

GEORGETOWN UNIVERSITY
University Information Security Office



DATE: 12/4/2007
TO: Georgetown University
FROM: David C. Smith, University Information Security Officer
SUBJECT: Securing your Georgetown Computer

As you may know, attacks against networks and computer systems have risen dramatically each year. What you may not know is that there are malicious groups that are dedicated to bypassing computer security and exploiting your workstation for financial gains. These financial gains include identity theft, misuse of confidential information, and fraud. As a result, it has become very difficult to protect workstations and laptops from attacks and still maintain an open and usable environment.

It can not be stressed enough; your workstation or laptop is a target for hackers, viruses, and malicious software. These tips will help, but will not completely remove the risks associated with accessing the Internet on today's operating systems. In response to this new level of risk, we are moving to a world where you may no longer store sensitive information on non-Georgetown computers and should never use public or poorly maintain systems to access Georgetown's information systems.

1. Confidential information and Electronic Protected Information (ePI).

Confidential information is defined as information that if disclosed, could cause harm to our organization. Confidential information includes salaries, performance reviews, financial information and information determined to be private such as research or personal information. ePI is a subset of confidential information that is explicitly protected by law, such as patient data, social security numbers, credit cards, and student records. We're asking folks to treat ePI as they would a precious jewel or pure gold.

To minimize the risk of confidential or ePI exposure, never store this information in your email inbox, on your workstation, or on a laptop or desktop machine you've taken home. Review how you use ePI and determine if you may already have stored ePI on your workstation or network shares - if you do, work with your technical staff to remove the data or store it in a more secure location. Ask your technical staff to use a "secure erase" utility rather than simply deleting files that contain ePI on your machine. Minimize your use of ePI and do not print or circulate ePI if possible.

2. Always use a strong password, on every account you maintain.

A strong password consists of at least eight characters (and the more characters, the stronger the password) that are a combination of letters, numbers and symbols (@, #, \$, %, etc.) if allowed. Passwords are typically case-sensitive, so a strong password contains letters in both uppercase and lowercase. Strong passwords also do not contain words that can be found in a dictionary or facts that can be easily associated with the person using the password, such as birthdays or phone numbers.

3. Don't use that same strong password on other systems, especially your NetID username and password.

Strong passwords can be tough to remember and use, but do not trust every system with the same strong password. It would take just one system failing to protect your information to unravel access to all of your personal and financial information – putting you and Georgetown at risk.

4. Take defensive measures to protect your workstation / laptop.

Turn off the workstation or laptop, or disconnect from the Internet, when you're not working for long periods. Make sure your workstation and laptop are protected from theft using cables and locks. Use special care in public or while traveling. Keep it out of sight. What thieves can't see, they can't steal. When you're not using the device, it should be in a locked area. Remember that thieves are specifically targeting laptops for the information they may contain, so protect your laptop as you would any valuable piece of jewelry.

5. Use your Georgetown computer as a work computer.

Minimize the addition of non-work provided software and be very selective about the toolbars, applications, games, and video software you use. Don't install peer-to-peer software, music sharing, or file sharing software. Don't use your home computer as your Georgetown work computer. Remember your home computer is attacked by the same thieves that attack your computer at work; it's safe to say, that if you're connected to the Internet then your machine is constantly being probed for weaknesses.

6. Practice safe computing.

Use a password protected screen saver to lock your computer while you are away. Make sure you have anti-virus software and that it is active and up to date at all times. Make sure you keep your operating system and applications up to date. Don't open software from unknown sources. Don't click on links from emails or IMs asking for information, instead type in the link of the desired website.

7. Know when to ask for help.

If any of these tips or best practices do not make sense, ask for help! Talk to the technical staff in your organization, they are there to help. You can also contact the Georgetown Information Security Office at security@georgetown.edu and x73031.

Make sure to ask for help with any of the following:

- Disposing of your old computer; never leave a computer out in the "trash" or give your older computer to another person without first ensuring you've "securely erased" the entire hard drive. Remember, deleted files can still be easily recovered, so it's important to use special tools to "wipe" your computer's hard drive before disposal.
- Deleting files that contain ePI to ensure they're really gone from your computer.
- Ensuring that your machine has the latest operating system patches and anti-virus tools installed.

8. Do not assume you are safe.

While the university takes steps to protect information and information systems as threats increase and change, do your part and take on the responsibility to practice safer computing and protect information entrusted to your care.