

Phishing Clues

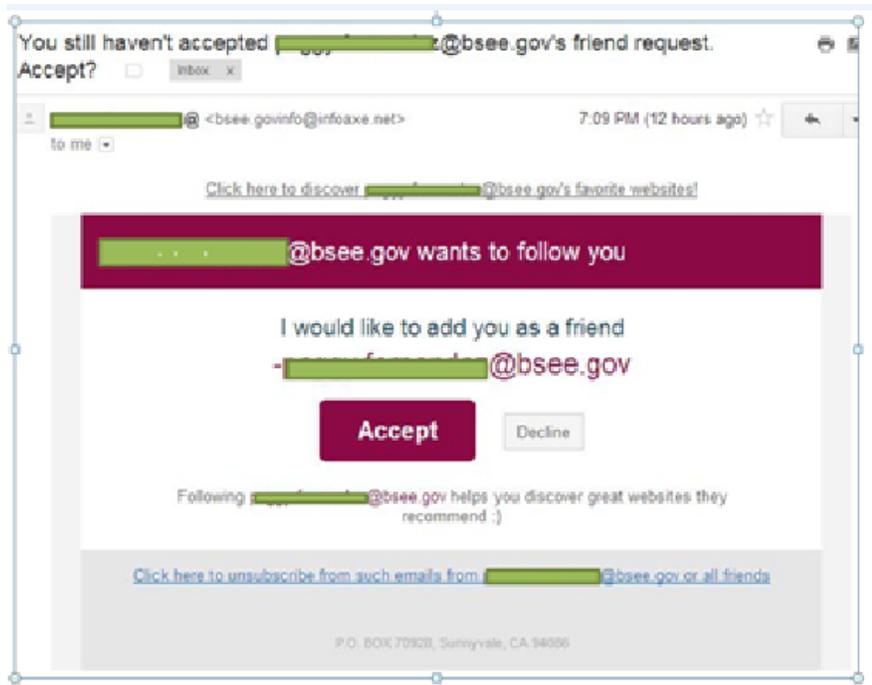
Phishing: a scam by which an e-mail user is duped into revealing personal or confidential information which the scammer can use illicitly.

Due to a multitude of recent events and other factors, chances are you will receive one or more phishing messages in your lifetime. In fact, DOI employees have already received Help Desk warnings of specific Phishing/SPAM messages targeting government employees. One of these warnings - the April 8, 2014 message-contains clues that will help you spot future phishing messages and can help you avoid being hooked.

How many phishing clues can you spot?

On April 8, 2014 the message read: "We have received notification of an active Phishing / SPAM campaign targeting users in BSEE, BOEM, and ONRR. The format of the messages may vary, but they are generally arriving to users' Gmail inboxes as "Friend Requests" from valid BSEE, BOEM, or ONRR employees"

Here's the phishing email sent with the April 8th message. How many clues do you count?
(The answer and explanations are on the back page)



How can you spot a phishing message?

- 1) Approach each email message knowing you ARE definitely a phishing target. Recent cyber attacks make this a known issue for you, a government employee. But even before recent attacks, you were a high phishing risk if your work email was posted on public sites such as doi.gov, conference presentors/attendees, social media sites, or working group public member lists. "Public" means everyone in the world.
 - a. To minimize your risk, ask that your official email address be provided to only those who need to know and preferably behind access controls-- not be posted on public websites and documentation available to everyone in the world.
- 2) Before you open emails: Stop- Look-Think about the sender's name, subject, date/time, and sender and receiver email address. Are there:
 - a. Unsolicited requests for protected information; such as User IDs, passwords, bank account or credit card information, or detailed personal or organizational information.
 - b. Unrecognizable or unknown sender addresses formatted differently or with slightly altered domains. Examples include .com when you expect .gov, like irs.com vs irs.gov or additional characters in the email addresses.
 - c. Is the subject irrelevant, full of hype/emergent/urgent, or totally unexpected?
- 3) Look at the message format. Are there:
 - a. Discrepancies, such as email banners or footers with physical addresses that don't make sense or a date sent outside normal timeframes for the business or individual (such as after business hours or after midnight).
 - b. An overabundance of clicking opportunities, including many buttons or clickable links.
 - c. Spelling or grammatical errors
- 4) Do not automatically open emails without reviewing them: Look for anything odd or out of context about an email subject line, sender name or email, or subject line format. Hover your mouse over sender name to see their email address.
- 5) Do not click on links without looking deeper:
 - a. Hover your mouse over the link and look at what is displayed-You should see the entire link address. Is it consistent with the message and sender? Is it what you expected?
 - b. Right click and copy the link and paste it in a new browser window so you see the full link/URL address. Is it what you expected and consistent?
 - c. Type in a link to the website yourself. If you need to look up the website first, search for the published company website, then type the URL in yourself, and do a search for on that site for the item you are looking for.
- 6) Evaluate attachments: Is the attachment something you'd expect, is it in the format you expect (ie .doc vs .zip/exe). If not, don't open it. Do not "Enable Macros" within attachments, as malware can be extracted through the Macros.
- 7) If in Doubt-Ask: If in any doubt about the email, links or attachments, call or email the sender at a known or publically published or previously known number/contact information. Call the Help Desk if you need help or questions.

Phishing Clues

Answers- Did you find all 9 clues pointing to the fact that this email isn't legitimate?

1. The From addressee is NOT "@bsee.gov" address –it's "@infoaxe.net"

2. Somewhat urgent sounding Subject

3. Your full or partial email address in Subject

4. Sent at a fairly late time (7:09 pm) for 'bsee.gov' offices

5. An overabundance of click options (buttons and Links) and big, bold shading

6. Tempting sounding offers and even an emoticon. Content is odd for a work related agency contact.

8. Look for good US English Grammar and content-That's an oddly worded sentence,

7. Odd 'bsee.gov' physical address (PO Box in California)

9. Hover your mouse over the links. Does the displayed web address, (aka URL) make sense with the context? We don't have live links for this email, but I'm betting that the site address (aka URL) that is shown when you hover over it is not a ".gov" URL . Hover 100% of the time before you click links.

