Phishing Attacks

Brad Christ - 2024-11-14 - Comments (0) - Security

What is a Phishing Attack?

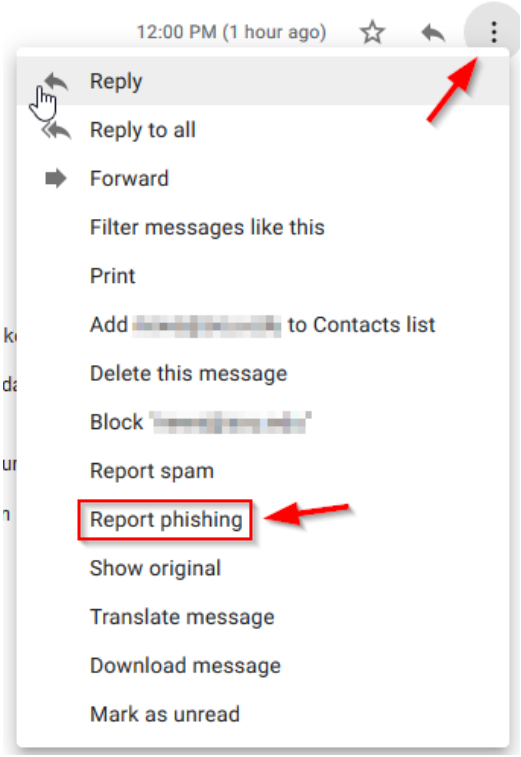
A phishing attack is a form of electronic fraud that often takes the form of spoofed emails. Spoofed emails will look similar to legitimate communications from the university or from people you may know, but are actually an attempt by malicious entities to steal information. Phishing attacks are designed to fool people into divulging things like SOU usernames, passwords, credit card details, and other personal information. They often ask you to follow a link to a page that looks like an official SOU webpage and request your username and password.

How do I know if an email is a phishing attack?

- Request for your SOU username and password: SOU IT staff will **never** ask you for your password. You should be suspicious of any email that asks you to provide login information.
- Exciting/upsetting statements: Phishing scams often rely on alarming (but false) statements to incite an immediate reaction from recipients. This could include warnings that your accounts will be suspended/deleted, that a delivery of goods/money is waiting for you, or that your information has been compromised elsewhere and needs to be verified.
- Poor spelling and grammar: Phishing and other untrustworthy emails can often be identified by their poor grammar or spelling. Many times these types of emails are not written in clear professional English. Examine the content of these emails to see if it is poorly written or contains strange unnatural wording.
- Strange URLs: If the email contains links to other pages that ask for information, hover your mouse over the link and check the bottom of your browser window to examine where the link will take you. Secure PSU login pages will have URLs that begin with "https://" (e.g. https://shib.sou.edu). If the URL looks strange to you, do not click the link.
- Unsecured pages: If you've already opened the link in the email, examine your browser's address bar. Secure SOU pages will display either a green padlock or a green bar to the left of the URL that says "Southern Oregon University". If you click on this green bar/padlock, it will display detailed information about the website's verified identity.

I think I received a phishing email, what do I do?

You can report these emails directly to Google, by clicking on the down arrow next to the reply button in Gmail. There will be an option to "Report phishing." Follow the directions that are displayed. You should also report the email to IT following these instructions.



I entered my username and password on a website that I don't think is legitimate, what do I do?

You should reset your password immediately. You can reset your SOU password by following these instructions.

If you've used the same password on any other website or service (e.g. personal Gmail account), you should also immediately change your password for those services too. **Do not use the same password for more than one website or service**.

If you need any assistance, contact the IT Help Desk or your Computing Coordinator. Also, faculty and staff members should be sure to let their Computing Coordinator know what happened.