The Security Blanket

Issue 12, November/December 2002
Helping you keep I.T. secure

In This Issue:

From the CISO

The Information Security Office: It's Mission and Future

As we rush headlong into the holiday season and I think about all that we have to be thankful for, and think further towards the new year and all that still remains to be done, I felt it would be a good idea to revisit the Security Office's mission and guiding principles.

Our mission is to identify and protect the information and information systems entrusted to the state through the development, deployment, and institutionalization of a structured, cost-effective process that provides reasonable assurance that valuable business and personal information will be: 1) Identified and prioritized based on value and privacy; 2) Adequately safeguarded from misuse and theft regardless of the technologies used and changes in business models; 3) Maintained in a manner that satisfies legal requirements and 4) Leveraged for business needs. Our guiding principles are as follows:

We believe that the traditional objectives of maintaining information confidentiality and integrity, while providing appropriate availability, are non-negotiable. The state is entrusted with the information and owns the accountability for its protection.

- Security exists only to mitigate risk.
- Security must be an enabler.
- Security must be value added.
- Security input must be practical and fast.

When we all return, my office will be revisiting where we've been in 2002 and where we need to go in 2003, keeping these things in mind while dealing with a new integrated department and all that entails. 2003 is full of promise and expectations -- it's up to us to see where we go and how we go about doing it. One thing that immediately comes to mind is that we have spent the major chunk of our time dealing with security issues internal to ITD, when we should have spent the majority of our time with external customers. It remains to be seen what the Department of Administrative Services means to our time allotments, especially during the planning and integration phases, yet my goal for 2003 is to provide more of an enterprise presence. I guess we'll have to wait until next year at this time to see how that turns out.

Kip Peters

Return to Table of Contents

Feature Articles

A Call to Action: Be a Cyber Secure Citizen!

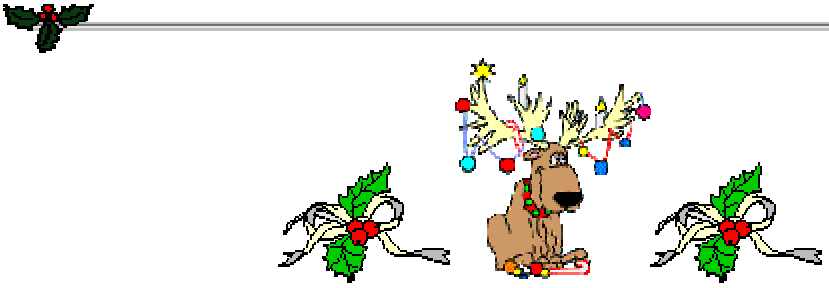
Securing your personal computer plays a crucial role in protecting our nation's Internet infrastructure, according to the Stay Safe Online effort. The www.staysafeonline.info website can help people do this, because the site is designed to give them the information needed to secure their home or small business computers.

Stay Safe Online is sponsored by the National Cyber Security Alliance. This voluntary coalition is made up mostly of businesses and a few government agencies, all of which believe that securing the nation's cyberspace is the responsibility of all Americans that use the Internet. Scott Algeier from the US Chamber of Commerce is the coordinator for the Alliance. Mr. Algeier stated in an interview with ITD that the goal of the National Cyber Security Alliance "...is to educate small businesses, home users and school children on what *they* can do to secure *their* portion of cyberspace."

Mr. Algeier went on to say that "Essentially, there are three aspects of cyber security: technology, policy, and people. The part we are focusing on is the people part." To this end, the Stay Safe Online website has a beginner's guide to cyber security, tips, and a quiz where you can test your security awareness skills. Another aspect of this awareness effort is the Kids Improving Security Poster Contest, which the Cyber Security Alliance is co-sponsoring with the FBI-NIPC. Each fall, students nationwide can participate in the contest. National winners of the poster contest receive a plaque, a trip to Washington for themselves and one adult to meet Governor Tom Ridge, the Director of Homeland Security, and Richard Clarke, Special Advisor to the President for Cyberspace Security, and $1,500.00 for their school to spend on computers or other technology efforts.

ITD is the first state agency in the nation to become an official sponsor of the National Cyber Security Alliance, and is proud to assist in their outreach efforts. We invite you to visit the Stay Safe Online site, and see how you can help yourself and the nation stay more secure.

Larry Brennan



Importance of Patches and The Speed of the Net

One of the most important actions that a computer user can do to safeguard their system is to stay current on updates and patches for their software. All software companies are constantly releasing patches and updates to fix security issues, as well as other flaws discovered in their products. Security experts and hackers are always finding new security bugs in software and releasing them to vendors and the general public. This usually means a flaw becomes well known, and many times an exploit to take advantage of that flaw is created and released. Some bug hunters submit the vulnerability to the vendor first and they wait for a patch to be released before releasing the security alert to the public. However, since most patches are not applied, hackers still have a window of opportunity to exploit the flaw. In other situations, hackers will not even release the vulnerability; they will create an exploit to keep for themselves or distribute it in the hacker underground.

With many users now having "always on" Internet connections, hackers that want to exploit these flaws have an abundant supply of targets on which to focus. The speed at which an exploit can be written for a particular vulnerability usually depends on the difficulty involved in exploiting the flaw. Many exploits can be written the same day, while others may take a week, or even a month.

The best example of the problem of ongoing vulnerability and the lack of adequate patching would be Code Red. Even though this worm was written over a year ago it still has a heavy footprint on the Internet. A machine connected to the Internet can get hit by this worm and its descendants hundreds of times per day. A patch for the vulnerability exploited by Code Red was released four months prior to the Code Red outbreak. If users had patched their systems, the impact would never have been close to what it was.

For comparison numbers, the State's intrusion detection system saw around 8500 attacks from Code Red, Code Red II, and Nimda in the past 28 days. Add to that another 5000 attacks from the Bugbear virus. And these are just the numbers from those specific attacks; this does not include the amount of directed attacks from hackers and automated scans that take place.

A computer that is connected to the Internet is going to be attacked, guaranteed. Patching and updating software and systems against known vulnerabilities is simply a necessary step users must take to try to keep their systems secure. If a system isn't patched, it is only a matter of time before it is compromised.

Reference: Seeing more than Red (2600)
Source: http://www.2600.co.za/stf/Seeing%20more%20than%20Red.html

Paul Schmelzel

Spam, Spam, Spam, Spam

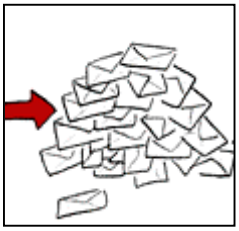
Spam, Spam, Spam, Spam
Spam, Spam, Spam, Spam
Spaaaam, Oh Lovely Spaaam! (Spam, Spam, Spam, Spam)
Spaaaam, Oh Wonderful Spam! (Spam, Spam, Spam, Spam)*
* Monty Python's Flying Circus

Wonderful? Well, for us, no, not really. It can clog your e-mail systems, fill up your inbox, bombard you with financial solicitations and body-modification offers, and otherwise annoy you and drain your department's time in dealing with it. Other than "a canned meat product consisting primarily of chopped pork pressed into a loaf", what exactly is Spam and why is it becoming so prevalent?

Spam is defined by the American Heritage Dictionary as "Unsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups; junk e-mail." Spam, or 'unsolicited bulk e-mail', is often being used as a marketing tool to blast out messages to the world, so to speak. Literally any e-mail address can become a target. Commercial Spammers don't really know who you are, and neither do they care. They are simply trying to send their messages to as many people as possible, hoping for someone to buy their product or service, or even just to respond to their email in order to verify a viable target email address.

I recently received a Spam message letting me know about a bulk e-mail (i.e. Spam) company's service. For the small fee of $200 they will send an advertisement from their servers out to 1,000,000 email addresses, sorted by certain specifications, of course. (They claimed to have over 50 million addresses.) That way your website or server won't be blocked by pesky system administrators, and you can reap the rewards of mass emailing while decreasing the risk of having your website shut down. What a deal.

Let's see, if I sell a product for $10, send out a million emails, and only 100 people out of the million are suckered – I mean, buy my product, I'm still up $800! I won't worry about the thousands of hours wasted by my target audience, deleting emails or attempting to filter Spam, because it's just business, right? Well, there really are lots of companies that provide mass e-mailer services, and they don't care who you are, you're just a target to them. So what can you do about it?



First, don't take it as a reflection on you. Your e-mail address has been gathered or collected in some way, and it's just an e-mail target. Second, don't respond to Spam, just delete the Spam message. Emailing sources often simply use your response or 'request to be removed from this list' to verify a viable address. They don't want to remove you from their lists; they want viable target addresses. Some states do have laws regarding list removal requests, but Spam can come from anywhere in the world, so it is best not to respond. Third, if your home email account gets lots of Spam from the same source (though Spam messages are easily spoofed), you can discuss the issue with your Internet Service Provider. If your work account gets lots of Spam from the same source, you can use your own e-mail client to

filter the source. (For example, by using Outlook's Tools, Rules Wizard, you can set your account to reject specific sending addresses. (See Helpful Hints, below, or contact your Help Desk or Desktop Support for questions.) Of note, ITD is currently looking into Spam filtering products and techniques to help alleviate the problem of receiving Spam. Fourth, if the Spam seems to be coming from *inside the State system*, contact your email administrator and security team immediately, as this may indicate a compromised internal workstation or server.

The Information Security Office has put together an Unsolicited E-mail SOP, but first a po-em, by Nipsy Russell:*

It is said that Spam may be good to eat,
But for getting emails it's not a treat.
It just wastes your time; there is no doubt,
So chuck it, delete it, and throw it out!

*Like many offers and solicitations in Spam, that citation isn't really true.

You can get the SOP for Unsolicited E-mail from the ISO website.

For further reading on past federal Spam legislation and the often legal-sounding but misleading references within Spam messages, check out "House Subcommittee Approves Anti-Slamming and Anti-Spamming Bill", Tech Law Journal, http://www.techlawjournal.com/internet/80807Spam.htm, and the article "Spam and the Law", http://www.jamesshuggins.com/h/tek1/Spam_and_law.htm.

And then, of course, there's the Spam Song.

William Hubbard

Return to Table of Contents

Current Activities

Let's see, things we've been up to… the Security Test Lab is now operational, and currently testing both the Enterprise Antivirus Standard software and Microsoft Active Directory issues. The ISO now has system Forensic capability, and plans to expand the IDS as well. In the future we'll also be testing wireless systems, planning a cyber-event exercise, and expanding our security awareness efforts. Pretty cool, huh?

Information Security Office Service Offerings

Would you like to have a vulnerability assessment performed on your systems? Do you need help with an incident? Are you looking for security services? Check out the ISO Service Offerings!

Visit the **ITD Billable Rates** web page for a complete listing of Security Service Rates. (Security Services are listed in the last quarter of the web page.)

- Security Consulting
- Vulnerability Assessments
- Physical Security Vulnerability Assessments
- Network-Based Intrusion Detection System
- Enterprise Business Continuity
- Incident Response
- Test Lab
- Awareness Briefings
- Enterprise IT Business Continuity

Information Security Office Certification Process

And lo, there arose in the East a Certification and Accreditation Process, new and fresh, from the wise men and women at NIST, complex but well formed, and it shone out as a hope to security administrators everywhere, and the voice said it shall be named "NIST Special Publication 800-37". And after the new process arose, the huge, ungainly, monstrous project of developing our own streamlined C&A Process was cast down into Heck, and troubled the ISO staff no more. And there was much rejoicing. (Yea…)

The National Institute of Standards and Technology (NIST), in cooperation with industry professionals and government agencies, has recently developed an extensive Certification and Accreditation Process for Information Systems. The process is well written and organized, and will be kept up-to-date by NIST personnel. The ISO will be using this process for our C&A efforts. By using the NIST process, we will leverage the knowledge and experience of not only the NIST development team, but of many other Information Security Professionals who are collaborating in the NIST C&A process effort.

The role of the ISO in the State of Iowa C&A process will be twofold. First, we will be available to guide the certification teams through the applicable steps of this process, providing appropriately tailored checklists, performing Security Testing, Evaluations and Validations, and providing security recommendations. Second, we will be involved with the final decision to approve or disapprove the Accreditation package.

Included below is a link to the NIST publication, and I highly encourage those who have the time to review it. For those with serious time constraints, start with Chapter 4, Certification and Accreditation Process Phases and Activities, which begins on page 35. Chapter 4 includes a well-written outline of the tasks that should be performed during the C&A Process. The specifics for some of the tasks will not apply to Iowa systems since they are written for Federal use, but the intent of each task is apparent and will still be

very useful to state personnel. The ISO will work with each certification team to assure that all tasks are appropriately tailored to the system being evaluated.

NIST Special Publication 800-37: http://csrc.nist.gov/sec-cert/SP-800-37-v1.0.pdf
NIST C&A Project Site: http://csrc.nist.gov/sec-cert/

Marie Hubbard

Information Security Officer Distribution List

The Information Security Office has a distribution list with which we can easily send out security mailings to security contacts within the State of Iowa. Mailings include the Security Blanket, Security Quickies, Lunch & Learns, Security Alerts, Daily News and Virus Reports, security events, or other announcements. Some contacts also disseminate the ISO mailings to their departmental personnel. If you are interested in being included in this distribution list, drop a note to Security Awareness.

If you would prefer to only get the Daily News and Virus Report, which is sent out every business day, send the note with this subject heading: Security Awareness.

Security Awareness Tutorial

The new Security Awareness Tutorial (SAT) is complete and ready to use! Topics covered in the Security Awareness Tutorial include training on Confidential Information, User Accounts and Passwords, Workstation Security, Malicious Code (Viruses, Trojans, and Worms), Laptops, and Modems. The training course is available online and on CD-ROM, and will take up to 90 minutes to complete. It is divided into separate lessons, so you can complete the lessons at different times if needed.

The SAT is currently being used by ITD for security awareness training. Because the Information Security Office has Enterprise-wide responsibilities, the SAT is also available to State of Iowa Enterprise agencies at no charge. In addition, the SAT will be available to non-Enterprise agencies and non-State of Iowa organizations as well, for a licensing fee.

For more detailed information such as system requirements and course content you can visit http://www.itd.state.ia.us/security/education.html#tutorial. Contact William Hubbard if you have questions regarding the SAT content, and Cory Oelberg for access to the course.

UPCOMING SERVICES

Risk Assessment
A standard risk assessment methodology for Enterprise systems is under development. Training will be provided on how to best utilize the methodology, and staff assistance will be available for agency assessments.

Vulnerability Profiling
A vulnerability profiling service utilizing existing Enterprise components is planned for the next quarter. The ISO will be taking a more proactive stance toward vulnerabilities by instituting alerts to appropriate personnel and developing response procedures to facilitate risk mitigation for state systems. More to come…

OTHER ACTIVITIES

Enterprise Security Website

From this site you have access to tons of security information: Security Awareness Resources, Operational Services, Policies, Procedures, Recommended Reading, and Mobile News, and Industry Best Practices. It's your free resource for Enterprise and ITD Security Information.

Educational Extras

Extra resources are available here for State security awareness efforts and home personal computer security.

Information Security Outreach

In an effort to assist with the federal security awareness outreach effort and to aid state employees, security awareness materials are being disseminated to various departments and Capitol Complex public areas. These materials include the ISO "Guidelines for Information Security and Internet Usage", the FTC "Safe at Any Speed" and "Identity Theft" guides, and password help sheets, and are designed to be beneficial both in the work place and at home. If you or your department would like to get more of these free documents contact Security Awareness.

ITD Guidelines and Procedures

Go here to see new ITD ISO Guidelines and Procedures for Workstations and Servers, Tips on Malicious Code, and non-IT General Security issues:

Configuring a Windows 2000 Desktop	IP Security Policies	Travel Security Guidelines
Windows IIS 5.0 Guide	Enterprise Messaging System Protection Measures	Letter and Package Handling
Apache 2.0 for Windows NT/2000 Secure Installation Guideline	Virus Detection and Prevention Tips	SOP for Unsolicited Mail
Preparing a Windows 2000 Server for Production	Virus Response Procedures	Hoax characteristics

Return to Table of Contents

Upcoming Classes and Consultations

This is the place to learn more about…
Information Sharing!
Security Training!
Conferences!
Programs!
Security Vendor Announcements!

The Information Security Office's Lunch &Learn Program continues… These informal meetings cover a variety of security-oriented issues. No sign-up or registration is necessary, just drop in. Change of location or time will be announced via e-mail, and sent to departmental Information Security Officer contacts. The past presentations (lots of them - in .pdf, .ppt, and/or video) and an updated schedule are available at the Lunch & Learn site.

Date and Time	Topic, Location, and Speaker
January	An Introduction to TCP/IP (Repeat) Dave Rowen

Please remember - we'll supply the place and the witty repartee, and maybe some cookies, but you will need to bring your own lunch. Questions or topic ideas on the Lunch & Learn program can be directed to William Hubbard.

ITD's Knowledge Access has Security-related training available. Courses available include security topics related to MS Windows 2000, MS IIS 4.0, Network Essentials, Java, and more. Visit the Knowledge Access site for more details and pricing info.

Security Vendors

SANS Offerings:
Each month SANS offers at least one training conference in a major U.S. city. In the next few months there are several upcoming events, but especially notable is the SANS 2003 event, March 5 –12, in San Diego. For this (and others) see:
http://www.sans.org/SANS2003

SANS also offers online and onsite security courses for those who are unable to travel much, but still wish to participate. SANS has also launched a **Win2K Gold Standard**

Tour, a special one-day course, which will take place in many cities around the nation. Details and registration information for the SANS programs:
http://www.sans.org/newlook/home.php

SANS also offers a free First Wednesday Webcast series. This series is dedicated to sharing information on current security issues. http://www.sans.org/webcasts/

SANS now offers its training courses in-house at user sites where 20 or 30 or more people need to learn to harden UNIX or Windows, learn intrusion detection in depth, learn the essentials of security, or learn the technical side of security auditing. These courses are taught by the same extraordinary faculty, for which SANS programs are best known. By bringing the courses in house you save travel costs, get reduced student fees, and facilitate information sharing among your co-workers. Details:
http://www.sans.org/onsite

If **State of Iowa employees** are interested in an Enterprise-shared SANS session, drop a note to Security Awareness, and note your specific interest, if known (Security Essentials, Securing Windows, Auditing, etc.). If there is enough response the ISO may be able to organize a reduced-cost session specifically for state employees.

Microsoft: (Vendor Announcements)

Free MSDN Webcasts

The MSDN Webcasts team holds 90 minutes of deep, how to technical webcasts presented by knowledgeable Microsoft software design engineers, developer evangelists, and a host of others. This free event is held live, and it's interactive. Customers can see code and application demos online, and ask the presenter technical questions, or listen to their peers ask questions.
Register at: http://www.microsoft.com/usa/webcasts/upcoming/default.asp
Recorded sessions can be found at:
http://www.microsoft.com/usa/webcasts/ondemand/default.asp.

Microsoft Online Training
In an effort to meet the demands for training and certification on Microsoft products and platforms, Microsoft Government is sponsoring Online Training for selected courses for a limited time. These courses will be provided on a first come first served basis. Government employees can register for training at a reduced cost, as we have arranged for the Microsoft discount to be extended to our government customers. To register, Government technical professionals need to go to the web site:
http://www.msgovernmenttraining.com/offer/

Other Events:

BlackHat Windows Security 2003 Briefings and Training
Feb. 24-27, Sheraton Seattle Hotel & Towers in Seattle, WA
The briefings will cover six tracks over 2 days. Subjects include policies, deep knowledge, networking and integration, and application development, as well as Microsoft .NET, Microsoft IIS, Microsoft SQL Server, and Microsoft Internet Security

and Acceleration (ISA) Server 2000. For more information see:
http://www.blackhat.com/html/win-usa-03/win-usa-03-index.html

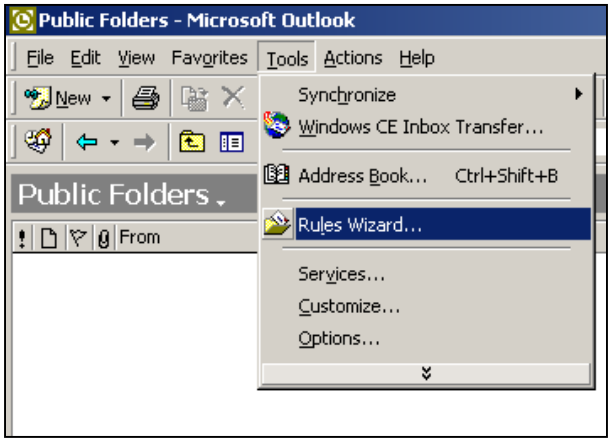
RSA Conference 2003, April 13-17, San Francisco, CA
The RSA conference has four main components: General Sessions, Expo, Tutorials, and Class Tracks. See http://www.rsasecurity.com/conference for details.

Return to Table of Contents

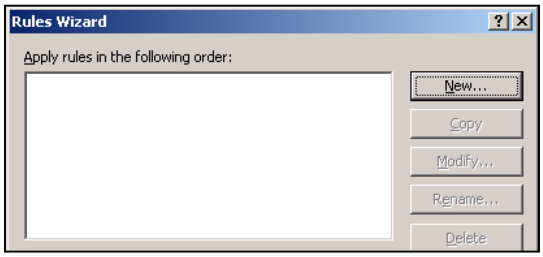
Helpful Hints

Filtering Unsolicited Email in Outlook

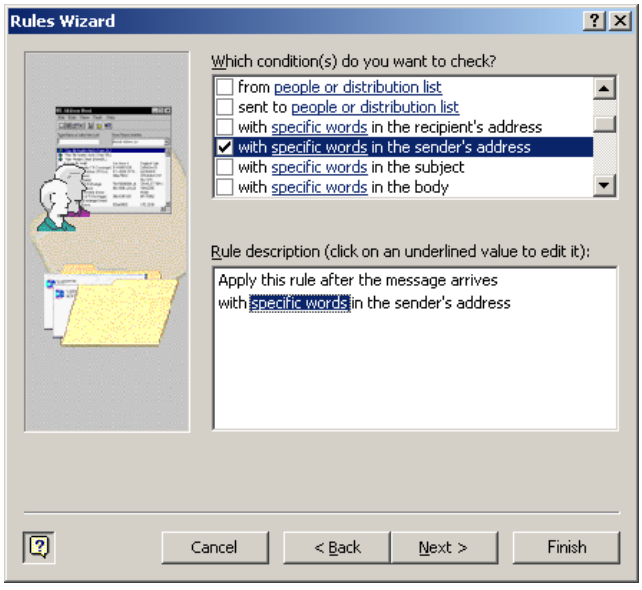
Spam got you down? Want to filter out that pesky source address? Well, you too can fight back against Spam by blocking source addresses within Outlook.



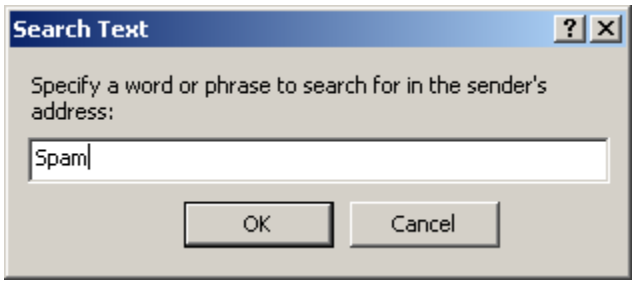
From the Outlook menu go to Tools on the Toolbar, and then select Rules Wizard.



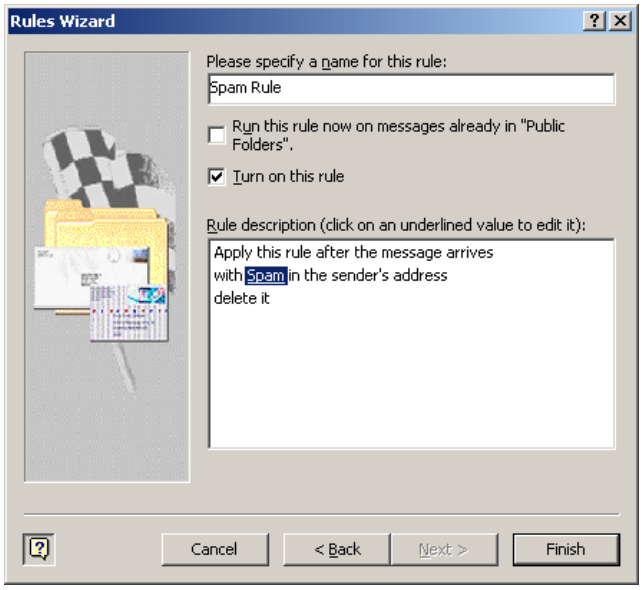
Click "New", highlight "Check messages when they arrive", then click Next.



Then make whatever appropriate criteria you want like "With specific words in the senders address", "suspected to be junk e-mail" or "containing adult content" and click Select Rule.



Then click on rule hyperlink to open Search Text box. Type in a word or phrase selection that you want Outlook to filter out (like the name of the fake Nigerian minister in the message 'From' box), click OK, and Next. Then choose what you want done with such e-mail messages, like 'delete' or 'permanently delete' (only Outlook 2000). Then select any exceptions you want and click 'Next'.



Finally, name the rule, choose to turn it on (or run it on all current mail folders to weed out your Outlook folders), and then click Finish.

Now you are done, and the specific filter you have created should sort out that particular unsolicited email. Please note that the term "Spam' has been used only as an example in this filter, you'll need to supply the specific term from the unsolicited mail you want to filter.

If you are getting spam from many different sources, its still easier to simply delete the messages and get on to your other email. If you are getting lots of spam from a specific sender or getting porn spam, then filtering it within your own Outlook is an option you may want to consider.

William Hubbard

Return to Table of Contents

Linked Articles

Education

2002 Security Awareness Index Report (tm): The State of Security Awareness among Organizations Worldwide
PentaSafe's Security Awareness Index (TM) represents the first major effort to measure how organizations improve security awareness and understanding, and how well employees understand and act upon information security policies, threats and issues in their respective organizations. Nov. 8, 2002, ITToolBox and Pentasafe

The Complete Windows Trojans Paper

This is a paper about Windows Trojans describing how they work, their variations and strategies to minimize the risk of infections. Sept. 26, 2002, Frame4 Security Systems

Dear Saddam, How Can I Help?
On the afternoon of July 17, a self-proclaimed expert in biochemistry composed an e-mail message to Saddam Hussein. Oct. 28, 2002, Wired
Editor's note: This article illustrates well that e-mail should never be considered private unless it is encrypted, and that email systems can be broken into, and that bad passwords can ruin almost any security.

The V-Files: A Dictionary of File Threats
This White Paper is an alphabetical lexicon containing descriptions of file types, formats, and virus information. Its purpose is to offer information about the types of files that can be infected by particular viruses. Nov. 25, 2002, ITToolBox

SQL Injection and Oracle
This is the first article in a two-part series that will examine SQL injection attacks against Oracle databases. The objective of this series is to introduce Oracle users to some of the dangers of SQL injection and to suggest some simple ways of protecting against these types of attack. Nov. 21, 2002, Security Focus

NIST Sets Security Checkup Standards
Federal agencies get their first peek Monday at proposed guidelines that, by spring, will begin to standardize the testing of systems security.
See also: http://csrc.nist.gov/

Reverse Engineering Hostile Code
This article outlines the process of reverse engineering hostile code. By "hostile code", we mean any process running on a system that is not authorized by the system administrator, such as Trojans, viruses, or spyware. This article is not intended to be an in-depth tutorial, but rather a description of the tools and steps involved. Armed with this knowledge, even someone who is not an expert at assembly language programming should be able to look at the internals of a hostile program and determine what it is doing, at least on a surface level. Oct. 28, 2002, ITToolBox

Fear Factor
This article promises a reality check on your top five concerns about reporting security incidents. Oct. 28, 2002, ITToolBox

Busting Pop-Up Spam
Nuisance messaging demonstrates the boundless ingenuity of Spammers. Here's how to nip it in the bud. Oct. 24, 2002, ITToolBox

Security training for IT managers
In the broadest sense, there are two ways that an IT manager can acquire this needed wisdom: through on-the-job training and through formal and informal learning. Nov. 15, 2002, Computer World

Comdex: Accept that the Net is vulnerable to attack, panel says

Companies and home Internet users need to accept that the global computer network is inherently vulnerable to attacks, worms, Trojans and anything else miscreants want to unleash on it, and then accept that securing the system is everyone's responsibility, a panel of security experts said yesterday at the Comdex trade show. Nov. 19, 2002, Computer World

Study: System admins slow to zap bugs
System administrators are still not patching systems frequently enough, according to a recently published study of a software security flaw that allowed the Linux Slapper worm to spread. Nov. 19, 2002, C/Net

Microsoft Revises Its Security Response Center Security Bulletin Severity Rating System
See: http://www.microsoft.com/technet/security/policy/rating.asp
Nov. 2002, Microsoft

A Greater Threat than Software Viruses?
Active Internet content, invisible software microbes that silently enter computer networks and provide sensitive information to outside agents, now poses a greater threat to companies than viruses, according to a report by the Aberdeen Group. Nov. 18, 2002, Advisor

Chinese DNS Spoofing
A report has been released to show how a large-scale DNS record spoofing attack has occurred in China that appears to be the work of the Chinese government in a new wave of Internet censorship. The report contains a full explanation. Oct. 2, 2002, DIT Inc

10 simple ways to stop hackers or at least slow them down
Hackers are always on the prowl for weaknesses in your systems, but there are ways to beef up security so you don't become the next easy target. Nov. 30, 2002, Security Portal

Charting Ethical Waters
Ethics-based security policies will prevent you from being submarined by privacy problems. Nov. 2002, CSO Online

Hardening Linux Systems
Linux Magazine has released a guide for hardening a Linux installation. They offer a final checklist to use to double-check all of your steps throughout the installation and configuration process. This guide would be appropriate for hardening things like a Linux web server or firewall. Sept. 2002, Linux Magazine

Winning the Cybersecurity War
There must be a fundamental shift from addressing vulnerabilities in a reactive mode to tackling them proactively. Nov. 25, 2002, NewsFactor

CompTIA Develops Vendor-Neutral Security+ Certification Course
NIST helped develop the credential and the certification test, which is billed as a global standard for both new and veteran IT workers, who fill "frontline" security-related positions. Dec. 2, 2002, CompTIA

Practice Makes Perfect
A walk through of an emergency management training-event at USAA, a Texas company with over 20,000 employees. Continuity plans cannot exist only on paper. Regularly putting them into practice lets the company see how it would function in a real situation. Nov. 2002, CSO Online

Six basic Tips for securing wireless networks
Wireless networks offer opportunities for hackers. But it doesn't have to be that way. The purpose of properly securing a wireless access point is to close off the network from outsiders who do not have authorization to use your services. Dec. 10, 2002, SNP

Homeland Security

Homeland security agency a reality
President Bush on Monday formalized the biggest government reorganization in more than 50 years, signing legislation creating a Department of Homeland Security. Nov. 25, 2002, MSNBC

Bush Signs $900 Million Cybersecurity Act
President Bush today signed legislation dedicating more than $900 million over five years to security research and education to protect the nation's technology infrastructure against hackers and terrorists. Nov. 27, 2002, Washington Post

Preparing for a Different Kind of Cyberattack
While many agencies are still licking their wounds from once again failing their annual information security test, the Department of Defense and the National Security Agency on Thursday will announce a new partnership that could go a long way toward shoring up the security of the government's networks. Nov. 20, 2002, eWeek

Pro-Iraq Hacker Threatens Virus Outbreak
A Malaysian virus writer who is sympathetic to the cause of the al Qaeda terrorist group and Iraq, and who has been connected to at least five other malicious code outbreaks, is threatening to release a mega virus if the United States launches a military attack against Iraq. Nov. 20, 2002, PCWorld

Tech Provisions Added to Homeland Security Bill
The homeland security legislation heading for likely approval in Congress this week includes last-minute changes that could have far-reaching implications for computer security and Internet privacy. Nov. 14, 2002, Washington Post

Secret U.S. court OKs electronic spying
A secretive federal court on Monday granted police broad authority to monitor Internet use, record keystrokes and employ other surveillance methods against terror and espionage suspects. Nov. 18, 2002, C/Net

Pentagon drops plan to curb Net anonymity
A Defense Department agency recently considered--and rejected--a far-reaching plan that would sharply curtail online anonymity by tagging e-mail and Web browsing with unique markers for each Internet user. November 22, 2002, C/Net

Pentagon data mining: Just say 'no'
This is a commentary on the Pentagon's Total Information Awareness (TIA) program's effort to create a massive database of personal citizen information. Nov. 20, 2002, InfoWorld – Ethics Matters

Can This Department Be Saved?
This is a commentary on the new Department of Homeland Security, dealing with bureaucracy and funding issues. Nov. 22, 2002, MSNBC

Guardent To Offer Free Vulnerability Testing of National Critical Infrastructure
Responding to the early warning signals from recent attacks on the Internet's DNS infrastructure, Guardent announced today its Critical Infrastructure Protection Program that offers free network vulnerability testing to critical infrastructure organizations. Nov. 7, 2002, Guardent

Cyber Crime

New Twist to Nigerian Net Scam
The new scam involves wiring bad cashier's checks and sending out transportation fees. Dec. 16, 2002, Wired

Alleged big music piracy ring busted
A New York based group was busted for music piracy in an operation worth millions of dollars. The Secret Service busted the largest ever seizure of music piracy equipment in the US. Dec. 13, 2002, MSNBC

It's Not Easy Being Breached
Surviving a security incident is just the beginning – then you need to figure out what it really cost. Dec. 2002, CSO Online

Feds: Largest identity theft ring in U.S. history busted
Federal authorities charged three men with orchestrating a huge identity-theft scheme in which credit information was allegedly stolen from more than 30,000 victims. Nov. 25, 2002, CNN – Law Center

Seething over Spam
New tools and legislation can help—but nothing can stop it all. Nov. 15, 2002, CIO

Aiding and Abetting Hackers A Crime
Cyber-crime laws and cops are now targeting those who write and distribute hacker toolkits. Oct. 30, 2002, Virus List

Attack targets .info domain system
An Internet attack flooded domain name manager UltraDNS with a deluge of data late last week, causing administrators to scramble to keep the servers that host .info and other domains up and running. Nov. 26, 2002, C/Net

Woman gets 9 years in piracy case

A California woman has been sentenced to nine years in prison for software piracy, in what may be the longest sentence ever given to a first-time felon in a software counterfeiting case. Nov. 26, 2002, C/Net

Bettor Pleas Guilty to Scam
One of three men charged with manipulating computerized bets worth $3 million in last month's Breeders' Cup pleaded guilty Wednesday to wire fraud conspiracy and money laundering conspiracy. Nov. 20, 2002, Wired News

What's real, what's a scam? eBay users wondering
EBay.com users are being peppered by e-mails saying there has been a security problem at the Web site, and requesting new account and password information. The problem: Some of the e-mails are legitimate, some are scams and it's hard to tell the difference. Nov. 20, 2002, MSNBC

Hacking syndicates threaten banking
The number of organized hacking syndicates targeting financial institutions around the world is growing at a disturbingly fast rate. Nov. 4, 2002, Computer World

British man charged in military hacks
U.S. authorities accused an unemployed British computer administrator of what they said was the largest successful hacking effort against American military networks, secretly breaking into scores of non-classified computer systems, including two inside the Pentagon. Nov. 12, 2002, Computer World

Hacker catches out unwary travel firms
NatWest has launched an investigation after a computer hacker walked away with tens of thousands of pounds in fraudulent credit card refunds following a series of raids on the computer systems of leading travel operators. Dec. 5, 2002, CW360

Hacker From the 'Hood Tells All
Twenty-one years worth of living doesn't usually merit a biography.
But hacker Ejovi Nuwere's new memoir is worth a read, not because it describes a particularly unique life, but because of its intimate look into the life of a technically inclined kid growing up in less than ideal circumstances. Dec. 7, 2002, Wired

DEA Data Thief Sentenced to 27 Months
A DEA employee was sentenced to 27 months in prison for selling information on private citizens he took from law enforcement databases. Dec. 16, 2002, Security Focus

News

NIPC Chief Ron Dick to Retire
Ron Dick, the director of the FBI's National Infrastructure Protection Center (NIPC), the cyber threat and warning arm of the bureau, plans to retire this month, bringing to a close a 25-year career in law enforcement. Dec. 10, 2002, Computer World

CyberWhoCares? IT Should!

In the end, it hardly matters which "cyber" label we use -- cyber terrorism, cyber warfare, cyber crime or cyberattacks -- as long as we pay attention to these early warning signs. Dec. 2, 2002, Computer World

ISS Goes Public With Vulnerability Disclosure Guidelines
Internet Security Systems Inc. on Monday released to the public the vulnerability disclosure guidelines that its internal X-Force research team uses in identifying flaws and notifying vendors and the public. Nov. 2, 2002, eWeek

Security Cert Provider Cries Foul
The non-profit owner of the leading professional certification program for security managers has charged that a rival group's plan to offer a comparable certification will confuse the market and force security professionals to obtain multiple credentials. Nov. 21, 2002, eWeek

Microsoft Spills Customer Data
Microsoft took a public file server offline Tuesday after Internet users discovered that the system contained scores of internal Microsoft documents, including a huge customer database with millions of entries. Nov. 20, 2002, Wired News

Microsoft bolsters security service for novice end users
Microsoft Corp. is expanding its security notification service in an effort to better serve end users who aren't technically savvy, the company said today. Nov. 19, 2002, Computer World

DOD directive aims for layered security
Defense Department agencies last month began following a new policy that sets standards for securing networks using a layered defense-in-depth approach. Nov. 18, 2002, GCN

Student hacks high school computer to LOWER his marks
Reid Ellison, an 11th-grader at Anzar High School in San Juan Bautista, recently decided a cool student project would be to hack into the school's computer grading system. Dec. 17, 2002, SNP
Editor's note: Neat project, and especially important is that he wanted to help the school, and that had permission to do the penetration test.

Hackers Fight Censorship, Human Rights Violations
A hacker group on Tuesday released a novel license agreement that gives end-users the power to enforce the agreement and sue governments and other entities that misuse software covered by the license. Nov. 26, 2002, eWeek

Create Value from Values: The Purpose of Business is Greater than Profits
In our unending quest for value, do we have to compromise our values? What is the relationship between values and value? Indeed, what is the purpose of a business? Nov. 15, 2002, CIO Magazine
Editor's note: Though not an information security news article, this piece from CIO Magazine is timely because it discusses the place of values and purpose in business. Though it is a commentary on corporate America, the concepts in it are easily

transferable to government. With that perspective, no matter what the departmental course, yearly goal, or business initiative is, the purpose of state government is to serve the needs of state citizens – an important concept to remember in uncertain times.

News Homepage links:
Advisor: http://advisor.com/doc/11501
CIO: http://www.cio.com/
C/Net: http://news.com.com/
CNN: http://www.cnn.com/
CompTIA: http://www.comptia.org/default.asp
Computer World: http://computerworld.com/
CSO Online: http://www.csoonline.com/
CW360: http://www.cw360.com/
DIT Inc.: http://www.dit-inc.us/
eWeek: http://www.eweek.com/
Frame4: http://www.frame4.com/
GNC: http://www.gcn.com/
Guardent: http://www.guardent.com/comp_news_press.html
InfoWorld – Ethics: http://www.infoworld.com/
ITToolbox: http://security.ittoolbox.com/news/
Linux Magazine: http://www.linux-mag.com/
MSNBC: http://www.msnbc.com/news/default.asp
Newsfactor: http://www.newsfactor.com/
PCWorld: http://www.pcworld.com/news/
Security Focus: http://online.securityfocus.com/
SNP: http://www.securitynewsportal.com/index.shtml
Washington Post: http://www.washingtonpost.com/
Wired: http://wired.com/
VirusList: http://www.viruslist.com/eng/index.html

Return to Table of Contents

Points of Contact

Kip Peters: Chief Information Security Officer (CISO), Enterprise Security Consulting, Enterprise Security, Policy, Standards, Overall Security Issues
515-725-0362

Marie Hubbard: Charter Projects: Transition Security Issues, Security Planning, Certification and Accreditation Process
515-725-0385

Paul Schmelzel: Security Operations: Vulnerability Assessments, Intrusion Detection, Incident Response, Test Lab
515-281-5956

Larry Brennan: Critical Infrastructure Assurance Coordinator, Iowa Crisis Action Team
515-725-0365

Wes Hunsberger: Business Continuity, Physical Security
515-725-0361

William Hubbard: Security Awareness
515-725-0452

Return to Table of Contents

Links to Resources

http://www.itd.state.ia.us/security/
The awesome Enterprise Security website. You can find tons of state or ITD security information here. Policies, procedures, guidelines, educational resources, lists of services, useful links, and more!

http://www.cert.org/nav/index.html
Homepage for CERT (Computer Emergency Response Team)

http://www.sans.org/newlook/home.htm
SANS (System Administration, Networking, and Security)

FBI and SANS List Top 20 Vulnerabilities
Security leaders led by the FBI's NIPC and the SANS Institute published a revised list of the top twenty Internet security vulnerabilities along with instructions on how to fix them.

Iowa Homeland Security
This site includes much information about Iowa's Homeland Security Initiatives, Press Releases, Preparedness Information, and more.

Homeland Defense Journal
This is the federal Homeland Defense journal homepage.

Stay Safe Online
A site dedicated to educating citizens and helping them secure their home systems. Sponsored by the National Cyber Security Alliance.

Return to Table of Contents

If you have questions or comments relating to this newsletter, or if there is a topic you would like to see an article on, please contact William Hubbard.
Cool artwork provided by Sam Wong.

The ISO Code:

Integrity…Service…Excellence

From the ISO Staff:

Have a Safe and Happy Holiday Season!