Network Firewalls

The Winthrop campus network is protected with firewalls at multiple locations. Although this level of protection is more than adequate for normal computing behavior, it is not a substitute for common sense and safe practices. Specifically, firewalls do not prevent email-borne viruses or other similar threats from spreading. A good and up-to-date anti-virus program is required on all computers connected to the campus network.

The firewalls installed at Winthrop divide the network into zones with different levels of protection. The network's connection to the Internet defines the first of such zones. The core network is yet another zone. And finally, each residence hall is an independent zone. Network traffic is only controlled in-between zones, not within a zone. To this effect, several network protocols and ports are permanently blocked by the firewalls. The list of blocked protocols and ports is always being modified as threats are recognized and handled. If a particular network-based application is not working as you expected, please contact the IT Service Desk at (803) 323-2400.

Operating System

All computers connected to Winthrop's network are required to run an up-to-date operating system. With most operating systems, receiving updates can be automatic. If your operating system offers automatic updates, we recommend that you turn on that feature. If you do not wish to use the automatic updates, be sure to manually check for updates at least once a week.

Malware

All personal computers connected to the Winthrop campus network are required to have a working and up-to-date anti-virus system. In addition, an anti-spyware or anti-popup utility is strongly recommended.

Recent viruses can send infected email messages from an infected computer and make the messages "look" like they came from you. Observe the following guidelines to minimize risk from computer viruses and spyware:

- If you receive documents or spreadsheets through email attachments, answer "NO" if asked to enable macros when loading the file (unless you are sure the sender is giving you a clean file). Similarly, do not execute any programs received through email attachments unless you are sure of the sender.
- Keep your anti-virus up-to-date. Also, scan your computer for "spyware" (programs that might track, display, or transmit information without your consent).
- Be sure to backup important data so it can be recovered should your computer become infected.

Free anti-malware products for Windows:

AVG:
www.avg.com

AdAware:
www.lavasoft.com

SpyBot:
www.safer-networking.org

Microsoft Security Essentials:
www.microsoft.com/security_essentials

Bear in mind that computer viruses and computer hoaxes often rely upon email to wreak

havoc. Please do not be a part of this havoc by overusing the email system to notify other users. System managers will generally take responsibility to notify their customers.

If you wish to know how to distinguish between genuine viruses and computer hoaxes, a reputable source can be found on the Symantec Web site. Hoaxes are listed at **www.symantec.com/avcenter/hoax.html**. Descriptions of real viruses are found at **www.symantec.com/avcenter**. Another reputable source of information is the CERT Coordination Center at Carnegie Mellon (**www.cert.org**).

Password Fraud

The latest trend in malware is the fake email from someone in the IT department. The email often comes as a notice that your account is over its limit or to announce an upgrade to the email system. The request invariably asks you to reply with your username and password or click on a link to a Web page that asks for the same information.

Please do not fall into that trap! The emails are forgeries and are not sent by anyone in IT. **In fact, IT will never ask for your password.** Your password is only known to you and should remain secret. If you suspect that someone knows your password, change it immediately. If you have any doubts about a request from IT, please contact the IT Service Desk.

Hoaxes

Numerous hoaxes circulate on the Internet. Anytime you see a message that asks you to "tell everyone you know," then it generally means that the message is a hoax intended to overuse email systems and networks. These messages often promise money or good luck. Others often threaten with viruses or pending legislation.

If you receive a message that appears to be a hoax, is offensive, or is in violation of law or University policy, please delete the message or forward it to **servicedesk@winthrop.edu** for analysis.

Spam

If you are like most people, you have experienced a dramatic increase in Unsolicited Commercial Email (UCE), otherwise known as "spam". You are not alone. Almost everyone is receiving these usually undesired messages. Businesses and universities, including Winthrop, are using various means (none 100% effective) to cope with and reduce the amount of spam that is delivered to users' mailboxes. These measures range from filters, to real-time black hole lists, and commercial anti-spam appliances. Unfortunately, machines cannot yet "read" an email message or "view" a photo and accurately discern whether or not a message should be considered spam. When you receive a spam message, it is usually best to simply ignore it and delete it. It is generally not a good idea to click on any part of the message, or follow any Web link.

Keep the following points in mind:

- Nothing is free. No matter what the message says, there is always a catch. Nobody is going to spend money to buy your email address in order to give you something at a loss.

- You are not the only one with that "exclusive" unique prize claim number. Everybody on our email system got that same "special" number!

- You are no more "pre-approved" for that credit card than anyone else - we're all pre-approved!

- There is no way to effectively count how many times an email has been forwarded. Microsoft will not donate money to a poor sick child for forwarding a message a bazillion times.

- The reply-to address on a spam message is often fake or forged. You might even receive a spam message designed to look like it came from your own mailbox.

Portions of the above text were written by David Kelley at the University of Hartford and adapted for publication at Winthrop University with permission.

Netiquette and Social Networking

In general, it is doubly important to be careful and use common courtesy when communicating via email where, for example, body language and tone of voice must be inferred.

- Use smileys or emoticons to indicate tone of voice, but use them sparingly. :-) is an example of a smiley (look sideways).

- Use mixed case. UPPER CASE LOOKS AS IF YOU ARE SHOUTING.

- Be careful when addressing mail or replying to messages. You may accidentally send a personal response to a great many people, embarrassing all involved. Know to whom you are sending.

- Apply common sense "reality checks" before assuming that a message is valid. Many viruses can spoof someone's address and cause chaos.

- Keep your communications brief yet explanatory. Few people like reading text on a computer screen. Also, many people now receive email on smart phones. The small size of the screens on these devices makes reading lengthy messages particularly challenging.

- Know how large a message is before sending it. Attaching large files such as pictures or music may make your message so large that it cannot be delivered or at least consumes excessive resources.

- Think before you hit the "Send" button, especially if you are upset or in a hurry. A good rule of thumb is to be conservative in what you send and liberal in what you receive. You should not send heated messages even if you are provoked. On the other hand, you shouldn't be surprised if you get such messages, and it's prudent not to respond.

- Emails are not instant communications. Don't think that an email has to be answered right away. Some folks may not check their mailbox until the next morning. Use your judgment when selecting a means of communications. In many cases, a phone call or even a personal conversation may be more appropriate than an email.

- When communicating on a social network, consider that a large audience will see your posts. That may include your present or your next boss. Was that goofy picture

really necessary? Remember that your words may be stored for a very long time in a place that many people can access.

- When publishing personal information on the Web, be mindful that it can be read by someone with particular motives. Can someone find out about your friends, birthday, habits, hobbies, etc., online? Could they use that information to gain your trust?

- Never post anything online that you wouldn't want shared publicly.

- Email is not secure. Never put in a mail message anything you would not put on a postcard. In general, assume that all information you send on the Internet is visible by many. Conversely, do NOT assume that any information you find on the Internet is up-to-date or accurate. Even though technology allows just about anyone to become a publisher, not all people have discovered the responsibilities that accompany publishing.

Portions of the above text were taken from RFC 1855, The Internet Engineering Task Force (ITEF).

Copyright

Most existing copyright laws are valid in the online realm just as they are offline. Downloading music files is very quick and easy. But with easy access comes responsibility. Always respect copyright laws! This includes printed and digital material. Do not engage in illicit music, video, or movie downloads. Please be advised that Winthrop's IT department will notify the appropriate authorities whenever requests are made by the Recording Industry Association of America or any other legitimate enforcement or monitoring entity. Offenders are also reported to the Dean of Students office for disciplinary action.

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Copyright infringement includes civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense. In addition to civil and criminal penalties, students face disciplinary action in accordance with the Student Code of Conduct and the Student Handbook. University penalties may be as severe as suspension of, or loss of, access to University computer resources (including the campus network), suspension, or expulsion from the University.