



## Holiday tips for securing your new computer

Computer ownership and use in the United States is growing. If you are one of the fortunate people who may receive a new computer this holiday season, ITaP offers the following tips to keep your new computer in peak operating condition:

1. Apply operating system security and software patches and updates regularly. Windows users can use Microsoft's Windows Update Service. Apple OSX users should install security updates when prompted by "software update." Also apply patches to application software such as word processors, IM clients, and other programs. Most computers come with documentation to teach you how to keep the computer up-to-date.

2. Install and use daily anti-virus software and set your computer to automatically update anti-virus applications daily. Purdue University users have access to McAfee Anti-Virus software for free. You can visit the SecurePurdue page and follow the "Downloads" tab to learn more.

3. Install firewall security software. Microsoft's Windows XP Internet Connection Firewall (ICF) software ships with Windows XP and should be activated.

4. Set the security settings to the highest level on Internet browsers.

5. Use separate adware and spyware removal programs when those services are not included with your anti-virus software.

Protecting yourself and your data is also important:

1. Always use strong passwords and keep them secret. There are many ways to create a strong password; but in general a strong password is a combination of letters, numbers, and symbols. A longer password is usually stronger.

### In this issue

Holiday tips for securing your new computer . . .	1, 2
CISO message . . . . .	1- 3
Spotlight: IRS Warning . . .	3
STEAM-CIRT News . . . . .	3
Online Shopping Tips . . . .	4
Security Product Downloads . . . . .	4
Security Resources . . . . .	4

See Online Shopping tips for securing your new computer Page 2

### FROM the CISO



By Scott Ksander  
Executive Director  
IT Networks & Security

It is fair to say that a whole section of the e-commerce industry is devoted to people like me. Cyberguys.com; thinkgeek.com; and geeks.com (among others) cater to the self-proclaimed "computer geek."

This issue of the SecurePurdue news offers tips on how to protect your personal information when shopping online

for that special gift or product. Protecting your personal information is of growing importance, especially when reports of data breaches from national retailers and organizations seem to occur daily. Following some simple tips for e-commerce can protect you from both fraud and identity theft. Not to leave you without security advice once that new wingding has been purchased, this issue also offers tips on how to secure new computers and mobile devices.

See CISO, Page 2

# Holiday Tips for Securing Your New Computer

(from page 1)

CISO from Page 1

2. Regularly back up files and data to storage media such as CDs, zip disks, DVDs, flash drives, or other media.
3. Never store sensitive personal information such as bank account numbers, usernames and passwords, or your Social Security Number on your computer.

Many of the same protection mechanisms recommended and available on computers can also be used to protect mobile devices such as PDAs and cell phones. PDA's, in particular, should be password protected if that feature is available. The password should block all access to the device until a valid password is enabled. Wire-

Taking steps to secure any new computer gadget that holds your personal data is another important step you can take to protect yourself. Even devices that hold data as innocuous as calendar entries, contacts, and pictures can pose a security risk and reveal information about you if the device is lost or stolen and not protected with security features.

These new gadgets and gizmos can also raise issues in the University environment when introduced to Purdue's network or when used by employees at work. As I have mentioned in the past, new technologies should be tested before they are introduced in the University environment. Testing new technologies in advance ensures that they are compatible with University systems. In addition, employees are reminded that the University's Data Handling Guidelines will apply to University data stored on any personally-owned gadget.

---

## *Be suspicious of any unexpected email requesting personal information*

---

4. Be suspicious of any unexpected email requesting personal information, or of any email attachment, even if it is from someone that you know. Never comply with requests for personal information from an email or phone call unless you initiated the contact (these are often phishing scams trying to steal your personal information).

Never comply with requests for personal information from an email or phone call unless you initiated the contact (these are often phishing scams trying to steal your personal information).

5. Do not keep computers online when not in use. Either shut them off or physically disconnect them from Internet connection.

less access, such as Ethernet, Bluetooth, etc., to the PDA and cell phones should be disabled when not in use to prevent unauthorized wireless access to the device; when used, wireless access should be configured to query the user for confirmation before connecting to wireless networks. In general, for all devices, keep your wireless connection on hidden mode unless you specifically need to be visible to others.

Taking steps to protect the University's data, as well as our own personal information, helps create a more secure computing environment for all of us.

In addition to new hardware technology, don't forget to read and understand the agreements that come with new options and online technologies. While reading these agreements is something very few of us consider doing, there can be considerable risk in these agreements. Consider the following clause from a popular on-line service.

"You (user) retain copyright and any other rights you already hold in Content which you submit, post or display on or through, the services.

**BY SUBMITTING, POSTING, OR DISPLAYING THE CONTENT YOU GIVE (online service) A PERPETUAL, IRREVOCABLE, WORLDWIDE, ROYALTY-FREE & NON-EXCLUSIVE LICENSE TO PREPRODUCE, ADAPT, MODIFY, TRANSLATE, PUBLISH, PUBLICLY PERFORM, PUBLICLY DISPLAY & DISTRIBUTE ANY CONTENT WHICH YOU SUBMIT, POST OR DISPLAY**

See CISO, page 3

## SPOTLIGHT

## IRS Warning

The Internal Revenue Service (IRS) has issued an alert warning taxpayers of new e-mail scams. In a variation on traditional e-mail scams claiming an IRS refund, the new e-mail scam claims to come from the IRS and the Taxpayer Advocate Service (a legitimate IRS program).

Like many scams targeting taxpayers, the newest variation directs the consumer to a link — often a Web site that appears to resemble the IRS Web site — that requests personal and financial information, such as Social Security number and credit card information.

The IRS reminds taxpayers that the IRS does not

send out unsolicited e-mails or ask for detailed personal and financial information via e-mail. Additionally, the IRS never asks people for PIN numbers, passwords, or similar secret access information for their credit card, bank or other financial accounts.

The IRS recommends calling 1-800-829-1040 if a taxpayer has any doubts about whether an e-mail message received from the IRS is authentic.

Taxpayers who receive an unsolicited e-mail claiming to be from the IRS should never click on any links in the message, open any attachments, or provide any personal or financial information to the sender.

For more information on IRS-related scams, visit the official IRS website at <http://www.irs.gov/>, and execute a search for “scams” or “phishing.”

CISO from Page 2

**THROUGH THE SERVICES...** You agree that this license **INCLUDES A RIGHT FOR [online services] TO MAKE SUCH CONTENT AVAILABLE TO OTHER COMPANIES, ORGANIZATIONS OR INDIVIDUALS WITH WHOM [online service] HAS RELATIONSHIPS** for the provision of syndicated services, and to use such Content in connection with the provision of those services.” (emphasis added)

In short, if you submit University Data to these services, you have just given the online service license to do just about anything with that data. I don't mean to suggest that on-line services for sharing, backup, collaboration, or whatever are problematic. That is absolutely not true. They can be very valuable and productive tools. The issue is not with the tool but the data entrusted to it. University Data in your care needs to be carefully protected regardless of the technologies in use.

As the year winds to a close, I thank you for your work in furthering the SecurePurdue effort. Information security is a partnership that requires many people doing their part to move toward a common goal. At Purdue, this partnership is improving every day.

Thanks for reading; and as always, be careful out there.



## STEAM-CIRT NEWS

STEAM-CIRT is a security team and IT incident response team organized under the ITNS group within ITaP.

For more information about STEAM-CIRT and for security updates throughout the month, visit the STEAM-CIRT Web page at:

<http://www.purdue.edu/securepurdue/steam/>

## Top 10 Purdue email viruses

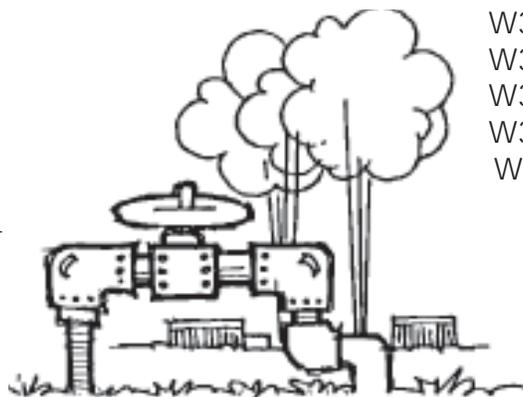
The following list is a 30-day snapshot of the most active email viruses on the Purdue campus.

The maximum occurrences found in one day are listed with the names of each major virus.

(30-day snapshot as of November 27)

**Viruses**                      **Max. Occurrences**

W32/MyDoom-O	417	129
W32/Mytob-E	192	16
W32/Netsky-P	122	19
W32/Sality-AA	147	3
W32/Mytob-GH	60	13



# HOLIDAYS

## Online Shopping Tips

The holiday shopping season is upon us. For many of us, that means that we will be shopping online in order to avoid crowded malls and long lines. Online shopping is growing in popularity. In 2004, the Monday after Thanksgiving (now known as Black Monday) replaced "Black Friday" (the Friday after Thanksgiving Day) as the highest volume e-commerce shopping day of the year. Total purchases were in excess of 5.2 million. According to the US Census Bureau, E-commerce sales for the second quarter of 2007 were \$33.6 billion, which was an increase of 6.4% from the first quarter of 2007.

Now is the time to think about precautions you can take to protect yourself, your personal information, and your purchases during this busy shopping season. IT Networks and Security offers the following tips for online shopping.

-Learn about product. It is important to know what you are buying, so watch out for words like "new," "re-furbished," and "open carton." Is the product sold by a number of sellers or has it been featured in standard news outlets? (if so, it tends to lend credibility to the product)?

Is the price that the online retailer is offering similar to the price offered by other retailers?

If a product or a price looks too good to be true, that could indicate a counterfeit product.

Learn about the seller. Has the online retailer been in business for a long time? Does the retailer have an actual physical location and are there a number of avenues (phone, email, snail mail) for contacting the seller? Consider checking the Better Business Bureau to learn if there have been any complaints against the seller.

-Understand retailer's refund policies. This is a key component of online shopping. Be sure to buy from retailers who have a clearly stated return and refund policy. Keep records of your transaction to ensure a smooth return or refund.

-Be sure that the retailer utilizes a secure checkout method. To make sure that the site is secure, look for the padlock icon on your browser's status bar or a URL that begins with "https:." Do not buy from a retailer that does not have a secure checkout method. In addition, do not buy from a retailer who asks you to email your personal information (like credit card number) to them.

-Do not give your bank account information to online retailers for automatic debit.

-Do not give your bank account information to online retailers for automatic debit. While automatic debit for some services, such as regular utility service payments can be relatively safe; allowing online retailers access

to your bank account and its contents can be risky. Do not do business with retailers who ask for this information.

-Consider using a specific credit card for only online shopping. That way, you can easily monitor your credit card statements for online purchases and fraudulent charges will be more apparent to you upon review. You can also check with your credit card company to see if it offers one-time use credit card numbers. These types of services of services never actually share your real credit card number with an online retailer, but instead creates a one-time-use credit card number in its place.

Online shopping is big business. Taking steps to protect your personal information and purchases just makes good sense.

Here are other online shopping tips from Matei and Internet research:

- Scour the Internet for discount and free shipping codes before purchasing. CheapUncle.com will search for coupons, deals and pricing of more than 14,000 online retailers.

- Read product reviews at Peinions.com or Amazon.com before purchasing online. Especially check out review sites such as Cnet.com or ConsumerReports.org before purchasing electronic equipment or an appliance.

- Read the bad reviews too. If only five reviews of 100 were bad, those five may be because of a specific detail important to you.

- If this site is new to you, call the seller's phone number, if there is one, or email the business. If neither is functional, shop elsewhere.

- Use a credit card for purchases so you can contest the charge if the item is not received.

## SECURITY RESOURCES

Use the following resources for online holiday shopping for new technology, geeky gadgets or gift ideas for the technophile in your life.

[www.apple.com](http://www.apple.com)  
[www.bhphotovideo.com](http://www.bhphotovideo.com)  
[www.smarthome.com](http://www.smarthome.com)  
[www.thinkgeek.com](http://www.thinkgeek.com)  
<http://www.smartlassy.com/>  
<http://www.techiediva.com/weblog/>  
<http://www.cnet.com/>  
<http://gizmodo.com/>  
<http://www.newegg.com/>  
<http://www.monoprice.com/>