

## PREVENTING ID THEFT & FRAUD:

- **DO** an annual credit check: <http://www.annualcreditreport.com/>
- **WATCH** for unauthorized charges.
- **VERIFY** that you are receiving all financial statements monthly.
- **DON'T** send personal or financial information over email or IM.
- **Use** a cross-cut shredder to destroy your personal documents that contain sensitive information including pre-approved credit card offers.
- **REPORT** fraudulent activities to:
  - IC3: <http://www.ic3.gov>
  - FTC: <http://onguardonline.gov>
- For additional ID theft prevention tips, visit the Hawaii State Attorney General's website:  
<http://hawaii.gov/ag/hitec/main/Identity%20Theft/>



## UH IT Safety Guide: Securing Your Computer and Protecting Your Information

Compiled by: Information Technology Services,  
Information Security Team: [infosec@hawaii.edu](mailto:infosec@hawaii.edu)

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/svpa/ep/e2/e2210.pdf>

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 – if you suspect someone else is using your UH Username, please report it to the ITS Help Desk: (808) 956-8883.
- **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
- Not falsely **represent** themselves or "spoof" another physical network connection
- **Observe** all laws relating to copyright, trademark, export and intellectual property rights. *Copying or sharing of copyrighted songs, movies, TV shows, software, games, etc. for purposes other than "fair use" is illegal. See <http://www.hawaii.edu/itsfilesharing> for more information.*
- **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:

ITS - <http://www.hawaii.edu/its>

IT security information at UH - <http://www.hawaii.edu/infosec>

<http://www.ic3.gov>

<http://onguardonline.gov>

<http://www.microsoft.com/athome/security>

<http://www.hawaii.edu/askus/705>

[http://www.webopedia.com/TERM/S/strong\\_password.html](http://www.webopedia.com/TERM/S/strong_password.html)

<http://www.webopedia.com/TERM/f/firewall.html>

<http://computer.howstuffworks.com/firewall.htm>

<http://www.antiphishing.org>

<http://windowsupdate.microsoft.com>

### Information for this document compiled from:

<http://www.hawaii.edu/svpa/ep/e2/e2210.pdf>

<http://onguardonline.gov>

<http://www.us-cert.gov/>

<http://www.copyright.gov/title17/>

<http://www.copyright.gov/legislation/dmca.pdf>

Last Reviewed: January 2012

