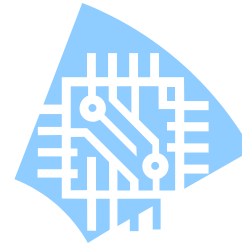


## PREVENTING ID THEFT & FRAUD

- Do an annual credit check.
- Watch for unauthorized charges.
- Report fraudulent activities at: [www.ifccfbi.org](http://www.ifccfbi.org)
- Don't send credit card information over email or IM.



## Using IT Resources at UH:

### Securing Your Computer and Protecting Your Information

### A safety guide for your computer and you.

Presented to you by Information Technology Services and ResNet.

## ADDITIONAL RESOURCES

[www.hawaii.edu/help](http://www.hawaii.edu/help)  
[www.housing.hawaii.edu/mResources/ResNet.cfm](http://www.housing.hawaii.edu/mResources/ResNet.cfm)

<http://computer.howstuffworks.com/firewall.htm>  
<http://www.antiphishing.org/>  
<http://www.ftc.gov/bcp/conline/edcams/infosecurity/coninfo.html>  
<http://v4.windowsupdate.microsoft.com/en/default.asp>

### Information for this document compiled from

[www.hawaii.edu/infotech/policies/itpolicy.html](http://www.hawaii.edu/infotech/policies/itpolicy.html)  
[www.nipc.gov/publications/nipcpub/computertips.htm](http://www.nipc.gov/publications/nipcpub/computertips.htm)  
[www.hawaiianharddrive.com/articleview.cfm?articleid=175](http://www.hawaiianharddrive.com/articleview.cfm?articleid=175)  
[www.cert.org/homeusers/HomeComputerSecurity/](http://www.cert.org/homeusers/HomeComputerSecurity/)  
[www.isalliance.org/resources/](http://www.isalliance.org/resources/)

## POLICY:



[www.hawaii.edu/infotech/policies/itpolicy.html](http://www.hawaii.edu/infotech/policies/itpolicy.html)

Complete text of this policy

[www.housing.hawaii.edu/mResources/resnet.cfm](http://www.housing.hawaii.edu/mResources/resnet.cfm)

Complete text of the ResNet policy

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.

A brief summary of “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 the principle.

Students are asked to practice responsible computing, to be responsible users of technology services. Students should respect property, security mechanisms, rights to privacy and freedom from intimidation, harassment and annoyance.

### Respect of Property

- Users must **observe all laws** relating to copyright, trademark, export and intellectual property rights (Note: copying or sharing of copyrighted audio or video files are illegal)
- University resources are intended to be used for **institutional purposes** and may not be used for private gain

### Respect of Security Mechanisms

- Users must adamantly **protect their personal passwords**
- Users may not **engage in activities which compromise institutional systems** or network performance for others



### Rights to Privacy

- 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

## Freedom from intimidation, harassment and annoyance

- **No individual may falsely represent themselves or "spoof"** another physical network connection
- 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

## SECURING YOUR COMPUTER:

- **System updates.** Regularly download and install operating system and application security patches from your software vendors. (Microsoft users can go to: <http://windowsupdate.microsoft.com> and click on "Scan for updates". Apple users can 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.nipc.gov/publications/nipcpub/password.htm>
- Current "best practices" state that you should use a properly configured **firewall** as a gatekeeper between your computer and the Internet. (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>
- **Turn off computers** or disconnect them from the network when done using them (or if leaving them unattended for long periods of time).
- 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: [www.symantec.com/securitycheck](http://www.symantec.com/securitycheck) or [www.grc.com](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.**
- **Scan** your computer regularly for "spyware" and use spyware removal tools.
- 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.

## 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** your files that contain personal information (TurboTax files, PDA information, password lists, etc.) Free encryption software can be found at: [www.pgp.com/products/freeware.html](http://www.pgp.com/products/freeware.html).
- **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://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!**

