CRIMINAL JUSTICE CONNECTIONS

September/October 2013
Volume 21 Issue 1

Policies and Benefits

An employee publication of the
Texas Department of Criminal Justice

Information Security: October is National Cyber Security Awareness Month

This year marks the tenth anniversary of National Cyber Security Awareness Month sponsored by the Department of Homeland Security in cooperation with the National Cyber Security Alliance and the Multi-State Information Sharing and Analysis Center to encourage government agencies, businesses, schools and the public to improve their cyber security preparedness.

In today's online, mobile society, every day brings increasing security risks from cyber threats. Information about virtually every aspect of our lives can be found on the Internet or some other computer database. The risks associated with the collection and storage of personal and financial information become clear when studies by Symantec, a major computer security system provider, show that there's a new victim of cyber crime every 18 seconds and each victim loses an average of nearly $200.

Everyone who uses a computer has a role to play in cyber security and now is a great time to evaluate your at-home online activities and take the following actions to protect yourself and your computer data.

Secure your computer: Be sure you have a security firewall installed and enabled on your computer. Use spyware, malware and adware protection software to protect against programs which can extract private information from your computer without your knowledge. Set these programs to auto-update so you won't miss critical updates.

Use strong passwords on all accounts: Use a minimum of eight characters and a mix of special symbols, letters and numbers. Use separate passwords for each account, so if one account password is breached, an attacker will not have access to all your other accounts. Do not re-use your work password on other systems.

Secure your online transactions: Before you submit sensitive information, look for the lock icon on the browser's status bar to be sure your transmission is secure. Be sure that "https" appears in the website's address before making an online transaction. The "s" stands for secure, and indicates that communication with the webpage is encrypted.

Don't reveal too much personal information online: The less information you post, the less data available for a cyber criminal to use in a potential attack or scam.

Protect your laptop, smartphone or other portable devices when traveling: Just as your wallet contains important personal information you wouldn't want to lose, so do your portable electronic devices. Don't let them out of your sight! Never store your laptop as checked luggage and if there is a secure room safe available at your hotel, use it to store your devices. Also, make sure you have strong passwords on these devices in case they are lost or stolen.

Be aware that public computers and public wireless access are not secure: On public sys-

Continued on page 2

September/October 2013
Volume 21 Issue 1

Continued from page 1

tems, cyber criminals can potentially access any information you provide, such as credit card numbers, confidential information, or passwords. Don't conduct any sensitive transactions at the local free Wi-Fi site.

Understand if and how location data is used: Check to see if GPS location data is being stored when you upload pictures to your social media site from your mobile device, and disable it if you don't want the world to know exactly where the picture was taken.

Do not e-mail sensitive data: Beware of emails requesting account or purchase information. Delete these emails. Never e-mail credit card or other financial information. Legitimate businesses don't solicit sensitive or confidential information through e-mail.

Dispose of information properly: Before discarding a computer or portable storage device, be sure that the data on the device has been erased or "wiped." Readable and writable media storage, including your hard drive, should be "wiped" using security software which has been certified to meet government and industry standards.

If you have questions, comments or suggestions regarding TDCJ information security, please contact the Information Security Office by e-mail at: iso@tdcj.state.tx.us or by calling 936-437-1800. ●