Tinucci's Tips
Secure Your Desktop
April 2007

Computer and email security is today's buzz. We hear it from all around – our system administrators, in the newspapers, online, and from other users. We may even know people whose computers were hit by a recent virus attack. However, for most of us the concept of network and/or system security is one with which we have very few common points of reference – network security is "someone else's job", not our job. Our network already has a system administrator, and taking care of these things is their responsibility. Often, they do not even want us to change things on our systems, even if we had the ability (administrator or power user rights) and knew how and what to do.

This common situation does not, however, relieve us from taking responsibility for securing our own systems. Each user should be proactive in protecting his or her computer, whether it is in your office, your desktop at home, or your laptop. Following is a list of steps that you can take to ensure the security of your own system and the safety of the data that resides on it.

Proactive security steps that you can take:

- Use good passwords
- Enable a screen saver and password-protect it
- Beware of downloaded screen savers
- Physically secure your machine
- Install anti-virus software
- Update your virus definitions daily
- Use safe email practices
- Install a personal firewall
- Use the proper user
- Remove unnecessary file shares
- Install security patches
- Scrub your web site of unnecessary information
- Log out of web sites when finished
- Be aware of social engineering

Use good passwords

The quickest, most easily implemented, and most effective security measure that you can employ also costs you nothing – use better passwords (or start using them now if you are not already so doing!). For most of us it is fairly simple to guess the passwords of one or two of our coworkers, particularly if we know a little information about them such as the name of their spouse, children, pets, anniversary or birthday dates, favorite sports team or player, and so forth. Other simply-guessed passwords that people commonly use are their license plate number, their favorite lottery numbers, or their user name plus the month number. (It also helps if you know where they've stashed the Post-It note with all their current passwords.)

Tinucci's Tips
Secure Your Desktop
April 2007

Good passwords have the following characteristics:

- They are at least 7 characters long
- They contain a mixture of upper and lower case letters, as well as numeric digits and special characters (~!@#$%^&*()_+{}|[]\)
- If the system allows, they also contain control characters (hitting a key while holding down the "CTRL" key)
- They do not spell any word that can be found in any dictionary (including foreign words)

There are two easy strategies that can assist you in remembering good passwords. The first is to use only the first letter of the words in a phrase, called a "pass phrase" (checking to make sure that the resulting letters do not spell a word). The second is to insert numerals and special characters between letters of words or pass phrases. Finally, it is important to remember that passwords should not be shared – if you must give out your password to someone, remember to change it immediately afterward to protect yourself.

Using a pass phrase to create a password works like this:

a) Choose a phrase – "All good boys like ice cream"
b) Take the first letters of each word in the phrase – agblic
c) Add some numerals and substitute numerals for similar-looking letters – ag16bl1c
d) Add some random capitalization and other characters – aG16#bL1C
e) Voila! A password that is very difficult to guess but easier to remember.

Enable a screen saver and password-protect it

Most of us leave our desks unattended for some period of time. Rather than closing all our work in progress, or logging out of any system in which we might be working, we often just walk away from our systems. If we have been working in sensitive documents or critical systems (banking or collection systems come immediately to mind) and just walk away, nosy coworkers can see

To enable the screen saver on Windows desktops:

- Right click on the desktop
- Choose "Properties"
- Choose the tab labeled "Screen Saver"
- Choose one of the screen savers
- Check the box for "Password Protected"
- Click "OK"

our activity in the best case and in the worst case can perform actions in the system as if they were us. This is obviously not good from an internal control perspective, and can be disastrous for us personally if they use our system to perpetrate crimes.

A quick adjustment to your desktop can at least discourage prying eyes from seeing your work in progress – enable your screen saver. Choose a fairly short interval (Wait time) so that the screen saver kicks in quickly after no activity. For additional protection, password-enable it so that someone accessing your computer must also know your password to get back into your system while you are away.

Beware of downloaded screen savers

Most desktop operating systems, and primarily Microsoft Windows© products, come with screen savers built into the system. However, most of us want to customize our computing environment and we can do so by downloading screensavers from the Internet. Unfortunately, many screen savers available over the Internet (particularly some free ones) contain Trojan Horses, viruses, or other malicious code that can compromise your system. Before downloading new screensavers, ask your system administrator if you are allowed to do so. You might even want to ask them for a recommended set of screensavers or sites from which it is safe to download. If they say no, or if you are at all uncertain about the safety of a particular screen saver, ***do not download and install it!***

Physically secure your machine

One of the first principles of computer security is that the only completely secure computer is one that is turned off. If allowed by your company policy, always turn off your system when you leave for the day or if you will be away from your system for an extended period of time. No hacker can break into it; you save the energy used to power the system; and coworkers (or

Traditional lore in the security business says that 70 – 80% of fraud and loss comes from inside the organization, with the remainder originating from the outside. While not all studies support this figure (numbers range from 20% to 80% of losses coming from inside the organization), it is clear that insiders have more opportunity and knowledge to commit fraud and perpetuate crimes against the organization. It may be surprising to consider who are really insiders. Obviously, current employees are insiders, but so are ex-employees, contractors, vendors, maintenance personnel, repairmen, and anyone else with access to and/or knowledge of our systems. While most of these people are ethical and honest, it is simply prudent to remove any opportunity for crime rather than blindly trusting in the honest nature of our associates.

others) must boot it up and guess your password before they can do anything to your data or programs.
Most computer crimes are crimes of opportunity. Examine your workspace to ensure that you have minimized opportunities to commit crimes against you and your company. Are passwords written down and obviously displayed? (At least hide them somewhere or, better yet, don't write them down.) Is your laptop visible in your office? (Lock it up in your desk or a secure closet or file cabinet.) Are manuals, reports, or operating procedures lying about, available to casual inspection? (File them away – out of sight, out of mind.) Take the necessary steps to eliminate clues and opportunities from your physical environment, and you will have gone a long way toward significantly enhancing your security.

Install anti-virus software

Viruses once seemed to attract all the press and media attention, as well they should have. While the best outcome of a virus infection is annoyance, many of the exploits circulating today can do genuine harm to your system (including reformatting your hard drives, deleting critical files from your system, logging your every keystroke, emailing files to unknown parties, and much more).
While not all anti-virus software is able to prevent infection by every known virus, the computing environment now requires that every machine in the organization be protected individually. This is because the central email server will not catch every email-attached virus; the host firewall will not screen every malicious web site; and the central server will not check infected USB drives or malicious CDs used on your local system. Does your system have a current anti-virus software program installed? If not, you should ask your system administrator to install a copy on your desktop – even if your network is already protected by anti-virus software on the network server. Most anti-virus programs can also be configured to operate in the background to protect you as you read email, open files, visit web sites, and download files. Make sure you enable this feature on your system for the best protection. Fortunately, the cost of anti-virus software is minimal, and will immediately pay for itself many times over the very first time it prevents your machine from being infected.

Anti-spyware software does the same thing as anti-virus software, except that it is aimed at a somewhat different class of malicious software, or malware. Spyware can be easily installed on your machine without your knowledge, and can do everything from pop up annoying ads to track every single keystroke you make and email them to hackers. Consider installing anti-spyware software or a combination anti-virus and anti-spyware package on your machine, and update daily as you would your anti-virus software.

Tinucci's Tips
Secure Your Desktop
April 2007

Update your virus definitions daily

Installing anti-virus software is only half the battle, however.
New viruses emerge on a daily basis. Most anti-virus software only protects against known viruses and so will not catch newly created ones. If you want to remain protected, you must update your definitions on a regular basis. Based on your computing habits you may not need to update your virus definitions daily; weekly updates may be sufficient. However, if you receive email or use the Internet on a daily basis make sure you carve the time out of each day to update your definitions. (Most programs can be scheduled to automatically update definitions at predetermined times or with specific activities – at a specific time, at startup, etc.). Do not leave yourself unprotected by out-of-date definitions!

Use safe email practices

In today's environment, the most common way to get into trouble is through email. Depending on your system settings, you sometimes may not even have to read your email to trigger a virus; safe email practices are crucial. And, even if the email doesn't contain malicious programs, it might try to point you toward malicious web sites or sites that try to gather your personal and banking information (phishing). Here are several steps you can take to protect yourself against malicious email:

- Restrict scripting (many viruses use scripts to spread themselves to everyone in your address book or to do nasty things to your computer).
- Disable HTML email (malicious scripts can be embedded inside the HTML code that makes a message look pretty).
- Disable the preview pane (some attacks do not even require you to read a message; appearing in the preview pane is sufficient to launch the attack).
- Never open attachments that you were not expecting (verify with the sender that they sent you a file and the type of file).
- ***Never open executable files! Never open executable files! Never open executable files!*** If the file ends in *.exe, it is executable. However, many other types of files are also executable, including Microsoft Word and Excel files with macros. A partial list of executable file types can be found at http://antivirus.about.com/library/blext.htm. Also, ***always*** assume that any file with double or triple extensions – such as "badfile.exe.jpg" or "worsefile.htm.doc.gif" – is malicious and ***do not open them***.
- If the sender is not familiar, or if the subject line is suspicious (or has extraneous characters in it), delete the message unread. If the message

truly was from someone that mattered to you, you can simply ask him or her to resend it.

- Configure your anti-virus software to monitor email and email attachments.

To disable scripting in your email program, search within your help function for "disable scripting" or similar language. For Microsoft Outlook, go to the Tools | Macro | Security menu. On the Security Level tab, enable "High" security, and then click "OK". For Outlook Express, go to the Tools |Options menu. Select the Security tab, and enable the "Restricted sites zone". Also check the boxes "Warn me when other applications try to send email as me" and "Do not allow attachments to be saved or opened that could potentially be a virus". Click "OK" to exit. For other email programs, refer to the help files or to your documentation.

You must decide if it is worth additional security to disable HTML format for email messages. The advantage is that it protects you from embedded scripts within the HTML code of the message; the disadvantage is that you do not see the pretty format originally intended by the sender. Unfortunately, with some email programs it is difficult if not impossible to disable HTML format for incoming messages (Microsoft Outlook). In this case, you need to disable scripting in your browser (Internet Explorer). To disable HTML format for email messages in Outlook Express, go to the Tools | Options menu, and click on the "Read" tab. Check the "Read all messages in plain text" box, and click "OK".

To set your security level in Internet Explorer, go to the Tools | Internet Options menu, and choose the Security tab. Click on the Internet Zone icon, then click on the "Default Level" box. The security settings should be at least "Medium", if not "High". (If you set the level to "High" and find that this level does not meet your needs, then return to this menu and change the setting to "Medium".) Then click "OK" to exit.

Install a personal firewall

Many companies have firewalls protecting the computers on the local network from the outside world. However, this is not always sufficient to ensure that your system is protected. In addition, your laptop and home machine are completely unprotected because they are outside the corporate security perimeter. One tool for protecting your individual machine is a personal firewall. The purpose of a firewall is to protect you from unwanted and/or unauthorized external connections to your machine, as well as to ensure that your machine does not connect to the outside world without your permission (say, if you've been infected by a virus, or if you've installed software that wants

to talk to a particular server on the Internet). The good news is that very competent personal firewall software can be obtained for no or little cost. The bad news is that it may take some "tweaking" to get the firewall software to coexist harmoniously with all the other software on your system. In the end, however, it is usually worth doing so as to have another layer of protection. To learn more about the available software and nuances involved in using this type of protection, do an Internet search on the topic "personal firewall".

Use the proper user

Most of us are familiar with the concept of system "users"; that is, identities with which we log onto our computer or network and use to do our daily computing. As most of us also know, some users are more "powerful" than others in that they have the ability to do more things in a system than less-powerful users. A good example is the "Administrator", which has the ability to do anything on a system – from installing and removing software, to creating and removing other users.

One principle of computer security is that we should never do our daily computing as the administrator. Should someone guess our administrator password or obtain access to our machine while we are logged on as the administrator, they can do anything to the machine – including removing other users and changing the administrator password! It is better to do our daily computing as a "normal" user without the powers of the administrator. That way, if our system is compromised, the intruder can only do the things that the "normal" user is allowed but not everything that is allowed to the administrator. If your current user identity is set up with administrative powers, create a new user with fewer powers and use that ID to do your daily computing (or ask your network administrator to create one for you).

Remove unnecessary file shares

Some virus attacks take advantage of a very old vulnerability in our systems. These attacks target the ability to share your hard drives with other users on your network. If you do not need to share the information stored on your local hard drives, disable file sharing so you do not become a victim of malicious software that uses these "file shares" to propagate itself to

To eliminate file shares on your system, double click on the "My Computer" icon to open it. Highlight your "C" drive, then right click and select "Properties". Select the "Sharing" tab, and click on the button for "Do not share this folder", then click "OK" to exit. Repeat this for every local drive on your system (generally your C and D drives). In some cases, this may not work if your system administrator has disabled this function.

other systems or to compromise sensitive information.

Install security patches

As operating system and application software vulnerabilities become known, most vendors immediately start work on a "patch" or a "hotfix" to correct or address the vulnerability. Microsoft issues patches once a month, on "Patch Tuesday", but they also issue hotfixes and upgrades on a periodic basis. If your system administrator is not downloading and applying these patches for you, you must do it yourself. (Surveys have repeatedly found that many system administrators simply do not do this for their servers or their network users.) This will require that your user identity have "super user" or "administrator" privileges on your local machine. Keep in mind that "patches" and "hotfixes" are different from "upgrades" or "service packs" – patches and hotfixes generally address a specific security problem, while upgrades and service packs can also include enhancements unrelated to security issues.

The first place to go for patches or hotfixes is your operating system or application vendor web site.

- For Microsoft operating systems (including Internet Explorer), begin at the Protect Your Computer page at http://www.microsoft.com/athome/security/computer/default.mspx. This page is a good resource for security issues and steps you can take to update and protect your computer, including turning on both the firewall included with Windows XP and the Automatic Update software.
- For Microsoft Office updates, go to http://office.microsoft.com/productupdates/.
- For all other software, contact your vendor.

Scrub your web site of unnecessary information

Today's fastest-growing crime is identity theft. This is where someone uses your private information to impersonate you and obtain goods and services (including loans and credit cards) in your name. Likewise, the bolder thieves now impersonate companies. While your corporate or personal web site is only one of many sources of information that identity thieves may find useful, you can do your part to prevent identity theft by ensuring that your web site does not contain information that could be useful to these crooks. Information such as Social Security Numbers, account numbers, banking information, wiring instructions, credit references, and the like are particularly useful to identity thieves.

Also, if your department has its own web site, you and your colleagues should make it your home page. That way, someone looks at the page every single day to ensure that it has not been defaced, hacked, or hijacked – common (and embarrassing) occurrences in the Internet world.

Ask yourselves the following questions when examining your web site:

- Is there too much personal information on the site?
- Is there any proprietary information on the site?
- Are there account numbers, banking information, home phone numbers, or other information that should not be publicly available?
- How could someone use the information on the site to do evil? (To catch a crook, one sometimes has to think like a crook.)

Log out of web sites when finished

When you are visiting a web site that requires you to log in (for instance, your bank's site or your ISP's email delivery site), know that your browser will generally store your login and password in your browser's temporary memory. If you then leave the web site to go to another site, the login and password are not automatically erased. Therefore, if you leave your desk immediately thereafter, someone else can press the "Back" button on your browser to get into the secure site (as you). In addition, malicious web sites may read the information about the last site visited from your browser cache, including any login names and passwords used. You should always log out of any secure site you have visited before visiting any other sites. Better yet, log out and then completely close the browser whenever you leave a secure site.

Be aware of social engineering

The World War II exhortation "the walls have ears" is particularly applicable in the today's business environment. Train your staff to refrain from discussing business in public places (or anywhere it is not appropriate), particularly when the discussion involves account numbers, credit card information, personnel matters, and personally identifiable information. Likewise, train your employees to be suspicious of people or web sites that ask for such information – particularly if they are outside your organization or do not need to know that specific information. While this is just common sense to be applied to every situation, it is particularly true when discussing computer issues such as access to bank sites, system set up and capabilities, collection information, vendors, and so forth. **Also, remember that everything discussed or**

Tinucci's Tips
Secure Your Desktop
April 2007

displayed over the Internet is publicized to the entire world – whether you are aware of it or not!

Summary

As you may have noticed from this list of security measures, better security often costs little or nothing. In most cases, computer and user security can be vastly improved by applying common sense and awareness to daily computing tasks. By implementing as many of these measures as you can, you are doing your part to support the security of your organization and the integrity of your data.

About Joseph D. Tinucci

Joseph D. Tinucci is the Assistant Director of Asset Management for the University of Colorado Treasurer's Office. He can be reached by email at joe.tinucci@cusys.edu.

Selected resources for learning more about safe computing habits:

- CERT® Coordination Center: http://www.cert.org/tech_tips/home_networks.html
- Microsoft Security & Privacy Home: http://www.microsoft.com/security/
- Federal Trade Commission Information Security site: http://www.ftc.gov/bcp/conline/edcams/infosecurity/
- Stay Safe Online: http://www.staysafeonline.info/
- For virus information, see the sites of the various anti-virus software vendors (Symantec, McAfee, etc.)
- Your organization's IT unit (visit their home page)