SECURITY UPDATES

Phishing Edition #1

CHARTERED PROFESSIONAL ACCOUNTANTS BRITISH COLUMBIA

INDEX

All Examples are screenshots of real phishing attempts that CPABC has received

Phishing

Phishing is just one of the many ways that the Internet can be used to get people to unknowingly provide their personal financial information to fraudsters.

57% of companies experienced social engineering or phishing attacks.

Ponemon Institute

Prepared By Anthony Green - Security Engineer

CHARTERED PROFESSIONAL ACCOUNTANTS BRITISH COLUMBIA

Three stages of Phishing

1 Observe

2 Bait

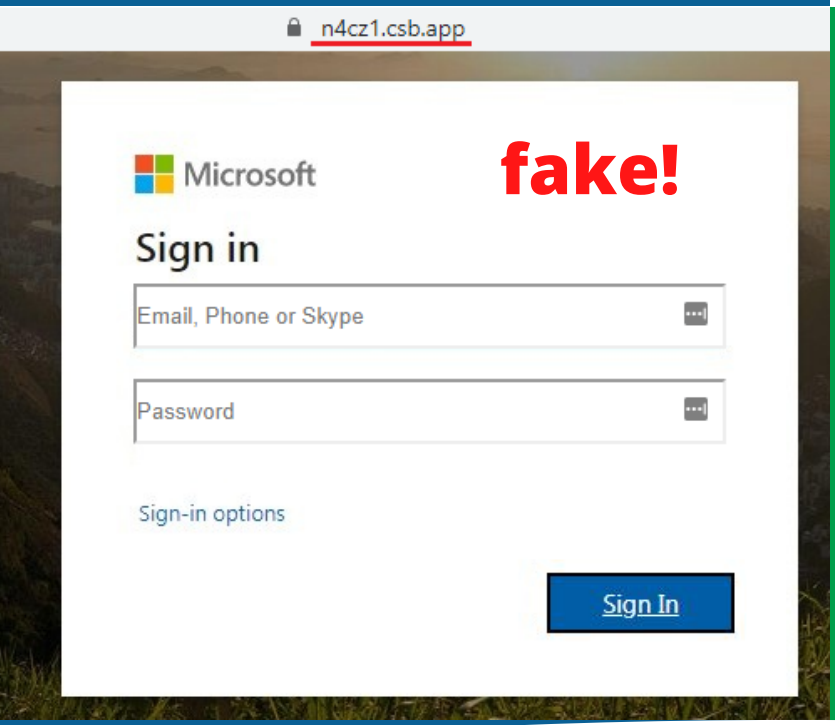
3 Penetrate

1. Observe

This is when the attacker will keep an eye on email traffic to learn about the organization in depth. This helps tailor the attack to the organization, as the attacker's knowledge of the organization's tools and technologies help disguise the attack.

2. Bait

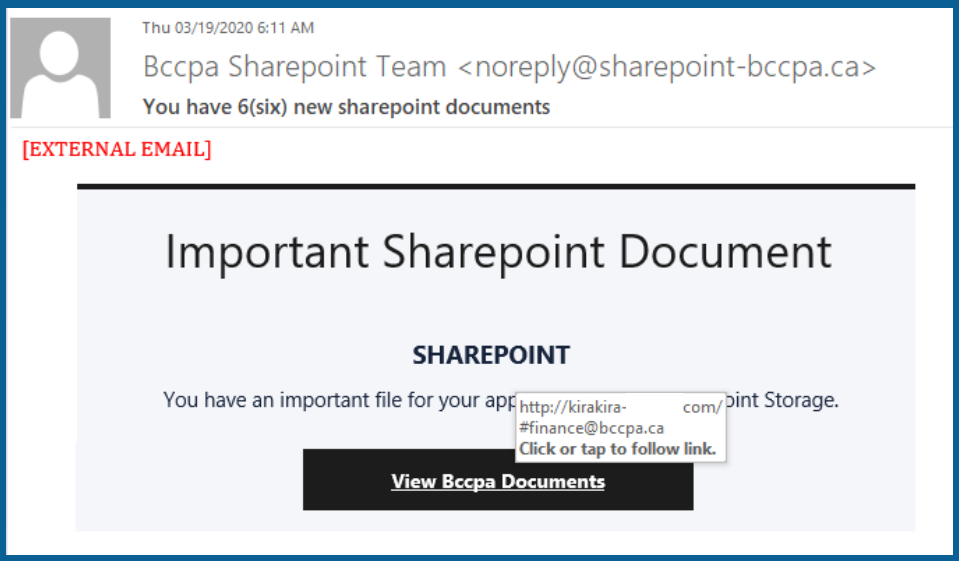
From all of the information an attacker collects from an organization, the attacker will personalize a phishing email. Common goals include: identity theft, blackmail, stealing a database of customer credit card details.



3. Penetrate

In this stage, attackers usually replicate the log-in page of the system they are trying to attack. The attacker will send recipients an email with a link. The visual appearance of the message, along with the link will closely replicate the appearance of the legitimate log-in site.

REAL LIFE PHISHING EXAMPLES


Thu 03/19/2020 6:11 AM

Bccpa Sharepoint Team <noreply@sharepoint-bccpa.ca>

You have 6(six) new sharepoint documents

[EXTERNAL EMAIL]

Important Sharepoint Document

SHAREPOINT

You have an important file for your app... oint Storage.

http://kirakira- com/ #finance@bccpa.ca
Click or tap to follow link.

View Bccpa Documents

Sharepoint Document Phishing Campaign

During a crisis, people want information and are looking for direction from their employers, the government, and other relevant authorities. This opens up opportunities for malicious actors.


bccpa.ca <quarantine@bccpa.ca>

Quarantine server has prevented delivery of 13 messages

www.bccpa.ca

Quarantine Server Withheld 13 Messages For A Quick Check

Over the past 24 hours, we saw a high influx of emails sent to your mailbox, for your protection, quarantine server moved them for proper screening.

As part of the ID Protection by bccpa.ca the messages have been screened and can now be released into your inbox.

https://firebasestorage.googleapis.com/ ...alt=media&token=9e213041-4a81-4154-a... 099-6720e5d5a7fd
Click or tap to follow link.

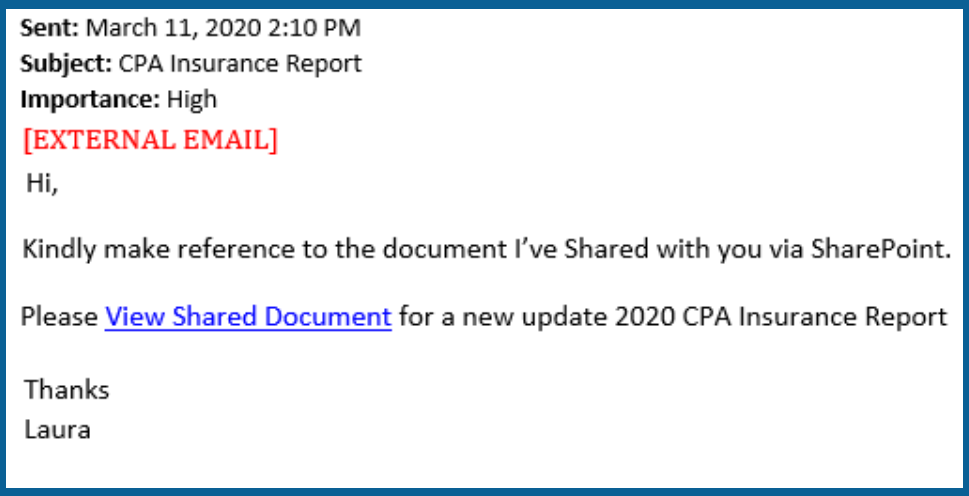
Sign in to the q... ges so as not to miss out on important messages. Upon successful logi... y from server.

Quarantine Mail Portal

bccpa.ca

Webmail Quarantine Center

© 2020 Webmail Service. All Rights Reserved.


Sent: March 11, 2020 2:10 PM
Subject: CPA Insurance Report
Importance: High

[EXTERNAL EMAIL]

Hi,

Kindly make reference to the document I've Shared with you via SharePoint.

Please View Shared Document for a new update 2020 CPA Insurance Report

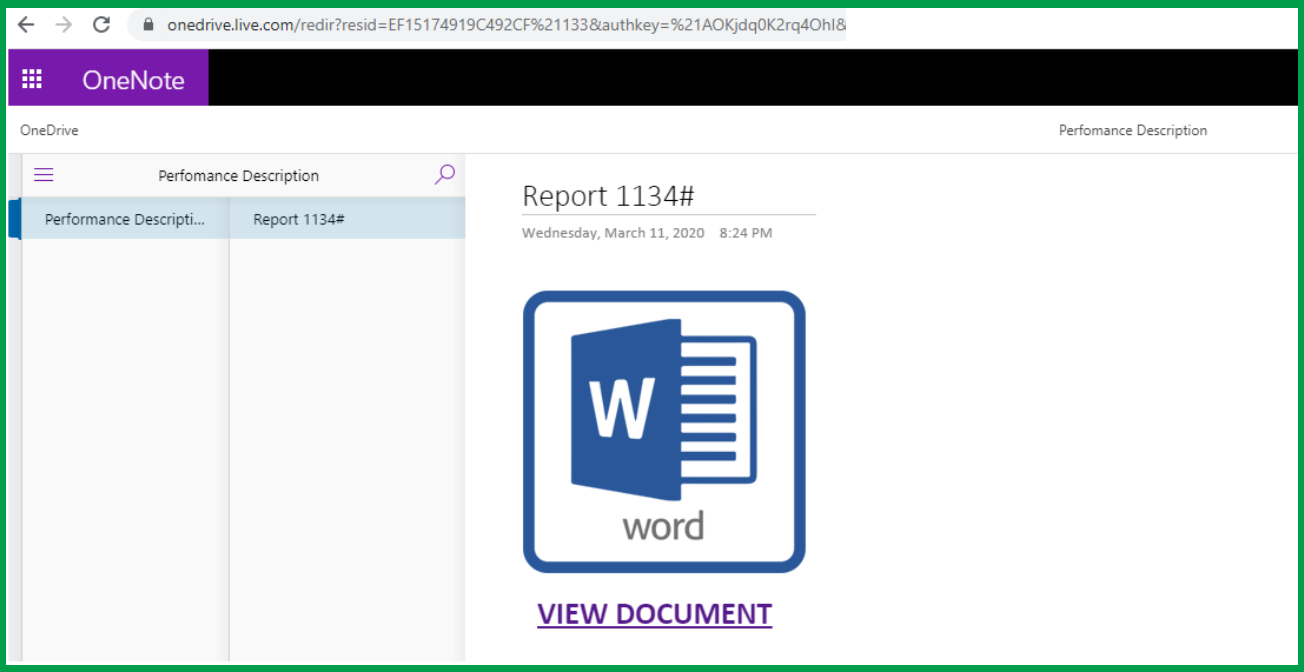
Thanks
Laura

The attacker knows that with more people working from home, sharing of documents via File Sharing is much more common than before.

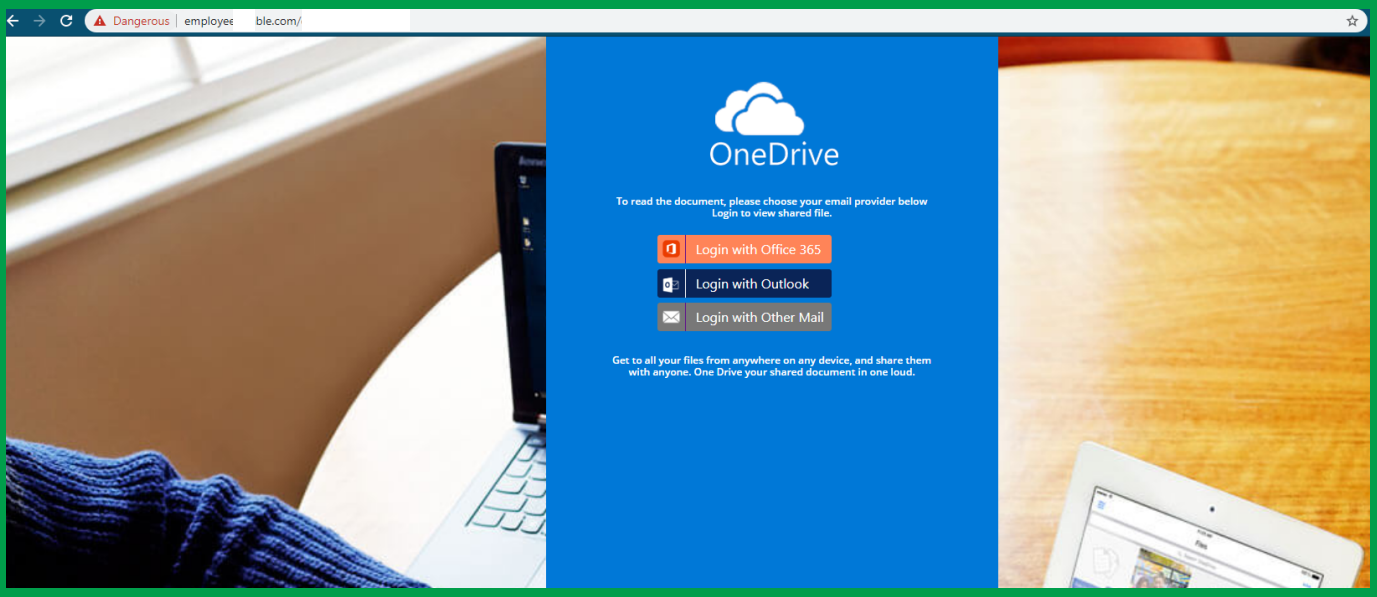
CPA CHARTERED PROFESSIONAL ACCOUNTANTS BRITISH COLUMBIA

EXAMPLES CONTINUED

You may receive an email stating there is an urgent issue that requires you to download a file from a link. The link can be leading to a legitimate site.



In this example you can see it is a legitimate OneDrive.Live site. However once you click on "View Document," you are redirected to an absolutely different page, pretending to be a Microsoft log-in page.



In the above example, the user would continue to be led to authentic-looking, yet fraudulent log-in pages intended to steal their Microsoft credentials.

How to Stay Ahead!

Tips & Techniques

- Update to the latest patches (PC, browsers, phones and any other software)
- Always check the spelling of the URLs in email links before you click or enter sensitive information (even if you are on the site)
- Watch out for URL redirects, where you're subtly sent to a different website with identical design
- Keep yourself protected by using preventive measures such as spam filters, antivirus or anti-malware software, and firewalls.
- If you receive an email from a source you know but it seems suspicious, contact that source with a new email or phone call, rather than just hitting reply
- Report any suspicious looking emails you receive so that the threat can be analyzed.