



An employee publication of the
Texas Department of Criminal Justice

July/August 2015

Volume 22 Issue 6

Policies and Benefits

Information Security: Don't fall for the social engineering scam

In the world of information security, social engineering refers to a type of confidence trick where cybercriminals use deception to get computer users to bypass security procedures and programs, resulting in the loss or theft of confidential data. Avoid becoming another victim by learning how to recognize social engineers and their bag of cybercriminal tricks.

Everyone who uses a computer connected to the Internet should beware of the following social engineering hazards.

Password insecurity

A password on a sticky note stuck to your monitor is a convenient reminder when logging in, but it also reveals your password to everyone who passes by. Never give your login credentials to anyone, even a trusted coworker. An angry colleague or other disgruntled employee might delete your files or use your name and email account to send forged correspondence to anyone, including your supervisors, and TDCJ employees are responsible for any actions performed using their login information. Keep this information secret and do not share it with anyone, even a friendly coworker.



The Information Technology Department's Computer Help Desk has administrative login credentials which allow them to do their work; if they ask if you know your password, tell them yes or no, but do not give them your password. They are only making sure that you will be able to login on your own after the help call has ended. If they need your password, they will specifically ask for it. Always change your password immediately after your computer problem has been resolved.

Tech support scams

Tech support scams involve unsolicited phone calls or computer pop-ups posing as a trusted source for computer help. Victims are told that their computer is at risk or is infected with malware, and that only the caller can fix the problem. If the victim turns control of their computer over to the scammer, they can install malware, steal confidential

information or even lock up the computer and demand a ransom be paid in order to regain access to your own data. If someone contacts you on the phone or via the Web, always verify their identity through an independent source; do not use the contact information they provide.

If you think you've been victimized by a social engineer while at work and may have accidentally created a security breach, report it immediately to your supervisor and the TDCJ Information Security Officer at (936) 437-1800 so network administrators can be placed on alert for any suspicious activity involving your account.

Information oversharing

Seemingly harmless information found online at various sources can be gathered by an industrious social engineer to steal your identity. Family and pet names are common security questions used to confirm user identities. Even an innocent-looking short survey might give away personally identifiable information like your name, date of birth and home address; knowing this, a social engineer can create a false identity which they can hide behind while committing other crimes.

Continued on page 2

Continued from page 1

Oversharing information can make you a target for “pretexting,” a con where scammers gather personal information and use it to create a detailed, seemingly legitimate scenario in the mind of the targeted victim. Vacation photos and information posted to social websites can be used to trick friends and family into sending money overseas; scammers monitor these websites to see when and where people are traveling, then contact the family members claiming that there’s been an emergency and money needs to be sent immediately. The information users post online is used to convince others that the situation is real and the caller is trustworthy.

Before posting any personal information online, consider how it might be used by a cybercriminal. Remind your friends and family to use caution and don’t be afraid to ask them to remove revealing information. ●