NECA Training Curriculum

DIGITAL LITERACY – INTERNET ACCESS

MODULE THREE – Internet Security and Family Safety

SLIDE-1: (cover slide) Internet Security and Family Safety

Class welcome and introductions

SLIDE-2: Recommended Prerequisites

Attendees should complete the first course, *First Steps,* and the first two modules of the *Internet Access* course prior to attending this session. It is recommended that students who did not complete this course material possess at minimum a general understanding and practical experience in computer functionality, Internet usage, and the use of emails.

SLIDE-3: Topic Structure

At the core of this module is family safety. Practicing family safety best practices helps protect a user and their family from potential harm. Best practices are used to:

- Secure sensitive information,
- Protect the computer and its operating systems,
- Assure financial transactions are secure and
- Avoid social dangers.

SLIDE-4 and 5: Agenda

This module begins with foundational concepts related to Internet security.

Strong passwords: Strong passwords provide a line of defense against would-be hackers.

Computer and data protection: Techniques on how to protect computing devices and sensitive information.

Financial protection: Techniques on how to safely conduct financial transactions online.

Social and family safety: Advice on how to protect loved ones while online.

SLIDE-6: (transitional slide) Introduction

This section provides a quick introduction to the topics covered in this module. The main message is while the Internet is very beneficial to the user, precautions must be taken

SLIDE-7: Introduction – Internet Access is rewarding!

This course is not meant to scare people away from the Internet. As a matter of fact, accessing the Internet can be very beneficial.

Here are some examples.

Telehealth offers rural families and medical facilities access to specialty health services and record management.

There are many sites and blogs (online discussion boards) available on a variety of caregiving and parenting topics.

Online gaming and easy access to movies, music, etc. improves entertainment options – without having to leave the sofa.

A growing trend is to have home appliances connected to the Internet to help provide reminders on shopping, maintenance, or even the best time to run the washer and dryer.

Many rural families have friends and family all over the country, sometimes in other countries. Email and access to Internet sites such as Facebook offer a convenient way to communicate and share pictures, videos, and event invitations.

Today, most companies, even retail stores and fast food restaurants, require an online application and resume submission.

With more and more people telecommuting or running businesses from their homes, the Internet is an absolute necessity. Rural families can easily gain access to online education without having to leave their community or the responsibilities at home.

SLIDE-8: Introduction – An educational necessity!

With most school systems facing constant financial pressures, it is essential for educators to implement more efficient learning methods and utilize resources such as digital textbooks and library resources. Parents can also monitor their children's progress by viewing online grade and assignment sites. There are even many colleges and universities offering online programs, allowing rural communities instant access to higher education without having to travel to remote locations.

SLIDE-9: Introduction – Becoming web smart

When visiting an unknown city, a street smart person remembers to lock up personal belongings, keep personal information private, be aware of strangers and take extra precautions. In much the same way, a web smart person should take similar precautions when using the Internet. Methods on how to protect sensitive data and avoid internet crimes will be detailed throughout this course.

To make participants aware of how important it is to become "web smart," class discussion can include the following:

- Refer to the Internet Crime Complaint Center (IC3®) report for more details, available at www.ic3.gov.
    - In 2012, 40% of Internet crimes reported financial loss
    - Common complaints and scams:
        - Auto/real estate/romance fraud
        - Impersonation/intimidation
        - Extortion
        - Copyright/trademark infringement

- After class, distribute the Online Crime Prevention Tips (available via www.ic3.gov, under Site Navigation).
- And/or refer to **c**urrent news stories readily available online. Web search "Internet crime news" or "cybercrime news" or access a related news site such as:
    - www.newser.com/tag/24728/1/Internet-crime.html
    - www.newsnow.co.uk/h/Technology/Internet/Crime

SLIDE-10: Introduction – Danger Zones

As a user explores the WWW and other Internet services, they must be aware of potential danger zones. These danger zones are often associated with interactive applications and websites such as instant messaging, chatting, gaming, emailing, software downloading, social networking and file sharing. While most of the time these applications can be used safely, caution must be exercised to avoid potential occasional dangers.

SLIDE-11: (transition slide) Strong Passwords – The First Step!

The password is the first line of defense.

When a computer is powered on, the user is required to log on. This step prevents someone other than the user from accessing the user's files without their permission. Likewise, many websites utilize passwords to protect user's personal information.

SLIDE-12: Strong Passwords

Passwords provide secure access to online accounts such as those offered by banking institutions. Passwords are also used to protect computing devices. In addition, most devices provide a *lock-out* features that self-engages after a short period of inactivity. Once engaged, the device can only be used after a password is entered.

Passwords also protect the user from attacks, so they must be strong. Those attempting to obtain unauthorized access to a user's accounts (sometimes referred to as hackers) may utilize software to easily crack weak passwords.

SLIDE-13: Strong Passwords – Common password mistakes

Users make several common mistakes when creating passwords. For example, creating passwords based on names, hobbies and simple patterns (for example, Luv2Golf). This is understandable as these passwords are easy to remember. However, often the easier a password is to remember, the easier it is to break.

SLIDE-14: Strong Passwords – Tips for creating strong passwords

This slide discusses best practices for creating strong passwords.

- Avoid using personal information, for example a child's name.

- Use passwords at least eight characters in length.
- Don't use the same password for multiple accounts. This will limit the number of accounts or devices that may be accessed if the hacker obtains an individual password.
- Avoid words that can be easily found in the dictionary. These words are already loaded in password hacking software so would be easy to decipher.
- Develop passwords with random characters such as upper and lower case letters, numbers, and symbols (e.g., $, #, etc.).
- Consider using a password generator. See www.pctools.com/guides/password/ or www.random.org/passwords/

Stronger passwords may be more challenging for a user to remember. The user should consider creating a mnemonic-based password. Examples of mnemonic-based passwords are shown on the next slide.

SLIDE-15: Strong Passwords [class activity]

Review the following mnemonic password example [list the bulleted descriptions on a flip chart or dry erase board]:

Bill and Kathy's 25th wedding anniversary celebrated in Cancun, Mexico.

Bill and Kathy's [BiKa] 25th [25] wedding anniversary celebrated in Cancun, Mexico [CM].

BiKa25CM

Encourage students to develop their own mnemonic password and discuss their choices.

SLIDE-16: Computer and Data Protection [transition slide]

The *First Steps* module discussed the type of information stored on the hard drive of computer and other devices. Protecting online information begins with protecting the computer.

SLIDE-17: Computer and Data Protection - Hide it or lock it away!

When someone goes on vacation and wants to protect their valuables, they lock the front door and hide (or lockup) their valuables. The same approach should be used to secure computing devices when they are not in use.

To protect computing devices and the sensitive data they contain, the user must employ *physical security*. This means securing computing devices such as tablets, laptops and desktop computers when not in use. These devices are costly and can be easily stolen. If stolen, not only is the device stolen, so is the sensitive data contained on those devices. When not at home, keep devices in a safe place. Ideally, the user should store devices in a locked room or a safe.

Users should not leave devices on while visitors, workers or house guests are present. To do so opens the device to unauthorized use.

When not in use, the device should be turned off. While the device is on, it remains connected to the Internet. Turning off the device closes this connection, limiting the opportunity for hackers to compromise information stored on the device. The user should also log off of online accounts and close applications after they are done using them. As discussed earlier, the user should also employ a password-protected screen saver. These security features may be set up to automatically engage after a preselected period of inactivity.

If computing devices are ever borrowed, files should be moved to an external drive, flash drive, or online storage service and removed from the device. If computing devices are given away or sold, all data files should be permanently deleted.

See online article "Six places to store your files online," available at news.cnet.com/8301-13515_3-9736064-26.html

---

SLIDE-18: Computer and Data Protection – Malware

There are many threats to computing devices and the sensitive data they transmit. In this section, several of these threats and best practices to avoid them are discussed.

Malware is malicious software used to corrupt, destroy, or steal data from computers. Following are categories of malware:

- *Viruses* are software that destroy data. They may attack specific data or entire directories.
- *Worms* are software that replicate and infect the computer and any computers that come into contact. Worms most often use the address book of an email program to send copies of the worm to other computers.
- *Spyware* is software that collects data stored or entered into the computer or changes computer settings without permission.
- *Adware* is software used for mass advertising.
- *Trojan horses* are software, often disguised as innocent links, that trick users into executing or downloading software.

SLIDE-19: Computer and Data Protection – Diagram

To protect against malware, the user should utilize *firewall* and malware protection software.

SLIDE-20: Computer and Data Protection – Protection against potential threats

[Transition slide – bullet points animated]

Computing devices should be equipped with three forms of protection.

The first is a firewall. The second is antivirus software. The third is antispyware software.

Each of these forms of protection is reviewed over the next few slides.

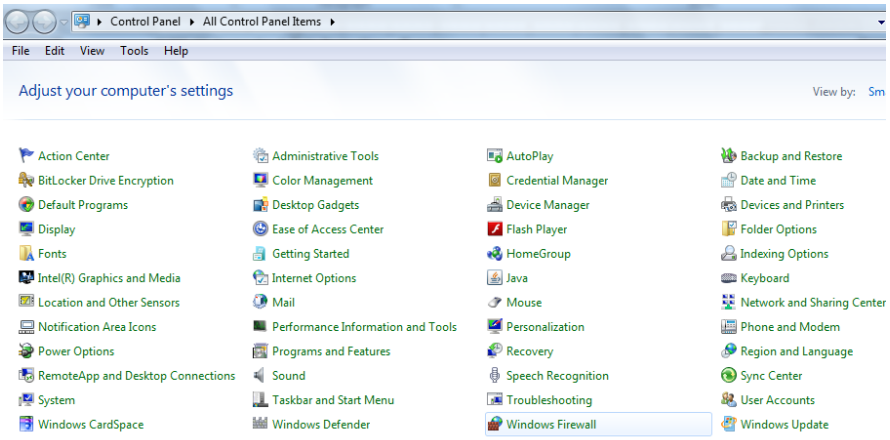
SLIDE-21: Computer and Data Protection – Firewalls

Firewalls are to a computer or computer network as the Transportation Security Administration (TSA) agents at an airport are to airplane travel. TSA agents screen travelers and their belongings to ensure nothing dangerous is brought aboard a plane.

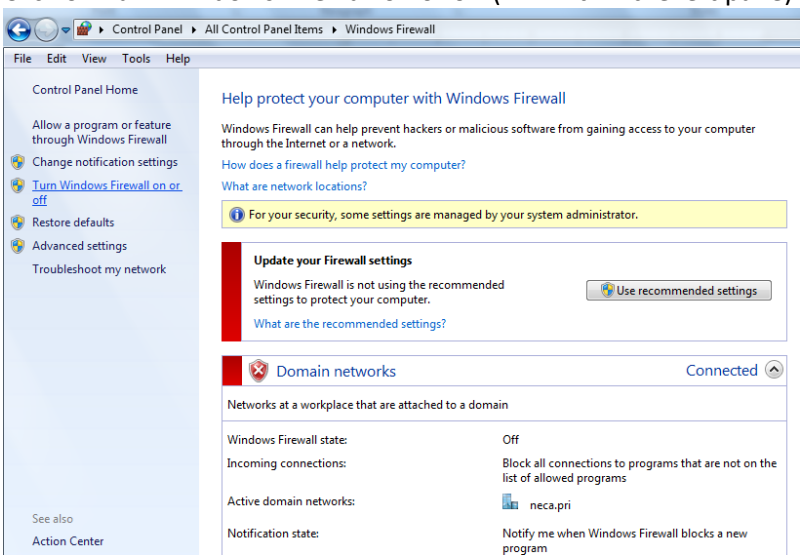
A firewall is designed to help keep a computing device or an entire network secure. The firewall acts like a traffic cop, controlling all incoming and outgoing traffic. While many newer operating systems have built-in firewalls, some users forget to turn on this safety feature.

The Windows operating system has a firewall built in to it. Check the Windows settings under Control Panel to be sure the Firewall is on.

Class demonstration: show how to find Firewall controls. The following instructions are for Windows 7 users:
Click Start – Control Panel – Windows Firewall



Click on Turn Windows Firewall on or off (link within the left pane):



Continue steps to show where to change status (if at work, do not actually change the status without the company's approval).

SLIDE-22: Computer and Data Protection – Antivirus Software

Antivirus protection software helps protect computers against malware such as viruses, worms and Trojan horses. Antivirus software searches for malware on the computer and computer downloads. Once detected, the malware is quarantined and removed. Good antivirus software will automatically update (using the user's Internet connection) to enable the detection of the most recently discovered malware. These updates may occur frequently, sometimes several times a week.

SLIDE-23: Computer and Data Protection – Antispyware Software

Spyware is a type of malware that gathers personal information from the user's computer. For example, it may manipulate and redirect users to advertisements or track websites visited, keystrokes, web searches, etc. As with antivirus software, it is important to ensure antispyware software is frequently updated.

SLIDE-24: Computer and Data Protection – Protection against potential threats

Although some anti-malware features may be built in to a computer's operating system, it is still recommended the user install additional protection. A simple way to obtain required protection is to purchase a package, or software suite, which bundles these three main forms of protection. The packages may also include additional features such as spam filters. Spam filters will be discussed on a later slide.

This slide displays a few examples of bundled protection software packages. It is advisable for consumers to conduct their own research and decide which package best suits their needs and budgeting concerns. The user should compare reviews, features and technical support provided by each vendor.

It should be noted here that some vendors provide similar software free of charge.

Instructor note: If the telephone company's affiliated ISP offers its own Internet security service or software, the instructor may wish to highlight that offering here.

SLIDE-25: Computer and Data Protection – Protection against potential threats

This slide displays a sample security report provided by one vendor (Norton Security). The instructor should draw the student's attention to links for news and tips, as well as a report of threats detected.

SLIDE-26: Computer and Data Protection – Best practices

An easy way the user can assure protection software is up to date is to take advantage of the software provider's auto-update features. The user should also follow prompts by the security provider to update security software. While keeping this software up to date may take some effort, the extra protection afforded the user makes it worthwhile.

It also helps to restart the computer at least on a daily basis as this action may prompt a software update.

The user should frequently copy personal files to a back-up storage device in case malware destroys some of their files or they experience a computer failure. The user can perform this back up manually or purchase a service that performs it automatically.

Instructor note: If the telephone company's affiliated ISP offers data back up or data storage services, the instructor may wish to highlight that offering here.

SLIDE-27: Computer and Data Protection – 3rd line of defense

The 3rd line of defense is careful information sharing. It is essential for families to make a concerted effort to keep information private. Don't give away "the goods"! This includes both information downloaded from the Internet and information sent to other users. For example, do not share sensitive information on a non-secure website.

SLIDE-28: Computer and Data Protection – 4th line of defense

The 4th line of defense is an awareness of "social engineering" attempts. Social engineering is the act of manipulating people into performing actions or sharing sensitive information.

For example, a user may receive an email from an individual pretending to represent the IT department of the user's bank. In the message, the user is told the bank is experiencing a problem and needs the user's help to fix it. The user is instructed to click on a provided link. When clicked, the user is directed to a mock web page with a similar look to the user's bank's actual web page. The web page then prompts the user to type their user ID and password. Once this information provided, the fake website owner is equipped with the information necessary to access the user's real bank account.

Note: for more details on this issue, see:

www.articlesbase.com/security-articles/what-is-social-engineering-examples-of-attacks-1761994.html

Also, www.webroot.com/us/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering

---

SLIDE-29: Computer and Data Protection – More Potential Threats

This slide reviews additional threats that may be encountered on the Internet:

- *Spam* is an unsolicited email. Spam may contain harmless advertisements or harmful malware, scam attempts or offensive content.
- *Clickjacking* is software that once downloaded onto the user's computing device will capture personal information by recording keystrokes and then transmit that information back to a hacker.
- *Scareware* are scams disguised as security warnings. For example, the user may receive a pop-up warning that their device has been infected by a virus, when in fact it has not. It may then prompt the user for credit card information to pay for an antidote to the virus.

- *Phishing* are scams that arrive via email or instant messages. They are often disguised to appear like official communications from a legitimate entity. The user is often instructed to provide personal information.
    - Class discussion opportunity: Visit www.consumerfraudreporting.org/phishing_examples.php and view actual examples of phishing attempts

These threats, and best practices to mitigate them, are discussed in greater detail later in this module.

SLIDE-30: Computer and Data Protection – Web Browsing

When browsing the Internet, the user should exercise extra caution when visiting websites that are not well known to them. While website extensions are not a 100% guarantee that associated websites are safe, the following website extensions might help in deciphering websites:

.com: short for "commercial"; most popular Web extension
.org: short for "organization"; mostly non-profits, but can be used for any type of organization
.gov: short for "government"; usually a federal site, but also can indicate a state site
.edu: short for "educational"; mostly education-related

SLIDE-31: Computer and Data Protection – Web Browsing

Best practices for safely browsing the Web:

- Users should follow their instincts and ignore questionable requests to click on a link.
- The user should not presume that every website that appears on a web search is safe.
- The user should never give out personal information on a website unless the website is trusted and encryption secured. [more details are provided in the next section]

SLIDE-32: Computer and Data Protection – File Sharing

There exist many file sharing websites that allow users easy access to music, movies, etc.
Peer-to-Peer (P2P) file sharing services should be avoided to prevent:

- Viruses and computer attacks
- Unintentional exposure of personal information and financial data

The unauthorized sharing of copyrighted files may be illegal. Users should be aware that such actions could lead to legal problems including law suits, fines or imprisonment.

SLIDE-33: Computer and Data Protection – Email Best Practices

While email facilitates communications, it also may expose the user to certain threats. Details on those threats and best practices to mitigate them are detailed over the next few slides.

SLIDE-34: Computer and Data Protection – Email Best Practices

This slide details best practices for mitigating email threats:

- The user should not share personal information (e.g., social security numbers, account details or their birth date) via email. Companies who maintain a business relationship with the user already have such information and rarely request confirmation via email.
- Don't automatically open all emails. Users should constantly be on the lookout for suspicious messages. When in doubt, the user can run a web search (e.g., Google, Bing, etc.) with contents of the email or the email's sender. Previous reports of suspicious activity might direct the user to a scam alert.
- Report suspicious emails to the Internet Service Provider (ISP) and/or the Internet Crime Complaint Center (IC3) at www.ic3.gov/default.aspx (click on *File a Complaint)*. [demonstration opportunity – pull up website and show how to file complaint]

SLIDE-35: Computer and Data Protection – Email Best Practices

Additional best practices:

Attachments may contain malware. The user should not open an unexpected attachment even if it appears to be from a trusted source. For example, if a friend or family member sends an email only containing a link or attachment (no message), it should not be opened. Instead, the user should contact the originator to determine if they truly sent the email. If not, their email address book may have been compromised and is being use by a hacker.

The user should install anti-malware and anti-spam software on their computer. As discussed earlier, there are a variety of free and fee-based software programs available. The user should keep this software up to date to ensure they are protected against the newest threats.

SLIDE-36: Computer and Data Protection – Email

There are best practices a user can employ to protect their computer from malware such as viruses:

- Assure email filtering is turned on. Many ISPs and email services provide this protection free of charge.
- As mentioned earlier,
    - A firewall is designed to help keep a computing device or an entire network secure
    - It is important to assure malware software is updated on a regular basis
    - Install antivirus software and keep it up to date
    - The user should back up data files frequently

SLIDE-37: Computer and Data Protection – Email Threats

As discussed in an earlier slide, Spam is unsolicited email. Because the cost of sending email is so small, spammers can send thousands or millions of email messages each day. This volume of email can result in information overload and an annoyance for many computer users.

Spammers collect email addresses from a variety of sources including chat rooms, websites, customer lists, newsgroups, and viruses which harvest users' address books. Often, these lists are sold to other spammers. They also use a practice known as email appending (Epending) in which the spammer uses known information about their target (such as a postal address) to search for the target's email address.

According to information compiled by Commtouch Software Ltd., email spam for the first quarter of 2010 can be broken down as follows:

Pharmacy 81%, Replica 5.40%, Enhancers 2.30%, Phishing 2.30%, Degrees 1.30%, Casino 1%, Weight Loss 0.40%, Other 6.30%.

Spam is also a medium for criminals to deceive users into providing personal information. This process is known as *phishing*. Criminals often disguise an email to appear as if it originated from a bank or other legitimate organization. The user is then prompted to click on a link taking them to a fraudulent website where they are prompted to enter personal information. The criminal may use this information to steal money or the user's identity. Targeted phishing, where known information about the recipient is used to create forged emails, is known as *spear-phishing.*

SLIDE-38: Computer and Data Protection – Email

This slide discusses best practices to reduce the quantity of spam reaching the user's email inbox.

- Report the problem to the Internet Service Provider (ISP) by forwarding copies of the spam email or phishing scam with the email headers intact. This may help the ISP determine who originated the email and may lead to improvements in the ISP's spam filtering software. The user should make clear in the subject line the complaint is about spam or phishing.
- Often, the offending email appears to originate from friends or family when in fact it did not. This may occur when a virus takes over their email account or a spammer has stolen their contact directory and modified the sender address. Users should contact their friend or family member via the phone or in person and advise them which account is affected. The user should also advise the victims to change their email password and run a virus scan.
- Turn on the spam filter. Today, most email service providers incorporate spam filters into their service offering. The user may also choose to install a third-party filter. Some filters can be "trained" to recognize email spam. Trainable filters typically eliminate or isolate fewer legitimate emails.
- The user should avoid posting personal email addresses on public message boards or newsgroups. Spammers often run programs that *harvest* email addresses from these sources. Today, many online forums provide safety measures designed to protect user email addresses.
    - The user should exercise caution when following "remove me" instructions contained in unwanted email. While reputable entities may offer this as a means for the user to be removed from their email lists, some spammers may use their *remove me* instructions to validate the user's mail address is *live*, paving the way for even more spam.

SLIDE-39: Computer and Data Protection – Email

Email *spoofing* occurs when a spammer/hacker alters the sent address and email subject line to make the user believe the email originated from a friend, family member or a legitimate business. This practice is commonly used to deceive the user into opening the email message and trusting the content**.**

Phishing is an attempt to acquire personal information such as usernames, passwords, credit card numbers and social security numbers by masquerading as a trustworthy entity. Emails purporting to be from social websites, auction websites, online payment processors or IT administrators are commonly used to lure unsuspecting users. Criminals often gain personal information after directing users to websites designed to appear legitimate. These websites may also be infected with malware.

SLIDE-40: Computer and Data Protection – Email

This slide contains best practices users should employ to protect themselves.

- Look for spelling or grammatical errors. Many phishing attempts originate in foreign countries. The "phisher" my not be fluent in English, hence the errors. Legitimate companies usually ensure their correspondence is error free.
- The user should be suspicious of any email asking them to "verify" information. This is true even if the source appears legitimate. Most legitimate companies do not ask their customers to confirm login information or passwords or to provide sensitive information via email.
- The user should be suspicious of any email informing them they have won money or a contest prize. They should ignore emails from foreigners requesting assistance to move money. As a general rule, if it sounds too good to be true, the user should be suspicious!

SLIDE-41: Financial Protection [transition slide]

Subscribers can benefit from the convenience of online services such as banking, bill paying and shopping. Users must always take steps to protect sensitive information when conducting these transactions.

SLIDE-42: Financial Protection – Best Practices for safe transactions

As mentioned earlier, the user should develop strong passwords for online accounts.

When finished using an online account, the user should log off the website.

The user should not provide sensitive information when responding to emails. Instead, the user should provide this information over the phone or in person. If provided over the phone, the customer should call the institution, not the other way around.

Where possible, the user should use a trusted third party to transact online payments. PayPal is a well know provider of this service. The user should avoid the use of debit cards when conducting online transactions. Debit cards provide direct access to the user's bank account and typically provide little, if any, fraud coverage. Instead use prepaid cards or credit cards that have both spending limits and robust fraud protection.

SLIDE-43: Financial Protection – Best Practices for Safe Transactions

The user should conduct online transactions using only a trusted, non-public computer (home or office) with a wired LAN connection or secure WiFi connection. Public computers (e.g., hotels), mobile devices and unsecure WiFi connections should not be used as they may expose the transaction to hackers.

As mentioned earlier, keep antivirus and firewall programs up to date and always make sure the firewall is turned on before performing online financial transactions.

SLIDE-44: Financial Protection – Best Practices for Safe Transactions

There are easy-to-spot indicators that a website is secure (encrypted). First, the website address will include the "https" prefix. The "S" identifies the site as secure. The user may also see a gold padlock symbol near the top of the computer screen.

SLIDE-45: Financial Protection – SSL Certificates

Note: slides 45-47 may be too technical for some audiences. If so, please take liberty to skip these slides.

In addition to using firewall and Internet protection software, always run the most updated version of the Internet browser. Most browsers will alert users if an Internet site's Secure Sockets Layer (SSL) Certificate is out of date. A Secure Socket Layer is an encryption protocol to provide security for transactions over the internet.

Users can even check the site's SSL Certificate to confirm if a site is secure by accessing the properties window.

SLIDE-46: Financial Protection – Sample SSL Certificates

This slide displays an example of an Internet Explorer properties window (on the left); click on the Certificates button. The Certificate window on the right shows current certificate information if one exists. Users should check to/from dates.

SLIDE-47: Financial Protection – SSL Certificates [class activity]

The instructor may wish to direct students to various websites so that they may search for the SSL Certificate.

SLIDE-48: Financial Protection – Best Practices for Safe Online Shopping

This slide discusses best practices for conducting safer online purchases:

- Assure the seller is legitimate. Check for a physical address, phone number, reputation, reviews, etc. Is this a well-known company like Toys-R-Us or Wal-Mart?
- Sometimes deals sound too good to be true until people take the time to read the fine print. The user should take the time to read and understand the terms and conditions of the service, delivery, refund policy, warranties, etc. While some sellers offer a better price, their terms and

conditions may prove they are not the best deal. The user should print the terms and conditions and the transaction receipt.

- The user should double check their credit card statement to ensure the statement accurately reflects the online transaction. If there is a mismatch, the user should contact their credit card company and report fraud and cancel the card.

SLIDE-49: Social Safety

An important aspect of Internet use is the incorporation of best practices to protect one's family from undesired online activity. These concerns include child predators, cyber-bullying and unwanted/ undesirable content. The following slides are used to promote a safe Internet experience.

SLIDE-50: Social Safety – Protecting your family

While the Internet provides users access to vast amounts of information, the ability to exchange ideas and thoughts and the opportunity to reconnect with old friends, it can also provide a conduit by which unscrupulous persons can pursue underage children or bully another person.

The draws of the Internet may also lead to its overuse, a condition commonly referred to as *Internet addiction*. Internet addiction is a growing problem and should be addressed promptly.

Parents should take proactive steps to protect their children from online predators. They should monitor their children's Internet use and block undesirable websites from their view.

SLIDE-51: Social Safety – Online Predators

Parents should talk to their children about sexual predators and other potential online dangers. They should also use family safety settings that are built into search engines.

Parents should assure their children follow the age limits of social networking websites. Most social networking sites require that users be age 13 and over. If a child is under the recommended age for these sites, prohibit their use.

Chat rooms should be avoided as the potential dangers are too great. As children get older, direct them towards well-monitored kids' chat rooms. Encourage teens to use monitored chat rooms. If a child is allowed to take part in chat rooms, discuss with them which ones they visit and with whom they chat. Monitor the chat website to observe a sample of the exchanges taking place. If undesirable, prohibit the use of that chat room.

Many chat rooms offer private areas where users can have one-on-one chats with other users. Chats exchanged in the private areas can't be monitored. Instruct children not to leave the chat room's public area.

Locate the computer in a common area of the house, never in a child's bedroom. It is much more difficult for a predator to establish a relationship with a child if the computer screen is visible by an adult. If possible sit with the child when they are online.

When children are young, they should share the family's email address. This allows the parent to monitor their children's email exchanges.

Instruct children not to respond to instant messaging or emails from strangers. If a child uses a computer in locations outside of their parents' supervision (i.e., a public library, school, or friends' homes) the parent should find out what computer safeguards are in place at those locations.

If all precautions fail and a child is exposed to an online predator, don't blame the child. The offender always bears full responsibility. Take decisive action to stop the child from any further contact with this person and notify authorities as appropriate.

SLIDE-52: Social Safety – Online Predators

Following are best practices for handling online predators.

Users should choose a gender-neutral screen name that doesn't contain sexually suggestive words or reveal personal information.

Users should not reveal personal information (including age and gender) or information about their family. They should also be instructed not to fill out online personal profiles.

Users should stop any email communication, instant messaging conversations, or chats if another user asks questions that are personal or sexually suggestive.

If a child receives sexually explicit photos from an online user, or if they are solicited sexually via email or instant messaging, the parent should contact local police immediately. They are trained to handle these situations. Save any documentation including email addresses, website addresses, and chat logs to share with the police.

SLIDE-53: Social Safety – Cyber-Bullying

Examples of cyber-bullying include mean text messages or emails, false rumors sent by email or posted on social networking sites, and embarrassing pictures, videos, websites, or fake profiles. Cyber-bullying may be based on prejudices related to sexual orientation, age, religion or other personal characteristic. The effects of cyber-bullying may range from being upset to depression and in the worst cases, suicide.

Many state education departments and school districts have rules governing the use of electronics at school. These rules often contain guidelines pertaining to cyber-bullying. They advise school administrators how to respond to cyber-bullying. However, these only apply to activities that occur on school premises. They do not apply to bullying that occurs off school property. Unfortunately, there are few laws regarding cyber-harassment. Only recently have some states begun enacting laws addressing cyber-harassment.

See *Important Questions Answered about Cyber Bullying* available at: cyber.laws.com/cyber-bullying

The instructor should consider distributing a copy of the Victims of Cybercrime Tip Sheet; available at: staysafeonline.org/stay-safe-online/for-parents/cyberbullying-and-harassment.

SLIDE-54: Social Safety – Cyber-Bullying

This slide discusses best practices to employ in the event a child becomes the target of cyber-bullying.

- Don't respond: If possible, the child should ignore the bullying. Sometimes bullies are encouraged by a victim's reaction to their comments.
- Block: The National Crime Prevention Council advises victims to stop all communication with the bully when possible. Block their phone number to stop their calls or texts. If that's not possible, consider changing phone numbers. Facebook and instant message providers allow users to block other users. If it's not possible to block a cyber-bully, screen the child's calls and leave the bully's messages unopened.
- Keep a record: When bullying does occur, paper copies and an electronic record of related communications should be maintained. This may make it easier to verify that cyber-bullying occurred and help determine who the bully is. If there is a hint of violence or threats of any kind, it's essential a law enforcement official is called immediately. The more information gathered by the parent, the faster law enforcement officials can act. The threat will be treated as a credible threat until proven otherwise.
- Report: Children should be instructed to seek help from a parent, teacher, school administrator or counselor when they become the victim of cyber-bullying. It may also be helpful for a student to talk to friends or a counselor to get their support when a student is feeling upset by hurtful comments.
    - If a child is being bullied, the bully may be violating the website's terms of use. The parent should report bullying to the website administrator and request the violator be blocked from the site. Some social networking sites provide *safety centers* to report bullying.
    - The parents should also contact their Internet service provider, cell phone service provider, or content provider to make them aware of the problem. Most Internet Service Providers have guidelines to assist law enforcement agencies in the event of online threats and harassment. In some cases, these providers can investigate the incident to uncover an anonymous bully. The provider may also be able to remove offensive posts.

SLIDE-55: Social Safety – Cyber-Bullying

In addition to the site on this slide, the user can type "cyber bullying" and their state name into a search engine to view local resources that may provide assistance.

SLIDE-56: Social Safety – Social Networking

For many, social networks have become the preferred method of communicating with friends and family. For example, in the past when a family went on vacation, they would send post cards showing pictures of places visited. Today, through the use of social networks, families post near real-time photos of themselves at their current location and the activities in which they are engaged.

SLIDE-57: Social Safety – Social Networking

As the popularity of social network sites grows, so does the risk of using them. Hackers, spammers, virus writers, identity thieves, and other criminals may visit these sites looking for their next victim.

Assume that everything posted on a social networking site is permanent. Even if an account is deleted, anyone on the Internet can easily print photos or text or save images and videos to a computer. The user should not post anything they would mind being viewed by anyone, including current and future employers.

Many social networking sites promote third-party applications called add-ons. Criminals occasionally use these applications to steal personal information. When downloading third-party applications, the user should take the same safety precautions used when downloading files and programs.

SLIDE-58: Social Safety – Social Networking

The saying relates to treating others the way one would like to be treated. Never be the unintended initiator of online negativity (arguments, bullying, etc.).

SLIDE-59: Social Safety – Social Networking

As in any form of communication, proper etiquette is required when communicating on social network websites.

As stated earlier, everything posted to the Internet is permanent. Hateful and mean-spirited postings should be avoided. This language could be misinterpreted as bullying.

Spelling, grammar and even language has its place on the Internet. Some Internet applications limit the number of key strokes and thus abbreviations are often used. Three very popular abbreviations are BFF (best friends forever), LOL (laugh out loud) and OMG (oh my God). There are other abbreviations used by some that are less tasteful. Most social networks attract a specific target audience and the users dictate what is appropriate and what is not.

The use of ALL CAPS denotes shouting and should be avoided unless that kind of emphasis is desired.

To assist the user, emoticons are often available to more accurately portray the user's intent or feelings, in absence of body language and facial expression.

SLIDE-60: Social Safety – Internet Addiction

Internet addiction is a growing problem for some Internet users. Internet addiction is the compulsive use of the Internet for a variety of purposes including online gambling, shopping, dating and social networking. The Stanford University's School of Medicine estimates that nearly one in eight Americans suffer from at least one sign of addictive Internet use. Internet addiction should be identified and treated seriously.

SLIDE-61: Social Safety – Internet Addiction

This slide discusses common warning signs of Internet addiction.

- Losing track of time online
- Trouble completing non Internet-related tasks.
- Isolation from friends and family
- Defensive about Internet use

Other signs:

- Neglecting friends and family
- Avoiding sleep to stay online
- Being dishonest with others regarding Internet use
- Feeling guilty, ashamed, anxious, or depressed as a result of online behavior
- Physical changes such as unexplained weight gain or loss, backaches, headaches or carpal tunnel syndrome
- Withdrawing from normal day-to-day activities

SLIDE-62: Social Safety – Internet Addiction

Like other addictions, both the user and their friends/families are affected. The user may feel moments of anxiety, depression, or increased stress levels when they are not using the Internet. They may spend more time in seclusion, spend less time with family and friends, and may suffer from a lack of social skills. The user may argue with family regarding the amount of time they spend online. Addicts may attempt to conceal the amount of time spent online, generating distrust and destabilizing relationships.

SLIDE-63: Social Safety – Internet Addiction

Combating Internet addiction can be very tough and stressful, not only on the Internet addict, but on those individuals trying to help the addict. Unfortunately, there is no one-size-fits-all approach to helping someone through their Internet addiction. Here are a few ideas:

- The addict should list out and pursue missed activities.
- The addict or family member should set reasonable time limits for Internet use.
- The addict should seek support from friends and family members.
- The addict should attend live events instead of virtual online events.
- The addict should treat the Internet as a tool or resource and not a way of life; to be used for job searches, school research, etc.

SLIDE-64: Social Safety – Internet Addiction

Class Time: Review the following two news stories for discussion on Internet addiction:

www.webmd.com/mental-health/news/20130226/internet-addiction-hard-kick-drugs

www.newser.com/tag/21000/1/internet-addiction.html

SLIDE-65: (transition slide) Family Safety

One of a parent's most important responsibilities is keeping their children safe from harm. This section provides the student with best practices to keep their family members safe from potential harms associated with Internet use.

SLIDE-66: Bad things can happen in the digital world

The adult should explain to their children that bad things can happen in the digital world just as they do in the physical (real) world.

SLIDE-67: Family Safety – Minimizing Risks

As previously discussed, there are many potential dangers associated with Internet use. This is particularly true for children and teens. This slide reviews several best practices that improve a parent's ability to monitor their children's online activity.

The user should locate the family computer in a location where its use can easily be monitored, for example the kitchen or living room. Ensure the computer has antivirus software installed and is kept up to date. Keeping antivirus software current will help prevent new viruses or virus-like software from infecting the computer. The parent should assure their child uses only child friendly search engines and parental controls are turned on. The parent should consider using these controls to set time limits and block inappropriate websites.

Visit: www.fbi.gov/stats-services/publications/parent-guide/parent-guide and download the PDF copy for a complete list of details. Possibly distribute in class.

SLIDE-68: Family Safety – Agree to Agree

The parent should set standards for the family's Internet use. The parent should teach their children to keep their personal information private. For example, they should not give out their name, address, age or birthday to anyone. The parent should teach their children to safely use social networking websites and then closely monitor their activities. The parent should teach their children about the potential harms of Internet use and the consequences of their actions. The parent should instruct their child to ask them questions and to bring to their attention any online activity that is suspicious or concerning.

SLIDE-69: Family Safety – Agree to Agree

Class Time: Watch the video via the website link on the training slide; access from the listed website is available free of charge.

SLIDE-70: Family Safety – Family Internet Safety Contract

The parent should consider having each family member read and sign a written agreement containing Internet use guidelines. This may be created together as a family or created using a sample contract available from the Family Online Safety Institute or other reputable organization. Signed agreements should be posted near the computer so it is always in sight.

SLIDE-71: Family Safety – Family Internet Safety Contract

Classroom Practice: The instructor should review with the class the website listed on the training slide from the Family Online Safety Institute. Next review the sample Family Internet Safety Contract. Consider printing the sample contract and distributing it to the class for discussion.

SLIDE-72: Summary transition slide to closing

SLIDE-73: Summary

[Animated slide. Each bullet appears one at a time based on mouse click]

Slide summarizes Internet Security and Family Safety best practices.

SLIDE-74-77: Handouts / Guides

SLIDE 75: summarizes online resources

SLIDE 76-77: summarizes key steps reviewed in the course; both slides could be printed for distribution to provide a brief summary guide that can be posted by the participant's computer.

SLIDE-78: Recommended Next Modules

Additional Resources for Instructor:

-Annual Symantec Internet Security Threat Report Reveals 81 Percent Increase in Malicious Attacks available at: www.symantec.com/about/news/release/article.jsp?prid=20120429_01

-Cyber Attack Update (2013 Cost of Data Breach Study: United States, by Ponemon Institute)

Available at ilccyberreport.wordpress.com/2013/07/20/cyber-security-cost-of-data-breaches-pci-court-challenge-role-of-cyber-insurance-and-cyber-attack-update

-Family Online Safety Institute website: www.fosi.org/resources/internet-safety-resources-for-parents

-Goodwill Community Foundation Available at: www.gcflearnfree.org/internetsafety

-Internet Crime Complaint Center (IC3®): www.ic3.gov

-Internet Security Suites Software Review Article available at: internet-security-suitereview.toptenreviews.com

-Microsoft Safety & Security Center, Six tips to help you stay safer online Available at: www.microsoft.com/security/family-safety/default.aspx#Overview

-Password Protection: How to Create Strong Passwords Article available at: www.pcmag.com/article2/0,2817,2368484,00.asp

-The Best Antivirus for 2013 Article available at: www.pcmag.com/article2/0,2817,2372364,00.asp

U.S. Department of Health & Human Services, stopbullying.gov Available at: www.stopbullying.gov/cyberbullying/