UNIVERSITY OF OREGON

Security Checklist

University of Oregon Computer Users

As employees of the University of Oregon, we are privileged to have access to a fast, efficient computing system to assist us with our jobs. Part of our jobs is taking personal responsibility for keeping our computer and the information stored on it safe.

Just as you would lock your office when you leave, you should be taking basic steps to protect your computer from intrusion.

Acceptable Use – We are required to follow the acceptable use policy. Be sure you've read and understand the policy. Be aware of uses which are allowed and those that are prohibited. The policy is available at the following URL: http://cc.uoregon.edu/policy/acceptable_use.html.

Password Protection - Your password is your first line of defense. Use these guidelines to insure your information is kept safe.

- ✓ Choose a strong password (i.e., 8-14 characters with a mix of letters and characters that are hard to guess). Do NOT use commonly used passwords like your birthdate, license plate, children's names, etc. "U0duck$f*n" is an example of a strong password (do not use this example).
- ✓ Many of us use multiple passwords and often write them down. Make every effort to avoid doing this. If you must, keep your passwords in a secured location.
- ✓ Do not share your password with other users.
- ✓ Do not save your password in web forms.
- ✓ Passwords should be changed every six months for optimal security. Set a reminder on your computer calendar to do this. Visit http://password.uoregon.edu/ if you need to change your uoregon.edu password.

Everyday Computer Protection – Many of us work with sensitive information on a daily basis. Take these steps to insure passersby do not have access to your system.

- ✓ Lock your screen when you leave your desk. In Microsoft Windows XP, "Windows Key, L" will do this.
- ✓ Keep your portable devices (such as thumb drives) in a safe place.
- ✓ Orient your computer screen to insure it is not visible to others.
- ✓ Turn your computer off at night. If this is not possible, be sure your screen is locked when you leave.
- ✓ Physically secure your office and work area when you are not present.

Use the Microcomputing Security and Duckware CD - UO's Microcomputer Services HelpDesk distributes a Security CD. This CD automatically configures your machine to enable a number of critical security settings. This is available at the Microcomputer Services Helpdesk in 151 McKenzie Hall, or call them at (541) 346-4412 and request a copy via campus mail. If you have technical support available at your location, confirm with them before installing this product.

Keep your System Updated - Systems that are not kept up to date are susceptible to attack. Accept automatic updates when you are prompted and shut your computer off at night. Both these actions will automatically run updates when Microsoft releases them insuring your computer is in good shape.

Use Safe Browsing Practices – Most of us the internet. Usually, our computers have a default browser on them such as an older Internet Explorer version which can be susceptible to viruses.

- ✓ Use a safe internet browser for general browsing such as Mozilla Firefox, instead. You can download Mozilla Firefox at http://www.mozilla.com. You can also use Internet Explorer 7 available at http://www.microsoft.com/windows/ie/downloads/default.mspx
- ✓ Do not visit unfamiliar or suspicious websites. If you must visit them, do not type any personal information into them.

Avoid Spam - All of us receive plenty of spam and unfortunately, some of us are forced to allow emails into our computer from unknown sources because of our positions.

- ✓ If you receive an email that you're not sure of, check with your technical support staff before opening it. If you don't have support staff, call (541) 346-4412 for assistance.
- ✓ You can reduce the amount of spam you receive by checking your spam filtering settings. You can do this at http://password.uoregon.edu/spam/. There is additional information available on configuring your spam settings at http://micro.uoregon.edu/email/junk/index.html.

No Phishing – Phishing attacks try to lure you into giving away personal or financial information.

- ✓ Never click on links in an email that appear to come from Ebay, PayPal or banking sites.
- ✓ Make sure you are using the latest browsers, such as Internet 7 or Firefox 2.0.
- ✓ Consider using add-on phishing protection such as Netcraft Toolbar or Norton Confidential.
- ✓ To report phishing abuse, visit: http://www.castlecops.com/pirt or http://phishtank.com.

Sensitive Information – Sensitive information ranges from human resource information, passwords, credit card information, personal identification numbers, to student information.

- ✓ Avoid storing sensitive information on your computer if possible.
- ✓ If you must store sensitive information on your computer, talk with your technical support staff about ways to ensure it is protected.

Useful Contact Information

Acceptable Use
http://cc.uoregon.edu/policy/acceptable_use.html
abuse@uoregon.edu
6-1635

Security Incidents
http://security.uoregon.edu
security@uoregon.edu

Microcomputer Services Help Desk
http://micro.uoregon.edu/
microhelp@lists.uoregon.edu
6-4412