TAKING ACTION

Taking action to personally ensure computer security helps protect everyone from data and identity theft, viruses, hackers, and other abuses. Everyone who uses a computer makes Purdue's computing environment more secure by following these strong recommendations.

PURDUE
UNIVERSITY

www.purdue.edu/securepurdue

ITaP
INFORMATION TECHNOLOGY AT PURDUE

SECURE PURDUE

How to protect computers, data, and personal information

SECURITY & PRIVACY

www.purdue.edu/securepurdue

SECURE PASSWORDS

Create strong passwords

Strong passwords are critical to system security. A strong password is:

> Something other than a word found in the dictionary
> Something other than the name of a person, character, or pet
> Without personal information, such as birthdates and telephone numbers
> Something unrelated to your institution or department name or other identifying information
> At least eight characters
> Both capital and lowercase letters and numbers, as well as punctuation; for example: "AgbdF&04"
> Up to 1,000 times harder to crack than a weak password

Change passwords

Over time, even strong passwords lose security.

> The best practice is to change passwords regularly.
> Use the password-changing frequency recommended by the system administrator.
> Password-changing frequencies are commonly monthly or quarterly.
> Use password-creation techniques to create strong, yet easily remembered, passwords.
> Don't write down passwords. The most easily cracked password system is a password written on a sticky note under the keyboard.

Avoid untrustworthy downloads

Virus writers use downloadable screensavers and other files to infiltrate computer systems. Free CDs may also harbor spyware and viruses.

Scrutinize attachments carefully

Email and instant messaging are major vehicles for viruses. Spammers are very skilled at making virus emails and attachments sound legitimate. Open only expected email attachments sent from known addresses, especially if the file extension of an attachment is .exe, .bat, .vbs, .pif, .scr, .cmd, .hlp, .lnk, or .com.

View email messages individually

Spam emails often contain code that automatically incites more spam or attempts to install viruses and spyware. Avoid this problem by viewing email messages individually, rather than in a previewing pane. To toggle the Preview Pane in Microsoft Outlook, click View»PreviewPane.

Install free antivirus software

Install and use antivirus software, and set it to automatically update daily. Purdue offers McAfee Antivirus for free to students, faculty, and staff, for use both at school and at home. McAfee Antivirus is updated frequently to keep pace with the latest viruses. To download McAfee Antivirus, or the MacOS equivalent, visit *http://www.purdue.edu/securepurdue*.

Ensure antivirus software is running

After starting up a computer, check that an up-to-date antivirus program is enabled. When using McAfee Antivirus for Microsoft Windows, hover the mouse cursor over the shield icon in the task bar to verify McAfee is enabled.

Ignore unsolicited emails

Spammers send emails that pretend to be from legitimate sources to trick you into providing your personal information. This practice is known as "phishing." Never click on links in an email. Phishers can make fake email links that:

> Browse to the legitimate Web site, but sneak in a pop-up window from a phisher's Web site that asks for personal info.
> Browse to a fake Web site that has a nearly identical look and address to the legitimate Web site.
> Cover up the browser address window with an image that makes it appear to be the legitimate Web site.
> Invisibly download a key-logging program that records and reports back every keystroke made on the computer, including entered passwords and credit card numbers.

Secure Internet settings

Change the security settings on your browser to "high," and adjust downward as necessary for your Internet use. The "high" security setting may prevent some Web sites from functioning properly, so use the highest setting that still allows for effective Web browsing.

Back up data

Back up critical data regularly. Keep a copy of important files on removable media, such as CDs, DVDs, or USB thumb drives. Securely store the copies out of sight and under lock and key.

Use firewalls

Install and use firewall security. A firewall is a hardware or software barrier designed to prevent unauthorized network activity. Microsoft's Windows XP Internet Connection Firewall (ICF) comes with Windows XP and should be activated.

Reduce incoming spam

Spam is the common term for unsolicited email and instant messages. Spam is most effectively reduced by keeping email addresses private and by using a properly secured Web browser and email client. For a list of best practices against spam, browse to *http://www.purdue.edu/securepurdue/bestPractices/spam.cfm*. For answers to questions regarding spam at Purdue on Purdue machines, email *itap-security@purdue.edu*.

Get updates and patches for operating systems and software

As new ways to exploit computer software vulnerabilities are discovered, it is critical to system security to regularly patch and update software. For Windows patches and updates, browse to *http://www.windowsupdate.com*.

Use your career account

Each Purdue student and employee has a career account that provides 500 MB of storage on a Web server. To access your career account from within the Purdue network, map a network drive to *\\rosetta.ics.purdue.edu*\<insert your own username>. If you are off campus, map a network drive to *\\offcampus.ics.purdue.edu*\<insert your own username>. To reset your career account password, browse to *http://www.purdue.edu/securepurdue*.

Log off or turn off the computer

When you leave your computer, make sure to lock it (Windows key + L) or log off. If you are leaving for an extended period (a weekend, for example), turn the computer off.

Visit the SecurePurdue Web site

Browse to *http://www.purdue.edu/securepurdue* for the latest in computer security and privacy.