

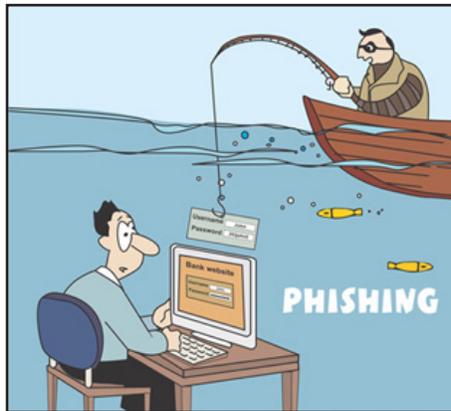
An employee publication of the  
Texas Department of Criminal Justice

## Information Security: Can you catch the phishing attempt?

In 2014, the Intel Security Group circulated a version of their Email Phishing Quiz to 100 attendees at the RSA Internet security conference. The quiz showed ten real emails collected by analysts at McAfee Labs; some were legitimate emails and some were phishing emails that looked believable. Participants were asked if they could identify the scams. When the results were tallied, industry experts could find only two-thirds of the fakes. Six percent got all the questions right and 17 percent got half or more wrong. Remember, these conference participants were Internet security pros.

When the quiz was released to the public, of the 19,458 people who took the quiz, 80 percent fell for at least one of the fake phishing emails they saw. Only 3 percent got a perfect score. Would you do any better? Take the quiz at [www.sonicwall.com/furl/phishing](http://www.sonicwall.com/furl/phishing) to find out.

Phishing scams are constantly evolving and fresh, effective emails appear every week. It's mostly a numbers game; phishers send out hundreds of thousands or millions of emails,



hoping 0.1 percent of the recipients will open them and click on links that will either direct them to give out personal information or download viruses onto their computers.

All it takes is one click to fall victim to a phishing attack. Here are some tips to avoid being hooked:

- Never click on links or attachments in unsolicited emails or texts.
- Be suspicious of messages asking for personal or financial information.

- Check to ensure that the sender's email address and company's URL match.
- Look for poor grammar and misspellings; these are signs that a message is fake.
- Be cautious of urgent call-to-action statements, like warnings that your account will be terminated.

It's also good practice to "hover" your mouse over links to make sure they look legitimate, and don't click on anything that looks suspect. If you receive a suspicious email at work, contact the TDCJ Information Security Office at (936) 437-1800. ●