TAKE A BITE OUT OF CYBER CRIME®

www.bytecrime.org

MIND WHAT YOU DO ONLINE

®

www.bytecrime.org

ABOUT "TAKE A BITE OUT OF CYBER CRIME"

McGruff the Crime Dog®, the National Crime Prevention Council (NCPC), the Forum to Advance the Mobile Experience (FAME), and the Chief Marketing Officer Council (CMO Council) have joined together to "Take A Bite Out Of Cyber Crime." The campaign is empowering and rallying millions of computer and digital device users in the battle against the continually growing plague of computer viruses, worms, spam, spyware, phishing, identity theft and online predators.

Presenters and Sponsors

The National Crime Prevention Council is one of America's most powerful forces for citizen mobilization. Prior to the 1980s, most people didn't believe that they had any useful role to play in preventing crime; they thought it was exclusively up to law enforcement to protect them. A quarter of a century later, thanks to NCPC and McGruff the Crime Dog®, that has changed—and for the good of all. Now people everywhere understand that preventing crime is their business!

Founded in 1982, NCPC promptly became the nation's focal point for crime prevention, undertaking efforts that, by 2005, had helped America achieve its lowest crime rate in more than 30 years. During NCPC's first 25 years, hundreds of millions of Americans learned from McGruff that they could "Take A Bite Out Of Crime®" and make themselves, their families, their workplaces, and their neighborhoods safer and better places to live. Studies in 1999 and 2000 documented that people who know McGruff are significantly more likely to take measures that reduce the risk of crime. Independent evaluations show that NCPC's work not only produces significant results but does so cost-effectively. **www.ncpc.org**

The CMO Council is an organization dedicated to high-level knowledge exchange, thought leadership and personal relationship building among senior marketing and brand decision-makers. It is an exclusive and influential peer-networking group of authority leaders in marketing under the direction of a rotating board of advisors and an annually elected chairperson. The CMO Council is an invitation-only affinity group working to further the stature, credibility, influence and understanding of the strategic marketing function among business executives, opinion leaders and critical stakeholders. CMO Council members are drawn from the upper echelons of corporate management to form a trusted, close-knit community of peers who use their access, connections and expertise for mutual benefit, support, referral and professional advancement. **www.cmocouncil.org**

The Forum to Advance the Mobile Experience™ (FAME™) is a member advocacy group and strategic authority leadership initiative to accelerate marketing programs and research around advancing the wireless user experience. Formed by the CMO Council, FAME promotes the adoption of wireless applications in the best interests of industry players. FAME brings together influential senior marketing leaders from top mobile technology companies who join in the pursuit of innovations and best practices tailored towards the advancement of end user wireless applications. **www.fameforusers.org**

TABLE OF CONTENTS

SM

Crime Fighting Goes Online

McGruff the Crime Dog® here… If I've learned anything in the past 26 years of fighting crime, it's that you need to be smarter than the crooks. Lately, they've found a new place to prowl – on the Internet. In the last five years, online crime – cyber crime – has really grown. In fact, last year the FBI Computer Crime Survey estimated annual losses from all types of computer crime at $67 billion a year. So join me now and let's work together to prevent cyber crime at home, at work and on the road. And let's start today!

McGruff the Crime Dog

NEW SPINS ON OLD SCAMS

Cyber crime affects all of us and comes in all shapes and sizes. Cyber scam artists drown us with spam– unwanted email that fills up our inboxes offering everything from cheap drugs, pornography, investment advice and get-rich-quick scams. Up to 80 percent of all emails are worthless junk that wastes your time or, if you take them seriously, can take you to the cleaners.

PHISHING – EMAIL THAT STEALS

Phishing is even worse than spam. Phishing is when crooks send fake emails that scare you into giving them private information, credit card numbers and online passwords, for example, then use that information to steal from you. This year, each time someone is caught in a phishing scam, it costs about $850, five times more than last year.[1]

SPYWARE: NASTY CODE THAT HITS WHERE IT HURTS

Cyber crooks also infect your computer with malicious stuff like spyware–software designed to watch your every move, and adware that buries you with pop-up ads. In the last six months, spyware infections forced nearly one million U.S. households to replace its computers. One in eight American Internet users had a major spyware infection costing an average of $100 to repair. Put all those spyware victims together and the damage added up to $2.6 billion last year.[2]

PROFIT AND PAIN THAT RUINS GOOD NAMES

Then there is identity theft: cyber crooks steal your identity and ruin your good name by taking out expensive loans, opening credit card accounts and writing bad checks. Last year, identity theft hurt 8.9 million Americans and cost each victim an average of $6,383. That adds up to $56.6 billion in damages from identity theft alone.[3]

The fact is, cyber crime hurts us because often we aren't doing everything we can to protect ourselves. One survey last year discovered that 81% of our home computers lack basic protection. More than half failed to have up-to-date protection against computer viruses and 39% did not have basic spyware protection. When experts tested home computers, 61% were infected with spyware – and even worse, only 46 percent of the people knew about it.[4]

It's time to put a stop to cyber crime. You can help the cops beat these thugs if you pay attention, get smart and protect yourself. To help you learn how, I worked with cyber security experts and other friends to create this booklet with practical tips to help you understand online risks and threats. You can learn even more at www.bytecrime.org. Join us and help "Take a Bite Out of Cyber Crime."

81% of our home computers lack basic protection.

Each time someone is caught by a phishing scam, it costs about $850.

Last year, identity theft hurt 8.9 million Americans and cost each victim an average of $6,383.

Is Your Home Cyber Safe?

I've worked for years to teach you how to prevent criminals from breaking into your house. Now it's time to lock up our computers, secure our wireless networks, help our kids online and make our homes cyber safe. Let's take a minute to look at all the ways that you can be hurt on the Internet.

First, you need to know who you are up against. If you think cyber crime is just kids having fun, think again. Today's cyber looter is older and smarter–and focused on stealing your money, not just getting your attention.

Watch out for Crimeware

Your computer can be infected in many ways, and viruses are just the beginning. Today, the main threats are adware and spyware. Adware either serves up annoying pop-up advertisements or tracks where you go online, or both. It slows down your computer and can even make it crash.

Spyware, software designed to track your every move online, is much worse. The mild stuff watches the websites you visit. The nasty stuff may record every key you hit, stealing your online passwords to rip you off. That's why you need to watch out for crimeware, so you can make sure you're safe and protected.

The Price of "Free" Stuff

All over the Internet, you can find free stuff. Search for free screensavers, music, videos and even little smiley faces and you will find lots of stuff to download – all free of charge. What you don't see is the real cost, the nasty surprise they fail to mention – adware and spyware, including crimeware that can steal from you.

New Spins on Old Scams

We all get spam – unwanted email that floods our inboxes to offer porn, low-cost drugs, investment scams, and other cyber garbage. Some spam tries to fool you into thinking you've won money, you can help someone recover money, or you have an investment opportunity that will earn big bucks in a hurry. The old rule of thumb still applies – if something sounds too good to be true, it probably is.

Email that Can Steal

Sometimes you receive official looking email that looks like it's from your bank, your Internet Service Provider, your credit card company or even the IRS. Open it and you'll see a warning that your account is about to expire or worse. To fix it, you need to click on a link to update your information, usually a Web-based form for entering your social security number, credit card or bank passwords. Don't do it.

This is called "phishing," and the cyber thief is trying to steal your credit card number and even your identity. Phishing uses your own fear against you, by threatening to take away something you value unless you act before you can think. Get smart. Call your bank, credit card company or service provider if you see a threatening email. They'll help you determine whether or not that email came from a crook.

The WebSite Shell Game

Crooks can also highjack Domain Name System (DNS) servers that directs you from one website to another, or they can corrupt your Web browser to take you to the wrong website. Here is how it works. You type in a World Wide Web address or click on a link in an email. You think you are going to one website, but really end up at a fake or spoofed site that looks like the real thing. At the fake site, you find many opportunities to enter your credit card number, maybe to buy something you want. You are rewarded by a cyber crook who steals your credit card number. This is called "pharming," where the cyber thief "harvests" your money.

Attack of the Zombies

"Bot herders" are another class of cyber crooks who try to take over your computer. They enter your computer through a corrupt website, through crimeware loaded in a free download, or by hacking into your PC. Once they are in your system, they install "bot" software that will secretly take over your computer and turn it into a mindless "zombie." These "bot-herders" build huge networks of computers they've taken over and rent out these networks to other crooks to send spam, and even attack other computers and networks.

Crimeware even your PC Can't See

Skilled cyber crooks also have created a new class of cyber threat called rootkits, designed to hide from your computer's operating system, and even from some security software. Once installed, rootkit malware is difficult to remove without crippling your computer system. The newest security software protects against these threats, but you have to make sure your security is up-to-date.

Wireless Sneaks, Thieves and Pickpockets

If you use wireless hotspots or home networks, you may be providing cyber crooks with a whole new way to rip you off. Without the right safeguards, Wireless Fidelity (Wi-Fi®) networks can let the bad guys capture everything you do online. With a little know-how and the right equipment they can tap into your Wi-Fi network connection and record everything you send and receive on the wireless network.

HOME SAFETY RULES
page 10

To prove what can be done, an expert built a computer specifically designed to eavesdrop on up to 300 wireless access points at the same time, downloading and saving all the information going to and from those access points.[5]

Failing to lock down your wireless home network can hurt you in other ways. Two Florida college students learned that lesson the hard way when the cops stopped by as part of a pornography investigation. Turns out their neighbor was downloading porn using their college network connection.[6]

In spite of stories like these, a lot of folks leave their wireless networks wide open. In fact, recent research shows that 40 percent of consumers failed to even turn on the most basic wireless security.[7] Why? Often they feel it's too difficult or they don't know how to secure their network.

If you don't know how, either buy wireless protection software or hire someone to do it. We are in a war between the good guys and cyber criminals who want to steal your information and ruin your lives. To fight these crooks, we need to lock down everything we can.

Cyber Predators and Pedophiles

Sexual predators are a parent's worst nightmare. In cyber space, they lurk in Web communities and playgrounds where your children like to hang out, such as the social networking sites that have become so popular. MySpace, with nearly 100 million members,[8] and Facebook are two online communities that attract these predators.

MySpace, Facebook and other social sites are no worse than the mall, beach or playground; in fact the same rules apply for parents. Keep an eye on your kids, know who their cyber friends are and make sure they don't do anything foolish. That other "kid" in the chatroom, blogging, emailing or instant messaging your child could be a sexual predator.

1. Secure your computer before you go online. The minimum you need is strong anti-virus, anti-spyware and anti-spam security along with a strong personal firewall to prevent hackers from sneaking in your computer.

2. Keep your security up-to-date. Cyber crooks continue to develop new crimeware and other nasty stuff. Security companies constantly research and update their protection, which you need to make sure your computer – and your family – remain safe from cyber crime.

3. Use a website rating service to help you avoid the "dark alleys" on the Internet. Several free services rate websites based on whether they offer nasty downloads, drown you with spam or infect your computer merely by visiting the site.

4. Avoid free screensavers, smiley faces and other free stuff unless you absolutely know the download is safe. It's the safest way to make sure you don't infect your computer with crimeware, adware and other nasty stuff that can steal your information and ruin your computer.

5. Safeguard your private information. Lots of websites offer benefits to folks who provide personal information that they turn around and sell to advertisers, marketers and sometimes crooks. Before you fill out that form, make sure you want whatever it is they are offering. The price may be too high.

6. Set up a free Web-based email address and provide that address to websites whenever you sign up for anything. That way, a lot of the spam will go to that free account instead of your personal inbox.

7. Create complex usernames and passwords for websites and email addresses. That makes it harder for the cyber crooks to break into your online accounts and steal your information or money.

8. Call your bank, service provider or institution to verify any emails before you click on any links or fill out any forms. Also remember, the IRS NEVER emails taxpayers, so anything from the IRS is really a phishing scam.

9. Avoid pop-ups (Web browser windows that pop up) like the plague. If you have a newer computer, pop-ups are usually blocked by default. Keep it that way. Above all, never enter personal information in a pop-up window, since it could be a phishing site. Be smart and don't become another identity theft victim.

10. Get a credit report from all three major credit reporting agencies at least once a year. The law says you can get a free annual report, which allows you to review your credit and check to see if someone has opened accounts in your name. If you find anything wrong, contact the credit agencies to report the error.

11. Review every credit card statement. If a charge looks suspicious, contact your credit provider to have it removed to help avoid future losses.

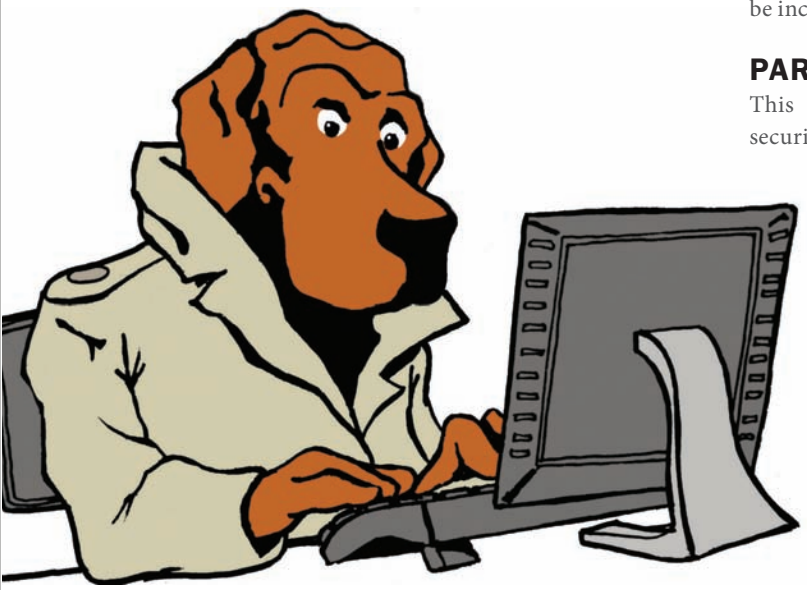
12. Take care when shopping online: Look for indicators that the website is secure, like a small lock icon on your browser's status bar, a trusted seal like those from VeriSign or TRUSTe and a website URL that begins with "https" (that "s" stands for "secure").

13. Lock down your wireless home network. If you don't know how, hire someone to help you or use wireless protection software that makes wireless security easier to manage. Unprotected wireless networks invite cyber crooks to rip you off.

14. Turn on or buy parental controls for your computer to manage when your kids can go online, and limit them to approved, safe websites. Some parental controls even limit your children's ability to share or download files, helping to ensure they don't load your system with spyware.

15. Watch and guard what your children post online. Kids don't know how risky and dangerous the world can be. If they use social networking sites, check their profile and review the photos and stories they post. You are not being nosy; you are being a good parent. They need to know that anyone can see what they post online, including parents AND sexual predators. Contact the website if you find anything that should be removed.

16. Review your children's instant messaging buddy lists. The last thing you want is to learn a sexual predator is exchanging messages with your kids. We owe it to them to protect them from these criminals.



HOME SECURITY Safeguards and Solutions

INTERNET SECURITY SUITES

Internet security suites include anti-virus, anti-spyware and anti-spam protection, and a personal firewall, all in one package. Most suites include automatic updates to make sure your protection remains up-to-date with the latest threats and risks. The best suites also include tools to back up your valuable files and maintain your computer system.

WEBSITE RATING SERVICES

These are services that focus on testing websites to see whether they include risky downloads, load your system with spyware or deluge visitors with spam. One of the best-known services is McAfee SiteAdvisor. You can download it for free at **http://www.bytecrime.org/security_center/store.html**

WIRELESS PROTECTION SOFTWARE

Wireless protection software makes it easier to secure and manage your home wireless network. It also makes it easy to share printers and files over the secured network. Wireless protection software is available as a standalone product and may also be included with some Internet security suites.

PARENTAL CONTROLS

This security software is included with several security suites and is also available as a standalone product. Buy it, install it and use it. Kids may not think it's fair, but it's much safer than leaving them unprotected.

BIOMETRICS

Several companies now offer security products that use your fingerprint or other personal features to make sure only you or people you approve can access your computer. You can use these tools to safely store passwords and keep your kids from outsmarting your parental controls.

Risks When You're Remote

Cyber safety at home is one thing; it's even tougher away from home. That's why you have to be careful every time you go online, whether you are at a cyber café, in a hotel business center or using a laptop at a coffee shop.

RENTING TIME ONLINE

Sometimes the easiest way to access the Internet away from home is to use someone else's computer. If you travel around the world, you can find a cyber café almost anywhere you go. Just remember, online safety doesn't stop when you leave your home.

Whether you go to a cyber café, a business center or even your public library, remember that anyone walking behind you can see what you are doing. Someone can steal your passwords, see where you bank and learn a lot about you, just by looking over your shoulder.

That computer you are using may not be secure. Don't assume that the person who owns that PC knows about cyber crime. Their security may be incomplete, outdated or weak.

The Web browser on that computer will also have a record of each site you visited that anyone with a little computer knowledge can find. Don't make it easy for the next person using that computer to find out where you went online.

If you download and save anything on the desktop, a trace remains on the computer's hard drive, even if you erase it. To be safe, you need to make sure you don't leave anything important behind for the next person to find.

COMPUTER LAB/CYBER CAFÉ RULES page 16

DANGER! NO WIRES, NO SECURITY

I see people using wireless networks everywhere I go, in coffee shops, airports, hotels, bus stations, restaurants and even in the park. I wonder if those people know the risks they may be taking.

You see, wireless networks may be convenient, but they are also dangerous. If you use a wireless network without locking down your connection, any cyber thief with the right technology know-how can see and steal any information you post or enter online. That includes passwords, personal information and possibly even credit cards and financial information.

Easier than Listening Through a Keyhole — Wireless Snooping

Here is the problem. On a normal network, a cyber crook who wants to steal from you must break through layers of security to access your personal transactions, private messages and online habits. With wireless networks, the crooks can eavesdrop on your network connection and literally pull your information out of the air. It's like having someone look over your shoulder and track everything you type and send online over your wireless connection, with one major exception: You can see when someone is looking over your shoulder. But you won't know about the cyber thief until it's too late to protect yourself.

Rogue Hotspots — Real Connection, Real Ripoff

It gets worse. Some crooks set up rogue hotspots to lure unsuspecting people to use their networks. This "free" access looks and seems legitimate. The problem is that once you access the "hotspot," the crook who set it up can monitor everything you do online, stealing your usernames, passwords, bank account information, credit card information and every other shred of data you type while online.

Hiding your Connection in a Tunnel

The only way wireless networks can be safe is if the wireless connection is encrypted. That can happen one of two ways. Home wireless networks should have strong encryption turned on to protect the network and your connection. If you are using a public network, you need a virtual private network (VPN) to be safe. A VPN acts like a secure, encrypted tunnel that links your wireless laptop to a secure network, usually at your workplace. Without a secure network or a VPN, cyber crooks can see everything you are doing online.

WIRELESS RULES
page 18

Locking your Front Door — But Leaving the Wireless Network Open

I talk about home wireless networks in the home security section, but one concern I have is worth repeating: 40 percent of all wireless home networks fail to turn on any security at all.[9] Why? The owner feels like it's too difficult to set up wireless security, or doesn't understand the risks. To fight these crooks, we need to use every layer of security we can. If you don't know how to set up wireless security, then call in an expert, use special wireless protection software that makes it easier, or consider not using a wireless.

MOBILE CYBER SAFETY

Even an old crime fighter like me knows you don't need a computer to go online anymore. Everywhere I go, I see people using smart phones and other mobile devices to read email and surf the Web. One research firm has projected that by 2007, 58 million business users worldwide will potentially use wireless email.[10] However, before you rush out and buy a smart phone, you should understand the dangers and risks involved with these mobile devices.

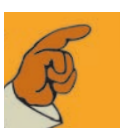
Easy to Use, Lose and Steal

You see, in reality, these devices are not just phones; they are powerful, tiny computers. That means they can be hacked and can get viruses. In fact, most of the risks involved with wireless network security apply to mobile devices. On the other hand, the mobile operator or carrier usually takes care of securing the network and the device.

Because they are small, mobile devices can be easy to lose and easy to steal. That places all of the information in your email, online habits and other confidential treasures out in the open where a cyber thief can steal them.

Who is Texting your Kids?

If you provide your kids with a mobile phone, they also may be sending and receiving text messages, which can be risky on several levels. How do they and you know who is exchanging text messages with them? Sexual predators often master the technologies that kids like. Also, text messages go to a mobile phone number. Do your children know who has access to their cell phone number?



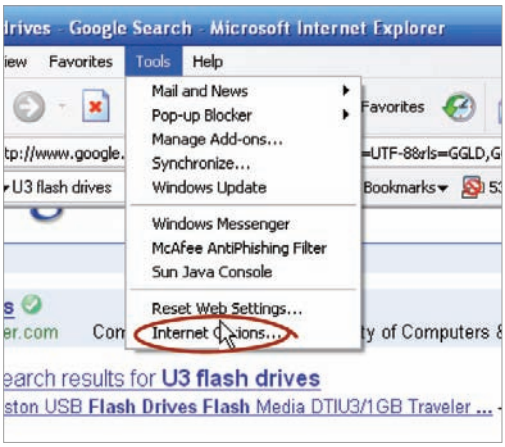
MOBILE SAFETY RULES
page 20

1. Find out what kind of security is loaded on the PC you're using, and make sure it's up-to-date. If the computer is not secure, don't use it.

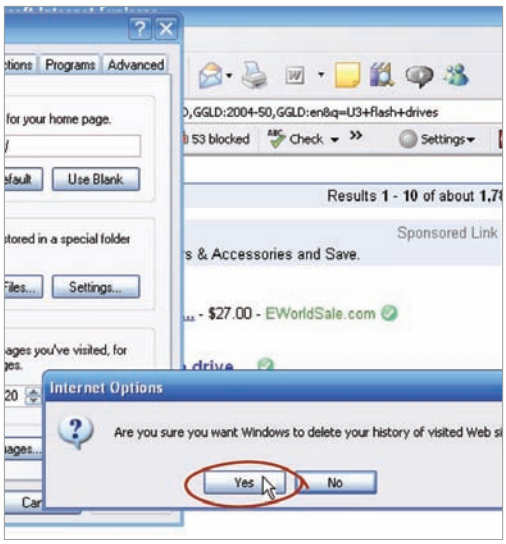
2. Save any documents you download directly to your own portable storage (floppy disk or USB flash drive) – not on the computer, especially if those documents are private.

3. Clean out the browser cache on the PC (that's the part that tracks where you've been online) to wipe out your online trails before you finish using the computer. This is easier to do than it sounds. Most of the time you will use Microsoft Internet Explorer, so here are step-by-step instructions for how to clean out the browser's cache.

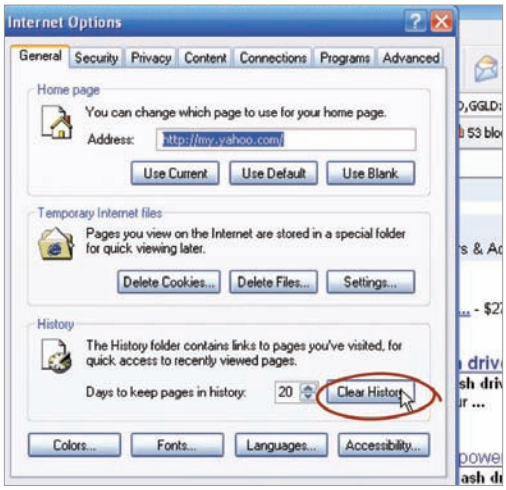
STEP 1. In the top menu, click on "Tools," then when the menu drops down, click on "Internet Options."



STEP 2. That will open a box called a "dialogue box." Near the bottom, you will see "History" with a button that reads, "Clear History." Put your mouse on that button and click.



STEP 3. Another box will appear asking you if you really want Windows to delete your history of visited websites. Click "Yes."



COMPUTER LAB/CYBER CAFÉ Safeguards and Solutions

USB FLASH DRIVES

PROS: Easy to carry, stores large files and works on most computers. You can store important documents directly on the flash drive, so it never leaves a trace on the PC hard drive.

CONS: Standard USB flash drives are not very secure. Because they are so portable, you can easily lose them, and anyone with access to a PC can access your files. If you forget to delete the browser cache on the PC, someone can still follow your online trail.

SECURE USB FLASH DRIVES

Provide secure, encrypted storage for storing large files and important documents.

U3 SMART DRIVES

These are USB flash drives with special software to mimic a personal computer that you carry with you. By using a U3 drive, you can carry your email, personalized Web browser, instant messaging, word processor and other tools and programs, all stored on the flash drive.

1. Secure your home wireless network with strong encryption. This security protects the data that is sent over the air and locks hackers out of your network. If you don't know how to set up encryption, there are software products that can walk you through the process and ensure you have the strongest security.

2. Avoid connecting to any Wi-Fi network unless you either know it's secure or you can set up a secure VPN connection. That goes for all public wireless networks, including the ones you subscribe to in the airport as well as the free networks now available in cities across America.

3. Confirm the Wi-Fi network you are accessing is legitimate. A recent test at Chicago's O'Hare airport revealed that more than 90% of wireless networks available in the passenger terminals were rogue connections with more than 80% advertising "free" Wi-Fi access.[11]

4. Use a virtual private network work connection to protect your wireless connection any time you connect to an insecure network.

5. Make sure the personal firewall on your laptop is turned on and updated. Consider cranking up your firewall settings when you use a wireless hotspot connection to make sure no cyber crooks wirelessly break into your PC. Your information going online is still visible, but at least the bad guys can't hack into your computer.

6. Turn off the wireless network connection on your laptop when you are not using it. That step will force you to manually review and select wireless network connections, not just the first one you find. It's a simple, effective way to stay safe.

7. Avoid using any websites that require password access when using a wireless hotspot. The last thing you want to do is provide a cyber crook with your username and password.

8. Never fill out forms that require confidential and personal information when using a wireless connection. You certainly don't want to give away those secrets to the wrong person, so keep it confidential.

9. Look around when you are online. Who can see your screen while you are online? Is anyone overly interested in what you are doing? Even cyber crooks will use a conventional way to find your private information, if you let them.

10. Keep your laptop with you at all times to ensure your private information stays private. Leaving a laptop open and running in a public place is an invitation to steal from you.

WIRELESS Safeguards and Solutions

WIRELESS PROTECTION

Use wireless protection software to set up a secure wireless home network. If the process feels too intimidating, hire a security service to do it for you. If it's worth going wireless, it's worth doing it right.

COMPLETE, UPDATED SECURITY SUITES

Get a complete security suite that provides multiple layers of protection (anti-virus, anti-spyware, anti-phishing, anti-spam along with a personal firewall). Make sure your security suite updates automatically.

VIRTUAL PRIVATE NETWORK (VPN)

Many businesses provide employees with virtual private networks to establish secure, encrypted connections to the company network. A VPN is the most secure way to go online on public wireless networks.

ENCRYPTION SOFTWARE

Encryption software can encrypt all of the data on your computer's hard drive, protecting you from any liability you may face if documents and plans fall into the wrong hands.

COMPUTER LOCKS

Sometimes the best way to restrict access to your computer is to literally lock it up. These locks work like bicycle chains and locks. They may be ugly, but computer locks are an effective deterrent.

BIOMETRIC SECURITY

Passwords can be cracked, but your fingerprint, retina print and iris (the colored part of your eye) are tough to fake. Biometric devices store your fingerprint, iris print, or other personal feature unique to you, making it much harder for the crooks to access your computer.

1. Keep your device with you at all times. Small and convenient works both ways, for you and for the cyber crook. Store the device in your pocket or purse; chain it to your wrist, just keep it with you at all times.

2. Lock down your mobile device. Make sure you have a strong password so if anyone does find your device; they'll have to work hard to crack your code.

3. Make sure all communication between your mobile device and your carrier or operator is fully encrypted. Most carriers can make sure all email and other information flying through their mobile networks are fully encrypted and safe.

4. Find out if your company or carrier has mobile device management capabilities that can remotely kill your device if it's ever lost or stolen. It's a sure way to protect confidential information if the worst ever happens and you lose your device.

5. Keep your mobile online habits out of the driver's seat in your car. Maybe it won't stop a cyber crook, but at least you won't get into an accident because you were distracted by your smart phone.

6. Monitor what your kids do with their mobile phone. Review their contact lists and make sure they exchange messages and phone numbers with people you trust.

7. Use a family-friendly cell phone service with child-safe phones for younger children. These services allow parents to define who can be called, how long the phone can be used and what children are allowed to do, keeping them safe.

MOBILE Safeguards and Solutions

MOBILE ANTI-VIRUS SOFTWARE

While mobile viruses and spyware are relatively new, protect yourself. The relatively low cost of protection provides great peace of mind when faced with the chance some cyber criminal will unleash a nasty mobile virus in the near future.

MOBILE FIREWALL SOFTWARE

Just like your PC, mobile devices can be hacked, so it makes sense to prevent anyone from accessing your personal and business information.

FAMILY–FRIENDLY MOBILE SERVICES

These services allow parents to define who can be called, how long the phone can be used and what children can do with their mobile phones.

CHILD-SAFE CELL PHONES

These phones are designed specifically for children, with limited buttons and features. Parents define who the phone will call, plus they usually have a button reserved for emergencies that calls 911.

Threats Faced in the Workspace

Most workplaces now use the Web to research, communicate and collaborate. The Internet makes us more productive, more informed and more in sync with our coworkers. Unfortunately, going online also exposes us – and our employers – to risks, threats and vulnerabilities and online crime. This section breaks out workplace security into three distinct subsections for people who work in a corporate office, at home or in a small business.

STAYING SAFE IN THE OFFICE

People who work in a corporate office usually have a technology pro who manages the security for all computers and related devices. Most organizations also have a security policy that sets the rules for using workplace computers in order to maintain security and keep things running. Your work policy may also include additional regulations to make sure employees use company computers for work, not personal business.

Computers in the workplace have different security software than consumers' PCs. Security is normally centrally managed and updated, and employees access the Internet from behind a corporate firewall, rather than having a personal firewall loaded on their PC. Any time you take your work laptop outside of the company network you face different risks and threats.

Keeping your Personal Life Personal

In your office, you deal with coworkers who may wander over to your desk and see what you are doing. Anything you print can be read or intercepted by coworkers. If you leave your PC on and unlocked, coworkers can also access your personal files when you are away from your desk. If they want to steal company secrets, files or data, they may choose to use your computer, so if the theft is discovered, you will get the blame.

If you use your PC for personal business, coworkers may be able to pick up private information and even access your online accounts – especially if you write down passwords where people can find them. The same risk applies if you allow your PC Web browser to remember your access informtion.

Infectious Fun and Games that Make the Network Sick

Co-workers often share jokes and multimedia files at work, which can introduce spyware and other malicious software into the network, where it can spread quickly if left unchecked.

While the workplace is in many ways more protected from cyber threats than your home, you still need to remain on guard.

OFFICE SECURITY RULES
page 26

SECURITY FOR TELECOMMUTING FROM HOME

If you have a company laptop, you may use it to work from home or take it with you when you travel. Any time you take a business laptop out of the corporate network, you expose it to risks it would not otherwise face when behind the corporate firewall. Unless you have a hardware firewall on your home network, your corporate laptop may be vulnerable to hackers outside of the office network. Laptops are easy to steal and easy to lose. Losing the data stored on the computer, or even worse, having unauthorized people steal it, can be devastating to your employer and to you.

While you are out of the office, you may be tempted to visit questionable websites or use your work computer for activities that violate corporate policy. Don't. That behavior can expose your PC to malware and crimeware infections that can potentially infect the whole office when you return.

Locking your Wireless Window – Keeping your Privacy Private

If you use your office PC to access unsecured wireless networks, you can also expose your computer to unforeseen risks. Any neighbor with the right know-how may be able to intercept and steal proprietary information from your work PC that could potentially jeopardize the business. Cyber criminals and crooks can also use an unprotected wireless network to hack into your work computer and load bot software, keyloggers and other spyware and crimeware onto your system that can then infect your coworkers when you return to the office.

While your work computer is at home, family or friends may be tempted to use it, without understanding the risks involved. Since you will be held responsible for anything that happens to your computer, they could get you into a lot of trouble.

SMALL-OFFICE AND HOME-OFFICE RISKS AND VULNERABILITIES

If you own a business, you already understand the responsibility you face in securing and maintaining your computer, network and any related devices and printers. Unless you hire someone, as the business owner, you are also the IT staff. If something breaks, you have to fix it yourself or buy a new one.

As a small business owner, you are also exposed to lots of new risks. Phishing in particular is a major concern, since you may be working with people you do not know. Other attacks can render your PC completely useless, which makes prevention doubly important since you cannot work without your PC. That vulnerability also exposes you to other targeted denial of service attacks from cyber crooks who want to distort your policies and practices so they can steal your information.

You may use a broadband Wi-Fi network as your primary office network. If you have secured it, that is wonderful and you may go online safe with the knowledge that you and your coworkers are protected. If you have not secured this network, you may be placing your entire business at risk of identity theft.

Friends and family who may not be computer literate may want to use your PC while visiting your home or small business office. While they may not have any intention of harming anything, they place your computer and potentially your entire business at risk if they download spyware or crimeware, or inadvertently change any settings on your computer.

If you work from a home network that includes other PCs, you may also expose your work computer to threats from any PC on your network that has been compromised. Attachments sent by contractors, or even employees, may potentially include malicious crimeware and spyware. No matter what the problem is, you remain stuck with the task of fixing it, no matter how limited your technology expertise.

TELECOMMUTING RULES
page 28

1. Learn your corporate security and technology policy – and follow it. Policies are set to prevent dangerous behavior that could threaten the business, your computer, the network and you.

2. Make sure your work computer has security software installed that is up-to-date. While an IT support pro may be responsible for maintaining and securing your computer, you are the one who pays if anything goes wrong.

3. Take responsibility for your work computer. Get to know the IT support staff and work with them to make sure everything is shipshape with your PC before you have a problem. It's a good way to avoid problems that affect your ability to do your job.

4. Password protect your office computer and any personal files on your PC. This rule is particularly important if you travel with your laptop, to make it harder for strangers to access your PC. Whenever you leave your desk, lock down your PC. It's a good way to eliminate temptation for coworkers to check out your PC.

5. Limit the use of your work computer for personal business. You can install privacy screens and other security measures, but the best way to keep your personal business personal is to keep it off your work computer.

6. Choose to remember your passwords, rather than let your PC browser do it for you. Your coworkers should not have access to your passwords in any way, because they can then use your access to steal information, violate security policies and download illicit files in your name.

7. Keep your passwords to yourself. Don't write them down where any visitor to your desk can see them. Walk by cubicles in any large office and you'll see many Post-It notes on computer screens with the employee's password. It's an unsafe practice.

OFFICE SPACE Safeguards and Solutions

ENCRYPTED USB FLASH DRIVES AND U3 DRIVES

The safest way to protect your personal and sensitive work information is to keep it with you at all times. Store sensitive files on encrypted USB drives, and take the drive with you whenever you leave your desk. These handy drives also make it easier to take work home with you if necessary. IMPORTANT: Some highly secure businesses prohibit USB flash drives to make sure secrets stay at the office and don't leak out on someone's memory stick.

BIOMETRIC SOLUTIONS

Fingerprint scanners and other biometric devices provide an enhanced way to prevent unauthorized access to your computer. Highly secure offices, such as military or police agencies, use a combination of biometric devices and tokens to verify your identity before providing you with access to the computer or the network.

PRIVACY SCREENS

Privacy screens mount on your computer display to make it hard for coworkers to look over your shoulder at your work. If you have a standard laptop, the screen is often difficult to see at an angle, and privacy screens may not be necessary.

SECURITY SOFTWARE

Most of the time, your security department or IT department will determine what security software is installed on your computer. It's often a good idea to ask the support professionals about the software so you can stay more informed and do a better job of abiding by the corporate security policy.

ENCRYPTION SOFTWARE

Encryption software can secure all of the data on your computer hard drive, protecting you from any liability you may face if documents and plans fall into the wrong hands.

COMPUTER LOCKS

Sometimes the best way to restrict access to your computer is to literally lock it up. These locks work like bicycles chains. They may be ugly, but computer locks are an effective deterrent.

WEB SITE RATING AND SAFE SEARCH TOOLS

If the corporate policy permits it, consider downloading and installing a Web safety rating tool. These tools will identify risky websites and help keep you away from the Internet's dark alleys.

1. Observe your corporate security policy, no matter where you use your work computer. This rule will keep you away from dangerous websites that can infect your PC and get you into trouble.

2. Connect your laptop to your company's virtual private network every time you go online. As I noted elsewhere in this booklet, a VPN acts like an encrypted tunnel between your PC and your corporate network, preventing anyone from accessing your PC or the information going back and forth to the corporate network. Because the VPN connection places your computer behind the corporate firewall, it then has the same protections you enjoy when using your PC in the office.

3. Make sure all access to your work computer is password protected, along with any sensitive files. Lock down your computer any time you leave it unattended at home, so no one is tempted to use it. Remember, you are liable for anything that happens to your work computer at home, plus you are responsible if someone uses it to steal any corporate secrets.

4. Consider encrypting all the files and emails on your work computer – if your corporate policy allows it. By encrypting all that data, you add an extra measure of protection in case your laptop is lost or stolen. You also reduce any potential liability your company might face if a customer's private information was stored on your work computer's hard drive.

5. Make sure the security software installed on your work laptop is up-to-date. Work with your IT support team to make sure you can maintain your security software while working from home.

6. Avoid letting your Web browser remember your online passwords. While it may be inconvenient, this practice makes it twice as hard for a friend, family member or even a cyber crook to access restricted websites and your email if they somehow gain access to your computer.

7. Change your work-related passwords regularly to limit the chance that someone will guess them. Always make it as hard for the bad guys as possible to access your computer and your information.

TELECOMMUTING Safeguards and Solutions

VIRTUAL PRIVATE NETWORK

Make sure you have VPN software installed on your laptop and test your connection before leaving the office to make sure it works properly. This is one of the most important steps to keeping your work PC secure away from the office.

BIOMETRIC SOLUTIONS

If your work policy allows it and your IT staff support it, consider adding biometric tools to restrict access to your laptop and sensitive files. These tools can also securely store online and work-related passwords to minimize concerns about forgetting them while keeping them safe from prying eyes.

ENCRYPTION SOLUTIONS

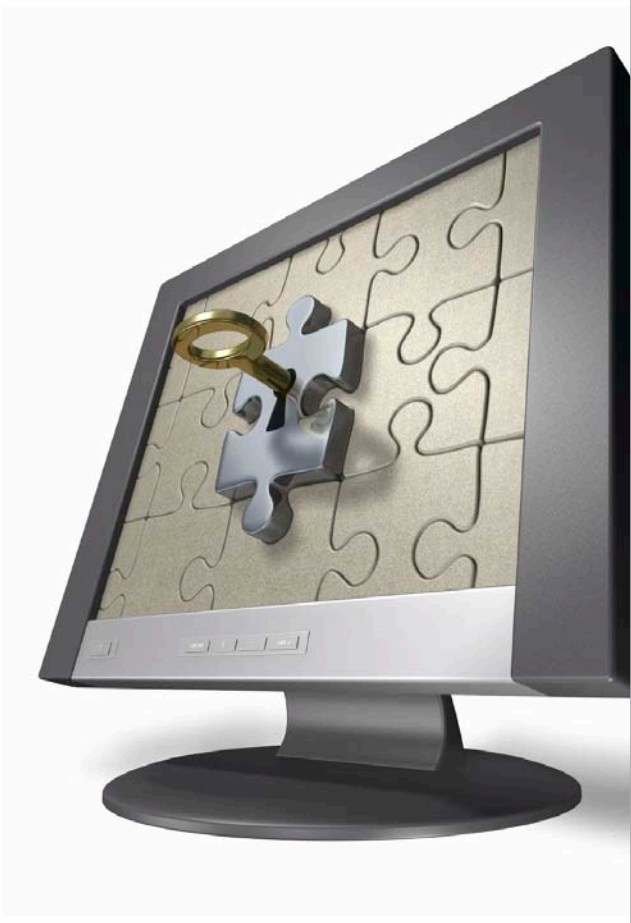
Work with your IT department to install encryption for your sensitive files and email. You can make the case that several laws reduce liability exposure when encryption software and measures are in place.

COMPUTER LOCKS

Sometimes the best way to restrict access to your computer is to literally lock it up. These locks work like bicycles chains. They may be ugly, but computer locks are an effective deterrent.

WEB SITE RATING AND SAFE SEARCH TOOLS

If the corporate policy permits it, consider downloading and installing a Web safety rating tool. These tools will identify risky websites and help keep you away from the Internet's dark alleys.



McGruff's Safety Rules

1. Purchase and install comprehensive security on your computer. At minimum, you need strong anti-virus, anti-spyware and anti-spam security along with a strong personal firewall to prevent hackers from sneaking onto your system. Secure your computer before you go online.

2. Keep your security up-to-date. Cyber crooks continue to develop new crimeware and other nasty stuff. Security companies constantly research and update their protection, which is important to keeping your business computer and your business safe from cyber crime.

3. Make sure all access to your work computer is password protected, along with any sensitive files. Make sure you lock down your computer any time you leave it unattended at home. Remember, your business may depend on your ability to protect your business computer and everything stored on it.

4. Encrypt all the files and emails on your business computer. By encrypting all that data, you add an extra measure of protection in case your laptop is lost or stolen. You also reduce any potential liability your business might face if a customer's private information was stored on your work computer's hard drive.

5. Consider hiring a managed security service to manage and maintain your business computer security. These services may also help you with complex business security issues and ensure your security remains comprehensive and up-to-date.

6. Purchase, install and use VPN software on your home server and your laptop to ensure your laptop remains safe when using Wi-Fi hotspots and remote connections. You may want to contract with a security service to manage this process.

7. Avoid letting your Web browser remember your online passwords. While it may be inconvenient, this practice makes it twice as hard for a friend, family member or even a cyber crook to access restricted websites and your email if they somehow gain access to your computer.

8. Change work-related passwords regularly to limit the chance that someone will guess them. After all, it's your business at stake if someone accesses your private information. Always make it as hard for the bad guys as possible.

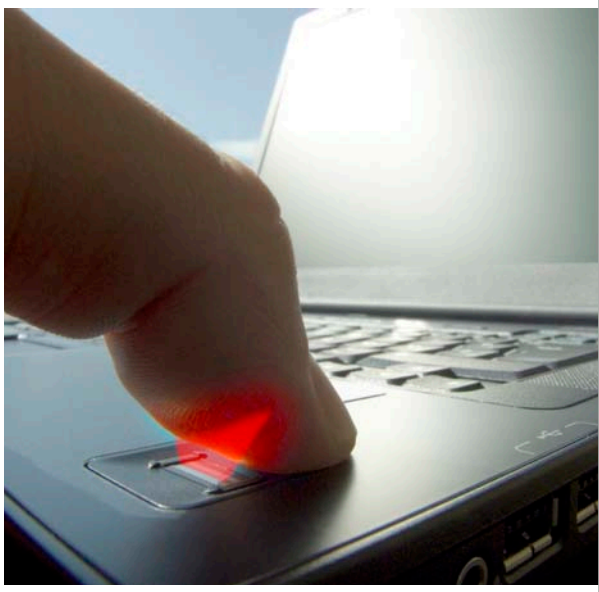
SMALL-OFFICE/HOME-OFFICE Safeguards and Solutions

VIRTUAL PRIVATE NETWORK

If you plan to travel or work outside of your office, set up a desktop computer as your office server, then install a VPN between your laptop and the office server. Since this process can be complex, you should consider contracting with a security service to manage this process.

BIOMETRIC SOLUTIONS

Buy and use biometric tools to restrict access to your laptop and any other business computers and sensitive files. These tools can also securely store online and work-related passwords to minimize concerns about forgetting them while keeping them safe from prying eyes.



ENCRYPTION SOLUTIONS

Install strong encryption to protect your sensitive files and email. If you store clients' or customers' private information, encryption can also reduce your potential liability in the event a computer is lost or stolen.

COMPUTER LOCKS

Sometimes the best way to restrict access to your work computer is to literally lock it up using computer locks that work like bicycles chains. They may be ugly, but computer locks are an effective deterrent.

WEB SITE RATING AND SAFE SEARCH TOOLS

Download and install a Web safety rating tool. These tools will identify risky websites and help keep you away from the Internet's dark alleys.

Repairing Cyber Crime Damage

Because prevention is the best cure for cyber crime, most of this booklet focuses on how to avoid it. However, even the most prepared cyber crime fighter can fall victim to spyware, crimeware and identity theft. Here are some tips to help you stop the damage and recover from cyber crime.

STOPPING MALWARE AND REPAIRING DAMAGED SYSTEMS

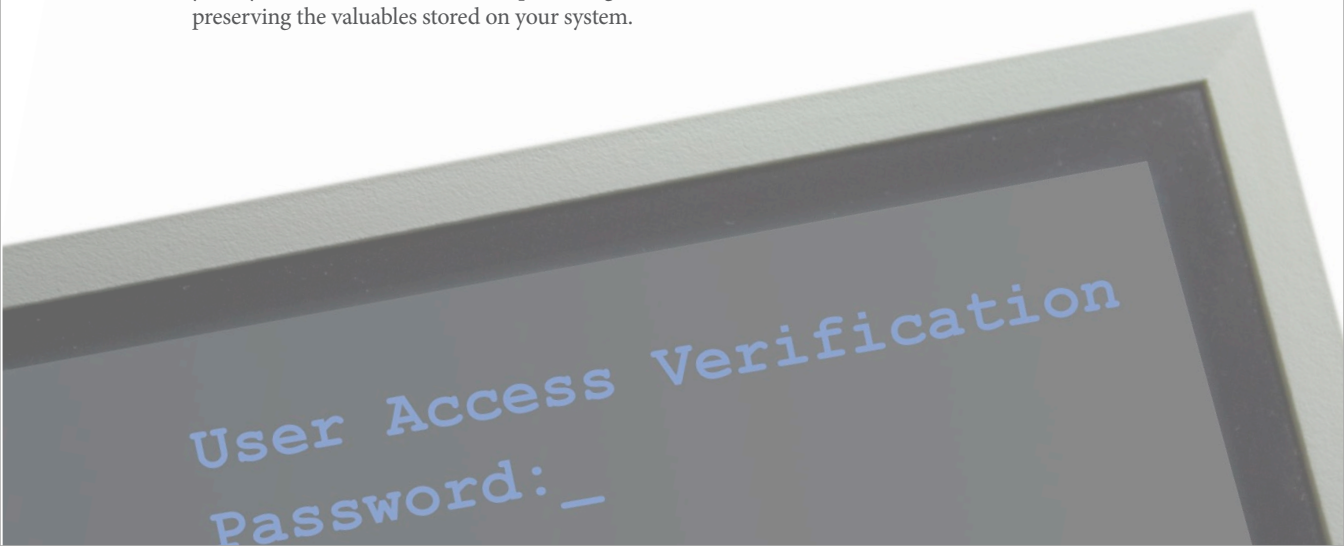
If you ever suspect some form of spyware, malware or crimeware has infected your computer, unplug or turn off your network connection and shut it down. While you are offline, do a full security scan with your security suite. If you've kept your security updated with automatic updates, chances are it will detect and quarantine the nasty software, and potentially delete it.

Once you've completed the scan, you need to recover your system. Microsoft Windows XP provides the option of restoring your system to previous settings, before the infection or attack. If this process seems too complicated, now may be a good time to call in a computer repair service to restore your system. Then use your backed-up files to replace any vital documents or other treasures that were lost or damaged from the cyber crime. The important thing is to get your system back to normal, while protecting and preserving the valuables stored on your system.

GETTING YOUR IDENTITY AND YOUR LIFE BACK

If you work hard to protect yourself online, you should be able to avoid becoming an identity theft victim. However, sometimes our best efforts to protect ourselves can fall short. If someone steals your identity or your credit card, here are some practical steps to minimize the damage and recover your life.

RECOVERY STEPS
page 28



1. Abort and Report: Close up shop and notify your credit card companies, financial institutions or other online service accounts about the fraud immediately. The longer you wait, the more time cyber criminals can play on your dime.

2. Contact the local police to file a report. Ask for a copy of the report, since you will need it to work with creditors to fix your credit.

3. Report the fraud to one of the credit reporting agencies (Equifax, Experian and TransUnion), which will prevent the identity thief from opening additional accounts in your name. Call only one—each is legally required to contact the others. That fraud alert then entitles you to free copies of your credit report, which you can use to identify and correct any fraudulent charges and make sure those charges won't smear your good name. After the first credit report, keep checking regularly to make sure no new identity theft crimes take place.

4. Close any accounts you suspect are compromised. Contact the security or fraud department of each business, then follow up in writing and include copies of supporting documents. Send all letters and documents by certified mail, return receipt requested, so you can prove which documents were sent, when they were sent, and when they were received.

5. If you spot bad charges, ask for the forms you need to dispute those transactions. Once your dispute has been resolved, request a letter that shows your account has been closed and the fraudulent debts removed. This letter will also help if further disputes come up.

6. File a complaint with the Federal Trade Commission. By sharing your experience, you help law enforcement track down identity thieves and cyber crooks. The FTC also investigates businesses that violate consumer privacy laws.

7. Reclaim your personal identification. Contact the agency that issued your driver's license or other identification. Follow its procedures to cancel and replace your identification or driver's license. Ask the agency to flag your file so that others cannot get a license or any other identification document in your name.

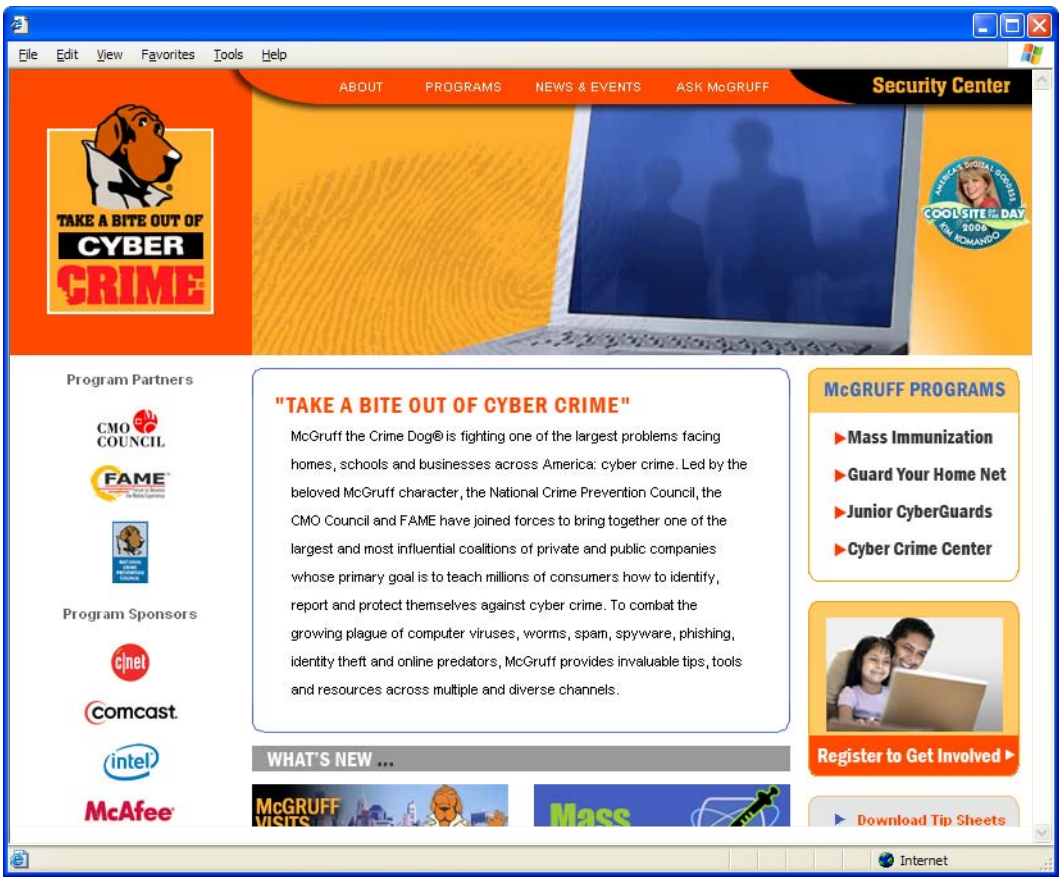
McGruff's Cyber Crime Fighting Tools and Resources

To win this fight against cyber crime, we all have to get smart, protect ourselves and everything that is important to us. You've taken the first step by reading this booklet and learning about all the ways cyber crime can hurt you.

Now it's time to take what you've learned and put it into action. To learn how, go to my new website at **www.bytecrime.org.** I have some friends who are experts in cyber security. They have put together some good tools and information to help you get smart and protect yourself. Check them out at **http://www.bytecrime.org/security_center/store.html**

It's a good place to learn how to lock down your computer and your networks, and how to protect our kids from dangers they are too young to see.

We have a lot of work to do before we stop online crime. Join me in this fight and help me "Take a Bite Out of Cyber Crime."



FOOTNOTES

[1] Consumer Reports, State of the Net 2006, August 2006, http://www.consumerreports.org/cro/electronics-computers/online-protection-9-06/state-of-the-net/0609_online-prot_state.htm

[2] Consumer Reports, State of the Net 2006, August 2006, http://www.consumerreports.org/cro/electronics-computers/online-protection-9-06/state-of-the-net/0609_online-prot_state.htm

[3] Javelin Strategy & Research, "2006 Identity Fraud Survey Consumer Report," http://www.javelinstrategy-com/uploads/603.R_2006IdentityFraudSurvey.pdf

[4] AOL and the National Cyber Security Alliance, "Online Safety Study," December 2005, http://www.staysa-feonline.info/pdf/safety_study_2005.pdf#search=%22AOL%2FNCSA%20Online%20Safety%20Study%2C%20December%202005%22

[5] TG Daily, "A Wireless Hacking Computer that Can't Be Hacked," August 30, 2006 http://www.tgdaily.com/2006/08/30/defcon2006_janus_project/print.html

[6] BusinessWeek, "5 Steps to a Safe Wireless Network," June 15, 2006 http://www.businessweek.com/technology/content/jun2006/tc20060615_290127.htm

[7] Jupiter Research, Home Wi-Fi Security: Understanding Consumer Behavior and Impact on Wi-Fi Adoption, June 22, 2006

[8] CNET News.com, "MySpace Blurs Line Between Friends and Flacks," July 31, 2006 http://news.com.com/MySpace+blurs+line+between+friends+and+flacks/2009-1025_3-6100176.html

[9] Jupiter Research, Home Wi-Fi Security: Understanding Consumer Behavior and Impact on Wi-Fi Adoption, June 22, 2006

[10] Portio Research, "Mobile Messaging Futures 2005-2010."

[11] PC Magazine, "Security Watch: Crimeware, SMiShing, and Cross-Platform Worms," Thursday, Septem ber 14, 2006

"Every parent in America needs to read this to protect themselves and their children. There's no reason to be a grim statistic. Knowledge is power."

—Kim Komando, Host of the Kim Komando Show and USA TODAY *Technology Columnist*

"Cyber crime can reach into your house, pocketbook and family in ways you may not have recognized. This booklet is a great place to start learning how to protect yourself."

— Parry Aftab, Internet privacy and security lawyer, author, A Parents' Guide to the Internet... *and* How to Protect your Children in Cyberspace, *executive director of WiredSafety.org, TeenAngels.org and StopCyberbullying.org.*

"It's no secret that the Internet is a powerful tool for families, businesses– and criminals. This booklet is a comprehensive up-to-date guide for parents and children to help equip them to stay safe online and prevent cyber crime."

— Donna Rice Hughes, President of Enough Is Enough (enough.org and protectkids.com) and author, Kids Online: Protecting Your Children in Cyberspace.

Every parent in America needs to read this to protect themselves and their children. There's no reason to be a grim statistic. Knowledge is power.

— Kim Komando, host of the Kim Komando Show and USA TODAY *Technology Columnist.*