




The Games Hackers Play

*And How You Can Improve Your Chances of Keeping Your
Computer and Your Information Safe*

Anthony Scaturro


Princeton University
IT Security Officer

October 15, 2008



Why be concerned? Personal information on your computer could be exposed or tampered with ...

- ◆ Many personal computers are used for preparing income tax returns, online banking, shopping, etc.
 - Such information could be used for “identity theft” purposes, e.g., your social security number, birth date, information about family members, work, income sources, etc.
- ◆ Your privacy could be violated.
 - Web sites visited, stored passwords (even encrypted), personal e-mail.
- ◆ Someone could destroy or tamper with the information on your system.
- ◆ Someone could use your personal information to make a friend or colleague trust virus-laden e-mail messages.



... or your computer could be used to launch an attack on other systems

- ◆ Even if you are virtually unknown and your computer holds no information you care about, your computer is still valuable to a hacker.
- ◆ Automated hacker programs are continually probing the Internet looking for any systems with weaknesses.
 - Logs showed that a Princeton system was probed hundreds of times within one minute of being built and placed on the network!
- ◆ Once an intruder exploits a weakness, mechanisms are available to give him or her administrative privileges to your system which allows malicious programs to be installed.
- ◆ From there an attack can be launched against other systems.

In either case, the techniques used to attack your system are based on the same principles that have been around for years. Knowing these “games the hackers play” can help you reduce your risk now and in the future.



Game #1 – Guess that password!

- ◆ Once an intruder uncovers a valid ID and password, he or she can:
 - Set up a remote connection to your computer,
 - Deposit new programs and files, view or alter existing programs and files, and
 - Execute the new or updated programs.
- ◆ Programs can be downloaded from the Internet that anyone can run to:
 - test for blank, trivial and default passwords, and/or
 - break dictionary-based, short and guessable passwords quickly.
- ◆ Defensive measures:
 - Never leave a password blank or set to its default value,
 - Use passwords that are difficult to guess,
 - Avoid sharing your password or writing your password down.
 - Vary your passwords from one site to another. Even old passwords could tip off new ones.
 - Change your password regularly.



What makes a password difficult to guess?

- ◆ Passwords should be at least 8 characters long.
- ◆ They should contain at least one character from each of the following four character groups:
 - Lower case alphabetic (a – z),
 - Upper case alphabetic (A – Z),
 - Numbers (0 - 9), and
 - Symbols (@ # ^ & + = , > < / ? | \ : ; ").
- ◆ At least one number or symbol should be embedded within the password, not just added to the beginning or end of a word.
- ◆ Do not take a dictionary word or common name and merely substitute numbers and symbols for similar looking alphabetic characters (e.g., “p@ssw0rd”).



How will I ever be able to remember a strong password?

- ◆ Take a phrase that means something to you and relate each word of the phrase to a corresponding letter, number or symbol.
- ◆ For example, the phrase “I am one happy camper at Princeton University” could become the password “Im1Hc@PU”.
- ◆ **IMPORTANT!!!** – Now that I’ve shared “Im1Hc@PU” as a good password, please don’t use it.
 - Hackers often try passwords given as examples in presentations and documents when trying to break in.



Game #2 – Biological warfare

- ◆ A computer virus is a snippet of program code that is usually:
 - carried by programs, documents, spreadsheets and other forms of program code,
 - delivered via e-mail, Web pages, removable media, etc.
 - programmed to perform a malicious activity,
 - capable of replicating itself into other programs, documents, etc.
- ◆ Computer viruses require your cooperation to be effective, e.g.,
 - Inserting removable media into your system from unknown sources,
 - Opening documents or clicking links in an e-mail from an unknown source,
 - Accessing questionable Web sites and downloading their programs/documents.
- ◆ Defensive measures:
 - Make sure anti-virus software is installed and running on your system. Subscribe to your vendor's automatic update service. Configure it to check for updates daily.
 - Be cautious about the files you are introducing into your computer.
 - Set up your Web browser and Office suite to prompt before executing anything.
 - Don't log into your computer with an administrator-level account for everyday use. A virus is only as powerful as your ID.



Game #3 – Probing for holes


- ◆ Worms are programs that:
 - Look for known vulnerabilities or “holes” in system software,
 - Exploit vulnerabilities that have not been addressed.
 - Once in your system, can create, destroy or alter data, load programs to launch attacks, learn your passwords, capture credit card numbers, etc.

- ◆ Defensive measures:
 - If your software vendors have an automatic software update service, use it.
 - Ensure that security patches provided by your software vendors are applied as soon after release as possible.
 - If your system has a built-in firewall, make sure it is active.
 - Firewalls provide additional protection by selectively blocking remote access to your system.
 - Anti-virus software helps here, too.



Game #4 – The Masquerade Ball

- ◆ Computer names and addresses, and “From:” fields in e-mail messages, etc., can all be modified at their source.
 - Network traffic can be altered to appear to be from a trusted source.
 - E-Mail messages could appear to come from individuals or organizations you know and trust, so that you are more likely to open their attachments or click their links.
- ◆ Defensive measures:
 - Look critically at e-mail messages before opening attachments, i.e., “Does this look like something that Charlie would send?”, “Is this anything my bank would send?”
 - Remember – Reputable organizations do not typically ask for private information in an e-mail.
 - The same for Web sites, especially those to whom you send confidential information. Check the Web address to see if it is what you expected.
 - Anti-virus protection won’t detect e-mail source spoofing but will help reduce the potential of an attachment compromising your system.




Game #5 – “I Spy”

- ◆ Spyware is a technology used to collect data from Web activity.
 - The original purpose of this technology was to learn computer user’s interests and shopping patterns and to provide that information to company marketing departments so they can target their advertising. When used for marketing, this technology is primarily known as Adware.
 - Since then, the same delivery mechanisms have been used to capture other information useful for identity theft.
- ◆ Some free Web accelerator services have Spyware-like capabilities, and can even expose encrypted data.
- ◆ Defensive Measures:
 - Install anti-spyware software on your computer and subscribe to your vendor’s automatic update service. Some anti-virus products have been enhanced with anti-spyware capabilities .
 - Only visit sites of well-known, trusted organizations.
 - Avoid free third-party Web services that promise to speed up your Internet access.



Game #6 – May I have a cookie?

- ◆ Cookies are NOT executable programs.
- ◆ BUT – They hold information, sometimes confidential information.
 - The purpose of a cookie is to keep track of the state of your communication with a specific Web site. Your login information, items in your “shopping cart”, information you entered into a prior page, etc.
- ◆ It is possible for a hacker to obtain a password, bank account or credit card number from a cookie.
- ◆ Defensive measures:
 - Disabling your browser from accepting cookies is the most effective approach, but many sites may no longer work unless you list them as exceptions.
 - Have your browser clear all cookies when you close it.
 - If you send confidential information or just log in to a Web site, close your browser (not just the browser tab) and reopen it before visiting another site.
 - Don't visit questionable sites.



Game #7 – Oh, I'm just browsing

- ◆ Any network devices that passes data can potentially capture and forward it to a malicious individual.
- ◆ Unencrypted data can easily be exposed over wireless, dial-up and Internet connections.
- ◆ Defensive measures:
 - When using a Web browser, make sure that a closed lock is displayed on your browser before sending any confidential data (including passwords) over a wireless network or the Internet. This indicates that the information is being encrypted.
 - If you must send e-mail messages or files containing confidential information over wireless or to/from off-campus, use an encryption product, such as PGP, to prevent anyone else from reading the information as it travels across the network.



Game #8 – Can we share? Part 1


- ◆ Every file and directory on a computer has a list of users and user groups that can access it and the privileges each ID and group has, e.g., read the file, update the file, delete the file, execute the file, etc.
- ◆ Many systems come with a “guest” account that may not require a login, and an “everyone” or “world” group that includes all valid users of the system.
- ◆ If “guest” or “everyone” or “world” is permitted to read files and documents that contain confidential information, the information can easily be exposed.
- ◆ If “guest” or “everyone” or “world” is permitted to update any of your programs, documents or folders, an intruder can easily introduce malicious code into your system or destroy data.
- ◆ Defensive measures:
 - Your system probably comes with a “guest” account. Remove or disable it.
 - Don’t allow files to be shared across the network unless you take an active role in maintaining access privileges.
 - Review access permissions regularly.



Game #8 – Can we share? Part 2

- ◆ Instant messaging and file sharing programs allow others to read and write files on your system.
- ◆ Loosely protected messaging and sharing programs could expose information or allow malicious software to be installed on your system.
- ◆ Defensive measures:
 - Only allow identified users to read and/or write files to your system.
 - Don't grant access privileges to everyone.
 - Restrict file sharing completely or limit it to a single file folder.
 - Don't execute any program dropped off into that folder unless you are sure of the source and you expected to receive the program.
 - Anti-virus software adds additional protection.

Game #9 – Thanks for letting me use your computer!

- 
- ◆ Sometimes, computer information is compromised through unattended, but logged in computers.
 - ◆ Anyone who uses your logged in session is YOU.
 - Anything you have access to is at risk,
 - All activity that is logged has your name on it,
 - E-mail sent from your session will have your name as the sender.
 - ◆ Defensive measures -
 - Use the password-protected screen saver option on your computer.
 - Set it to lock after 20 minutes of inactivity.
 - EVEN BETTER - When you leave your computer, lock it
 - Press the CTRL-ALT-DELETE keys simultaneously
 - Click the “Lock Computer” button.

Game #10 – Communicating with the great beyond

- ◆ The act of deleting a file does not remove its image from hard drives, diskettes, etc.
- ◆ Formatting the disk also leaves an image of the file.
- ◆ There have been “identity thefts” where the information was taken from the hard drives of discarded and donated computers.
- ◆ Defensive measures:
 - When deleting files that contain confidential information, use one of the many commercial products in the marketplace that can completely destroy the content of selected files.
 - “Darik’s Boot and Nuke” is a free program available on the Internet that can completely erase your hard drive before you discard or donate it.