your list, think of an example you could use to explain the safety concern.
3. Circle the three items on your list that you think are most important or that best illustrate Internet safety concerns, and use these as the basis of your guidelines. Then think about the best order in which to present these three points in your assignment. Order the three items you circled first, second, and third.

Structuring Your Guidelines

Use the following instructions to structure your guidelines:

* Write an opening paragraph that states your topic and clearly outlines the main points you want to discuss.
* Write a paragraph about each of the three most important safety concerns that people should keep in mind when using the Internet. Use specific examples and explanations that refer to the material you have learned during this lesson.
* Write a concluding paragraph that summarizes what you have learned about online crime and privacy concerns.

Example Assignment

The topic for this writing assignment is different from your topic, but you can use this as an example of a good way to structure your guidelines and the types of information and examples to include.

Things to Keep in Mind When Drafting a Writing Assignment

It takes time and a lot of thought to create a good writing assignment. Before I begin, I plan what I am going to write. I make sure to think of specific examples for each point I plan to make. While I write, I am careful not to use slang words. I also know that I will have to rewrite the first draft before turning the final version in. Lastly, throughout the writing process, I try to keep important tips in mind to ensure my writing assignment turns out well.

My most important guideline for crafting a well-written assignment is to carefully plan what I will write before I begin writing. This means I create an outline of the points and examples I plan to use. For example, when I wrote about the causes of the Civil War, I wrote each cause down and thought about at least two examples that would go with each cause. Preparing a detailed outline like this helped me stay on topic when I started to write and has helped me get better grades on my writing assignments.

The more I write, the more I learn what to do and what not to do. For example, in one assignment for English, I used too many slang words, like *sweet*, *cool*, *lame*, and *hot*. My teacher told me slang words could make it hard for some readers to understand what I am saying. Another example of what I have learned is that I get a better grade if I write a second draft. In my first drafts, I focus on making my points and giving examples. I then rewrite the assignment on a clean piece of paper. This gives me a chance to make sentences read better. Rewriting the draft also lets me focus on extra-neat handwriting.

I think the three most important tips to keep in mind when working on a writing assignment are (1) make sure you understand the topic, (2) make an outline of what you want to write, and (3) include specific examples. It is easy to write a good assignment on the wrong topic if you do not really understand what the question is. I read the question a couple of times and make sure to talk to the teacher if I am not sure I understand.

In conclusion, I think it is important to give yourself enough time to create a good writing assignment. Before you begin writing, create a detailed outline with specific examples. When you start writing, use clear language and good detail. Finally, plan to rewrite your first draft to correct mistakes and make it easier to read.