

Transforming Victims Into Cyber-Border Guards

Education as a defense strategy

Jeannette Jarvis
Group Program Manager - PSS Security
Microsoft

Protect Your computer

video

Agenda

- Introduction to End User Security Awareness
- End User Security Awareness Challenges
- Understanding End User Security Awareness
- Developing End User Security Awareness Initiatives
- Using Security Awareness Materials and Resources
- Examples of Security Awareness Campaigns
- Best Practices
- Summary

Introduction

- Why implement a security awareness campaign?
 - Communicate policy to the user community and encourage compliance
 - Mitigate the Security versus Usability equation
 - Defend against social engineering threat components
 - User awareness enhances the overall security profile
- What do we want to accomplish by making users aware of security?
 - Encourage safe usage habits and discourage unsafe behavior
 - Change user perceptions of information security
 - Inform users about how to recognize and react to potential threats
 - Educate users about information security techniques they can use
- How do we get the desired results?
 - Build interest
 - Educate
 - Communicate
 - Repeat

End User Security Awareness Challenges

- Delivering a consistent message about the importance of information security
- Convincing user to develop and maintain safe computer usage habits
- Motivating users to take a personal interest in information security
- Giving end user security awareness a higher priority within your organization
- Developing materials that deliver a clear message about security topics

Positioning End User Security Awareness For Business

- End User Security and Awareness programs reside in the Policies, Procedures, and Awareness layer of the Defense in Depth security model
- User security awareness can affect every aspect of an organization's security profile
- User awareness is a significant part of a comprehensive security profile because many attack types rely on human intervention to succeed



The Business Case For End User Security Awareness

2006 E-Crime Watch Survey¹

- 63% of survey respondents reported security incidents that resulted in operational losses
- Insiders were responsible for 27% of all incidents and 55% of respondents reported at least one incident that was the result of insider activity

2006 CSI/FBI Computer Crime and Security Survey²

- 43% of respondents view user awareness training and education as the most critical security issue in their organization

2005 Committing to Security Benchmark Study³

- Human error, not systems weakness, is the leading cause of serious security incidents

1. The E-Crime Watch Survey is sponsored by CSO Magazine in cooperation with CERT, Microsoft Corporation, and the U.S. Secret Service
2. The CIS/FBI Security Survey is sponsored by the Computer Security Institute and the U.S. Federal Bureau of Investigation
3. The Committing to Security Benchmark Study is sponsored by CompTIA

The Personal Case For End User Security Awareness

- Online Survival Guide, Consumer Reports, September 2005
 - Americans have spent \$9 billion to repair problems caused by viruses and spyware over the past two years
 - Nearly 65% of internet users have experienced a computer virus infection over the past two years
 - It's estimated that more than 2 million children nationwide have inadvertently viewed pornographic content
- AOL/National Cyber Security Alliance Online Safety Study, December 2005
 - Nearly one in four Americans are affected each month by phishing attacks designed to enable identity theft
- Internet Security Threats, Better Business Bureau, November 2005
 - 79% of computer users want to learn more about how to protect themselves and their computers from viruses and spyware

End User Awareness Business Process

Recommended six phase end user awareness process

1. Planning

- Ownership
- Funding
- Roles

2. Development

- Campaign Materials
- Awareness Content
- Delivery Methods

3. Deployment

- Pilot Deployment
- Message Refinement
- Final Deployment

4. Assessment

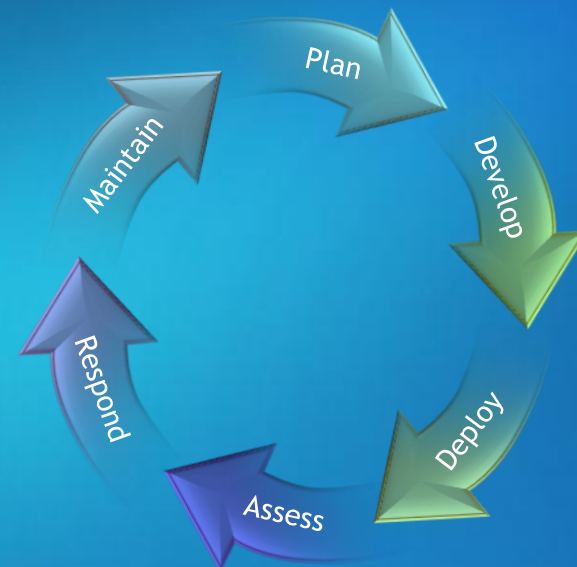
- Pre-assessment
- Pilot Assessment
- Questionnaires

5. Response

- Policy
- Communication
- Refinement

6. Maintenance

- Business Changes
- Technology Changes
- Threat Changes



What Users Need To Know

Users need to know about information security issues that affect their work, their home, themselves, and their families. They need to understand the threats and risks as well as the methods they can personally use to defend against those threats.

- Malware
 - Defending against Viruses and Threat and the appropriate software
- Spyware
 - Anti-spyware techniques and understanding End User Agreement language's role
- Scams
 - Recognizing Scam messages, social engineering attacks, and spam
- Safe Internet and Email Usage
 - Protecting the workplace and family from unwelcome or unsafe content
- Account Security
 - Strong Password practices and using appropriate account privilege levels
- Information Theft/Identity Theft
 - Shredding confidential documents, protecting personal and private information from theft
- Physical Security
 - How to protect data on mobile devices and why premise security is important
- Regulations, Policies, and Trust
 - What regulations affect information security and why security policies exist

Motivating The End User Community

Understand the human side of the security equation and use it to tailor the security awareness message for the audience it needs to influence

- **Self Interest**

- People tend to retain facts better when they can personally identify with or use that information personally, show how organizational security policies can translate to safe home usage practices as well

- **Memory Persistence**

- Current news stories or recent situations that affected the organization recently help reinforce the consequences of security lapses better than outdated stories no matter how sensational they may be

- **Perceived Importance**

- Policy adherence depends on perceived importance, communicate the need for stated security policies in context and enforce existing policies

- **Self Efficacy**

- People are more inclined to follow procedures that they feel they have an good understanding of so users who understand the concept of complex password creation policies are more likely to follow those principles

Overcoming The Hurdles To Security Awareness

Effective End User Security Awareness initiatives are not merely training sessions, they are concerted efforts from the top down focused on changing behaviors and encouraging a security minded culture.

- End user security education is not a one-way knowledge transfer, reinforce the messages often and get feedback on the effectiveness of the program.
- Make security threats seem real and pertinent, make it believable.
- Use social marketing techniques to encourage safe practices, make security seem interesting and cool.
- Make security less of a hurdle to productivity, show how unsafe practices and shortcuts can actually hinder productivity by introducing risks.
- Don't fall victim to the "Do as I say and not as I do" trap, enforce security policies fairly and consistently, lead by example!
- Acknowledge the different learning styles

Education Awareness Opportunities

Internal security web site

Targeted articles on internal company news site

Internal blog

Mandatory security training

Annual security forum

Surveys

Computer Security Day

Awareness

Enterprise Computing Annual Newsletter

Usability Study

Monthly attention grabbing security info tip

Tips and Tricks for home use brochures

Prize drawings for those who complete training and surveys

Lunch time 'Brown Bag' briefings

On-going Awareness team

Targeted Awareness Campaigns

Target Factory Workers or least experienced computer users

Team meeting Presentations

Pop-ups or Toolbars for Critical Information Sharing

“What to do if you’ve been phished”

Focus on Company Policy

Emphasis Identity Theft

Offer employees home use security software

Posters

Good Password Practices

Pamphlets

Malware Specific

Magnets with critical info links

Screensavers

Patch Awareness

How your Security Tools Work

Lunch & Learn

Brown Bag Lunch Topics



Credit Card Security

Password Management

Keeping Personal Information Safe

Internet Threat briefing

Phishing education

Tell-tale signs of a virus

E-mail scams

Personal and home security

Physical security

Privacy

What to do if...

Evil Twin Attacks

Regulatory Compliance

How to Use Firewalls

Social Engineering

Keeping Kids Safe Online

Product Usage Demos

Spam Specific

Security Certification Training

Threat Landscape

Tools & Techniques

Security Resources

Phishing Specific Education Program

- Phishing targeting relevant business operations
 - Corporate credit card
 - Company credit union
 - Customer and Partners
 - On-line businesses
- Some targeted programs are valid business applications
- Key-logging a security risk for our enterprise



Computer Security Day

- Kiosks strategically placed
 - Demos showing
 - Weak passwords; Phishing attacks; Malware attacks; Evil Twin attack; Recognizing spam; Spoofing; Keylogging
- Provide list of security courses
 - Internal and external offerings
- Brochure and checklist for home and office
- On-line quizzes

Measuring Effectiveness

How many employees clicked on the 'more information' link on our Company news articles

How many employees hit your tips and tricks link off security Web site

Which employees comprised the % that did not take the mandatory training

Add Security Training to all employee's Performance Development Plan

End User Security Awareness Resources

- Microsoft Security at Home - <http://www.microsoft.com/athome/security>
 - Useful services, resources, and information to help users and families improve online safety
- Staysafe - <http://www.staysafe.org>
 - Home page for the non-profit Staysafe organization that offers online safety educational content for end users, educators, and families
- GetNetWise - <http://www.getnetwise.org>
 - Home page for the GetNetWise non-profit organization with information about online safety for children and adults
- OnGuard Online - <http://onguardonline.gov>
 - Resources and information from a coalition of different governmental agencies concerning online safety and security awareness topics

End User Security Awareness Resources

- i-SAFE - <http://www.isafe.org>
 - Non-profit organization site dedicated to outreach and educational campaigns to keep children safe online, provides educational materials, services, and courses for teachers, students, parents, and law enforcement agencies
- NetSmartz - <http://www.netsmartz.org>
 - Online partnership between the National Center for Missing and Exploited Children and the Boys and Girls Club of America that offers online child safety information and materials for educators, parents, law enforcement, and children
- CERT Coordination Center Home Network Tips - <http://www.cert.org/tech-tips/home-networks>
 - This FAQ offers some more detailed technical information for end users about information security and what they can do to protect their home networks

Best Practices

- Communicate to Users How this is important to them personally
 - People are more receptive to information that affects them personally or that they can identify with. When training give examples to how safe usage not only applies to the workplace but how it can be used at home as well
- Discuss Safe Practices in context with examples
 - Security awareness can seem dry to some people, keep everyone's attention by citing examples the audience can identify with, use audience participation techniques, and convey the potential consequences with recent organizational incidents or recent high profile media events
- Inform users of security initiatives that may affect them
 - Keep everyone in the loop and keep communication lines open. Create an information security group with members from different business groups to establish lines of communication about security initiatives, get buy-in from management, and let the end user community know why security policies are necessary
- Understand the importance of End User Security Awareness Efforts
 - Remember that vulnerabilities are not only exploited from the outside, but can also be exploited from within your organization. Approach security awareness with the same seriousness as any other security related initiative, give the users the tools to help with security efforts

Security At Home
What's New
Latest Security Updates
Download Security Products
Protect Your Computer
Protect Yourself
Protect Your Family
Resources
Worldwide Sites

security at home



Protect Your Computer →

Four steps to help you protect your computer from viruses, spyware, identity theft, and more.

[Learn More](#)

Protect Yourself →

Internet safety guidelines to help protect against spam, identity theft, e-mail hoaxes, and more.

[Learn More](#)

Protect Your Family →

Advice and tools to help protect your family from inappropriate content and contact, viruses, identity theft, and more.

[Learn More](#)

Get Windows Vista today.



See special offers.



Identity Theft

[Taking your laptop with you on summer vacation?](#)

See tips for keeping your computer, your data, and your precious vacation time trouble-free.

[Check your password strength](#)

Spyware & Viruses

[Weird error messages, inexplicable crashes and restarts, sloooooow computer performance?](#)

Know the signs that indicate your computer might be infected with a virus.

Newbie Corner

[Block unwanted instant messages](#)

Learn how to use the Contact List feature of your instant messaging software to let friendly messages in and help keep intrusive messages out.

Spotlight



[Download the June security updates](#)

Help keep your computer secure. Get the latest updates for Microsoft Windows.

Blog: Security Tips & Talk

[About our blog](#)

[Identity theft Web sites triple in one month](#)

June 7, 2007

[Want information about our security bulletins sooner?](#)

June 6, 2007

Downloads, Products, & Services

Protect Your Computer from spyware and other unwanted software

- [Windows Defender](#)
- [Windows Live OneCare](#)
- [Windows Live OneCare Safety Scanner](#)
- [Microsoft Update](#)
- [Internet Explorer 7](#)
- [Windows Vista](#)

Protect Yourself from identity theft, fraud, and spam

- [Microsoft Phishing Filter](#)
- [2007 Microsoft Office System](#)

Protect Your Family from unwanted content and contact

- [Xbox Family Settings](#)
- [Windows Live OneCare Family Safety \(Beta\)](#)
- [Windows Vista: Parental Controls](#)

Related Links

[Microsoft Security Portal](#)

Related Links

[Controls](#)

• [Windows Vista: Parental](#)

[Safety \(Beta\)](#)

• [Windows Live OneCare Family](#)

- Security At Home
- What's New
- Latest Security Updates
- Download Security Products
- Protect Your Computer
- Protect Yourself
- Protect Your Family
- Resources
- Worldwide Sites



How to help your kids use social networking Web sites more safely

Published: November 9, 2006



You may already know that blogging—keeping a public "Web log" or personal journal online—is common among teens and even younger kids.

Now kids can also create personal Web pages on social networking Web sites hosted by services like [Windows Live Spaces](#), MySpace, Friendster, Facebook, and others. These Web pages can often be viewed by anyone with access to the Internet.

With these services, which are extremely popular among teenagers, kids can fill out profiles that can include:

- Photos
- Videos
- Personal information such as full names, locations, and cell phone numbers

Often the services that host the social networking sites provide several different ways for people to communicate with one another, including blogging and instant messaging features.

Kids use social networking sites to connect with kids who might live halfway around the world and with kids whom they pass every day in the hallways at school.

Social networking can provide a helpful way for kids to express their emotions or even to perform unofficial background checks on other kids they meet at parties and at school. For example, after they meet another kid in person, a kid might visit that other kid's Web site to find out if he or she might be someone they'd like to be friends with.

Unfortunately, the information that kids post on their pages can also make them vulnerable to predators.

Here are several ways you can help your kids can use social networking Web sites more safely.

- **Set your own house Internet rules.** As soon as your children begin to use the Internet on their own, it is a good idea to come up with a list of rules that you all can all agree on. These rules should include whether your children can use social networking Web sites and how they can use them. For more information on setting rules, see [Using family contracts to help protect your kids online](#).
- **Ensure your kids follow age limits on the site.** The recommended age for signing up for social networking sites is usually 13 and over. If your children are under the recommended age for these sites, do not let them use the sites. It is important to remember that you cannot rely on the services themselves to keep your underage child from signing up.
- **Educate yourself about the site.** Evaluate the site that your child plans to use and read the privacy policy and code of conduct carefully. Also, find out if the site monitors content that people post on their pages. Also, review your child's page periodically. For more suggestions, see [Tips on blogging safely for parents and kids](#).
- **Insist that your children never meet anyone in person that they've communicated with only online, and encourage them to communicate only with people they've actually met in person.** Kids are in real danger when they meet strangers in person whom they've communicated with only online. You can help protect your children from that danger by encouraging them to use these sites to communicate with their friends, but not with people they've never met in person.

It might not be enough to simply tell your child not to talk to strangers, because your child might not consider someone they've "met" online to be a

stranger, but not with people they've never met in person. You can help protect your children from that danger by encouraging them to use these sites to communicate with people they've actually met in person. Kids are in real danger when they meet strangers in person whom they've communicated with only online, and encourage them to

- Security At Home
- What's New
- Latest Security Updates
- Download Security Products
- Protect Your Computer
- Protect Yourself
- Protect Your Family
- Resources
- Worldwide Sites



10 things you can teach kids to improve their Web safety

Published: September 20, 2006



Before you allow your child to go online without your supervision, make sure you establish a set of rules that you can all agree on.

If you're not sure where to start, here are some ideas on what to discuss with your kids to teach them about using the Internet more safely.

1. Encourage your kids to share their Internet experiences with you. Enjoy the Internet along with your children.
2. Teach your kids to trust their instincts. If they feel nervous about anything online, they should tell you about it.
3. If your kids visit chat rooms, use [instant messaging \(IM\) programs](#), online video games, or other activities on the Internet that require a login name to identify themselves, help them choose that name and make sure it doesn't reveal any personal information about them.
4. Insist that your kids never give out your address, phone number, or other personal information, including where they go to school or where they like to play.
5. Teach your kids that the difference between right and wrong is the same on the Internet as it is in real life.
6. Show your kids how to respect others online. Make sure they know that rules for good behavior don't change just because they're on a computer.
7. Insist that your kids respect the property of others online. Explain that making illegal copies of other people's work—music, video games, and other programs—is just like stealing it from a store.
8. Tell your kids that they should never meet online friends in person. Explain that online friends may not be who they say they are.
9. Teach your kids that not everything they read or see online is true. Encourage them to ask you if they're not sure.
10. Control your children's online activity with advanced Internet software. Parental controls can help you filter out harmful content, monitor the sites your child visits, and find out what they do there.

[↑ Top of page](#)

Printer-Friendly Version Send This Page Add to Favorites

Related Links

- [Kids and the Internet: Frequently asked questions](#)
- [Using family contracts to help protect your kids online](#)
- [Helping kids tell fact from opinion on the Internet](#)
- [Help prevent online piracy at home](#)

Safety tips by age

Get tips by age to help guide your children's use of the Internet:

- [Up to age 10](#)
- [11-14 years old](#)
- [15-18 years old](#)

For more about each of these stages, read [Age-based guidelines for kids' Internet use](#).

- Security At Home
- What's New
- Latest Security Updates
- Download Security Products
- Protect Your Computer
- Protect Yourself
- Protect Your Family
- Resources
- Worldwide Sites

[Security At Home](#) > [Personal Information](#)

Password checker

Your online accounts, computer files, and personal information are more secure when you use strong passwords to help protect them.

Test the strength of your passwords: Enter a password in the text box to have Password Checker help determine its strength as you type.

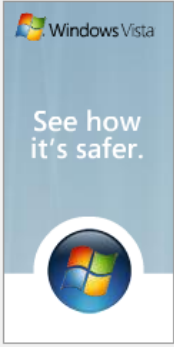
Password:

Strength: **Strong**

Note: Password Checker can help you to gauge the strength of your password. It is for personal reference only. Password Checker does not guarantee the security of the password itself.

Related Links

- [Strong passwords: How to create and use them](#)
- [How to recognize spoofed Web sites](#)
- [Shop online more safely](#)



Do you use strong passwords?

A strong password should appear to be a random string of characters to an attacker. It should be 14 characters or longer, (eight characters or longer at a minimum). It should include a combination of uppercase and lowercase letters, numbers, and symbols.

For tips on how to create passwords and pass phrases that are easy for you to remember but difficult for others to guess, a strong password checklist, and more, read [Strong passwords: How to create and use them](#).

About Password Checker

Password Checker does not collect, store, or transmit information beyond the computer that you use to access Password Checker. The image works on your computer desktop until you navigate away from the page.

The security of the passwords entered into Password Checker is similar to the security of the password you enter when you log into Windows. The password is checked and validated on your computer, but is not sent over the Internet.

Was this information useful?

[↑ Top of page](#)

[Printer-Friendly Version](#) [Send This Page](#) [Add to Favorites](#)

[Manage Your Profile](#) | [Contact Us](#)

© 2007 Microsoft Corporation. All rights reserved. [Terms of Use](#) | [Trademarks](#) | [Privacy Statement](#)

Security At Home

What's New

Latest Security Updates

Download Security Products

Protect Your Computer

Protect Yourself

Protect Your Family

Resources

Worldwide Sites



Windows Live OneCare
Seamless antivirus protection for Windows Vista.
1
Try it FREE

Protect your computer: Beyond the basics

More ways to protect your computer



[How the right user account can help your computer security](#)

It's simple to set up multiple accounts on your computer. And it's wise to avoid surfing the Internet from an administrator account.



[Browser hijacking: Help avoid it and undo damage](#)

Help protect your Internet browser and regain control over what you do and see online.



[Disable unwanted programs with Windows Vista or Windows XP SP 2](#)

If you've downloaded a program that you don't want, here are some ways to remove it.



[5 steps to help protect your computer before you go online](#)

Help secure your computer against viruses, hackers, spyware, and other Internet threats.



[Improve the safety of your browsing and e-mail activities](#)

Use high-level security settings, designate trusted Web sites, read e-mail in plain text format, and use a pop-up blocker to maximize your safety online.



[How to tell which version you are running](#)

If you are not sure which software version you are running, or even if you have the software installed, here's how to check.



[Find tools you can use to remove unwanted software](#)

Download detection and removal tools provided by Microsoft and other companies.

[↑ Top of page](#)

[↓ Top of page](#)

Beyond the basics

- [Firewalls](#)
- [Updates](#)
- [Viruses](#)
- [Spyware](#)
- [About downloading](#)

Get more guidance

- [Protect yourself](#)
- [Protect your family](#)

Get security tools:


- [Downloads to help protect your computer](#)
- [Downloads to help protect yourself](#)
- [Downloads to help protect your family](#)




Download detection and removal tools provided by Microsoft and other companies.
Find tools you can use to remove unwanted software

- Security At Home
- What's New
- Latest Security Updates
- Download Security Products
- Protect Your Computer
- Protect Yourself
- Protect Your Family
- Resources
- Worldwide Sites

Get Windows Vista today.



See special offers.



How to recognize spoofed Web sites

Published: October 26, 2006



Some malicious individuals use [phishing scams](#) to set up convincing spoofs of legitimate Web sites. They then try to trick you into visiting these Web sites and disclosing personal information, such your credit card number.

Fortunately, there are several steps you can take to help protect yourself from these and other types of attacks.

What is a spoofing attack?

Spoofing attacks are commonly used in conjunction with phishing scams. The spoofed site is usually designed to look like the legitimate site, sometimes using components from the legitimate site. The best way to verify whether you are at a spoofed site is to verify the certificate.

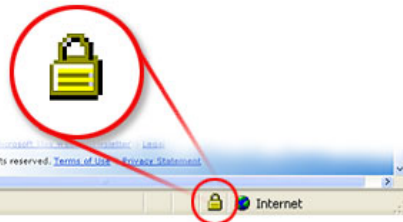
Do not rely on the text in the address bar as an indication that you are at the site you think you are. There are several ways to get the address bar in a browser to display something other than the site you are on.

How to verify a site certificate

Always verify the security certificate issued to a site before submitting any personal information. Before you submit any personal information, ensure that you are indeed on the website you intend to be on.

In Internet Explorer, you can do this by checking the yellow lock icon on the status bar.

This symbol signifies that the website uses encryption to help protect any sensitive personal information—credit card number, Social Security number, payment details—that you enter.



Secure site lock icon. If the lock is closed, then the site uses encryption. Double-click the lock icon to display the security certificate for the site. This certificate is proof of the identity for the site.

When you check the certificate, the name following **Issued to** should match the site you think you are on. If the name differs, you may be on a spoofed site.

If you are not sure whether a certificate is legitimate, do not enter any personal information. Play it safe and leave the Web site.



- Security At Home
- What's New
- Latest Security Updates
- Download Security Products
- Protect Your Computer
- Protect Yourself
- Protect Your Family
- Resources
- Worldwide Sites

Browser hijacking: How to help avoid it and undo damage

Published: September 23, 2006 | Updated: February 22, 2007



"Browser hijacking" is a common type of online attack in which hackers take control of your computer's Internet browser and change how and what it displays when you're surfing the Web.

If you keep your computer updated with the latest security software and updates, and practice safe Internet browsing, you're already doing a lot to keep the hijackers away.

But if your browser has already been "hijacked," there are several ways you can free it from the hackers and restore its settings.

How do I know if my browser has been hijacked?

The following are indicators:

- Home page or other settings change on your computer. Links are added that point to Web sites that you'd usually avoid.
- You can't navigate to certain Web pages, such as antispyware and other security software sites.
- A seemingly endless barrage of ads pops up on your screen.
- New toolbars or Favorites are installed that give you icons and links to Web pages that you don't want.
- Your computer runs sluggishly. Malicious software can slow down your computer.

[↑ Top of page](#)

Preventing browser hijacks

You can take a few basic precautions to help keep your browser running normally:

Avoid disreputable Web sites

You should always use good judgement about visiting sites that might be involved in illegal activities. These sites are often more likely to practice browser hijacking.

If you have children who use your computer, encourage open communication about what Web sites they are allowed to visit. [Windows Vista](#) and [Windows Live OneCare](#) both include parental control software.

Be very careful what you download and install onto your computer

A warning like the one in the following graphic might appear when you are about to download new software onto your computer.

Consider this warning seriously. Disreputable online games and media services can attach spyware and other malicious software to the "free" software they require to use their services. Unless you are certain that a program or piece of software is completely trustworthy, do not download or install it on your computer.

Further, if you see a pop-up window that asks for your permission to install software, click **No** unless you are absolutely sure you want this new software on your computer.

Related Links

- [Update your computer automatically](#)
- [Windows Defender](#)
- [Get the Malicious Software Removal tool](#)

Choose products that are Certified for Windows Vista

Enter now for a chance to win

www.lookforlogo.com

個人ユーザー向けセキュリティ

At Home : PC で、生活をもっと豊かに | At Work : PC で、仕事をもっとスマートに

個人ユーザー向けセキュリティ

はじめてのセキュリティ対策

はじめてのセキュリティ対策 ▶

コンピュータを守る

最低限必要なセキュリティ対策

更新と保守

ウイルスとワーム

スパイウェア

自分を守る

プライバシー

オンライン取引

電子メールとスパム

家族を守る

子供の安全

リソース

ビデオ

クイズ

ダウンロードとトライアル

サポート

セキュリティで困ったら



PCの保護対策、ウイルスなどのセキュリティ問題へのサポートを無料で提供

今すぐ開始 ▶

security at home



コンピュータを守るための3つのポイント

インターネットを使う前にぜひとも知っておきたい基本的な情報や、ウイルスの予防対策をまとめてご紹介します。



お子様を守るための3つのポイント

子供達がインターネットを安心して利用するために、保護者のみなさんへお知らせしたい情報をまとめました。



プライバシーを守るための3つのポイント

あなたの個人情報を安全に管理するための情報と、インターネットを悪用した詐欺や迷惑メールについてご紹介します。



- ウイルス対策情報
- 絵でみるセキュリティ情報
- 最低限必要なセキュリティ対策
- セキュリティ用語集
- 悪意のあるソフトウェアの削除ツール
- その他

- ユーザー別情報
- ホームユーザー向け
- 中小/個人企業向け
- IT プロフェッショナル (TechNet)
- 開発者 (MSDN)



セキュリティ問題に関する情報提供及びお問い合わせをお受けする専用の窓口を開設しています。

ご質問やご不明な点などありましたらお気軽にご連絡ください。

[詳しくはこちらをクリック](#)



みんなで「情報セキュリティ」強化宣言！

情報セキュリティ対策推進コミュニティ

私たちは、「みんなで『情報セキュリティ強化宣言』」に賛同し、情報セキュリティについて啓発活動を行っています。本ページでは、パソコンやインターネットを安心して利用できる対策方法をわかりやすく紹介しています。

安全なインターネットの利用方法

[インターネットの安全な利用方法](#)
[金融機関のサイトで個人情報を入力したり、公共のパソコンを利用する場合](#)
[迷惑メールの対処法](#)



安全な携帯電話の利用

[携帯を落としてしまった…](#)
[子供を出会い系サイトやアダルトサイトから守る](#)



個人情報保護

[個人情報を守る](#)



会社のネットワーク環境

[会社のネットワーク環境を安全に](#)
[ツールを使って集中管理](#)
[もしもドキュメントが流出してしまっても](#)



サイバー犯罪の調査協力

[意外と身近なハイテク犯罪](#)



印刷用ページを表示 | メールで紹介 | お気に入り追加

보안 업데이트 솔루션

1. PC Smile 보안업데이트는?



Microsoft 사는 Windows 보안을 강화하기 위하여 꾸준히 보안 업데이트를 발표 하고 있으며, 이 **보안 업데이트를 설치** 하는 것만으로도 대부분의 보안 위협으로부터 개인 컴퓨터를 안전하게 지켜 낼 수 있습니다. PC Smile 보안업데이트는 PC에 설치되어 있는 보안업데이트를 조사하여 누락되어 있는 항목들을 자동으로 설치 하여 주며 그 PC가 최신의 상태를 유지 하고 있는 지를 알 수 있게 해줍니다. PC Smile보안업데이트 프로그램 다운로드, 보안 업데이트에 대한 검사 및 Microsoft보안 업데이트 다운로드에 대한 모든 트래픽은 별도의 서버에서 이루어 지기 때문에 **귀하의 서버에 아무런 부담을 주지 않습니다.**

2. 자동업데이트, Microsoft Update 흉과의 차이는?

자동업데이트는 귀찮다 혹은 자동업데이트에 대해 잘 알지 못하는 이유에 의해서 활성화 되어 있지 않을 수 있으며 Microsoft Update 혹은 사용자가 직접 방문 해야 한다는 번거로움이 있지만 PC Smile 보안업데이트는 이것을 배포하는 사이트를 방문 하거나 해도 최신의 보안 업데이트를 자동으로 설치해 줌으로 보안업데이트 설치를 보다 강제 할 수 있습니다.

3. 배포 방법

01. ActiveX 를 정의해둔 pcsmile.js 파일을 다운로드 받습니다.
02. pcsmile.js 을 작성할 수정하여 웹서버에 pcsmile.js 를 저장 합니다.
03. 배포를 위한 페이지에 다음 코드의 콜아웃명을 변경하여 추가 합니다. (script src="/물대명/pcsmile.js"/script)

03' <script src="/물대명/콜아웃명"></script>

05' <script src="/물대명/콜아웃명"></script>

01' <script src="/물대명/콜아웃명"></script>

3. 배포 방법

PC보안 3단계비법

PC보안 3단계 비법 > Windows XP 사용자

→ Windows XP 사용자

비법 1 비법 2 비법 3

비법 1. 철저히 문단속 하라! 인터넷 방화벽 사용



방화벽이란 해커 및 다양한 종류의 컴퓨터 바이러스와 웜으로부터 PC를 보호해 주는 소프트웨어 또는 하드웨어입니다. 방화벽만으로는 컴퓨터를 100% 안전하게 보호할 수 없지만 그래도 가장 **첫번째 방어선**은 방화벽이므로 컴퓨터를 인터넷에 연결하기 전에 먼저 방화벽을 설치해야 합니다. 인터넷 연결 방화벽을 작동 하면 PC동작에 해로운 영향을 줄 수 있는 특정 종류의 네트워크 통신이 차단됩니다.

그러나 동시에 파일 공유, 네트워크 프린터, 인스턴트 메시징과 같은 응용 프로그램을 통한 파일전송, 멀티 플레이어 게임등 여러가지 유용한 네트워크 통신도 차단될수 있습니다. 이 때에는 언제라도 유용한 네트워크 통신 작업에 대한 차단을 해제할 수도 있으므로 안심 하셔도 됩니다. 자세한 내용은 방화벽에 대한 질문과 대답을 참조하세요.

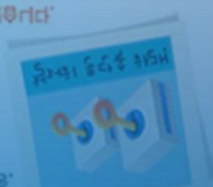


Windows XP 운영체제를 사용하는 다음과 같이 기본 제공 인터넷 연결 방화벽을 사용할 수 있습니다.

Windows XP 운영체제를 사용하는 다음과 같이 기본 제공 인터넷 연결 방화벽을 사용할 수 있습니다.

가장 첫번째 방어선은 방화벽이므로 컴퓨터를 인터넷에 연결하기 전에 먼저 방화벽을 설치해야 합니다.

인터넷 연결 방화벽을 작동 하면 PC동작에 해로운 영향을 줄 수 있는 특정 종류의 네트워크 통신이 차단됩니다. 그러나 동시에 파일 공유, 네트워크 프린터, 인스턴트 메시징과 같은 응용 프로그램을 통한 파일전송, 멀티 플레이어 게임등 여러가지 유용한 네트워크 통신도 차단될수 있습니다. 이 때에는 언제라도 유용한 네트워크 통신 작업에 대한 차단을 해제할 수도 있으므로 안심 하셔도 됩니다.



Wherever you are in your life, choose one of the categories below to learn how you can stay safe online.



▶ TEENAGERS



▶ PARENTS



▶ 50+



▶ EDUCATORS



▶ THE TOOLBOX

Stay Safe from Online Fraud

- ▶ [On Phishing, Pharming, and Pheeling Safe Online by PayPal](#)
- ▶ [Targets Too: Youth and Identity Theft](#)
- ▶ [Use Technology to Help You Avoid Phishing Scams](#)
- ▶ [Online Fraud: Giving Your ID Away in One or More Clicks](#)

Current News

Week of June 10, 2007

- ▶ [Online 'stalking,' for good or bad](#)
- ▶ [Cellphone monitoring on steroids](#)
- ▶ [Real-time \(very\) mobile dating](#)

▶ [View the Archives](#)

staysafe.org is made possible in part by our dedicated partners.

Microsoft



iSAFE



SafeKids.Com

American Academy of Pediatrics
DEDICATED TO THE HEALTH OF ALL CHILDREN



OnGuard Online
YOUR SAFETY NET™



NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN
www.missingkids.com

PayPal



Microsoft



iSAFE



TEENAGERS

PARENTS

50+

EDUCATORS

TOOLBOX



HELP
Looking for some answers?

SEARCH
 GO

HOME » TEENS

LEARN TO PROTECT:

Yourself

- Online Fraud
 - Social Networking
 - Shop Without the Drop
- Find Out More »

Your Computer

- Setting Up Your Computer
 - Spyware: Keep Spies at Bay
- Find Out More »

Make a Difference

STUDENT SPOTLIGHT



Predator

A junior high student from Utah makes a film and a difference.

Online Fraud:
Giving Your ID Away in One or More Clicks

[Read More](#)

I STAY SAFE

My name is Kayla.



I Stay Safe and don't rip off the artist I like.

GETTING SET



Getting Set for Security

Get Ready, Get Secure, Go!

TOOLBOX

- Updates
- Viruses
- Spyware

a difference: makes a film and student from Utah A junior high

Predator

- Spyware
- Viruses
- Updates
- TOOLBOX



LEARN TO PROTECT:

[Yourself](#)

- Online Fraud
- Social Networking
- Shop Without the Drop

[Find Out More »](#)[Your Computer](#)

- Setting Up Your Computer
- Spyware: Keep Spies at Bay

[Find Out More »](#)Make a **Difference** ▶

STUDENT SPOTLIGHT

**Predator**

A junior high student from Utah makes a film and a difference. ▶

PROTECT YOUR COMPUTER

Spyware

Keep Spies at Bay

You just found a great file-sharing service and downloaded the free software easily. With this service, you're not only filling up your MP3 player with songs and albums, you're also finding games, screen savers, and movies.

At the end of this article, you'll have an opportunity to **Talk Back** and share your useful tip, comment, or point of view.

But soon you see a lot of advertising pop-ups—LOTS of them, most for stuff you'd never consider buying. And your computer goes slower, and slower. Sometimes it even seems like your Web browser just doesn't work. Maybe that "free" file-sharing software might not have been free after all.

Chances are, it came with spyware, software that is loaded into your computer without your knowledge and almost always with a negative consequence. Is this real? It is, and it's everywhere—experts estimate as many as 80 percent of all home computers have spyware somewhere in them. Spyware is not the same as a virus—software that replicates itself and spreads itself to other PCs—nor adware, which launches banner or pop-up advertising on your computer (even without an Internet connection). It is also not the same as cookies, which are a simple line of text, not an executable program.

As the term "spyware" suggests, it can send information about you—and how you use the computer—to someone else. It does this by using your Internet connection without you knowing it. Information it sends away can include Web sites you visit, what you buy online, who you send e-mail or instant messages to, and more.

When 'Free' Can Be Costly

Where does spyware come from? Typical sources are free software downloads, certain Web sites, clicking on pop-up ads, file transfers

downloads, certain Web sites, clicking on pop-up ads, file transfers

When 'Free' Can Be Costly

you send e-mail or instant messages to, and more.

I STAY SAFE

My name is Kayla.



I love to IM with my friends.

I **Stay Safe** and **don't pick pointless fights.**

GETTING SET

Getting Set for Security



Get Ready, Get Secure, Go! ▶

TOOLBOX

- Updates
- Viruses
- Spyware

TEENAGERS

PARENTS

50+

EDUCATORS

THE TOOLBOX

staysafe.org for Parents

HELP

Have some questions?



SEARCH

GO

HOME PARENTS

LEARN TO PROTECT:

Your Family

- Blogging
 - Cyber Bullies
 - Parental Controls
- Find Out More >

Yourself

- Identity Theft
 - Spam Scams
 - Effective Passwords
- Find Out More >

Your Computer

- Use a Firewall
 - Control Spam
 - Stop Viruses
- Find Out More >



KIDS CORNER



Games, activities and more!

[Go There](#)

I STAY SAFE

I am Margo.



I know about illegal downloading. I **Stay Safe** and make sure my kids respect **other people's** property

IN THE NEWS

Week of June 10, 2007

- Online 'stalking,' for good or bad
- Cellphone monitoring on steroids
- Real-time (very) mobile dating

[View the Archives...](#)

LEARNING RESOURCES

NetSmartz®

Help keep your family safe online.

Information and tools for communicating with your kids about Internet safety.

[Find Out More](#)

TOOLBOX

- Updates
- Viruses
- Spyware

- Spam
- Search
- Safe Mode

TOOLBOX

[Find Out More](#)



THE TOOLBOX:

[Get the Basics](#)

- ▶ Stay Safe from Scams and Frauds
- ▶ Take Control of the Web
- ▶ What are Viruses, Worms and Trojans?

[View All Content »](#)
[Take Action](#)

- ▶ A Quick Guide to Passwords
- ▶ Chat Room Safety
- ▶ New Computer Security Checklist

[View All Content »](#)
[Learn More](#)

- ▶ Video Library
- ▶ Resources
- ▶ Perspectives
- ▶ Glossary

TAKE ACTION

New Computer Security Checklist

Before taking off on a flight, most pilots run through a "pre-flight" checklist. We suggest you run through our "New Computer Security Checklist" before unleashing your new home computer on your family. Here's what you need to do:

Protect your PC:

- **Install a firewall** (either one that is included with your operating system or one that you buy additionally).
- Make sure keep computer security systems **set to update automatically**, if possible.
- **Install anti-virus software**.
- **Install anti-spyware software** (if it is not included in your anti-virus package).

Protect yourself, your family and your information:

- Set IDs and passwords on your systems, making sure that **properly secure passwords are used**.
- **Set any parental controls** that you want to be associated with certain IDs (ie. limiting the Web sites that young children may be allowed to see).
- Make sure that everyone who will use the family computer **understands computer security basics**.

I STAY SAFE

I am Eric.



IN THE NEWS

[Week of June 10, 2007](#)

- ▶ Online 'stalking,' for good or bad
- ▶ Cellphone monitoring on steroids
- ▶ Real-time (very) mobile dating

[▶ View the Archives...](#)



THE TOOLBOX:

[Get the Basics](#)

- ▶ Stay Safe from Scams and Frauds
- ▶ Take Control of the Web
- ▶ What are Viruses, Worms and Trojans?

[View All Content »](#)
[Take Action](#)

- ▶ A Quick Guide to Passwords
- ▶ Chat Room Safety
- ▶ New Computer Security Checklist

[View All Content »](#)
[Learn More](#)

- ▶ Video Library
- ▶ Resources
- ▶ Perspectives
- ▶ Glossary

TAKE ACTION

Chat Room Safety

Chat rooms enable people to have group conversations online. Some chat rooms have predetermined topics; others are free flowing. When you type something in a chat room, it is seen immediately by everyone in the room as soon as you press Enter.

Chat room risks

While chat rooms can be interesting places for conversation and learning, they also pose some risks. If you or members of your family participate in chat rooms, it is a good idea to keep in mind:

- Some chat rooms restrict entry, but most are open to anyone. There is usually no way to know the real identity of fellow chatters.
- Personal information typed in a chat conversation can be seen and used by anyone in the room, or copied and sent to others.
- Chat rooms can be used by predators to find potentially vulnerable children or adults.
- Many chat rooms have an option to go into a "private" area for one-on-one conversation. Although this can be a good way for two adults or children who are already friends to converse, it can be dangerous to chat with unknown users in a private area, especially for kids. Predators can use private chats to draw children into a potentially dangerous online or even face-to-face relationship.

Making chat rooms safer

One way to reduce chat room risk is to use services that are open only to paid subscribers. By requiring members to enter a valid credit or debit card number, services make it more difficult for people to abuse the system and other users. Mandatory identification can make it easier for system administrators and law enforcement officials to track people who break the rules, and it can help police solve crimes.

I STAY SAFE

I am Eric.



My PC is always on.

IN THE NEWS

[Week of June 10, 2007](#)

- ▶ Online 'stalking,' for good or bad
- ▶ Cellphone monitoring on steroids
- ▶ Real-time (very) mobile dating

[▶ View the Archives...](#)

who break the rules, and it can help police solve crimes.
 for system administrators and law enforcement officials to track people
 the system and other users. Mandatory identification can make it easier
 debit card number, services make it more difficult for people to abuse
 to paid subscribers. By requiring members to enter a valid credit or
 One way to reduce chat room risk is to use services that are open only

Spotting a fraud: 7 signs of a scam

If you think an e-mail you received is a scam, one place to check is the Urban Legends Reference Pages [list of examples](#). However, these scams can come in thousands of different forms.

Here are seven more telltale signs of a scam:

- You don't know the person who has sent you the message.
- You are promised untold sums of money for little or no effort on your part.
- You are asked to provide money up front for questionable activities, a processing fee, or to pay the cost of expediting the process.
- You are asked to provide your bank account number or other personal financial information, even if the sender offers to deposit money into it.
- The request contains a sense of urgency.
- The sender repeatedly requests confidentiality.
- The sender offers to send you photocopies of government certificates, banking information, or other "evidence" that their activity is legitimate (these are fake).

[Top of Page](#)

What to do if you are a victim of fraud

If you do become a victim of fraud, here's what you should do:

- **File a report with your local police department.** Get a copy of the police report to notify your bank, credit card company, and other creditors that you are a victim of a crime, not a credit abuser. Depending on where you live, you may be required to file a report in the jurisdiction where the crime actually took place.
- **Place a fraud alert on your credit reports.** Ask that no new credit be granted without your approval. Review your reports carefully; look for things like inquiries you didn't initiate, accounts you didn't open, and unexplained debts. In the United States, you can contact these three credit bureaus:

Equifax (800) 525-6285
Experian (888) 397-3742
TransUnion (800) 680-7289

- **Outside the United States, you can contact your bank or financial institution,** who can direct you to the relevant organization or agency.

Outside the United States, you can contact your bank or

TransUnion (800) 680-7289
Experian (888) 397-3742
Equifax (800) 525-6285



HOW TO HAVE
FUN



HOW TO STAY IN
CONTROL



HOW TO
REPORT



WELCOME TO
THINKUKNOW.CO.UK

GET INVOLVED AND POST ON
OUR 'BLOGGING' SITE TODAY



This website is brought to you by the Child Exploitation and Online Protection (CEOP) Centre and contains loads of information on internet safety and safe surfing for young people. All hot topics about online safety are covered – including **mobiles**, **blogging** and **gaming** sites – and you can tell us if you feel uncomfortable or worried about someone you're chatting to online.



WOULD YOU LIKE TO
TAKE PART IN OUR SURVEY?



MOBILES	GAMING	SOCIAL NETWORKING	CHATTING	PODCASTS	BLOGS	P2P TV	SHARE
---------	--------	-------------------	----------	----------	-------	--------	-------

The link below will take you to the CEOP reporting page - this is like a virtual police station where you can make a complaint or report a problem. Your problem will be seen by a police officer, or a specialist investigator and they will contact you to let you know what will happen.

INTERNET SAFETY TIPS

THINK U KNOW...
If you publish a picture or

if you publish a picture or
THINK U KNOW...

SAFETY TIPS
INTERNET



Learn About...



LAPTOP SECURITY

Your laptop can help you work and keep in touch, no matter where you are. It's convenient - but are you doing all you can to keep your laptop in your hands (and out of the hands of others)? Learn the steps you can take to help keep your laptop safe.

[READ MORE](#)



Online Shopping



P2P File-Sharing



VoIP



Cross-Border



Investing Online



MISSION: LAPTOP SECURITY
Test Your Knowledge, Click to Play!

US-CERT
Coordinating Virus & Spyware Defense
NEW TIP FROM HOMELAND SECURITY

Get Email Alerts
Get **free alerts** from Homeland Security's U.S. Computer Emergency Readiness Team.
[READ MORE](#)

Stop · Think · Click

You can minimize the chance of an Internet mishap by adopting these practices:

- 1 **Protect your personal information. It's valuable.**
- 2 **Know who you're dealing with.**
- 3 **Use anti-virus and anti-spyware software, as well as a firewall, and update them all regularly.**
- 4 **Make sure your operating system and Web browser are set up properly and update them regularly.**
- 5 **Protect your passwords.**
- 6 **Back up important files.**
- 7 **Learn who to contact if something goes wrong online.**

[READ MORE](#)

Word of the Day

Software

A computer program with instructions that enable the computer hardware to work. System software — such as Windows or MacOS — operate the machine itself, and applications software — such as spreadsheet or word processing programs — provide specific functionality.

[GLOSSARY](#)

BE CAREFUL WITH THIS LAPTOP — ONE FALSE MOVE AND IT COULD END UP IN THE WRONG HANDS. AS LONG AS YOU ANSWER QUESTIONS CORRECTLY, YOU'LL PROBABLY ACCOMPLISH YOUR MISSION. BUT IF YOU MISS A FEW QUESTIONS, WE'LL BE VERY DISAPPOINTED... IN FACT, WE MAY HAVE TO REVOKE YOUR SECURITY CLEARANCE. GOOD LUCK.

CONTINUE ▶

STOP • THINK • CLICK™

STOP • THINK • CLICK™

CONTINUE ▶

SECURITY CLEARANCE. GOOD LUCK.
WE MAY HAVE TO REVOKE YOUR

Good, Smith — you have the laptop. But our double agent also gave you a note with the laptop's password written on it. Now what should you do?

A. Attach the sticky note to the laptop screen

B. Hide the password inside the laptop carrying case

C. Commit the password to memory and destroy the note

D. Save the password on a removable hard drive device or 'flash' memory stick

22:45

THE EXCHANGE

THE EXCHANGE

22:42

All right, Agent Smith, it's time for breakfast. While you're making a stop, what should you do with the laptop?

A. Lay it on the passenger seat and lock the doors to your car

B. Stow it in the trunk

C. Bring the laptop in with you

D. Store it in the space under the driver's seat

09:40

THE PARKING LOT

THE PARKING LOT

09:40

http://onguardonline.gov/certtips/st06-009.html

OnGuard Online - US-CERT Tip: Safeguarding Yo...

OnGuard Online
YOUR SAFETY NET™

onguardonline.gov provides practical tips from the FBI and the technology industry to help you be on guard against fraud, secure your computer, and protect your personal information.

Home Topics About Us File a Complaint

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Coordinating Virus and Spyware Defense

This tip brought to you by the Department of Homeland Security & US-CERT

Using anti-virus and anti-spyware software is an important part of cyber security. But in an attempt to protect yourself, you may unintentionally cause problems.

Isn't it better to have more protection?

Spyware and viruses can interfere with your computer's ability to process information or can modify or destroy data. You may feel that the more anti-virus and anti-spyware programs you install on your computer, the safer you will be. It is true that not all programs are equally effective, and they will not all detect the same malicious code. However, by installing multiple programs in an attempt to catch everything, you may introduce problems.

How can anti-virus or anti-spyware software cause problems?

It is important to use anti-virus and anti-spyware software (see [Understanding Anti-Virus Software](#) and [Recognizing and Avoiding Spyware](#) for more information). But too much or the wrong kind can affect the performance of your computer and the effectiveness of the software itself.

Scanning your computer for viruses and spyware uses some of the available memory on your computer. If you have multiple programs trying to scan at the same time, you may limit the amount of resources left to perform your tasks. Essentially, you have created a denial of service against yourself (see [Understanding Denial-of-Service Attacks](#) for more information). It is also possible that in the process of scanning for viruses and spyware, anti-virus or anti-spyware software may misinterpret the virus definitions of other programs. Instead of recognizing them as definitions, the software may interpret the definitions as actual malicious code. Not only could this result in false positives for the presence of viruses or spyware, but the anti-virus or anti-spyware software may actually quarantine or delete the other software.

Abby Video: Defend Yourself Against Viruses and Worms - Windows Internet Explorer

http://onguardonline.gov/tutorials/virus/vir_wind.html

Defend Yourself Against Viruses & Worms

Pause

To-Do List

Defend Yourself Against Viruses

4. Never open an e-mail attachment unless you know exactly what the attachment is.
5. Never open an e-mail attachment from a stranger-- delete it.



Audio ON Transcripts OFF

Done Internet | Protected Mode: On 100%

FACEOFF

Worms & Viruses

Play Video

quarantine or delete the other software.

of viruses or spyware, but the anti-virus or anti-spyware software may actually quarantine or delete the other software.

recognition of the definitions of other programs may misinterpret the definitions as actual malicious code. Not only could this result in false positives for the presence of viruses or spyware, but the anti-virus or anti-spyware software may actually quarantine or delete the other software.

Worms & Viruses

Play Video

http://onguardonline.gov/certtips/index.html#safe_browsing

OnGuard Online - US-CERT Tips

US-CERT Tips

General information

- Why is Cyber Security a Problem?
- Guidelines for Publishing Information Online
- Understanding Internet Service Providers (ISPs)

General security

- Choosing and Protecting Passwords
- Understanding Anti-Virus Software
- Understanding Firewalls
- Coordinating Virus and Spyware Defense
- Debunking Some Common Myths
- Good Security Habits
- Safeguarding Your Data
- Real-World Warnings Keep You Safe Online
- Keeping Children Safe Online

Attacks and threats

- Dealing with Cyberbullies
- Understanding Hidden Threats: Corrupted Software Files
- Understanding Hidden Threats: Rootkits and Botnets
- Preventing and Responding to Identity Theft
- Recovering from Viruses, Worms, and Trojan Horses
- Recognizing and Avoiding Spyware
- Avoiding Social Engineering and Phishing Attacks
- Understanding Denial-of-Service Attacks
- Identifying Hoaxes and Urban Legends

Email and communication

- Understanding Your Computer: Email Clients

Email and communication

- Understanding Your Computer: Email Clients
- Using Caution with Email Attachments
- Reducing Spam
- Benefits and Risks of Free Email Services
- Benefits of Blind Carbon Copy (BCC)
- Understanding Digital Signatures
- Using Instant Messaging and Chat Rooms Safely
- Staying Safe on Social Networking Sites

Mobile devices

- Protecting Portable Devices: Physical Security
- Protecting Portable Devices: Data Security
- Securing Wireless Networks
- Cybersecurity for Electronic Devices
- Defending Cell Phones and PDAs Against Attack

Privacy

- How Anonymous Are You?
- Protecting Your Privacy
- Understanding Encryption
- Effectively Erasing Files
- Supplementing Passwords

Safe browsing

- Understanding Your Computer: Web Browsers
- Evaluating Your Web Browser's Security Settings
- Browsing Safely: Understanding Active Content and Cookies
- Understanding Web Site Certificates
- Understanding International Domain Names
- Understanding Bluetooth Technology
- Avoiding Copyright Infringement

Software and applications

Client software and applications

Software and applications

Understanding the risks of software

Understanding the risks of software

Understanding the risks of software

Understanding the risks of software

Understanding the risks of software

Understanding the risks of software



search [GO](#) [customize](#)

- Software Assurance
- Secure Systems
- Organizational Security
- Coordinated Response
- Training**

Training

[CERT Training Courses](#)

[Incident Handling Certification](#)

Remote Training & Resources

[Virtual Training Environment](#)

[Survivability & Information Assurance Curriculum](#)

documents

[Publications Catalog](#)

[Historical Documents](#)

Training

Computer users are frequently cited as the weak link in an organization's computer and network security strategy. CERT works to create an international workforce skilled in information assurance and survivability by developing curricula on information assurance and security incident response for executives, managers, educators, software engineers, and network administrators and front-line system operators. CERT disseminates these curricula through its own training courses, academic institutions, and through innovative approaches, such as the Virtual Training Environment (VTE).

Upcoming Courses

June 11-15 (PGH)
Information Security for Technical Staff

July 10-12 (PGH)
OCTAVE Training Workshop

July 16 (PGH)
Creating a Computer Security Incident Response Team

July 17-19 (PGH)
Managing Computer Security Incident Response Teams

July 24-26 (PGH)
Computer Forensics for Technical Staff

[more on training](#)

Virtual Training Environment (VTE)

CERT's Virtual Training Environment (VTE) is a library of information assurance and computer forensics best practices. It contains more than 160 hours of multimedia-based instruction targeted at system



Virtual Training Environment (VTE)

[more on training](#)

Incident Handling Certification

CERT has created a program to certify individuals in computer security incident handling. This certification program complements our existing incident handling training curriculum.



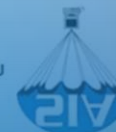
CERT®-Certified Computer Security Incident Handler
Learn about the requirements and benefits of earning certification, who should apply, and how to renew your certification.

Curriculum

CERT has developed a downloadable three-course curriculum in survivability and information assurance (SIA). This curriculum offers a problem-solving methodology built on key SIA principles that are independent of specific technologies.



technologies.
principles that are independent of specific
problem-solving methodology built on key SIA
assurance (SIA). This curriculum offers a
course curriculum in survivability and information
CERT has developed a downloadable three-



Curriculum



The Leader in Internet Safety Education

Username:

Password:



[Create Account](#) | [Forgot Password?](#)

[About iSAFE](#)

[Kids & Teens](#)

[Educators](#)

[Outreach & Parents](#)

[Law Enforcement](#)

[Get Involved](#)

Welcome to iSAFE

iSAFE Inc. is the worldwide leader in Internet safety education. Founded in 1998 and endorsed by the U.S. Congress, iSAFE is a non-profit foundation dedicated to protecting the online experiences of youth everywhere. iSAFE incorporates classroom curriculum with dynamic community outreach to empower students, teachers, parents, law enforcement, and concerned adults to make the Internet a safer place. Please join us today in the fight to safeguard our children's online experience.

Assessments



U.S. Senate Designates June Internet Safety Month:

Get involved. iSAFE helps you spread Internet safety awareness to your friends, your family and community, as well as throughout Cyberspace. For more details [Click Here](#).



X-BLOCK



iSAFE Store



News

Just Released

Internet Life Skills Workbook & Teachers Guide



Quick Links

News from iSAFE
Newsroom
[i-EDUCATOR Times](#)
[i-PARENT Times](#)
Kewl Timez
[i-Buddy Times](#)

Join iSAFE's Mission
Calendar of Events
Web Banners
Donations
National Assessment Center
Contact Us/FAQ

Education Resources
[I-LEARN Online](#)
Surveys/Assessments
Webcasts
Implementation Plan
Educator Information

[Kids & Teens](#)
[I-MENTOR Training Network](#)
Be an i-Mentor
Chatroom
Celebrity Corner



[i-Mentors](#)

[i-Mentor
Training](#)

[i-Drive TV](#)

[Get the 411](#)

[Contests](#)

[Chatroom](#)

Username:

Password:



[Create an Account](#)



Get the 411

Welcome to i-SAFE's Celebrity Corner. This is the only place to get an inside look at the actors and athletes who help i-SAFE. Each month i-SAFE profiles a new celeb! Check out their bio and see how they answer five questions from i-SAFE. It's the scoop on what they're doing now and what they're working on next. Get a sneak-peak at how they surf the web and find out what they think you should do while online. It's all here in i-SAFE's Celebrity Corner.



A composer writes the instrumental music that supports the action or emotion of a scene in a TV show or movie. It can be a huge orchestral sound like "Lord of the Rings" or a small intimate sound like "American Beauty." Jonathan has composed the scores for many TV shows including, *Joan of Arcadia*, *She Spies*, *Scrubs (additional music)*. He has also written some songs for films such as, *Sometime They Come Back Again*, *Max and Grace*, and *Full Tilt Boogie*.

[View Jonathan's Bio/Q&A](#)



→ **Jonathan Grossman**

Celebrity Community:

Adrianna Sgarlata

[View Adrianna's Q&A](#)

Danny Way

[View Danny's Bio/Q&A](#)

Paul Rodriguez Jr.

[View Paul's Bio/Q&A](#)

Kyle Sullivan

[View Kyle's Bio/Q&A](#)

Percy Daggs III

[View Percy's Bio/Q&A](#)

Dean Collins

[View Dean's Bio/Q&A](#)

Teddy Dunn

[View Teddy's Q&A](#)

George Stults

[View George's Bio](#)
[View George's PSA](#)
[View George's Q&A](#)

Jason Dohring

[View Jason's Bio/Q&A](#)

Willy Santos

[View Willy's PSA](#)
[View Willy's Q&A](#)

Rat Sult

[View Rat's PSA](#)
[View Rat's Q&A](#)

Jeff Garcia

[View Jeff's Bio](#)
[View Jeff's PSA](#)



[View Willy's Q&A](#)
[View Willy's PSA](#)
Willy Santos

[View Rat's Q&A](#)
[View Rat's PSA](#)
Rat Sult

[View Jeff's PSA](#)
[View Jeff's Bio](#)
Jeff Garcia

Session Summary



Deliver security information that users will view as being valuable to them personally and professionally



Communicate with users, let them know why policies exist and why they are enforced for everyone



Be mindful of security solutions that can impact usability and communicate the need to users whenever such solutions are implemented



Remember that security awareness isn't a one shot fix but a long term process designed to educate AND to change user behavior

Questions?

jjarvis@microsoft.com

Microsoft[®]

Your potential. Our passion.[™]

© 2007 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows Vista and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.

MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.