

## PREVENTING ID THEFT & FRAUD

- Do an annual credit check:  
<http://www.annualcreditreport.com/>
- Watch for unauthorized charges.
- Verify that you are receiving all your credit card, bank, and other financial statements every month.
- Don't send personal, credit card, or other financial information over email or IM.
- Report fraudulent activities to:
  - the Internet Crime Complaint Center (IC3): <http://www.ic3.gov>
  - the Federal Trade Commission (FTC): <http://onguardonline.gov>



## Using IT Resources at UH: Securing Your Computer and Protecting Your Information

Use of all University of Hawaii Information Technology Resources are governed by **UH Executive Policy: E2.210 -- Use and Management of Information Technology Resources**. Continued use of your UH Username and University Information Technology Resources indicates your acceptance of and agreement to E2.210. The complete policy can be found on-line at: <http://www.hawaii.edu/infotech/policies/itpolicy.html>

A brief summary of Section III: "Principles of Responsible Use" are provided for your convenience. These examples are intended to illustrate the range of unacceptable actions rather than to exhaustively elaborate all specific behaviors that may violate this Policy.

Users of University information technology resources should engage in responsible computing and network practices. All users must respect property, security mechanisms, rights to privacy and freedom from intimidation, harassment and annoyance in accordance with all University policies and procedures.

- Users must adamantly protect their personal passwords
- Users must **respect the privacy** of others' passwords, information and communication, and may not attempt to use University resources to gain unauthorized access to any site or network or to maliciously compromise the performance of internal or external systems or networks
- **No individual may falsely represent themselves or "spoof"** another physical network connection
- Users must **observe all laws** relating to copyright, trademark, export and intellectual property rights (Note: copying or sharing of copyrighted audio or video files for purposes other than "fair use" are illegal)
- Users must ensure that their electronic communications **do not infringe the rights of others** and are conducted in accord with the same standards of behavior that apply in other forms of communication
- University resources are intended to be used for **institutional purposes** and may not be used for private gain
- Users may not **engage in activities which compromise institutional systems** or network performance for others

## ADDITIONAL RESOURCES

<http://www.hawaii.edu/help>  
<http://www.housing.hawaii.edu/resources/resnet.cfm>

<http://www.ic3.gov>  
<http://onguardonline.gov>  
<http://www.microsoft.com/athome/security>

<http://computer.howstuffworks.com/firewall.htm>  
<http://www.antiphishing.org>  
<http://www.consumer.gov/idtheft>  
<http://www.ftc.gov/bcp/online/edcams/infosecurity/coninfo.html>  
<http://windowsupdate.microsoft.com>

### Information for this document compiled from:

<http://www.hawaii.edu/infotech/policies/itpolicy.html>  
<http://onguardonline.gov>  
<http://www.cert.org/homeusers/HomeComputerSecurity/>  
<http://www.us-cert.gov/>

## SECURING YOUR COMPUTER:

- **System updates.** Regularly download and install operating system and application security patches from your software vendors. (Microsoft users, go to: <http://windowsupdate.microsoft.com> and click on "Scan for updates". Visit <http://www.microsoft.com/athome/security/update> for more details. Apple users, click on "Software Update" in "System Preferences")
- Use **anti-virus software** & UPDATE VIRUS DEFINITION FILES REGULARLY! Scan all files and email attachments before opening them. UH faculty, staff and students can download antivirus software from [www.hawaii.edu/antivirus/](http://www.hawaii.edu/antivirus/)
- Make regular **backups** of critical data (and test your backups to ensure they are readable). Take advantage of your UH username and backup your critical documents to your UNIX account.
- Use **strong passwords.** Do not leave passwords blank or use simple passwords. Change default passwords. For more information visit: [http://www.hawaii.edu/help/security/pdf/Password\\_Guidelines.pdf](http://www.hawaii.edu/help/security/pdf/Password_Guidelines.pdf) and [http://www.webopedia.com/TERM/S/strong\\_password.html](http://www.webopedia.com/TERM/S/strong_password.html)
- Use a properly configured **firewall** as a gatekeeper between your computer and the Internet. The latest versions of Windows and OSX have built-in firewalls. Warning: a misconfigured firewall can provide a false sense of security and will allow viruses, worms, and hackers into your computer. For more general information about firewalls, visit:  
<http://www.cert.org/homeusers/HomeComputerSecurity> and  
<http://computer.howstuffworks.com/firewall.htm>
- Do **not open email attachments** from strangers AND be suspicious of any unexpected or unusual email from people you do know. Disable "previews", automatic viewing and downloading of attachments/files.
- **Test your systems** for vulnerabilities. Use web-based vulnerability assessment tools such as: <http://www.symantec.com/securitycheck> or <http://www.grc.com> (click on "ShieldsUp")
- **Do not run unnecessary services** such as web servers (IIS), databases (MS SQL), Telnet, FTP, IRC, etc.
- **Download software from reputable sources.**
- Use **anti-spyware software, update the software frequently & scan** your computer regularly for spyware.



- Visit only **legitimate websites.** Malicious websites can download and install malware on your computer turning it into a "spam generator" or a "zombie" which can be used to attack other machines.
- If you use P2P filesharing software, know & monitor which directories and files are being shared.

## PROTECTING YOUR INFORMATION:

- **Do not reply** to unsolicited (spam) email.
- Use free web-based email addresses (Yahoo, Hotmail, etc.) when subscribing to email lists (to minimize the amount of **spam email** you might receive on your primary email account.)
- **Do not give out personal information** (address, SSN, passwords, etc.) in response to unsolicited requests.
- **Protect your passwords.**
- **Encrypt or password-protect files** that contain personal, confidential information such as tax return files, on-line banking information, etc. Use the encryption capabilities of your operating system or use other third party products such as PGP (<http://www.pgp.com/downloads/desktoptrial.php>) or TrueCrypt (<http://www.truecrypt.org>)
- **Be suspicious** of email from what appears to be a legitimate organization (such as Citibank, eBay, PayPal, FirstUSA, etc.) asking you to click on a link to update your personal information such as name, address, SSN, bank accounts, and credit card numbers. These are fraud schemes known as "phishing". Personal information gathered will be used/sold to commit fraudulent financial activities. Do NOT update your personal information by clicking on the link. If it seems legitimate, call the organization to verify the request and always type in the URL yourself. For more information on "phishing", visit:

<http://onguardonline.gov/phishing.html>

<http://www.antiphishing.org>



## On-line Transactions

- Do not use public computers or wireless networks for personal/confidential transactions.
- Use only one credit card (with a low limit) for ALL online purchases.
- For all EFT (Electronic Funds Transfers) transactions, use only one checking account.
- Don't use your SSN if at all possible.

Don't let your  
money walk away!

