Haekka

Lesson 8 | Phishing

Updated 2020-09-14

Phishing is a form of attack that attempts to trick you into giving up certain sensitive information - username / password, social security number, financial info. Gaining access to credentials (username and password), account for about 3/4 of all phishing attacks. The primary account targets are SaaS (hosted software programs) accounts.

Phishing is a massively common form of attack and, due to the scale of it, accounts for 80% or more of all security incidents. This is an incredible statistic and speaks to the reason phishing is a category of threat to which all people need to be educated.

Software packages, sold and distributed on the dark web, are used by malicious groups to automate and scale these attacks. Email blasts of millions of phishing messages can be sent at once. These messages will typically have a link to a bogus website that appears to be legitimate or an attachment. Statistics show that roughly 1/4 of recipients will open a phishing email and roughly 1/10 will open a phishing attachment. These are staggering statistics given the fact that phishing campaigns often send thousands or even millions of messages. And, the recent trend is towards email targeting employees at small to medium size companies.

And phishing attacks are getting more and more targeted. As more information is available about people online through social networks or other public places, this is being combined with public information about companies to launch highly customized phishing attacks, often called spear-phishing attacks.

Phishing attacks are by and large email attacks. They can take other forms, including messages through SMS and even Slack, but these are much, much less common. It is imperative that you be suspicious of emails you get, regardless of how "real" they look. Phishing attacks can look like legitimate emails from services like Netflix of Salesforce.

Some email warning signs to look for are below.

- **Requests for personal info**. How often do you get legitimate requests via email for personal information? Not much. Any request you get for personal info, or to reset something that requires your login information, should throw up red flags.
- **Suspicious wording**. If a message or even a sentence in a message does not read correctly, be highly suspicious. Phishing messages are auto-generated and information is merged into them. This often results in errors in grammar or spelling.

- **Inconsistent wording and tone**. As phishing messages are pieced together by software programs, the tone of sentences and subjects can be inconsistent with each other. If the tone suddenly changes or transitions seem abrupt, be suspicious of the message you are reading.
- **Urgent requests**. Phishing attacks play into human nature. They often attempt to scare you, put you on the defensive, and make you feel rushed. When you get this sense from a message, especially during a usy or otherwise stressful time, you may decide just to click on a link or open an attachment.
- **Inconsistent email addresses**. If you are suspicious of an email in any way, hover over or click on the address info to see more. Often, the email displayed name looks real but the address is not.
- **Messages from senders you don't get messages from**. How often does your CEO or CFO or other leaders in your organization send you emails? How often do those emails ask you to urgently take some action? Likely not frequently, or at all. This is a telltale sign of phishing emails.
- **Generic signatures**. Look for messages signed by a group, like IT or Support or HR, and not an individual.

Some of the most common phishing email subjects are below. Look out for emails with these subjects.

- Company policy updates
- Secure document to review
- System test
- System / Server / Email maintenance
- Task assignments / updates

Phishing is prevalent. You will get phishing emails. You have likely gotten phishing emails in the past. When suspicious, to any degree, ask questions of the sender. But, do not ask by replying to the suspicious message. Ask the sender on a different channel such as phone or chat.

Be suspicious of all emails you get, especially those that request some form of action (clicking a link or opening an attachment).