Best Practices To Avoid Email Phishing Attacks

Phishing has become one of the most common risks of the internet, with even tech-savvy and cautious users falling victim. Being phished might lead to the theft of personal details like your social security number or banking passwords — and it can also put your business at risk as well. Common phishing tactics include:

Using the name of a real company, as well as the company's signature look and feel

- Making the email appear to come from an actual employee, using the names of real people working for the company
- Using spoofed URLs that "look right"
- Creating a sense of urgency to cause a fear reaction from the recipient.

The one thing these spoofed sites have in common is they require the user to have a personal ID or account. The phishing email informs the user their account is somehow at risk — that they may need a security update, or to reset their password.

The following are the best practices to avoid phishing attacks.

1. Never Click on Hyperlinks in Email- Never click on a hyperlink included within the confines of an email if the link is included in an email from an unknown sender. If you feel the need to check out the website the link supposedly is associated with, you should manually type the URL into the web browser itself.

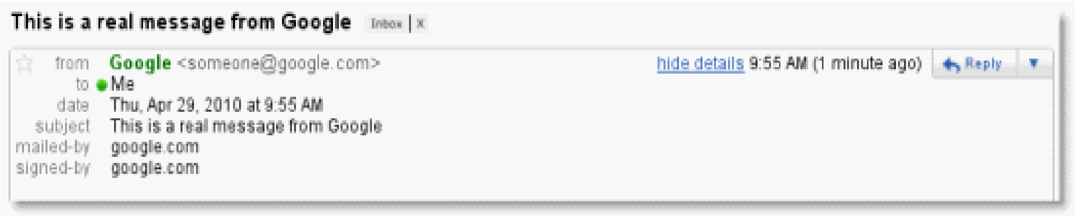
2. Never Enter Sensitive Information in a Pop-Up Window- Pop-up windows represent another tool used by phishers with illicit agendas. An important tactic to prevent phishing attacks is to never enter information into a pop up window. In fact, you are best served restricting pop-up windows all together, except at those sites that you know to be trustworthy.

3. Verify HTTPS on Address Bar-Whenever you are conveying confidential information online, you must confirm that the address bar reads "HTTPS" and not the standard "HTTP." The "S" confirms that the data is being conveyed through a legitimate, secured channel.

4. Utilize Anti-Spam Software-A number of reasons exist for taking advantage of anti-spam software. It filters out a good amount of phishing emails that would otherwise end up in your inbox. Do exercise extra caution when releasing/opening emails that were already quarantined.

5. Downloading Attachments- Be cautious about opening attachments and downloading files from emails, no matter who they are from. It is best to open attachments only when you are expecting them and know what they contain, even if you know the sender.

6. Authenticating Email-Check whether the email was authenticated by the sending domain. Open the message and click on the drop-down arrow below the sender's name. Make sure the domain you see next to the 'mailed-by' or 'signed-by' lines matches the sender's email address.



This is a real message from Google

from Google <someone@google.com> 9:55 AM (1 minute ago)
to Me
date Thu, Apr 29, 2010 at 9:55 AM
subject This is a real message from Google
mailed-by google.com
signed-by google.com

7. Password Security- Do not use the same password for all your online accounts and do not write them down. Using the same password will allow scammers to gain access to all accounts without any needed effort. Also, it is recommended that you reset your password regularly.