Don't Be Caught by Phishing Schemes

Protect your organization from vicious online stings.

By Nidhi Rao

A dangerous breed of phishing has become increasingly common among nonprofits. Phishers attempt to steal funds by sending deceptive messages in the form of e-mails, phone calls, or websites. These messages are designed to trick an employee into divulging confidential personal or business information such as a user name, password, bank account number, social security number, or Employer Identification Number (EIN).

Phishing attacks most often appear as e-mails, but can also be conducted via instant messages or over the phone. While most organizations' e-mail services and firewalls are equipped with spam filters, cyber criminals can craft messages that appear trustworthy or impart a sense of urgency, and can sometimes penetrate security filters.

A typical phishing e-mail includes one or all of the following:

- slight variations on an e-mail address of the sender
- misspellings and grammar mistakes
- an urgent request to complete the task (for example, "I need you to do this ASAP").

Cyber criminals are persistent when devising new ways to capture sensitive information from unsuspecting individuals, and spam filters and firewalls are only the first line of protection against malicious online schemes. To proactively mitigate these risks, take the following steps:

Educate employees. Provide training on the risks associated with phishing schemes. Caution employees away from offering confidential information, such as user names and passwords, over e-mail or executing banking transactions based on instructions received via e-mail. Employees should be advised to follow internal policies and procedures when executing transactions or sharing confidential information.

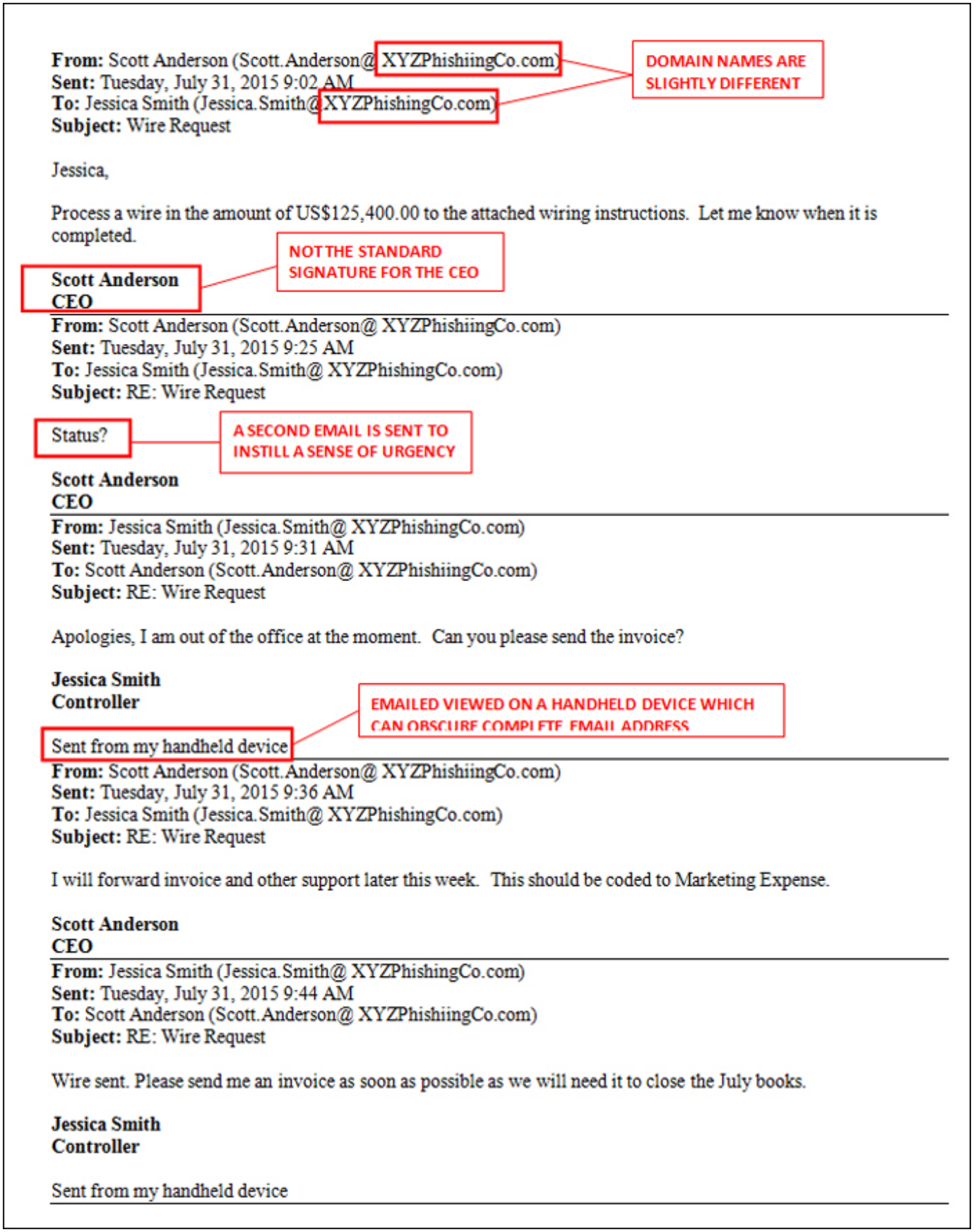
Institute two-party authentication controls. Online banking systems now offer electronic security and authentication controls so that an individual initiating a wire transfer can't also authorize the transfer. If these systems are in place, an unknowing victim of a phishing scheme can't make a wire transfer until a second individual authorizes the transaction. Such a precaution increases the chance an error will be discovered.

Require verbal confirmation. Organizations can protect themselves by instructing employees to obtain verbal authorization, no matter how urgent the request might seem, from the sender of an e-mail before processing a transaction such as a wire transfer.

Use a code word. If an organization regularly communicates requests to process transactions via e-mail, a "secret word" can be established internally to include in all e-mail transaction requests in order to differentiate a valid e-mail from a phishing e-mail. This should be a unique word or phrase agreed upon by the financial executive department and known only internally.

Notify IT staff if employees receive phishing e-mails so that spam filters and firewall settings can be adjusted to lessen the risk of future messages bypassing these defenses. And if your organization *does* fall victim to a phishing scheme, quickly investigate the source of the e-mail. Given the ever-changing cyber landscape and the speed at which digital attack tactics evolve, mitigating risk from both an IT and a personnel perspective is your best line of defense.

Note the red flags in the sample document on the next page. When you see warning signs such as these, pay special attention so you don't get hoodwinked.



Look out for these red flags that indicate possible phishing.

In our next issue, we'll provide a brief case study of a fraudulent scheme. We'll also detail tactics you can use to identify and remediate such a scheme if it occurs.