# Safe Computing Practices

***Information for this document compiled from:***
*http://www.hawaii.edu/askus/729*
*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

- 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 anti-virus software from http://www.hawaii.edu/antivirus/ .
- **System updates.** Regularly download and install operating system and application security patches from your software vendors.
  1. **Microsoft users**
     - Go to http://windowsupdate.microsoft.com
     - Click on “Custom"
     - Select all appropriate updates and install them
     - Repeat process until there are no more updates
     - Visit http://www.microsoft.com/athome/security/update for more details
  2. **Apple users**
     - Go to your system preferences
     - Click on software update
     - In stall necessary updates
     - Repeat process until there are no more updates
- Do **not open email attachments** from strangers **AND be suspicious** of any unexpected or unusual email from people you do know. **Do not reply** to unsolicited (spam) email. Disable "previews", automatic viewing and downloading of attachments/files.
- For more detailed information about "Securing Your Desktop Computer", please read:
  1. http://www.hawaii.edu/askus/593

## Protecting your Information

- **Do not give out personal information** (address, SSN, passwords, etc) in response to unsolicited requests. **Protect your passwords.**
- **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:
  1. http://www.onguardonline.gov/phishing.html
  2. http://www.antiphishing.org

## Additional Resources

- http://www.hawaii.edu/its
- http://www.housing.hawaii.edu/resources/resnet.cfm
- http://www.ic3.gov
- http://onguardonline.gov

- http://www.microsoft.com/athome/ssecurity
- http://computer.howstuffworks.com/firewall.htm
- http://www.antiphishing.org
- http://www.consumer.gov/idtheft
- http://www.ftc.gov/bcp/conline/edcams/infosecurity/coninfo.html
- http://windowsupdate.microsoft.com