CRIMINAL JUSTICE CONNECTIONS

July/August 2016
Volume 23 Issue 6

An employee publication of the
Texas Department of Criminal Justice

Policies and Benefits

Spyware: information security's invisible enemy

Spyware is a frightening name; the word conjures up images of the dangerous, cloak-and-dagger world of valuable state secrets.

Actually, in the context of information security, spyware means any software that monitors your computer activity, such as your internet usage, without your knowledge. One type of spyware is known as adware and, although it may seem invasive, this activity is usually benign as it is used to target advertising based on your online viewing history.

Spyware can also be used in more nefarious ways. Attackers could use spyware to track keystrokes and steal usernames, passwords, banking information, credit card numbers, purchase order data and other types of valuable information. At TDCJ, spyware can be a serious threat to purchasing and contract details, vendor contact information, employee identity information and criminal history information.

How can you tell if you have spyware on your computer?

Spyware, like many other forms of potential malware, uses your computer's processing

power and memory in order to run. This use of the computer's resources can cause a noticeable slowdown of the computer's performance. Symptoms of a spyware infection may include:

- Endless pop-ups
- Webpage redirection
- New toolbars installed in your browser
- New icons appearing on your screen
- Changes to you browser homepage
- Changes to your default search engine
- Windows error messages
- Diminished system performance

These symptoms are not unique to spyware; they might also indicate the presence of some other malware, or even multiple malware infections. If your work computer shows any of these symptoms, contact the Information Technology Division's Service Center right away so the issue can be remedied as quickly as possible.

How can you reduce your risk of getting a spyware infection?

TDCJ's Information Technology Division uses a variety of technologies to help protect agency computers and data from security threats, including spyware. ITD provides anti-malware software on all desktops and laptops, full-disk encryption on laptops and agency-issued smartphones, and secure VPN access for employees who need to connect to the TDCJ network while away from the office.

ITD strives to ensure all agency computers have no security vulnerabilities; however, no matter how sophisticated these technologies are, they're not effective if employees do not actively abide by and enforce the agency's security policy. Employees must do their part to protect the agency's computers.

Continued on page 2

September/October 2016
Volume 24 Issue 1

Continued from page 1

There are a several steps you can take to further reduce the risk of getting a spyware infection on your TDCJ computer:

- Do not click on any attachments or links inside of an unexpected email. If an email contains a file that looks suspicious, even if it comes from another TDCJ employee, contact the sender by some other method than email to make sure their email security has not been compromised. When in doubt, let your supervisor know and report the email to the ITD Service Center.

- Avoid going to suspicious sites and consider the potential danger a site may pose before you go to it.

- Do not click on pop-up windows or links within pop-up windows. The only exception to this rule is for tried-and-trusted websites that sometimes need pop-up windows to function.

- Always make sure your computer software is kept up to date. At TDCJ, most of this is handled automatically by system administrators who test the updates before installation to ensure they won't cause problems. If you use an agency laptop, make sure it spends sufficient time connected to the TDCJ network so it receives updates. If your TDCJ laptop is not used outside the workplace, be sure to keep it secured in your office or workspace, powered up and connected to the agency's network.

- Always make sure you have the most recent anti-malware software installed. Keep in mind that the anti-malware software on your laptop is preconfigured to keep itself up to date, but it needs to be connected to TDCJ's network to download and apply updates.

If you have any questions about spyware, malware or information security in general, contact the ITD Office of the Information Security Officer by phone at (936) 437-1800 or by sending an email to iso@tdcj.texas.gov.