SECURITY AWARENESS NEWSLETTER

Volume 1; Issue 3

In This Issue:	Workstation Security
The GOT Mission Statement	Physical Security Initiatives
Security Initiatives	The Information Security Checklist
Security Alerts and Updates	Acceptable Use
Security Incident Reporting	Featured Article
Password Protection	Useful URL's

THE GOT MISSION STATEMENT

To work in partnership with state agencies in meeting the needs of Kentucky's citizens by addressing business problems and opportunities through the effective use of information technology and services.

Back to Top

SECURITY INITIATIVES

Security objectives have become a focal point as the Commonwealth of Kentucky progresses toward providing greater access, more information, and new services to state employees and citizens. These objectives include, yet are not limited to, providing timely security alert notifications and updates as well as weekly security alert recaps, upgraded standards and procedures for security incident reporting and handling, continued awareness and safety tips on password protection and workstation security, and the latest initiatives toward physically securing Commonwealth facilities. Enhancements such as incident reporting and handling are used to prevent further similar incidents from occurring, as well as building security awareness across the Commonwealth of Kentucky. GOT now

offers a bimonthly Security Awareness newsletter to help GOT staff stay abreast of security-related issues. The newsletter also focuses on the principles contained in the GOT Security Policies and Procedures Manual, including virus protection. In addition to this, Security Awareness Training will be provided in an effort to educate users annually on their security responsibilities. Please remember, "Security Is Everyone's Responsibility."

Back to Top

SECURITY ALERTS AND UPDATES

Reporting

The GOT Security Services Division is currently working toward improving their process of security alert notification. This process and your response to it is considered to be a vital component in securing assets belonging to the Commonwealth of Kentucky. GOT is providing this information so that you can be aware of the latest security threats, vulnerabilities, software patches, etc. The Division of Security Services and the System/Network Administrators who are responsible for implementing security measures must continue to stay updated of security alerts issued by GOT.

These security alerts are obtained by GOT from a variety of sources including vendor subscription services like Security Focus. It is the intent of GOT to be the clearinghouse for the identification, collection, and dissemination of information to other Commonwealth Agencies to save each of them the effort of performing the same tasks. The basic criteria for Agency emergency notification will be 1) Alerts rated at least "9," (out of 1 to 10); 2) impacts enterprise standard tools; and/or 3) has the potential to cause harm if ignored. GOT has the philosophy that they would rather send too much information than risk not sending something important.

In addition, on a weekly basis, GOT will produce a "Weekly Security Alert Recap." This recap will attempt to cover all security alerts not deemed as an immediate threat to the Commonwealth of Kentucky computing environment. This weekly recap will also be emailed to the GOT regular security contacts and other appropriate distribution lists. Security Alerts that are sent out both daily and weekly will also be posted on the Security Alerts web page at: http://kygovnet.state.ky.us/protected/got/secalert/security_news.htm. After 90 days, older Security Alerts will be moved to an Archive section of the Security home page.

Back to Top

SECURITY INCIDENT REPORTING

It is the responsibility of all Governor's Office for Technology (GOT) staff to report suspected security violations immediately. A security incident is defined to be any event or threat of an event, affecting normal operation of a GOT managed computer system and/or facility. A Security Incident Reporting Form has been revised and is made available for use

in reporting security incidents. This can be found at: http://www.gotsource.net/dscgi/ds.py/Get/File-1921/GOT_F012.rtf Staff should send the completed form to their branch manager who will notify the appropriate executive level management and the Director of the Division of Security Services. If the branch manager is not available, it should be sent to the Director of the Division of Security Services.

Within 60 days, a follow up report should be completed by the branch manager involved describing what actions were taken to remedy the breach.

The Division of Security Services encourages GOT customers to complete the Security Incident Reporting Form and send it to the Director of the Division of Security Services.

Back to Top

PASSWORD PROTECTION

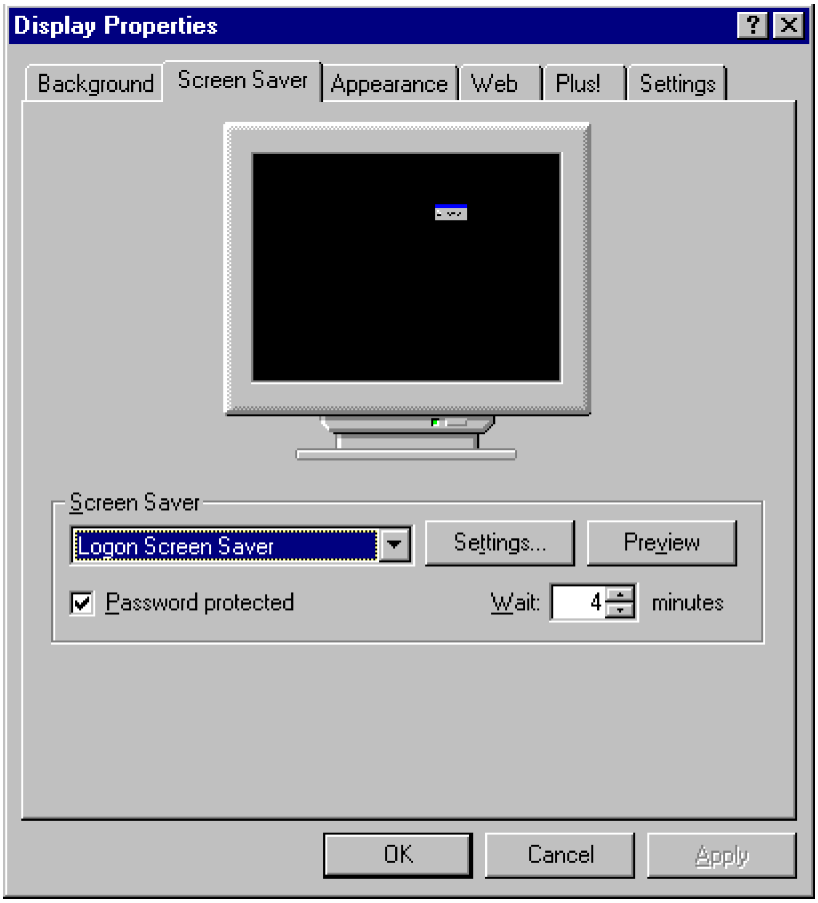
The GOT policy for UserIDs and passwords will improve the likelihood that the identification of the user is correct and that a user's access is controlled effectively. The individual to whom the UserID belongs will be responsible for every action initiated by that account. UserIDs and passwords are important deterrents to vulnerabilities. This policy also pertains to those individuals that are provided with administrative access to support servers. These UserIDs grant the utmost authority; therefore, it is absolutely critical that a good, effective password policy be implemented, monitored, and enforced. Passwords should include mixed-case alphabetic and include non-alphabetic characters. Please click here to view the May 2001 Security Newsletter for additional User IDs/password information as well as password creation tips.

Please remember that security is everyone's responsibility. Ifinadvertent disclosure is known or suspected, the password must be changed immediately. In the event misuse is suspected, do NOT change the password; IMMEDIATELY notify the Division of Security Services or the Network Administrator. For additional details on the password policy, please see Section 3.0 (pg. 28-31) of the 067 Security Policies and Procedures Manual.

Back to Top

WORKSTATION SECURITY

In an effort to protect Commonwealth equipment and standards, and abide by the GOT policy set forth in the Security Policies and Procedures Manual, the following instructions detail how to automatically have your screensaver lock your workstation:



- Right click anywhere on the desktop.
- Click "properties" to display the "Display Properties" dialog box below (or Control Panel/Display), and click the "Screen Saver" tab.
- Click the "password protected" box under the "Screen Saver" settings, and select the number of minutes you desire.
- Click the OK button.
- Always use C-A-D (Control-Alt-Delete), and then click on "Lock Workstation" when leaving your workstation for any amount of time. Do NOT leave your workstation unattended and open for easy target.

End-user workstations used in sensitive or critical tasks must have adequate controls to provide continued confidentiality, integrity, and availability of data stored on the system.

Workstations must be configured with screensavers to blank the screen and require a password to resume operation whenever the workstations are unattended for more than 15 minutes.

For more information on workstation security, please see Section 1.5 (pg. 24-25) of the 067 Security Policies and Procedures Manual. Also, more detail can be found at http://kygovnet.state.ky.us/protected/got/secalert/security_news.htm

Back to Top

PHYSICAL SECURITY INITIATIVES

The GOT Cold Harbor facility houses the staff and resources for most enterprise solutions for state government. Many of the systems housed and managed within this facility are also key systems for government agencies. While there may not yet be many noticeable

changes in state government facilities around the Frankfort area, it is likely that changes will begin to be implemented soon. GOT staff will be working to change and/or enhance security within this facility over the upcoming months in order to better protect the resources maintained at Cold Harbor. GOT staff will continue to work with other state and federal agencies to review and enhance physical security for state facilities. In the next few weeks and months, you and your staff will begin seeing these changes. We are all responsible for making this a safe and secure environment for staff and for the systems we manage for the Commonwealth. Please encourage your staff to be aware of their surroundings and to understand and implement security policies that are in place today, as well as new policies that will be implemented in the future. An important "quick win" today is to ensure all staff wear their GOT ID badges everyday, which will also ensure they are in compliance with policy.

Back to Top

THE INFORMATION SECURITY CHECKLIST (DO 'S AND DON'TS)

- Do report any suspicious activity immediately by completing GOT F012;
- Do change your password regularly for every Commonwealth system;
- Do use a combination of letters, symbols, and numbers for passwords;
- Do not share your password with anyone including staff;
- Do enable your screen saver password and lock your workstation when unattended;
- Do not visit inappropriate web sites (e.g., hacker sites, pornographic sites).

Back to Top

ACCEPTABLE USE

Internet and Email Acceptable Use Enterprise IT Policy

In compliance with the laws of the Commonwealth and the guidelines provided below, employees of the Commonwealth of Kentucky are encouraged to use the Internet and Email to their fullest potential to further the State's mission. However, inappropriate use of these tools not only risks putting the Commonwealth in a compromising position, but also bounds resources that may potentially affect the Commonwealth statewide. The Division of Security Services encourages you to read the following policy.

	Internet and Electronic Mail Acceptable Use Policy, GOT-060

Back to Top

FEATURED ARTICLE

The potential for serious problems is heightened when networks are flooded with the sending

e-cards. The following article depicts Christmas to be the primary time to send and receive h
forget about Mother's Day and upcoming Valentine's Day - two holidays that are notorious for

EGADS! Watch Those E-Cards (by Anne Saita)

Watch out for those holiday e-cards--they could bring more than goodcheer. Between anthra
times, more people plan to sendelectronic season's greetings this month. At last count, 67 mi
sent through October using popular companies likeFlowgo.com, AmericanGreetings.com and

With that number expected to spike in December, more people also areexpecting to receive e
serious problems for enterprises if employees mistakenly release a virus instead. One commo
virus via e-card is a bogus e-mail directing recipients to a download that unleashes malicious
greeting. Recipients are first sent a note directing them topick up a personal message at a fa
the real thing, including legitimate-sounding URLs like www.sweetcards.cc and www.kindcard
www.loveagreeting.com (all no longer available online). Clicking the URL instead installs a Tr
user noticing. "For some reason, a lot of these (earlier) scams includedvariants of the Subsev
Sundermeier, project manager for antivirus vendor Central Command. In some cases, Sunde
viewers are sent to amirrored Web site and asked to first download a file such as "setup.exe"
browser so they can view the message. Those that doare instead connected to pornography s
malware, once a program is installed, the worm will rummage through address books topropa

"We are seeing more and more of these types of sites popping up,"Sundermeier says. Worms
on recipients' curiosity and ignorance. Circulating an upbeat e-mail message with an attachm
member that looks like an e-greeting, such as "ecard.vbs," is a favorite. "And now, with virus a
remove user intervention--exploiting known vulnerabilities in Internet Explorer to automatically
by viewing the message--I expectthings will continue to get worse," he adds.

So what should e-mail recipients and their employers do? Make sureantivirus software is up t
culprits, establish firm security policies that address e-greetings and personal Internet use,an
Once word gets out on a site (like those mentioned in this story), theyusually do get shut dow
do everything here to make sure that happens,"Sundermeier says. The legitimate e-greeting c
additional help. Most of the top Web sites recently announced they will start charging fees to
e-greetings, providing a little less incentive for tightwads to use electronic means to spread h

Security Wire Digest and Information Security magazine are published by TruSecure, the wor
security services. Copyright (c) 2001. All rights reserved. Redistribution of this newsletter is
content (including this notice) is reproduced verbatim with proper attribution to Security Wire I
Security magazine. http://www.infosecuritymag.com

Back to Top

USEFUL URL 'S

www.nipc.gov

The National Infrastructure Protection Center (NIPC) is the national focal point for gathering

information on threats to critical infrastructures. It is the principal means of facilitating and coordinating the federal government's response to an incident, mitigating attacks, investigating threats, and monitoring reconstitution efforts.

www.incidents.org

Incidents.org is a virtual organization of advanced intrusion detection analyst experts and forensic incident handlers from across the globe. The organization's mission is to provide real time driven security intelligence and support to both organizations and individuals.

www.sans.org

The SANS (System Administration, Networking, and Security) Institute is a cooperative research and education organization through which more than 96,000 system administrators, security professionals, and network administrators share the lessons they are learning and find solutions to the challenges they face.

www.cert.org

The CERT Coordination Center (CERT/CC) is a center of Internet security expertise, at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. The CERT studies Internet security vulnerabilities, handles computer security incidents, publishes security alerts, researches long-term changes in networked systems, and develops information and training to help you improve security at your site.

www.nai.com

Network Associates aspires to be the worldwide leader in network security and availability for e-business. Founded as McAfee Associates in 1989, Network Associates, Inc. was created by the merger of McAfee Associates and Network General in December of 1997.

www.securityfocus.com

Security Focus ensures the integrity of enterprises' assets through its SIA – Security Intelligence service. SIA enables IT managers to get the latest vulnerability information as soon as it becomes available through e-mail, voice message, fax, or SMS (Small Message Service) on wireless phones. SIA provides all known information available about vulnerabilities, their causes, and severities creating actionable information to bolster computers from attack.

Back to Top