What is phishing?

Phishing is not new!

1995

The first phishing attack was reported in 1995. AOHell was created to steal users' passwords and use algorithms to create randomized credit card numbers.

2013

In September of 2013, Cryptolocker ransomware infected 250,000 personal computers, making it the first cryptographic malware spread by downloads from a compromised website.

2018

2019

Phishers start adopting HTTPS with gift card phishing campaigns starting in 2018 only to evolve to vendor email compromise in 2019.

2020

In 2020, 74% of organizations in the United States experienced a successful Phishing attack.

Phishing emails are the leading cause for ransomware attacks, with 54% of MSPs selecting it as the top cause of ransomware attacks

Top types of phishing attacks

Mass campaign

A wide net phishing scam is sent to the masses from a knock-off corporate entity asking them to enter their credentials or credit card details.

How to spot them:

Attacks that rely on email spoofing appear to be sent by a trusted sender

- Identify errors or inconsistencies like misspellings or a sender email address with the wrong domain.
- Review the message for any logos that look odd because they may contain, malicious HTML attributes.
- Ignore emails that have only an image and very little text.

Spear phishing

Emails that directly target a specific organization or person using tailored information.

How to spot them:

- Look out for internal requests that come from people in other departments or seem out of the ordinary for the job function.
- Be wary of links to documents stored on shared drives like Google Suite, O365, and Dropbox because these can redirect to a fake website.
- Avoid documents that require a user login ID and password. This may be an attempt to steal your credentials.
- Don't click a link from an alleged known website. Instead, open your browser and type in the website yourself. This way, you can be sure you're getting to the right website and not a phishing one.

Whaling

Is a spear-phishing attack explicitly directed at senior executives and other high-profile targets.

How to spot them:

- Rethink taking the requested action if a senior leadership member has never made contact before.
- Make sure that any request that appears normal is sent to a work email, not personal.
- If the request seems urgent and might be costly if it is fake, send a separate email\text or call the recipient and verify his request. Better safe than sorry.

Clone phishing

A legitimate email message is copied, then altered, sent from a trusted organization, and replaced with a link redirecting to a malicious website.

How to spot them:

- Be wary of unexpected emails from a service provider, even one that might be part of normal communication.
- Look out for emails requesting personal information that the service provider never asks for. If you know the request is legitimate, it is best to go to the browser and type the information directly into the website.

Other things to look for

The webpage

- Is it really needed to enter your credentials into a form?
- Does it look like the real webpage you were expecting?
- Pay attention to its structure, colors, other pages within the site, and the main menu.

Social engineering signs

- Is the email relaying a sense of urgency?
- Is the email asking you to click something to get something?
- Are you being offered something that you were not expecting?

Is this real or just looks real?

- Is the email coming from an unexpected sender?
- Check the sender's actual email address.
- Look for odd grammar mistakes.

Double-check the URL

- Look for confusing spelling mistakes in the URL.
- Look for confusing spelling mistakes.
- Are several subdomains being used?

Keep Your Business Safe

By staying aware of phishing tactics and promoting safe email habits like the ones we mentioned above, **coupled with technology** Datto SaaS Defense stops phishing across email and other collaboration platforms, before they reach the end-users.

To learn more
Contact us today

Sources:
wikipedia.org/wiki/AOHell
knowbe4.com/ransomware
Datto's State of the Channel Ransomware Report
datto.com/blog/new-research-dattos-2020-global-state-of-the-channel-ransomware-report