stay protected

The security requirements outlined in the Desktop and Portable Security Standard have become necessary because of rapidly increasing Internet computer threats. An unpatched computer can be infected within minutes of connecting to the Internet—it can then be used to send spam, host files, or attack other computers on the network. In fact, almost 90% of the emails received by RIT are spam, phishing attempts, or contain viruses or worms.

Yes, it’s a lot to do, but it’s a reasonable response to today’s ever-increasing level of threats. You don’t have to do it all at once—if you’re supporting your own system, set your virus scan to run daily, and check for patches another day. Check for detection updates before running the programs.

Fixing or recovering from attacks is hard work and a lot more difficult than preventing them. Following these requirements will provide protection from a broad spectrum of Internet threats, including viruses, worms, trojans, spyware, and adware. They will also protect your computer from direct attacks.

get the software

Visit the RIT Information Security website for a list of suggested products. Please keep in mind it is not always best to use more than one product for the same purpose—check with the manufacturer to avoid potential conflicts prior to installation.

If products are not available from reputable commercial or reliable open source communities for a specific requirement, then the specific requirement is waived until an appropriate solution is available.

get informed

Visit the RIT Information Security website to read the security standards, get the schedule for our Digital Self Defense workshops, access security tools and software, or find out more ways to protect yourself.

RIT INFORMATION SECURITY
http://rit.edu/security
infosec@rit.edu
(585) 475-4123
introduction

To protect the RIT community and the Institute network from computer-borne threats, RIT has created a set of minimum security requirements for desktop and laptop computers.

This brochure provides an overview of those requirements, as outlined in the Desktop & Portable Computer Security Standard. For more specific information, please consult the standard on the RIT Information Security website.

who does it apply to?

The Desktop & Portable Computer Security Standard applies to:

- All RIT-owned or leased computers
- Any computer (physical or virtual) connecting to the RIT network through a physical, wireless, dial-up, or VPN connection

Currently, the standard does not apply to:

- Computers used only to access RIT-affiliated webpages or webmail from off-campus
- Cell phones, smart phones, and other special-purpose devices

RIT reserves the right to quarantine or block compromised or vulnerable non-RIT computers from the network.

what do I have to do?

In order to comply with the Desktop & Portable Computer Security Standard, you may need to change some practices and begin using additional protective software on your computer.

ANTIVIRUS SOFTWARE

Install anti-virus software, keep it up to date, and scan your system at least weekly. RIT provides McAfee antivirus software free for both home and campus use via the http://start.rit.edu. Make sure to turn on its auto-update feature for the best protection.

ANTI-SPYWARE

Spyware sends information to others without your permission. Current antivirus should include an anti-spyware component.

PATCHES

Regardless of what operating system you use (Windows, Mac, Linux, etc.), make sure it is up to date with security patches. For continuous protection, make sure auto-update is turned on as well. Running out-of-date versions can put you at risk of being exploited by web-based attacks.

BUFFER OVERFLOW PROTECTION

Install software that provides memory (buffer overflow) protection to prevent one of the most common attacks. Some products such as McAfee Antivirus already provide built-in memory protection, in which case a separate product isn’t necessary.

FIREWALLS

Personal firewalls play a crucial role in network and computer security. Essentially, they control the traffic flow in and out of networks or computers—protecting you from outside intruders and also preventing you from sending private data into the wrong hands. We recommend using products from reputable vendors such as Microsoft, McAfee, Symantec, and JavaCool Software.

HOST INTRUSION PREVENTION

A Host Intrusion Prevention System (HIPS) provides an extra layer of security by monitoring system activities—particularly those relating to network connections—to guard against malicious or unwanted behavior. HIPS is required for RIT-owned and leased computers, but is recommended for all users.