Keeping Your Family Safe in a Highly Connected World

Marie Baker
Jonathan Frederick

August 2011

Table of Contents

Executive Summary

As our world becomes highly connected where endless data is just a click away and using networked devices has become almost a necessity, protecting your personal information and family privacy is of great concern. Because of the anonymity provided by networked devices, our families are more likely to be attacked, be victims of theft, be subjected to inappropriate people or materials, or become involved unknowingly in illegal activities over a networked device than they are in person. Children are even more vulnerable and need greater protection because they are less mature and use some networked devices and online applications more skillfully and comfortably than their parents or guardians.

This document discusses various dangers to be aware of and safeguards to reduce the risk of these dangers. First, multiple concepts dealing with education and awareness are defined so that parents and guardians understand what they or their children may encounter and how to deal with it. Next, technical tools are described that can help parents and guardians limit what children can and cannot do and monitor their activity. Additionally, technical tools are recommended that can mitigate the personal computer threats that endanger both adults and children. Finally, threats and safeguards are discussed that are unique to mobile devices and video game consoles that have been networked to play online.

Introduction

Purpose and Scope

The purpose of this document is to increase the awareness of current cyber communication trends, their associated dangers, and techniques for mitigating their associated risks. Because members of a household have the desire or need to stay in communication with others through various mediums and electronic forms, parents many times are behind the curve of where their children are with technical know-how. Parents, guardians, and teachers can better protect young users if they familiarize themselves with how these current networking tools and applications are used, know what things to watch out for, and learn what they can do to achieve a safe computing environment.

The scope of this document does not include specific details on how to lock down or safeguard your computer or other device. Many resources are available that provide operating system or application-specific instructions on how to protect your computer or other device. The main focus of this document is to make you aware of threats you should consider when interacting with the cyber world and safeguards for protecting against them.

Audience

The primary audience for this document includes parents, guardians, and teachers of young children and teens actively using any type of technology for online activities such as social networking, file sharing, and gaming. This document was written to help adults keep young ones safe online while still allowing them to get the most from their online experiences, whether for communication, education, or entertainment purposes.

Document Structure

This document has four sections, each concluding with a comprehensive checklist of the topics discussed in it. The document concludes with an Additional Resources section that contains pointers to suggested websites and links to additional information on the tools mentioned.

- The first section, Education and Awareness, introduces the first and most important step in safe computing. For many threats, there are no magic applications or tools that can guarantee safety; education and awareness are the only safeguards. This section discusses several popular or common threats and ways to identify and avoid them.
- The second section, Monitoring Activities and Filtering, discusses ways to monitor your home users' activities and techniques for restricting the content they can access.
- The third section, Personal Computer Technical Threats and Safeguards, describes safeguards that can reduce a computer's risk of being infected by viruses, malware, and other malicious content.

- The fourth and final section, Other Technologies, presents common threats associated with mobile devices and video games and describes what you should consider in order to defend against them.

Education and Awareness

The first and most effective way to ensure smart, safe computing is through education and awareness. All users must have a good understanding of the dangers of online activities and what it means to be an aware, responsible user. Education and awareness is imperative: it is the foundation for building trust and confidence in users and their computing environment. And it is the only defense to many of today's threats, yet it is commonly overlooked or not taken seriously.

It is easy to tell children something and then watch them nod in understanding and agreement. But how can parents or educators ensure that the message was comprehended or actually "sunk in," and that the child will make smart, conscious, thoughtful decisions in varying situations? Unfortunately, most lessons are learned through experience; everyone must "touch the stove" for themselves. When it comes to personal risks such as protecting privacy or online predators, we want children to avoid learning through experience.

Several real-world examples of personal compromises can be found with a simple Internet search, many of which are highlighted throughout this document. To make a child aware of online dangers and educate them on ways to protect themselves, consider using actual real-world examples of what somebody else went through to help them better relate. What happened to this user? Why did it happen? What could that user have done to avoid the situation? What were the consequences or repercussions?

In addition, resources are available to help initiate discussions of Internet, mobile phone, and gaming dangers with children. These resources include scenarios or specific situations that can be presented to young users to help them work through the best choice or action to take. They come in several forms including videos or "What Would You Do" situation card games, which are fun activities for younger children to engage in while learning important lessons. The Additional Resources section contains links to several cyber safety sites with educational resources.

Age-Based Education

To effectively educate users, their age, experience with technology, and comprehension ability must be considered. Some children who started using computers at a very young age are much more advanced than others. In addition to the appropriate subject matter and language, children's sensitivity and level of understanding are important considerations.

When young children begin using computers, supervision is required to avoid their inadvertent exposure to inappropriate content or websites. Even innocent search terms for child-related content may return a not so child-friendly website. Consider keeping the computer in a family-centric area of the home, as well as using child-friendly search engines for younger children and even preteens. Doing so will allow easier adult supervision, while still allowing the independence that preteens typically desire.

Many of the sites that offer tutorials, videos, and interactive games, cater to children of all ages. Some of these sites provide videos for parents and advice on how to talk to children about online safety. The federal government and the technology industry put together one such website: http://www.onguardonline.gov. This site contains numerous free educational topics in the form of videos, games, and articles, as well as tools for helping adults educate children on cyber safety.

Preteens and teenagers want to constantly have access to, and be communicating on, the Internet and the devices that allow unlimited access are readily available. Safe use, privacy, education, and awareness are important for teens to understand and exercise because social networks and other applications will almost certainly play a major role of their everyday lives. While safeguards and monitored use are possible, teens may seek out ways to avoid them. In addition, numerous tools can help teens disguise their activities and discover any parental controls that may have been put in place.

As real-world examples show, many teens have suffered negative consequences from not practicing smart, safe, social-networking practices. Teens may be able to better relate if they are shown news articles about peers whose internet carelessness or naivety caused them embarrassment or loss of privacy or possessions, or made them the victim of a horrible crime. Discuss with them why these consequences occurred and what could have been done to prevent them. Then follow that discussion with guidelines and safe use practices your teen must follow. Educational resources geared towards teens are also readily available. Many of the sites listed in the Additional Resources section have content sections divided by age group.

Privacy and Personally Identifiable Information

Information, personal or not, that individuals post to the Internet, whether through social networking or activities such as online shopping, is no longer private information or even data that the individual owns. Once something is released online—pictures, blog postings, email, etc.—it is virtually impossible to take back. Nearly everything that is posted on the Internet lives online forever.

Personally identifiable information (PII) is information that can be used to identify an individual through unique facts about him or her. There are several uses and misuses of PII. Websites collect PII through online forms where users enter their information and through cookies where information can be gathered from browsing and online activities. This collected information is then used for marketing or sold to a third party.

Social-networking sites are a gold mine of PII. People intending to share information such as their vacation plans, school activities, or new purchases with friends and family are actually sharing it with a large network of people. Unfortunately it is not uncommon for people with malicious intent to use this information to coordinate illicit activities such as stalking, blackmail, theft, identity theft, or worse.

A Florida couple posted their vacation plans as well as vacation status updates and photos on their Facebook page. They returned home to find $30,000 worth of possessions stolen.

http://mycodetrip.com/2010/11/25/couple-post-vacation-photos-on-facebook-come-home-to-find-30000-worth-of-jewelry-electronics-stolen_693/

Users may believe they are not revealing information that could identify themselves or be used for devious purposes, because they were careful not to disclose information unique to them such as their social security number, birthday, or address. However, combining multiple pieces of generic information such as gender, race, school attended, or job position may be enough to identify or exploit someone.

Many sites require registration or a subscription to obtain a service. Registering/subscribing entails entering personal information in an online form. Before filling in these forms, know how personal information will be used. Many sites use it for marketing purposes or sell it to a third party for their marketing and research purposes. Be sure that children are aware of these forms and what information is permissible to disclose, or preferably, have an adult review the form and then complete it together with the child.

In April 2000, the Children's Online Privacy Protection Act (COPPA) federal law was enacted. It applies to websites collecting information online from persons under the age of 13 within the U.S. The act outlines

- the responsibility of the website owner to protect children's privacy and disclose how the website may use personal data obtained from a user 13 years of age or younger
- valid ways for the website to obtain parent or guardian consent

Because of COPPA, social-networking sites such as Facebook and Myspace do not allow children under the age of 13 to join. However, children can find ways around that rule simply by lying about their age. External organizations have placed pressure on these sites to audit accounts and remove those of underage users, but that is an insurmountable task for any site no matter how many resources they can dedicate to it.

While laws are in place that require organizations to protect personal information, such as the Health Insurance Portability and Accountability Act (HIPAA) aimed at protecting patients' care records, there are no laws against or expectations of privacy or protection from misuse of information that was posted by individuals voluntarily or unsolicited. If a user uploads a picture to a social-networking site, someone else has the ability to take that picture and repost it as they desire. Any comments, status updates, or videos someone may have posted to share with friends and family may be duplicated, edited, reposted, or misused elsewhere. When online, be mindful of groups joined, opinions expressed, and statements made in haste. These words or actions can have adverse consequences.

Avoid letting adolescent indiscretions impact adulthood. Teens and young adults especially, need to be conscious of this. When applying for college admission or employment, employers or admission offices may do an online search to see if there is more to learn about an applicant than what was disclosed in an interview or application. It would be unfortunate for a person to be judged on something that he or she posted years ago and that now seems immature or insensitive, or be rejected because a profile page on a social-networking site contains risqué photos and conversations.

A 2009 survey from CareerBuilder.com found that 45% of hiring managers use social-networking sites to research job candidates. As many as 35% found content that caused them to reject the candidate.

http://thehiringsite.careerbuilder.com/2009/08/20/nearly-half-of-employers-use-social-networking-sites-to-screen-job-candidates/

Encouraging Reporting

Communicate your expectations to young users regarding online behavior and the consequences of violating those rules. However, if a child encounters something inappropriate online, they should feel comfortable confiding it to an adult. Discuss how it may have happened and how to prevent it from occurring again. Reward children and provide positive feedback. Make them feel that disclosure to an adult after the discovery of something suspicious was a mature decision and played a crucial role in protecting the home-computing environment and its users.

It may be appropriate, depending on the situation, to alert school administrators or even local authorities. Cyber bullying, stalking, or other types of electronic harassment may need immediate attention to ensure personal safety. Keep situations from escalating to the point where there is damage to feelings, relationships, or personal property.

External reporting to Internet entities may also be necessary. Internet service providers (ISPs) and email service providers such as Google encourage the reporting of suspicious activities or abuse including spam and compromised accounts. Know your ISP (e.g., Comcast, Verizon, Time Warner) and how to contact it to make a report. Microsoft products such as Internet Explorer and Hotmail have options in the menu bar to report unsafe websites and email scam attempts. There are also websites that investigate and report details of hoax emails and scams. If your child receives a message that warns of something, requests that some action be taken, or makes you feel uneasy, investigate its validity by visiting a site such as http://www.snopes.com/ that researches email hoaxes, rumors, and misinformation.

Legalities

Legalities in the arena of computing and online activities are commonly known as cyberlaws. Cyberlaws and regulations are legal issues related to computing devices and online activities in an effort to protect individuals' privacy, property, and legal rights. Many of these laws are new and still evolving; however there are some situations in which precedents have not yet been established. Also, some traditional laws have been amended to include electronic activities such as stalking and harassment.

The term Cyberlaw is used broadly and is not a specific field of law such as estate law. The term includes many areas of law and regulation such as jurisdiction and intellectual property. In addition, Information Technology (IT) law governs how information is processed and disseminated digitally. IT laws cover many areas including software protection, Internet usage, access of electronic information, and privacy.

Laws certainly apply in cyberspace, but under what jurisdiction? Electronic transactions and communications may involve servers in other states or even other countries. Usually, the laws of the location where the communication was initiated are enforced, and the Internet is considered a form of interstate commerce. Any illegal activities that involve Internet use will be considered a threat over interstate lines. The difficulty arises when the Internet communications involved in the illegal activity are international. The laws in different countries vary as to what is deemed illegal.

Be conscious of legalities and cyberlaws because young home users, especially teens, may be involved in activities such as cyberbullying, stalking, file sharing, or attempted cyber attacks. Users can and will be prosecuted for participating in these types of cybercrimes, some of which are discussed further later in this document. Make sure children understand the seriousness and possible consequences of their actions.

A 14-year-old New Jersey boy faces charges of harassment and making terroristic threats for allegedly threatening two 12-year-old boys on Facebook.

http://www.nbcnewyork.com/news/local/117966829.html

Cyberbullying

The days of children writing notes to each other during school and talking on their parents' home phone in the evening is a thing of the past. In the current information and social-networking age, most teens and tweens have their own cell phone and home computer. They communicate with each other via social-networking sites, blogs, and Twitter. Today's kids can easily form relationships with more people than just their classmates at school during school hours. Communication that was traditionally contained within schools or neighborhoods is now exchanged worldwide. Socialization—good, bad, or indifferent—is now done electronically and is accessible anywhere 24 hours a day. Because communication is no longer just face to face, children and young adults can no longer escape from it at home.

Cyberbullying or cyber harassment are electronic forms of bullying and harassment. They typically entail threatening or harassing texts, emails, instant messages, blog and chat postings, or websites used for the sole purpose of tormenting an individual. Cyberstalking is another form of electronic harassment and probably the most serious. Several states have laws tied within traditional harassment and stalking laws to include the electronic forms of these crimes.

Because schools have made a concerted effort to crack down on traditional bullies and educate students about them, cyberbullying is frequently included in schools' policies and education. Even if cyberbullying did not originate on school property, it can disrupt and have a negative effect on the learning environment.

Online bullying has the same effects on an individual as face-to-face bullying. The embarrassment, humiliation, isolation, blows to self-esteem, and other negative effects a person may feel can be even more damaging electronically, since a larger audience has the potential to view or participate.

Education and awareness are the only defenses against cyberbullying. This defense strategy is most effective when approached as individualized education with varying levels of sensitivity, and depends on whether the child is the victim or taking part in the bullying. Some individuals have thick skins, while others may need to have frequent discussions and be assured more aggressively. Talk with children about the negative effects of bullying and ask them how they would feel if it happened to them. If it's age appropriate, cite specific examples of bullying from the news where bullied people have retaliated violently or even committed suicide. Children are more likely to say or do things online that they would not say or do in person. Help them to keep in mind that profiles and screen names are real people with real feelings.

Nine teenagers have been charged with bullying a 15-year-old girl at school, using text messages and Facebook. The bullying caused the girl to commit suicide.

http://abcnews.go.com/Technology/TheLaw/teens-charged-bullying-mass-girl-kill/story?id=10231357

Copyright Infringement

According to the U.S. Copyright Office (http://www.copyright.gov), copyright infringement occurs when a copyrighted work is reproduced, distributed, performed, publicly displayed, or made into a derivative work without the permission of the copyright owner. It is important to note that copyright, as a legal term, is automatically established when a creative work is created; no registration or other act needs to occur for something to be protected by copyright. The copyright symbol and date are used to identify the copyright owner and date of creation, not establish copyright protection.

Copyright infringement occurs frequently with the Internet because there is an endless supply and availability of electronic copyrighted material. Music, movies, and books are downloaded thousands of times a day by thousands of people. Not all of these people are downloading them legally or obtaining these materials from a legitimate source. What seems to be misleading, especially for younger people, is that just because content is available for free downloading on the Internet, it might not be legal to do it.

There are numerous music- and ringtone-sharing websites that are frequented by teens and young adults. Large digital libraries containing the latest popular song, new movie releases, games, or trendy alert tones are just a click away. However, the original creator or author is protected by copyright laws. In many cases, music companies and movie studios have sought financial compensation from users who have illegally accessed or distributed their copyrighted work.

The first online copyright infringement case to go to trial in the U.S. was against a 32-year-old woman from Minnesota in June 2009. She was accused of downloading 24 songs illegally. She was fined $80,000 for each song for a total fine of $1.9 million. Even though you can download songs for less than a dollar each, the music industry takes into account what they believe they may have lost in royalties. Several cases have been filed since then as the music and movie industry aggressively work to publically make an example of a few individuals to discourage illegal downloading by others. If you want a song on your MP3 player, the only legal way to get it is to purchase it through one of the many online legitimate music distributors or copy it from a CD you purchased.

The good news is that the trend of downloading illegal music or movies is declining. Services such as YouTube allow searching for popular songs and watching a music video for free as many times as desired. Other services, such as Grooveshark and Pandora, stream music that can be listened to for free. There is no need to illegally download and store the music files. The same concept is true with similar services for watching movies or TV shows.

A federal judge approved the U.S. Copyright Group's request to subpoena ISPs in order to recover the identities of individuals who downloaded a major motion picture film illegally. Each of the 23,000 defendants faces a maximum penalty of $150,000 per offense.

http://www.huffingtonpost.com/2011/05/10/expendables-bit-torrent-download-case_n_860048.html

File Sharing

Obtaining and sharing illegal copyrighted material is typically done through file sharing using peer-to-peer network applications. The application connects a user's machine (peer) to another user's machine (peer) and enables the downloading of shared files. While file sharing is not illegal if it involves files created by the user, it can be dangerous because a good percentage of content shared by file-sharing programs is malware or malicious in nature. The ignorance of users may also lead them to unintentionally allow others to access their personal data.

If users in the home are using peer-to-peer file sharing, be sure there is a legitimate, legal reason for it. If file sharing is legitimately needed, there are several other ways to share files without enabling file sharing on a machine through peer-to-peer applications and making it vulnerable to potential attacks. A safer, simpler alternative to file sharing is to use removable storage devices such as CDs, USB flash drives, or external hard drives. Simpler yet is the use of file-hosting services.

File-hosting services allow online electronic storage and the exchange of files. Web links to request file downloads or uploads via applications like email or forums are examples of file hosting. File hosting ranges from no charge for individuals who store and share individual small files to subscription services for companies requiring larger amounts of storage typically for backups or other business needs.

Regardless of the way files are shared, one important thing must be kept in mind: viruses. Be cautious of the file's source and content. Be sure to scan any file before copying it from removable media or executing a file downloaded from an online source. Threats from viruses and other malware will be discussed more later.

Awareness

Awareness efforts aim to change behavior and reinforce desired practices. While these efforts can be carried out in many ways, they ultimately rely on good communication. Whether that communication consists of repetitious reminders and stimulated discussions or written reinforcements, it must be audience appropriate and easily comprehended to be effective. Many times, awareness relies on using attention-grabbing, real-world scenarios and consequence details in order to reach users of all ages.

Awareness is especially important when it comes to cyber safety. It's the only defense against many of the dangers of the cyberworld. Prepare home users to be diligent in protecting themselves against these risks, to identify them, and to know how to react if they become a victim. For the most effective results, be diligent with education and awareness, and enforce rules and best practices using the many training resources available. Awareness is the what, education is the why, and training is the how.

Managing and Protecting Passwords

Passwords, passcodes, or PINs are required in many places in our everyday world. In addition to needing a password to unlock a computer or cell phone, you also need a password for many websites used for online banking, shopping, checking email, and social networking. As online memberships or registrations are expanded, it becomes increasingly difficult to manage all of these passwords. Conscientious password creation and management is very important, but it is frequently thought of as burdensome and ignored or neglected. It is common for users to use the same password for multiple sites. For instance, children will use the same password for email, online games, and important school files or websites. Another common risk is using passwords that are easy to recall and therefore easy to compromise. Some users mistakenly use personal information or the name of a specific site. An example would be using the password *amazon* for the shopping site amazon.com. While that password is easy for the user to recall, it is also easy for the hacker to guess. Passwords do not have to be hard to remember, just hard to guess.

Several techniques can help with password management and secure password creation. Use a different username and password for each site and purpose. If one account is compromised, it will not put all accounts at risk because the same password was used everywhere. A good way to help manage all of these credentials and where they are associated is to use a password management application. Password management applications are password-protected tools that allow the storage of all usernames and passwords and where they belong. This allows a user to have different passwords for each site without being tempted to write them down anywhere, and the user only needs to remember a single password—the one for the password management application. Several free password management applications are available for download. For instance, Password Safe and KeePass can be used freely and will protect all passwords using strong encryption. Such programs eliminate users' temptation to create weak passwords in the fear that they will forget them.

Password protection is important for all family members. Children having passwords that are easy to guess can lead to trouble with social-networking sites, online gaming, or even identity theft. Teach children that passwords are never to be shared and how to create strong passwords. Strong passwords are at least 8-12 characters long—the longer the better. Use a mix of letters—upper and lower case, numbers, and punctuation. Do not include any personal information or words that can be found in a dictionary. Another good tip is to use a phrase and mix in characters. For instance, soccer ball converted to *S0cc3rb@11* is a strong password, or *ILikeToKickMySoccerBall* is an example of a strong passphrase. For additional help, search the Internet to find dozens of free password generators. A link to one of these password generators is listed in the Additional Resources section of this document. Creating strong passwords can be fun and easy, while increasing safety.

Barack Obama, Britney Spears, and other celebrities allegedly had their Twitter accounts hacked after an attacker was able to guess their passwords.

http://www.metro.co.uk/news/world/819061-barack-obamas-twitter-account-hacked-after-password-guessed

Social Engineering

Unfortunately, there are no protective applications or tools for many of the Internet threats. In fact, most attacks are nontechnical; they simply take advantage of the naïve user and information that is readily available. And even though these attacks are not sophisticated, they are very successful. These types of attacks are known as *social engineering*.

Social engineering is the act of preying on individuals in an attempt to get them to reveal personal information or provide access. Again, it requires little-to-no technical know-how by the aggressor. The predator simply tricks or otherwise convinces the honest, trusting user to provide personal information or complete an act such as visiting a website and downloading an infected file. Social engineering plays on the human desire to help others in need, or the urgency to act in order to avoid negative consequences or receive personal gain. This type of manipulation attack can be accomplished in various ways and used for various deceptions.

A common form of social engineering is spam. Spam is any unsolicited form of communication. Spam emails often describe an offer too good to ignore or detail some urgent threat that requires immediate attention. Inboxes fill quickly with this junk email, but it can also be received via text, social-networking forums, fax, and regular mail. Spam and other email filters may be set up and working properly, but they will not catch every piece of spam mail every time. The filters can also incorrectly identify valid emails as spam, causing you to miss legitimate correspondence.

Phishing and Spear Phishing

Phishing, another approach to gaining personal information from individuals, is done by masquerading as a trusted entity. Phishing is also a form of social engineering. An example phishing attempt would be an email that arrives in the inbox that looks to be from the Internal Revenue Service (IRS). The email claims that there is a problem with a recent tax return and the user needs to logon to the IRS's website and verify information. The email contains a handy link for the user to click to go directly to that site, and that linked website will, of course, be made to look identical to a legitimate website. Following through with this solicitation could reveal and compromise a username and password or other personal information. When you receive a suspicious communication, think before acting on it, or confirm the legitimacy through other channels. Spear phishing is a form of phishing that targets specific people or groups with specific interests such as politics, celebrities, or sports.

Again, the only protection from falling victim to a phishing attack is awareness. Constant reminders of their existence and dangers, or even bringing a suspicious email to everyone's attention for reinforcement will help. Do not open attachments or click on links contained in email from unknown people. If you receive an email from what looks like a legitimate company, double check that it truly is from that company before taking any actions.

> Federal Express and UPS customers have reported receiving emails claiming to be from the shipping companies, warning them that a package went undelivered and asking for information. Or the customers are sent an attachment to print out, but when they click on it to open the file, a virus is downloaded.
>
> http://www.walletpop.com/2010/12/19/phishing-scam-uses-ups-fedex-notices-as-bait/

Online Predators

The "Stranger Danger" warnings everyone is taught as a child also apply in cyberspace. It is much easier for child predators to deceive children when hiding behind a computer. There, predators have anonymity and can be whomever or whatever they want to be. Predators are good at deceiving and manipulating children to the point where they lose their sense of awareness. Children become victims by trusting this new "friend" who claims to have the same interests, listens to and sympathizes with their problems, and pretty much tells the victim things they want to hear.

The growth and popularity of social networking and the ease of searching profiles have made it easier for predators to find victims. Young users reveal personal information about themselves without considering their safety. There seems to be a trend among teens using social-networking forums to report their every thought or minute details about their day. These revelations along with what school they attend, sports or other activities they are involved in, or posted pictures gives a predator a good synopsis to help them initiate their targeted conversation with the young user. Once the online relationship grows to the point where the young user is trusting and openly communicating with the predator, the predator may initiate the exchange of pornographic images and scare or blackmail the victim into participating.

Again, the only defense against this type of threat is awareness. Talk to children about communicating with strangers online. Watch for warning signs that may indicate a young user has become the victim of a predator. Some of these indicators include finding pornographic images on the computer, noticing that the user quickly changes computer screens when someone approaches, or noticing that they seem to act withdrawn. Closely monitor your children's computing activities; monitoring will be discussed in a later section.

Using a fake Facebook account, a 43-year-old man created a persona, became online friends with several teenagers, and coerced and then blackmailed them into sending him nude photos of themselves and others.

http://www.wtae.com/news/28028464/detail.html

Facebook and Myspace

Social-networking sites such as Facebook and Myspace are used for sharing pictures, videos, and other files among friends, family members, and acquaintances.

While social-networking sites were intended to be positive tools, their use for negative or malicious purposes is almost as popular. Cyberbullies, cyber stalkers, and online predators are just a few threats that have increased with the growing popularity of these sites.

Facebook and Myspace will not accept registration from anyone under the age of 13. This restriction is due to the Children's Online Privacy Protection Act, which dictates that websites cannot collect personal information from children younger than 13 without parental consent. Because it is difficult to verify consent, sites have chosen to simply prohibit underage users. While the policy banning young users appears to help parents to protect their children from potential social networking dangers, that is not the case.

Besides children being dishonest about their age on their own, many parents are assisting their children in registering on social-networking sites. A survey conducted by the Pew Research Center in mid-2009 found that 38 percent of 12-year-olds in the U.S. were using social networks. Facebook investigates reports of underage account holders and deletes around 20,000 accounts per day, but it is nearly impossible to manage the volume of policy violations.

Parents may not realize the potential threats of exposing their child to this digital world. Also, they may find that nearly all of their child's peers are users of these social-networking sites and therefore also permit their child to use them at home. Again, education and awareness are the only safeguards for protecting users actively involved in social networking.

Discourage underage users from being dishonest and registering on these sites. Young users who are registered on a social-networking site should have their profile set to private where only confirmed friends can visit. As with all online activities, parents will want to monitor what content is posted or shared, and who their children are communicating with. Regularly discuss posting personal information, posting inappropriate content, and meeting strangers online. It is disheartening when bad people try to exploit and ruin a good thing, but with awareness and diligence, social-networking sites can be a safe and positive experience.

Meeting Face to Face

There are news reports too often about children, most frequently teenage girls, who have been reported missing. In many of these reports, it was not a circumstance of forced abduction but rather a case where the teen went willingly to meet in person someone they met in cyberspace. Even though the child exercised poor judgment and willingly went to meet this person, it is against the law for strangers to entice or "lure" children they meet online. Have discussions with children about the dangers of meeting people online and disclosing personal information to strangers, and monitor their email and chat activities. Know who children are communicating with. If you suspect suspicious conversations or other threats to a child's safety, contact law enforcement.

> Parents of two girls who ran away with a man in his 30s suspected right away that they met him over the Internet.
>
> http://www.daytondailynews.com/news/dayton-news/parents-suspect-runaway-teens-met-man-on-internet-148552.html

Education and Awareness Checklist

□ Initiate discussions of cyber safety frequently. Get all family members involved by discussing current events, and use scenarios or other tools to help with interaction.

□ Be sure that your discussions and the educational tools you use are age appropriate to ensure impact.

□ Monitor children's computing activities and ensure they are not revealing personal information.

□ Discourage home users from participating in cyberbullying or harassment. Teach them how to recognize and report these cyber threats.

□ Educate users on the legalities of sharing music, videos, and other copyrighted material.

□ Encourage all home users to practice good password creation and management practices.

□ Be diligent and have regular discussions regarding social-engineering threats.

□ Stay actively involved in children's social-networking activities. Know who they are communicating with and the type of content they are viewing or sharing.

□ Abide by websites' policies prohibiting underage users.

Monitoring Activities and Filtering

Education and awareness are the fundamental pieces of cyber safety. However, no matter how well versed household members are on the threats of the digital world, it is inevitable that one of them will make a bad choice or ignore a best practice. Adults cannot be available at all times to supervise every user's activities. This is where monitoring and filtering are invaluable.

There are several ways to monitor children's activities on a computer when an adult is not in direct supervision. This activity does not necessarily have to be considered playing "big brother" instead, it can help ensure that others are using the computer in a safe, smart, and secure way. Confirm that measures for achieving a safe computing environment are effective.

Parental Controls

Parental controls are optional features or automated tools used to enforce restrictions while using services or devices including computers, cell phones, and televisions. Restrictions can include the types of websites that can be viewed, the television channels that can be watched, or limitations on how long the devices can be used.

OpenDNS

OpenDNS is a free DNS resolution service and content-filtering system that can be easily set up without special software. Essentially, instead of using the home network ISP's DNS servers to locate websites, configure the home router or web browser to use OpenDNS servers. OpenDNS includes faster name resolution (website locating) and additional features such as phishing protection and URL misspelling correction.

FamilyShield is a free parental content filter from OpenDNS that was launched in June 2010. It uses the OpenDNS servers previously mentioned, while also blocking adult websites, some phishing and dangerous malware sites, and finally proxy and anonymizer sites that kids may try to use to get around the content filter. In addition to filtering and protecting desktop computers, FamilyShield blocks content on all wireless devices used to access the Internet such as iPods and video game consoles that are configured on a home network's wireless network.

For more information on OpenDNS and FamilyShield including how to set up the free service, go to http://www.opendns.com/. *The New York Times* published an article about OpenDNS titled "Simplifying the Lives of Web Users" in August 2010. The reporter reviews OpenDNS and simplifies its functionality so that everyone could understand OpenDNS' capabilities.

Browser Control

Another form of filtering is through browser controls and the use of child-safe search engines or whitelisting. Some browser controls are built into web-browsing applications. For example, Internet Explorer has a Content Advisor you can use to deny access to specific websites and restrict access to content such as nudity and violence. The settings are secured using a Supervisor password so that other users cannot change or disable them.

Whitelisting is a term used to describe an approved or accepted list of some entity such as email addresses or websites. For example, if filtering is set up in the web browser, the permitted sites appear on a whitelist; those filtered out or blocked would be considered *blacklisted*. Plugins are available for web browsers, as well as free applications, such as KidZui, that provide a child-safe internet front with a significant whitelist of websites.

Another way to filter out undesired web content is using child-safe search engines like RefSeek and Yippy, rather than the more common, well-known search engines that don't allow parents to control or anticipate all the results returned. These kid-friendly search engines have filtered out sites that contain content parents and teachers may find inappropriate for children. A few are even free of advertisements.

Using a combination of browser controls and child-safe search engines, along with parental supervision is a very strong defense against offensive content reaching young users. A more robust filtering tool such as FamilyShield, discussed previously, is probably required for the older, more computer-savvy user who may know how to get around or disable these controls.

Key Loggers

Keylogging, is capturing (usually covertly) the key strokes of a user. A similar technique, screen scraping, captures visual activities from a user. Key loggers are typically software applications installed on a computer, although there are hardware versions as well. Generally, logging applications run in the background without the user's knowledge, recording activities the user performs while operating the computer. The recordings can be played back as a video file with the ability to rewind, fast forward, pause, and so forth. If a password or other text was entered that does not display in clear text on the screen, it can be displayed using one of the recording application's special options.

While users won't notice the capturing of their activities by the application, they might notice that over time the computer operates more slowly. Since these activity captures are video files that are recorded and saved on the computer, they will begin to take up hard-drive space. They may even slow other processes as the application runs in the background. For this reason, it is a good idea to frequently view and delete these video files and only save what is absolutely needed. Some key-logging applications will send the data to another machine and even send email notifications. These more sophisticated options are probably not practical for the home user.

When selecting a key-logging application, make sure it is from a legitimate source. Installing a keystroke-capturing application that is actually from someone with malicious intent could be devastating. Referencing the highlighted article from "Webcams," the attacker was able to take control of the user's computer and webcam, and capture passwords because the user unknowingly installed a malicious key logger. Use a legitimate cyber safety website, such as http://kids.getnetwise.org that provides details of available tools and guidance on selecting a key logger or other monitoring application.

Because key loggers run covertly and save all activities and keystrokes including passwords, privacy issues and the ethical ramifications of such user monitoring will need to be considered. Should users be informed that their computing activities are being monitored?

Log/History Audits

Besides using software that will monitor and record all user activity, activities can also be investigated using system and application logs. The operating system, as well as the applications installed on a computer, may store data regarding the user's computing activities. For instance, the history of a web browser stores the details about each visited website. This data can be located in temp, cache, and cookie files of the associated browser. Of course, it is possible to delete these history files, and many savvy users may do just that.

One of the administrative tools included in Windows operating systems is the security log, which is used to investigate activity and troubleshoot problems. Events that can be set up to be logged include account login attempts, accessed applications, and policy changes. If you follow safe computing best practices, don't give user accounts administrative privileges, and allow users to only use their own account, monitoring activity and accountability becomes much easier. The use of individual user accounts also allows customized restrictions for each user. For instance, the web browser for a younger child's account can be configured to use whitelists and child-safe search engines.

A challenge in monitoring activities of today's teens may be understanding their language. When reviewing logs from an instant chat conversation or text messages, you might encounter abbreviations such as GTG and POS. Many adults are not familiar with adolescent messaging slang, making it difficult to monitor conversations and activities. GTG can be translated to Got to Go, while POS means Parents Over Shoulder. Several websites are great resources for helping adults translate these abbreviations. Groups such as the National Center for Missing and Exploited Children and the Partnership for a Drug-Free America list slang terms on their websites including those specific to drug or sexual activity. "Additional Resources" lists a few of these useful sites.

Logging and history audits can be performed for varying activities and applications. Depending on the desired information, monitoring can begin on the home router viewing all incoming and outgoing traffic, all the way down to individual applications on the networked devices. Parents can determine the degree of log and history review required, based on the user and their risk or exposure potential.

Monitoring and Filtering Checklist

□ Configure parental controls and use child-safe search engines to limit the websites and other content that young household members can view.

□ Consider using a content-filtering system such as OpenDNS that will protect all home devices that access the Internet from malicious content.

□ To capture computing activities as a way of thoroughly monitoring users, install key loggers or similar capture software **from a legitimate source**.

- □ Use individual accounts for each user and review history files and event logs to audit each user’s activity.

Personal Computer Technical Threats and Safeguards

In the previous sections, we talked about protecting against human or content-related threats. In this section, we focus on protecting a personal computer from threats that are more technical in nature. While education and awareness are important elements in defending against these threats, they are not foolproof, and technical safeguards need to be applied to ensure greater protection. For the purposes of this document, technical threats are those that modify the personal computer in an undesirable manner to benefit the creator of the threat. They are typically pulled down from the Internet or an attached device either inadvertently or after the user is tricked into downloading through social engineering as previously described in “Social Engineering.” However, they can also be initiated by a malicious external party without requiring any actions from the computer user. We will describe some of the safeguards necessary to defend against both of these user-initiated applications or content, as well as those that are initiated in other ways.

This document is not meant to cover all of the safeguards for every version of each operating system. Nor is it intended to present everything you would need to know in order to understand how each safeguard works. Instead, it will cover general categories of safeguards and the threats they defend against. You may need to conduct further research before applying these safeguards to your particular operating system.

Safeguards for Malicious Applications

We categorize a malicious application as one that originates as an executable file that is then used to install a malicious program. Most malicious applications need to be installed to ensure that they run continuously without requiring further input from the computer user, therefore allowing them to go undetected without the proper technical safeguards. The executable files are downloaded from the Internet or accessed on an external device and typically, depending on the type and version of operating system, generate an internet browser and/or operating system warning message. That message asks users if the application should be run, giving them an opportunity to authorize or decline the execution of the file. Unfortunately, research indicates that most computer users accept the warning without taking the time to read it thoroughly—thus unintentionally installing the malicious program on their computer.

As previously mentioned, malicious applications are designed to benefit the creator in some way. Many early malicious applications were designed to target personal home computers and harm them by making them unusable, thereby providing the creator with bragging rights. Today, attackers are willing to take the risk of getting caught because of the promise of a significant financial gain. Most recent malicious applications are designed to steal and report back usernames and passwords, credit card information, and any other personal information that could be used by the creator or more likely sold to other criminals.

Safeguards Prior to Execution

The best-case scenario is to prevent these malicious applications from executing in the first place, because once a system has become infected, there are a limited number of ways to clean it.

Accounts and Privileges

Unlike typical business computer users, home users can initiate the execution of any application with their default out-of-the-box user account. The initial user account created when the system is first booted up is set as an administrative account with full control to install or modify the system. However, all current home operating systems allow the creation and use of limited user accounts that are designed to allow the execution of most applications, while not allowing the user to modify the experience of other accounts or the security of the operating system. This includes installing or updating any software. Limited user accounts, also known as "guest" or "standard user," can be set up and used by those members of the family who may have less security awareness or for whom special user customizations are not required.

Parental Controls

In addition to the benefits of limiting time use and web filtering (as described earlier in this paper), parental controls can also be valuable in safeguarding against malicious applications. Most parental controls allow the system administrator to specify only the applications that specific user accounts can run. All other applications, including those that are malicious in nature, would not be permitted to execute. Setting up a standard user account with limited installation rights and parental controls allowing only specified programs to run would create the ultimate safeguard because some malicious software can execute without first needing to be installed. Individuals should create this protected user account for everyday tasks until they need to perform system updates or maintenance or install new software. Only then should they log out of the protected user account and log back in with an administrative account in order to perform those tasks.

Real-Time Scans

Various tools can perform real-time scans for malicious applications as they are executed. These scans

- compare the files themselves against files known to be malicious
- compare the actions those files take when executed against actions known to cause problems with the system

The list of known malicious files is, depending on the product vendor, called the definitions, signatures, or DAT files. This list needs to be configured to perform automatic updates at least once a day because new malicious applications are always being discovered.

Plenty of antivirus and anti-malware products are available, some for free. Many products strive to protect against the various forms of malware such as trojans, spyware, and adware. AVG and Avast are two popular free antivirus vendors, while Malwarebytes is a popular free anti-malware vendor. Many purchasable products are bundled with new systems as free trial versions. The vendors of those products pay the computer manufacturer to include their products in hopes that the consumer will purchase them after the typical limited free trial is up. This setup can create confusion with some consumers who continue to think that they are protected without first activating the free trial, purchasing the product after the free trial, or removing the software completely in order to instead run a free or purchasable product from a different vendor. Ensuring that an active product is actually running, hasn't expired, and is receiving updates is more important than worrying about selecting the "best" product.

Safeguards After Execution

No protection software is 100-percent effective. With signature-based software, there will always be a delay between the time that protection software vendors discover the malicious application and the time that a user's computer begins to protect against it. Malicious application writers also have ways of evading detection by constantly changing their application so it doesn't match those on the known malicious list. Neglecting to implement any of the previous safeguards or becoming infected with malicious applications that are not able to be caught by your protection software will allow those malicious applications to execute. At that point, the system must be cleaned to avoid further damage or theft of personal information.

Scheduled Scan

In addition to running real-time scans for viruses or malware, the tools mentioned above typically allow for scheduled scans to be run to compare file characteristics against a list of those known to be malicious. A scheduled scan is beneficial when the malicious application's actual installation file or process does not generate a product alert or action. The free version of Malwarebytes will only allow a scheduled scan and will normally discover malicious logic in places that the real-time scan of a virus scan product may have missed during installation.

Online Resources

If users can identify malicious applications in some way, such as by its name or symptoms, they can usually find some resources describing how to clean the infection. How much information is available depends on how long the malicious application has existed and how many other systems it has infected. When researching how to clean system infections, be sure to consult only the websites of reputable security product vendors in order to avoid potential new infections.

Known Good State

Assuming that a personal computer was purchased new from a reputable source or that a used computer was reconfigured back to its original new state, it should be free of malicious applications. When buying a used system, you should ensure that the seller reconfigured it back to its original state using the directions and media that were provided by the system manufacturer at the time of the initial purchase. Despite education, awareness, and additional safeguards, there will inevitably be times when a newly created malicious application executes successfully and the available tools are unable to effectively clean it. In that case, the best option is to restore the system to its known, good, original state using the directions and media provided by the system manufacturer and then immediately enable the firewall and install all of the missing updates. Continuously backing up important files is necessary to ensure that this return to the original state can be performed without losing data. Using an online storage system, a thumb drive, or external hard drive for backups can ensure that information is stored safely.

Safeguards for Malicious Content

We categorize malicious content as a non-executable file or downloadable content such as Microsoft Office and Adobe Reader documents and content from websites. Malicious content can exploit weaknesses in the software being used and open files to perform threatening actions. These threatening actions typically involve downloading and installing malicious applications previously described without the computer user's knowledge. For this reason, you must consider the content's source and ensure that the software opening the content is not vulnerable to known abuses being used by criminals or others with malicious intent. The three most popular content threat vectors are described next, as well as steps that can be taken to reduce their risk.

Microsoft Office Documents

In the past, Microsoft Office content including Word documents, Excel spreadsheets, and various others were the most heavily used attack vectors. However, over time, significant improvements were made to the way in which Microsoft applications were updated. As a result, attacks became less effective because fewer individuals were running the vulnerable and out-of-date software versions. Additionally, Microsoft made improvements to its software so it was less likely to execute code without the user's knowledge. Antivirus signature creators have also done a good job of looking at the content while it is opening and stopping it if it is deemed to be malicious. Even with all these changes, Microsoft Office content can still introduce a threat if a new vulnerability is discovered and remains unpatched, or users ignore the warning box that usually pops up advising them that the content may be suspicious.

PDFs

Adobe's PDF, or Portable Document Format, has gained popularity primarily because it is not dependent on any one operating system or platform and because its reader software can be downloaded for free. Over the years, Adobe has extended the capabilities of the format to allow a lot more than just reading written text. The latest versions of Adobe Reader software are capable of reading PDFs that can display multimedia, can be secured in several ways, and contain numerous other files and programmed logic. Attackers have used these additional capabilities as vectors to introduce malicious actions into the software. By default, Adobe Reader allows Javascript, a programming language that the attackers can use to introduce these vulnerabilities. Javascript also allows PDFs to perform some of their more advanced capabilities such as multimedia or calculations within forms. Disabling Javascript within Adobe Reader options will remove these capabilities by default and allow them to run only on selected documents, but it will also make the computer less vulnerable. Attackers can hide malicious PDFs within a website, so they are clicked on by an unsuspecting user or automatically opened by the default web browser. Setting the Adobe Reader options to prevent a web browser from automatically opening a PDF can provide users an opportunity to decline opening a document that they did not request to download. To disable Javascript and the ability to display PDFs in the web browser, follow the instructions posted at http://www.kb.cert.org/vuls/id/970180. Although these instructions are part of a solution to a 2009 vulnerability in Adobe Reader that has since been patched, following them can prevent any future vulnerabilities. Finally, ensuring that Adobe Reader options are set to automatically download and install new updates is another essential security practice.

> A March 2011 report by Symantec estimated that 65 percent of targeted attacks in 2010 were originated by malicious PDFs.
>
> http://www.messagelabs.com/mlireport/MLI_2011_02_February_FINAL-en.PDF

World Wide Web

Over its 20-year history, the World Wide Web has transitioned from simple text-only pages to the multimedia-rich content that it is today. All the advanced content that can be viewed on webpages today relies on capabilities within the web browsers or add-on software. Any discovered vulnerabilities in these browsers and add-ons can be abused by content and can allow the execution of malicious actions. For example, content can use functionalities such as ActiveX or Java. Web browsers are typically installed with the minimum level of security necessary, which increases compatibility with content across the web. These web browsers can and should have their security levels increased within the options so that users have to authorize potentially malicious actions more often to view content than would be necessary with the minimum, default level of security. For more information on securing the most commonly used web browsers, see http://www.cert.org/tech_tips/securing_browser/.

Finally, similar to recommendations for other software capable of executing malicious content, web browsers and add-ons should be updated continuously to the latest version to ensure that they are no longer vulnerable to the most recently discovered threats.

Updating

In addition to the few types of software presented throughout this section, all software on a system should be the latest version. Vulnerabilities are discovered in software on a daily basis. Immediately after those vulnerabilities are published on the Internet, attackers are developing content or applications to take advantage of those vulnerabilities. Each software vendor is responsible for providing patches for their own vulnerabilities, but some vendors more effectively help the user ensure that they are using the latest version than others. One free tool that can be used to watch all of the software on an entire system comes from Secunia. Secunia Personal Software Inspector can be installed to watch over every unique piece of software installed on your system to ensure that it is the latest version. It can be set to notify the user when something is out of date or even update the software without the user's intervention in some cases. The Microsoft Windows and Apple Macintosh operating systems both have an option for automatically downloading and installing new updates.

Remote Access Safeguards

In addition to those for protecting a system from malicious applications and content, safeguards are needed to protect systems from access by other individuals outside of a family's home network. Like malicious applications and content, this remote access could lead to the theft of personal or financial data that could be used against an individual or to the malicious attack of other systems via their home network. While users would certainly be aware if someone broke into their home and sat down at their system, it is much more difficult to identify when someone is accessing it from another system outside of their home.

Firewalls

A firewall is either software based and installed as part of, or in addition to, the operating system or hardware based and commonly bundled with gear used to connect to broadband internet connections or Wireless Access Points used in the home. You should think about communication going into or out of a computer as travelling along a highway with hundreds of lanes. A firewall is going to block all of the uncommonly used or higher risk lanes to allow only what is necessary to pass. All current operating systems enable their software to implement a firewall by default. Normally, an individual may only need to worry about the firewall when allowing new lanes of communication into the system for atypical software or connections. Third-party vendor firewalls, normally bundled with a suite of other security software, may have improvements over some operating system's firewalls such as blocking outbound connections in addition to the operating system's version which performs inbound only blocking. If available with a family's internet service gear, a hardware-based firewall can be beneficial over a software-based one because it ensures that malicious traffic is blocked before it ever reaches the system.

Wireless Access

Wireless access has made our lives easier and more convenient because we no longer need to run cabling throughout the house to access the network. However, our wireless networks reach beyond the walls of our home and can be accessed by others when security has not been enabled. After enabling a wireless network, an optional security password can be used to access that network from wireless devices. However, if a password is not used, the network can be accessed by any user within range. GetNetWise.org provides guidance for wireless network users: http://spotlight.getnetwise.org/wireless/wifitips/. One trend with recent purchasable wireless access points (which also can be bundled with the gear used to connect to broadband internet connections) has been to have wireless access enabled by default with the security password written on the wireless access point itself. This is very convenient for consumers because they never need to log in to the device to set it up as required with older models.

A family's home in Buffalo, New York was raided by police after their Internet Service Provider was told to release their location because authorities observed that a significant amount of child pornography was being downloaded through their IP address. (IP addresses are uniquely identifiable through logs and used by computers to communicate with others.) It turns out that a neighbor had simply joined that family's wireless network and was using that same traceable IP address because no password was ever set.

http://www.foxnews.com/scitech/2011/04/26/mistaken-fbi-porn-raid-underscores-wi-fi-privacy-risks/

Personal Computer Technical Controls Checklist

□ Use standard user accounts without rights to install or modify system configurations at times when such rights are not needed.

□ Determine if parental controls are available with your operating system and use them to allow specific accounts to only run preapproved applications.

□ Ensure that free or purchased antivirus/anti-malware software is running real-time scans and updating properly.

□ Run scheduled scans to determine if there are infections.

□ Save critical files on external storage systems and rebuild the system from scratch when infections are present and cannot be cleaned.

□ Never open Microsoft Office or PDF documents that come from unknown senders or that are attempting to open on their own.

□ Modify default Adobe Acrobat Reader security settings to increase protection from malicious PDFs.

□ Follow the technical tips at http://www.cert.org/tech_tips/securing_browser/ to secure your web browser.

□ Ensure that all the applications running on the system are the latest versions.

□ Set passwords and encryption for all wireless access points under your control.

Threats and Safeguards for Other Technology

Personal computers are no longer our only access to an outside world full of others attempting to steal from or take advantage of us or our children. New technology has led to new opportunities for attackers to initiate their crimes or malicious actions from anywhere in the world, with greater anonymity and in a matter of seconds.

Mobile Security

As users' computing experiences on mobile devices and personal computers become more and more synonymous, so do the threats they pose. While some parents might buy a feature-rich phone for their children, they might choose to buy themselves a basic phone that can only send and receive calls. As a result, many parents are unfamiliar with commonly used features such as messaging and content downloads, so they overlook the content delivered to mobile devices and the actions taken on them. They don't yet realize the threats that these features can pose.

Several incidents involving such threats have been reported in the news recently, but many more have occurred and not been reported by users in an attempt to avoid embarrassment to themselves and their families.

While spending too much time on these devices can have substantial social, behavioral, and psychological effects on users, those effects are not covered in this paper. Instead, we describe the incidents and risks associated with failing to identify and use security and parental safeguards. Without these safeguards, our families and children are exposed to risks that are common to personal computers and additional, new risks that are less often understood. These risks include unwanted social interactions that take place through digital communications; for example, bullying and predators' attempts to exploit our families. Risks can be technical in nature and involve the content these devices allow us to access, malicious applications, and, if we lose our devices, the loss of our personal data.

Next, we describe technical and behavioral safeguards that we can use mitigate the risks posed by our mobile devices.

Technical and Administrative Safeguards

Technical safeguards are typically easier to control than behavioral ones, since the behavior of most people, especially children, is very unpredictable. They are also easier because they specify a definite allowed or disallowed activity, whereas behavioral safeguards lead to many gray areas.

Selecting the Right Device for Children

The first and most effective step in mitigating risks is selecting a device that has the necessary feature sets, depending on an individual's needs and risk tolerance. When deciding which device to select, consider limited devices that contain only the necessary feature sets and controllable devices that allow parents to disable the ability to use risky features. Before purchasing a device for a child, ask yourself whether the child really needs to have it. The answer will depend on many factors including the child's age and maturity, potential situations where the child needs to contact others, and your risk tolerance.

In addition to removing or delaying the need to understand the risks that each feature might pose, selecting a limited device will remove the user's temptation to circumvent any security safeguards already in place. Safeguards are not even necessary in the first place if you choose a limited device that lacks risky, built-in features. Although rare, a few devices available for purchase allow the absolute minimum features necessary. These phones allow children to only dial pre-programmed phone numbers and also screen incoming calls to allow only a limited set to come through. They may also provide children with the ability to play pre-installed games and customize their phones without connecting to a data network or using any of the other risky features such as messaging or downloading content. These minimum-feature phones are a great way to provide children with phones for emergency purposes without worrying about security or out-of-control phone bills. They can also be a great resource for teaching children about technology and how to be responsible with devices until peer pressure makes them ask for more advanced features.

Parents also have the option of buying their children devices that have all the latest feature sets but can be disabled and password-protected. Controllable devices offer parents the benefit of having more mobile devices and carriers to choose from. Parents can enable the features slowly over time, without having to purchase an entirely new device. Before purchasing a controllable device, parents need to research it by reading through its documentation or speaking with a sales associate to determine which features can be disabled at the device level. Some devices require a third-party application to password-protect a feature. For example, the operating system used on iPhones allows restrictions on features, but the Android operating system requires third-party applications to establish parental controls.

Parental Controls

Parental controls have come a long way since the introduction of mobile devices. As the popularity of mobile devices attracted younger consumers and standard features were expanded beyond those of just voice communications, the carriers, manufacturers, and parents have all become aware of the need for these safeguards. Unfortunately, at least one reported incident is typically what it takes for parents to seek out and use these safeguards. However, depending on the severity of the incident, that one incident may be one too many, and parents need to be challenged with implementing these safeguards before such an incident occurs. While something like overcharges associated with service contract overuse can be quantified, it is obviously impossible to place a value on the reputation of your children when they get involved in something such as a "sexting" lawsuit. Parental safeguards can be implemented through the mobile carrier, the device itself, and third-party applications.

Six high-school students Pennsylvania are facing child pornography charges after three girls allegedly took nude or semi-nude photos of themselves and shared them with male classmates via their cell phones. One implication of conviction could force the teens to register as sexual offenders for at least 10 years.

http://www.msnbc.msn.com/id/28679588/ns/technology_and_science-tech_and_gadgets/t/sexting-surprise-teens-face-child-porn-charges/

In order to market their family plans and get parents who are concerned about safety to add their children to the network, mobile carriers have created more parental safeguards over the past few years. Most provide, as a free service, the ability to restrict the content being downloaded to their children's devices based on age levels but charge a monthly fee for restricting actual features such as browsing or messaging. If parents can afford that fee and do not want to worry about setting up safeguards on the device, carrier-level restrictions are the ideal method for establishing parental safeguards. They are device independent and possibly easier to manage over time. Examples of restrictions that can be set at the carrier level for a fee include

- Voice minutes usage
- Messaging usage (including only picture and video messaging)
- Periods of time in a day when usage can occur
- Numbers that someone does not want to call/send messages to, or receive calls/messages from
- Application downloads
- Mobile web usage
- Content downloads (music, ringtones, pictures, etc.)

As previously stated, the key to device-level safeguards is selecting a device that can manage these safeguards at an administrative level, on a password-protected basis, and unbeknownst to the device's primary user. Because children under 18 cannot purchase mobile carrier service on their own, parents have the opportunity to purchase the device and then change its settings and set a password or PIN to restrict children from accessing them. Then, depending on the device and operating system, parents can disable unwanted features and specify age-appropriate content. A challenge with device-level safeguards is that very few devices actually provide built-in safeguards; most rely on third-party applications.

Third-party applications for disabling features are also available for purchase, but they are typically limited to specific devices and operating systems and require some pre-purchase research. For example, Android devices have no built-in parental safeguards and therefore require a third-party application if those safeguards are needed. Parents need to consider ways of setting up parental safeguards prior to giving their children a newly purchased device.

Blocking Inappropriate Content

Mobile device application stores and carriers provide applications that users can install and interact with and content such as videos, photos, and music. Over the past few years, these stores and carriers have responded to consumer and political pressure to provide ratings for their applications and content. However, before consumers can actually benefit from those ratings, the parental safeguards must be set through the carrier, on the device, or using the third-party applications. Additionally, application stores and carriers are receiving between hundreds and thousands of submissions for content and applications daily. They rely on the subjective view of a reviewer to actually rate content and applications. Inappropriate content can certainly slip by due to a miscategorization.

In addition to applications and content, children may be subjected to inappropriate content through browsing the web on their devices or receiving it from other individuals through text or multimedia messaging. With the exception of performing technical safeguards to completely disable these services, this content is hard to filter, if it can even be filtered at all. To date, default mobile device browsers themselves do not have parental control capabilities, so they allow children to access any site that they could by using a personal computer. However, third-party applications are available for purchase to keep children away from websites identified by the application creator as having adult content. Because new websites with adult content are created every minute, keeping that list updated can be a challenge.

Monitoring and Tracking Children

While many parents may not feel comfortable monitoring their children’s mobile device activities, parents must remember that they are ultimately responsible for their children’s actions on those devices. Mobile carriers can drop a parent’s account for abuse of the system, and devices can be confiscated or parents can be fined when devices are involved in law enforcement cases. While a lot of parents may think that their child would never initiate bullying or “sexting,” simply receiving a message from a perpetrator or forwarding it to another can quickly involve the child in the crime. Parents can sometimes prevent these negative actions merely by letting their children know they are being monitored.

Simply knowing the password and reviewing children’s calls and messages or browsing history may not be enough. Children are smart enough to delete those messages or potentially install applications developed for removing that type of information. One quick Internet search or a chat with a friend with a similar device can show a child the steps necessary to clear their history. Depending on parents’ risk tolerance, the child’s technical abilities, and the situations the child may be a part of, parents need to consider purchasing third-party applications for devices that allow applications to be installed. For example, if a parent has been diligently attempting to review messages but doesn’t find any, the child has most likely figured out how to remove them. In that case, third-party monitoring applications may be necessary. These applications can be purchased on the Internet, but are not offered by the vendors, mobile carriers, or the application stores. They are typically frowned upon because of their nature and their ability to illegally track anyone outside of one’s family. These monitoring methods are illegal when used on a device not owned by the person installing them. As mentioned before, it is extremely beneficial for parents to mention to their children that they are, in fact, being monitored.

These third-party applications can vary, but most can monitor and track call logs, text and multimedia message logs, web access, and locations where the mobile device is or has been. This information can then be accessed by supplying a password on the device itself to open up the management interface, by logging into a website that the information has been uploaded to, or by having reports emailed to the parent's account. Parents who use such a service should keep in mind that this sensitive information regarding their family is now being stored either on the device itself or in another location. Criminals may be able to track down this information if the device is lost or stolen or if the system where it resides out on the Internet is compromised.

Physical Loss and Passwords

We cannot describe mobile device security without mentioning physical loss. Whether it is accidental or a criminal act, these high-value devices typically are not returned to their original owners once they go missing in a public place. While the financial aspects of a physical loss are a concern, even more troubling are the privacy issues associated with a person now having someone else's device. Depending on how well the device is secured, the person who finds the device might have access to the owner's contacts, logs, schedule, online accounts if their username and password information is being stored, voice minutes or data access, and much more.

The primary and easiest method for mitigating the risks associated with a physical loss is enabling passwords or PINs on mobile devices. This is very easy to do, yet many people neglect to do it because it's inconvenient to enter the password each time they want to use their device. Passwords are typically used on devices with a keyboard and can be enabled through the Settings menu on a device. PINs are primarily associated with devices containing only a number pad. For more information on a specific device, refer to its documentation. The same rules that apply for passwords on a computer also apply to mobile devices: select passwords of reasonable length and complexity. Avoid passwords and PINs that can be associated with you or the device itself, so they are not easily guessed. The most commonly used PINs that should **never** be used are 0000, 1234, and the last four numbers of the device's telephone number.

> Out of the 734 smartphone-owning consumers surveyed in a March 2011 study conducted by the Ponemon Institute LLC and sponsored by AVG Technologies, less than half used keypad locks or passwords to secure their devices.
>
> http://aa-download.avg.com/filedir/other/Smartphone.pdf

Even with a password, an individual may be able to retrieve data on the device by using forensics on the hardware. Besides actually encrypting the storage on the device (an option available only with recent versions of Blackberry-device software), there are no ways to defend against this risk.

Whereas the chances of recovering a lost or stolen device a couple of years ago were slim to none, software and services that can be added for an additional cost have since increased those chances.

Third-party developers have also written their own custom applications. These applications and services allow device owners to access the GPS coordinates of their devices, so they can report that information to law enforcement. However, once the criminal turns off the device, that functionality is no longer present.

Multiple Communication Paths

As new feature sets are added, additional connections and communication paths are created on our devices and prone to risks. They include Bluetooth connections for accessories, WiFi connections that can open up devices to many of the same vulnerabilities that personal computers are exposed to, and physical connections for downloading content from another device. If a user never needs these features or only needs them at certain times, they should be disabled until actually needed. In addition to saving battery life, disabling these features reduces the risk of exposing the device to vulnerabilities.

Bluetooth connections are vulnerable primarily in two instances: (1) when using first-generation Bluetooth devices and software and (2) during the discovery process of pairing a mobile device to an accessory. Mobile devices are typically backwards-compatible to support the use of first-generation Bluetooth devices. Typically, the easiest way to mitigate the risks associated with vulnerable devices is to replace them with newer generation ones. Pairing is the process used to associate a trust between a Bluetooth device and the mobile device that will be using its services. Pairing should only be done in a private location where malicious individuals cannot read the pairing process using special equipment or pair their own Bluetooth device with the mobile device. Once pairing has been completed, pairing mode needs to be disabled on the mobile device until it’s needed again.

Using an unsecured or secured but compromised WIFI hotspot can put an individual at risk. Unsecured hotspots can have attackers on the same network as users capturing traffic that is not secured. If you must use an unsecured network, avoid sending anything personal to websites that do not start with *https* instead of simply *http*. On mobile devices, it can be challenging to determine the web address, so it may be best to turn off WIFI and use the cell-phone network security instead. In addition to risks with unsecured WIFI hotspots, attackers can set up legitimate-looking secured WIFI networks alongside the hotspot that a user is expecting. As a result, users can accidently connect to the wrong one. At that point, the attacker could also set up legitimate-looking, commonly used websites and then capture usernames and passwords as they are sent. In this scenario, it is best to access websites that require usernames and passwords only while connected to the cell-phone network.

In order to manage these devices and supply them with new applications, content, and updates, high-end devices have the ability to physically connect to personal computers. These physical connections also introduce a path for malicious software being installed on the device. Users must be careful not to connect to a computer that is infected by malicious applications because they could potentially be used to infect the mobile device or retrieve sensitive information.

Data Management

An important consideration to keep in mind when mitigating risks is the data being stored or transmitted on the device. If no personal or confidential data is being stored or transmitted on the device, the risks associated with malicious software infections are really limited to the device being disabled or users being charged for services that they did not initiate. For example, when device users have limited or nonexistent data plans, malicious data usage can generate overage charges or calls to 900 number services that can initiate undesired charges. Alternatively, as soon as a mobile user begins to perform online banking and bill paying, or logging into websites, many additional consequences need to be considered in addition to device disabling and premium service charges.

Malicious software can record sensitive information being typed into a device such as usernames and passwords. This type of malicious software is typically referred to as key loggers. That sensitive information can then be posted to a website of the attacker's choosing or sent out via text message unbeknownst to the device user. Even if users realize that their device has been compromised and then avoid typing sensitive information into the device after that point, they may still be at risk. Usernames and passwords are commonly saved in the device, and attackers know how to retrieve them. Usernames and passwords are not the only type of information that users should consider. Making purchases from a device may give malicious software a chance to record credit card information or bank account and routing information as well.

Device users should also be aware of the information that is being recorded about them, their actions, their preferences, and their location. Typically, this capturing of data is outlined in the fine print of the terms of service that many of us neglect to read. If users did not agree to the information being recorded, it is in violation of consumer-protection laws. This privacy-related information is used by advertisers for the purposes of targeted marketing. If a website can narrow down a user's location, they will then be able to show ads for stores specific to that location. Additionally, many of the photos, videos, and other content can contain the latitude and longitude coordinates of the location they were captured from. These coordinates are attached unbeknownst to a user with the help of the GPS built into the device. Attackers can view the hidden coordinates and know the precise location of the user at that moment in time. Permissions on the devices can be set to either allow or disallow a response to the location request. For example, users can turn on location awareness for their Twitter accounts so that their friends and relatives can be aware of their location. An individual's decision to allow or disallow the publishing of such coordinates will ultimately depend on their preferences for targeted marketing over privacy concerns. Even after disallowing an application or website from gaining access to their location, they still may be at risk. Recent locations may be stored locally on some devices for the purpose of faster connections to cellular and WIFI networks, and attackers can access that information if they have physical access to the device.

Malicious Software

Just as some of us have begun to get a handle on how to prevent malicious code from being executed on our personal computers, we are now in the beginning stages of dealing with similar issues on our mobile devices. This malicious code can be received via any of the newer connections to include messaging, internet browsing, and application downloads, or as a transfer from a personal computer. Malicious code has the potential to steal and forward off personal data, make the device unusable, incur charges through limited data plans or by calling or messaging costly services, and many other malicious acts.

In April 2011, researchers discovered that Apple's IPhone was storing, in a retrievable file on the device itself, the locations of network access points it discovered.

http://articles.cnn.com/2011-04-21/tech/iphone.tracker.explainer_1_3gs-location-data-iphone?_s=PM:TECH

Apple responded to the research by explaining the purpose of its need to store access points and released an update to reduce the risk of the information falling into the wrong hands.

http://www.apple.com/pr/library/2011/04/27location_qa.html

Malicious code for mobile devices is in its infancy for a variety of reasons. Most individuals have not yet been affected and there has been little news coverage because criminals have historically lacked the motivation to create malicious code for mobile devices. With personal computers, we store and send website logon credentials or work with financial data that a criminal can benefit from financially. However, mobile devices have just recently begun to be used for similar purposes. It stands to reason that much more malicious code will be developed to attempt to steal this type of information, as it becomes more and more common on our advanced devices and we feel the need to have instant access to it at all times.

The popularity of downloading and installing free or purchasable third-party applications on devices has also increased the risk of *accidently* placing malicious software on a device. Some of the application stores do not analyze the security or content of an application prior to making it available for download. For stores that do review the applications, malicious code can remain hidden and undetected by the reviewer. This malicious code is typically bundled with a legitimate application to make users want to download and use it. Users need to thoroughly research an application prior to installing it. Even during installation and use, many devices will provide a warning that these applications are attempting to access another service of the mobile device. Many users do not take the time to actually read the warnings or fully understand the implications of accepting them. Users need to use common sense and realize that something like a game should not be asking for access to the device's call logs.

Users are being tricked into opening their devices to these vulnerabilities in nearly all instances to date. Whether it is through downloading an application that they thought was clean from vulnerabilities or accepting a multimedia message from someone they do not know, the device owner unknowingly allows these vulnerabilities to be introduced.

Updating

The earliest implementations of mobile devices did not have the capability to be updated. Today's devices can be updated from the carrier over the air or when plugging into a computer to manage it. Device users need to understand the importance of updating. Not only do software updates introduce new or improved features, they also fix flaws or security vulnerabilities found since the last update. Some users will delay updates to avoid being inconvenienced by the sometimes necessary reboot or having to physically connect it to the computer for a period of time. The longer that an update is delayed, the more opportunity they are giving an attacker to take advantage of an unpatched security vulnerability.

Behavioral Safeguards

Although easier to implement, technical safeguards alone are not sufficient for mitigating risky behavior. Parents need to follow both technical and behavioral safeguards. Not only is it great for a parent or guardian to establish a dialogue with their children about risky behavior, but it will also help both children and parents understand the technology better and the expectations that parents have for their children up front. Mobile device users are also vulnerable to unique social engineering tactics. Everyone should be aware of these tactics, so they can modify their thinking and behavior appropriately.

Ground Rules and Family Contracts

A child's mobile device behavior is heavily dependent on the existing relationship between the parent and child. If parents neglected to establish any rules with their children concerning other situations where there is a risk of negative actions, setting rules for mobile device use is going to be much more challenging. For example, parents who allow their teens to watch mature content movies and video games will find that restricting similar content on devices will result in a dispute. In these instances, parents will need to rely primarily on the technical safeguards.

It is important that ground rules be established prior to letting the child use the device. Parents should review the device's product guide with their children and discuss how to use the enabled features. When applicable, parents should also explain which features have been disabled and why. Parents should also teach their children how to keep track of the number of minutes that they are using or number of messages that they are sending and receiving if they are not on unlimited plans. Most carriers provide free methods for keeping track of these numbers.

Ground rules should be documented in some form of a family contract. This is a good practice because it keeps both the parent and child from forgetting the rules over time and signing a contract may help the child commit to the rules. Family contracts should also define punishments for breaking the rules.

Device Availability and Review Sessions

Parents have numerous options regarding when and for how long the device is in the possession of their child. These options can range anywhere from unlimited access to the device to "for emergency purposes only" when outside the home without a parent or trusted adult. The setup a parent chooses should depend on many factors as well. The child's age and maturity, the amount of time parents want children to spend interacting with technology instead of being social, and the increased risk of negative abuse due to increased time with the device are all factors that should influence a parent's decision. Parents also need to check with their child's school and other groups the child is involved with to determine if there are restrictions for having devices. A lot of school officials do not allow devices in the classroom. Finally, parents should allow some room for flexibility and change the rules depending on the situation. Access to the device can be used as a reward for good behavior and vice versa. They may also want to begin taking the device away during bed time if they find their child not receiving a sufficient amount of sleep.

If parents decide to give their children unlimited access to the device, parents should establish regular times to review the device's logs. Limited access to the device enables parents to reviews those logs every time it is back in their hands. Prior to providing their child with the device and at the same time that ground rules are being established, a regular interval should be defined for times when the parent will be able to look through the logs on the device with the child. The child can also be told that in addition to that regularly scheduled review session, the device can be taken and reviewed at any time so the child does not become accustomed to removing content that they do not want their parents to see just before the regular review sessions. Children and parents should be able to identify every phone number or email address they are contacting or being contacted by. Parents should consider actually calling the number to verify that it belongs to who their children say it does.

In the same way that device logs are reviewed with the child, the mobile carrier bill should be detailed and reviewed with them as well. Device logs are beneficial to stop negative activity prior to the end of the billing cycle, but they can be removed by the child as well. Mobile carrier bills cannot be modified in this same fashion, and parents showing children they still have access to all of the details should help deter them from removing device logs.

Legal and Moral Considerations

When parents decide to give their children the freedom to use text and multimedia messaging, they are accepting the risk that their children may engage in, or be the victim of, activities such as "sexting" and bullying. Children are more likely to get involved with cyberbullying or "sexting" using a mobile device than in face-to-face interactions because they feel a sense of anonymity or courage because they can "hide" behind the device. Additionally, their lack of maturity and life experiences keep them from being able to think beforehand about the consequences of their actions.

There are some fine lines between moral and legal implications. While it is seen as immoral for an adult to transmit pornographic photos of themselves to someone other than their spouse, there is no law stating that this act is illegal. However, forwarding that same photo to an individual under the age of 18 is in violation of child endangerment laws and can lead to jail time. There are also a lot of grey areas within the laws. This is particularly true when two minors are involved. Many states have been working to pass laws that reduce the severity of the crime when child endangerment laws are broken by other minors. This can include taking a picture of oneself or forwarding one after having received it from a third person. As was previously described in the monitoring and tracking section, parents need to remember that the actions taking place on those devices can also be deemed by the authorities or court systems as their responsibility when their name is on the account of a child's or family plan.

It is difficult to describe exactly what is and is not illegal when it comes to mobile device abuse because it depends on the laws of that state or multiple states involved; the authorities, courts, judges, and juries; the outcome of the actions; and the public attention that the action may generate. Using cyberbullying as an example, simple cyberbullying over a mobile device may not be punishable by a court of law. However, if that cyberbullying leads to the victim committing suicide, then the publicity alone will more than likely destroy the reputation of the perpetrator and their family for years to come. Criminal charges are also more likely to be brought against the perpetrator.

While disabling services that allow children to perform these actions is the only way to completely stop them, parents who allow children to use these services can also take steps to educate them on what is and is not appropriate and the consequences that will follow. Children may not care when they are told that their parent could be fined for their actions, but explaining to them that their reputation is at stake when becoming involved with such actions and that they could go through the remainder of their school years being called names or viewed in a negative way may get their attention. Parents keeping up with the news on cases related to mobile device bullying or sexting and relaying that information to them could also help to keep them informed of the implications. Parents also need to perform the previously described device review sessions to ensure that children are adhering to ground rules.

Parents attempting to teach their children to report embarrassing or painful details about their lives can be a challenge. Children can be fearful they may get into trouble with their parent even when they are the victim of an incident. They also are trying to become completely independent of parental support around the timeframe when parents may consider providing them with a mobile device. Parents need to establish a trust with their children so they are comfortable reporting when they are the victim of, or involved in, an incident. Reported incidents should be handled with caution and care so children feel comfortable reporting future incidents. Parents should avoid embarrassing them but not be afraid to seek external help when necessary either. Finally, it is a good idea for parents to get to know the parents of their child's friends. Once an incident is reported to a parent and they know the others who are involved, they can tactfully reach out to other parents depending on the scenario.

Pew Research Center's Internet & American Life Project found that 4 percent of cell-phone-owning teens ages 12-17 say they have sent sexually suggestive nude or nearly nude images or videos of themselves to someone else via text messaging, a practice also known as "sexting;" 15 percent say they have received such images of someone they know via text message.

http://www.pewinternet.org/Reports/2009/Teens-and-Sexting.aspx

Social-Engineering Mobile Devices

Today's extensive features of mobile devices introduce numerous chances for attackers to take advantage of innocent individuals. Our curiosity, desire to help, need to be in the know, or fears provide attackers an opportunity to get mobile device users to respond, click, or install whatever it is they need them to do to bypass built-in security that disallows actions to take place without the user first authorizing them.

While most people have gotten used to ignoring email spam requesting that they respond with personal information or requesting help with money laundering, similar requests from text or multimedia messages are new and our curiosity can get the best of us. Smishing through SMS or text messages is the equivalent of the phishing through emails described previously. Smishing can ask mobile device users to go to a website or call a number to verify a financial charge or to reactivate a debit or credit card in some way. The attackers are trying to capture the information necessary to duplicate the victim's cards to use. Just like with emails, mobile users should avoid opening or responding to text messages from numbers that they do not know. This is also true for numbers that differ from the normal telephone format, such as those that display '5000' as the sender's number. This indicates it was sent from an email address and more likely to be a smishing attempt.

Mobile devices are great because of their portability. However, their small size also forces them to have unique qualities and limitations that attackers can take advantage of. For example, mobile device web browsers do not display the web address of the site that a user is browsing to because it would take up valuable space on the screen. For this reason, attackers can direct a mobile user to a web address that is mimicking a real site the user would use. While seeing a completely different site address in the browser on a personal computer will tip off a user, not being able to see that address in the mobile browser limits a user's defenses. Additionally, users are likely to store credentials for applications on the device because it can be cumbersome to type in usernames and passwords each time. So when a device is lost, stolen, or hacked in some way, the attacker now has access to all of these stored usernames and passwords.

Video Game Security

According to the Entertainment Software Association, 68 percent of households played video games as of 2009. Similar to our discussion on mobile devices, the intent of this technical report is not to discuss the negative impact that spending too much time playing video games may have on children. Instead, it is intended to introduce parents to risks and safeguards associated with video game consoles they may not be aware of. We focus primarily on those risks associated with connecting video game consoles to the Internet access because it is a popular capability of the latest and presumably all future generations of video game consoles.

Content and Online Predators

Parents should already be well aware of the ESRB (Entertainment Software Rating Board) rating placed on the cover of video games that is used to identify the age appropriate for viewing that game's content. However, the ESRB does not rate any of the material that a game player would come across while playing that game online. This includes the voice and text chats with other players or any content created by other players and uploaded for all to see or use. A game may be rated "T" for teen, but if another player uploads an inappropriate image to the servers hosting the game to be used as their character, the system cannot differentiate between that and any other picture.

In addition to the chats and game content, all of the content across the Internet can also be a concern as Sony's Playstation 3 and Playstation Portable, Nintendo's Wii and DS Series, and Microsoft's Xbox can all browse the web just like any other web browser on personal computers. Safeguards for gaining access to all of this content will be discussed in the Parental Controls section.

The individuals talking to children and attempting to become their new friend can also be a concern. Online predators will try to build trust between themselves and children. Children who have not been forewarned will have no problem giving out their personal information and being lured by promises of gifts, favors, or money because they are gullible and lack life experiences. Sony's Playstation network and Microsoft's Xbox network will allow anyone to reach out and meet anyone else subscribed to their services. There is less risk of communication with strangers on Nintendo's Wii network because unique Wii numbers associated with a gamer must be shared through a separate medium before communication can be established.

A 36-year-old woman is accused of flying across the country to have sex with a 13-year-old boy she befriended while playing Xbox Live online.

http://www.ktla.com/news/landing/ktla-xbox-mom-rape,0,2120242.story

Parental Controls

Fortunately the video game console manufactures have included various parental controls within their systems. The easiest and most low-risk method of safeguarding a system is to avoid purchasing the subscription or physically or wirelessly attaching it to the home network in the first place. Doing so will also ensure that game players do not interact socially. Deciding on the appropriate age of the gamer to allow network access is critical.

After deciding to allow access, the game player's interactions need to be monitored and controlled depending on their age. The latest versions of each of Sony's, Nintendo's, and Microsoft's gaming consoles have the ability to allow access to their networks while limiting the use of some of the features. For directions and a list of features that can be controlled on Sony's Playstation 3 and Playstation Portable, Nintendo's Wii, Microsoft's Xbox, and Windows Vista, refer to the ESRB's guide located at http://www.esrb.org/about/news/downloads/ESRB_PTA_Brochure-web_version.pdf.

Once a passcode or PIN has been set, parents are then able to limit web browsing, voice and text chat capabilities, the maximum rating of games and DVDs that can be played on the system, and other features, depending on the console. Parents should also ensure that their children are aware that they need to report anything they are uncomfortable with.

Data and Privacy

Similar to personal or financial information stored in other locations, data stored on these game networks is also at risk. While there is no way for consumers to protect against risks such as this except for avoidance, it is important to keep in mind that an individual's financial and personal information is stored in a lot more places than they make think, even if kept at a minimum.

In April 2011, the information of individuals using Sony's Playstation network was compromised on the servers within Sony's corporate network. The full extent of the information taken has yet to be determined.

http://articles.cnn.com/2011-04-26/tech/playstation.network.hack_1_patrick-seybold-credit-card-sony-first? s=PM:TECH

Webcams

Webcams (video cameras connected to the Internet, are common devices that are built into most new computers or can be inexpensively purchased and added on. Newer mobile phones with 3G technology also support video-calling capabilities. These devices that can record video and still images are most commonly used for video conferencing or live video "chatting." While they may be a welcomed technology advancement that gives geographically distant loved ones or hearing-impaired people an inexpensive, interactive means of communicating and that allows more people to work remotely with virtual face-to-face interaction, webcams also have privacy and security concerns.

Webcams have the ability to be remotely activated without the user's knowledge through a malicious Trojan horse program or through a feature left enabled intentionally described as a "security feature." Several articles have been published detailing webcam vulnerabilities and how to avoid being a victim of one of these malicious programs. The best protection, and what should be a common practice, is to decline a Friend or Contact request from someone unknown. Accepting a stranger's request may initiate an attempt by them to have malicious software installed or make the user susceptible to information theft.

A school district in Pennsylvania was highlighted in several news articles and faced lawsuits in early 2010 when it was made public that they installed a remote administration program on laptops issued to their students. The school district made the case that their actions were an attempt to keep track of school-owned equipment and that they would only use the remote capabilities if a laptop was reported missing or stolen. They ceased using the program after they were accused of capturing tens of thousands of snapshots including ones of students at their homes in private situations. Not only did the controversy question whether the school had violated privacy issues by knowingly spying on students, but the program contained a security hole that put the students at risk of being spied on by anyone who exploited the vulnerability.

In addition to only accepting Friend or Contact requests from people you know, be sure to disable the webcam's remote administration feature. For information on how to do that, consult the webcam manufacturer's website or websites that describe specific vulnerability information and how to address it, such as US-CERT: http://www.kb.cert.org/vuls/id/932217. When the webcam is not in use, cover the camera lens and don't leave USB cameras plugged in. If possible, use a webcam that has either a lens cap or an LED that indicates when the camera is activated.

> A hacker used the family's webcam to spy on them and attempt to lure a teenage girl.
>
> http://www.click2houston.com/technology/3324710/detail.html

Safeguarding other Technologies Checklist

□ Ensure you purchase a mobile device for children that you can set parental controls on.

□ Establish safeguards to protect children from unwanted features or content on mobile devices.

□ Monitor mobile device usage by children.

□ Set passwords for mobile devices and disable unnecessary features when not in use.

□ Consider the impact of a loss of any information prior to entering it into a device.

□ Only install applications from reputable sources and read through the permissions that you are giving each application carefully before accepting.

□ Establish rules and device review sessions with children to ensure there is no confusion or disregard of ground rules.

□ Explain the impact of participating in negative behaviors such as "sexting" or cyberbullying, and encourage children to report incidents to you.

□ Avoid opening or responding to anything coming from an unknown number on mobile devices.

□ Understand and set parental controls on video game consoles for online features that you do not want your child to participate in.

□ Make sure that the remote administration feature is disabled on webcams, and use webcam with a lens cap or LED light that indicates when the camera is on.

Additional Resources

Cyberbullying Education Sites

http://www.beatbullying.org/

http://www.cyberbullying.us/

http://stopbullying.gov/

Child-safe Search Sites

http://searchenginewatch.com

http://www.sldirectory.com/searchf/kidsafe.html

Password Generator

http://www.pctools.com/guides/password/

Web Browser Security Tips:

http://www.cert.org/tech_tips/securing_browser/

Text Abbreviation Translators:

http://www.noslang.com/

http://www.teenchatdecoder.com/parental-lookup/teenchat-a.html

http://www.1337talk.com/

Setting Video Game Parental Controls

http://www.esrb.org/about/news/downloads/ESRB_PTA_Brochure-web_version.pdf

Family-safe Computing Educational Resources

http://www.onguardonline.gov/

http://kids.getnetwise.org/safetyguide/

http://www.staysafeonline.org/

http://www.bbc.co.uk/webwise/guides/children-and-social-networks

http://www.familysafecomputers.org/

Wireless Network Security

http://spotlight.getnetwise.org/wireless/wifitips/