# get connected

Running your own wireless network is easy, but it's critical to secure it properly. The steps that you need to take vary by device so make sure you check your manual.

Make sure you configure the following settings on your router/access point:

- **Enable WPA2 Encryption.** Enabling encryption helps prevent attackers from sniffing your traffic and forces anyone attempting to access your wireless network to enter in a passcode. Without the right passcode, they can't "piggyback" on your network.
- **Change the default SSID and administrative password.** The SSID (Service Set Identifier) is essentially the "name" of your network. Beware of using the default router name and password – hackers can easily find the default login information from the vendor.
- **Disable SSID Broadcasting.** Many public networks broadcast their SSID to make the network easy to find. Disabling SSID broadcasting hides your wireless network from the casual observer. Anyone attempting to connect must know the SSID.
- **Enable MAC Filtering.** Each wireless network card has a unique identification number known as a Media Access Control (MAC) address. Set your network to only allow approved MAC addresses to prevent network break-ins.

INFORMATION SECURITY

- **Keep your router software and drivers up to date.** A driver is just a piece of software, and like any software, is not immune to bugs. Keeping the drivers up to date ensures that your wireless device has the latest protection and support from product vendors.

# using wireless at RIT

All wireless users at RIT are strongly urged to use the encrypted WPA2 network. **The use of wireless routers is prohibited in residential areas on campus.**

# get informed

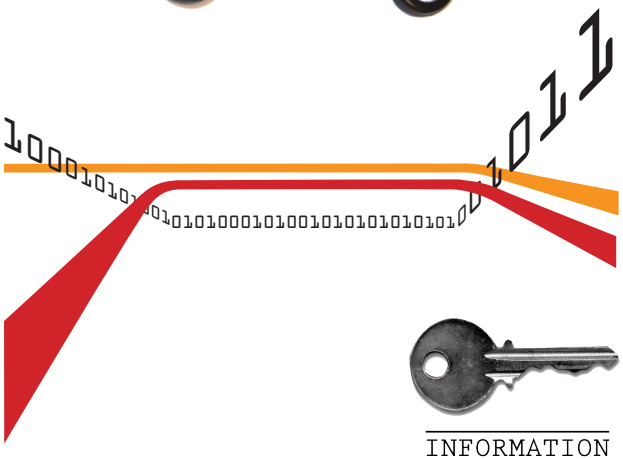
Visit the RIT Information Security website to read the security standards, get the schedule for our Digital Self Defense workshops, access security tools and software, or find out more ways to protect yourself.


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


DIGITAL SELF DEFENSE:

# accessing wireless networks safely

Protection Without Wires





INFORMATION SECURITY


Revised 7/17/2013

# introduction

Wireless networking allows you to connect to a network or the Internet without a cable. Some of the networks you may connect to wirelessly include:

- The RIT public network and encrypted WPA and WPA2 networks through campuswide wireless access points
- A wireless router connected to your home Internet connection
- A wireless "hotspot" at an airport, hotel, coffee shop, or rest area

As more people purchase laptops, smartphones and other mobile devices, wireless network access has become increasingly popular and convenient. Unfortunately, most wireless access points are set up in a manner that is insecure, placing your privacy, your data and your computer at significant risk.

# network security

### SECURE NETWORKS

Secure wireless networks use WPA2 encryption protocols, and should prompt you for a passcode or key in order to gain access. Some protocols, such as WEP and WPA, will require a password but do not provide adequate security. Make sure to identify what protocol the network is using by checking your wireless settings.

### INSECURE NETWORKS

If the wireless network you are trying to access uses WEP or WPA encryption or does not require a passcode at all, then it is probably insecure.

Insecure wireless networks are susceptible to "sniffing." Anyone with a laptop or mobile device in range of your computer can read your network traffic, including unencrypted websites, e-mails, instant messages and any file you download. It's similar to a home phone line—someone in another room can pick up a different receiver and listen to your entire conversation.

### PIGGYBACKING

If you are hosting your own wireless network and have not enabled encryption, anyone within range will be able to access your Internet connection. If an unauthorized person uses your network to commit a crime or send spam, the activity can be traced back to your account.

# protect your privacy

Accessing an insecure wireless network is inherently risky, but there are some things you can do to help protect yourself (and your private information):

### USE A VPN

A Virtual Private Network, or VPN, is a private network that uses the Internet to connect remote sites or users together. In doing so, it encrypts all network traffic at the sending and receiving ends, and uses authentication to deny access to unauthorized users. If you have VPN access through RIT or another service, use it whenever you access a wireless network.

### STAY ON "SECURE" SITES

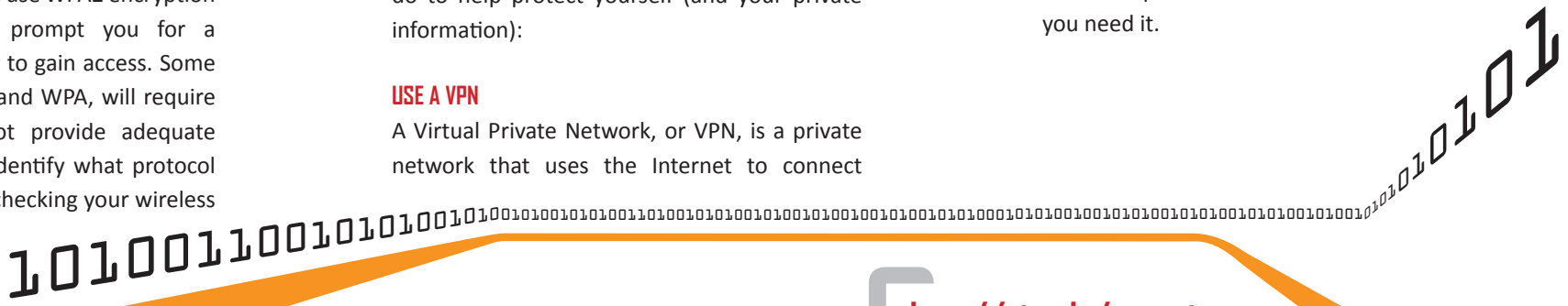
Some "secure" websites encrypt traffic to and from them automatically. You can recognize these sites by checking for "https://" (note the "s") and a lock icon either in the address bar or the lower right-hand corner of your browser.

### ENCRYPT YOUR TRAFFIC

Encrypting your Internet traffic makes it much harder for others to "listen in" on what you're doing. Check the settings on your e-mail and instant messaging software for some method of encrypting your traffic. Enable settings for "Secure Socket Layer" or "SSL."

### DISABLE AD-HOC NETWORKING

Ad-hoc networking allows computers to connect directly to one another without an access point between them. These types of networks can pose a security threat because they usually have little protection. Disable this feature unless you need it.



http://rit.edu/security