



Presenter note: This presentation is designed to run in "slide show" mode. Select "Slide Show" from the menu bar and then click on "From Beginning." Press the arrow keys or click to advance slides. On the video slides, click on ► to begin the video. To print these notes, select "File" and "Print" then click on the drop down under "Slides" and choose "Notes Pages." Have fun with your presentation!

"Hi, my name is _____, and I'm a _____ at McAfee." [Give a brief description of your role at McAfee and introduce any other volunteers that might be with you.]


"McAfee, an Intel company, is the world's largest dedicated security technology company. We are relentlessly focused on finding new ways to keep our customers and our communities safe, and especially our most vulnerable population, children.

In order to do that, McAfee has partnered with the Department of Homeland Security, the National Cyber Security Alliance, the Anti-Phishing Working Group, and other organizations to develop curriculum aimed at helping kids understand how to stay safe and act responsibly online. Through McAfee Cares – Online Safety for Kids, McAfee empowers its employees to volunteer in communities where they live and work to deliver these important messages to school-aged kids.

One critical component of the Online Safety for Kids program is to educate parents on some of the risks their kids may encounter online, as well as offer some tips on how to help keep them safe as they use the Internet."


AGENDA

- **Introduction**
 - What is the Online Safety for Kids program?
 - STOP.THINK.CONNECT.™
- **Your Family's Digital Life**
 - What role does the Internet play in your home?
 - The "Wild Wild Web"
 - The Digital Divide between parents and kids.
- **Identifying the Risks**
 - Cybersecurity (Keeping your stuff safe)
 - Cybersafety (Keeping yourself safe)
 - Cyberethics (Treating others with respect online)
- **Action Plan**



©2010 STOP.THINK.CONNECT. Messaging Convention, Inc. Used under license. All rights reserved.

2

 McAfee
An Intel Company

“First, we’ll examine your family’s “digital life”. What role does the Internet play in your (and your KIDS’) lives?

We’ll also look at a recent study conducted by McAfee, which revealed some of the risky behaviors teens reported being involved in on the Internet, as well as how few parents are aware of these behaviors. For those of you with younger children, we feel that it is important for you to be aware of what lies ahead. By discussing important safety messages with your children as early and as often as possible, they will gain a solid foundation for making good decisions when they are older.

Lastly, we’ll cover some simple solutions you can implement in your home to help keep your family safe.”



“At McAfee, we believe that everyone, everywhere has the right to be safe—especially children. The primary messages delivered in our Online Safety for Kids program center on three pillars. They are:

- Cyber-security = Keeping your devices and information safe
- Cyber-safety = Keeping yourself safe
- Cyber-ethics = Acting responsibly and keeping the web a safer place for everybody

We call these the *Three C's* and hope that by exploring these three key areas, students will learn the importance of making good decisions online.

The universal message we are promoting is STOP.THINK.CONNECT.”

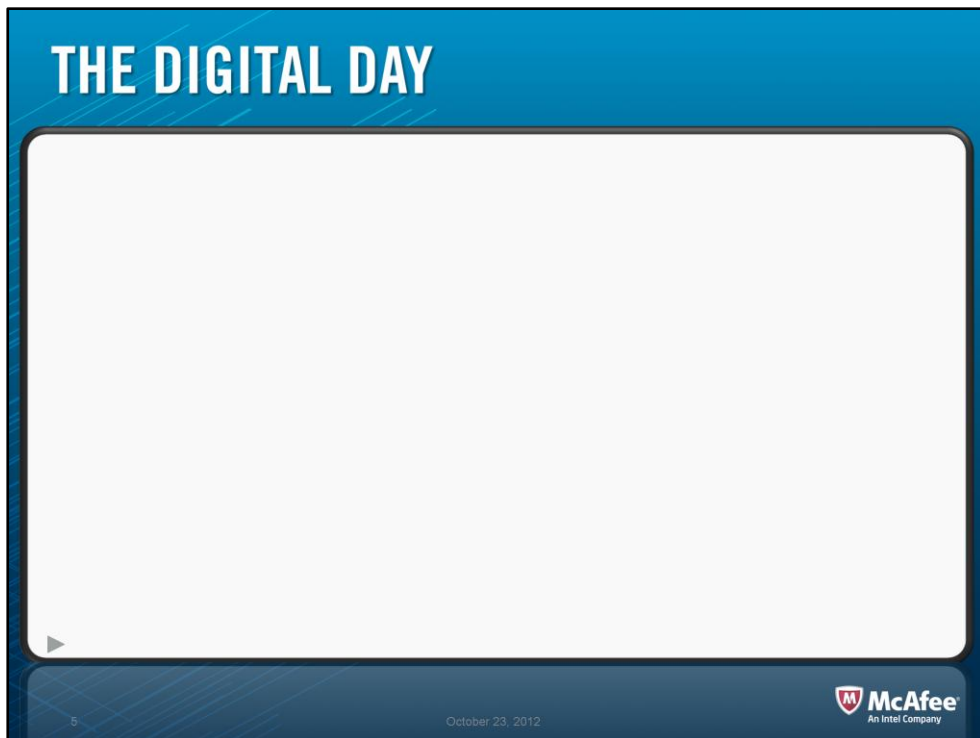


“When your children were little, most of you probably taught them to “stop, look and listen” before crossing the street. Well, they should take the same precautions when they’re about to connect to the Internet. Any time kids are about to go online, they need to make sure they’re avoiding putting themselves or their personal information (as well as that of their family) at risk. In order to do that, it’s important to:

Stop – Before using the Internet, take time to understand the risks and learn how to spot potential problems.

Think – Take a moment to be certain the path is clear ahead. Watch for warning signs and consider how your actions online could impact your safety, or your family’s.

Connect – Enjoy the Internet with greater confidence, knowing you’ve taken the right steps to safeguard yourself and your computer.”



“The internet is an amazing tool. Many of you may remember when research meant taking a trip across town to the library where you might have found what you were seeking, but more often didn’t. Today, we can access up-to-the-minute information from all over the world in our pajamas before breakfast. It’s an important tool, a great educator and good entertainment. That’s the up side. What we hope to do today is show you ways to lessen some of the risks associated with the enormous benefits of connecting with the Internet.

Let’s watch a video that shows a digital day in the life of a family. As the video plays, I’d like to draw your attention to all of the information that is going INTO each device, as well as the information that is being sent OUT with each family member’s activity.

GREEN ARROWS indicate safe connections.
YELLOW ARROWS indicate questionable connections.
RED ARROWS indicate dangerous connections.”

[To start video, hover your mouse over the slide until you see the “play” button in the lower left-hand corner, and then click.]



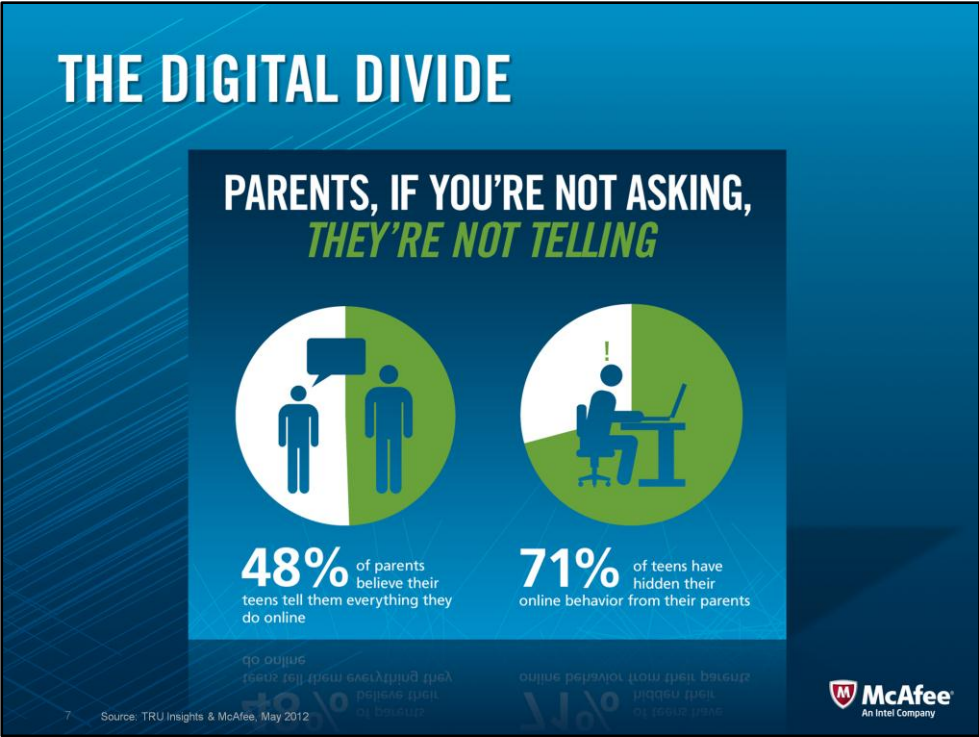
[Possible discussion questions:]

- What are the top three reasons your kids use the Internet? (For example: homework, social networking, research, music, gaming, etc.)
- Are there any websites you know your kids visit regularly?
- What is your biggest concern about your kids online activity?"

[Take a few parent responses.]

“It used to be that you needed a computer and phone line to use the Internet. Now people connect wirelessly, via gaming systems like Nintendo DS, PlayStation 3, Xbox Live, as well as tablets, smartphones, and even some television sets. Millions of families worldwide use the Internet every day to learn, research, shop, share photos, play games, download movies and music, connect with friends, meet new people—and the list goes on.

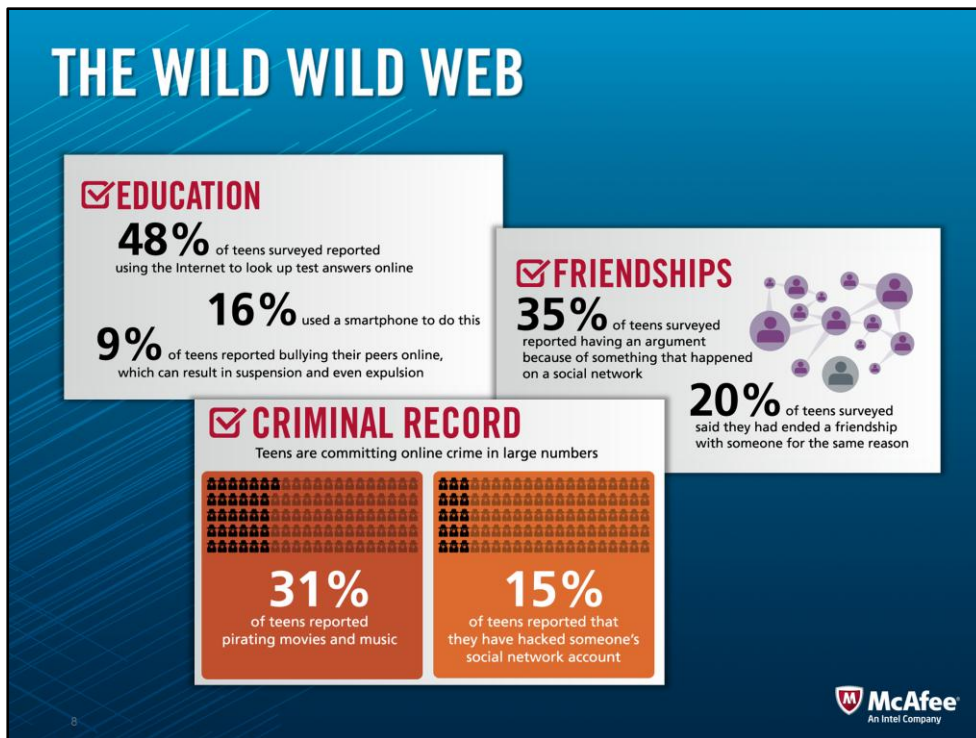
It’s no surprise that cybercriminals are taking advantage of the Internet and the people who use it. As soon as family members become active online – and no matter what their age – it’s time to educate them about cyber safety. It’s important for you, as parents, to understand the capabilities that each of these devices has, so that you can be proactive in the ways you look after your children’s safety.”



“Because our kids were born into this highly digital world, using the Internet is second nature to them. It is not at all unusual for kids to be more tech savvy than the adults in their lives.

Some people compare the Internet to the “Wild Wild West” because it is a wide open territory where anything can happen. As your kids are navigating in this environment, even the best of kids can accidentally—or sometimes intentionally—visit some risky sites.

McAfee’s recent study revealed that 48% of parents believe that their teens tell them everything they do online. In contrast, 71% of teens report having hidden their online activities from their parents at some point. We call this the *Digital Divide*—that is, the disconnect between what parents believe their kids are doing online, and what they actually are doing. We’ll explore what some of those behaviors are in a few minutes, but, first, let’s take a look at what is at stake for our children.”

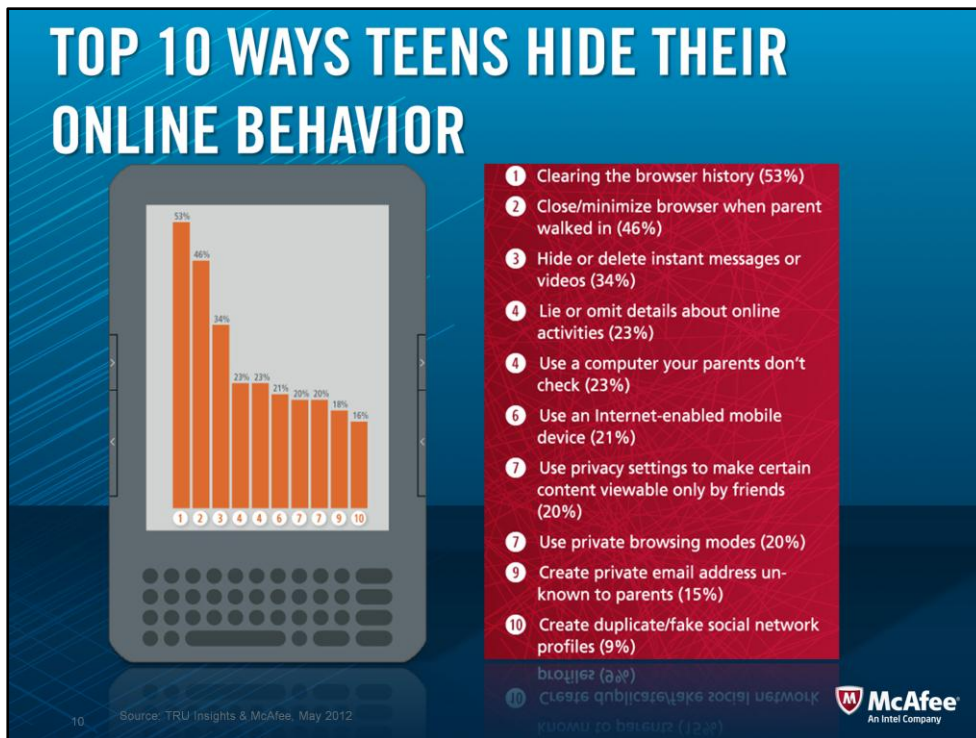


“Being online and behind a computer can create a feeling of anonymity, and we are all more likely to do things we wouldn’t even consider in real life. This is especially true for children.

For example, one in five teens reported ending a friendship because of something that happened online. What starts out in the school yard no longer gets left behind at school. When kids get home, aggressive online behavior, like cyberbullying, can continue, often denying kids of the refuge they would normally find at home.

While a majority of kids would not consider cheating in front of a teacher, or shoplifting, almost half of teens reported looking up test answers on the Internet, and a third of teens reported pirating movies and music.

Bullying, cheating and stealing aren’t new issues, but even kids who wouldn’t normally engage in these behaviors might be tempted online. Adding peer pressure to the equation makes it even more likely that kids will engage in risky behaviors.”



“In this same study, McAfee identified the top 10 ways teenagers hide their behavior online. Let’s take a minute to read through them.

Why do you think so many kids are hiding their behavior?”

[Take a few parent responses.]

“If your child is clearing the browsing history on your computer, or hiding activities, it may be because he or she is too embarrassed or ashamed to talk to you about it. Opening up the lines of communication, and letting kids know about the risks to their safety (not to mention the risks to the digital devices they love) is likely to convince them to start being more responsible and honest about their actions on the Internet.

Some signs that your child may be involved in risky behaviors online include:

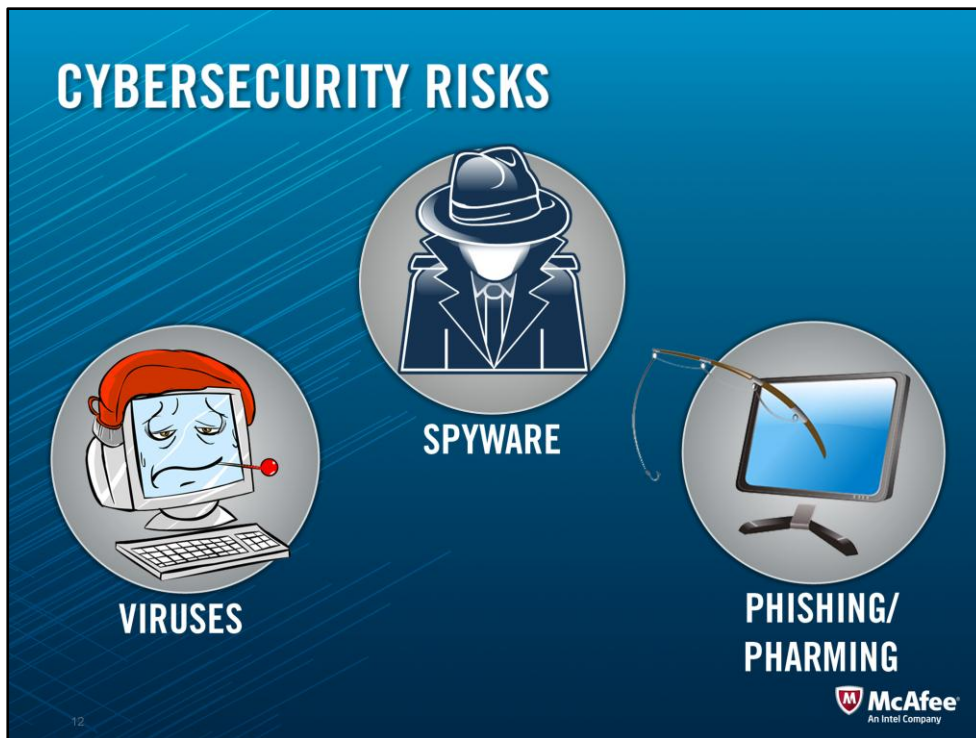
- Changes in behavior
 - Excessive time spent online and on social networks
 - Acting distant and avoiding details
 - Acting guilty when confronted about online behavior and actions”
- (Source: James Hendrix)

CYBERSECURITY: Keeping your stuff safe



“Throughout this presentation, we’ll offer some tips in three categories – actions, communication and tools -- actions you can take, messages to communicate to your kids and tools that are available to assist you as you chart out the best course for keeping your family safe and secure.

If we’re going to attempt to teach our kids how to keep their devices and personal information safe, we need to first discuss some of the most common types of malware (malicious software) that they might encounter while traveling the world wide web.”



“What are the security risks to your digital devices? We saw several examples in the video we watched earlier, but what are they, really?”

Phishing/pharming

Imagine the online “bad guys” throwing out virtual bait (such as a Pop-Up Ad for a free iPad) to get you to enter personal information, like your name, address or account information that can be used to hack into your online accounts, steal your financial assets or spread malware to other computers that connect to yours.

Spyware

These malicious programs run in the background on your system in order to capture private data, like user names and passwords. It doesn’t necessarily affect how your device operates – you might not even know it is infected.

Viruses

A virus is a malicious program that replicates itself and can spread from one file or device to others, via email and file sharing. Some viruses can cause major damage to data and computer systems.

Let’s take a closer look at these types of threats.”



“Here’s a screenshot from the video we watched earlier, which shows a very common way that cybercriminals lure young kids to offer some of their personal information, known as pop-ups.

If you recall, seven-year-old Michael was playing a video game at breakfast when he saw this AMAZING pop-up for a free download of a game. In exchange for the game, not only did Michael download malware to his computer, but he also provided his name, phone number, school name and town in the process.

These types of pop-ups are designed to entice you to connect so that they can take advantage of you in any one of several ways, like

- Downloading malware onto your computer
- Taking you to a malicious website
- Getting you to share personal information.”

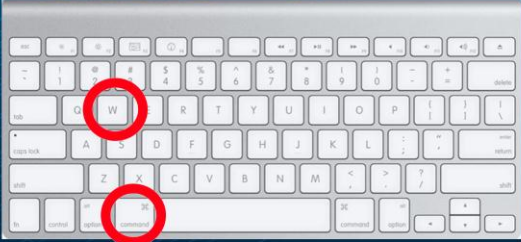
It’s important to remind kids that if something seems too good to be true, it probably is! They should never click on pop-up ads—not even to close them. Here are some tips to closing pop-up ads safely and securely.”

TO SAFELY CLOSE A POP-UP


PC: ALT + F4



MAC: COMMAND + W



14



McAfee
An Intel Company

“To safely close a pop-up on a PC, hold down the Alt key and press F4.

For Mac users, hold down the Command key and press W.”



“Here’s an example of spyware from that same video. Jennifer checks her Facebook before school, and starts surfing on the Internet. What she doesn’t realize is that when she searches for her favorite celebrity, she actually downloads a keylogger as well.”

FYI: Keylogger—also called *key logging* and *keystroke logging*, is malware that usually runs hidden in the background of your computer automatically recording all keystrokes, including user names and passwords. Users are typically unaware of its presence.

“Here’s a great tip to safe searching on the Internet: at McAfee we offer a free software product called **Site Advisor**. It let’s you know BEFORE you go to a website if it’s a threat to your computer’s security by showing you a green, yellow, or red light.”

OPTIONAL: “How does it work? Each day, thousands of times a day, McAfee visits Websites and tests them for a comprehensive set of security threats. From annoying pop-ups to back door Trojans that can steal your identity, we find the danger zones before you stumble on them.”

Mommy, how did Daddy become a zombie?

Well Timmy, Daddy wasn't always living dead.

Botnet Threat

zom-bie noun \ˈzām-bē\

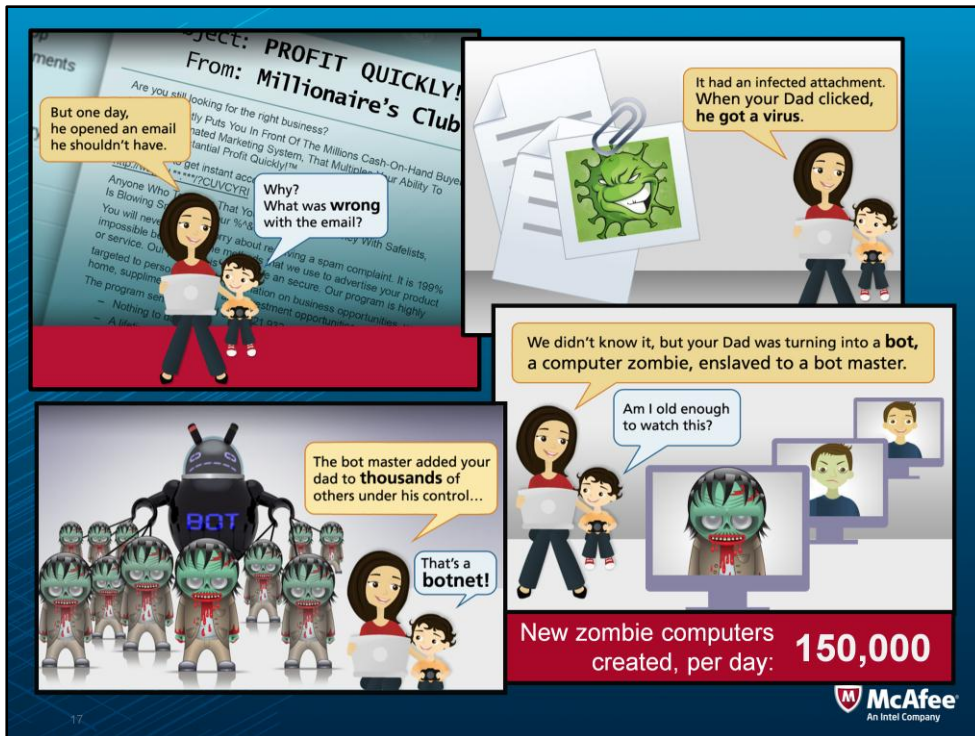
1. the living dead
2. a computer that a remote attacker has accessed and set up to forward transmissions, including spam and viruses, to other computers on the Internet

16

McAfee
An Intel Company

“We’ve all heard of viruses, but there’s a new type of virus that is of growing concern because it enables criminals to take control of your computer for illegal purposes, turning it into what is referred to as a robot or “zombie.” These zombies are then joined together in a network known as a BOTNET. BOTNETS are a serious concern because they enable criminals to harness the combined computing power of individual computers to operate illegal activities. Typically, the owners of the infected computers have no idea that their systems are being used in this way.

This little story illustrates how a computer can become a zombie, why this is a bad thing, and outlines some steps you can take to prevent it from happening.”



“How many of you have ever clicked on an attachment or a pop-up and then regretted it? I think most of us have at one time or another and that is exactly how 150,000 computers are infected EVERY DAY with viruses sent out by BOT NETWORKS.

Often these networks are used to send out massive amounts of SPAM or to launch distributed “denial of service” attacks on large businesses, such as on financial institutions, which cause so much traffic that legitimate users are unable to access the site. BOTNETS are also used to create additional zombie bots to add to their army of computers.

You may or may not notice a difference in computing power if your computer has been compromised, but there are steps you can take to avoid being used in this way.”

You know how I said Daddy got sick with the Zombie virus?
There's a medicine called **Anti-Virus**.

Hacker Kryptonite!
What are we waiting for?

3 Steps

to be zombie free:

1. Update your anti-virus
2. Run a complete scan
3. Stop opening attachments from people you don't know!

18

McAfee
An Intel Company

“The best way to protect your devices from any type of virus is to make sure you have installed a comprehensive security software package, including anti-virus, anti-spyware and firewall software, and to set the preferences to automatically update as frequently as possible, as thousands upon thousands of new malware threats emerge every day.

If you suspect that your family’s device is compromised, update your software and run a complete scan, then make sure you scan your system on a routine basis. If this doesn’t solve the problem, you should shut down your system and seek professional advice.

Most importantly, make sure that your family (adults and kids) and anyone else that may use your digital devices to access the internet, are reminded to stop and think before connecting, especially before clicking on any link or opening any attachment, to make sure that it is from a trusted source.”



“It’s also important to keep mobile devices—such as smartphones—secure. Think about all of the information that’s at risk if one of your family members phones end up in the wrong hands:

- Pictures
- Contacts
- Texts
- Emails
- Personal and financial information

In addition, someone with access to your child’s phone can pose as your child to send inappropriate emails, text messages or photos, or can install malware designed to capture personal information, like passwords, or to even track your child’s activities.

Have your child use a complex security passcode to lock their mobile device and help them understand how important it is to keep it secret.

Remind them to log out of games and accounts like email and Facebook and to never leave their device unattended.


Keep in mind, that anti-virus security software is available for mobile devices.”

CREATING A STRONG PASSWORD

Great Way To Be	→	GR8way2B
Reading is fun	→	Reading,is\$fun
Dinosaur	→	Dino%saur
Popcorn Ball	→	ppcrnbll
Hard To Crack This Password	→	htc5tp

Never Share Your Passwords!

20



“A strong and complex password should contain a mix of upper and lower case letters, numbers and special characters. Here are some tips:

- Use a vanity license plate: “GR8way2B”
- Use several small words with punctuation marks: “reading,is\$fun”
- Put punctuation in the middle of a word: “Dino%saur”
- Use an unusual way of contracting a word: “ppcrnbll”
- Use the first letter of each word in a phrase, with a random number “hard to crack this password”: “htc5tp”

CYBERSECURITY: Parent tips

ACTIONS

- Be aware of all the ways your child connects to the Internet
- Get to know the devices your child uses and what protections are available
- Use strong passwords, keep them private, and change them often

change them often
keep them private and

COMMUNICATION

- Teach kids to keep passwords private and to safeguard their personal information
- Reinforce the STOP. THINK. CONNECT. message
- Let your kids introduce you to their favorite online activities

online activities
you to their favorite

TOOLS

- Use comprehensive, up-to-date security software on all your devices
- Take advantage of free security software, such as Site Advisor (www.siteadvisor.com)



“Let’s summarize the ways you can take charge to keep you families’ devices secure.” [A.C.T. = Actions, Communication and Tools]

“Take action:

- Think of all the ways your kids access the Internet and all the places that they access them. Consider all of these when planning for your family’s safety.
- Get hands-on with the digital devices your kids use and explore the device settings, as well as safety and privacy options. Check out software reviews for security and family protection solutions. Talk with other parents to get recommendations.
- Finally, go home and change your passwords. That is the simplest thing you can do to protect your devices and information.

Communicate with Your Children:

- Frequently remind your child about the importance of keeping passwords private. Be sure that mobile devices are password protected and that kids never leave devices unattended
- Reinforce the STOP. THINK. CONNECT. message. and train them to be cautious about clicking on, downloading, posting, and uploading content.
- Encourage your children to show you their favorite websites and games. Surf the Internet with them. Help them identify safe, credible websites and other digital content and explore preferences and settings with them.

Tools:

- Make sure your devices are protected at minimum with up-to-date anti-virus, anti-spyware and firewall software. Your local big box store can be a resource for helping you find what will meet your needs. Consider downloading McAfee Site Advisor, a free software program to add security ratings to your browser and search engine results, helping you and your family know which websites pose a security threat before you click on them. Visit www.siteadvisor.com to learn more.”

CYBERSAFETY: Keeping yourself safe



“A century ago, a marvelous new invention, the automobile, made the world much smaller as people were able to comfortably travel great distances in a fraction of the time that had ever before been imagined. With this great innovation came new dangers and risks. Society had to adapt and make a whole new set of rules, accommodations and a shared code of behavior to promote public safety.

Similarly, our kids are the first generation to grow up with hands-on access to the entire world. With that access comes expanded risk. As a society we are adapting and making our way through this new frontier to develop new ways to keep users, especially children, safe.

Helping our kids to develop good decision-making skills with regard to the internet is critical to their safety and that process needs to start as soon as they are old enough to connect for the first time.”



“So, where are the most likely places that kids will encounter threats to their safety?”

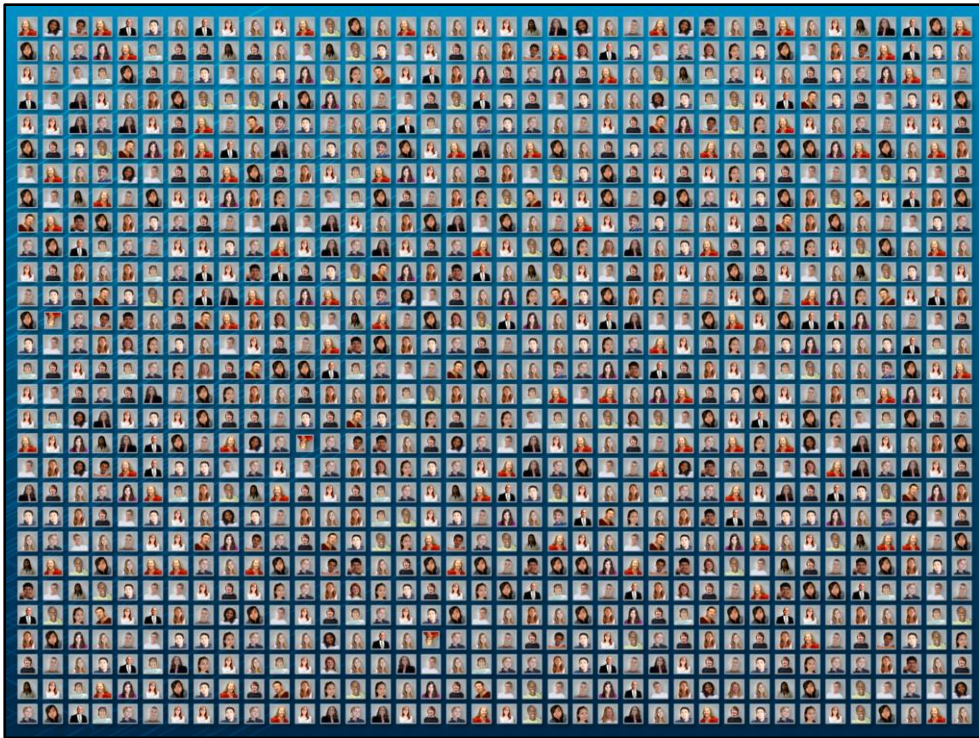
When we were growing up, the word “friend” had a much different meaning than it has with kids today. When we were young, we met kids and made friends in playgrounds. Today’s social environments are the new playgrounds, and kids are making “friends” with total strangers who may, or may not, be who they say they are.

Because of this, it’s important to explain to children from a very early age that people they meet online are STRANGERS, not friends

While sites targeting children under 13 have parental control settings that can limit a child’s exposure to strangers, parents have to proactively go into their child’s account and set those preferences. Most of these websites default to “open” settings.

While some websites, like Facebook, require that kids be 13 or older to request an account, kids can easily bypass these rules.

Perhaps the biggest concern regarding social networking can be summed up with the acronym “TMI” or “too much information.” Kids need to understand that if they reveal too much about their personal lives, it could lead to problems – like susceptibility to cyberbullies, online predators, invasion of privacy, and identity theft.”



“Here’s an example of what can happen when someone shares too much information online. This is Emma. Emma has a picture of herself that she thinks is funny, so she emails it to four of her best friends with the subject line “Don’t show anyone!” Even though Emma’s friends respect her, they think it’s funny too and they can’t resist sending it to a few more of their friends...”

<Click for more faces> “who send it to a few of their friends...” <Click for more faces>

“and so on. Eventually, the private picture that Emma had sent to her 4 best friends has been sent to hundreds of people including her teachers, parents, and... strangers. Even if Emma tries to delete this picture, it’s too late – it has already been forwarded, saved and possibly even altered.

Kids need to understand that **anything they post or send over the Internet (photos, messages, or personal information) is there forever—even if they try to delete it.**

This is a good example of why it is so important to THINK about what you post, send or upload before you do it – you never know who might get a hold of your information.”

SHARING TOO MUCH INFORMATION



“In addition to being able to save and alter the photos you share on the Internet, some people can also find out exactly where you were when you took the picture. Many new phones and cameras “geotag” photos, which embeds the GPS coordinates of the location where you took the picture.

What is geotagging?


The process of adding geographical identification information to various media such as a geotagged photograph or video.

Why is this a concern?

If you take a picture in your home, or at your school, and post it, people can figure out exactly where you were when you took the picture

Check your phone’s manual for instructions on how to disable the geotag setting.”


SHARING TOO MUCH INFORMATION



Google

Savannah Christian High School

↓



McAfee
An Intel Company

“Keep in mind, even after disabling the geotag feature on your devices, you still need to be very careful about what you post. For example, if your child posts a picture with some unique identifying information, they can often be located by doing a simple Google search.

For example, the name of the school that was visible on the wall in the photo was all that was needed to Google the location.

Introducing these safety tips when kids are young and then reinforcing them frequently will help prepare them to make good decisions when they are old enough to use social networks. If they are already in online social environments, then it is even more critical to help them understand the importance of keeping their personal information private and to remember that strangers met online are not actual friends.”

CHILD IDENTITY THEFT



“Another growing threat is described in this NBC story about children’s identity theft.

Video Summary: *This is a story featuring Chief Privacy Officer, Michelle Dennedy, and talks about how identity thieves use children’s identities to open credit accounts, buy real estate, access healthcare services and escape their criminal histories. As a result, the victimized children may lose out on jobs and internships, student loans and other opportunities that require a clean background check – before they ever step out into the real world.*

So, what can you do to prevent this from happening to your children?


Actively monitor credit reports for unauthorized activity, making sure to check your child’s social security number as well as your own. Other red flags include:

- Receiving pre-approved credit offers in the mail in your kid’s name,
- Receiving collections phone calls from creditors for your child, and
- Learning that your child’s classmates or friends have recently been compromised.”

CYBERSAFETY: Parent tips

ACTIONS	COMMUNICATIONS	TOOLS
<ul style="list-style-type: none"> • Choose a central and open location in your home for internet use • Get to know the online social environments where your kids hang out • With your child, review their list of "friends" • Disable geotagging for photos • Check that screen names are non-identifying 	<ul style="list-style-type: none"> • Remind kids to STOP. THINK. CONNECT.™ when posting, accepting "friends" and chatting online • Discuss "stranger danger" • Encourage kids to talk to you about anything unsettling 	<ul style="list-style-type: none"> • Check credit reports or use a service such as AllClearID.com to guard your child against ID theft. • Consider installing protective software with parental controls and tracking • Report issues or abuse in social environments

28



“Let’s summarize the ways you can take charge to help keep your family safe.

Actions:

- Consider designating a central and open location in your home for computer use, and agree on a central place to charge and park smart phones, tablets, Internet-enabled games and other devices when not in use.
- Know the social environments (networking, gaming and other social tools) where your children have accounts, particularly if they may encounter strangers. Create your own accounts. Play the games. Have your child add you to their network. Check their list of friends. Adjust privacy settings.
- Disable geotagging for photos
- Make sure that your child’s screen names and “gamertags” are non-identifying

Communicate with Your Children:

- Make sure your kids understand the importance of STOP. THINK. CONNECT. when it comes to posting on social networks, blogs, and games. Set expectations about the appropriate age for joining certain networks. Let your child know that you will be tracking the device and checking history -- it will give them extra incentive to avoid risky behavior and provide them with an “out” if they are experiencing peer pressure.
- Emphasize that people don’t always tell the truth online (stranger danger) and that they should never post detailed information about their whereabouts.
- Let kids know that if they experience anything unsettling online, they should come talk to you,

CYBERETHICS: Acting Responsibly Online



“Up until now, we’ve discussed all of the different ways your children’s safety can be affected by others on the Internet. Now we’re going to spend some time to explore the ways that your child may interact with others while online, as well as some signs that your child may be the victim of online harassment.”

CYBERBULLYING

43% of teens aged 13 to 17 report that they have experienced some form of cyber bullying in the past year.

 McAfee
An Intel Company

“When school children leave campus, they don’t necessarily leave their classmates and their conflicts behind. Using computers and cell phones, students can be in touch with each other at all times and they may abuse this technology to pester, bully, and harm others. Rumors, embarrassing messages and pictures circulate MUCH more quickly than any “playground rumor” as messages can spread to literally hundreds of kids with the click of the mouse.

As we mentioned earlier, the feeling of anonymity that the Internet often produces only adds to the problem.

Here are some warning signs that indicate your child might be a victim of cyberbullying:

- Being ill at ease when receiving an email, IM, or text message
- Feeling upset after using the computer
- Refusing to leave the house or go to school
- “Withdrawing from friends and family”



“Video Summary: *In this video, we see a young girl go on stage to publicly harass one of her classmates at a talent show. We see the reaction of the students and the victim. The video ends with the message, “If you wouldn’t say it in person, why say it online?”*


WHAT ARE THE CONSEQUENCES?

FOR THE VICTIM

Depending on where you live, cyber bullies can face:

- Anxiety
- Depression
- Fear
- Suspension
- Loneliness
- Expulsion
- Low self-esteem
- Arrest and jail time
- Serious long-term health issues

32

 McAfee
An Intel Company

[This slide features graphics that are animated and can only be properly viewed in Slide Show mode.]

<click>

“Depending on where you live, consequences for the BULLY range from being **blocked** from school sports and activities, to **suspension** or **expulsion**, to **arrest** and **jail time**.

You as parents can also be sued for damages resulting from cyber bullying.

<click>

Consequences for the victim may include **anxiety**, **depression**, **fear**, **loneliness**, low **self-esteem**, drop in **academic achievement**, serious long-term **health issues**, and **injury**.

To report online abuse, contact www.cybertipline.com.” If you that you or your family are in immediate danger, call 911.



“If your kids are going to go online he or she needs to know how to respond if they encounter cyberbullying—whether they are the victim or not.

Teach your kids that if they receive a mean or inappropriate text, post, email, or photo they should:

<click>

STOP correspondence with the bully, and NOT respond or forward

<click>

BLOCK that person from their friends lists

<click>

TELL an adult – such as you, a teacher, or other trusted adult.”

<click>



“Part of teaching your kids to be responsible cybercitizens is to point out the real-life consequences of their online behavior. Remind them that if they wouldn’t do something in person, they shouldn’t think it’s okay to do it online.

Here’s what we usually tell kids with regard to cybercrime—we encourage you to have a similar conversation with your kids:

*“I’m going to give you examples of a few different cybercrimes. I want you to **THINK** about whether you’ve done any of these things, or know of anyone who has. You don’t have to say anything out loud – I just want you to think about it.”*

<click 4 times to go through examples>

<click 5th time>

“All of these things are illegal and have serious consequences.”

**WOULD YOU PAY
\$675,000
FOR 30 SONGS?**



NYDailyNews.com
DAILY NEWS
News Sports Gossip Entertainment
Court Orders Boston University Student Joel Tenenbaum \$675,000 Fine for Illegally Downloading 30 Songs

PCWorld News Reviews How-To's Downloads Shop & Compare Apps Business Center
Supreme Court Lets \$675,000 Fine for Music Downloads Stand
By Cameron Scott, IDG News May 21, 2012 3:08 pm

McAfee
An Intel Company

“Here’s a real-life example of a serious consequence for stealing music—some of you may have heard about it. This student from Boston University lost a lawsuit for downloading 30 songs. In May, 2012, the Supreme Court upheld the very stiff penalty. This college student could have purchased the music for about \$30, but will end up paying over half a million dollars.”

CYBERETHICS: Parent tips

ACTIONS


- Choose a central and open location in your home for internet use
- Limit the amount of time your child is allowed to use the Internet
- Have your children add you to their social networks

COMMUNICATIONS

- Agree on a game plan: what's ok and what's not
- Discuss the consequences of posting or forwarding inappropriately – the Internet is forever
- Behavior that is unprincipled or illegal in real life is the same online

TOOLS

- Become a net-savvy parent. A good place to start is www.LearnTheNet.com. Stay current with the latest in online technology at www.mashable.com
- Software is available that can block inappropriate websites, filter content, restrict the amount of time that your kids spend online and monitor chat to flag cyber bullying or potential predators

 McAfee
An Intel Company

“Actions:

- As we discussed earlier, consider having a central and open location in your home where kids can connect to the Internet with all of their devices and agree on a reasonable amount of time that child is allowed to use the Internet.
- Establish your own accounts in the social environments that attract your children and become familiar with their use. Again, you will want your children to add you to their “friends” lists. Parents that quietly observe as a “fly on the wall” tend to get less resistance from their kids on this request than others.


Communications:

- Agree on a game plan: decide what’s okay and what’s not okay. Engage your kids in the conversation -- you’ll get more cooperation if they have been involved in creating the plan. Visit the McAfee Security Advice Center for an example of an Internet Safety Agreement.
- Discuss the consequences of posting or forwarding inappropriate photos or messages, and help kids understand that what goes out to the Internet remains there forever.
- Help kids understand that, while they may feel invisible online, they’re not. Every device that connects to the internet has an address that can be traced, and device history can be tracked even if the browsing history is deleted. Emphasize that behavior that is

unprincipled or illegal in real life is also unprincipled or illegal online and may carry severe consequences.


Tools:

- Become a net-savvy parent. If you feel like you need a beginner's guide, a good place to start is www.LearnTheNet.com. More advanced users can stay current with the latest in online technology by reviewing sites like www.mashable.com
- And, once again, consider installing software on your devices that can block inappropriate websites, filter content, restrict the amount of time that your kids spend online and monitor chat to flag cyber bullying or potential predators.”



PARENT ACTION PLAN

- Update old passwords with new complex passwords
- Keep devices such as computers, smart phones, and online games in open high-traffic areas
- Disable geotagging
- Reinforce key messages:
 - STOP and THINK before you CONNECT
 - Keep personal information private and NEVER share passwords
 - You can't take it back: the Internet is forever so be careful what you post
 - Cyberbullying: Don't do it. Don't forward it. Don't respond to it. If it happens to YOU, stop and block all correspondence and tell an adult
- Use parental controls to block, filter and monitor content
- Keep a clean machine with up to date comprehensive security software
- Consider downloading *SiteAdvisor*, a free tool from McAfee that provides website safety ratings

 McAfee
An Intel Company

“Thank you for being here today to discuss Online Safety for Kids. You have already taken a big step in helping to insure your family’s online safety and security. We encourage you and your family to create your own Online Action Plan. In the meantime, here is a recap of steps you can take immediately to help safeguard your family. [Review steps listed on the slide.]

For more information, and links to additional resources, please visit www.mcafee.com/onlinesafety.

For a fun, interactive way for kids 13 and under to learn about online safety, visit www.everloop.com/loops/mcafee” [Everloop is a fun, monitored/filtered online environment for kids age 13 and under which complies with U.S. child privacy laws. Children can visit the McAfee loop and engage in activities without becoming an Everloop member, however, membership is required to enter Everloop and experience full functionality. Children cannot become members without parent permission validated by a \$1.00 account transaction.]

Questions?”