awareness

Awareness is the key to protecting yourself online, so keep these tips in mind:

THINK BEFORE YOU CLICK

Make sure you know where a link is going before you click on it. Never just click on anything that seems suspicious! Links in pop-ups, email and instant messages can be dangerous.

- To find out where a link really leads, hover your mouse over the link for a few seconds before clicking it. The full URL displays in the browser status bar.
- Type or paste links into your web browser by hand, or surf there manually from a central website.
- Never click a pop-up just to make it go away. Instead, carefully close the browser window by pressing Alt-F4.

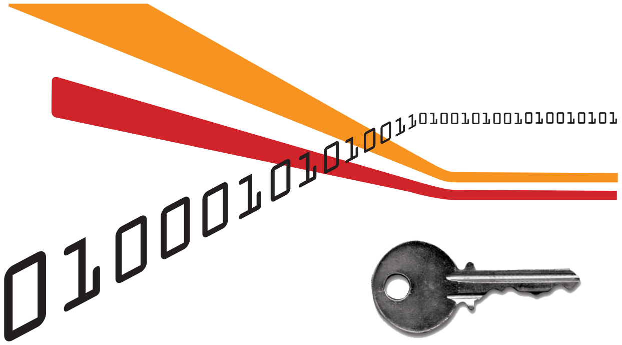
BEWARE OF COMMON SEARCH TERMS

Attackers often use common keywords to place malicious pages in search results. When searching for things like “free games” or “free screensavers”, be careful which results you select.

USE “SECURE” CONNECTIONS

All websites asking for sensitive information should be secured using a technique called SSL (Secure Socket Layer). SSL ensures your connection is encrypted, which means your traffic will be difficult to monitor. Check for

- “**https://**” instead of “**http://**” in the prefix of the web address.
- A padlock icon in the browser window. The lock icon is not just a picture – it links to details of the site’s security.



INFORMATION
SECURITY

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.

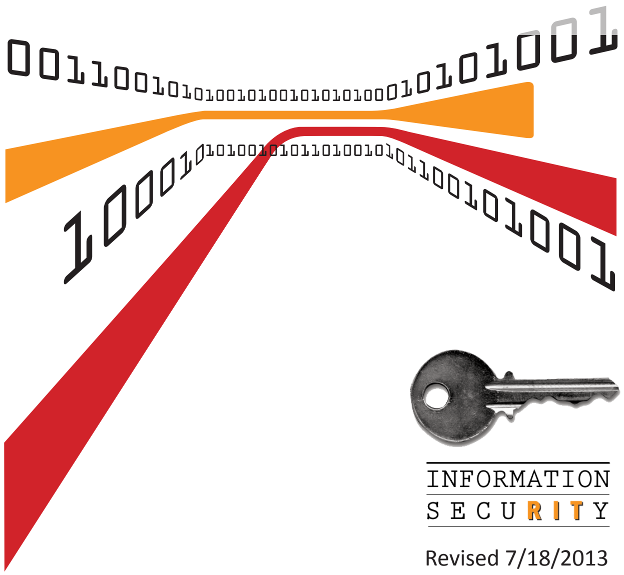
RIT INFORMATION SECURITY

http://rit.edu/security
infosec@rit.edu
(585) 475-4123

DIGITAL SELF DEFENSE:

web browsing safely

Avoid “Getting Caught” in the Web



INFORMATION
SECURITY

Revised 7/18/2013

introduction

The World Wide Web has become a primary source of entertainment, news, communication, and shopping for people all over the world. Unfortunately, the anonymity of the Internet creates an ideal environment for cyber criminals, and everyone connected is a potential target.

This guide will provide some tools and tips for protecting yourself, your computer, and your personal information while surfing the Web. With the right combination of software and common sense, you can browse worry-free.

what could happen?

There are a variety of ways you could be attacked while using a web browser, and these forms of attacks are becoming increasingly more common. Attackers could use any combination of the following techniques:

BROWSER EXPLOITS

One common way an attacker can gain control of your computer is by exploiting vulnerabilities in its operating system or software. By using webpages that take advantage of these flaws, attackers can download and install programs such as spyware and adware on your computer without your knowledge or permission. Merely visiting the site will trigger the attack.

PHISHING SITES

Waiting behind misspelled web addresses and links in fraudulent e-mails are sites that look like legitimate financial institutions and businesses. These sites capture your private information. In order to further hide the true nature of these sites, attackers will often exploit browser flaws that allow them to mask the true address.

SNIFFING

Unless you're using a "secure" connection, anyone with the right tools can monitor the webpages you visit and files you download by "sniffing" the network traffic between your computer and the Internet. When in range of a wireless network, an attacker with a laptop and a wireless card can capture all unencrypted traffic over an insecure network.

protect yourself

Follow the recommendations below to stay safe online.

PATCHES & UPDATES

Always patch/update your OS, applications, and web browser! All browsers need to be updated regularly to fix the security flaws. Many browsers have automatic update features, but not all do. Internet Explorer is updated automatically when you update Windows, and Firefox checks for updates every time you open the web browser. Stay current!

ANTI-PHISHING TOOLS

Current versions of Internet Explorer, Safari, Firefox, Chrome and Opera all provide some protection against phishing. For added protection, install one of these browser plug-ins:

- **Netcraft Toolbar** helps stop phishing attempts by blocking known phishing sites and providing hosting information about the sites you visit.
- **Web of Trust (WOT)** provides website reputation ratings based on input by millions of web users.
- **McAfee SiteAdvisor** warns you of websites known to have malicious downloads or links by checking them against a database at McAfee.

LIMITED USER ACCOUNTS

If you are using Windows XP on your computer, you may want to set up a limited user account. That will help stop malicious websites from installing malware on your computer, because limited user accounts are not capable of installing software. If you're using Windows 7 or 8, the system will notify you if software tries to install itself.

CONFIGURE BROWSER SETTINGS

See our reccomendations at https://www.rit.edu/security/content/browser-configuration

http://rit.edu/security