AMERICA'S TIRE DISCOUNT TIRE DISCOUNT TIRE DIRECT

Cyber Attacks – Phishing Schemes

Introduction

In an effort to further enhance our company's cyber defenses, we want to highlight a common cyber-attack that everyone should be aware of: phishing, and its various other forms.

"Phishing" is the most common type of cyber-attack that affects organizations like ours. Phishing attacks can take many forms, but they all share a common goal, getting you to share sensitive information, such as login credentials, credit card information, or bank account details.

This document describes phishing variations with examples:

- Phishing
- Spear Phishing
- Whaling
- Shared Document Phishing
- Smishing
- Vishing

Avoid phishing schemes

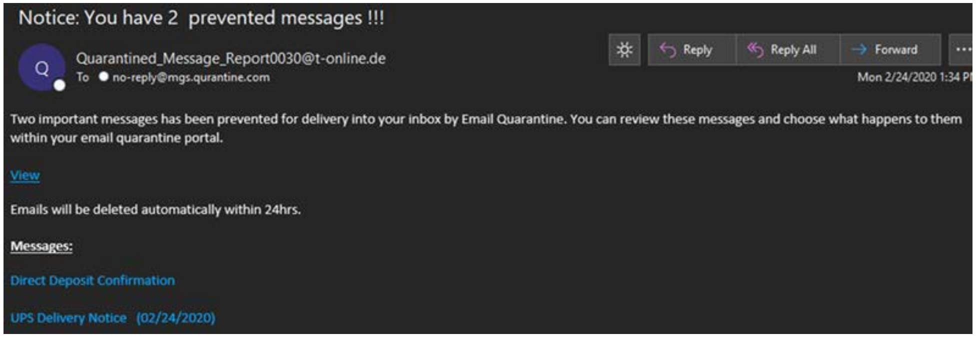
To avoid these phishing schemes, please observe the following email Best Practices:

- Do not click on links or attachments from senders that you do not recognize. Be especially wary of .zip or other compressed or executable file types, such as .exe.
- Do not provide sensitive personal information (like usernames and passwords) over email; legitimate businesses will never ask for this information over email.
- Watch for email senders that use suspicious or misleading domain names.
- Inspect URLs carefully to make sure they are legitimate and not imposter sites.
- Do not try to open any shared document that you are not expecting to receive.
- If you cannot tell if an email is legitimate or not, please delete or let the Service Desk or Security know.
- Be especially cautious when opening attachments or clicking links if you receive an email containing a warning banner indicating that it originated from an external source.

Phishing

In a phishing attack, hackers impersonate a real company to obtain your login credentials. You may receive an email asking you to verify your account details with a link that takes you to an imposter login screen that delivers your information directly to the attackers.

Example:



Notice: You have 2 prevented messages !!!

Quarantined_Message_Report0030@t-online.de
To no-reply@mgs.qurantine.com

Mon 2/24/2020 1:34 P

Two important messages has been prevented for delivery into your inbox by Email Quarantine. You can review these messages and choose what happens to them within your email quarantine portal.

View

Emails will be deleted automatically within 24hrs.

Messages:

Direct Deposit Confirmation

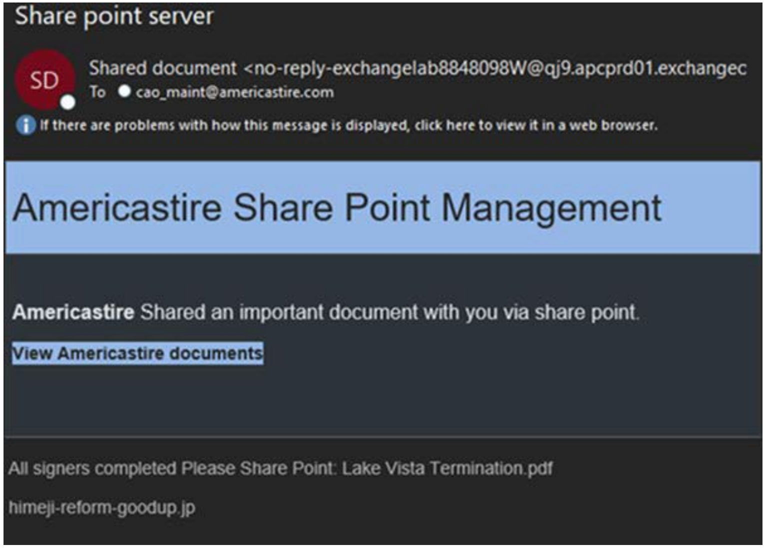
UPS Delivery Notice (02/24/2020)

Provided by: Security – John Pontrelli
Designed by: L&D – EM

Spear Phishing

Spear phishing is a more sophisticated phishing attack that includes customized information that makes the attacker seem like a legitimate source. They may use your name, phone number, and refer to our Company in the email to trick you into thinking they have a connection to you, making you more likely to click a link or attachment that they provide.

Example:



Share point server

SD

Shared document <no-reply-exchangelab8848098W@qj9.apcprd01.exchangec

To ● cao_maint@americastire.com

If there are problems with how this message is displayed, click here to view it in a web browser.

Americastire Share Point Management

Americastire Shared an important document with you via share point.

View Americastire documents

All signers completed Please Share Point: Lake Vista Termination.pdf

himeji-reform-goodup.jp

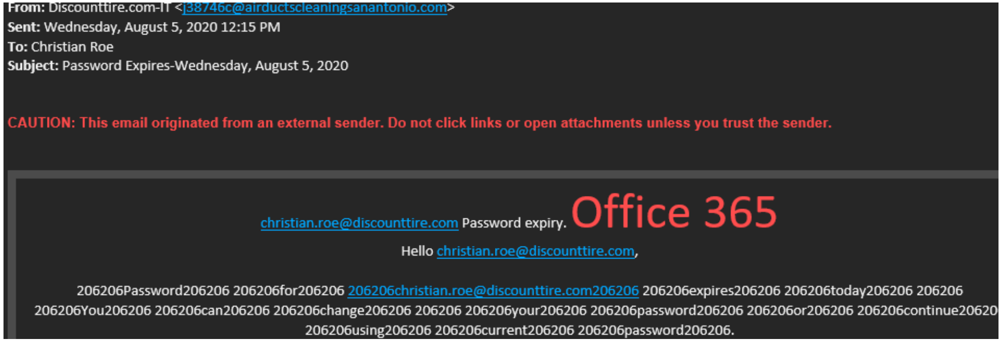
Whaling

Whaling is a popular trick aimed at getting you to transfer money or send sensitive information to an attacker via email by impersonating a real company executive. Using a fake domain that appears similar to ours, the email looks like a normal one from someone of the executive management team , typically the CEO or CFO. The email also asks you for sensitive information, including usernames and passwords.

Shared Document Phishing

You may receive an email that appears to come from file-sharing sites, like Dropbox or Google Drive, alerting you that a document has been shared with you. The link provided in these emails will take you to a fake login page that mimics the real login page and will steal your account credentials.

Example:



From: Discounttire.com-IT <j38746c@airductscleaningsanantonio.com>
Sent: Wednesday, August 5, 2020 12:15 PM
To: Christian Roe
Subject: Password Expires-Wednesday, August 5, 2020

CAUTION: This email originated from an external sender. Do not click links or open attachments unless you trust the sender.

christian.roe@discounttire.com Password expiry. Office 365

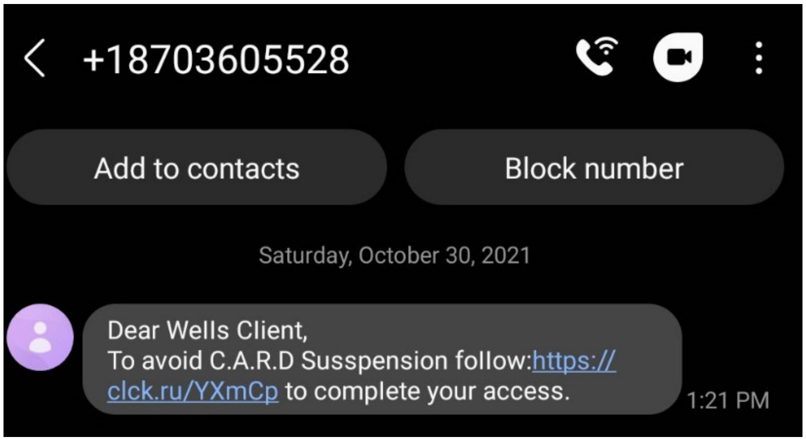
Hello christian.roe@discounttire.com,

206206Password206206 206206for206206 206206christian.roe@discounttire.com206206 206206expires206206 206206today206206 206206 206206You206206 206206can206206 206206change206206 206206 206206your206206 206206password206206 206206or206206 206206continue20620 206206using206206 206206current206206 206206password206206.

Smishing

Smishing comes in the form of a SMS text message. It is the fraudulent practice of ending text messages purporting to be from a reputable company or known individual, in order to induce individuals to reveal personal information such as passwords or credit card numbers. A smishing text may request a response from you to take additional steps, or open a link, and is often identified as 'urgent.' The recipient should delete the SMS text message AND block the caller. Do not respond as this only verifies your number to the sender.

.



+18703605528

Saturday, October 30, 2021

Dear Wells Client,
To avoid C.A.R.D Susspension follow:https://clck.ru/YXmCp to complete your access.

1:21 PM

Vishing

Starts with a phone call from a scammer who tries to use social engineering tactics to get you to share information. Attractive to social engineer attacks because it bypasses technical safeguards. The goal is to get you to share personal information, financial information, or install software on your computer.
Some common scenarios include fabricating that you have:

- A compromised account of importance to you
- IRS Tax Scam, threatening to garnish wages or call law enforcement.

What to do: hang up and contact the institution through publicly available information if you are uncertain if it is legitimate

- The number on their website
- Verify accounts yourself (do not let the attacker shadow this)

Contact

Please contact the Service Desk with any questions or concerns.
