

THE DARTMOUTH INFORMATION SECURITY COMMITTEE

The Dartmouth Information Security Committee (DISC) meets monthly to assess vulnerabilities of information security, and to develop and revise information security policy. All divisions of the College are represented on DISC, which is chaired by Dartmouth's Chief Information Security Officer.

www.dartmouth.edu/comp/security/resources-security/disc

INSTITUTE FOR SECURITY, TECHNOLOGY, AND SOCIETY

The Institute for Security, Technology, and Society (ISTS) is dedicated to pursuing research and education to advance information security and privacy throughout society.

www.ists.dartmouth.edu

THE DARTMOUTH CYBER SECURITY INITIATIVE

The Dartmouth Cyber Security Initiative (CSI) is an ongoing collaboration between faculty, students, and staff with Computing Services, the Department of Computer Science, Thayer School of Engineering, and the Institute for Security, Technology, and Society (ISTS).

Our goals include:

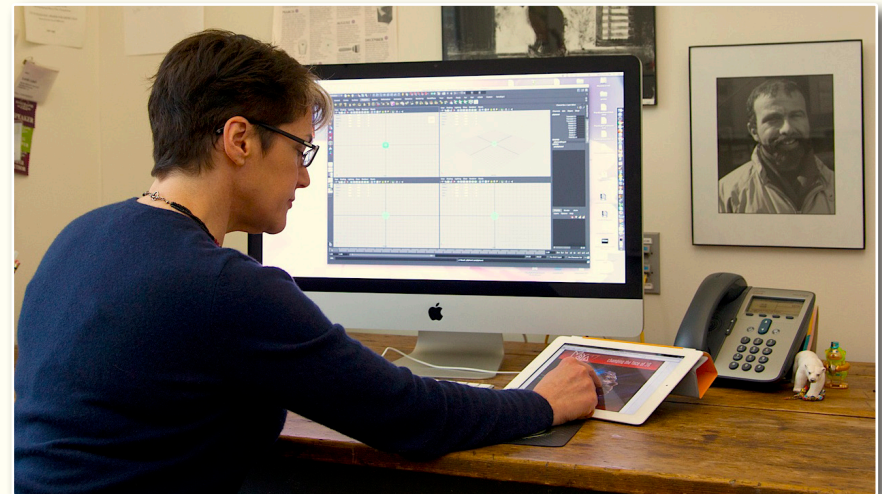
- Assessing vulnerabilities in infrastructure, desktops, and applications
- Making recommendations for improving the security of Dartmouth's assets
- Developing applications and procedures to improve the operational security of the College's information systems
- Training people to use more secure ways to access and transfer data, and to recognize security holes

www.dartmouth.edu/comp/security/csi

Photo courtesy of Joseph Mehling '69

Dartmouth

Faculty Information Security Guide



Your information is vitally important to your teaching, research, and scholarship.

If unprotected, your computer is a gateway to thieves and hackers, who can access and modify research data, students' grades, and other confidential items. Unauthorized access to information could also expose the College to financial and compliance risks. A few simple techniques can help protect your information.

THE DARTMOUTH INFORMATION SECURITY COMMITTEE
INSTITUTE FOR SECURITY, TECHNOLOGY, AND SOCIETY
THE DARTMOUTH CYBER SECURITY INITIATIVE

WHAT YOU CAN DO

Encryption If it's confidential and portable, encrypt it. Laptops, netbooks, smartphones, thumb drives, and CDs containing private information can be encrypted. Encryption is fast, easy, inexpensive, and in some cases, already built in to the device (e.g., the iPhone and iPad). Examples of confidential information include research data, students' grades, evaluations of graduate students, and email. If you are sending confidential information by email, it's a good idea to encrypt it, especially if the destination is outside Dartmouth. Internet email is not secure, and encryption is the only way to guarantee confidentiality.

Computer Systems Turn off your computer when you are not using it, or configure a screen saver time-out so the computer locks after a period of inactivity. For highly sensitive information, we suggest 15 minutes. This feature can be easily disabled when you are using your computer for presentations.

Passwords Choose a phrase that is easy for you to remember, but that has no meaning to others. Passwords must be exactly 8 characters, and must include a special character (, - _ ! @ # \$ % ^ & *) in any position other than the last two positions. Use two unrelated words, e.g., shoe\$ice. Note the joining of two unrelated words (shoe and ice) with a special character (\$)

The number of laptop thefts at Dartmouth has steadily increased since 2008, and laptop and smartphone thefts at airports are also on the rise.

in the middle, and not in the last two positions of the phrase. Remember to use passcodes on mobile devices like phones and iPads.

Paper Documents Lock confidential paperwork in desk drawers or filing cabinets. Never leave it on desks or meeting rooms when you are not present. Shred this material when you no longer need it, and discard it in trash bins.

Web Use Be wary of public computers in airport kiosks, libraries, etc. Viruses and key loggers can steal your information. On the Web, look for a lock icon showing a secure connection. If you receive a certificate warning, consider abandoning the connection. Think before you click: phishing attacks are designed to trick you into providing personal information.

A server in a Dartmouth lab was hijacked and used for over 200,000 downloads of botnet malware within 24 hours.

HOW WE CAN HELP

The Dartmouth Information Security Committee; the Institute for Security, Technology, and Society; and the Dartmouth Cyber Security Initiative offer the following solutions:

- Whole-disk encryption
- Email encryption (service planned for 2012)
- iPad and iPhone security
- Identity Finder: Computing Services can scan computers to locate personally identifiable information (e.g., SSNs) that should be protected or deleted
- IT consultants to assist with password selection and screen-saver timeout settings

Dartmouth has experienced several breaches of security in which hackers obtained userIDs and passwords of Dartmouth employees and posted this information on the Internet.

ADDITIONAL SUPPORT

Computing Services For technical questions and support, email us at help@dartmouth.edu.

Records Management For advice about the proper disposal of paper documents, contact dartmouth.records.management@dartmouth.edu.

For all other questions about online security, contact:

Steve Nyman

Chief Information Security Officer
steven.m.nyman@dartmouth.edu

A professor at The University of North Carolina had confidential breast cancer research data on thousands of patients. The computer did not have the appropriate security patches installed. A hacker compromised the information by breaking into the computer at the university.