

Digital Self-Defense for Brandeis University Students (2009-2010)



Information Security @ Brandeis

During your years at Brandeis you are going to be spending a lot of time connected to the Internet as part of your learning and scholarship.

- The Internet is a very hostile place. Viruses, worms, identity theft, phishing, hacking and other similar threats are a daily fact of life. Any unprotected computer is vulnerable to attack and information theft.
- Information security is about protecting the confidentiality, integrity and availability of your information.



Protect Your Confidential Information

It is possible that you may store personal or financial information on your computer or Brandeis network share space. Additionally your computer will likely contain your personal scholarship and research.

- It is very important to limit access to your computers to you and only necessary authorized users.
- Treat passwords like a toothbrush -- pick a good strong one, change it regularly, and never share it!
- Clear private data from your web browsers regularly. Browsers store a cache of cookies, accounts, passwords and a history of sites you visit. Check your browser's help section for how to do this.



Protect Confidential Information in Your Custody

Some information that you may deal with during your time at Brandeis is confidential, sensitive and/or regulated as to how it needs to be protected. Brandeis is required by law to protect certain categories of information about individuals including for example, health records, student records, records about human subjects, and some financial and employment records. The University also considers certain information that is not specific to individuals confidential including, for example, financial records or internal plans.

- While you are at Brandeis you could potentially serve as a teaching assistant who has access to and is responsible for student records, you could participate in research with confidential data, or you could perform administrative work that involves confidential or sensitive information.
- If you have authorized access to confidential information you are required to properly protect it and not store, copy or distribute the information in a way that compromises confidentiality.
- The ability to access confidential information does not imply that you also have the authority to do so.
- **NEVER put confidential information in an open file share or the Public or WWW folders in your Brandeis UNet file space!** Files in your Public UNet folder are open to the campus. Files in your WWW UNet folder are exposed to the Internet (and indexed by Google as soon as they are exposed!)



Protect Your Identity

Identity theft is one of the fastest growing information security threats. Criminals seek to obtain financial account information (credit card numbers, bank account numbers, etc.) and personal information that can be used to create new accounts (SSN's, driver's license numbers, etc.).

- One of the best ways to prevent identity theft is to not store sensitive information on your computer in the first place. You can't lose what you don't have stored.
- Periodically clean out the web browser caches on your computer.
- Never provide account information to a website that you do not completely trust. Look for a lock on the screen and https in the URL indicating the session is encrypted.
- Don't click on links or forms in an email message. Type or paste in the URL instead to make sure that the website you access is what actually the website you think it is.

Digital Self-Defense for Brandeis University Students (2009-2010)



Protect Your Privacy

Privacy is about your control over the disclosure and subsequent use of your personal information.

- You do not necessarily need to provide every piece of information that someone asks for.
- In general never disclose any information that is not absolutely necessary for the transaction.
- If you have any doubts ask about what data is being collected, how it will be used, whether you can opt out, whether you can see your data and correct errors, and how your data will be protected.
- Share with care on social networking sites like Facebook, and limit access to people that you know.



Secure Your Computers and Smart Devices

It is very important to keep all of your computer software up to date and patched to protect your computer. Free, site-licensed security tools are available to all members of the Brandeis community to help do this.

Tools are at software.brandeis.edu, and how to information is at lts.brandeis.edu/techhelp/security.

1. Keep your operating system and all applications updated with the latest security patches.
2. Install anti-virus software and keep the software and signatures updated and current.
3. Enable and use the personal firewall that comes with your operating system.
4. Select a strong password consisting of letters, numbers, special characters and change it periodically.
5. Use open source applications like Firefox for web browsing and Thunderbird or Zimbra for email.
6. Use common sense opening suspicious email messages, attachments, web links or web forms. No legitimate organization will ever ask you for your password or account number in an email message!
7. Backup your important documents. Hardware inevitably fails and can be replaced. Your work can't.
8. Limit physical access to your computer. Never leave a running computer unattended in an unlocked area. Use a password screensaver, log out, or close and lock the door.
9. Create a limited User account for everyday use and use Administrator account only for special tasks.
10. Use secure connections. NEVER enter financial account information, your user ID or your password into a website that you do not trust, or a website whose URL address does not begin with https://...



Respect Intellectual Property

Brandeis is committed to respecting intellectual property rights and complying with laws

- Do not use Brandeis's network to share copyrighted work using peer to peer technologies. It is a violation of Brandeis policy and you may be subject to lawsuits and fines from the copyright holder.
- A federal jury recently ordered a BU graduate student to pay \$675,000 to four music companies for illegally downloading about two dozen songs. Brandeis students have paid \$3,000 pre-settlements.
- LTS monitors bandwidth usage and will shut off any computer using excessive bandwidth.
- Brandeis does deliver complaints and settlement letters from the MPAA and RIAA to offenders.



Don't Tolerate Online Harassment

Online harassment can be disconcerting, and can make it difficult to concentrate on school.

- If you ever encounter online harassment you can report it to security@brandeis.edu.
- Harassers can often be identified, blocked and if necessary reported to Public Safety.
- If you feel threatened in any way report it immediately to Brandeis Public Safety at [6-3333](tel:6-3333).



Additional Questions?

- Brandeis Library and Technology Services (LTS) Website: lts.brandeis.edu
- LTS Help Desk: call [6-HELP](tel:6-HELP) (6-4357) –or– walk-in help is available on level one in Goldfarb Library
- Brandeis LTS Information Security: security@brandeis.edu –or– lts.brandeis.edu/techhelp/security