These materials were created collaboratively by the New Mexico Department of Information Technology, Fast Forward New Mexico, and the New Mexico State Library, under grants provided by the National Telecommunications and Information Administration. These materials are not to be used for profit.
Table of Contents

SECURITY AND SAFETY IN THE DIGITAL AGE  MODULE 1: .................................................. 2
  Summary, challenges, and instructional strategies.................................................. 2
  Presentation and Text............................................................................................... 3
  Demonstration Instructional Video .......................................................................... 16
  Handout ................................................................................................................... 17
  Assessment ................................................................................................................. 18

SECURITY AND SAFETY IN THE DIGITAL AGE  MODULE 2: ............................................. 19
  Summary, challenges, and instructional strategies.................................................. 19
  Presentation and Text............................................................................................... 20
  Demonstration instructional Video ......................................................................... 32
  Handout ................................................................................................................... 33
  Assessment ................................................................................................................. 34

SECURITY AND SAFETY IN THE DIGITAL AGE  MODULE 3: ............................................. 35
  Summary, challenges, and instructional strategies.................................................. 35
  Presentation and Text............................................................................................... 36
  Demonstration Instructional Video ......................................................................... 44
  Handout ................................................................................................................... 45
  Assessment ................................................................................................................. 46

RESOURCES FOR SECURITY AND SAFETY IN THE DIGITAL AGE .................................. 47
  Websites and Online Training .................................................................................. 47
  Instructional Strategies for Security and Safety in the Digital Age............................. 48
SECURITY AND SAFETY IN THE DIGITAL AGE   MODULE 1:
General expectations and guidelines

Summary, challenges, and instructional strategies

This module introduces the changes that have occurred with the introduction of cell phones and digital devices into all of our lives. It engages these issues as points to explore and consider and not from a judgmental or biased point of view. The goal is to help students recognize the depth of the impact made by the diffusion of technology into our lives and to provide some strategies for dealing with the changes and disjunctions that this change may have effected. It’s important to keep the tone solution and practically oriented, and neither create nor contribute to polarization between different points of view on these matters.

The class also provides some very general guidelines for security and safety in the digital age. While these topics will be repeated or discussed in more depth in later modules, they are provided here as an introductory framework.

This is a topic about which many have fears and concerns. Provide a sense of practical caution and the importance of following a few simple rules.
In this module, we will explore the Internet and learn basic features, terms, and key concepts.
Online interactions
The Internet has changed our lives in many ways. One of the most significant changes it has made is to our interactions with each other.

When we think of the changes that the internet has brought to our lives, we usually think of the dramatic increases in access to information, or the fact that we can communicate with people thousands of miles away in an instant. We don’t often tend to think of how the Internet has impacted our daily interactions with people. Yet more and more, we are discovering that the ways in which we used to engage with other, in personal, direct, face to face exchanges, are lessening. Instead, our interactions now often occur through technology – when we speak to each other, collaborate on work, or even take a class, our interactions with each other are mediated by computers.

What’s changed?
How do computers, cell phones, and other digital technology impact our interactions?

Some might wonder what has really changed, or if interactions are that different. After all, we are still human, we still live and work in the same environments. We still eat dinner, try to exercise, value our families, and enjoy the company of friends. Are these things any different just because we live in the digital age?
What's changed?
We behave and interact differently as a result of new
digital technologies.

The quick answer is yes. The
technologies of computers and mobile
phones have dramatically changed the
way in which we behave and interact
with each other. One of the most
striking consequences of this is that we
now favor digital communications over
those with people who are physically
present.

What was once considered rude behavior is
now considered acceptable.

Even when we are in the presence of
only one other person, our interaction
may focus on someone who is not
present rather than on the person who
is with us physically.
This behavior overturns our previous
code of conduct that told us ignoring
someone was an insult to that person
and did not reflect good or mature
behavior.

What do we lose if our interactions occur
through digital rather than live modes?

We lose the visual impression that our
bodies communicate – our body
language, and all the messages it
delivers.
We lose the facial expressions, and the
information that these convey.
What else do we lose if our interactions occur through digital rather than live modes?

We lose all the visual, tactile, aural, and experiential information that these senses provide about our environment and the people with whom we interact.

Everything looks the same in a text or email message,

Quack. Quack quack.
Quack.
Quackquackquackquack

but actual circumstances may be quite different from what we imagined.
What can you do?
Follow some basic guidelines: Interact

Make a point of interacting with people whose company you share, even if that interaction is only temporary. Ignoring people completely is rude.

We may not have a completely successful resolution to the consequences that have resulted from these changes. It would also be unrealistic to think we could reverse the growth of digital tools in our interactions and communications.

So what can we do?
Following some simple guidelines can help.
First, make sure that you don’t ignore people completely, especially if you are with them, know them, or they make overtures to communicate with you. If you return to your cell phone or computer after a few minutes of conversation with others, it is much less offensive than if you never engage at all.

Turn off media devices in all places and circumstances in which they would be disruptive. You will be expected to have these devices off during class and work hours. You should not use cell phones in libraries, museums, theatres, or at any professional appointments. Nothing is more embarrassing than having a phone go off in the middle of a class or a performance, so make sure these are turned off before you go in.
Follow some basic guidelines: Turn it off

Turn off all cell phones and electronic devices before entering a small business or engaging in transactions.

You should not be on the phone while you are in line, shopping, checking out, completing a transaction, or performing any business activities. These activities require attention and the people assisting you with them deserve your respect. Many small businesses now have signs requesting this.

Follow some basic guidelines: Accept differences

Remember that not everyone has the same expectations around cell phone and computer use.

While consideration needs to guide our basic terms of behavior, we also need to understand that there are enormous differences, especially generationally, about behavior and use of digital equipment. Those under forty have been raised in a world dominated by computer and cell phone interactions, and take them more for granted than do people of previous generations. Be aware of these differences in your audience or in the people around you, and try to make some accommodations. Younger people may blend digital and face to face interactions more comfortably than those over 40. Those over 40 are more likely to see digital interactions as interruptions that interfere with communication. Try to adapt your behavior to your social context, being aware that not all people will have the same set of expectations.
But computers and cell phones do not only impact the way in which we interact in person. They create an entirely new realm of interactions that occur mostly or solely through digital modalities. These include interactions via email, text messaging, instant messaging (IM-ing), and those that occur through social media sites, such as Facebook or MySpace. These interactions may supplement face to face encounters with people we already know and see regularly.

But other communications may come from someone we do not know. We often receive unsolicited emails inviting us to join organizations, participate in shopping deals, or download free software that we might need.

Sometimes these offers seem too good to be true! We are told that we will inherit a fortune, win a free computer, or are the lucky grand prize winner. All we need to do in order to claim our prize is “click here.” When unsolicited offers like this appear, you should ignore them. If it seems too good to be true, it is! These are scams, designed to get you to buy something you do not want or need, or to infect your computer with malware. Never join or participate in unsolicited requests.
Never click on a link in an email from someone you do not know.
Never open an attachment sent by someone you do not know.

Other emails may tell you that your email, business, or banking security has been compromised. They can sound very official and are intended to be alarming. They will generally ask you for your password, your bank account number, or your social security number, or some other piece of security information. These are also scams, intended to trick you. Never give out this information, regardless of who the sender claims to be.

If you have genuine concerns, call your bank, credit card company, or place of work. If something really is wrong with your account or security codes, you should handle it by phone anyway, not by email.
Our greatest concern is often about social media interactions with those we do not know.

Perhaps our greatest concerns are focused around social media interactions with people we do not know.

Because social media is, by definition, social, we interact with groups of people rather than just with one other person. This makes interactions more open and fluid, but also more challenging to manage.

And because social media sites can link you to people who you don’t know personally, but may be a friend of a friend, it’s more difficult to know anything about the person with whom you’re interacting.

Online and offline, not everyone is trustworthy.

And just as in the offline world, in the online world, not all people are individuals we should trust and befriend.
But why are social media interactions different than those offline? At a real party, we might meet strangers as well. But we can watch them, see who else they interact with, ask our friends about them, and read the other signals they are giving out – body language, facial expression, and demeanor. We can also verify their age, appearance, and their behavior.

In online and social media interactions, we can’t observe someone we just met in real life. All we can observe is what the person shows us online. This could give us a positive and reassuring view of the individual, but we can’t be certain that it is a true view. Since, in online and social media environments, people manage all the information that appears about them, they are free to present themselves however they like. They may present themselves honestly, but they may also present themselves falsely, using pictures, descriptions, and even language that is not really their own. You could be interacting with an image of a person that is different from the reality.
As we know from recent news stories, this can be damaging and even dangerous, especially for young people.

Instructor:
You will probably want to discuss some of the recent stories surrounding abuse of social media identities and the damage it has caused young people. Bullying is an important topic to engage.

It’s important to paint a balanced view, emphasizing that social media can provide the networking and support that young people need and that may be difficult to find face to face, especially in more remote locations. It’s also important to keep these dangers in perspective relative to other things young people do, such as driving. In general, younger students will tend to be overly positive and naive about these interactions, but older student may be overly negative, fearful, and alarmist.

What can you do? The first thing you can do is to use common sense in your online interactions, just as you would in face to face interactions. Set boundaries and talk with friends or family if any interactions feel strange or inappropriate.
Follow some basic guidelines: be respectful to others.

One of the best policies is to be respectful yourself. This announces your style and your boundaries, and makes it easier for other people to respect you in turn.

Follow some basic guidelines: don’t escalate interactions with people you haven’t met.

If you haven’t met someone in person, it’s wise not to get too involved with them in an online format, either through social media, email, or texting. If you are meeting someone in person for the first time, do so in a public space and with other friends present.

Follow some basic guidelines: if it feels wrong, disengage.

Trust your instincts if they are telling you that something doesn’t feel quite right. You can disengage from online interactions. You can block emails from any sender and prevent people from accessing your Facebook page.
We wouldn’t discuss personal and private matters face to face someone we didn’t know. We shouldn’t do this in online venues either.

Don’t discuss sex with strangers in any context, online or face to face. It sends the wrong signal and opens the door to problems. Young people need to be especially careful about this.

Review what we learned

General guidelines for interactions
Expectations and behaviors around technology
Dealing with email, texting, & social media
We appreciate the time you spent with us.
We hope to see you at the next training!

These materials were created collaboratively by the
New Mexico Department of Information Technology, Fast Forward New Mexico,
and the New Mexico State Library, under grants provided by the
National Telecommunications and Information Administration.
These materials are not to be used for profit.

Connecting you to a world of opportunities

Demonstration Instructional Video
Basic guidelines for using of technical devices, email, and social media

DO interact with people whose company you are sharing.

DO limit cell phone use in public settings.

DON'T leave your cell phone or electronic devices on at work, school, appointments, libraries, museums, banks, and theatres.

DON'T leave your cell phone or electronic devices on while in a place of business or engaging in a business transaction.

DO be tolerant if others have different use parameters than you. Ask politely for adjustments, if necessary.

DON'T give out personal, financial, or password information over email.

DON'T respond to email messages from unknown senders; DON'T open attachments or click links in such email.

DON'T accept unsolicited offers received via email or cell phone text.

DO use respect, common sense, and control settings when using social media.

DON'T engage with any interaction that feels inappropriate.

DON'T discuss personal information or sexual matters with strangers or new acquaintances.

DON'T tolerate bullying.

DON'T meet someone whom you met online in person for the first time in a private or unknown location. Choose public settings with other people present and bring a friend along.
Assessment

SECURITY AND SAFETY IN THE DIGITAL AGE
MODULE 1 – ASSESSMENT

1. Have computers and similar technologies, such as cell phones, changed the way in which we interact with each other?
   Yes  No

2. What types of information about each other do we lose when we communicate through technologies such as computers and cell phones?

3. In what locations is it expected that we turn off our cell phones?

4. What should you do if you receive an email saying you have won a large sum of money and can claim it by clicking on a link in the email?

5. Imagine you receive an email telling you there has been suspicious activity on your credit card. In order to authenticate these transactions and stop further charges, you will need to submit your social security number so your account password can be reset. What should you do?

6. What are some of the guidelines everyone should follow when interacting through social media?

7. If someone you have gotten to know through Facebook wants to meet you, what should you do?
Summary, challenges, and instructional strategies
New Mexico Broadband Program
Security and Safety in the Digital Age
Module 2
Protecting your Personal and Financial Security Online

Slide 2

Learning Outcomes
- Understand general guidelines for online security
- Understand secure websites and passwords
- Understand precautions needed for social media
- Understand how to avoid hacking, phishing, & identity theft

By the end of the class, you should
Know how to install and use anti-virus software
Know how to update operating and security software
Know how to maintain clean file systems
Most of us know that using the Internet can pose a potential threat to our online security and safety. But fewer of us know exactly what those threats are and how to avoid them. Understanding the dangers posed by Internet use can help us guard against them effectively.

Internet threats often aren’t as dangerous as some people imagine. They are also often very different from what we might think they are.

Threats usually involve other people gaining access to our personal or financial information.
Two guidelines for keeping personal and financial information secure:

1. Take basic precautions.
2. Don’t give information away!

How does this happen?
Personal information is actually difficult for other people to get if we follow some simple guidelines. The first is to take basic precautions, just as we would in a face to face format. The second is to make sure that we do not unintentionally give that information away!

Precaution: Don’t broadcast personal information such as your birthday, home address, or marital status unless it is required by the business you are engaging.

What are the basic precautions for keeping personal information safe?
First – don’t broadcast this information by posting it unnecessarily. There is no reason why most people or sites would need to know your home address, your marital status, your birthday, your vacation plans. Be thoughtful about how you share this information, and do so only when it would logically be required for the business you are engaging.

Precaution: Use secure websites that begin with https.

When you do need to provide this sort of information, as you might if you are completing a job application or arranging for delivery of something you have purchased, make sure you are using a secure website. Secure websites are identified with a different beginning letters of the URL than other websites. Regular websites begin with http Secure websites begin with https
Secure websites show a gold lock somewhere on the website.

You will also see a small gold lock somewhere on a secure website, often on the right side of the address bar. Secure websites do not send information directly, but encode it when it is transferred. If the information is intercepted, it cannot be decoded or used without the special decoding formula. Secure websites are common for banking and other financial websites. The sales section of many websites, which process the actual transactions, are also generally secure websites. This means that even though you are giving your payment information, such as credit card or account numbers, the information will be seen only by you and the recipient of the payment, and cannot be decoded by anyone else.

One of the best precautions you can take is to create strong passwords. Strong passwords are hard to break and protect our information. What makes a password strong?
Strong passwords are ones that are difficult to break. Commonly, they have the following characteristics.

- They contain both letters and numbers.
- They also contain symbols. Symbols are things like the pound sign, the dollar sign, parentheses, or asterisks. They may also include punctuation.
- They are long. A good password should be at least 8 characters long. Longer passwords are better. Some people feel that if a password is over 15 characters, it is almost impossible to break.
- Strong passwords mix up letters, numbers, and symbols, in combinations that are almost impossible to guess or replicate. They contain no full words or names, no strings of numbers of common length (5 = zip code, 6 = birthday), and no patterns.

Another precaution you can take is to change your passwords frequently. Standard recommended time is once every 6 months. Changing them frequently diminishes the chance that someone will discover and use a password over a period of time. It also makes it more difficult for anyone to “narrow in” on your password, since a frequently changed password is a moving target.
If you use social media sites, such as Facebook, you should consider some additional precautions. Because social media sites are generally friendly and social, we may at times forget to consider safety and may want to share more personal information. Keep these key points in mind as you add information to social media sites.

Remember – social media sites are public. Even though you can set controls for who views your information, it is still a public forum. If you wouldn’t say it in front of a group of your friends, don’t post it online.

When we first make friends, we may know relatively little about them. If we invite new friends to our social media site, we will be sharing more personal information with them. Make sure that the information on your site is information you are comfortable sharing with relatively new acquaintances. Keep this “new friend standard” as your threshold for any information that you post online.
The best strategy for protecting your safety and security on a social media site is to set the controls appropriately. If you are no longer friends with someone, you should not allow that person access to your social media sites. If someone is acting inappropriately towards you, bullying you, or makes you feel uncomfortable, you should block that person as well. Blocking does no harm, and you can always unblock the person. But continuing to interact with anyone who acts inappropriately or bullies can do harm.
So far, we’ve covered a lot of precautions and best practices that you can follow to help you stay safe online. There are a few more issues of online safety and security you might want to consider. The first of these is hackers. What is a hacker, and do these people pose a threat to you online? Technically, a hacker is someone who accesses a computer system by circumventing its security system and without the owner’s knowledge or permission. Often, but not always, the goal of hacking is to steal information. It may be email lists, bank account passwords, or any other information stored on the computer.

One of the best ways you can protect your computer against hacking is to update your software regularly. One of the things updating does is apply “patches,” new areas of protection needed at those spots that have been found to be vulnerable to attack. When the patches are applied frequently and as soon as they are available, hackers have a more difficult time finding a way in to your system.
Another way that you can protect your computer against unwanted attacks of any sort is to keep it turned off when you are not using it.

For earlier computers, it was often recommended that users keep their computers running and connected to the Internet 24/7. This was true for earlier models, in which frequent booting up was difficult for the computer to handle and wore out the hard drive.

This is no longer the case; computers can be turned on and off frequently without damage to the key systems or components. In fact, keeping the computers off when not in use helps maintain the longevity of some parts, saves electricity, and minimizes the amount of time the machine is online and thus vulnerable to attacks. If your computer is off, it cannot be hacked.

Another threat we often hear about is “phishing.” Phishing refers to attempts to get access to private information, such as passwords and logins, by communicating and pretending to be a legitimate entity. Phishing commonly occurs via email. A “phisher” will send an email that looks like it comes from your back asking you to provide your password or social security number. It may tell you that this is needed because someone appears to be using your account inappropriately. By frightening people, phishers can often scare them into giving away personal and security information. In fact, rather than protecting you from a threat, the phisher is the threat!!
Don’t be fooled. Be suspicious of any request that you receive via email asking for secure information. If you feel uncertain, call the institution that claims to be making the request.

Remember, most business institutions know they should NOT ask for this information through online correspondence, and they won’t.

Identity theft: According to the Federal Trade Commission, “identity theft ... consists of] someone using your personal identifying information, like your name, Social Security number, or credit card number, without your permission to commit fraud or other crimes.”

The most common cases we think of are those in which other people are able to find our credit or banking information and make purchases on our credit card or withdraw money from the bank because they can provide information, such as passwords and
Identity theft is becoming more common. How can you protect yourself against this? Keeping your personal and financial information private is the best guard against identity theft.

It’s also important to monitor your financial and personal accounts regularly. Look for unusual patterns. If you see a charge or transaction that you did not authorize, report it immediately. Catching identity theft early helps minimize the consequences.
Changing your passwords frequently is another good safeguard against identity theft. If your password has been stolen, changing the password will mean that the stolen password will no longer provide access to your information. This can stop the theft from continuing.

With all these threats, it may not feel like the online world is very secure. But in reality, the online world isn’t any more or less secure than other environments. Because it is still new to many of us, it may feel less familiar and thus more threatening. Staying informed, taking the precautions we’ve discussed, and keeping your information private really will increase your chances of staying safe online.

Let’s review what we’ve learned:
- Keeping information private
- Secure websites
- Passwords
- Security and social media sites
- Hacking, phishing, and identity theft
We appreciate the time you spent with us.
We hope to see you at the next training!

These materials were created collaboratively by the New Mexico Department of Information Technology, Fast Forward New Mexico, and the New Mexico State Library, under grants provided by the National Telecommunications and Information Administration. These materials are not to be used for profit.

Connecting you to a world of opportunities

Demonstration instructional Video
Guidelines for Personal and Financial Security Online

**DO NOT** give out any personal or financial information over the Internet unless it is required by a transaction that you have initiated.

**DO NOT** broadcast details about your personal or financial life over the Internet unless needed for a transaction that you have initiated. This includes social security information, birthday, home address, names and birthdates of family members, as well as account and password information.

**DO** use secure websites, marked with an “https” at the front of the URL and with a gold lock on the site, for all business transactions.

**DO** create strong passwords. These should be 15 characters in length, if possible, and include an interweaving of letters, numbers, and symbols.

**DO** change your passwords frequently. The minimum recommendation is once every 6 months.

**DO** be conservative when using social media sites, and do not share information with strangers.

**DO** use control settings on social media sites to limit your engagement to those you know.

A **hacker** is one who attempts to gain access to computers illicitly. Protect against hacking by keeping your operating system and security systems up to date, and turning your computer off when not in use.

A **phisher** is one who attempts to get personal information by sending email or text messages that appear to be from legitimate individuals or institutions. Protect yourself against phishing by never responding to unsolicited emails and never opening attachments or links in these emails. Block the sender or mark it as SPAM. Report the sender to the email service provider if possible.

**Identity theft** consists of one person using another person’s personal identifying information without permission and in order to commit fraud or other crimes.  
Protect against identity theft by following the recommendations given for protecting personal and financial information. In addition, make sure you change your passwords frequently. Finally, monitor all your accounts and report any unauthorized transactions or activity immediately.
Assessment

SECURITY AND SAFETY IN THE DIGITAL AGE
MODULE 2 – ASSESSMENT

1. How should we handle our personal information, such as address, birth date, or marital status, in our online interactions?

2. What should you look for on a website that claims to be secure to confirm that it is in fact a secure website?

3. What are some characteristics of strong passwords? Use these guidelines to help you make up a strong password.

4. What is a “new friend standard”?

5. What should you do if you feel someone is bullying you online?

6. What are two things we can do to protect our computers from hackers?

7. What can we do to protect ourselves from identity theft?
SECURITY AND SAFETY IN THE DIGITAL AGE  MODULE 3:
Monitoring and controlling Internet content

Summary, challenges, and instructional strategies
New Mexico Broadband Program
Security and Safety in the Digital Age
Module 3
Monitoring and controlling Internet content

Learning Outcomes
• General guidelines
• Blocking email and spam
• Monitoring browsing history
• Using Windows’ controls
• Using monitoring and filtering software

By the end of this module, you can expect to
• understand the general guidelines regarding monitoring and controlling Internet content
• Know how to monitor browsing history
• Know how to block email and spam
• Know how to use Windows’ controls
• Know about monitoring and filtering software
When we begin using the Internet, many of us feel awed by the amount of information available.

While we appreciate the openness and access that the worldwide web has made possible, we are sometimes dismayed and affronted when we encounter information that is unpleasant or inappropriate. This is especially true when we encounter information that affronts our sensibilities or goes against our sense of privacy, security, or values.

This occurs when we get unsolicited emails advertising unwanted drugs, when we unintentionally view violent or pornographic content, or when we become concerned that our children may become exposed to these and other material that we feel is inappropriate for their age, their maturity, or our family values.
While the Internet does provide a new level of open access to information, it's important to remember that such material has always existed and fairly readily available. Tabloid headlines with violent images line the check-out stands at grocery stores and pornographic magazines are available in bookstores. What is different now is that virtually everyone has unrestricted access to this content, simply by turning on a computer.

Our first guideline in staying safe and feeling secure online is to make smart choices. We can delete uninviting email and close unappealing websites. Doing so will greatly limit the impact these sites have on us.

If we receive inappropriate or offensive email, we can do more than delete it. We can block email messages that are inappropriate or that look like phishing scams.
Any email message that appears to be spam or is from a sender you do not feel is trustworthy should be marked as spam and/or blocked. Gmail allows you to report email as spam.

To do so, open the email, then click on the exclamation point icon in menu of icons above the email message. This will send a message to Google that you are flagging this message and sender as spam.

Other email programs allow you to block email from a specific sender. Look for the tool that allows you to control your unwelcome email and use it!!

We can also help ourselves, others, and our children stay safe online by learning as much as we can about computers and the Internet. This will help make us more aware of where real risks lie and where risks are more limited.

For example, if you understand how Facebook personal settings work, you are more likely to understand how to improve security when using this social media site. This knowledge will help you feel more secure and allow you to give constructive advice to children that
Another general guideline for staying safe online is to limit the amount of time you spend on a computer. You can do this by building activity around other interests. If you make dinner together with your family, go for a bike ride on the weekend with your children or friends, or even watch TV with your husband or wife after a long day, there will be that much less time for being on the Internet and that much less likelihood of computer security being compromised. While using a computer is now part of all our lives, it important to find time for other activities, both individually and with others.
We can also help guide our children to act responsibly when using the Internet. This includes knowing what they should and should not view. This shows our expectations and our engagement. Our guidance shows young people that we are paying attention to their online activity, and this attention can help instill a sense of greater caution.

Even with our best efforts, the Internet now plays a large role in our lives and those of our children. How can we know our children are safe in their online activities. We cannot know with certainty what our children are doing at all times. As they grow older, our involvement in their activities lessens. But we can monitor their online activity to a degree consistent with their age and with our personal and parenting values.

You can easily check the browsing history of any computer. To do this, click the small drop down arrow on the right end of your address bar. A list of websites that have been visited on your computer will appear. If you have children using your computer, you will know what sites they are viewing.
You can also access a more complete history by clicking on the “Favorites” tab at the left of the top menu on the Internet Explorer screen. The menu that opens contains a “History” tab. Clicking on the history tab will show you a list of sites by date or by frequency of visits. It will also allow you to search for a certain site.

Windows tools included in the operating system software that will allow you to manage the content that is displayed on your computer and to restrict certain websites from being displayed.

You can access these controls by clicking on the drop down arrow next to “Tools” in the menu bar on the top right hand corner of the Internet Explorer screen. Click on Internet Options at the bottom of the menu.

Instructor: Note that in Firefox, this tool appears in a different location. Review locations before including Firefox in the demonstration.
The “Content” tab will ask you to select a user. Once you have selected a user, you are taken to a screen that allows you to set up controls. These controls enable you to limit the time a particular person is on the computer, the specific computer games that can be played, if any, and also allows you to specify exactly what programs can be used.

When you select a User, you will also be able to select “Additional Controls” that will allow you to prohibit access to specific websites. Let’s look at how to set up additional controls on a computer.

Instructor: Review this process on the computer screen for the class. You may need to install additional controls.

There are also programs available for purchase that do a more thorough job of monitoring and controlling computer use and access. There are several of these on the market, some appropriate for parental use and others developed more for business or industry.

For a good review of these programs, visit the site given here. Prices vary, generally between $40 and $100, and many companies offer free trial periods.
Review what we learned

- General guidelines
- Blocking email and spam
- Monitoring browsing history
- Using Windows’ controls
- Using monitoring and filtering software

We appreciate the time you spent with us.
We hope to see you at the next training!

These materials were created collaboratively by the New Mexico Department of Information Technology, Fast Forward New Mexico, and the New Mexico State Library, under grants provided by the National Telecommunications and Information Administration. These materials are not to be used for profit.

Connecting you to a world of opportunities

Demonstration Instructional Video
Guidelines for managing Internet content

**Block** unwanted email. You can block the sender, mark as SPAM, and report to email server.

**Learn** about the Internet. Staying up to date and informed will help you make smart choices about content.

**Develop** other interests. This provides a basis of communication and activity that does not involve the Internet and helps provide perspective.

Provide **guidelines to your children**. Teach them the rules they will need to know in order to operate safely and effectively in an online environment.

Use **browsing history** to track the sites that have been viewed from your computer, if you are concerned about access to inappropriate material by minors.

Use **Windows Parental Control** tools to manage content that specific users will see.

If needed for businesses or institutions, consider purchasing monitoring and controlling software programs.

**Skills**

**Block** email by using the “Report SPAM” or block sender links on your email program.

Review **browsing history** by clicking the arrow to the right side of the address bar. You can also click on “Favorites” on the left side of the top Windows menu. The “History” tab allows you to view the history of the sites that have been viewed. Note that if you are deleting history regularly, these lists may only show results for a few days.

To set **Parental Controls** on Internet Explorer, click on Tools, then click on Internet Options. Open the “Content” tab by clicking. The first option given is Parental Controls; click on the button. You will first have to select a user for whom controls will be valid. Once you have chosen a user, you will be able to set time limits, control the games that are used, and allow or block specific programs. For controls to be applied, you must click the “on” radio button. On the page on which you selected a user, you will also be able to set up additional controls that allow you to block specific websites.

For more stringent monitoring: www.monitoringsoftwarereviews.org//
Assessment

SECURITY AND SAFETY IN THE DIGITAL AGE
MODULE 3 – ASSESSMENT

1. How has the Internet changed our relation to explicit, violent, or inappropriate material?

2. What should you do if you receive an inappropriate, unsolicited email or phishing email?

3. How can learning more about the Internet improve your Internet security and safety?

4. How can developing additional interests that are not computer based improve your online security and safety?

5. How can we tell what Internet sites have been viewed from a computer?

6. What do Parental Controls allow you to do?
RESOURCES FOR SECURITY AND SAFETY IN THE DIGITAL AGE

Websites and Online Training

http://www.gcflearnfree.org/internetsafety
This site is the larger class on Internet safety from the from gfclearnfree and includes a class on protecting your computer against viruses, selecting anti-virus software, and updating and backing up your computer. The majority of the topics deal with Internet-based safety risks and address subjects such as cyber-harrassment, email scams, financial security, and more. There is also a separate link for “Internet Safety for Kids” (http://www.gcflearnfree.org/internetsafetyforkids), which speak to Internet security issues particularly relevant for children and parents. A very good and up to date resource that covers all the important information in a single online class.

http://staysafeonline.org/
This website deals with the topic of online security and safety in its broadest interpretation, blending a larger consideration of cyber-crime and cyber security with issues of online security and safety for home and school computers. The site deals with all aspects of computer security and includes resources for schools and parents and emphasizes the motto: “Stop. Think. Connect.” Information sheets present good summaries of best practices, but resources beyond these basics are limited.

Microsoft provides a website for computer security and safety that is a robust resource. The site provides information and advice on updates, software, scams, and passwords. Additional tabs for “Privacy” and “Family Safety” give information on social media safety and online bullying. Opening the menu items in the list on the left will provide information about specific tools such as Parental Controls. A no-frills but extensive and useful site for anyone with a PC and especially those using Window products. Also a good source of written directions for many tasks such as updating and adjusting settings.

http://www.commonsensemedia.org/
Common Sense Media is dedicated to exploring the impact of digital media on our lives, especially those of younger people. Their goal is to provide “trustworthy information, education, and independent voice they need to thrive in a world of media and technology.” They provide excellent information and resources, for parents and schools, in the form of studies and reports, online professional development for teacher in media literacy and security, videos and webinars for students and parents, and ongoing reviews of online games, movies, learning software, and more. The approach is balanced and intelligent with the goal of providing information that will allow parents and educator to make informed, critical choices.
Instructional Strategies for Security and Safety in the Digital Age

Slide 1

New Mexico Broadband Program
Train the Trainer Toolkit
Security and Safety in the Digital Age
Challenges and Instructional Strategies

Slide 2

Introduction to the Internet
Instructional Strategies and Challenges

Learning Objectives
Security and Safety in the Digital Age
Understand key challenges
Acquire tools for successful delivery
Slide 3

Greatest challenge is differentiating between important and unimportant security and safety concerns

- Many are overly cautious about security issues without having awareness of how they can protect themselves.
- Yet they are unaware of the security risks involved in other activities or processes.
- Try to create a balanced view, neither frightening nor under-estimating, in the class.

Slide 4

Emphasize the importance of what they can do:

- Change passwords
- Monitor all accounts regularly
- Don’t give away personal information online
- Don’t respond to email from unknown senders
- Don’t accept unsolicited offers
- Don’t open email attachments from unknown senders
- Keep all software updated

Slide 5

Compare to non-virtual security and safety to establish perspective

- We don’t leave the house unlocked
- We don’t speak to or share information with strangers
- We don’t give people our bank account numbers if they ask us on the street

We are in the process of establishing the same codes of safe behavior online. Online isn’t more dangerous, but it is a new mode of communication and interaction.
Monitoring content and using controls

- Walk through History view and Parental Controls in class.
- Emphasize the importance of making age-appropriate choices.
- Engage the importance of teaching children online security skills, just as we teach them to cross the street and drive a car.
- Utilize resources in the Toolkit for excellent websites and videos.

Thank you for helping to bring digital literacy to your community!!

These materials were created collaboratively by the New Mexico Department of Information Technology, Fast Forward New Mexico, and the New Mexico State Library, under grants provided by the National Telecommunications and Information Administration. These materials are not to be used for profit.

Connecting you to a world of opportunities.