THE FUNDAMENTALS OF EMAIL PHISHING

How to identify fraudulent emails and prevent phishing attacks

Today, email is one of the most ubiquitous forms of communication around the globe. However, this proliferation has been accompanied by a growing number of cyber criminals who use it as a tool for cyber attacks. Frequently hitting the headlines as a popular – and very successful – cyber criminal method of attack is email phishing.

So, what is phishing exactly?

Email phishing is a method used by fraudsters to access valuable personal details, such as usernames and passwords. The most common example is when you receive a fake email that looks like it came from a trusted source (e.g. your bank), but takes you to a forged website that is designed to steal confidential or personal data (e.g. your bank login details).

The UK consumer association ***Which?*** found that **people receive, on average, up to 20 phishing emails a month.** These messages tend to be sophisticated spoofs pretending to be from government departments, banks and major brands, and it's becoming progressively more difficult for consumers to distinguish between mimics and genuine correspondence.

"It's becoming progressively more difficult for consumers to distinguish between mimics and genuine correspondence."

PHISHERS OFTEN USE A WIDE VARIETY OF

VARIETY OF SOCIAL ENGINEERING PLOYS

TO TRICK THEIR VICTIMS INTO

UNGUARDED BEHAVIOR

Phishers often use a wide variety of social engineering ploys to trick their victims into unguarded behavior, such as requiring recipients to respond to an email or clicking on a link immediately by claiming that they will lose something of value (e.g. a subscription or bank account access) if they do not.

The danger is that email phishing is becoming more and more sophisticated so it is increasingly difficult for consumers to distinguish between legitimate and fraudulent emails. Organizations such as **Google** and **Microsoft** offer tips for recognizing phishing emails and advice on reporting phishing emails to the relevant organizations and authorities.

Email Phishing Examples and How to Spot Them

Not that long ago, phishing attempts were quite primitive and often full of errors, and it was easier for consumers to identify when something was amiss. In addition, consumers weren't accessing their inboxes from multiple devices and mobiles, nor did they expect to receive highly personalized emails detailing their transaction history with a company.
A recent example of email phishing illustrates how sophisticated today's cyber criminals are in using social engineering to plan and execute phishing attacks.

A highly publicized phishing attack centered on the US Federal Government's Office of Personnel Management (OPM) data breach. In the wake of the breach, OPM issued a statement saying that email would be its primary form of communication with users around the breach. However, almost immediately after these emails went out, cyber criminals started distributing almost identical phishing emails.

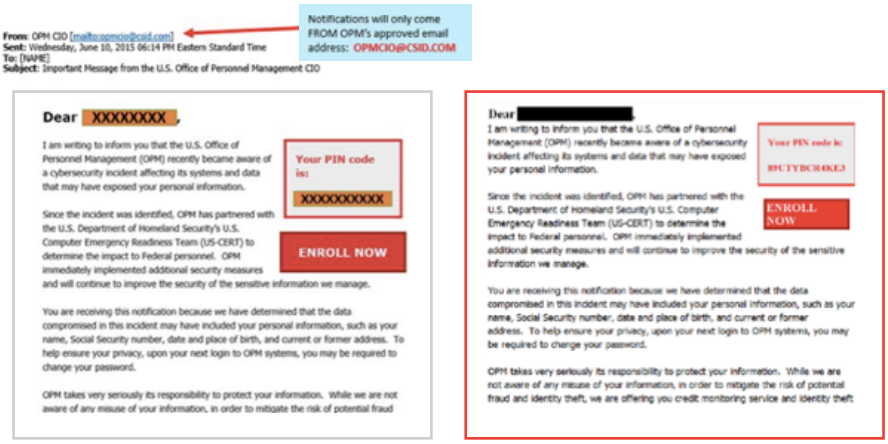
This example of phishing highlights some of the popular tactics used by cyber criminals. Taking advantage of the fact that OPM used a third-party domain, csid.com, fraudsters used something similar to convince users of email's authenticity. In addition, since the OPM email address used was not secure, anyone could send emails claiming to be from it and recipients couldn't tell the difference.

TODAY'S CYBER CRIMINALS ARE CLEARLY

HIGHLY SOPHISTICATED

IN THE PLANNING AND EXECUTION OF

PHISHING EMAILS



REAL **PHISHING**

Furthermore, OPM's legitimate email included an "Enroll Now" button, prompting victims to sign-up for credit monitoring services. Savvy cyber criminals were able to include a similar feature that directed victims to a malicious website instead. The "Enroll Now" button could be used to obscure the link (which in OPM's case was a long, questionable-looking URL) that meant receivers were unable to tell the difference between the real and phishing emails. In this particular example, the US Army flagged legitimate emails as a phishing attack.

As OPM's experience shows, today's cyber criminals are clearly highly sophisticated in the planning and execution of phishing attacks, leveraging social engineering tactics to get email receivers to do what they want, especially in times of crisis.

To help consumers protect themselves from cyber attacks there are various organizations that are driven to educate the users on cyber safety. **Stop.Think.Connect.** is one such organization. It is a global awareness campaign that helps digital citizens around the world to practice safe practices online. The group encourages internet users to be more vigilant about their online habits.

DON'T BE AFRAID TO

HOVER

PICK UP THE

PHONE

IF YOU HAVE TO

DON'T GET

ATTACHED

The Stop.Think.Connect. message is perfect to keep in mind when checking your email:

Stop

Pay attention when checking your email. If you have multiple emails and are viewing them on your phone, make sure to check each one closely - do not just blindly open them.

Think

Take a moment to be certain the subject is legitimate. Make sure to notice red flags, such as messages that only contain links or attachments or a large amount of spelling and grammatical errors.

Connect

Make sure you stay connected with the right people by filtering your email. Most providers allow you to pick and choose who should be considered a high priority, and will filter unknown names into another folder.

You can also practice a few additional email safety tips to keep yourself secure:

- **Don't be afraid to hover:** Hovering over the sender's name will bring up the domain the message is sent from, so if you don't recognize the domain, it's a safe bet that message is not legitimate. Additionally, if there is a hyperlink within the message, hovering over it will bring up the full URL.
- **Pick up the phone if you have to:** Unless you know the sender, any request for personal information should be ignored. If you receive an email from your bank asking for sensitive information and you are not sure if it's legitimate or not, click out of the email and call the sender.
- **Don't get attached:** Be wary of attachments in emails that you are not sure about. Well-known companies and brands rarely send out attachments, so it's a safe bet you should ignore one should it come through.

While cyber security is a topic that should be at top of mind every month (and every day!), using the information and resources available during National Cybersecurity Awareness Month is a good idea to refresh your online behavior and make sure you're keeping your sensitive information safe.

A SURVEY BY PONEMON INSTITUTE FOUND THAT

43%

OF BUSINESSES SUFFERED AT LEAST ONE BREACH AFFECTING

MORE THAN

1000

RECORDS IN 2014

What is a Phishing Attack & How to Avoid Being Phished?

As cyber criminals continue to become more sophisticated, there is the potential for anyone to fall victim to the dark forces of an email phishing attack. However, customers that are victim of such scams are far less likely to trust or interact with the brand again. The good news is that as a business there are key triggers representing an opportunity for cyber criminals to spoof the brand for email phishing, which you can look out for in order to protect customers.

Phishing attacks tend to peak at various times of the year and can also be triggered by events affecting specific businesses, industries, countries or even natural disasters.

For example, in the ecommerce and retail market, seasonal cycles like holiday gift-shopping, means phishing scams reach a high. While, Agari's 'State of Email Trust' report that measures the amount of fraudulent email sent using a company's domain also uncovered a spike in the volume of phishing emails aimed at payment customers in the later half of a year.

An increasingly common trigger for phishing attacks is organizational data breaches. It's an unfortunate fact that data breaches are the new normal – a survey by Ponemon Institute found that almost half (43%) of businesses suffered at least one breach affecting more than 1000 records in 2014. With most breach response plans relying on email to reach out to customers as a first line of communication, this is often also a trigger for phishing attacks.

So how can you ensure your organization's email channel is secure and prevent phishing attacks from plaguing your brand and customers, whether it be after a data breach and on a day-to-day basis?

The Phishing Kill Chain

To truly prevent email phishing attacks we need to consider the 'Phishing Kill Chain'. This uses the principles of the popular Cyber Kill Chain methodology, a military-theoretical approach to network asset defense that can be quite valuable, especially when you expand the definition of "assets" to include your customers. If you're not familiar with the concept, CSO Online has an article on it that's appropriate for any level of pre-existing knowledge.

TARGET
DELIVER
DECEIVE
CLICK
SURRENDER
EXTRACT
ACT

Military Kill Chain	Cyber Kill Chain	Phishing Kill Chain
Find	Reconnaissance	Targeting
Fix	Weaponization	Delivery
Track	Delivery	Deception
Target	Exploit	Click
Engage	Installation	Surrender
Assess	Command & Control	Extraction

So what does the Phishing Kill Chain look like?

Cyber criminals need to achieve seven steps in order to conduct a successful phishing attack on email:

1. **Target:** decide who they're going to try to defraud and assemble an email list
2. **Deliver:** send messages to the people on their target list
3. **Deceive:** the criminal needs to trick the user into following their call to action
4. **Click:** the customer clicks on the phishing site and attempts to load it in their browser
5. **Surrender:** the user needs to input their data to the phishing site, surrendering it to the criminals
6. **Extract:** the phishing site needs to transmit the stolen credential or other information to the criminal
7. **Act:** the criminal, or one of their agents, needs to log on to the account in question and transfer money, use the stolen card number online or in person, or place an order to perpetrate the final fraud.

According to **numbers published by the Canadian Government** the success rates are alarming:

- **Targeting:** 156 million messages sent per day.
- **Delivery:** 16 million make it through filters, for a 10.2% success rate
- **Deception:** 8 million are opened, for a 50% success rate
- **Click:** 800,000 are clicked, for a 10% success rate

These numbers reflect the poor controls against phishing compared to, say, generic spam.

The key point to note is that many security solutions aim to stop criminals later in the chain, such as at the **Click, Surrender** and **Extract** stages. But the earlier in the kill chain that controls can be inserted, the better the chance that organizations have of preventing their customers from being phished.

To that end, DMARC and Agari deliver a solution that can cut the chain at **Delivery**, where a proactive DMARC reject policy can prevent the message from even having a chance of landing in the inbox.

Even beyond initial rejection, Agari uses DMARC forensic data to extract threat details and provide them to takedown vendors, who validate and classify the threat. This intelligence is then passed onto Google and Microsoft for inclusion in their anti-phishing lists so that browsers block the threats. This makes the controls at step 4 in the kill chain, the **Click**, far more effective in preventing emerging threats.

If your organization is serious about preventing phishing and defending your customers as well as your brand reputation, you need to be deploying systems that help you move up the kill chain. Only then can you ensure your organization is safe from falling victim to the growing pain of phishing attacks.