The CYBER SECURITY Handbook

www.NJConsumerAffairs.gov ■ 1-888-656-6225

CYBER SECURITY

A CONSUMER GUIDE TO CYBERSECURITY

Dear New Jersey Consumer,

"Cybersecurity" refers to the protection of everything that is potentially exposed to the Internet: our computers, smart phones and other devices; our personal information; our privacy; and our children.

The Internet is an amazingly useful and versatile tool that has become indispensable for work, education, personal entertainment, and staying connected with family and friends. Use it responsibly, while taking care to protect yourself and your data, and you will continue to find it a valuable resource.

This booklet covers the three main topics of **"Viruses, Phishing, and Identity Theft," "Ads, Apps, and Your Personal Safety,"** and **"Online Predators and Cyberbullies."**

Although the basic information about personal protection stays the same, specific facts may change as the Internet rapidly changes. For that reason, the booklet concludes with a list of online resources that provide regularly updated consumer-friendly information.

For regularly updated Consumer Alerts and other information, check our website, **www.NJConsumerAffairs.gov**, and find us on Facebook. Check our calendar of upcoming Consumer Outreach events at **www.NJConsumerAffairs.gov/outreach**.

Sincerely,

New Jersey Division of Consumer Affairs

Table of Contents

Table of Contents

Be an Informed Consumer....*We can Help!*

CYBER SECURITY

Chapter One

A CONSUMER GUIDE TO CYBERSECURITY

The Problem: Technological and Psychological Trickery

A Primer on Identity Theft

Identity theft is considered the fastest-growing financial crime. It occurs when a thief assumes the victim's identity in order to apply for credit cards, loans or other benefits, in the victim's name, or uses this information to access your existing accounts. The thief will accumulate massive debt or deplete your current assets and then move on to another stolen identity.

The victim, meanwhile, may end up thousands of dollars in debt, with a ruined credit history or with an empty bank account. Until cleared up, this can make it difficult to find a job, buy a car or home, obtain a student loan, or engage in other activities that depend on the use of your own good name.

Your identity might be stolen through **phishing**, in which criminals trick victims into handing over their personal information such as online passwords, Social Security or credit card numbers. It might be done by invading your computer with **spyware** that reads your personal information, or it may be as easy as stealing your wallet. ***Note:*** For information on what to do **If You Fall Victim to Identity Theft,** refer to Appendix I of this booklet, at page 44.

The Many Forms of Malware

"Malware," or "malicious software," refers to programs designed to invade and disrupt victims' computers. Malware might be used to delete and destroy valuable information; slow the computer down to a standstill; or spy on and steal valuable personal data from the victim's computer.

The best-known types of malware are viruses and worms, which infect computers, replicate, and spread to other computers. They might be transmitted via email or across networks. Another type of malware is the Trojan horse. Like its namesake from Greek legend, a Trojan horse looks like a gift – but when you click on it, you're downloading a hidden enemy.

Spyware is a type of malware that collects information without the victim's knowledge. Some forms of spyware gather personal information including login accounts and bank or credit card information. Some may redirect your browser to certain websites, send pop-up ads, and change your computer settings.

Phishing and Social Engineering

Kevin Mitnick, once a notorious computer criminal and now a security consultant, summed up in an August 2011 TIME magazine interview the ways criminals combine plain old psychological trickery with malware-creation skills – a combination referred to as social engineering.

He said a hacker may learn your likes and dislikes from your posts on Facebook. "If I know you love Angry Birds (a popular smartphone game), maybe I would send you an email purporting to be from Angry Birds with a new pro version. Once you download it, I would have complete access to everything on your phone," Mitnik said.

Attacks like this are a form of phishing. Through phishing and social engineering, computer hackers trick victims into handing over sensitive data – or downloading malware – without thinking twice.

Social engineering may take the form of emails or instant messages that appear to come from a trusted source. You may get fraudulent email that appears to come from your bank, a

shopping website, a friend, or even the State government. The message may even contain links to a counterfeit version of the company's website, complete with genuine-looking graphics and corporate logos.

In a phishing attack, you may be asked to click on a link or fraudulent website which asks you to submit your personal data or account information – and end up giving it to an identity thief. Or you might receive a suspicious email with an attachment containing a virus. By opening the attachment, you may download a Trojan horse that gives complete access to your computer.

As an example of a phishing scam, in March 2012, the State of New Jersey learned of an "Attorney General Impostor" scam. Consumers as far away as Baltimore received an 11-page, official looking letter that claimed to be from the Attorney General of New Jersey.

The fraudulent letter invited consumers to apply for their share of a fictitious multimillion-dollar legal settlement. It even contained a phone number and email address, manned by perpetrators of the scam. Anyone who called would speak with a con artist posing as a State employee, who would ask victims to send their Social Security numbers or other information.

The New New Internet, a cybersecurity news site, has noted that hackers launch phishing scams through instant messaging, Facebook, Twitter, and other social networking sites. In one attack, Facebook users found fake video links that bore the title "distracting beach babes" and a thumbnail image of a woman in a bikini. The posts appeared to come from the users' friends. A similar attack used posts with the title "try not to laugh," and a link to what looked like a humor website. In both cases, the links attempted to install malware on users' computers.

An Exponentially Growing Threat

The Wall Street Journal reported in May 2011 that "one in every 14 downloads is a piece of malware." SecureWorks, an information security service provider, reported in 2010 that the United States is the "least cyber-secure country in the world," with 1.66 attacks per computer during the previous year – compared with just 0.1 attempted attacks per computer in England. Symantec, a maker of security software, reported in 2008 that new malware released each year may outnumber new legitimate software.

Phishing is also extremely widespread. Of the 140 billion emails sent every day, some 90

percent are spam, or electronic junk mail, according to a 2010 report in The Economist; of those, about 16 percent include phishing scams. It is easier than ever for con artists to craft personalized emails that their victims are more likely to trust and open – and this is because there is more information online about individuals than ever before.

Consider how much information may be available online about you or your loved ones, thanks to social networking sites, your company's website, online records and other sources – including advertisers and advertising networks (see Chapter 2 for more information).

The Solution: Build Your Defenses

The following tips are adapted from those offered by the United States Computer Emergency Readiness Team (US-CERT), within the U.S. Department of Homeland Security. For more information go to **www.US-CERT.gov.**

Virus Protection Tools

Use and maintain a reputable antivirus software. Good antivirus software packages recognize and protect your computer against most known viruses. (You can check online

reviews to learn about the best versions currently available.) Once you have installed an antivirus package, you should use it to scan your entire computer periodically. Find a package that includes antispyware tools.

Keep antivirus software up to date. Install software patches and security updates for your antivirus software on a regular basis. They will help protect your computer against new threats as they are discovered. Many vendors and operating systems offer automatic updates. If this option is available, you should enable it.

Install or enable a firewall. Firewalls protect against outside attackers by shielding your computer or network from malicious or unnecessary Internet traffic. They are especially important for users who rely on "always on" connections such as cable or Digital Subscriber Line modems. Some operating systems include a firewall; if yours has one, you should make sure it is enabled. If not, consider purchasing a hardware- or software-based firewall.

Use antispyware tools. Many antivirus software packages are sold with antispyware tools included. ***Note:*** Many vendors produce antivirus software. Deciding which one to choose can be confusing. All antivirus software essentially perform the same function, so your decision

may be driven by recommendations, particular features, availability or price.

It is not a good idea to install too many types of security software. Too many programs can affect the performance of your computer and the effectiveness of the software itself.

Finally, **beware of unsolicited emails or pop-up ads** that claim to contain antivirus software. Don't open them or click on their links or attachments. These are often Trojan horses, waiting to infect your computer.

Check Your Web Browser's Privacy and Security Settings

Almost all computers and smart phones come already installed with one or more web browsers (such as Safari, Firefox, Internet Explorer, Chrome or others). The browsers come with default settings that seek to strike a balance between keeping your computer secure, and allowing you to get the functionality you expect from most websites.

The settings create limits for the extent to which the computer will allow Internet applications – such as cookies, ActiveX and Java – that help websites perform important functions. For example, they may keep track of what's in your shopping cart, or remember your login

information so you don't have to re-enter it every time.

If your browser allows unlimited interaction with cookies and other applications that track your Internet activity, you may be at greater risk of a malware attack – or of being solicited by advertising software (more on this in the next chapter). But if you block these applications completely, websites may not function as efficiently.

Find the balance that works for you. Check the privacy and security settings of all web browsers that are installed on your computer, and adjust them as necessary.

For specific information on a given web browser, visit the vendor's website (for example, visit the Microsoft Windows website to learn how to adjust security settings for Internet Explorer; or the Apple site to learn about the Safari browser). If a vendor does not provide information on how to secure the browser, contact them and request more information.

If You Use a Wireless Router

Wireless router systems broadcast your Internet connection over a radio signal to your computers. Failure to properly secure this connection could potentially open your Internet connection to other users, and expose you to potential problems.

Refer to your router's user manual for information on how to: hide your wireless network (sometimes called creating a "closed network"); rename your network (change the default "service set identifier" or "extended service set identifier" to a designation that hackers won't be able to guess); encrypt your wireless network (convert the traffic between your computer and the route into code); and change your administrator password.

In addition, refer to the user manual to disable the file sharing option on your computer (unless you need to share directories and files over your network, in which case you should password-protect anything you share). Keep your wireless software patched and up to date, by periodically checking the manufacturer's website for updates. In addition, it's a good idea to learn whether your Internet service provider (ISP) offers wireless security options.

Use Smart Passwords

Don't use passwords that are based on personal information a hacker can easily access or guess; and don't use words that can be found in the dictionary. One method for creating passwords is to rely on a series of words and memory techniques, or mnemonics, to help you remember how to decode it. US-CERT gives this example: Instead of using the word "hoops"

for a password, use “IlTpbb” for “[I] [l]ike [T]o [p]lay [b]asket[b]all.” Using both lowercase and capital letters adds another layer of obscurity, as does using a combination of numbers, letters and special characters. Change the same example to “Il!2pBb.” and see how much more complicated it becomes just by adding numbers and special characters.

Don’t Get Phished

Never trust an unsolicited email, text message, pop-up window, Facebook message, etc. that asks you to: give sensitive information such as your Social Security or bank account numbers; click on a link or open an attachment; or send someone money.

Don’t trust the message no matter how convincing or official it looks; no matter if it appears to come from your bank, the government, your ISP, or your best friend.

Always independently verify the authenticity of the message before you respond. Don’t use an email address, link, or phone number in the message itself. If it’s from your bank, search online for the customer service line and call the bank.

In June 2012, consumers nationwide received scam emails that were almost identical to the

real email alerts Verizon sends out to its customers, to remind them of their monthly payments, according to the Better Business Bureau. The emails included a link to "View and Pay Your Bill" – a link that sent victims to a fraudulent site.

Rather than follow those links, consumers could independently verify the message's authenticity by opening a separate browser and looking for Verizon's actual website – or by calling Verizon's customer service.

Use common sense. Never open email attachments unless you know from whom they were sent. Never execute programs unless they are from a trusted source. Never click on links within pop-up windows. Be wary of free downloadable software, or any email link that offers antimalware programs.

Beware of homemade CDs, floppy disks and flash drives. If you plan to use them in your computer, scan them with your antivirus software first.

What To Do If Your Computer System Becomes "Infected"

First, disconnect your computer from the Internet. This will prevent malware from being able to transmit your data to an attacker.

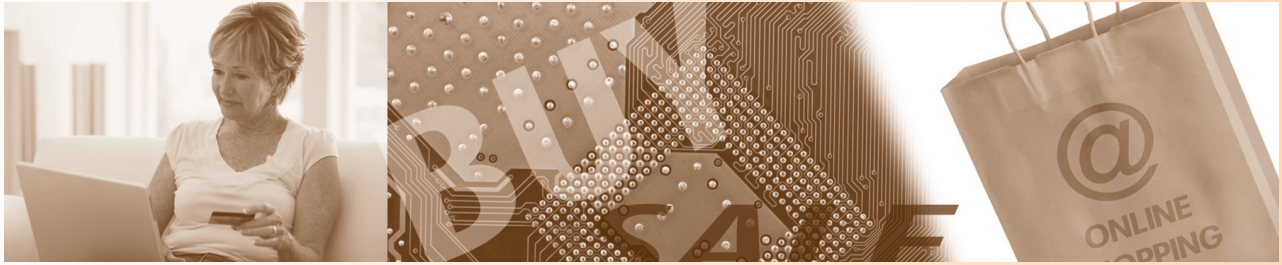
Next, try to remove the malicious code. If you have antivirus software installed on your computer, update the virus definitions (if possible) and perform a scan of your entire system. If you don't have antivirus software, you can purchase it at a local computer store.

If the software can't locate and remove the infection, you may wish to bring your computer to a local tech-support company for help. As with any purchase, conduct some research to find a company with a good reputation and online reviews; and contact the Division of Consumer Affairs to learn if complaints have been filed against any company you consider using.

US-CERT notes that, as a very last resort, you may choose to reinstall your operating system, usually with a system-restore disk that is often supplied with new computers. Be aware, however, that this will typically erase everything on your computer, including all files and any software you may have installed.

CYBER SECURITY

Chapter Two



A CONSUMER GUIDE TO CYBERSECURITY

The Problem: Confusing, Deceptive or Non-Existent Privacy Policies

Online Advertising: A Multibillion-Dollar Business

Computers have the capability to collect a great deal of information about you, and to transmit that information to third parties including advertisers and advertising networks.

America's online advertising industry generated $31.7 billion in revenue in 2011, an increase of 22 percent over the previous year, according to media reports. This big and competitive business is fueled in large part by the buying and selling of personal data, such as Internet browsing habits and user characteristics.

Advertisers want to learn all they can about you, in order to create ads finely calibrated to make you want to buy what they're selling. They have several ways of obtaining this data. They may contract with social networking websites. They may place cookies on your web browser to track your online behavior, or they may contract with the developers of smartphone applications – which can even use a GPS device to report on your physical location.
You have the right to protect your privacy by opting out of their tracking systems. You can

do this by managing the privacy settings on your social networking accounts, on your web browsers, and on your smartphone or other mobile device.

A Primer on Behavioral Advertising

"Behavioral advertising" involves gathering information on your online activities, and using it to target you with ads relevant to your apparent interests. Behavioral advertising companies typically seek to gather this information in ways you won't notice. For example, they might place cookies – small text files – on your Internet browser to track which websites you use and how long you remain on each page.

"First-party" behavioral advertising is limited to the confines of a single website. For example, if you browse a shopping website in search of a specific type of car, the site may make a note of your interests – and show car ads or recommendations for vehicles sold on the site.

"Third-party" behavioral advertising occurs when a company seeks to track your activities across multiple websites. The company might then use that information to target you with ads. Most cookies placed by third-party advertisers will track your activities even after you leave the company's website.

Web Browsers and Privacy Settings

Many web browsers have privacy settings that can instruct websites not to place third-party cookies on your computer – and, therefore, not to track your activities from one website to another. This chapter concludes with information on how you can adjust the privacy settings on the web browsers you use. But, as we shall see several times in this chapter, your privacy settings are not tamper-proof.

The Federal Trade Commission in August 2012 announced a $22.5 million settlement with Google, over charges that Google misrepresented certain privacy assurances to consumers related to cookies and web browsers. According to the FTC, Google misled users of the Safari web browser, by telling them Safari's default privacy setting would block third-party cookies. The FTC alleged that, despite making these promises, Google circumvented the Safari browser's default setting and placed advertising tracking cookies on users' computers for several months in 2011 and 2012.

Mobile Phones: "Your Apps Are Watching You"

Few devices know as much about you as your smartphone or tablet computer. Devices like the iPhone, iPad, and Android phone are capable of tracking your online activities and more. They may include a GPS that knows the device's current location, or a unique device ID (UDID) number that can never be turned off.

The debut of the iPhone in 2007 spawned a multibillion-dollar market for mobile applications, or apps – the games and other programs available for use on mobile devices. Today, more than 500,000 apps are available in the Apple App Store and another 480,000 in the Android Market. They have been downloaded 28 billion times by hundreds of thousands of users, according to a 2012 survey by the Federal Trade Commission (FTC). One observer called apps "the future of digital marketing" because of their use for everything "from watching movies to ordering groceries."

A large number of entertainment and educational apps are marketed specifically for children. More than a quarter of all parents have downloaded apps for their children to use, according to a 2012 study by the Joan Ganz Cooney Center at Sesame Workshop.

However, many apps have been found to transmit data about their users. A December 2010 Wall Street Journal study of 101 popular apps, headlined "Your Apps are Watching You," found that 56 transmitted the device's UDID to a third party, 47 transmitted the phone's location, and five sent age, gender, and other personal details to outsiders. The FTC reported in February 2012 that the great majority of children's apps are marketed without adequate privacy disclosures, which would help parents know whether they collect and transmit personal data.

The New Jersey Division of Consumer Affairs in June 2012 sued the California-based developer of some of the top-selling and most popular educational apps for children from preschoolers to second graders. Consumer Affairs investigators found its apps had transmitted personal information – including users' first and last names, as well as their phone's UDID – to a third-party data analytics company.

The company collected and transmitted this data without providing notification on its website and without obtaining verifiable parental consent. The lawsuit was the first filed in New Jersey under the federal statute, the Children's Online Privacy Protection Act. In a settlement, the app developer agreed to stop collecting data without the informed consent of parents, and to ensure the destruction of all previously transmitted data.

Parents should be aware that some apps have a built-in purchase mechanism which allows users to make purchases while interacting with an app (for example, enabling the user to purchase additional stories while using a storybook app). Some apps may also be integrated with social networks such as Facebook or Twitter. These apps may be marketed without information that would make parents fully aware of these capabilities, according to the FTC's study, titled "Mobile Apps for Kids: Current Privacy Disclosures are Disappointing."

Social Networking: How Exposed Is Your Life Online?

Facebook, MySpace, and other social networking sites have transformed the way millions of people connect with each other and share information. They have emerged as a powerful new medium – and an important potential data source for advertisers. New Jersey's State government uses Facebook and Twitter to communicate with the public, and the New Jersey Division of Consumer Affairs maintains its own Facebook page.

Facebook has more than 955 million active users; Twitter has more than 500 million active users; Google+ has 250 million registered users; LinkedIn has more than 175 million registered users; and MySpace reported 25 million unique U.S. visitors in June 2012.

However, you use these sites at your own risk – and at the risk of exposing your personal information to the world. **Nothing online is private.** Even the most ironclad privacy setting doesn't change the fact that whatever you post online – or send through a "secure" chat message – can be copied and shared with others.

The next chapter of this booklet deals with the dangers posed by sexual predators, cyberbullies, and their use of social networks and other platforms. This section, however, covers the limited control you can exert over your own privacy while using social networking sites responsibly.

In December 2009, the FTC accused Facebook of deceiving users by telling them they could keep their information private – and then repeatedly allowing their information to be shared and made public. Among other charges, the FTC argued that Facebook shared personal data with advertisers, after promising not to do so. In an August 2012 final settlement with the FTC, Facebook agreed to give consumers clear notice and obtain their express consent before sharing their information, and to obtain biennial privacy audits.

The FTC accused Google of deceiving consumers, and violating its own privacy promises, with the launch of its first social network, called Google Buzz, in 2010. Google launched the social network through its Gmail web-based email system. The FTC alleged that Google led Gmail users to believe they could choose whether or not to join the Buzz network, but the options for declining or leaving the social network were ineffective; and for those who joined, the controls for limiting and sharing their personal information were confusing and difficult to find. In its October 2011 final settlement with the FTC, Google agreed to implement a comprehensive privacy program as well as independent privacy audits for the next 20 years.

It's Too Easy to Share Too Much Information

Most social networking sites will ask you to create a personal profile with detailed information. You may be asked to identify your current and past places of employment, your education history, current hometown, and even your email address, cell number and instant messaging ID. All of this information can expose you to the possibility of identity theft or social engineering attacks, as described in Chapter 1 of this booklet.

As we will see in Chapter 3 of this booklet, predators have used personal information about victims in order to take over their email or social networking accounts. If you forget your password, most websites you do business with will ask security questions: "What was the name of your first pet?" "What was your mother's maiden name?" "What street did you grow up on?" If you post too much information online, criminals can use it to hack those questions.

Before posting that information online, consider that too much information in your public profile can also expose your political and religious views, relationships, or other sensitive information to third parties such as current or prospective employers, schools, friends and acquaintances, or business competitors. Indiscriminate public posts could harm your professional reputation, career and educational prospects, or personal relationships.

New Jersey lawmakers have proposed legislation that would prohibit employers from requiring employees or job applicants to give the employer the passwords to their social networking profiles.

As will be seen in Chapter 3, revealing too much about your day-to-day activities may expose you to danger, or your home to being burglarized when people know you'll be away.

Many social networking sites also allow other people to share information about you – or "tag" you in photos or videos – that you would prefer to keep private. The websites generally include privacy settings that give you some control over who can see your profile information, who can read your posts, who can "tag" you, and who can see items in which you have been tagged.

However, even the best and most clearly understood privacy settings do not change the possibility that anything and everything you post on a social networking site can become public – just as any email you send can be saved and forwarded to the world by a single person who receives it.

The Solution: Taking Charge of Your Privacy

Social Networking Sites: Use Common Sense

Some people become so comfortable with the Internet that they feel comfortable sharing information online that they wouldn't ever share with strangers on the street. Even with the best privacy settings, you should consider that what you post may be seen by others.

Use common sense at all times when posting information publicly online – whether providing details for your user profile, sending tweets, updating your status, posting blogs, or even sending messages that you believe are just between you and one other person.

Even if you are caught up in the moment, stop and think about what you're posting. How would you feel if it were seen by your employer, future prospective employers, your coach or teachers, your parents, children or friends? You should also consider the privacy of others, especially when posting a photo, video, or comment about a friend or relative.

Remember that even if you delete something you posted, it might still remain visible on web servers and accessible to search engines.

Social Networking: Evaluate Your Privacy Settings

Take the time to look for the privacy settings and privacy policies of any and all social networks, blogs, and other venues on which you have a profile and/or post information. If you can't find the privacy settings, contact the website publisher and ask for this information.

After adjusting your privacy settings, you should re-check them on an ongoing basis. It's important to remember that many social networking sites have changed their privacy settings and policies over the years. Be aware that those settings and policies may change again.

Social Networking: Defend Against Phishing and Malware Attacks

As noted previously, some posts or messages you receive through social networking sites may actually be phishing attacks or Trojan horses.

You also need to beware of third-party applications, such as games and quizzes, found on some social networking sites. Using these applications may expose your computer to malicious code – or may make your information available to advertisers.

Protect yourself by following the steps on pages 10 through 17. Protect your computer by keeping your antivirus software up to date. Protect your profile by using smart passwords. And always independently verify the authenticity of a message or invitation before you click on it.

Your Web Browser: How to Block Advertising Cookies
Protect Yourself: Check Your Web Browser

When using a web browser, it is a good idea to check the browser's privacy settings. Also consider whether you want to manually delete any cookies that may have been placed in your computer on a regular basis. Refer to pages 12 and 21 for additional information.

For information on how to adjust your browser's security settings, visit the website of the browser's vendor, or contact the vendor and ask for instructions.

Keep an Eye on Smartphone Apps

As noted above, many smartphone apps collect personal data and send it to a third party, or allow users to interact with social networking sites. Parents should communicate with their children about the games and educational apps they use on these devices. See "The Solution: Communicate and Empower Your Family" beginning on page 39.

CYBER SECURITY

Chapter Three

A CONSUMER GUIDE TO CYBERSECURITY

The Problem: Predators, Bullies and Inappropriate Content

Cyberstalking, Sexual Assault and Sexual Extortion

A Perth Amboy man pleaded guilty in August 2012 to sexually assaulting two teenage girls he stalked through Facebook. The 29-year-old created a profile using a fake name, pretending to be 17. He "friended" the 14-year-old girls, and began sending sexually explicit text messages.

One girl met with him in person. The other rejected his advances – but by reading her Facebook status updates he was able to track her whereabouts. Both girls were sexually assaulted.

Befriending teenagers with a fake online identity. Gradually coercing them with friendly, then flirtatious, then overtly sexual messages. Using a victim's online posts to learn when and where she would be hanging out. These are common ways sexual predators use the Internet.

One of the best-known cases of cyberstalking from the last decade is that of Jonathan Vance, who hid behind the screen name Metascape, according to media reports. He attempted to take over the Facebook, MySpace, and email accounts of more than 200 girls and young women, ages 14 to 26, and terrorized and blackmailed at least 53 of them into sending sexual photos of themselves.

He had several methods for gaining access to his victims' online accounts. In many cases he used information found on social networking sites and other online databases, such as their birth dates and the names of their schools and hometowns. As described on the previous page, he went to the girls' accounts, clicked the "Forgot Password?" button, and used that information to answer the security questions.

On other occasions, he would contact his victims through instant messaging. Pretending to be a friend or relative, he would say he was locked out of his own online account, and ask for the girl's online password to "borrow" her Facebook, MySpace or email account.

In all cases, once Vance had access to his victim's online account, he would immediately change the password – taking complete control over the account. He would then threaten

to humiliate the girls by posting embarrassing secrets or other information, unless they sent nude photos. In April 2009, Vance was sentenced to 18 years in federal prison.

The Crimes Against Children Research Center at the University of New Hampshire reported in December 2011 that the percentage of youth receiving unwanted online sexual requests declined from 13 percent in 2005 to 9 percent in 2010 – and noted that greater public awareness may have contributed to the decline.

Cyberbullying: Escalating, Long-Distance Cruelty

Cyberbullies use computers, cellphones, or other devices to harass, threaten, humiliate, or otherwise torment their peers. It may include hurtful text messages to the victim, or rumors spread through cellphones or online.

Teens have created web pages and videos to make fun of their peers; and have created fake, humiliating profiles of the people they wish to intimidate on social networking sites. Cyber-bullies have used mobile devices to take embarrassing photos or videos, and uploaded them for the world to see and discuss.

Some bullies find it easier to be vicious online because there is no personal confrontation. For victims, the viral spread of cruel words and pictures can make it feel as if everyone is aware of their humiliation; and the barrage of harassing emails and text messages can feel inescapable. The emotional consequences for victims can be devastating.

There have been numerous high-profile instances in which teenagers have committed suicide, at least in part because they were victims of cyberbullying. The Cyberbullying Research Center notes that all forms of bullying are connected with increased thoughts of suicide, and cyberbullying victims are almost twice as likely to have attempted suicide, as nonvictims.

Approximately 20 percent of 11- to 18-year-old students indicated they had been victims of cyberbullying, according to the Cyberbullying Research Center. The Crimes Against Children Research Center found that online harassment appears to be increasing for youth, particularly girls.

Sexting: Potential Lifetime Consequences

Sexting – the transmission of nude or sexually suggestive photos – has serious potential

consequences. About 4 percent of people ages 12 to 17 who own cellphones have sent sexually suggestive photos of themselves to someone else, and approximately 15 percent have received such images.

Some teenagers who sent sexual photos of themselves or others, have been charged with distribution of child pornography, and some individuals who received such photos have been charged with possession of child pornography. Violators may end up on their state's sex-offender registry.

An 18-year-old Ohio girl sent nude photos to her boyfriend – who circulated them to others after they broke up, leading to extensive and unremitting verbal humiliation and abuse at school. Two years later, she committed suicide.

Other Ways to Chat with Strangers

The Internet offers a seemingly endless variety of ways for users to meet strangers – and ways that children may be exposed to stalkers or inappropriate content.

Mobile phone apps: Mobile apps, and their GPS capabilities, bring the risks of meeting strangers to a new level. Skout, an app for flirting, lets users find and contact other users nearby. Its owners suspended the service for teenagers in June 2012, after three separate incidents in which adults, pretending to be teens, contacted youths on Skout and sexually assaulted them. The victims were two girls, ages 12 and 15, and a 13-year-old boy, according to media reports.

Video game consoles: Many video game consoles – such as Microsoft's Xbox, Sony's PlayStation and Nintendo's Wii – offer users the ability to browse the Internet, send and receive pictures and messages, and compete against players around the world.

Sexual predators have targeted children by finding them through video games – and many see them as the perfect way to make a child feel comfortable with a complete stranger. Grooming of a young victim may begin by communicating about the games they play, then developing a "friendship" and seeking to entice the child to meet them.

Anonymous chat rooms: Chatroulette and Omegle, both created by teenagers, are online chat sites that pair strangers together for video- or text-based conversations. A 2010 survey

conducted by the data analytics company RJMetrics, found that one in eight video pairings on Chatroulette yield "something R-rated (or worse)," although Chatroulette now reportedly flags users who broadcast sexual content.

The Solution: Communicate and Empower Your Family

The following tips are adapted from those offered by the National Center for Missing and Exploited Children (NCMEC) and its NetSmartz resources.

Set Rules For Your Children's Time Online

Post simple, clear, and easy-to-read rules indicating where and how you will allow Internet use in the home, and regularly review the rules with your children. Set limits on which websites your children can access, and when they can go online. Examples of rules can be found at **www.NetSmartz411.org.**

Remind children not to give out personal information, photos or videos, unless you have reviewed and approved of the materials they wish to post. Remind them of the risks, described throughout this handbook, posed by scam artists, hackers and predators.

Computers, video game consoles, and other devices that can access the Internet should be kept in the living room, or a similar place in the home where there is adequate adult supervision. Learn about the other places your child may access the Internet, such as friends' homes, libraries or schools. Have a plan in place to closely monitor your children's online activity, wherever they go online.

Consider giving your child a cellphone with limited Internet access, rather than a smartphone. Talk to phone manufacturers or dealers to learn about the options.

What if you're a parent who is not familiar with computers and the Internet? **The National Center for Missing and Exploited Children (NCMEC)** offers **www.NetSmartz411.org**, a resource for parents and guardians about Internet and computer safety; NetSmartz experts also provide direct answers by phone at **888-NETS411 (888-638-7411)**. NCMEC also provides **www.NetSmartz.org** with videos and tutorials for parents, educators, teens and younger children.

Sit down and talk with your children about the risks and benefits of responsible Internet use. Go online together, and have them show you the sites they visit and other ways they use the Internet; this can be a fun activity for you and your children.

To block pornography or other objectionable material, consider purchasing Internet filter and Internet monitoring software. Filters restrict access to certain types of websites, and can limit the amount of time children spend online. Monitoring software lets you track another person's activities on a computer. Remember that these tools are not foolproof, and they are not an adequate substitute for parental supervision.

Remind your children not to talk to strangers – and to communicate freely with you about anyone who contacts them.

The same rules apply for life online as for life in the world. In addition to the NetSmartz sites listed above, the **National Center for Missing and Exploited Children** provides important information at **www.MissingKids.com**, including the "Know the Rules" series on various aspects of child safety.

If your child tells you that someone he or she "met" online wants to meet in person, praise the child for telling you this; that will help keep the lines of communication open. If you suspect the person is an adult attempting to meet a child, contact the police – and file a CyberTipline report with NCMEC at **www.CyberTipline.com or 800-843-5678.**

If you want to consider a meeting, talk to the other child's parents or guardians. If you agree to the meeting, accompany your child and meet with the other child and his or her parents in a public place.

A Word for Adults Concerning Online Dating. Don't give your address or other personal information to anyone you don't know. If you choose to meet someone, meet for the first few times in a public place, and let a friend know where you're going and with whom you will be meeting.

Tips on Sexting and Cyberbullying

Talk with your children about the possible consequences of sending inappropriate pictures to anyone. Check your home computer and your child's cellphone for any pictures that can be misconstrued if seen by others. If you find inappropriate pictures, remove access to the Internet and take away digital cameras. Also, find out if the pictures were sent to anyone. Contact the **CyberTipline**, described above, if you find that sexually explicit pictures of your child are being circulated.

Make sure your child does not respond to rude and harassing emails, messages or web posts. Keep a record of them in case you need proof. Call law enforcement and inform your ISP if necessary. If your child continues to receive harassing emails, have him/her delete the current account and open a new one. The new email address should only be given to a few people who can be trusted with it. Help your child block instant messages or emails from the numbers or accounts of those who have been sending offensive messages.

If a cyberbully has set up a website to defame or mock your child, contact your ISP or the site administrator immediately. If necessary, inform law enforcement to try to get the website removed.

Get your child's school involved. Learn about the school's cyberbullying policy, and urge the administrators to **take a stand against all forms of bullying.**

APPENDIX I: If You Fall Victim to Identity Theft ...

IMMEDIATELY report any incident of identity theft to a law enforcement agency, i.e., your local police department, or to the Office of the County Prosecutor of the county where the theft is believed to have taken place. Once a report has been filed, request a copy of the report so that it will be available to send to credit reporting agencies and creditors.

File a complaint with the Federal Trade Commission at **www.ftc.gov/complaint or 1-877-438-4338;** TTY: 1-866-653-4261. Your completed complaint is called an "FTC Affidavit." Take your FTC Affidavit to your local police, or to the police where the theft occurred and your police report was filed.

Obtain a copy of your credit report from all three credit reporting agencies, by contacting:

Equifax Credit Information Services-Consumer Fraud Division
P.O. Box 740250
Atlanta, GA 303748
(800) 525-6285 • www.equifax.com

Experian
P.O. Box 1017
Allen, TX 75013-2104
(888) 397-3742 • www.experian.com/consumer
(800) 301-7196 (fax)

Trans Union
Fraud Victim Assistance Department
P.O. Box 6790
Fullerton, CA 92634
(800) 680-7289 • www.tuc.com

Additional assistance concerning how to obtain credit records can be obtained from the New Jersey Division of Consumer Affairs at **1-800-242-5846** or **www.NJConsumerAffairs.gov/credit.**

Report to the above credit reporting agencies the theft of any credit cards or credit card numbers and request that all your accounts be flagged with a fraud alert.

Contact all of your credit card companies, creditors, banks and financial institutions with whom you have a business relationship. Close affected accounts and get replacement cards with new account numbers. Change any passwords on the accounts, including PINs. Follow up all telephone contacts with a written confirmation.

Contact the United States Social Security Administration at:

Social Security Administration, Fraud Hotline
Office of the Inspector General
P.O. Box 17768
Baltimore, MD 21235
(800) 269-0271
(410) 597-0018 (fax)
www.ssa.gov/oig/hotline
oig.hotline@ssa.gov

Keep a complete set of records: Write notes and keep records of all telephone conversations with credit reporting bureaus, creditors or debt collection agencies. Confirm all telephone

conversations in writing. Keep copies of all correspondence sent and received. Send correspondence by certified mail, return receipt requested. Keep a record of the time spent and any expenses you incurred, in case you can request restitution in a later judgment or conviction against the thief.

You can also contact nongovernmental nonprofit groups established to provide assistance to victims of identity theft. For example:

Privacy Rights Clearinghouse
Identity Theft Resource Center
3108 Fifth Avenue, Suite A
San Diego, California 92103
(858) 693-7935
www.privacyrights.org
www.idtheftcenter.org

APPENDIX II: Additional Resources

The **United States Computer Emergency Readiness Team (US-CERT),** within the U.S. Department of Homeland Security, provides cybersecurity tips (including the basis for the tips in Chapter 1 of this booklet), as well as ongoing alerts, updates, and other valuable materials, at **www.us-cert.gov.**

The **Federal Trade Commission (FTC)** provides important cybersecurity information at **http://onguardonline.gov.**

The **National Center for Missing and Exploited Children (NCMEC)** offers important information about Internet safety, for parents at **www.NetSmartz411.org** with experts available by phone at **888-NETS411 (888-638-7411)**; and for teens and younger children at **www.NetSmartz.org.**

Additional information about cyberbullying and sexting can be found at the **Cyberbullying Research Center, www.cyberbullying.us.**

notes

notes

notes

The CYBER SECURITY Handbook

A CONSUMER GUIDE TO CYBERSECURITY

www.NJConsumerAffairs.gov ■ 1-888-656-6225

2013