DON'T BE A SUCKER

8 THINGS YOUR EMPLOYEES SHOULD UNDERSTAND

DON'T BE A SUCKER! "PHISHING" AWARENESS

"PHISHING"

WWW.JECTECH.CO.ZA

CONTENTS

INTRODUCTION

Hackers today are sophisticated, the times of sloppy, phishing emails are gone. They are sly, and highly skilled at concealing their attacks from users and email filters. They select their victims carefully and conduct extensive research before launching attacks. Security awareness training is highly recommended but as users get busy, they are bound to let their guards down. Your business at risk for a breach, when this does happen.

Hackers use a number of techniques to mimic the look and feel of an email from a known brand, including using legitimate brand logos, images, and call-to-action buttons.

1. PHISHING EXPLAINED

PHISHERS IMPERSONATE THE BRANDS YOU TRUST THE MOST

Over 20 years ago, phishers selected victims at random, sending phishing campaigns to many recipients. To improve their success rate, phishers now research their targets and find out the brands that victims are related to , including banks, software and app vendors, e-commerce companies, and more.

In 2019, the most impersonated brands ranged from cloud services companies to financial corporations, to streaming companies. What they all have in common is a trusted, instantly recognizable brand and a large pool of victims to choose from, such as PayPal / Facebook / small banks / Netflix, even Office 365.

A hacker sends an email that appears to come from Microsoft asking the user to log in to their Office 365 account, a common example of a phishing attack, in the email is a link which the user clicks on, it takes them to a "factious" Office 365 login page. The Microsoft branding and logos both in the email and on the phishing page, an untrained user will not recognize the email as a phishing attempt.

2. VERIFY EMAIL ADDRESSES

Cybercriminals have many methods to disguise emails. They trick their victims into thinking a sender is legitimate, when the email is really coming from a malicious source. The most common types of spoofing are visible alias spoofing and cousin domains.

So, what is **EXACT SENDER SPOOFING?** The hacker creates a replica of a brand's email address. Also known as domain spoofing, this method is less common than other types of spoofing, because it is easy for most email filters to detect due to DMARC (Domain Message Authentication Reporting) and DKIM (DomainKeys Identified Email).

When a hacker displays the brand's name and email address in the sender field of the email, this is known as **DISPLAY NAME SPOOFING**. This is the most common form of spoofing, and it is effective because many users look only at the sender's name and not the email address.

The company may be legitimate name as the email sender, such as microsoftsupport@microsoft.com, but the email underneath is a random address like xyz@yahoo.com, not always noticed by the busy recipient.

The most effective is visible alias spoofing, when a user views the email on a mobile device because the sender's email address is often hidden. Phishers count on the fact that most mobile users will not expand the sender's name to view the email address.

CLOSE COUSIN SPOOFING, a hacker creates an email address that is close enough to the real thing to fool users, through extensions, such as co, company, ca, and ml are added to the end of email addresses to create the illusion of a brand's domain.

Hackers will use extensions to trick users, some examples include apple-support.org, apple-logins.net, and apple-securities.com. We are also seeing an increase in lengthy, confusing subdomains, such as icloud.accounts@apple.it.support.zqa.ca.

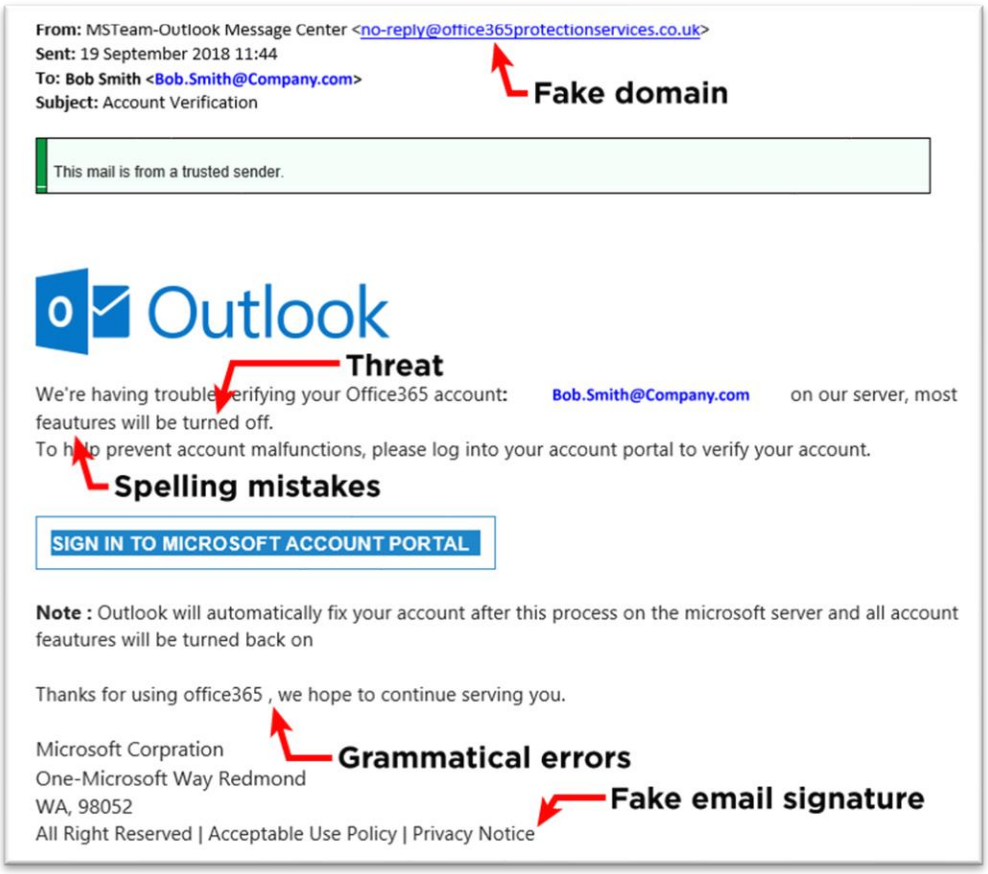

Figure 1: *Example of "Spoofing"*

3. SUBJECT LINES AND EMAILS MESSAGES

Cybercriminals may promise "free iPhones to the primary 100 respondents" or threaten that "your mastercard are going to be suspended without immediate action." Evoking a way of panic, urgency, or curiosity may be a commonly used tactic. Users are typically quick to reply emails that indicate potential loss or that would end in personal or gain .

Emails that have an aggressive tone or claim that immediate action must be taken to avoid repercussions should be considered a possible scam. this system is usually wont to scare people into abandoning tip . Two samples of this are phishing emails telling users their critical accounts are locked or that an invoice must be paid to avoid services being suspended.

In some spear phishing attacks, personalized emails from purported colleagues are designed to evoke fear of consequences at work. A classic example of this is often an urgent email from a CEO requesting gift cards or a wire transfer. Receiving such an invitation from a baron creates pressure

for the worker and makes them more likely to reply quickly—without thinking it through. Another example is that the direct deposit spear phishing email, which is meant to pressure an HR employee into changing direct deposit information.

4. ATTACKS ARE TARGETED—AND PERSONAL

Many phishing attacks of the past were sent in bulk to an outsized group of users directly , leading to impersonal greetings. The emails would often address a user with a generic term like “customer,” “employee,” or “patient.” Your employees should take care of those terms, because professional organizations commonly address users by their given name in email, but a customized email isn't a sure sign of a legitimate email. Today’s phishers are including the victim’s name within the subject line and prefilling the victim’s email address on the phishing webpage.

5. PHISHING EMAILS EVOLUTION

The earliest phishing cases transpired quite 20 years ago. within the beginning, fake emails were pretty easy to detect. Starting within the '90s, phishing attackers targeted the AOL users (History of AOL). Phishing attacks progressed into sending automated campaigns to people to steal their credentials.

Employees got to read their emails carefully, not just skim them. Many phishing attacks and spear phishing attacks are launched from other countries, and although this will end in glaring grammar and stylistic issues, phishers became more sophisticated. they need the resources to compose clean emails in their target language, and that they make fewer mistakes. during a recent Office 365 phishing page discovered by Vade Secure, there was just one discrepancy between the important Office 365 page and therefore the phishing page: an additional space between “&” and “Cookies” within the “Privacy & Cookies” link within the footer of the phishing email.

6. LINKS AREN’T ALWAYS WHAT THEY SEEM

Every phishing email includes a link, but phishing links are deceptive. While the link text might say “Go to Office 365 account,” the URL takes the user to a phishing page designed to seem like Microsoft. confirm your employees hover over all links before clicking them to ascertain the pop-up that displays the link’s real destination. If it's not the web site expected, it's probably a phishing attack.

It is most vital to form sure that the core of the URL is correct. Be especially cautious of URLs that end in alternative domain names rather than .com or .org. Additionally, phishers use URL shorteners, like Bitly, to bypass email filters and trick users, so take care of clicking on shortened URLs. IsItPhishing.AI can determine if a URL is legitimate or a phishing link. If you or your employees are unsure of the legitimacy of an internet site, IsItPhishing.AI can determine if a URL is legitimate or a phishing link.

7. BE WARY OF ATTACHMENTS

All phishing emails contain a link, but it’s not always within the email. To avoid detection by email security filters, hackers will include a phishing link in an attachment, like a PDF or Word doc, instead of the body of the e-mail . and since sandboxing technology scans attachments for malware, not links, the e-mail will look clean. the e-mail itself will appear to be from a legitimate business, vendor, or colleague, asking you to open the attachment and click on on the link to review or update information.

8. HACKERS USE REAL BRAND IMAGES AND LOGOS

In less sophisticated phishing attacks, phishers might include a single image in the phishing email, typically a poor-quality logo, which is easy for users to detect.

Sophisticated phishing pages also leverage high-quality images to achieve the look of authenticity. Very often, it is nearly impossible for the average user to tell the difference between a quality phishing page and authentic brand webpage.

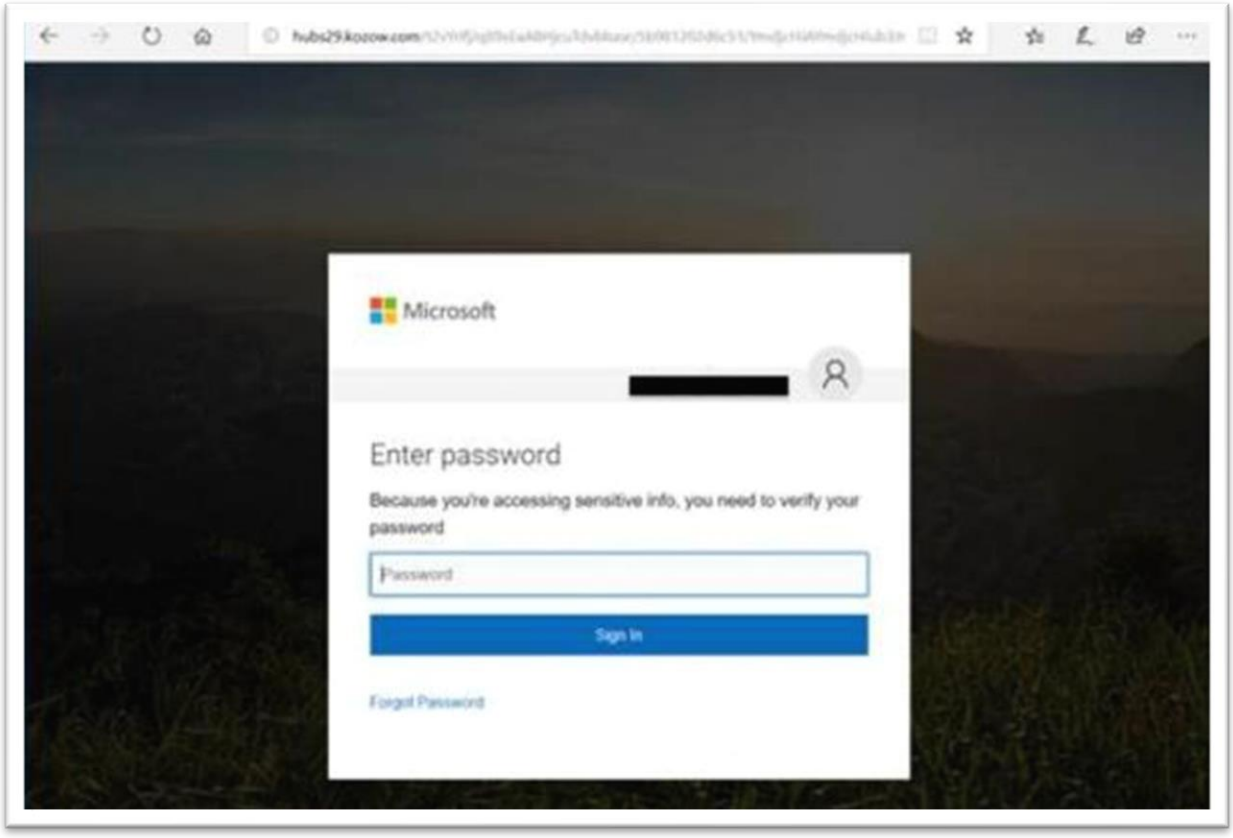

Figure 2: *"PHISHING PAGE" Visually this page appears identical to the legitimate Microsoft 365 login. The hacker copied CSS from the real Microsoft 365 landing page and inserted it into the code of the phishing page to achieve the visual authenticity and fool the end user.*

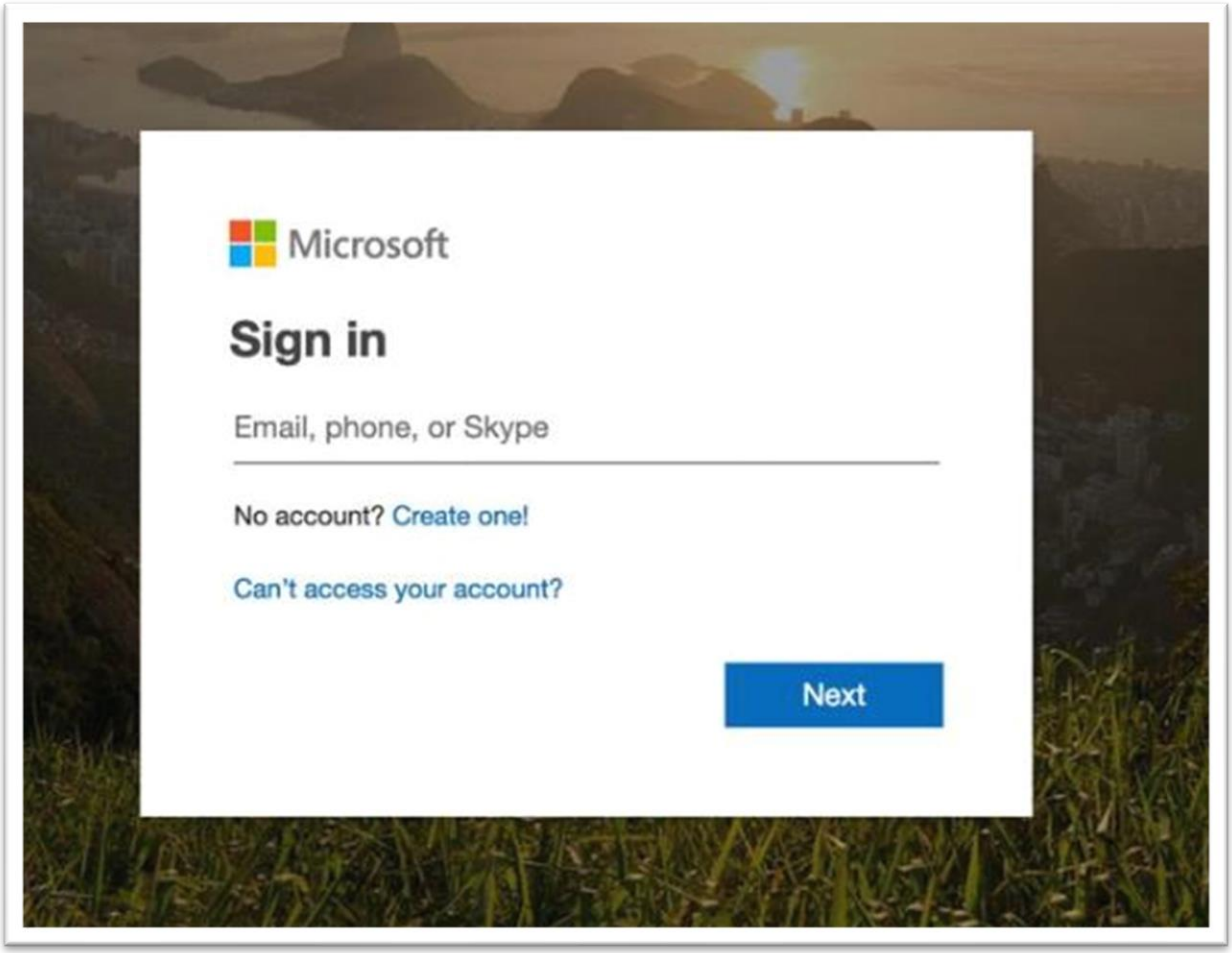

Figure 3: *Real Office 365 Page*

Brand logos and trademarks are no guarantee that an email is real. These images are public and can be downloaded from the internet or easily replicated. Even antivirus badges can be inserted into emails to persuade victims into thinking an email is from a legitimate source. While most email filters can spot a known phishing URL, they cannot spot a counterfeit image unless they have machine learning and computer vision capabilities.

9. AN EMPLOYEE RECEIVED A PHISHING EMAIL—NOW WHAT?

Dealing with the repercussions of a phishing attack is not only time consuming but costly. One careless click has the potential to compromise your entire network, so it is important that everyone works as a team to protect the company.

Make sure there is a system in place to report attacks, and make sure all of your employees understand how important it is to follow through in reporting it. Deleting the offending email is not the solution—IT needs to know that your company is being targeted.

Train your employees to contact your IT department immediately so that IT can take appropriate action and create a feedback loop to help improve the email filter. While structured annual or semi-annual training is recommended, employees should also receive on-the-fly training when an attack occurs.

If an employee clicks on a phishing link, they should receive immediate feedback and additional training. Review the email with them, show them the red flags and indicators they missed, and provide additional training materials to help them avoid being phished in the future.

10. ADDITIONAL RESOURCES

Phishing 101 Video

Social Engineering 101 Video

Infosec 101 Video

Avoid_Phishing_EN (2).pdf

11. REFERENCES

https://www.vadesecure.com/en/phishing-awareness-training-8-things-employees-understand/

https://www.intelligentcio.com/africa/2019/10/14/south-africa-among-top-20-countries-targeted-in-new-phishing-influx/

https://www.phishingbox.com/products-services/security-awareness-training/phishing-awareness-training