



# State of Louisiana

Division of Administration  
Office of Information Technology

## MONTHLY SECURITY TIPS

October 2010

### Why Cyber Security is Important

#### What Is Cyber Security?

Cyber security involves protecting the information and systems we rely on every day, whether at home, work or school.

There are three core principles of cyber security: **Confidentiality**, **Integrity**, and **Availability**.

**Confidentiality:** Information that is sensitive or confidential must remain so and be shared only with appropriate users.

**Integrity:** Information retains its integrity when it is not be altered from its original state.

**Availability:** Information and systems must be available to those who need it.

Different types of data and systems require different levels of appropriate security. For example, your confidential medical records should be released only to those people or organizations (i.e. doctor, hospital, insurance, government agency, you) authorized to see it (confidentiality); the records should be well protected so that no one can change the information without authorization (integrity); and the records should be available and accessible to authorized users (availability).

#### Why Is Cyber Security Important?

The increasing volume and sophistication of cyber security threats, including targeting phishing scams, data theft, and other online vulnerabilities, demand that we remain vigilant about securing our systems and information. The average unprotected computer (i.e. does not have proper security controls in place) connected to the Internet can be compromised in moments. Thousands of infected Web pages are being discovered every day. Hundreds of millions of records have been involved in data breaches. New attack methods are launched continuously.

These are just a few examples of the threats facing us, and they highlight the importance of cyber security as a necessary approach to protecting data and systems.

**Denial-of-service:** refers to an attack that successfully prevents or impairs the authorized functionality of networks, systems or applications by exhausting resources. What impact could a denial-of-service have if it shut down a government agency's Web site, thereby preventing citizens from accessing information or completing transactions? What financial impact might a denial-of-service have on a business? What would the impact be on critical services such as emergency medical systems, police communications or air traffic control? Can some of these be unavailable for a week, a day, or even an hour?

**Malware, worms, and Trojan horses:** These spread by email, instant messaging, malicious Web sites, and infected non-malicious websites. Some Web sites will automatically download the malware without the user's knowledge or intervention. This is known as a "drive-by download." Other methods will require the users to click on a link or button.

**Botnets and zombies:** A botnet, short for robot network, is an aggregation of compromised computers that are connected to a central "controller." The compromised computers are often referred to as "zombies." These threats will continue to proliferate as the attack techniques evolve and become available to a broader audience with less technical knowledge required to launch successful attacks. Botnets designed to steal data are improving their encryption capabilities and thus becoming more difficult to detect.

**"Scareware" - fake security software warnings:** This type of scam can be particularly profitable for cyber criminals, as many users believe the pop-up warnings telling them their system is infected and are lured into downloading and paying for the special software to "protect" their system.

**Social Network Attacks:** Social networks can be major sources of attacks because of the volume of users and the amount of personal information that is posted. Users' inherent trust in their online friends is what makes these networks a prime target. For example, users may be prompted to follow a link on someone's page, which could bring users to a malicious Web site.

## What Can You Do?

It's important that we each understand the risks as well as the actions we can take to help protect our information and systems.

- Properly configure and patch operating systems, browsers, and other software programs.
- Use and regularly update firewalls, anti-virus, and anti-spyware programs.
- Use strong passwords (combination of upper and lower case letters, numbers and special characters) and do not share passwords.
- Be cautious about all communications; think before you click. Use common sense when communicating with users you DO and DO NOT know.
- Do not open email or related attachments from untrusted sources.
- Allow access to systems and data to only those who need it, and protect those access credentials.
- Follow your organization's cyber security policies, and report violations and issues when they occur.

*The information provided in this Monthly Security Tips Newsletter is intended to increase the security awareness of end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the State's overall cyber security posture.*