# THE STATE OF PHISHING ATTACK VECTOR

# Table of Content

- Bio
- What phishing is?
- Types of Phishing
- Anatomy of Phishing
- Counter Measures
- Reports on Phishing

Isaac K. Acheampong

Facilities Manager

BSc IT, Dip. IT, Sec+

OWASP
Open Web Application Security Project

# STATE OF THE PHISH

As the point of entry for 91% of cyber attacks, email is every organization's biggest vulnerability. From malware to malware-less attacks including impersonation attacks like CEO fraud, a single malicious email can cause significant brand damage and financial losses. Understanding these ever-evolving attacks and identifying the tactics used, is key to staying one step ahead of cyber criminals. 1

# WHAT IS PHISHING?

**Phishing** is a type of deception designed to steal your valuable personal data, such as credit card numbers, passwords, account data, or other information.

# Types of Phishing Attack

Phishing attacks come in many different forms but the common thread running through them all is their **exploitation of human behaviour**. The following examples are the most common forms of attack used.

# Spear Phishing

is a more targeted attempt to steal sensitive information and typically focuses on a specific individual or organization. These types of attack use personal information that is specific to the individual in order to appear legitimate.

# Vishing

refers to phishing scams that take place over the phone. It has the most human interaction of all the phishing attacks but follows the same pattern of deception.

Eg; MTN momo fraud

# Whaling

What distinguishes this category of phishing from others is the high-level choice of target. A whaling attack is an attempt to steal sensitive information and is often targeted at senior management.

# Smishing

Smishing is a type of phishing which uses SMS messages as opposed to emails to target individuals.

# A successful phishing attack can result in:

IDENTITY THEFT

THEFT OF SENSITIVE DATA

THEFT OF CLIENT INFORMATION

LOSS OF USERNAMES AND PASSWORDS

LOSS OF INTELLECTUAL PROPERTY

THEFT OF FUNDS FROM BUSINESS AND CLIENT ACCOUNTS

REPUTATIONAL DAMAGE

UNAUTHORISED TRANSACTIONS

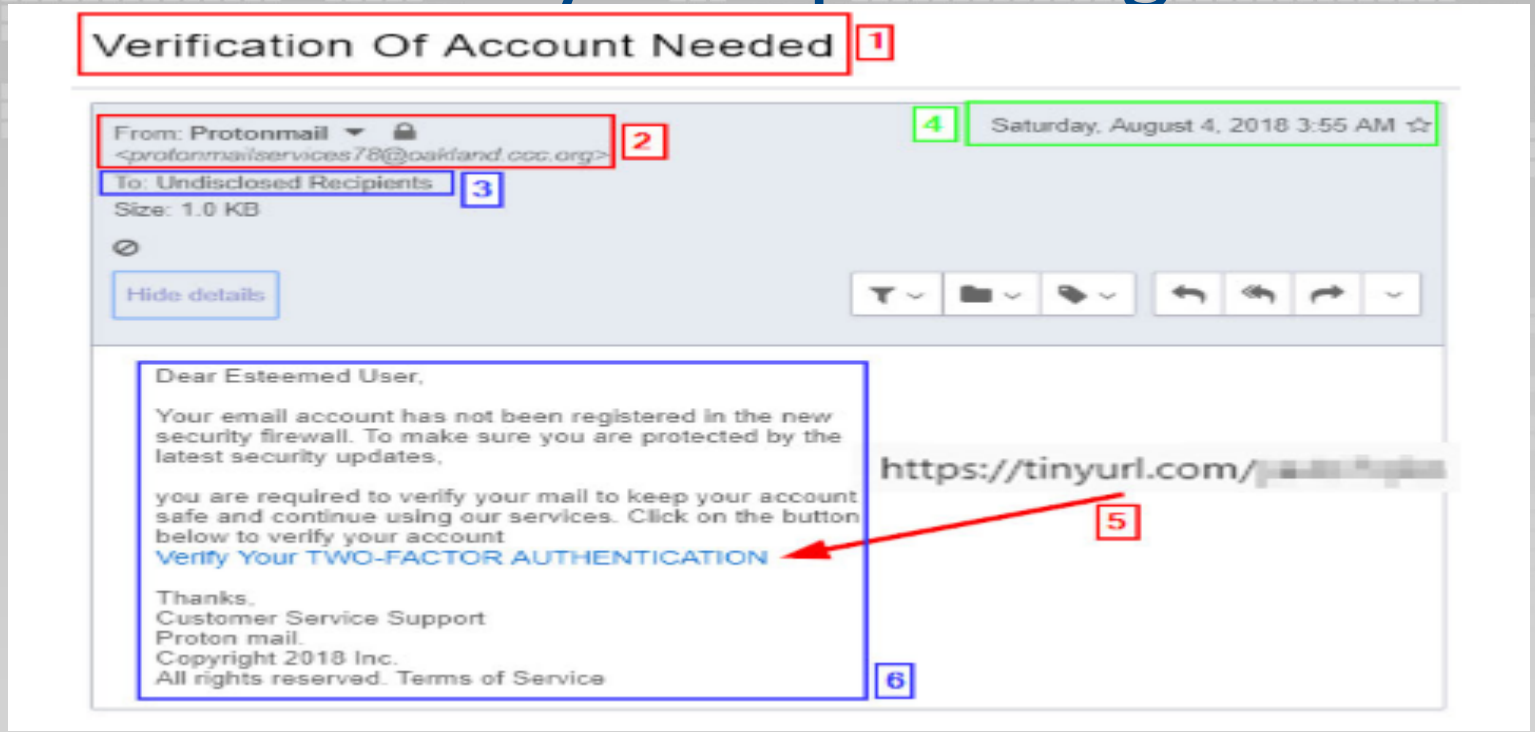
CREDIT CARD FRAUD

INSTALLATION OF MALWARE AND RANSOMWARE

ACCESS TO SYSTEMS TO LAUNCH FUTURE ATTACKS

DATA SOLD ON TO CRIMINAL THIRD PARTIES

# Anatomy of a phishing email



# First: Investigating the subject field

- Phishing emails often use urgent, scaring or threatening language in the subject line.

# Second: Investigating the “From” field

The “From” field show the sender name (display name) as “Protonmail”. However, the sender email address does not originate from “ProtonMail” domain name as it is from (**ccc.org).**

# Ask yourself the following questions:

- Did I receive emails from this address before? Is it normal to receive emails from this address?

- If you are familiar with the sending address, read it carefully and check for any misspelling in the sender name or the domain name associated with the email (e.g. paypal.com can misspell to become paypall.com).

- Do you have any business relationship with the sending address? If yes, read the email carefully; Do they ask you to handle any of your account credentials? Or to access an online form to update your personal details of some service? Or simply asking you to download attached file?

- Check if the sender domain name is malicious. **WARNING: Only attempt this if you understand how to do this safely.** There are many free online services to check whether a particular domain name is malicious. The following are the most popular ones:

## Tools to Check Phishing Domains

| | |
|---|---|
| Phishtank | https://www.phishtank.com |
| Virus Total | https://www.virustotal.com |
| Comodo Web Inspector | https://app.webinspector.com |
| Cisco SenderBase | https://www.senderbase.org |
| IsItPhishing | https://isitphishing.org |
| Norton Safe Web | https://safeweb.norton.com |
| Openphish | https://openphish.com |

# Third: Investigating The “To” field

- The “To” field displays “Undisclosed Recipients”.

- If the “CC” field is populated with addresses, check them one by one. Are you familiar with any of them?

# Fifth: Investigating hyperlinks

- Check hyperlinks within the body of the email by hovering your mouse over the link in the email to display the real address.

- Some attackers may use short URL services to mask the real phishing URL sent to the user. Services like Bitly (https://bitly.com), TinyURL (https://tinyurl.com).

- Sometimes a phishing email can only contain a hyperlink without any additional contents.

- Hyperlinks can be misspelled intentionally to mislead the recipient.

From: **ProtonMail** <*service@eureka-mail-login.ccc.org*> 07/23/2018 (7 months ago)

To: Undisclosed Recipients

Show details

Hi,

You have 1 new message(s) in your inbox and custom folders.

https://tinyurl.com/

Please log in at https://mail.protonmail.com to check them.

These notifications can be turned off by logging into your account and disabling the daily notification setting.

Have a great day,
The ProtonMail Team

# Sixth: Investigating Email body & attachments

- Does the sender ask you in urgent words to respond promptly?

- Does the sender ask you to click on a link to update your info online or to renew your subscription?

- Emails from legitimate organizations will rarely contain poor spelling, grammatical errors, and text translated using machine translator (such as Google Translate).

- Does the sender ask you to open the attached PDF/MS Office document?

- And finally, were you expecting an email attachment from the sender? Is it ordinary for the sender to send you this type of attachment?

# Countermeasures against phishing attacks

There's no magic bullet to help protect you against all phishing attacks. But a combination of software, scepticism and common sense will go a long way. Here's a few things to consider:

- Do not reveal any sensitive information.
- Pay attention to the URLs included in emails.
- Use latest version of web browsers. Eg Chrome has suspicious domains detections.

- If you suspect that an email could be a legitimate **verify it by contacting the company by phone.**

- **Do not install programs or download files sent as attachments** in emails from unknown senders.

- **Always discard pop-up screens** and never enter information using them.

- Make sure the web site you deal with to enter any information is **protected by an SSL certificate (HTTPS).** Do keep in mind that this does not guarantee a site's legitimacy. Over 20% (and rising) of phishing sites actually utilize HTTPS.

- Most virus scanners nowadays have some form of protection which prevents you from accessing known phishing domains. Make sure you **keep your antivirus software up-to-date and activated.**

- **Do not publish your primary email address online**. Create and use another account for public use.

# 2019 Data Breach Investigations Report by Verizon

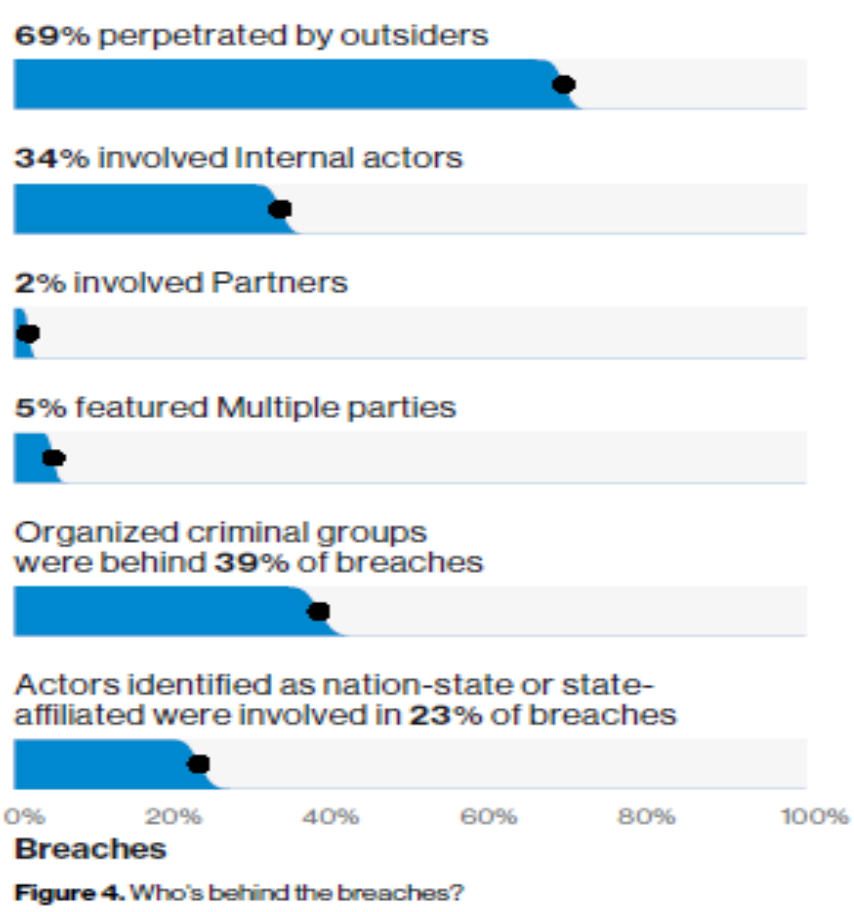



**Figure 4.** Who's behind the breaches?

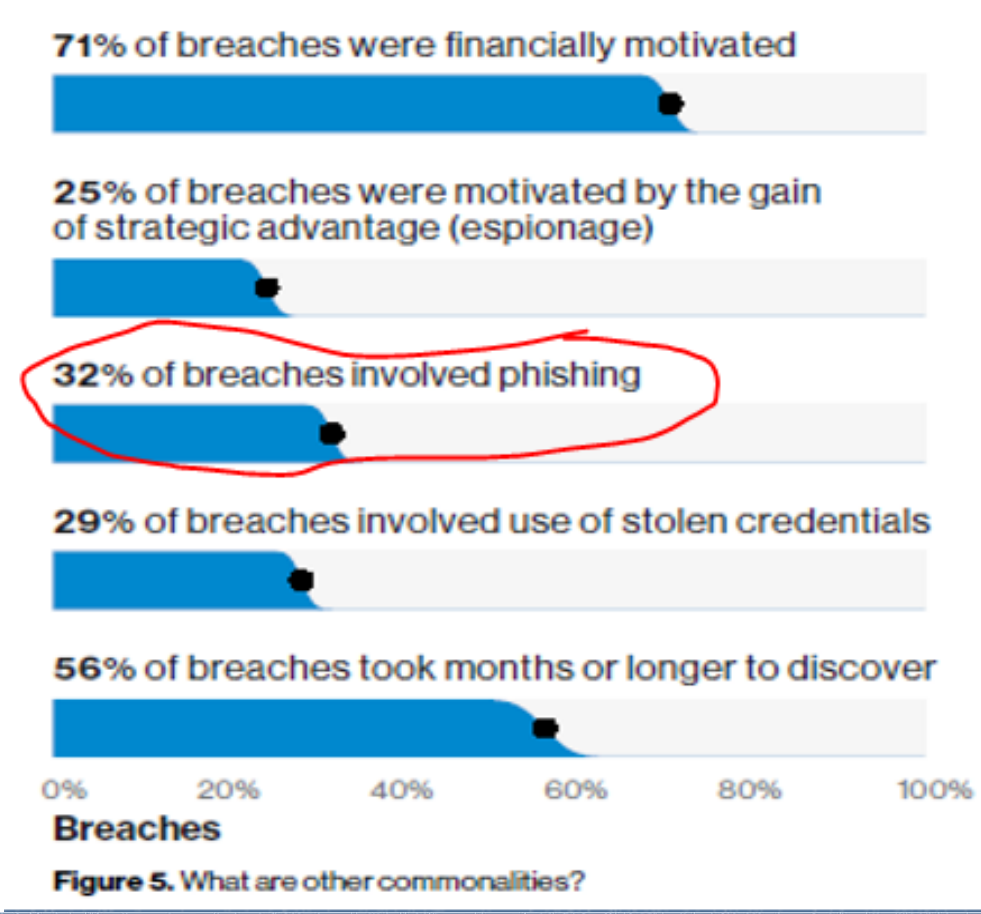
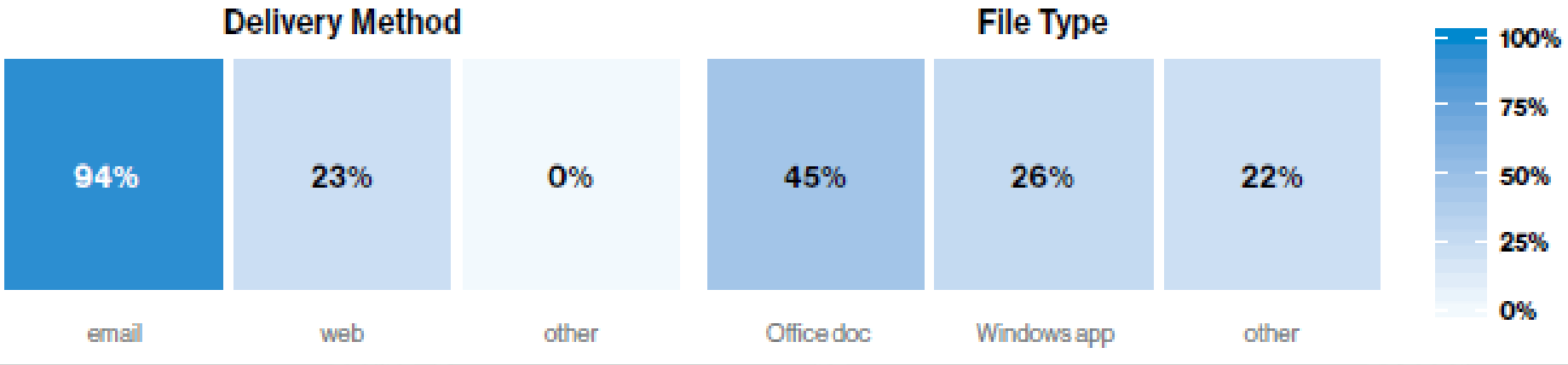



**Figure 5.** What are other commonalities?

# Malware types and delivery methods



# REFERNCE


- https://www.metacompliance.com/resources/ultimate-guide-to-phishing/
- https://www.hoxhunt.com/blog/ultimate-guide-to-recognizing-phishing-attacks/
- https://enterprise.verizon.com/resources/reports/dbir/
- https://content.fireeye.com/email/rpt-email-threat-report-en

# THANK YOU!

# QUESTIONS?