November 2018

What is "Phishing"? How does it attack you?

A Phishing Attack (pronounced "fishing") is an attempt from a bad guy to get your account information. It could be for your bank account or email account. Maybe a credit card or your Amazon account.

You may think that you are not susceptible to this type of attack, I mean who would readily give away their account info to a stranger or criminal? You would be surprised at how many people are tricked into giving away their information every hour.

And… do not use the same password for everything.

Who is being phished?

- According to PhishMe's Enterprise Phishing Resiliency and Defense Report, phishing attempts grew 65% in 2017.
- According to Wombat Security State of the Phish, 76% of businesses reported being a victim of a phishing attack in the last year.
- According to the Verizon Data Breach Investigations Report, 30% of phishing messages get opened by targeted users and 12% of those users click on the malicious attachment or link.
- According to the SANS Institute, 95% of all attacks on enterprise networks are the result of successful spear phishing.
- According to Symantec, phishing rates have increased across most industries and organization sizes — no company or vertical is immune.
- According to the Webroot Threat Report, nearly 1.5 million new phishing sites are created each month.

If you think your organization is safe from a phishing attack because you haven't yet been targeted, think again.

Your employees remain your organization's weakest security link.

Many, if not all, of your employees are unlikely to be able to spot a phishing email — according to Intel, 97% of people around the world are unable to identify a sophisticated phishing email.

Office 877.797.8776 support@viener4gates.com

What does a successful attack mean for your business?

In short, it's pretty devastating.

- According to Deloitte, one-third of consumers said they would stop dealing with a business following a cyber-security breach, even if they do not suffer a material loss.
- According to Aviva, after your company is breached, 60% of your customers will think about moving and 30% actually do.

Your brand image, and the brand trust that you've worked so hard to build up, can be obliterated if news of a data breach surfaces to the public.

Thankfully, defending against an attack is possible with dedication, buy-in, and resource allocation for defense tools.

How can you suspect the Email request is fake?

You can start with - Almost no one asks for you to provide information in an email format. Account changes are done through customer portals. Do not email your account info to anyone.

Here is a good one - Reading the email address that the reply is going to. If it looks funny, it is a fake. For example, a request from Microsoft will have a reply address of Microsoft.com. Not gmail, or outlook.com. Check who the response is going to.

Only open and reply to emails that are intended for you. For example, if you are not in the accounts payable department, do not reply or interact with requests for payments. It is most likely a phishing attempt.

Do you know any Roylaty? If the prince of (fill in the blank) country emails you for help moving millions of dollars, it is probably a fake.

Office 877.797.8776 support@viener4gates.com

Your Office365 Account

So many people use Microsoft's Office365 that a fake Office365 log-in has become one of the best ways to get unsuspecting people to give away their username and password information.

How the scam works is that you are emailed a link to a document. Usually the document is purported to be on a SharePoint site. When you click on the link to SharePoint, a fake Office365 login screen comes up. Users are so accustomed to the O365 login screen that they just type in their secure username and password. And BOOM, they have you.

It's not just email anymore

Phone scams and Text messages are now targets of Phishing Scams. That's right, if you get a text message from a number you don't know that reads "call me" – it could be a scam. There are numbers that are setup to charge you, real money, to call that number. They are like 888 numbers. If you call and get charged for it, you have been phished.

Phone scams have been around for years. They now deal with technology. A "representative" from Microsoft, Dell, etc. calls you and says that "someone is hacking your computer right now" and asks you to log on and give the so called representative access to your computer. It sounds very legitimate, the representative (who is a criminal) looks around and says everything is fine. The whole time they were searching your computer for account names and passwords or installing software that will allow them to access your computer and steal information. Very clever and effective.

What to do now?

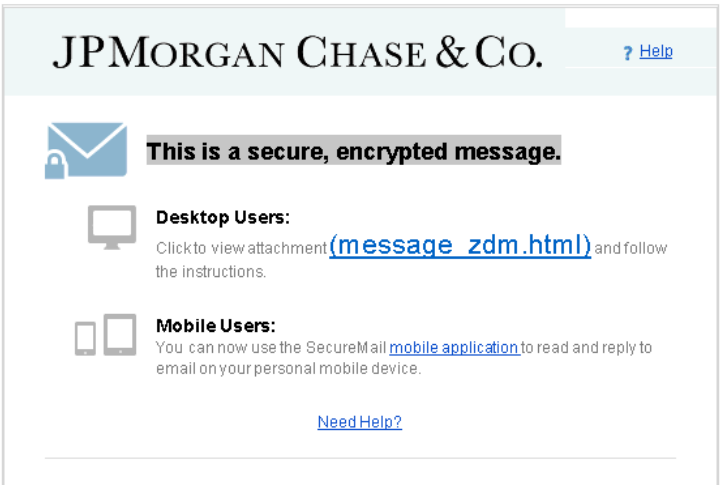
If you have been phished, first thing to do is change your passwords. Immediately get in-touch with your IT professional. You will need to run scans for penetration and malware.

The faster you get the issue straight, the less damage that can be done.

Office 877.797.8776 support@viener4gates.com

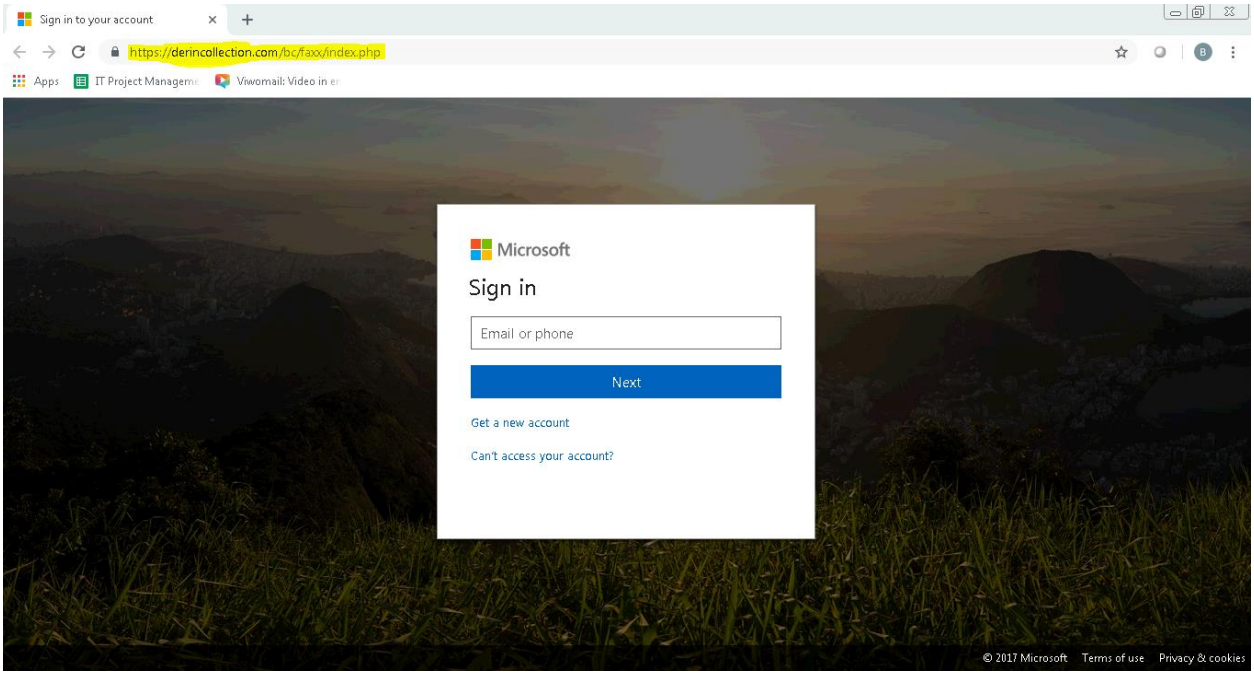
First Title – here are some examples that Ben sent over of screen shots of attempted phishing scams

From: Wilson, Lisa Maria [mailto:lisa.maria.wilsonfieldreply-fec7107371600d7d-12_HTML-14046593-7217344-39@echase.com]
Sent: Wednesday, November 14, 2018 3:53 PM
To: Wilson, Lisa Maria <lisa.maria.wilsonfieldreply-fec7107371600d7d-12_HTML-14046593-7217344-39@echase.com>
Subject: *FT-6898 -Final approved CD*



This is a fake JP Morgan Chase web site portal.

Office 877.797.8776 support@viener4gates.com



And here is a fake Microsoft portal login.

Office 877.797.8776 support@viener4gates.com