ThinkHR
Human Powered

CYBERSECURITY PART 1: PHISHERS ARE TRYING TO FOOL YOU

CYBERSECURITY PART 1: PHISHERS ARE TRYING TO FOOL YOU

Corporate networks in companies of all sizes are under siege by a growing number of increasingly sophisticated attacks from cyber criminals across the world. These attacks can happen at any time, both to your business or to you personally on your own private networks. There are steps you can take to reduce the risks as the first line of defense against data breaches, malware infiltration and various other security risks.

This is Part 1 in the series of prevention steps you can take to help make your information networks more secure.

Things have changed over the past few years…cyber criminals are now focusing increasingly on you and your fellow users as the weak link in the security chain.

You…

are the primary line of defense in preventing really bad stuff from happening in your company and to yourself.

There is nearly a one in four chance…

that you will mistakenly click on a phishing email.

One click on a phishing email…

could cost your firm $377 per employee.[1]

A single Trojan horse exploit…

caused the State of California to shut down a business a few days after the attack occurred.[1]

One stolen laptop…

from the car of an HR professional who worked for Godiva Chocolatier revealed the names, addresses, Social Security numbers and drivers' license numbers of other employees.[1]

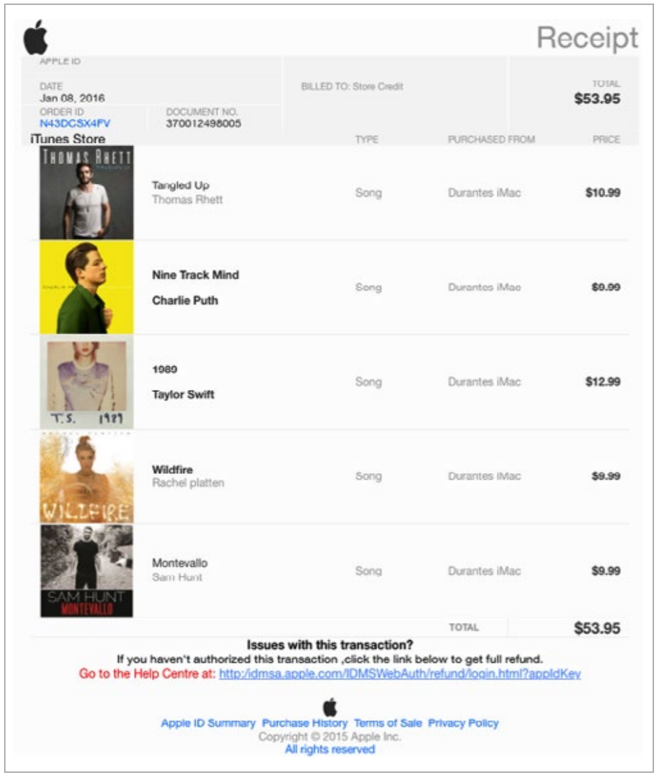
Edition: 4.2116

What Is Phishing?

A phishing attack is typically a bogus email, web page or social media post generated by a cyber criminal that pretends to be from a legitimate source. The goal of a phishing attack is to trick you into sharing sensitive or confidential information, such as login credentials, credit card numbers, financial account information or similar types of information.

Phishing is successful if it can fool you into believing that what you're seeing is genuine, particularly when it coincides with your expectations. For example, during your company's open enrollment period for healthcare benefits, it's logical that you would receive an email about your company's benefits package. Phishers know this and exploit this to their benefit by sending you messages that you would naturally expect to receive.

An important variant of phishing is **spearphishing**. While the ultimate goal of a spearphishing attack is identical to a phishing attack–i.e., stealing financial or other valuable information–a spearphishing attack is much more targeted, typically aimed at a small group of people within your company, such as C-level executives, members of a design team or others with highly sensitive information. A variant of spearphishing is "**whaling**," which tends to be even more highly targeted, sometimes focused on your CEO, COO or some other individual within a company. Cyber criminals who launch spearphishing or whaling attacks are typically after the most sensitive types of information, such as the login credentials to a company's financial accounts.



Receipt

APPLE ID

DATE
Jan 08, 2016

ORDER ID
N43DCSX4FV

DOCUMENT NO.
370012498005

BILLED TO: Store Credit

TOTAL
$53.95

iTunes Store	TYPE	PURCHASED FROM	PRICE
Tangled Up Thomas Rhett	Song	Durantes iMac	$10.99
Nine Track Mind Charlie Puth	Song	Durantes iMac	$9.99
1989 Taylor Swift	Song	Durantes iMac	$12.99
Wildfire Rachel platten	Song	Durantes iMac	$9.99
Montevallo Sam Hunt	Song	Durantes iMac	$9.99
		TOTAL	$53.95

Issues with this transaction?
If you haven't authorized this transaction ,click the link below to get full refund.
Go to the Help Centre at: http:/idmsa.apple.com/IDMSWebAuth/refund/login.html?appIdKey

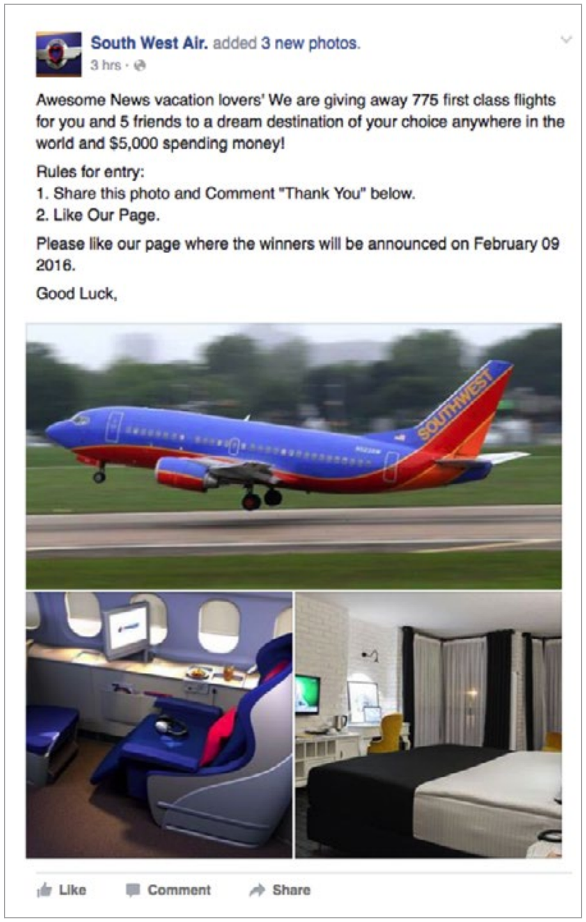
Apple ID Summary Purchase History Terms of Sale Privacy Policy
Copyright © 2015 Apple Inc.
All rights reserved

Figure 1: Phishing Attempt With a Bogus Apple iTunes Receipt
Source: Osterman Research, Inc.

Some Real-World Examples

Phishing and spearphishing can cost an organization hundreds of thousands of dollars and can actually put your company out of business. Here are some examples:

- An employee of Penneco Oil Company in Delmont, PA received a **phishing email** and either clicked on a link or opened an attachment within the email. This installed a keystroke logger that allowed cyber criminals to transfer almost $2.2 million from the company's financial accounts to a bank in Russia, and $1.35 million to a bank in Belarus. Cyber criminals attempted to transfer another $76,000 to a bank in Philadelphia shortly thereafter, but were not successful.[2]
- **CEO fraud**, a type of spearphishing attack, victimized The Scoular Company, an Omaha-based commodities trader. The controller of Scoular received an email that was supposedly from the company's CEO, instructing him to wire $780,000 to a bank in China, but instead the request came from a cyber criminal with email addresses in several different countries and servers operating in Moscow. The controller believed that the email was genuine and was instructed to keep the transaction secret so as not to violate Securities and Exchange Commission regulations. The initial request was followed by two more requests to transfer a total of $16.4 million, bringing the total theft to $17.2 million.[3]
- Efficient Service Escrow Group, a California-based escrow firm, was the victim of a **Trojan malware** infiltration that resulted in three wire transfers from their financial accounts to banks in Russia and northern China totaling $1.5 million. The transfer of $432,000 to the Russian bank was recovered, but the transfer of $1.1 million to the bank in China was not. California state law requires immediate disclosure of loss of funds for title and escrow companies, and so the company was given three days to replace the missing funds. Because they were not able to do so, the State of California shut the business down.



South West Air. added 3 new photos.
3 hrs ·

Awesome News vacation lovers' We are giving away 775 first class flights for you and 5 friends to a dream destination of your choice anywhere in the world and $5,000 spending money!

Rules for entry:
1. Share this photo and Comment "Thank You" below.
2. Like Our Page.

Please like our page where the winners will be announced on February 09 2016.

Good Luck,

Figure 4: Example of a Bogus Facebook Page
Source: Facebook

While these may seem like unusual examples, unfortunately they are not. Verizon analyzed 150,000 phishing emails from its partners and found that 23% of recipients open the phishing emails they receive and 11% open the attachments contained within them. Moreover, the length of time between the launch of a phishing attack until the first recipient responds to it is 82 seconds; one-half of phishing messages are opened in less than one hour.[4]

While email is the most common venue for phishing attempts, cyber criminals can also hijack pages on a website and make them appear to be valid, or post links on social media that will instruct users to “like” or otherwise interact with a social media site.

While email is the most common venue for phishing attempts, cyber criminals can also hijack pages on a website and make them appear to be valid, or post links on social media that will instruct users to “like” or otherwise interact with a social media site.

How to Defend Yourself

While cybercriminals are often very good at disguising their phishing emails, web pages and social media posts, there are things that you can do to reduce the likelihood of becoming a victim:

BE SKEPTICAL

First and foremost, be skeptical of any email, web page or social media post that appears to be even remotely suspicious, makes an offer that is too good to be true, or contains strange information. For example:

- In the bogus iTunes message shown on Page 3, the date on the email is January 8, 2016, but it was received on February 8, 2016. If you have ever ordered content from iTunes, you would know that Apple almost always emails receipts within two or three days from the purchase date. Moreover, the URL in the link near the bottom of the email does not match the URL in the tag that hovers over the address when the cursor is placed above it. An even more careful observation of the email reveals that the Apple logo appears slightly narrower than the Apple logo in a genuine iTunes receipt.
- The Facebook post on the previous page is slightly more obvious. For example, if you saw this post in Facebook you should question why Southwest Airlines would refer to themselves as “South West Air,” or why the airline would be giving away 775 first class flights and $5,000 in cash simply for “liking” their page. Plus, Southwest does not offer first class seats, probably would not advertise using an aircraft with their old color scheme, and they most certainly would not have first class seats with the logo of Malaysia Airlines on the television monitor.

Ask Questions

Since emails are the most common method for distributing phishing attacks, it’s important for you to ask some questions about any email you receive. Here are some good questions to ask:[5]

- Do you recognize the sender’s email address?
- Do you recognize anyone else copied on the email?
- Are others in the email seemingly from a random group of people, or do these recipients’ last names all begin with the same letter?
- Is the domain in the email address spelled correctly or is it simply close to the actual URL (e.g., bankofamerica.com vs. bankofarnerica.com).
- Would you normally receive an email from this individual?
- Does the subject line make sense?
- Is the email a response to an email you never sent (e.g., does it begin with “re:”)?
- Does the URL in the email (if there is one) match the URL in the tag when you hover over the link with your mouse cursor?
- Does the email contain an attachment that does not make sense in the context of the email or sender?
- Does the attachment end in “.exe,” “.zip” or some other possibly dangerous attachment type?
- Did you receive an email at an unusual time, such as 3 a.m. on a Sunday morning?
- Is the sender asking you to keep the contents of this email or any requests within it a secret?
- Does the email contain spelling or grammatical errors?
- Is there even a hint of extortion in the email, such as a request to look at compromising or embarrassing photos of you or someone else?

BE VERY CAREFUL WHEN REVIEWING YOUR QUARANTINED MESSAGES

If an email that seems to be valid has been captured by a spam quarantine, it is essential to be extremely careful before assuming it was mistakenly identified as spam and bringing the email out of quarantine. These “false positives” are not the norm, and so the spam quarantine that has captured a phishing email probably did so correctly.

DO NOT CLICK

Finally, you should never click on a link in an email or open an attachment until you are absolutely certain that the link or attachment is valid.

THINK!
DON’T CLICK!

References

1 http://www.privacyrights.org/data-breach

2 http://bigstory.ap.org/article/8c8160dc9a9449e8a962e6531e60311c/moldovan-bank-phishing-scheme-cost-drilling-firm-35m

3 http://www.omaha.com/money/impostors-bilk-omaha-s-scoular-co-out-of-million/article_25af3da5-d475-5f9d-92db-52493258d23d.html

4 Source: Verizon Data Breach Investigations Report

5 Source: KnowBe4 and Osterman Research, Inc.

About ThinkHR

ThinkHR provides expert HR knowledge solutions designed to help people and companies thrive. Combining the best of human expertise and innovative technology, ThinkHR's solutions include the industry's first and most used HR hotline, an award-winning online HR knowledge base, and a comprehensive eLearning platform.

ThinkHR's mission is to give its partners a powerful competitive advantage to help them strengthen their client relationships, manage risk and win more business. Equally important, the company is passionate about empowering HR professionals and other executives to become more efficient, productive and successful.

For more information, visit thinkhr.com

ThinkHR
855.271.1050
contact@thinkhr.com

About Osterman Research

Osterman Research provides timely and accurate market research, cost data, cost models, benchmarking information and other services to technology-based companies. We do this by continually gathering information from IT decision-makers and end-users of information technology through in-depth market research surveys. We analyze and report this information to help companies develop and improve the products and services they offer, and to help organizations make better decisions about their security, archiving and other capabilities.

For more information, visit ostermanresearch.com.

This document is offered for general best practice information only. It does not provide, and is not intended to provide, legal advice.