Phishing Scenario #7

On January 29th at 10:00 AM we sent our seventh phishing simulation from PhishMe.com. Until this point all of our phishing scenarios were asking for a username and password, but in January we sent an attachment to see who would open it. The simulation was sent to 953 mailboxes, and of those 58 individuals opened the attachment, which was claiming to be their year-end tax forms.

The Phishing Email

From: Tax Forms <tax-forms@emich.edu>
Subject: Tax Forms for 2013
Attachment: 2013-Employee-Tax-Forms.doc

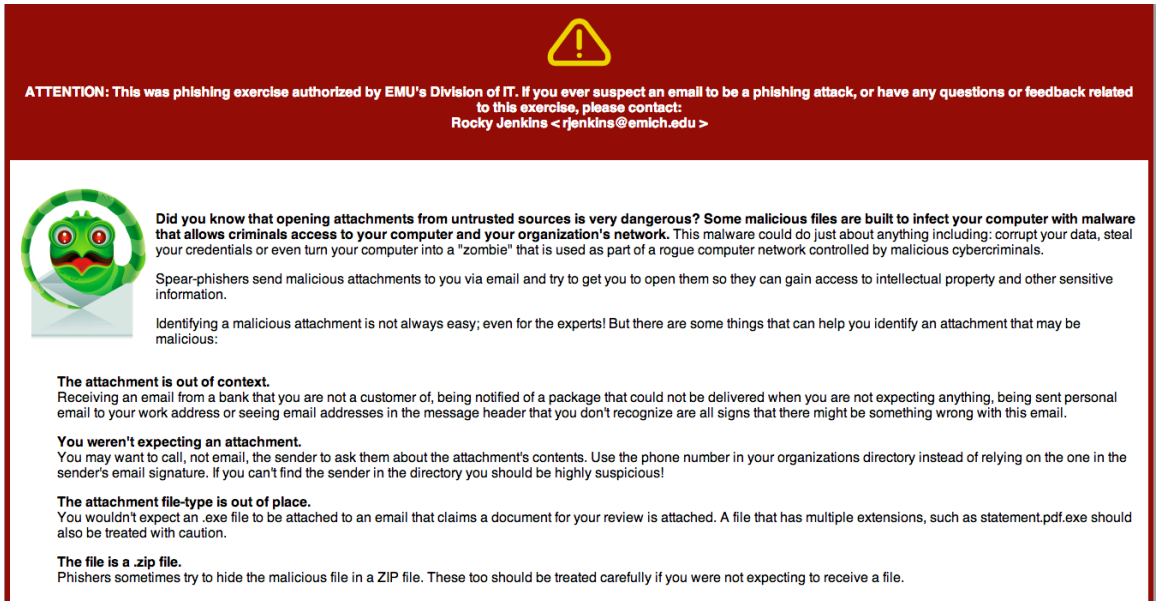
As stated in our previous email we have attached your year end tax forms.

Please take a moment to review your financial documentation for 2013 in the form attached.

For security reasons please use the following password to open the attached file: **D27W4RE0**

Eastern Michigan University
734-487-1849

The Attachment/Education



ATTENTION: This was phishing exercise authorized by EMU's Division of IT. If you ever suspect an email to be a phishing attack, or have any questions or feedback related to this exercise, please contact:
Rocky Jenkins < rjenkins@emich.edu >

Did you know that opening attachments from untrusted sources is very dangerous? Some malicious files are built to infect your computer with malware that allows criminals access to your computer and your organization's network. This malware could do just about anything including: corrupt your data, steal your credentials or even turn your computer into a "zombie" that is used as part of a rogue computer network controlled by malicious cybercriminals.

Spear-phishers send malicious attachments to you via email and try to get you to open them so they can gain access to intellectual property and other sensitive information.

Identifying a malicious attachment is not always easy; even for the experts! But there are some things that can help you identify an attachment that may be malicious:

The attachment is out of context.
Receiving an email from a bank that you are not a customer of, being notified of a package that could not be delivered when you are not expecting anything, being sent personal email to your work address or seeing email addresses in the message header that you don't recognize are all signs that there might be something wrong with this email.

You weren't expecting an attachment.
You may want to call, not email, the sender to ask them about the attachment's contents. Use the phone number in your organizations directory instead of relying on the one in the sender's email signature. If you can't find the sender in the directory you should be highly suspicious!

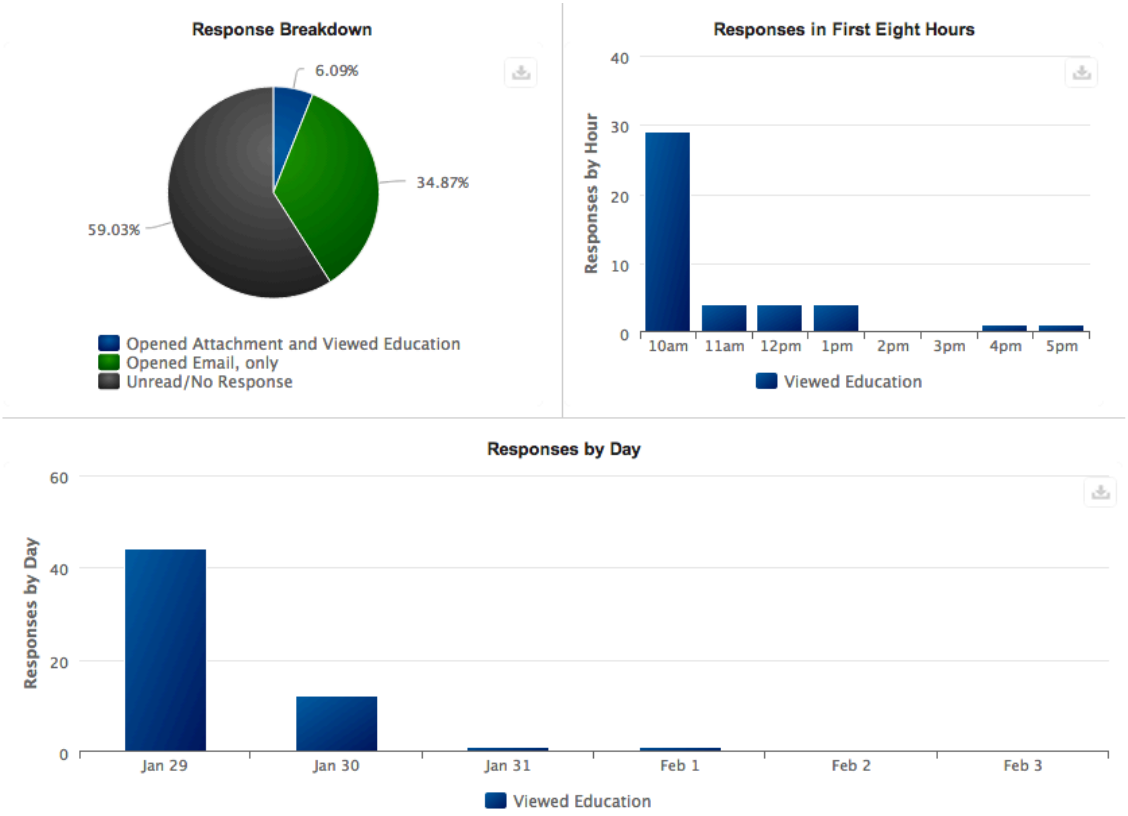
The attachment file-type is out of place.
You wouldn't expect an .exe file to be attached to an email that claims a document for your review is attached. A file that has multiple extensions, such as statement.pdf.exe should also be treated with caution.

The file is a .zip file.
Phishers sometimes try to hide the malicious file in a ZIP file. These too should be treated carefully if you were not expecting to receive a file.

How it Works

When the recipient opens the email, they are instructed to open the attached ZIP file, in this case Tax-Forms.zip, using the password included in the email. In the ZIP file was a Microsoft Word document named 2013-Employee-Tax-Forms.doc which, when opened, reported back to PhishMe and presented the viewer with security education.

The Results



- Of the **332** individuals who opened the email in a way we could track, **58** opened and viewed the email attachment.
- Of those **50%** opened the attachment within the first hour.
- This month only **5** individuals used the 

button to mark the message as spam.

Conclusion

- This month **13** of the individuals who opened the attachment have fallen victim to a prior PhishMe scenario.
- **5** of these individuals were already two-time offenders, and **1** was caught by four prior scenarios.
- This was the first attachment scenario we presented to our user base, which may account for the higher than average number of offenders.
- With this type of scenario we are unable to track how long each individual spends viewing the educational material.
- There was a dramatic drop in the number of people who used the Spam button in EagleMail for this scenario.