Focus On...

Helping you bring your organization into focus.™

January 2021 • Volume 11, Issue 01

CYBER

How to Avoid the Phishing Bait in 2021

What can be the cruelest but most effective way to test your employees [to see] if they are aware of the risks and preventions of a phishing attack? GoDaddy, the world's largest domain registrar and web-hosting company, simulated a phishing test for employees to increase alertness levels against phishing attacks.

On December 14, an email tucked underneath the snowflake banner with the words "GoDaddy HOLIDAY PARTY" from Happyholiday@Godaddy.com" was sent to hundreds of GoDaddy employees offering a holiday bonus. The message in the email said, "2020 has been a record for GoDaddy, thanks to you!"

"Though we cannot celebrate together during our annual Holiday Party, we want to show our appreciation and share a $650 one-time Holiday bonus!" it further added.

To ensure that the recipients receive the bonus, they were asked to fill in [their] personal details by December 18. But instead of receiving the bonus, two days later, almost 500 employees received an email from the company's Chief Security Officer, Demetrius Comes.

GoDaddy is not the first company this year to provide phishing email awareness for employees. Earlier this year, Tribune Publishing, a giant newspaper company in America, sent out a similar phishing email to [their] employees.

The email, circulated by several employees on Twitter, said the company was providing targeted bonuses between $5,000 to $10,000, only to find out later that it was a phishing test sent from the company.

Why Should Organizations Run Employee Phishing Tests?

Imagine the consequences, if GoDaddy's phishing test was not a test but a real phishing attack from a hacker! Roughly 500 employees failed the test, so, almost 500 of them would have submitted their personal information to hackers. This could have led to a complete disaster for the company.

Providing this kind of real scenario phishing attacks helps employees understand what the falsified email might look like [and] how it can trick them into falling for the scam by offering some incentive or creating a sense of urgency. The test helps the employees in recognizing phishing emails as well as to avoid and report it.

According to phishing statistics, in 2020, 97% of the users are unable to recognize a sophisticated phishing email. This is probably why phishing attacks, Business Email Compromise (BEC) attacks and other email-based attacks are rapidly increasing every passing year. In fact, BEC attacks yielded the most profit for cybercriminals in 2020.

How to Detect Phishing Attacks

Phishing attacks today have evolved and become more sophisticat-

Inside This Issue

[*Cyber:* How to Avoid the Phishing Bait in 2021]

[*Compliance:* Landmark BSA/AML Legislation Enacted]

[*Awareness:* Securing Wi-Fi at Home]

Focus Audits will be closed on Monday, January 18, 2021 in observance of Martin Luther King Jr. Day.

FOCUS AUDITS™

CYBER

ed than ever before. These attacks are becoming increasingly difficult to differentiate between a legitimate email and a fake email. But here are a few ways that your organization can follow to detect phishing attacks and protect your organization and employees against phishing attacks:

Email domain name
It is advisable to always check the name, email address and [to] make sure no alterations (additional letters or numbers) have been made in the email domain or the email address. For example, a legitimate email address might be john@business.com but an altered email address can be john@busineess.com or john@busiiness.com. If you are receiving an email from an unknown organization, then you can also check the organization's domain name by [searching for it in an internet search engine].

Sensitive information and sense of urgency
A legitimate company or any government agency would never ask you to send your sensitive information over email. So, if an organization is asking you to send your credentials or personal information like username or password through email, it is recommended to not send it and get the mail verified personally. Moreover, most of the time, scammers create a sense of urgency, because if there is not much time left, you don't have enough time to think or cross-check. But you do not want to be in a hurry when it comes to losing your personal information.

Poor spellings and grammatical errors
You can often spot a phishing email if it contains poor spelling and grammar errors in the message. Legitimate companies have qualified and trained employees to write emails and the emails are double-checked before the emails are sent out to their staff or clients. So, if a message has poor spelling or grammar errors, it's always better to cross-check if the email is from a legitimate company.

Too good to be true or designed to make you panic
It is common for phishing emails to offer a coupon for free stuff or to instill panic. The email message will either be offering some rewards which you were not expecting or will create panic by claiming that your account is compromised. To receive the reward or to secure your compromised account, you will need to verify you are the legitimate person by either giving out your credentials or by entering your login details. The common goal of both messages is to get your credentials or personal information.

Suspicious links or attachments
Phishing emails come in many different forms but no matter how the email is delivered to you, it always comes with a gateway. It can either be a link to redirect you to a bogus website or an attachment that you are asked to download. No legit companies will randomly send you links or attachments and if they want you to download something then it will be from the official website.

How to Prevent Phishing Attacks
Your email spam filters might help you keep away numbers of phishing emails from landing in your inbox, but malicious actors are constantly finding ways to outsmart spam filters; so it is highly recommended to add extra layers of protection against phishing attacks. Here are some steps your organization can implement:

1. Protect devices by keeping software up to date with the latest security updates and patches.
2. Enforce strong password policy, passwords that are not easily guessed and avoid sharing passwords.
3. Add an extra layer of security for passwords with multi-factor authentication.
4. Encourage employees to report suspicious emails.
5. Routinely backup confidential or important data on an external hard drive or cloud storage and also encrypt all sensitive company information.

Source: *Security Boulevard, Richard Singha, January 5, 2021*

Focus On..

COMPLIANCE

Landmark BSA/AML Legislation Enacted

The National Defense Authorization Act was enacted by Congress on January1, 2021, and includes language which contains long sought BSA/AML legislation.

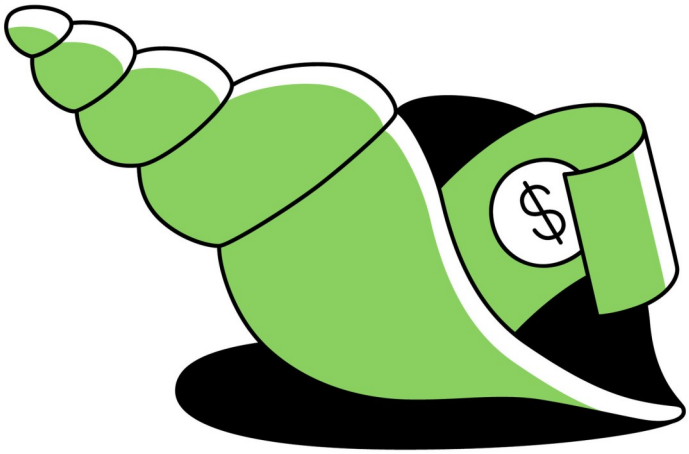
For the first time, shell companies – often used as fronts for criminal activity – are required to disclose their true owners to the U.S. Department of Treasury. This signals a shift of the burden financial institutions have long shouldered. The Treasury Department has a year to issue regulations spelling out the finer points of how companies need to comply.

Nearly 2 million corporations and limited liability companies are registered each year in the U.S., at the state level. Few states required companies to disclose their true owners.

Many new companies created in the U.S. will immediately have to disclose the name, birth date, address, and a government-issued identification number - such a driver's license number or passport number - of the company's beneficial owner. Existing companies have two years to comply. Companies only must update the information when there is a change in ownership.

The Act contains a long list of exemptions meant to limit its scope to the entities most likely to be used for illicit purposes. Banks, broker-dealers, public issuers, insurance companies, nonprofits, public accounting firms, and others are exempt, as are entities with more than 20 full-time employees and $5 million in revenue, and operate in the United States, which are deemed more likely to be real, legitimate businesses.

Those who fail to disclose their ownership or provide false information face fines of up to $10,000 and up to two years imprisonment. The legislation also establishes a new FinCEN whistleblower program for financial crimes.



AWARENESS

Securing Wi-Fi at Home

Overview
To create a secure home network, you need to start by securing your Wi-Fi access point (sometimes called a Wi-Fi router). This is the device that controls who and what can connect to your home network. Here are five simple steps to securing your home Wi-Fi to create a far more secure home network for you and your family.

Focus on The Basics
Often the easiest way to connect to and configure your Wi-Fi device is while connected to your home network. Point your web browser to the specific IP address documented in your device's manual (an example of this would be https://192.168.1.1), or use a utility or mobile app provided by your Wi-Fi device vendor.

1. **Change the Admin Password:** Your Wi-Fi access point was most likely shipped with a default password for the administrator account that allows you to change the device configuration. Often these default passwords are publicly known, perhaps even posted on the Internet. Be sure to change the admin password to a unique, strong password, so only you have access to it. If your device allows it, change the admin username as well.

2. **Create a Network Password:** Configure your Wi-Fi network, so it has a unique, strong password as well (make sure it is different from your device admin password). This way only people and devices you trust can join your home network. Consider using a password manager to select a strong password and to keep track of all of your passwords for you.

3. **Firmware Updates:** Turn on automatic updating of your Wi-Fi access point's operating system, often called firmware. This way you ensure your device is as secure as possible with the latest security options. If automatic updating is not an option on your Wi-Fi access point, periodically log into and check your device to see if any updates are available. If your device is no longer supported by the vendor, consider buying a new one that you can update to obtain the latest security features.

4. **Use a Guest Network:** A guest network is a virtual separate network that your Wi-Fi access point can create. This means that your Wi-Fi access point actually has two networks. The primary network is the one that your trusted devices connect to, such as your computer, smartphone, or tablet devices. The guest network is what untrusted devices connect to, such as guests visiting your house or perhaps some of your personal smart home devices. When something connects to your guest network, it cannot see or communicate with any of your trusted personal devices connected to your primary network.

5. **Use Secure DNS Filtering:** DNS is an internet-wide service that converts the names of websites into numeric addresses. It is what helps ensure your computer can connect to a website when you type in the website's name. Wi-Fi access points typically use the default DNS server supplied by your internet service provider, but more secure alternatives are available for free from services such as OpenDNS, CloudFlare for Families, or Quad9 that can provide extra security by blocking malicious or other undesirable websites. Log into your Wi-Fi access point and change the DNS server address to a more secure alternative.

Securing your home Wi-Fi access point is the first, and one of the most important, step in creating a secure home network. For more information about securing your Wi-Fi access point, refer to the device's manual, or if your internet service provider provided your Wi-Fi device, contact them for more information on security features.

Source: *SANS OUCH! Newsletter*
Joshua Wright, Senior Director, Counter Hack Challenges, LLC

Focus Audits, LLC
11301 N. US Hwy. 301
Ste. 105
Thonotosassa, FL 33592
(813) 638-8565
www.FocusAudits.com