How to:
Recognize and Respond to a Phishing Email

Educational eBook Series

hubTGI

How to Recognize a Phishing Email

Would you recognize a phishing email if you received one? Do you think your team would? Phishing is one of the most common attack vectors for cybercriminals – and the most effective.

The effects of a phishing attack can be severe. It can paralyze a business, stop employees from doing their work, result in stolen or damaged data, and customers may not be able to access your services resulting in a blow to customer confidence and loss of our reputation.

Hackers are becoming more sophisticated with disguising the nature of these emails and recognizing one can be increasingly difficult unless you know what to look for.

In this ebook we'll go over some of the common methods hackers use to deliver a phishing attack and how to recognize one.

What is Phishing?

Phishing is when a criminal sends a malicious email to try and trick the recipient into falling for a scam. The email usually impersonates a trusted source, such as a government organization or a well-known business.

Like fishing, some phishing emails use "bait" (the promise of money or gift cards, or a time-based threat like account suspension, etc.) to trick the victim into giving up sensitive information or granting access to protected resources, like a corporate network.

Other phishing emails contain malware within attachments or links in the body of the email. By clicking on the link or downloading an attachment the user may unknowingly infect their device or network, enabling attackers to gain access to protected applications and data.

Common Threat Vectors

The main purpose of most phishing emails today is to deliver, directly or indirectly, some form of ransomware designed to steal money, data, or personally identifiable information (PII) and hold it for ransom.

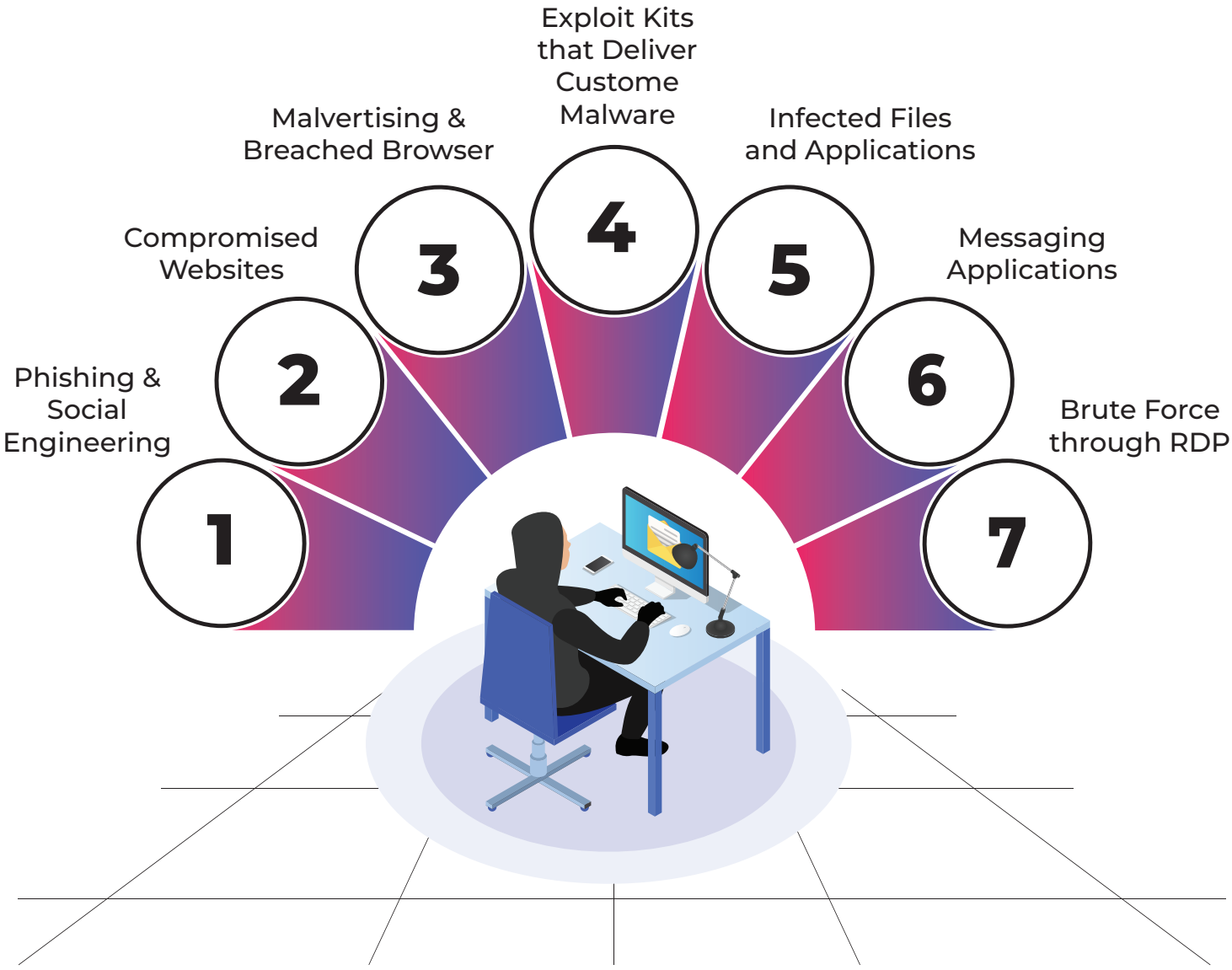
Phishing (a form of social engineering) is the most popular ways for bad actors to deploy ransomware, but it's not the only way. Other methods include:

1. Phishing and Social Engineering
2. Compromised Websites
3. Malvertising and Browser Breaches
4. Delivery of Custom Malware via "Exploit Kits"
5. Infected Files or Applications
6. Messaging Apps
7. Brute Force Through RDP

> **Over 70%**
> of phishing emails are opened by their targets.
> *– Office tech insider*

hubTGI

7 Ways Ransomware Infects Organization



Phishing/social engineering and breaches via un-patched software have been the number one and two most successful hacking methods for decades.

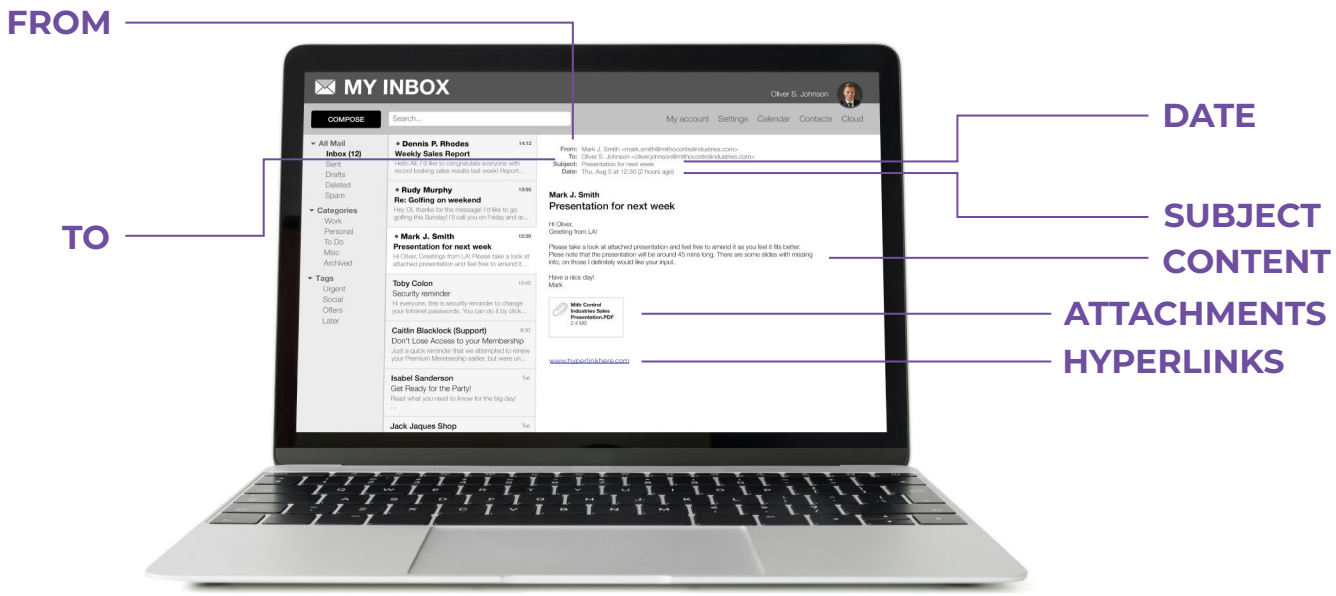
These two vectors alone account for 90 – 99% of cybersecurity risk in most environments.

> **91%**
> of all cyberattacks begin with a phishing email, and phishing techniquesare involved in 32% of all successful data breaches.
> *– Deloitte*

> **25%**
> of phishing emails bypass Office 365 security.
> *– Avanan*

How to Recognize a Phishing Email

There are many red flags to look out for if you suspect you are being phished. Clues can be found in every element of the email if you know what to look for. Here are some examples:



FROM

- Do you recognize the sender's email as someone you ordinarily communicate with?
- Is the email from someone outside of your organization, and is not related to your job responsibilities?
- Is it sent from someone within your organization, or a customer, partner, or vendor, but is unusual or very out of character?
- Is the sender's domain suspicious, like microsoft.support.com?
- Do you know the sender personally, or are they vouched for by someone you trust?
- Do you have a business relationship or past communication with the sender?
- Is this an unexpected communication that includes an embedded hyperlink or attachment from someone you have not communicated with recently?

TO

- Were you CC'd on an email sent to one or more people, and you don't personally know the other people it was sent to?
- Did you receive an email sent to a strange mix of recipients, for example, a random list of co-workers whose last names start with the same letter, or a list of unrelated addresses?

HYPERLINKS

- When you hover over a hyperlink in the email, is the link-to-address for a different website? (BIG RED FLAG!)
- Does the email only contain a long hyperlink with no other text or information?
- Did you receive an email that includes a misspelled web domain, for example, **www.bankofarnerica.com** – look closely, the m is really two characters, r, and n.

DATE

- When was the email sent? Did you receive an email at 3 a.m. that would normally get sent during business hours?

SUBJECT

- Does the subject line match the contents of the email?
- Is the email a reply to something I never sent or requested?

ATTACHMENTS

- Did the email include an unexpected email attachment or one that makes no sense in relation to the email?
- Is the attachment a potentially dangerous type of file?

CONTENT

- Is the sender asking you to take an action like clicking a link, opening an attachment to gain something of value, or avoiding a negative consequence?
- Does the email seem out of the ordinary, have bad grammar or spelling errors?
- Do you have an uncomfortable gut feeling about the sender's request?
- Is the email asking you to look at a compromising picture of yourself or someone you know?

Knowing what to look for and being diligent can help you to identify potentially dangerous emails before you have a problem. The first step to avoiding a breach is knowledge. Look for clues in every element of your email, from the sender's name and address to the date and time it was sent.

> “
> Distraction is the leading cause of employees clicking on phishing emails.
> *– Statista*

10 Common URL Tricks to Avoid

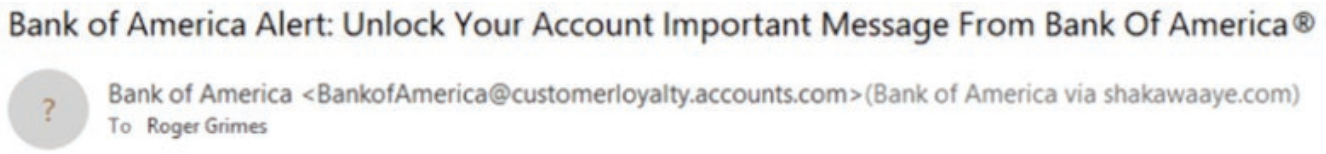
Cyber criminals often use a combination of elements to trick you into taking an action that can then compromise your system or network. Here are some common URL tricks a bad actor may include in the links embedded within their phishing emails.

1 Look-a-Like Domains

This is one of the most commonly used URL tricks. A phisher will use a look-alike domain containing the name of a well-known brand to gain trust.
For example **www.paypal.com.bank**, NOT paypal.com - the correct address.

2 Domain Mismatches

These are a red flag and a sign of malicious intent, not a trick. The phisher sends an email purportedly coming from a well-known brand, but it contains multiple domain names, none of which are related to the actual brand's domain.



3 URL Shortening

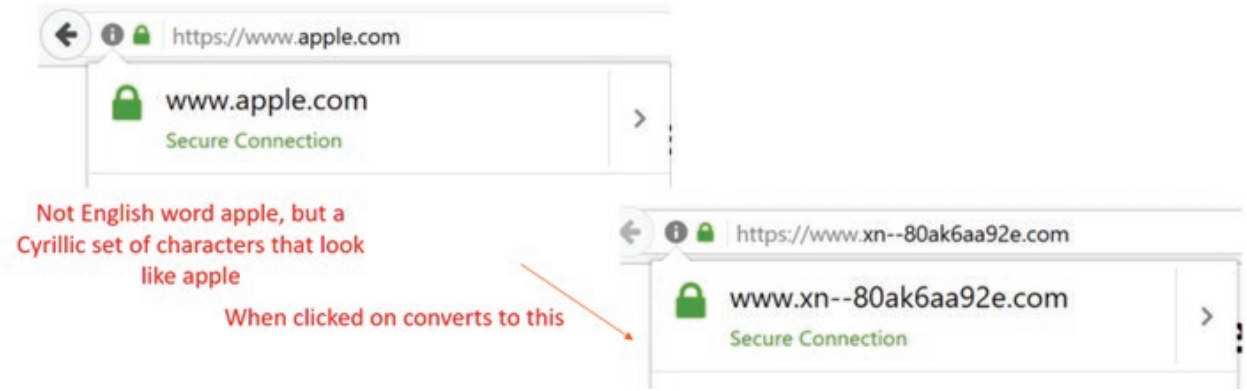
Many bad actors use URL shortening services, which convert longer, malicious URLs into shorter, innocuous URLs. This makes it harder for potential victims to investigate.

4 URL Character Encoding

URLs can be encoded in several different ways. The most common is called “percent escaping”. Each ASCII character is replaced with its hexadecimal digit counterpart and is followed by a % sign.

5 Homograph Attacks

This method uses another language's characters that look like similar characters in a different language. The new domain looks like a trusted brand but in fact has a completely different domain addresses. For example, the Latin “a” and Cyrillic “a” may look the same to a browser.



6 Overly Long URLs

Sometimes a cybercriminal will use overly long URLs with hundreds of random characters to overflow the screen when a browser hovers over the link to investigate. The idea is that the user will give up and just click on the malicious link prematurely.

7 Cross-Site Scripting

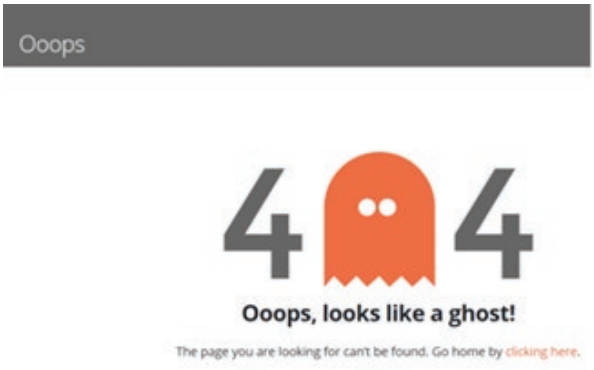
Cross-site scripting or XSS, is a method that uses HTML code that is meant to be displayed only or executed on a server, to execute code on a client instead. XSS code can be included in a URL, or more commonly, the URL redirects the user to a malicious page that then tries to execute the XSS.

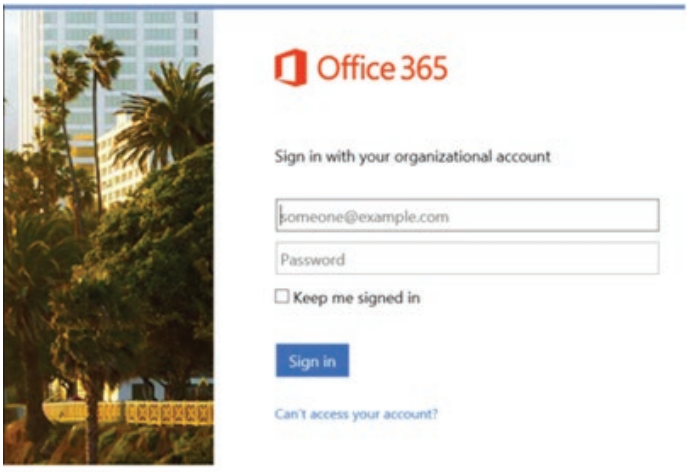
8 Malicious Redirect

Some innocent websites contain coding that allows their URL to be misused by hackers who use it to redirect victims to malicious locations. In this instance, the user investigating a URL would see and trust the originating domain, not knowing it is automatically sending them somewhere else.

9 Fake 404 Pages

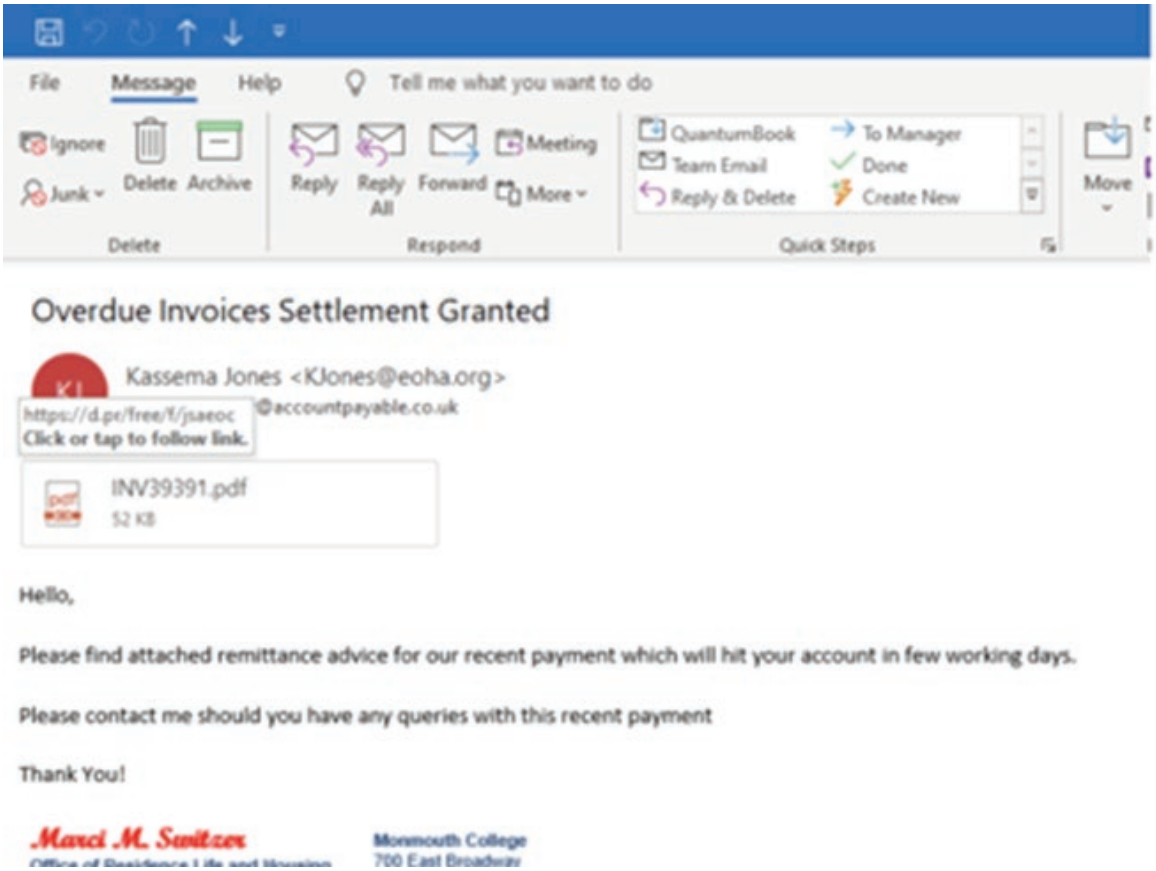
When someone asks for a web page or object that does not exist, they get a 404 error message that tells them that what they asked for doesn't exist. Bad actors will break into an otherwise innocent website and change the 404 error message to a redirect to a malicious website. Then they send out millions of phishing emails pointing to a non-existing object or page on the site, which then redirects the user to an even more malicious site.





10 Fake File Attachment Images

This is a relatively new scam over the past year or so. The use of fake file attachments which are really images with links to other objects hosted on a malicious website.



These are the 10 most common URL tricks that cyber criminals are using to redirect users to malicious websites where their systems may become infected with a virus or ransomware. While these tricks are a bit more difficult to spot than the common email elements we discussed earlier, with training and diligence, you can begin to see some of the red flags and avoid falling victim.

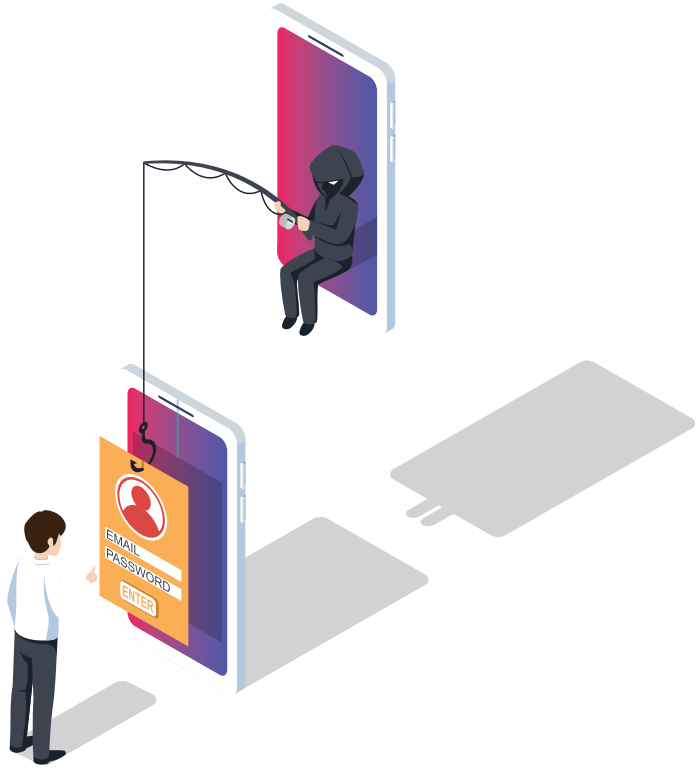
The bottom line, if you're not sure, don't click!

Employee Awareness Checklist

Your employees are the first line of defense against malicious phishing attempts. Training your team to recognize a phishing email and deal with it appropriately can add an important layer of protection to your business.

Here are some of the most important computing best practices that can help keep your business, team, and data safe from cyber criminals:

- ☑ **DO NOT** open emails if you do not know the sender.
- ☑ **NEVER** click on a link in an email if you are unsure. Only click on it if you know exactly where it is going.
- ☑ To add an additional layer of protection, if you do get an email from a source you are unsure of, navigate to the provided link manually by entering the legitimate website address into your browser.
- ☑ Look for, and check, the digital certificate of a website.
- ☑ If you are asked to provide any sensitive information, check that the URL of the page requesting the info starts with HTTPS, not just HTTP. The “S” stands for “secure.” It is not a guarantee that the site is legitimate, but most legitimate sites use HTTPS because it is more secure. HTTP sites, even legitimate ones, are vulnerable to hackers.
- ☑ If you believe that an email or link is not legitimate, take a name or some text from the message and put it into a search engine to check and see if any known phishing attacks exist using the same methods.
- ☑ Mouse over any suspicious links to check if it is legitimate before clicking on them.
- ☑ When in doubt, ask. If you receive a suspicious email from within your organization and you are unsure, check with someone to verify it. For example, if you receive an email from the CFO asking for sensitive information and you never correspond with that person, always verify the information before taking action!



hubTGI

Phishing Know-How: Where Does Your Business Stand?

Ask yourself these questions to gauge your phishing awareness:

01

Are you confident your team could recognize a phishing email?

02

Have you trained your people to detect email & online security threats?

03

Have you performed a phishing simulation test to inspect your team's readiness?

04

Have you implemented email security measures to minimize phishing emails?

05

Does your team realize the repercussions of a phishing attack on your business?

06

Do you have a plan in place should your business become a victim?

Did your answers to these questions give you a sense of confidence about your current security practices? Or perhaps it made you realize that it's time to revisit your security strategy.

We recommend all businesses undergo a data risk assessment, which is a review of how an organization protects its sensitive data and what improvements are needed. Organizations should conduct these assessments regularly to help identify information security and privacy control shortcomings and to reduce risk

Conclusion

Data breaches continue to rise with no signs of slowing down. This problem affects every business regardless of industry, or size. Phishing is popular among cybercriminals because it is much easier to get a human being to make a mistake than it is to infiltrate a network through hacking.

The good news is that you can significantly lower your risks if you practice safe computing best practices, and you know what to look for. Phishing emails and cybercrime are serious threats to every business. Stay diligent and educate yourself and your people on what to watch for and how to respond to keep your business and your information safe.

About Hub TGI

From a printed page to advanced IT services, we make you feel like a customer again.

Together we can help you leverage technology to control costs, boost productivity and secure your data. You benefit from insightful analytics, our long-standing vendor relationships and unsurpassed customer service that reaches from coast to coast.

hubTGI

416-747-1500

hubtgi.com