The Security Blanket

Issue 14
March-April 2003

Keeping I.T. Secure.

In This Issue:

From the CISO

CISO Letter: Vigilance

Any time events in the world "heat up," we typically see an increase in nefarious activity; however, despite the war in Iraq, we have yet to see an increase in activity to date. We did see some activity last week but we attributed it to spring break and students having more time on their hands. That tends to happen during every major break. Even though we have not seen an increase, it makes sense to ensure you have all your patches in place and you should step up your monitoring activities. In today's world, it becomes difficult to distinguish between a general hacking attack and something larger, which could possibly be a strategic attack on the United States. Since we manage and protect a portion of our nation's technological infrastructure, we need to do our duty to ensure they are protected and do not contribute to an attack somewhere else.

On another tact, this is my last issue of the Blanket. As you read this, I will have already begun at Farm Bureau Financial Services as their first Director of Enterprise Information Protection. The last four years have been equal parts excitement, exhilaration, and frustration, but it has always been enjoyable. I wish you all the best.

Kip Peters

Return to Table of Contents

Feature Articles

What Do You Do When Someone Leaves?

With the departure of the current Chief Information Security Officer, we are reviewing our exit procedures. And frankly they could use some more work.

Exit procedures are as important as the initial interview for a new hire. Project status reports for uncompleted tasks, turning in office equipment (before the scavenging begins!), planning the farewell party… so much to do, you certainly need a checklist to be sure you get it all done.

Whatever the reason an employee is leaving, there should be a process to ensure all the security authorizations they had are cancelled, all their physical access permissions are terminated, any keys and pass cards collected.

Of course, this assumes you have a policy in place to limit access to the things the employee actually needs for their job, and can therefore easily determine what access the employee has been granted. It also assumes you occasionally audit the access lists to see who may have been authorized in error or whose changing duties no longer require access. It is nearly impossible to discover who has access rights without a policy and audit procedures.

This is also a good time to get feedback for improving your organization. After all, this person agreed to be an employee in the past and now no longer desires to work for your agency. It might be enlightening to find out the reasons instead of assuming you know why the person is leaving,

But apart from the physical and personnel matters, there is another aspect to employee departure that needs attention. Besides locking them out of your building and your network, verify any online accounts are cancelled, especially those accessible from the Internet.

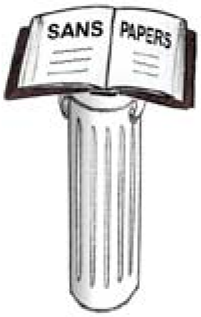
Your departure policy should also include what happens to the work left behind - who gets access to the electronic and paper files this person used to have in their custody. The departing employee should be asked to delete any personal items - no matter what your policy is there will be some things the person would rather not share. Depending on he situation, the employee may need to be supervised during this process.

Losing an employee is always disruptive, whatever the reason. They take their personality, habits, experience, and familiar patterns and leave a void that has to be addressed by the remaining staff. A good departure policy can keep this disruption at a minimum; no departure policy leaves you exposed to any number of unhealthy possibilities.

John Maxwell

Return to Table of Contents

ITD Personnel SANS Papers



Over the past year, several members of ITD have completed SANS security certifications. This process required not only lots of studying and taking challenging exams; it also required an in-depth ‘Practical’ paper on a specific security subject. Feel free to peruse these papers if any of them pique your interest, or drop by the SANS or GIAC sites to check out many other security issues or papers.
SANS: http://www.sans.org/index.php
GIAC: http://www.giac.org/

Improving Risk Estimation Accuracy
http://www.giac.org/practical/Larry_Brennan_GSEC.doc
Lawrence W. Brennan

Integrating Security into Network Redesign
http://www.giac.org/practical/Marie_Hubbard_GSEC.doc
Marie Hubbard

Methods and Techniques of Implementing a Security Awareness Program
http://www.sans.org/rr/aware/methods.php
William Hubbard

Security Complexity – Consultant Myth?
http://www.giac.org/practical/John_Maxwell_GSEC.doc
John Maxwell

Secure Open-Source Network IDS
http://www.giac.org/practical/Jared_McLaren_GSEC.doc
Jared McLaren

Nessus: Vulnerability Scanning and Beyond
http://www.giac.org/practical/Paul_Schmelzel_GSEC.doc
Paul Schmelzel

Nimda – Surviving the Hydra
http://www.giac.org/practical/GCIH/Paul_Schmelzel_GCIH.pdf
Paul Schmelzel

Return to Table of Contents

Current Activities

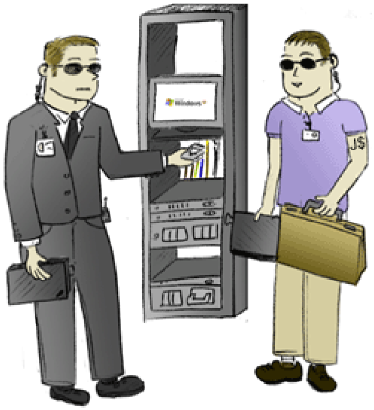
Things we've been up to… ITD/Enterprise security policy drafts, testing lab activity, IDS, Anti-Virus, working towards the departmental integration, ICAT Exercises - lots of cool stuff!

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 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 Security Awareness Tutorial (SAT) is an online/CD-ROM based training course that covers security topics like Confidential Information, User Accounts and Passwords, Workstation Security, Malicious Code (Viruses, Trojans, and Worms), Laptops, and Modems. 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 is 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.

OTHER ACTIVITIES

Enterprise Security Website

The ISO site contains Security Awareness Resources, Operational Services, Policies, Procedures, Recommended Reading, and Mobile News, and Industry Best Practices. It's a free resource of Enterprise and ITD security information.

Educational Extras

Extra resources are available here for State of Iowa security awareness efforts and home personal computer security. New additions include the CERT Home Computer Security Guide, the CIAC Home Security Guide, and others.

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 offered to Enterprise departments.

These materials include the ISO "Guidelines for Information Security and Internet Usage", the Federal Trade Commission's "Safe at Any Speed" and "Identity Theft" guides, and password help sheets, all of which are designed to be beneficial both in the work place and at home. If you or your department would like to obtain some of these free documents contact Security Awareness.

New Policies, Guidelines, and Procedures

We have two new policies, the Information Security Officer Policy Draft, and the Enterprise Security Awareness Policy Draft. Also take a look at our Guidelines and some Procedures and Guidelines from Other Sources on our website. Some newer ones include Securing Web Applications (OWASP Project) and Building and Configuring More Secure Websites.

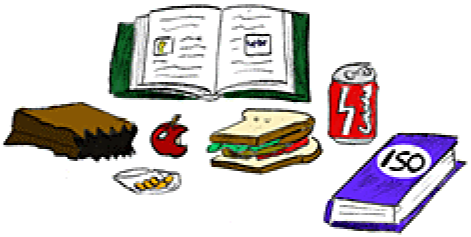
You can find a complete list of Enterprise and ITD security policies, guidelines and procedures, as well as great industry guidelines at http://www.itd.state.ia.us/security/reading.html.

Return to Table of Contents

Upcoming Classes and Consultations

This is the place to learn more about information sharing, security training, conferences, programs, and 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.



Planned Future Sessions Include:

- ITD and Enterprise Policies
- Safe Data Removal
- Business Continuity
- Secure Application Development

An updated schedule and past presentations (lots of them - in .pdf, .ppt, and/or video) are available at the Lunch & Learn site.

Please remember - we'll supply the place, the conversation, and the flannel-graph, 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. 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. Visit http://www.sans.org/newlook/home.php for more info.

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. SANS often can arrange a special on-site session for a reduced cost. Details: http://www.sans.org/onsite

SANS next free Webcast: April 2, 2003 (1st Wednesday of each month)
Intellectual Property: Protection, Detection, and Remediation.
Check this and others out at: http://www.sans.org/webcasts/

Sun Microsystems
Sun is conducting beta tests for its "Solaris Security Administrator" certification exams, and is offering a free certification program for those that help to test it. They recommend that a tester have 6-12 months experience administering security on Solaris.
http://www.netsys.com/cgi-bin/displaynews?a=464

Microsoft: (Vendor Announcements)

Free MSDN Webcasts
Microsoft offers free 90-minute live, interactive webcasts on a variety of topics, including security. 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
Microsoft offers online training for a number of their products. Government workers also get discounts. To register for a course, or just to check them out, visit their website:
http://www.msgovernmenttraining.com/offer/

Other Events:

Gartner IT Security Summit
Date: June 2-4, 2003
Location: Washington, D.C

The combination of Gartner's established Enterprise IT Security Conference and the SECTOR 5 Summit on cyber terrorism and critical-infrastructure protection, creates the authoritative event for both private and public-sector IT security professionals. Attendees of the Summit will learn about:
* Detecting and preventing intrusion and security breaches
* Best practices in security and risk management
* How to select the right security products and which vendors to trust
* Measuring information-security effectiveness and return on investment

USENIX 2003
Date: June 9-14, 2003
Location: San Antonio, TX

A six-day, multiple-track event which includes tutorials, technical sessions composed of refereed papers, invited talks, Guru-Is-In, and Birds-of-a-Feather sessions. Choose from 24 full-day tutorial classes. Topics include: Managing LDAP Directories; Managing Samba 2.2 & 3.0; Advanced Topics in Sysadmin & Security; Solaris Internals; Inside the Linux Kernel; Network Security; WiFi Security; Intrusion Detection; Disaster Planning; and more.

FIRST Computer Security Incident Handling Conference
Date: June 22-27, 2003
Location: Ottawa Canada

This conference focuses on the field of computer security incident handling and response. In recognition of the global spread of computer networks and the common problems faced by computer owners, the conference is held in a different part of the world each year. The presentations are international in scope and include the latest in incident response and prevention, vulnerability analysis, and computer security. Additionally, these events serve as the foundation for the improvement of computer security worldwide via the sharing of goals, ideas, and information.

Other notable events in the month of April:
http://security.ittoolbox.com/events/event_body.asp?c=Security_Press&r=http%3A%2F%2Fsecurity%2Eittoolbox%2Ecom%2Fevents%2Fevent%5Fbody%2Easp
Yearly calendar hosted by ITToolbox

Return to Table of Contents

Helpful Hints

Security Incidents – Who Ya Gonna Call?

Email isn't working! My workstations won't boot! My project directories are gone! Cats and dogs are living together! Mass hysteria! Aaaiiieeeee!!! Who ya gonna call?!?

Well, actually, for all these, just call your agency Help Desk. They can either help you directly or forward your problem to someone who can. For ITD, security incidents should first be reported to Help Desk personnel. Not only does this serve to easily route the problem to the appropriate personnel, it can also provide the Help Desk with a situational overview if the problem becomes widespread.

For serious security issues like worm or virus propagation, Help Desk personnel can assist with the determination of how fast the intrusion is spreading, how far it gotten, and how many workstations, websites, or services it has disrupted. Your Help Desk personnel may not be highly trained, professional Ghost Busters with unlicensed nuclear accelerators on their backs, but they are awfully good at what they do – helping departmental employees with workplace problems. Give them a call - they're ready to believe you!

William Hubbard

Return to Table of Contents

Linked Articles

Featured Link

Honestly?!
Ethical behavior isn't easy, just essential. Here's how to run an honest organization and be an ethical leader. 3/15/03, CIO
Editor's Note: Good advice for everyone in the workplace.

Helpful Security Guides

Incident Response Tools For Unix, Part One: System Tools
This article is the first in a three-part series on tools that are useful during incident response and investigation after a compromise has occurred on an OpenBSD, Linux, or Solaris system. This installment will focus on system tools, the second part will discuss file-system tools, and the concluding article will look at network tools. 3/27/03, Security Focus

CIS Releases New Benchmarks - W2K Server, Solaris, Cisco IOS Router
The Center for Internet Security (CIS) has released a new security configuration benchmark for Windows 2000 Server and updates to the benchmarks for Solaris and Cisco IOS Routers. Other Benchmarks include: W2K, W2K Pro, Windows NT, Linux, and HP-UX.
http://www.cisecurity.com/

The Microsoft Security Update Offers Home User Edition

Microsoft is making non-technical alerts available for home users. This service is designed to make it easier for home users to keep aware of and deal with new vulnerabilities and patches. Visit the following site for more information or to sign up: http://www.microsoft.com/security/security_bulletins/decision.asp

Education

Four basic steps can get hackers into most computers

Every breach of computer security is different, depending on the skills of the attacker and the defenses in your system. But most hackers follow the same four basic steps to perpetrate an attack — profiling, scanning, enumerating and exploiting. 03/17/03, SNP

Experts repeat: Security is a people—not technology—problem

A survey released today by the Computing Technology Industry Association showed that nearly two-thirds of reported security breaches were primarily the result of human error. 03/18/03, GCN

Picking up the pieces

There are few things more critical to an IT department than having a good, thoroughly tested backup and disaster recovery program in place. 3/10/03, GCN

Disaster scenario reveals private-sector misperceptions, concerns

On the eve of military action by the U.S. and with terrorist attacks against the private sector still possible, CIOs and IT managers remain confused about the roles and missions of various organizations involved in response and recovery efforts stemming from a major disaster, according to former CIOs and experts. 03/06/03, ComputerWorld

Security in a box: It's not enough

What will be the next security device du jour? 3/11/03, ComputerWorld

Virus Hoaxes and the Real Dangers They Pose

Virus hoaxes are not real viruses, by definition, but that doesn't mean they don't have negative effects. In fact, virus hoaxes can be quite damaging in a number of different ways. 3/25/03, Security Focus

CERT® Summary CS-2003-01

Each quarter, the CERT® Coordination Center issues the CERT Summary to draw attention to the types of attacks reported to our incident response team, as well as other noteworthy incident and vulnerability information. 3/21/03, CERT

IDS Logs in Forensics Investigations: An Analysis of a Compromised Honeypot

This paper deconstructs the steps taken to conduct a full analysis of a compromised machine. The objective of this paper is to show the value of IDS logs in conducting forensics investigations. 3/18/03, Security Focus

Homeland Security

Feds: Chinese Hack Attacks Likely
Chinese hacker groups are planning attacks on U.S.- and U.K.-based Web sites to protest the war in Iraq, the Department of Homeland Security warned in an alert that it unintentionally posted on a government Web site. 3/31/03, Washington Post

States need cyber security focus
A new Zeichner Risk Analytics LLC study found 36 state governments have failed to prepare, adopt and implement acceptable cybersecurity policies, which could have damaging consequences to citizen services, communication systems and critical utilities if the nation were to undergo cyberattacks. 3/24/03, FCW
The Report: http://www.zra.com/docs/summaryReport.pdf
Editor's note: It is gratifying to see that Iowa is one the 15 states in compliance with the GBLA Safeguard Statutes and Regulations.

HSD warns of cyberattacks, names officials to top IT posts
Shortly after President Bush set a 48-hour deadline last week for President Saddam Hussein to leave Iraq or face invasion, the Homeland Security Department reminded Internet users to be vigilant for cyber attacks. 3/24/03, GCN

DOD sets net security plan
The Pentagon's latest information assurance directive offers specifics that Defense Department users need to secure military systems, but some observers fear that the new policy could complicate the acquisition and budget processes. 3/10/03, GCN

Terror Suspect's Photos Cited
Trade Center Pictures Found on Computer of Saudi Student. 3/12/03, Washington Post

Wireless infrastructure goes unguarded
The national wireless infrastructure "is one of the most important and least protected parts" of U.S. communications capability, a technology strategist said today. 3/26/03, GCN

NIST rates facial recognition systems
After testing 14 facial recognition products, the National Institute of Standards has identified software from Cognetic Networks Inc. of Houston, Eyematic of Los Angeles and Identix Inc. of Minnetonka, Minn., as the most reliable. 3/17/03, GNC
The Test Results: http://www.itl.nist.gov/iad/894.03/face/face.html#FRVT2002

"F" is for Feds
Beleaguered public sector CSOs are grappling with tight budgets and red tape in a battle to secure their systems. How do the government's security efforts stack up against the private sectors'? 3/03, CSO

Cyber Crime

ID theft costs banks $1 billion a year
While only an estimate, it is one of the first attempts to put a detailed price tag on what has been called the nation's fastest growing crime. 3/26/03, MSNBC

Cybercriminals threaten economic, personal safety
Michigan's computer community is at war -- a cyberwar against organized gangs of computer criminals who are attacking businesses, government agencies and financial and medical institutions. 3/20/03, ITToolBox

Computer Security Experts Scramble to Keep Up with Hackers
Information security is not a point in time; it's a learning process that never ends. 3/17/03, ITToolBox

Hackers Evolve From Pranksters Into Profiteers
Computer identity theft has long been a fast-growing cyber crime. But increasingly, hackers are seeking profit rather than just fun. 3/17/03, ITToolBox

The darkest side of ID theft
Losing your clean credit history is one thing; losing your freedom is another. And victims of America's fastest-growing crime are discovering they often have much more to worry about than the hundreds of hours of paperwork necessary to clean up the financial mess associated with ID theft. Sometimes, they have to worry about ending up in jail — again and again. 3/9/03, MSNBC

LapLink says hackers left key clue
LapLink had been hacked, a situation becoming increasingly common among corporations. But LapLink's crisis had an unusual twist. 3/15/03, Seattle Times

Forecast: Cyberlitigation
Legal experts say rising security breaches will result in more civil and criminal court cases. 3/03, InfoSec Mag

Hackers strike Georgia Tech computer and grab data on 57,000 credit cards
Computer hackers invaded a computer at Georgia Tech and copied names, addresses and, in some cases, credit card information for 57,000 patrons of the Ferst Center for the Arts. 3/28/03, Security Focus

News

War Worms Inch Across Internet
The U.S. military action in Iraq has stirred up computer virus writers and malicious hackers, who have apparently decided to vent by defacing websites and releasing e-mail worms that prey on people's fears and curiosity. 3/21/03, Wired News

Info seekers, hackers besiege government sites

War protesters and hackers are assaulting .gov and .mil Websites “in digital retaliation” for the war in Iraq in record numbers, according to the security firm mi2G Ltd. of London. 03/21/03, GCN

Washington struggles with privacy vs. security
At two conferences on technology and homeland security here Thursday, controversy arose over whether technological measures designed to protect the U.S. from terrorism should proceed unhindered or if such things as data-mining programs must be halted until there are protections to civil liberties in place. 3/20/03, InfoWorld

Media Gone Mad
Why last week's big Windows security hole is nothing more than technology press hot air. 2/24/03, Security Focus

Hackers replace Al-Jazeera Web site with American flag
Hackers today replaced the English-language Web site for Arab satellite television network Al-Jazeera with a U.S. flag and the message "Let Freedom Ring." 3/27/03, Seattle Times

Tighter security vowed for CSU computer records
Faced with complaints that it was violating student and employee privacy, California State University announced on Wednesday that it would immediately tighten security on its controversial computer system, which allowed users access to Social Security numbers and other confidential information. 3/27/03, ITToolBox

$100K study to assess universities' e-security
Arizona's Board of Regents is spending $100,000 to assess the security of computer networks at the three state universities, as campus experts say not a day passes without an attack. 3/21/03, ITToolBox

Florida Launches Cyber Security Website
The Florida Department of Law Enforcement launched a cyber security Web site targeted at better securing small businesses and home users from hackers and computer fraud. 3/24/03

Hotmail takes steps to freeze spam
Microsoft's free web-based email service limits users to sending 100 emails per day. 3/25/03, VUNNet

ACLU cyber chief worried about privacy
Since the September 11 attacks, trying to beat back a technology-propelled surveillance society has been Steinhardt's No. 1 mission. He believes he will probably lose -- but not without trying to at least win greater court oversight or other limits. 3/30/03, CNN

News Homepage links:

CERT: http://www.cert.org/nav/index_main.html
CIO: http://www.cio.com/
CNN: http://www.cnn.com/

Computer World: http://computerworld.com/
CSO: http://www.csoonline.com/
FCW: http://www.fcw.com/
GNC: http://www.gcn.com/
InfoSec Magazine: http://www.infosecuritymag.com/
InfoWorld: http://www.infoworld.com/
ITToolbox: http://security.ittoolbox.com/news/
MSNBC: http://www.msnbc.com/news/default.asp
Seattle Times: http://seattletimes.nwsource.com/html/home/
Security Focus: http://online.securityfocus.com/
SNP: http://www.securitynewsportal.com/index.shtml
VNUNet: http://www.vnunet.com/News
Washington Post: http://www.washingtonpost.com/
Wired News: http://wired.com/

Return to Table of Contents

Points of Contact

The Unknown CISO: Chief Information Security Officer, Enterprise Security Consulting, Enterprise Security, Policy, Standards, Overall Security Issues

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, Exercise Design
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

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. Includes the final version of the Iowa Homeland Security Initiative.

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