Keep a Clean Machine:

MALWARE & BOTNETS

The Internet is a powerful and useful tool, but in the same way that you shouldn't drive without buckling your seat belt or ride a bike without a helmet, you shouldn't venture online without taking some basic precautions.

Viruses Viruses are harmful computer programs that can be transmitted in a number of ways. Although they differ in many ways, all are designed to spread themselves from one computer to another through the Internet and cause havoc. Most commonly, they are designed to give the criminals who create them some sort of access to those infected computers.

Spyware The terms "spyware" and "adware" apply to several different technologies. The two important things to know about them is that:

- They can download themselves onto your computer without your permission (typically when you visit an unsafe website or via an attachment)

- They can make your computer do things you don't want it to do. That might be as simple as opening an advertisement you didn't want to see. In the worst cases, spyware can track your online movements, steal your passwords and compromise your accounts.

Botnets Botnets are networks of computers infected by malware (computer virus, key loggers and other malicious software) and controlled remotely by criminals, usually for financial gain or to launch attacks on website or networks.

If your computer is infected with botnet malware, it communicates and receives instructions about what it's supposed to do from "command and control" computers located anywhere around the globe. What your computer does depends on what the cybercriminals are trying to accomplish.

Many botnets are designed to harvest data, such as passwords, social security numbers, credit card numbers, addresses, telephone numbers, and other personal information. The data is then used for nefarious purposes, such as identity theft, credit card fraud, spamming (sending junk email), website attacks, and malware distribution.

SPAM & PHISHING

Cybercriminals have become quite savvy in their attempts to lure people in and get you to click on a link or open an attachment.

The email they send can look just like it comes from a financial institution, e-commerce site, government agency or any other service or business.

It often urges you to act quickly, because your account has been compromised, your order cannot be fulfilled or another matter.

If you are unsure whether an email request is legitimate, try to verify it with these steps:

- Contact the company directly.

- Contact the company using information provided on an account statement or back of a credit card.

- Search for the company online – but not with information provided in the email.

Spam

Spam is the electronic equivalent of junk mail. The term refers to unsolicited, bulk – and often unwanted – email.

Here are ways to reduce spam:

- **Enable filters on your email programs:** Most ISPs (Internet Service Providers) and email providers offer spam filters. However, depending on the level you set, you may wind up blocking emails you want. It's a good idea to occasionally check your junk folder to ensure the filters are working properly.

- **Report spam:** Most email clients offer ways to mark an email as spam or report instances of spam. Reporting spam will also help to prevent the messages from being directly delivered to your inbox.

- **Own your online presence:** Consider hiding your email address from online profiles and social networking sites or only allowing certain people to view your personal information.

Phishing

Phishing attacks use email or malicious websites (clicking on a link) to collect personal and financial information or infect your machine with malware and viruses.

Spear Phishing

Spear phishing is highly specialized attacks against a specific target or small group of targets to collect information of gain access to systems.

For example, a cybercriminal may launch a spear phishing attack against a business to gain credentials to access a list of customers. From that attack, they may launch a phishing attack against the customers of the business. Since they have gained access to the network, the email they send may look even more authentic and because the recipient is already customer of the business, the email may more easily make it through filters and the recipient maybe more likely to open the email.

The cybercriminal can use even more devious social engineering efforts such as indicating there is an important technical update or new lower pricing to lure people.

Spam & Phishing on Social Networks

Spam, phishing and other scams aren't limited to just email. They're also prevalent on social networking sites. The same rules apply on social networks: When in doubt, throw it out. This rule applies to links in online ads, status updates, tweets and other posts.

How Do You Avoid Being a Victim?

- **Don't reveal personal or financial information in an email**, and do not respond to email solicitations for this information. This includes following links sent in email.

- Before sending sensitive information over the Internet, **check the security of the website**.

- **Pay attention to the website's URL.** Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com versus .net).

- If you are unsure whether an email request is legitimate, **try to verify it by contacting the company directly**. Contact the company using information provided on an account statement, not information provided in an email. Information about known phishing attacks is available online from groups such as the Anti-Phishing Working Group by visiting www.apwg.org

- **Keep a clean machine.** Having the latest operating system, software, web browsers, anti-virus protection and apps are the best defenses against viruses, malware, and other online threats.

What to do if you think you are a Victim?

- **Report it to the appropriate people** within the organization, including network administrators. They can be alert for any suspicious or unusual activity.

- If you believe your financial accounts may be compromised, c**ontact your financial institution immediately** and close the account(s).

- **Watch for any unauthorized charges** to your account.

- **Consider reporting the attack** to your local police department, and file a report with the Federal Trade Commission or the FBI's Internet Crime Complaint Center.

Protect Yourself with these STOP. THINK. CONNECT. Tips:

- **When in doubt, throw it out:** Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.

- **Think before you act:** Be wary of communications that implores you to act immediately, offers something that sounds too good to be true, or asks for personal information.

- **Secure your accounts:** Ask for protection beyond passwords. Many account providers now offer additional ways for you verify who you are before you conduct business on that site.

- **Make passwords long and strong:** Combine capital and lowercase letters with numbers and symbols to create a more secure password.

- **Unique account, unique password:** Separate passwords for every account helps to thwart cybercriminals

HACKED ACCOUNTS

If your account has been compromised or hacked, here are ways to regain control.

How do I know if my email or social network account has been hacked?

- There are posts you never made on your social network page. These posts often encourage your friends to click on a link or download an App.

- A friend, family member or colleague reports getting email from you that you never sent.

- Your information was lost via a data breach, malware infection or lost/stolen device.

If you believe an account has been compromised, take the following steps:

- Notify all of your contacts that they may receive spam messages that appear to come from your account. Tell your contacts they shouldn't open messages or click on any links from your account and warn them about the potential for malware.

- If you believe your computer is infected, be sure your security software is up to date and scan your system for malware. You can also use other scanners and removal tools.

- Change passwords to all accounts that have been compromised and other key accounts ASAP. Remember, passwords should be long and strong and use a mix of upper and lowercase letters, and numbers and symbols. You should have a unique password for each account.

If you cannot access your account because a password has been changed, contact the web service immediately and follow any steps they have for recovering an account.

Protect Yourself with these STOP. THINK. CONNECT. Tips:

- **Keep a clean machine:** Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.

- **Make passwords long and strong:** Combine capital and lowercase letters with numbers and symbols to create a more secure password.

- **Unique account, unique password:** Separate passwords for every account helps to thwart cybercriminals.

- **When in doubt, throw it out:** Links in email, tweets, posts, and online advertising are often the way cybercriminals compromise your computer. If it looks suspicious, even if you know the source, it's best to delete or if appropriate, mark as junk email.

SECURING YOUR HOME NETWORK

A protected home network means your family can use the Internet safely and securely.

Most households now run networks of devices linked to the Internet, including computers, laptops, gaming devices, TVs, tablets, and smartphones that access wireless networks. To protect your home network and your family, you need to have the right tools in place and confidence that family members can use the Internet safely and securely.

The first step is to Keep a Clean Machine and make sure all of your Internet-enabled devices have the latest operating system, web browsers and security software. This includes mobile devices that access your wireless network.

Secure Your Wireless Router

A wireless network means connecting an Internet access point – such as a cable or DSL modem – to a wireless router. Going wireless is a convenient way to allow multiple devices to connect to the Internet from different areas of your home. However, unless you secure your router, you're vulnerable to people accessing information on your computer, using your Internet service for free and potentially using your network to commit cybercrimes.

Here are ways to secure your wireless router:

- **Change the name of your router:** The default ID - called a service set identifier" (SSID) or "extended service set identifier" (ESSID) – is assigned by the manufacturer. Change your router to a name that is unique to you and won't be easily guessed by others.

- **Change the pre-set password on your router:** When creating a new password, make sure it is long and strong, using a mix of numbers, letters and symbols.

- **Review security options:** When choosing your router's level of security, opt for WPA2, if available, or WPA. They are more secure than the WEP option.

- **Create a guest password:** Some routers allow for guests to use the network via a separate password. If you have many visitors to your home, it's a good idea to set up a guest network.

- **Use a firewall:** Firewalls help keep hackers from using your computer to send out your personal information without your permission. While anti-virus software scans incoming email and files, a firewall is like a guard, watching for attempts to access your system and blocking communications with sources you don't permit. Your operating system and/or security software likely comes with a pre-installed firewall, but make sure you turn on these features.

Protect Yourself with these STOP. THINK. CONNECT. Tips:

- **Keep a clean machine:** Having the latest security software, web browser, and operating system are the best defenses against viruses, malware, and other online threats.

- **Automate software updates:** Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option.

- **Protect all devices that connect to the Internet:** Along with computers, smart phones, gaming systems, and other web-enabled devices also need protection from viruses and malware.

- **Plug & scan:** "USBs" and other external devices can be infected by viruses and malware. Use your security software to scan them.

- **Protect your $$:** When banking and shopping, check to be sure the sites is security enabled. Look for web addresses with "https://" or "shttp://", which means the site takes extra measures to help secure your information. "Http://" is not secure.

- **Back it up:** Protect your valuable work, music, photos, and other digital information by making an electronic copy and storing it safely.

Protect Your Personal Information:

ID THEFT, FRAUD & VICTIMS OF CYBERCRIME
If you're the victim of cybercrime, you need to know what to do and respond quickly.

The Realities of Cybercrime
When dealing with cybercrime, an ounce of prevention is truly worth a pound of cure. Cybercrime in all its many forms (e.g., online identity theft, financial fraud, stalking, bullying, hacking, e-mail spoofing, information piracy and forgery, intellectual property crime, and more) can, at best, wreak havoc in victims' lives through major inconvenience and annoyance. At worst, cybercrime can lead to financial ruin and potentially threaten a victim's reputation and personal safety.

It's always wise to do as much as possible to prevent cybercrime.

But, despite our best efforts, our increasingly digital lives may put us in harm's way. The fact remains that the bad guys continue to find new uses for ever-expanding—but easily accessible—online technologies to steal, harass, and commit all sorts of crime. If cybercrime happens to you, you need to know what to do and to respond quickly.

Should I Report Cybercrime? Cybercrime can be particularly difficult to investigate and prosecute because it often crosses legal jurisdictions and even international boundaries. And, many offenders disband one online criminal operation—only to start up a new activity with a new approach—before an incident even comes to the attention of the authorities.

The good news is that federal, state, and local law enforcement authorities are becoming more sophisticated about and devoting more resources to responding to cybercrime. Furthermore, over the past several years, many new anti-cybercrime statutes have been passed empowering federal, state, and local authorities to investigate and prosecute these crimes. But, law enforcement needs your help to stop the nefarious behavior of cyber criminals and bring them to justice.

Who to contact:

- **Local law enforcement**. Even if you have been the target of a multijurisdictional cybercrime, your local law enforcement agency (either police department or sheriff's office) has an obligation to assist you, take a formal report, and make referrals to other agencies, when appropriate. Report your situation as soon as you find out about it. Some local agencies have detectives or departments that focus specifically on cybercrime.

- **IC3.** The Internet Crime Complaint Center (IC3) will thoroughly review and evaluate your complaint and refer it to the appropriate federal, state, local, or international law enforcement or regulatory agency that has jurisdiction over the matter. IC3 is a partnership between the Federal Bureau of Investigation and the National White Collar Crime Center (funded, in part, by the Department of Justice's Bureau of Justice Assistance). Complaints may be filed online at http://www.ic3.gov/default.aspx.

- **Federal Trade Commission**. The FTC does not resolve individual consumer complaints, but does operate the Consumer Sentinel, a secure online database that is used by civil and criminal law enforcement authorities worldwide to detect patterns of wrong-doing, leading to investigations and prosecutions. File your complaint at https://www.ftccomplaintassistant.gov. Victims of identity crime may receive additional help through the FTC hotline at 1-877-IDTHEFT (1-877-438-4388); the FTC website at www.ftc.gov/IDTheft provides resources for victims, businesses, and law enforcement.

- **Your Local Victim Service Provider**. Most communities in the United States have victim advocates ready to help following a crime. They can provide information, emotional support and advocacy as needed. Find local victims service providers here: http://ovc.ncjrs.gov/findvictimservices/search.asp

Collect and Keep Evidence Even though you may not be asked to provide evidence when you first report the cybercrime, it is very important to keep any evidence you may have related to your complaint. Keep items in a safe location in the event you are requested to provide them for investigative or prosecutive evidence. Evidence may include, but is not limited to, the following:

- Canceled checks

- Certified or other mail receipts

- Chatroom or newsgroup text

- Credit card receipts

- Envelopes (if you received items via FedEx, UPS, or U.S. Mail)

- Facsimiles

- Log files, if available, with date, time and time zone

- Messages from Facebook, Twitter or other social networking sites

- Money order receipts

- Pamphlets or brochures

- Phone bills

- Printed or preferably electronic copies of emails (if printed, include full email header information)

- Printed or preferably electronic copies of web pages

- Wire receipts

Additional Tips for Specific Types of Cybercrime Once you discover that you have become a victim of cybercrime, your response will depend, to some degree, on the type and particular circumstances of the crime. Here are useful tips to follow for some specific types of cybercrimes:

In cases of identity theft:

- Make sure you change your passwords for all online accounts. When changing your password, make it long, strong and unique, with a mix of upper and lowercase letters, numbers and symbols. You also may

need to contact your bank and other financial institutions to freeze your accounts so that the offender is not able to access your financial resources.

- Close any unauthorized or compromised credit or charge accounts. Cancel each credit and charge card. Get new cards with new account numbers. Inform the companies that someone may be using your identity, and find out if there have been any unauthorized transactions. Close accounts so that future charges are denied. You may also want to write a letter to the company so there is a record of the problem.

- Think about what other personal information may be at risk. You may need to contact other agencies depending on the type of theft. For example, if a thief has access to your Social Security number, you should contact the Social Security Administration. You should also contact your state Department of Motor Vehicles if your driver's license or car registration are stolen.

- File a report with your local law enforcement agency. Even if your local police department or sheriff's office doesn't have jurisdiction over the crime (a common occurrence for online crime which may originate in another jurisdiction or even another country), you will need to provide a copy of the law enforcement report to your banks, creditors, other businesses, credit bureaus, and debt collectors.

- If your personal information has been stolen through a corporate data breach (when a cyber-thief hacks into a large database of accounts to steal information, such as Social Security numbers, home addresses, and personal email addresses), you will likely be contacted by the business or agency whose data was compromised with additional instructions, as appropriate. You may also contact the organization's IT security officer for more information.

- If stolen money or identity is involved, contact one of the three credit bureaus to report the crime (Equifax at 1-800-525-6285, Experian at 1-888-397-3742, or TransUnion at 1-800-680-7289). Request that the credit bureau place a fraud alert on your credit report to prevent any further fraudulent activity (such as opening an account with your identification) from occurring. As soon as one of the bureaus issues a fraud alert, the other two bureaus are automatically notified.

In cases of Social Security fraud:

- If you believe someone is using your social security number for employment purposes or to fraudulently receive Social Security benefits, contact the Social Security Administration's fraud hotline at 1-800-269-0271. Request a copy of your social security statement to verify its accuracy.

In cases of online stalking:

- In cases where the offender is known, send the stalker a clear written warning saying the contact is unwanted and asking that the perpetrator cease sending communications of any kind. Do this only once and do not communicate with the stalker again (Ongoing contact usually only encourages the stalker to continue the behavior).

    o Save copies of all communication from the stalker (including: emails, threatening messages, and messages via social media, etc.) and document each contact, including dates, times and additional circumstances, when appropriate.

- File a complaint with the stalker's Internet Service Provider (ISP) and yours. Many ISPs offer tools that filter or block communications from specific individuals.

- Own your online presence. Set security and privacy settings on social networks and other services to your comfort level of sharing.

- Consider changing your email address and ISP; use encryption software or privacy protection programs on your computer and mobile devices. (You should consult with law enforcement before changing your email account. It can be beneficial to the investigation to continue using the email account so law enforcement can also monitor communication.)

- File a report with local law enforcement or contact your local prosecutor's office to see what charges, if any, can be pursued. Stalking is illegal in all 50 states and the District of Columbia.

In cases of cyberbullying:

- Save any of the related emails, texts, or messages as evidence.

- Keep a record of incidents.

- Report the incident to the website's administrator; many websites including Facebook and YouTube encourage users to report incidents of cyberbullying.

- Block the person on social networks and in email.

- Avoid escalating the situation: Responding with hostility is likely to provoke a bully. Depending on the circumstances, consider ignoring the issue. Often, bullies thrive on the reaction of their victims. If you or your child receives unwanted email messages, consider changing your email address. The problem may stop. If you continue to get messages at the new account, you may have a strong case for legal action.

- If the communications become more frequent, the threats more severe, the methods more dangerous and if third-parties (such as hate groups and sexually deviant groups) become involved—the more likely law enforcement needs to be contacted and a legal process initiated.

How Did This Happen To Me? A Word about Malware. Many cybercrimes start with malware—short for "malicious software." Malware includes viruses and spyware that get installed on your computer, phone, or mobile device without your consent—you may have downloaded the malware without even realizing it! These programs can cause your device to crash and can be used to monitor and control your online activity. Criminals use malware to steal personal information and commit fraud.

Avoid malware with the following tips:

- Keep a clean machine by making sure your security software, operating system and web browser are up to date.

- When in doubt throw it out. Don't click on any links or open attachments unless you trust the source.

- Make your passwords long and strong and unique. Combine capital and lowercase letters with numbers and symbols to create a more secure password. Use a different password for each account.

- Set your browser security high enough to detect unauthorized downloads.

- Use a pop-up blocker (the links in pop-up ads are notorious sources of malware).

- Back up your data regularly (just in case your computer crashes).

- Protect all devices that connect to the Internet. Along with computers, smart phones, gaming systems, and other web-enabled devices also need protection from malware.

- Make sure all members of your family follow these safety tips (one infected computer on a home network can infect other computers).

- **Automate software updates:** Many software programs will automatically connect and update to defend against known risks. Turn on automatic updates if that's an available option.

- **Protect all devices that connect to the Internet:** Along with computers, smart phones, gaming systems, and other web-enabled devices also need protection from viruses and malware.

- **Plug & scan:** "USBs" and other external devices can be infected by viruses and malware. Use your security software to scan them.

- **Protect your $$:** When banking and shopping, check to be sure the sites is security enabled. Look for web addresses with "https://" or "shttp://", which means the site takes extra measures to help secure your information. "Http://" is not secure.

- **Back it up:** Protect your valuable work, music, photos, and other digital information by making an electronic copy and storing it safely.

PASSWORDS & SECURING YOUR ACCOUNTS

Passwords are like keys to your personal home online. You should do everything you can prevent people from gaining access to your password. You can also further secure your accounts by using additional authentication methods.

Passwords When creating a password, make sure it is long and strong, with a minimum of eight characters and a mix of upper and lowercase letters, numbers and symbols.

You should also remember to:

- *Never* share your password with others.

- Make your password is unique to your life and not something that is easily guessed.

- Have a different password for each online account.

- Write down your password and store it in a safe place ***away*** from your computer.

- Change your password several times a year.

Other Ways to Secure an Account Typing a username and password into a website isn't the only way to identify yourself on the web services you use.

- **Multi-factor authentication** uses more than one form of authentication to verify an identity. Some examples are voice ID, facial recognition, iris recognition and finger scanning.

- **Two-factor authentication** uses a username and password and another form of identification, often times a security code.

Over time, more websites will be adopting multi-factor authentication. In some cases, the services may be available, but are not required.

Many email services offer two-step verification on an opt-in basis. Ask your financial institution and other online services if they offer multi-factor authentication or additional ways to verify your identity.

STOP. THINK. CONNECT. Tips:

- **Secure your accounts:** Ask for protection beyond passwords. Many account providers now offer additional ways for you verify who you are before you conduct business on that site.

- **Make passwords long and strong:** Combine capital and lowercase letters with numbers and symbols to create a more secure password.

- **Unique account, unique password:** Separate passwords for every account helps to thwart cybercriminals.

- **Write it down and keep it safe:** Everyone can forget a password. Keep a list that's stored in a safe, secure place away from your computer.

ONLINE SHOPPING

It's important to take steps to protect yourself when shopping online.

Online shopping is convenient, easy, and quick. But before you start adding items to your cart, make sure you are up-to-date and have the latest security software, web browsers and operating system. Keeping a clean machine is the best defense against viruses, malware, and other online threats.

Here are some other ways to protect yourself when shopping online:

- **Check out sellers:** Conduct independent research before you buy from a seller you have never done business with. Some attackers try to trick you by creating malicious websites that appear legitimate, so you should verify the site before supplying any information. Locate and note phone numbers and physical addresses of vendors in case there is a problem with your transaction or your bill. Search for merchant reviews.

- **Make sure the site is legitimate:** Before you enter your personal and financial information to make an online transaction, look for signs that the site is secure. This includes a closed padlock on your web browser's address bar or a URL address that begins with shttp or https. This indicates that the purchase is encrypted or secured. Never use unsecured wireless networks to make an online purchase.

- **Protect your personal information:** When making a purchase online, be alert to the kinds of information being collected to complete the transaction. Make sure you think it is necessary for the vendor to request that information. Remember, you only need to fill out required fields on a vendors checkout form. Before providing personal or financial information, check the website's privacy policy. Make sure you understand how your information will be stored and used.

- **Use safe payment options:** Credit cards are generally the safest option because they allow buyers to seek a credit from the issuer if the product isn't delivered or isn't what was ordered. Also, unlike debit cards, credit cards may have a limit on the monetary amount you will be responsible for paying if your information is stolen and used by someone else. Never send cash through the mail or use a money-wiring service because you'll have no recourse if something goes wrong. Don't forget to review return policies. You want a no-hassle ability to return items.

- **Keep a paper trail:** Print and save records of your online transactions, including the product description, price, online receipt, terms of the sale, and copies of any email exchange with the seller. Read your credit card statements as soon as you get them to make sure there aren't any unauthorized charges. If there is a discrepancy, call your bank and report it immediately.

- **Turn your computer off when you're finished shopping:** Many people leave their computers running and connected to the Internet all day and night. This gives scammers 24/7 access to your computer to install malware and commit cybercrimes. To be safe, turn off your computer when it's not in use.

- **Be wary of emails requesting information:** Attackers may attempt to gather information by sending emails requesting that you confirm purchase or account information. Legitimate businesses will not solicit this type of information through email. Contact the merchant directly if you are alerted to a problem. Use contact information found on your account statement, not in the email.

BACK IT UP

Protect yourself against data loss by making electronic copies of important files, commonly referred to as a backup.

Our computers contain vast amounts of data, from family photos and music collections to financial records and personal contacts. In fact, a recent National Cyber Security Alliance/Symantec study found that more than 68% of Americans store more the 25% of their photos digitally. For most people, the loss of that information could be devastating.

Data can be lost in several ways: computer malfunctions, theft, viruses, spyware, accidental deletion, and natural disasters.

Data backup is a simple, three step process:

- Make copies of your data

- Select the hardware or method to store your data

- Safely store the backup device that holds your copied files

Make Copies of Your Data

Many computers come with a backup software program installed, so check to see if you have one. Most backup software programs will allow you to make copies of every file and program on your computer, or just the files you've changed since your last backup.

Select Hardware to Store Your Data

When you conduct a backup, the files will have to be stored on a physical device - such as CDs, DVDs, or USB flash drives, an external hard drive, or on the web using cloud-based online storage.

- **CDs, DVDs, and flash drives:** These are best for storing a small amount of pictures, music, and videos.

- **External hard drive:** If your computer serves as the family photo album and music library, it's best to get an external hard drive that plugs into your computer (preferably via a USB port). This way, you can assure more adequate storage space for all your files. Copying information will also be faster with these devices.

- **Online backup services:** If you don't want to hassle with new hardware, there are many online backup services available, usually for a monthly fee. Some security software includes this service with your subscription, so be sure to check that you don't already have this service available. You simply backup your files to a secure server over the Internet. These services have the added advantage of safely storing your files in a remote location and the files can be accessed anywhere you have a connection to the Internet. This can be valuable for people who travel a lot and may need to recover files or if you live in area prone to natural disasters that might require an evacuation.

Safely Store the Backup Device that Holds Your Data

After setting up the software and copying your files on a regular basis, make sure you keep your backup device somewhere safe. Some ideas include a trusted neighbor's house, your workplace, a safe, or a secure place at home that would likely survive a natural disaster. Keep your backup device close enough so that you can retrieve it easily when you do your regular backup.

Other software programs are available for purchase if your system does not have a backup program or if you're seeking other features. Ideally, you should backup your files at least once a week.

For Parents:

RAISING DIGITAL CITIZENS
Teach your children to become good digital citizens with these resources.

The Internet is a wonderful place for learning and entertainment, but like the world around us, it can pose dangers if precautions are not taken. Allowing free access puts your child, your computer and your personal data at risk.

- **Remain positively engaged:** Pay attention to and know the online environments your children use. Surf the Internet with them. Appreciate your children's participation in their online communities and show interest in their friends. Try to react constructively when they encounter inappropriate material. Make it a teachable moment.

- **Support their good choices:** Expand your children's online experience and their autonomy when developmentally appropriate, as they demonstrate competence in safe and secure online behavior and good decision making.

- **Keep a clean machine:** Safety and security start with protecting all family computers with a security suite (anti-virus, anti-spyware, and firewall) that is set to update automatically. Keep your operating system, web browsers, and other software current as well, and back up computer files on a regular basis.

- **Know the protection features of the websites and software your children use:** All major Internet service providers (ISPs) have tools to help you manage young children's online experience (e.g., selecting approved websites, monitoring the amount of time they spend online, or limiting the people who can contact them) and may have other security features, such as pop-up blockers. Third-party tools are also available. But remember that your home isn't the only place they can go online.

- **Review privacy settings:** Look at the privacy settings available on social networking sites, cell phones, and other social tools your children use. Decide together which settings provide the appropriate amount of protection for each child.

- **Teach critical thinking:** Help your children identify safe, credible Web sites and other digital content, and be cautious about clicking on, downloading, posting, and uploading content.

- **Explain the implications:** Help your children understand the public nature of the Internet and its risks as well as benefits. Be sure they know that any digital info they share, such as emails, photos, or videos, can easily be copied and pasted elsewhere, and is almost impossible to take back. Things that could damage their reputation, friendships, or future prospects should not be shared electronically.

- **Help them be good digital citizens:** Remind your children to be good "digital friends" by respecting personal information of friends and family and not sharing anything about others that is potentially embarrassing or hurtful.

- **Just saying "no" rarely works:** Teach your children how to interact safely with people they "meet" online. Though it's preferable they make no in-person contact with online-only acquaintances, young people may not always follow this rule. So talk about maximizing safe conditions: meeting only in well-lit public places, always taking at least one friend, and telling a trusted adult about any plans they make – including the time, place, and acquaintance's contact information (at least a name and cell phone number). Remind them to limit sharing personal information with new friends.

- **Empower your children to handle issues:** Your children may deal with situations online such as bullying, unwanted contact, or hurtful comments. Work with them on strategies for when problems arise, such as talking to a trusted adult, not retaliating, calmly talking with the person, blocking the person, or filing a complaint. Agree on steps to take if the strategy fails.

- **Encourage your children to be "digital leaders:"** Help ensure they master the safety and security techniques of all technology they use. Support their positive and safe engagement in online communities. Encourage them to help others accomplish their goals. Urge them to help if friends are making poor choices or being harmed.

More Ways to Keep Your Children Safer and More Secure Online

- **Keep your home computer in a central and open location:** If your computer is in the open, you can physically monitor your children while they are online.

- **Be aware of all the ways people connect to the Internet:** Young people have many options to connect to the Internet beyond a home computer. Phones, tablets, gaming systems and even TVs have become connected. Be aware of all the ways and devices (including what they do at friend's houses) your children are using and be sure they know how to use them safely and responsibly.

- **Talk to other parents:** When and how you decide to let your children use the Internet is a personal parenting decision. Knowing what other parents are thinking and allowing their children to do is important and can be helpful for making decisions about what your children do online.

- **Know the rules:** Not all online services are for kids. Even some of the most popular social networking services and other sites are meant only for use by people 13 and older. There are many terrific sites designed specifically for younger children that provide a safer, more secure and age-appropriate environment.

- **Stay current. Keep pace with new ways to stay safe online:** The online world is ever changing. New services with great features continually emerge. Knowing about them and how young people use them can help you better understand the digital life your children experience as well as any concerns you may have for your children.

- **Consider separate accounts on your computer:** Most operating systems allow you to create a different account for each user. Separate accounts can lessen the chance that your child might accidentally access, modify, change settings and/or delete your files. You can set up certain privileges (the things that can and can't be done) for each account.

For Emergencies

- **If you know of a child in immediate risk or danger, call law enforcement right away**. Report instances of online child exploitation to the National Center for Missing and Exploited Children's Cyber Tipline. Reports may be made 24-hours a day, 7 days per week at www.cybertipline.com or by calling 1-800-843-5678.

Additional Resources

- ConnectSafely.org has basic guidelines for teens and parents about cyberbullying, sexting, social networking, and more.

- GetGameSmart.com provides information and resources to help families make smart choices about what they play, browse, and watch.

- GetNetWise.org is a useful resource for families to learn how to protect themselves from online danger and create the safest online experience possible.

- iKeepSafe.org seeks to give parents, educators, and policymakers the information and tools which power them to teach children the safe and healthy use of technology and the Internet.

- NetSmartz.org is a safety resource from the National Center for Missing and Exploited Children (NCMEC) and Boys & Girls Clubs of America (BGCA) for children aged 5 to 17, parents, guardians, educators, and law enforcement that uses activities to teach Internet safety.

- OnGuardOnline.gov is the FTC's main consumer facing website to educate everyone on staying safe and secure online.

- WebWiseKids.org is a unique organization that offers fun, challenging and interactive simulations based on real-life criminal cases. Each program has been designed specifically for use with young people in classrooms and computer labs and is guaranteed to be easy to use and flexible with your classroom schedule.

- Wired Safety.org provides help, information and education to Internet and mobile device users of all ages. They help victims of cyber abuse ranging from online fraud, cyber stalking and child safety, to hacking and malicious code attacks. They also help parents with issues, such as social networking and cyberbullying.

CYBERBULLYING & HARASSMENT

Cyberbullying can range from embarrassing or cruel online posts or digital pictures, to online threats, harassment, and negative comments, to stalking through emails, websites, social networks and text messages.

Every age group is vulnerable to cyberbullying, but teenagers and young adults are common victims. Cyberbullying is a growing problem in schools. Cyberbullying has become an issue because the Internet is fairly anonymous, which is appealing to bullies because their intimidation is difficult to trace. Unfortunately, rumors, threats and photos can be disseminated on the Internet very quickly.

Protect Your Children from Cyberbullying:

- **Limit where your children post personal information:** Be careful who can access contact information or details about your children's interests, habits or employment to reduce their exposure to bullies that they do not know. This may limit their risk of becoming a victim and may make it easier to identify the bully if they are victimized.

- **Avoid escalating the situation:** Responding with hostility is likely to provoke a bully. Depending on the circumstances, consider ignoring the issue. Often, bullies thrive on the reaction of their victims. If you or your child receives unwanted email messages, consider changing your email address. The problem may stop. If you continue to get messages at the new account, you may have a strong case for legal action.

- **Document cyberbullying:** Keep a record of any online activity (emails, web pages, social media posts, etc.), including relevant dates and times. Keep both an electronic version and a printed copy.

- **Report cyber bullying to the appropriate authorities:** If you or your child are being harassed or threatened, report the activity to the local authorities. Your local police department or FBI branch are good starting points. There is a distinction between free speech and punishable offenses. Law enforcement officials and prosecutors can help sort out legal implications. It may also be appropriate to report it to school officials who may have separate policies for dealing with activity that involves students.

STOP. THINK. CONNECT. Tips:

- **Own your online presence:** When available, set the privacy and security settings on websites to your comfort level for information sharing. It's ok to limit how you share information.

- **Safer for me more secure for all:** What you do online has the potential to affect everyone – at home, at work and around the world. Practicing good online habits benefits the global digital community.

- **Post only about others as you have them post about you.**

PARENTAL CONTROLS

Parental controls are available on most Internet-enabled devices, like computers, smartphones, tablets, gaming systems. When enabling parental controls, use age-appropriate settings to filter, monitor and block your child's activities.

As a parent, you'll likely want to allow your children to use technology for communications, learning and more. You're also going to want to be sure that your children use the Internet safely and securely. Parental controls are a great way to be proactive about your child's online safety and activities.

OnGuardOnline.gov gives a breakdown of different types of parental controls:

- **Filtering and blocking**: This limits access to specific websites, words, or images.

- **Blocking outgoing content**: This prevents your children from sharing personal information online and via email.

- **Limiting time**: This allows parents to set time limits for how long their children are online and the time of day they can access the Internet.

- **Monitoring tools**: This alerts parents to their children's online activity without blocking access and can be used with or without the child's knowledge. Some software records websites a child has visited. Others display a warning message when a child visits a certain website.

Mobile & On the Go:

MOBILE DEVICES

Today's mobile devices are as powerful and connected as any PC or laptop. Take the same precautions on your mobile device as you do on your computer with regard to messaging and online safety. The first step is STOP. THINK. CONNECT.

Keep a Clean Machine

Mobile devices are computers with software that need to be kept up-to-date (just like your PC, laptop or tablet). Security protections are built in and updated on a regular basis. Take time to make sure all the mobile devices in your house have the latest protections. This may require synching your device with a computer.

- **Keep security software current:** Having the latest mobile security software, web browser, and operating system are the best defenses against viruses, malware and other online threats.

- **Protect all devices that connect to the Internet:** Computers, smartphones, gaming systems and other web-enabled devices all need protection from viruses and malware.

Protect Your Personal Information

Phones can contain tremendous amounts of personal information. Lost or stolen devices can be used to gather information about you and. potentially, others. Protect your phone like you would your computer.

- **Secure your phone:** Use a strong passcode to lock your phone.

- **Think before you app:** Review the privacy policy and understand what data (location, access to your social networks) the app can access on your device before you download.

- **Only give your mobile number out to people you know and trust** and never give anyone else's number out without their permission.

Connect with Care

Use common sense when you connect. If you're online through an unsecured or unprotected network, be cautious about the sites you visit and the information you release.

- **Get savvy about Wi-Fi hotspots:** Limit the type of business you conduct and adjust the security settings on your device to limit who can access your phone.

- **Protect your $$:** When banking and shopping, check to be sure the site is security enabled. Look for web addresses with "https://" which means the site takes extra measures to help secure your information. "http://" is not secure.

- **When in doubt, don't respond:** Fraudulent texting, calling and voicemails are on the rise. Just like email, requests for personal information or for immediate action are almost always a scam.

Be Web Wise

Stay informed of the latest updates on your device. Know what to do if something goes wrong.

- **Stay current. Keep pace with new ways to stay safe online:** Check trusted websites for the latest information, and share with friends, family, and colleagues and encourage them to be web wise.

- **Know how to cell block others:** Using caller ID, you can block all incoming calls or block individual names and numbers.

- **Use caution when meeting face-to-face with someone who you only "know" through text messaging:** Even though texting is often the next step after online chatting, it does not mean that it is safer.

Be a Good Online Citizen

It is easy to say things via phone or text message that you would never say face to face. Remind your kids to maintain the same level of courtesy online as they would in the real world.

- **Safer for me and more secure for all:** What you do online has the potential to affect everyone - at home, at work and around the world. Practicing good online habits benefits the global digital community.

- **Text to others only as you would have them text to you.**

- **Only give your mobile number out to people you know and trust** and never give anyone else's number out without their permission.

- **Get permission before taking pictures or videos of others with your phone:** Likewise, let others know they need your permission before taking pictures or videos of you.

MOBILE PARENTAL CONTROLS

Parental controls aren't limited to just computers. Mobile devices have evolved into Internet-ready tools that can perform a variety of tasks. Enable mobile parental controls to ensure a safer, more secure online experience for your children.

Mobile phone service providers have different options for controlling privacy and usage, filtering content and location and monitoring settings.

- **Usage controls:** Most companies will allow parents to turn off features, such as downloading videos or images, texting, and accessing the Internet. These controls can also be used to limit the number of calls or texts and set time restrictions.

- **Content filtering:** These controls can block certain websites to allow for safer mobile browsing on the Internet. Some filters can also limit videos and other multimedia.

- **Location and monitoring settings:** These controls allow parents to track their child's whereabouts using GPS systems that are built into the phone.