Information security starts with you.

You can help keep your computer and data safe by following some simple steps and staying aware of threats to your data. This guide of secure computing best practices is intended for use by all members of the Colby community.

Colby faculty, staff and students are encouraged to review all current policies and procedures for computing at the College, which can be found online at **http://www.colby.edu/info.tech/policies**, including:

- Colby Web Policy
- E-mail Policy
- Discussion Forum Policy
- Information and Data Security Policy
- Code of Ethics for Information Technology

Faculty and staff should be aware that some of the practices in this guide are policy requirements and should visit the ITS policy page and/or consult with their department heads.

If you have questions about these guidelines or any other aspect of information or computer security, do not hesitate to contact the appropriate ITS support desk.

Colby

Colby College Information Technology Services
105 Lovejoy
4201 Mayflower Hill
Waterville Maine 04901-8842

ITS Faculty/Staff Support : support@colby.edu : x4222
Student Computer Services : scshelp@colby.edu : x4224
Online : http://www.colby.edu/its

Colby **Information Technology Services**

Secure Computing

Best Practices

ITS Support Center

Faculty and Staff : support@colby.edu   x4222

Students : scshelp@colby.edu   x4224

Keep your identity, data, and computer safe and secure.

Account and Password Security

Your passwords are the keys to your digital accounts and information. By following some simple guidelines and common sense, you can ensure they are kept secret.

Set strong passwords that meet the following criteria: at least eight characters in length, contain one or more punctuation characters (! , &, etc), do not contain words that can be found in dictionaries, and do not contain part of your name or account/login.

- **Never** share password or account information with anyone—*including Colby ITS*.
- **Never** use a Colby account password with a non-Colby account, like Facebook.
- **Never** send account, password or personal information (credit card, social security numbers) through unencrypted electronic communication (like e-mail or chat).
- **Avoid** writing down passwords. If you must write down a password, do not write the account (login) associated with it.
- **Avoid** having web browsers or other programs 'remember' passwords.

If you suspect your account/password has been compromised, contact ITS and change it immediately.

Workstation and Computer Security

*Require a login and/or password to access all workstations and computer*s, and ensure there are no other unnecessary or unused accounts. Do not allow others to use your computer on a regular basis unless they have their own account.

Set your computer to password-lock automatically or log off when not in use.

Turn off (do not just sleep/hibernate) your computer at night or when you will not be using it for a long period of time.

Never leave your computer unattended in public spaces. Whenever possible, lock doors and windows to prevent unauthorized access or theft.

Internet and Software Security

Regularly check for and download/install all software and operating system updates. Whenever possible, set these to be installed automatically.

Employ anti-virus and anti-spyware software and ensure that it is up-to-date. Have all security software run regular scans and enable auto-protection mechanisms.

Don't fall victim to e-scams, fraud and identity theft. Delete fraudulent (junk) e-mails or any messages from an unknown sender or source. Never click on links within unsolicited e-mails or open programs or documents attached to them. Learn how to recognize fraudulent messages (see the ITS support website for more information on phishing and electronic fraud).

Never click on browser pop-ups. If you are receiving too many or suspect a problem, contact the appropriate ITS support desk.

Data and Information Security

Be organized—keep track of where your information has been and is going to—including CD/DVD's, flash drives, and paper printouts.

Back up important data to at least one other source. Password-protect and/or encrypt data containing sensitive information (tying names to accounts or identification numbers). If your computer is stolen—what will the thief have access to? Will your data remain secure?

Network Security

Activate your operating system firewall (it should be turned on by default) and turn off any services (sharing, discovery, etc) that are not required.

Beware of open (unencrypted) wireless networks—especially those in public spaces. Use encrypted/password-protected wireless networks, such as 'Colby Access,' whenever possible.

Avoid having your computer automatically connect (using profiles) to open wireless networks; don't 'remember' networks.

Do not connect to a network unless you need to. Use a wired (Ethernet) network connection if available. *Turn off* the wireless network port when not in use.

Use the VPN (Virtual Private Network) to securely access Colby on-line resources from off campus.

Colby

ITS Faculty/Staff Support : support@colby.edu : x4222
Student Computer Services : scshelp@colby.edu : x4224
Online : http://www.colby.edu/its