CRIMINAL JUSTICE CONNECTIONS

May/June 2013
Volume 20 Issue 5

An employee publication of the
Texas Department of Criminal Justice

Policies and Benefits

Information Security: No Phishing

Sending and receiving computer-based digital messages is a common aspect of everyday life, and email communications are an important part of our personal and professional lives. Vendors confirm online purchases through email, and banks send email notifications about our online bank statements. We share personal and private information with our family and friends.

With so much valuable information traveling across the Internet, it didn't take long for cyber criminals to find ways to trick users into granting unauthorized access to their own computer systems. One of the most common cyber attacks which every email user should beware of is called "phishing." Phishing was originally used to describe email attacks designed to steal banking usernames and passwords. Since then, the term has evolved to indicate almost any email-based attack.

Phishing uses social engineering, a technique where cyber attackers attempt to fool you into taking action. Attacks often begin when a cyber criminal sends an email pretending to be from a person or organization you trust, such as a friend, your bank or your favorite online store. These emails entice you to click on a link, open an attachment or respond to the message. When you follow the email instructions, you're caught.

Cyber criminals craft these emails so they appear genuine, and then send them to millions of people. Individuals are not targeted, as the criminals don't care who might fall victim; they only know that sending out more emails increases the number of people who might fall for their scheme.

Phishing attacks often employ one of the following methods.

Information harvesting: The goal is to get you to click a link and take you to a website which asks for your login and password, or perhaps your credit card or ATM number. These websites might seem legitimate, even to the point of copying the look and feel of your online bank or store, but they are fakes designed by thieves trying to steal your important personal information.

Malicious links: Again, the cyber attacker's goal is for you to click on a link, but instead of harvesting information, their goal is to infect your computer. Clicking on the link directs you to a website which silently launches an attack on your computer.

Malicious attachments: Some phishing emails have malicious attachments which, if opened, attack your computer.

Scams: Scams are criminal attempts to commit fraud. Classic examples include announcements that you've won the lottery, false-charity schemes seeking donations for a recent tragedy, and the foreign dignitary who will pay for your help transferring millions of dollars into the country. Don't be fooled, these are scams created by criminals who are after your money.

Continued on page 2

May/June 2013
Volume 20 Issue 5

Continued from page 1

Catch and Release

Simply opening an email you've received is usually safe. Most attacks only work if you take a subsequent action, such as opening an attachment, clicking on a link, or responding to a request for information.

Red flags which might indicate that an email hides a malicious attack include email which requires "immediate action" or creates a sense of urgency. This technique is used by criminals to rush people into making a mistake. Beware of any email which uses a generic salutation such as "Dear Customer." If it is from your bank or store account, they will know who you are and address you by name. Grammar or spelling mistakes indicate a potential problem, as scrupulous businesses and organizations proofread correspondence carefully. Finally, if you receive a generous, once-in-a-lifetime opportunity through an unsolicited email, remember the old saying, "If it seems too good to be true, it probably is."

You can avoid falling victim to most phishing attacks by following a few simple guidelines:

- Avoid opening unsolicited attachments. Only open attachments you were expecting to receive.
- Hold your mouse over onscreen links to see their actual web address. If you don't recognize the address, it may conceal an attack.
- Never click on an email link. It is much safer to type the web address into your browser.
- If you get suspicious email from a trusted friend or colleague, call to confirm the sender. When you call, use a telephone number you know or can independently verify, not one that was included in the message.

If your agency email account is targeted for attack, or if you'd like more information about information security, contact TDCJ's Information Security Office at iso@tdcj.state.tx.us or by calling 936-437-1800. ●