SECURITY Smart™

NEWSLETTER SPRING 2015 • BRIEFING

SAFEGUARDING YOUR SECURITY AND PRIVACY AT WORK AND AT HOME

Don't Get Hooked by a Phishing Attempt

Scammers use tricky techniques to lure their victims via email. Know what to look for so you won't take the bait.

WHEN THE EDITORS of a magazine in Framingham, Mass., received via email what appeared to be a poorly written news pitch from a company called Fiserv, offering information about its email security products, at first they were inclined to dismiss it. Like anyone else, magazine staffers receive email from known and unknown sources on a daily basis. Many contain mistakes that detract from their credibility. Most just get deleted. However, this email looked especially treacherous for a host of reasons:

The tone was overly formal. A note addressed to "Dear Business Associate," or something along those lines, as this one was, should either be deleted or treated with skepticism.

The list of addressees was questionable. The "To:" field included the editorial team plus two other employees; one had left his position several months prior, and the other never existed. Those bogus email addresses caught the other recipients' attention.

The body of the email included a request for information. If an email asks you for details that you'd normally hesitate to share with an unknown entity, look more carefully at the message.

The message had a ZIP file as an attachment. An attachment from an unknown sender should always be considered a red flag.

The email specifically asked that the attachment be opened, and that the included password be used to decrypt its contents. Another red flag.

The magazine staff agreed that the email was extremely suspicious and was most likely a phishing email, or an email designed to elicit proprietary information by masquerading as a note sent from a trustworthy entity. This particular message somehow managed to get past both the company's email gateway and its anti-spam service.

The staff told the company's IT department that a malicious email had made it past its filters, and then deleted the message itself (it's a bad idea to forward suspicious messages with un-known attachments). Later, the staff looked up Fiserv, the company that allegedly sent the email, and learned that it's a financial services organization in Wisconsin that has nothing to do with secure email products. Unfortunately, its brand was hijacked by scammers in order to make it seem legitimate when people Googled the company.

It can be easy to fall for a phishing email if you're in a hurry or if the content of the message is a familiar topic. To avoid being the victim of a phishing attack, slow down, read and analyze the entire message, and think critically.