

A Note on Antivirus Software

Trial versions of antivirus software are often distributed with a new computer. The biggest problem with trial antivirus software is that it expires sooner than you would expect. Typically, installations of trial antivirus software on a new computer work for only a few months before they stop protecting you.

Computers often have problems when more than one version of antivirus software is installed. It is strongly recommended that you uninstall your current version of antivirus and use the campus site-licensed version. The campus version will not expire, is well supported by campus technical support staff—and best of all, it's free to current students.

Where to get UO site-licensed McAfee Antivirus

The UO's site-licensed McAfee Antivirus software is available from the Duckware CD or online at <https://password.uoregon.edu/av/>.

Where to get answers to your questions

If all of this is confusing or you need help, consult the list of technical support contacts on the back of this handout. Technical support staff can help you solve antivirus or other computer problems to make sure you stay secure.

Where to get more security information

For information, best practices, and documentation on common computer security problems, please visit <http://security.uoregon.edu/>.

Technical Support

- **IT Resources at the UO**
<http://it.uoregon.edu>
- **Microcomputer Services Help Desk**
346-4412
microhelp@lists.uoregon.edu
<http://micro.uoregon.edu>
- **UO Residence Halls**
ResNet: 346-4223
reshelp@resnet.uoregon.edu
<http://housing.uoregon.edu/resnet/>
- **Knight Law Center (law students only)**
UO Law Help Desk: 346-0485
<http://www.law.uoregon.edu/tech/>
- **Architecture & Allied Arts (AAA students)**
346-0576 / 346-2081
<http://aaa.uoregon.edu/computing/>
- **Network Services**
346-4395 nethelp@ns.uoregon.edu
- **Acceptable Use of Computing Resources**
346-5837 abuse@uoregon.edu
<http://cc.uoregon.edu/policy/>
- **Security Incidents**
346-5837 security@uoregon.edu
<http://security.uoregon.edu>



*Basic Checklist
for Safe
Computing*



UNIVERSITY OF OREGON

INFORMATION SERVICES
1212 University of Oregon
Eugene, OR 97403-1212

3 essential steps for protecting your Windows PC before connecting to the network:

1. Run the Duckware CD

Running the Duckware CD helps to ensure that your computer is up-to-date and protected from Internet threats. The Duckware CD can configure your computer to implement many industry standard security practices, such as enabling Windows Firewall, running Windows Update, and installing additional antispyware programs. These measures should not impact the operation of your computer.

2. Use an alternative web browser (e.g., Firefox)

The Duckware CD provides a copy of the Firefox web browser. It is strongly recommended that you use Firefox instead of Internet Explorer to help protect you from malicious websites.

3. Keep your computer up-to-date

The Duckware CD configures your computer to receive automatic updates from Microsoft. Be sure to restart your computer when prompted so that critical security patches are applied.

Perils of P2P

Peer-to-peer (P2P) filesharing software such as Gnutella, LimeWire, BitTorrent or AresWarez may seem like a convenient way to download music and movies, but this convenience is a double-edged sword.

When you download files using P2P filesharing applications, they are shared with everyone else on the Internet. Copyright holders are vigilant and are always poised to pursue legal action against people who are sharing these files.

Legal risks

Sharing files without the permission of the copyright owner puts you at risk of a criminal and/or civil lawsuit. Unauthorized distribution of copyright material also violates the University Acceptable Use Policy (<http://cc.uoregon.edu/policy>) and is subject to further disciplinary action by Student Judicial Affairs.

Security risks

P2P filesharing applications expose you to unnecessary security risks. Most successful computer viruses propagate through P2P networks now. Computers that are infected with viruses are removed from the campus network until the damage can be repaired.

Need help removing P2P-related contamination?

UO students living in student housing:

Call ResNet at 346-4223

All other UO students:

Call Microcomputer Services at 346-4412

Extensive clean-up jobs are usually referred to the Electronics Shop in 151 McKenzie, where technicians remove viruses and malware for a fee.

Network Quarantine System

What's network quarantine?

Information Services recently deployed a new system to temporarily remove computers from the network that are infected with viruses or are in violation of the campus Acceptable Use Policy. It is designed to provide users with easy-to-understand information about why their network access has been removed and what they can do to fix the problem.

What happens if you're quarantined?

If you are placed in "Network Quarantine," when you open your web browser you will see a website explaining why you have been removed from the network. Often this message is a warning that includes instructions on how to fix a problem. Occasionally, to protect you and others on the network, the block may be permanent until you talk with technical support.

If your computer has been placed in quarantine, any attempts to reconnect the computer elsewhere on the network may result in serious consequences.

Questions?

If you have questions or concerns about the quarantine system, please email the Information Services Security Group at security@uoregon.edu.

Note: At the time this article was written, network quarantine service was configured only for the networks providing Internet service to UO residence halls and the Greek houses. It may be more widely deployed in the future.