Vade Secure
Predictive Email Defense

Phishing Attacks

Advanced Techniques That Evade Detection

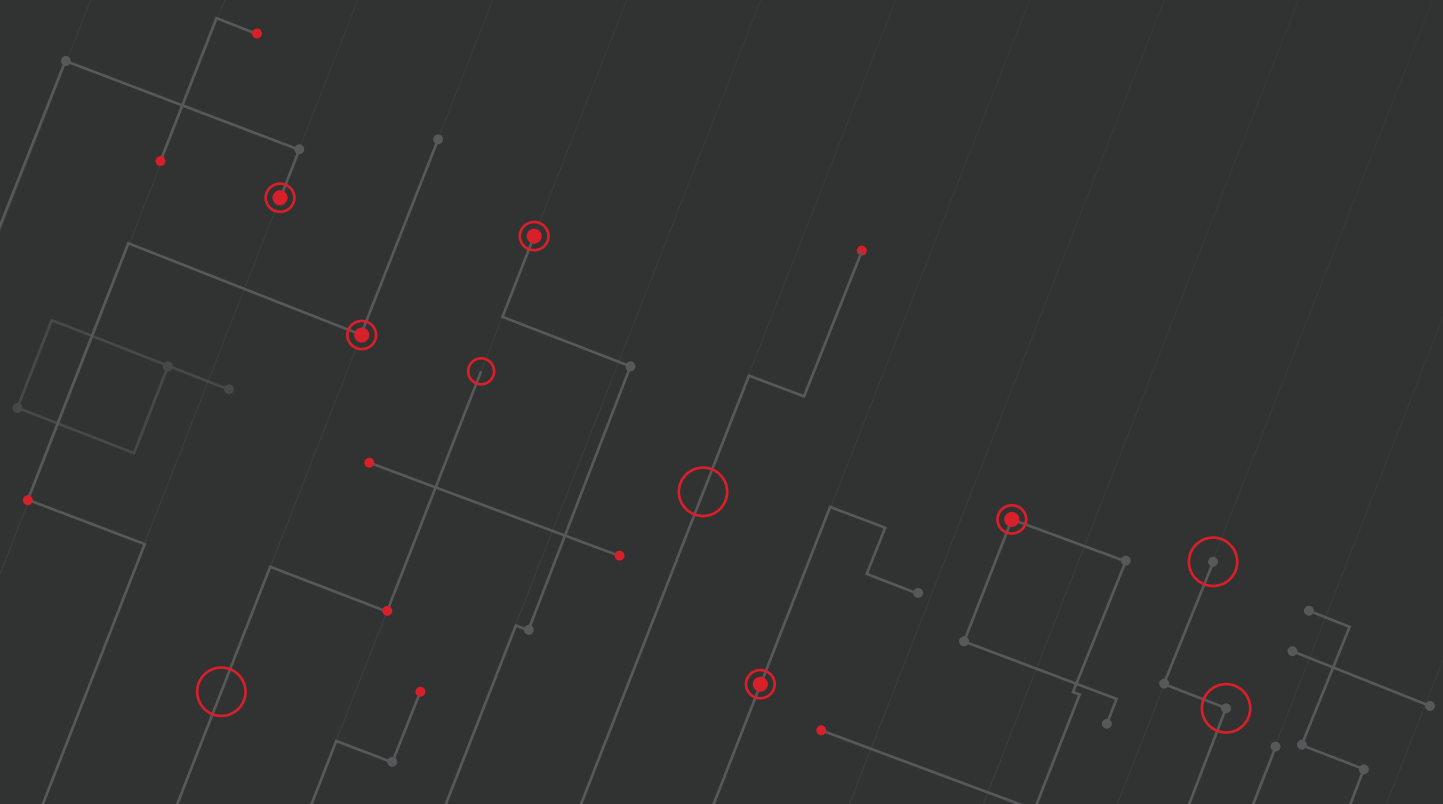


TABLE OF CONTENTS

INTRODUCTION

The days of sloppy phishing emails are gone. Hackers today are sophisticated, 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. Even with security awareness training, busy users are bound to let their guards down. When they do, it puts your business at risk for a breach.

Phishing/social engineering is the #1 cyberattack reported by SMBs. [1]

As phishers hone their techniques and focus on more targeted attacks, they have shifted their focus from enterprises to SMBs. While they might offer bigger payouts when a breach is successful, enterprises are more difficult to penetrate due to big IT budgets and extensive IT staff. For SMBs, the threat is real, it's growing, and attacks are becoming harder to detect.

66% of SMBs experienced a cyberattack in the past 12 months. [2]

PHISHERS IMPERSONATE THE BRANDS YOU TRUST THE MOST

In the past, phishers selected victims at random—if at all—sending phishing campaigns to hundreds, even thousands of recipients. To improve their success rate, phishers now research their targets and discover the brands that victims are associated with, including banks, software and app vendors, ecommerce companies, and more.

The most impersonated brands of 2019 range 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.

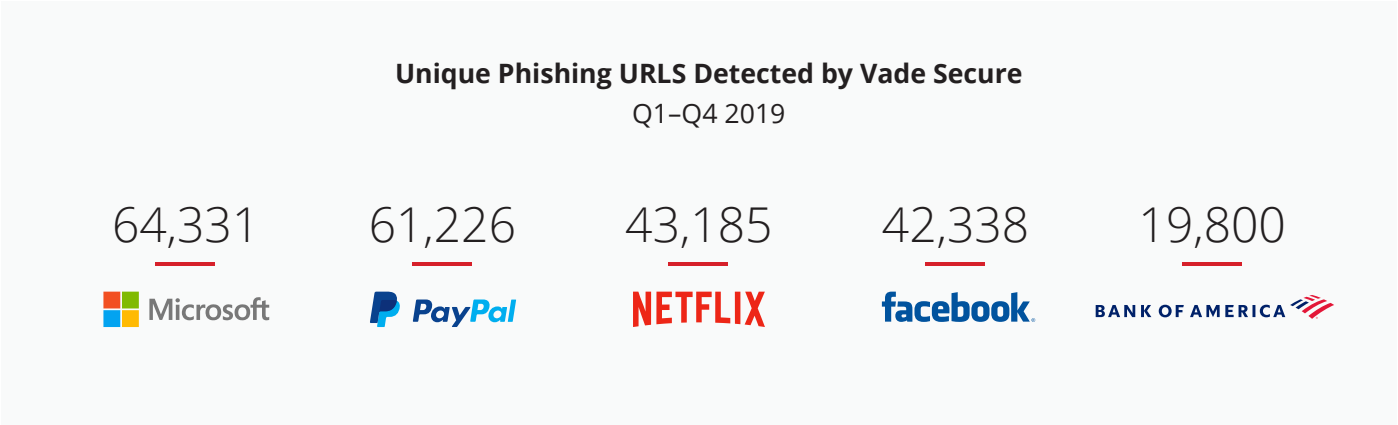


Figure 1: Unique phishing URLs refers to the number of phishing pages detected, not the total number of phishing emails sent.

[1] Keeper Security, Inc. & Ponemon Institute, LLC. 2019 Global State of Cybersecurity in Small and Medium-Sized Businesses. October 2019.

[2] Ibid.

PHISHING TECHNIQUES

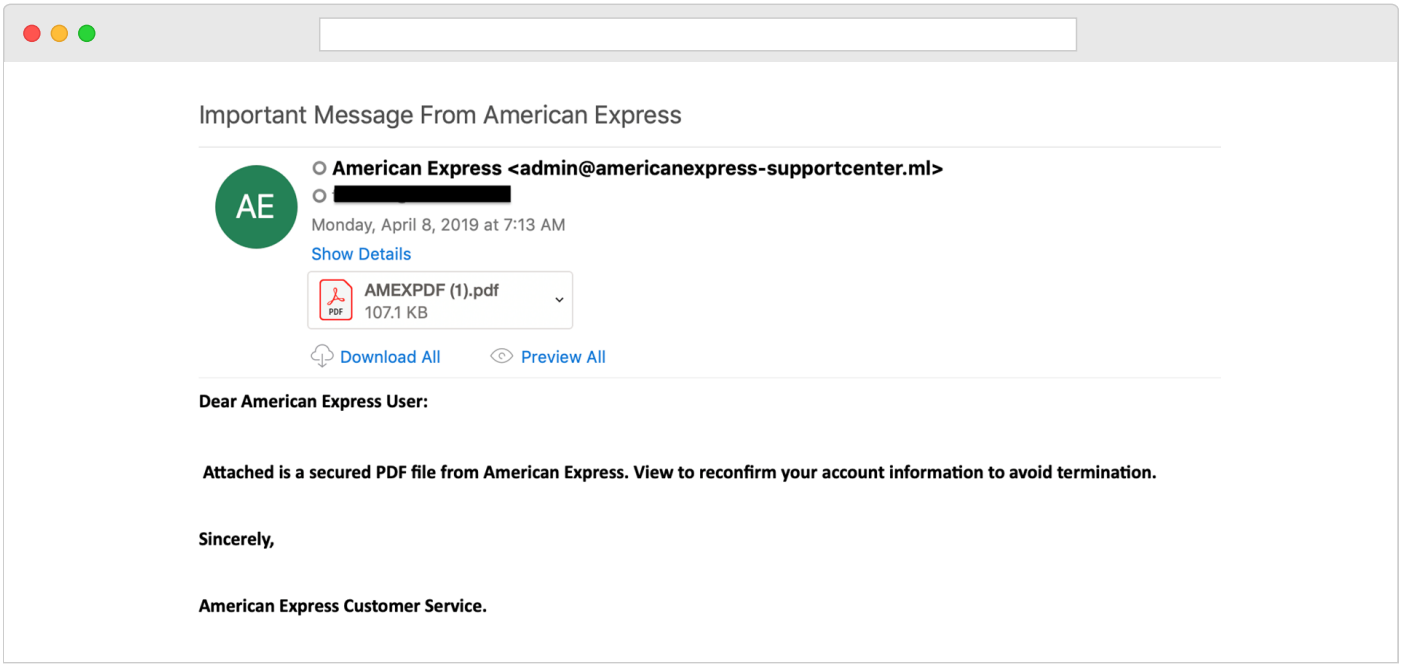
Hackers use a number of techniques to mimic the look and feel of an email from a known brand, including using legitimate brand logos, images, and call-to-action buttons. While clean copy might add to the authenticity of a phishing email, it is the technical aspects of phishing emails that convince users they are from a trusted brand.

SPOOFING EMAIL ADDRESSES

Exact sender spoofing is a technique in which a hacker creates a replica of a brand's email address. Also known as domain spoofing, exact sender spoofing 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).

With display name spoofing, a hacker displays the brand's name and email address in the sender field of the email. Display name spoofing 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. It is especially effective on mobile devices because the email address is often hidden and the sender field must be expanded to reveal the sender's email address.

With close cousin spoofing, a hacker creates an email address that is close enough to the real thing to fool users. For example, 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.



Another method of spoofing is to include Cyrillic (Russian) letters in the email address, making it a challenge for a filter to distinguish between similar characters, such as the Cyrillic letter 'a' and the Latin letter 'a'.

Examples:

americanexpress.com ⤮ **americanexpress.com**

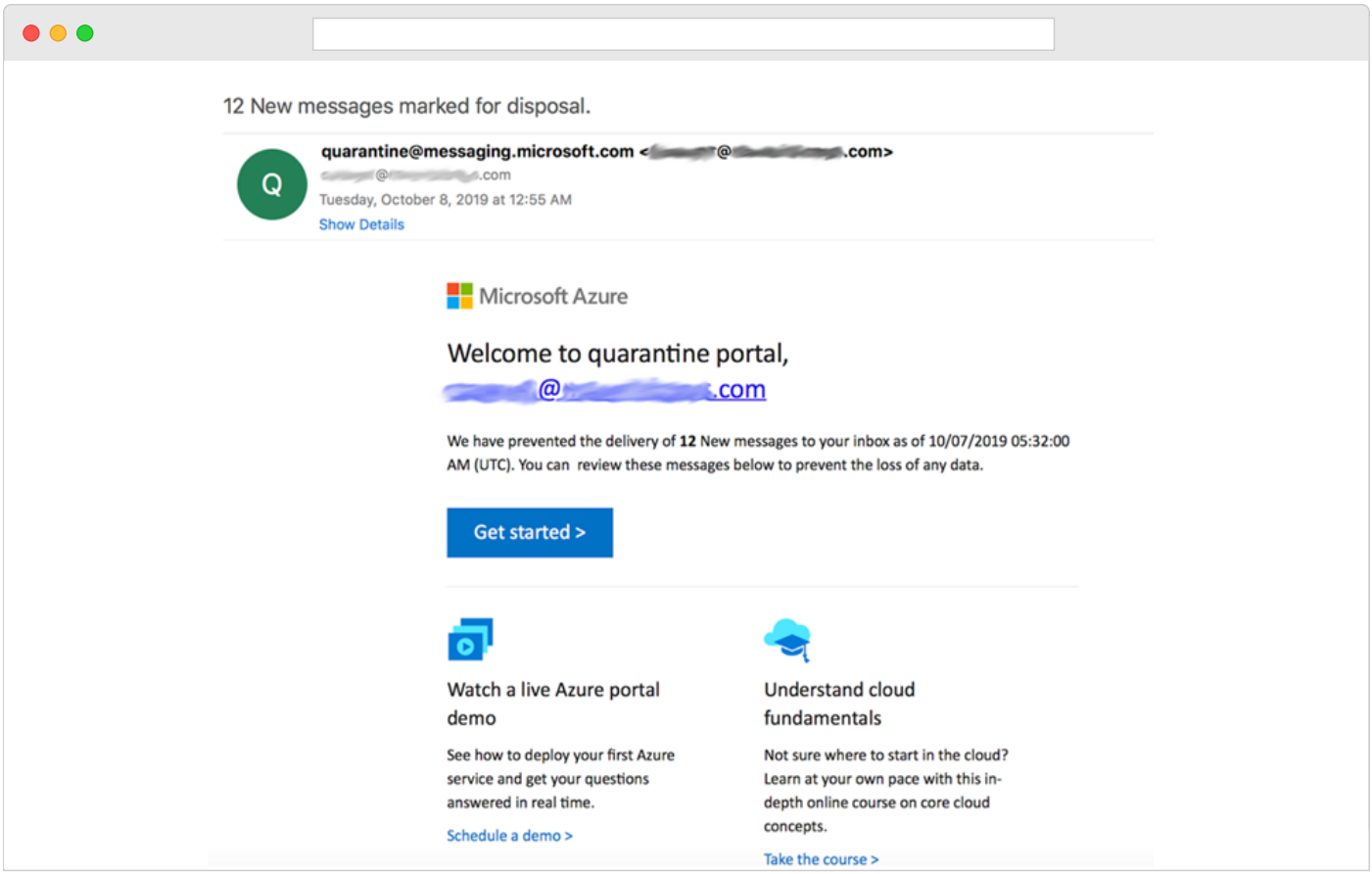
microsoft.com ⤮ **microsoft.com**

Why do spoofed emails bypass filters?

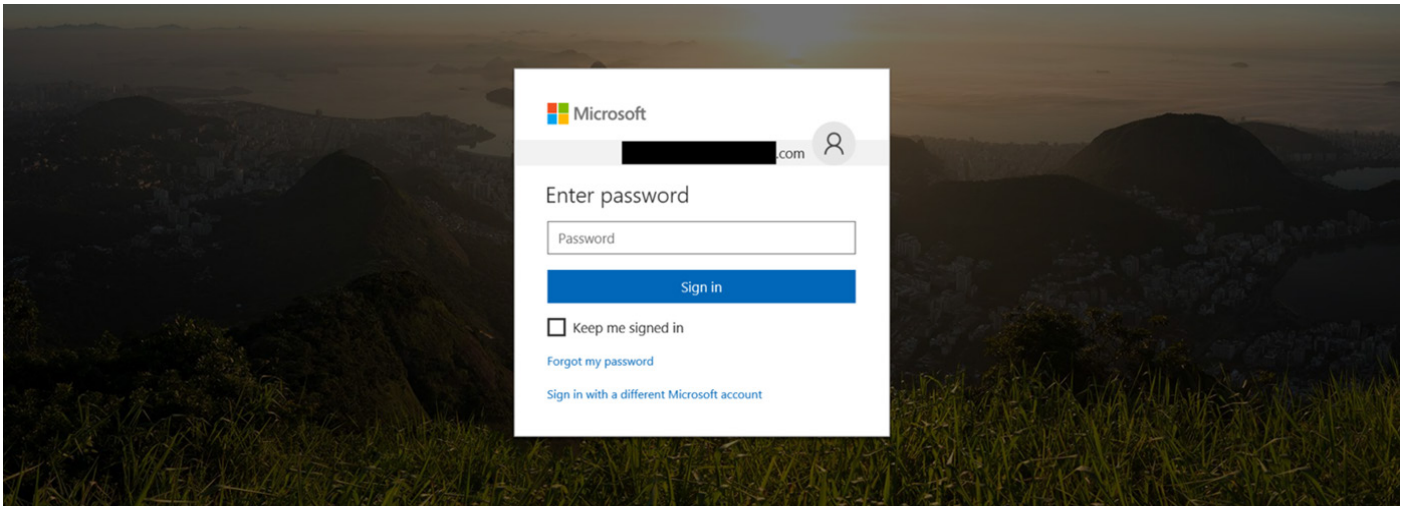
Traditional filters are searching for senders with a bad reputation; e.g., IPs that are known to send high volumes of spam and domains that are known to host phishing webpages. If IPs and domains are unique, unknown to a filter, and have good reputations, the spoofing attempt could bypass a filter.

USING 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. In sophisticated attacks, images are used throughout the email, adding to the authenticity and increasingly the likelihood that a user will believe the email is legitimate. Often, the brand's logo has been manipulated slightly to bypass filters that can recognize an image by its signature (cryptographic hash), but these changes are not visible to the naked eye.



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.



Office 365 Phishing Page

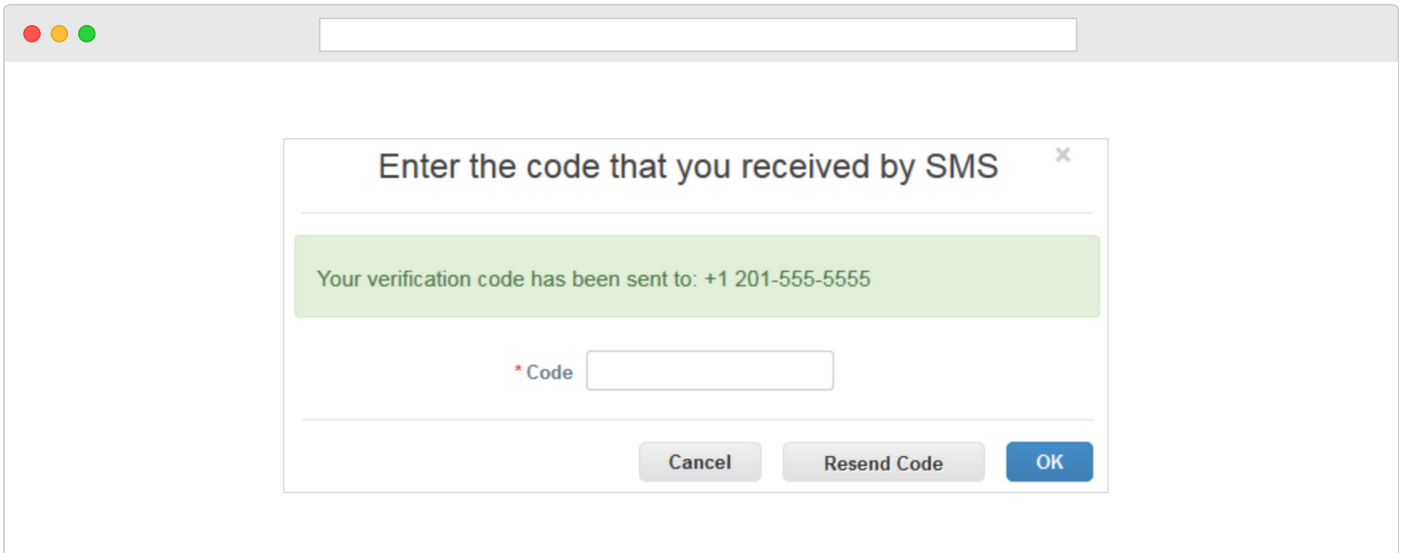
Visually, the above image appears identical to the legitimate Office 365 login page. The hacker copied CSS from the real Office 365 landing page and inserted it into the code of the phishing page to achieve the visual authenticity and fool the end user.

> **"I reported this phishing email last week? Why did I receive it again?"**
>
> Most filters are scanning for reputation (IP, domain) and signatures (code)—but they cannot see an email like a human can. While visually the email might be an exact replica, hackers will make subtle changes to the signature to convince a filter that the email is unique—thereby passing the scan.

EXPLOITING AUTHENTICATION TOOLS

Two-factor authentication (2FA) is one of the best defenses against credential theft and is a well-known form of authentication. Users have become accustomed to authenticating with 2FA and trust that their accounts are being protected when they are prompted to authenticate with 2FA.

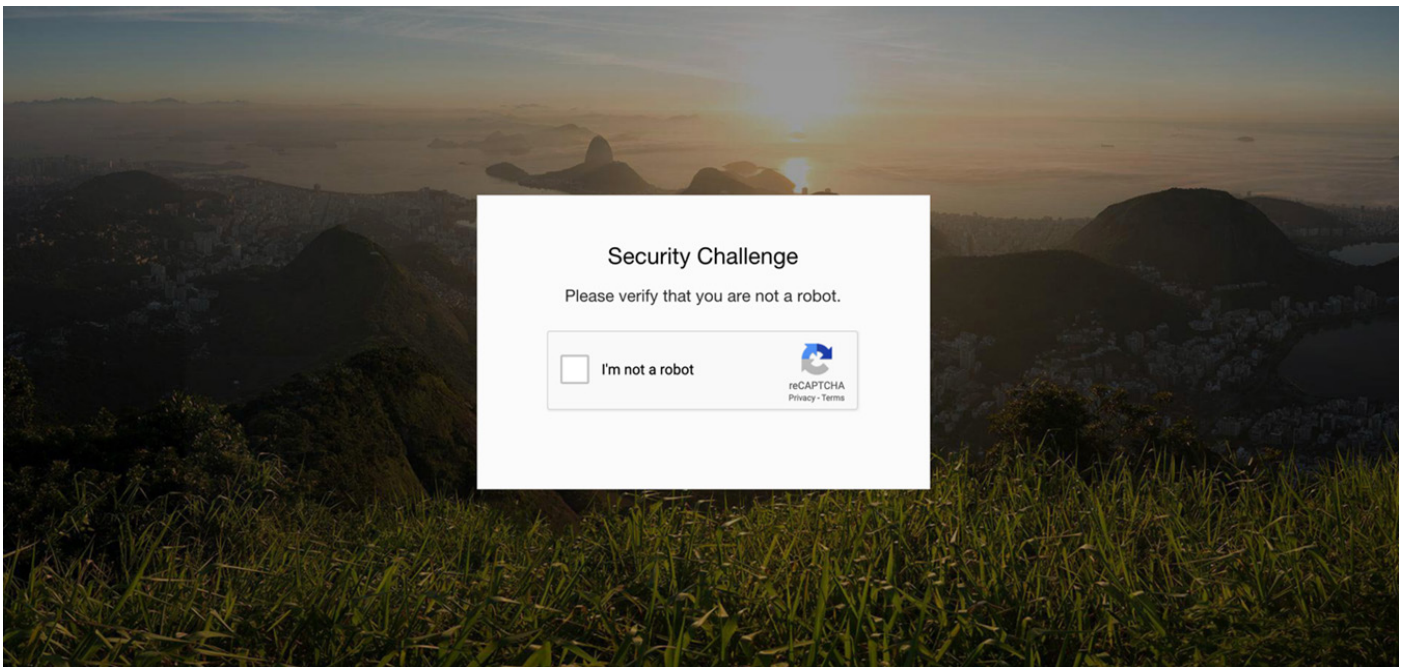
To take advantage, hackers arm phishing pages with fake 2FA pop-ups designed to steal credentials rather than protect them. When a user enters their login credentials on a phishing page, the credentials are immediately stolen by the hacker. When the hacker attempts to log in to the user's real account, it prompts an authentication code to be sent to the user's mobile phone. The fake 2FA pop-up then appears on the phishing page, and the user enters the code to verify their identity. The hacker now has the 2FA code to access the victim's real account.



In another example of a 2FA exploit demonstrated by security expert, Kevin Mitnick, a hacker copied a session cookie from a developer tool in an internet browser when the victim entered their authentication credentials with 2FA. A hacker can then paste that session cookie into a browser and access the victim's account.

Designed to protect websites from bots, CAPTCHA and ReCPATCHA tests are other forms of authentication. Again, users are accustomed to seeing these authentication methods, and when they do, they tend to trust that they are being protected.

Recent phishing attacks detected by Vade Secure feature fake CAPTCHAs and ReCAPTCHAs designed to fool users into thinking that a webpage is secure. Whether the user passes or fails the CAPTCHA test is irrelevant, because the CAPTCHA is designed only to make the phishing page appear authentic.



How can you tell if an authentication method is legitimate?

Look for long, complicated URLs and URLs with country codes that do not match the country of origin for the legitimate website. Also note whether the pop-up is a working or non-working form. Often, when you enter credentials on a non-working form, the form will lead to nowhere.

OBFUSCATING URLS AND URL STUFFING

If an email contains a known phishing URL, the email will be blocked by a filter. This presents a problem for a phisher and one that can be solved with URL obfuscation. With a URL redirect, a legitimate method of directing outdated webpages to new ones, a phisher can insert a URL from a known, trusted brand into an email and add a URL redirect to point the URL to a phishing page.

URL shorteners, which not only shorten URLs but create aliases of them, are also used to obfuscate URLs and confuse filters. A known phishing link with a normal URL structure has no resemblance to a shortened version of the URL.

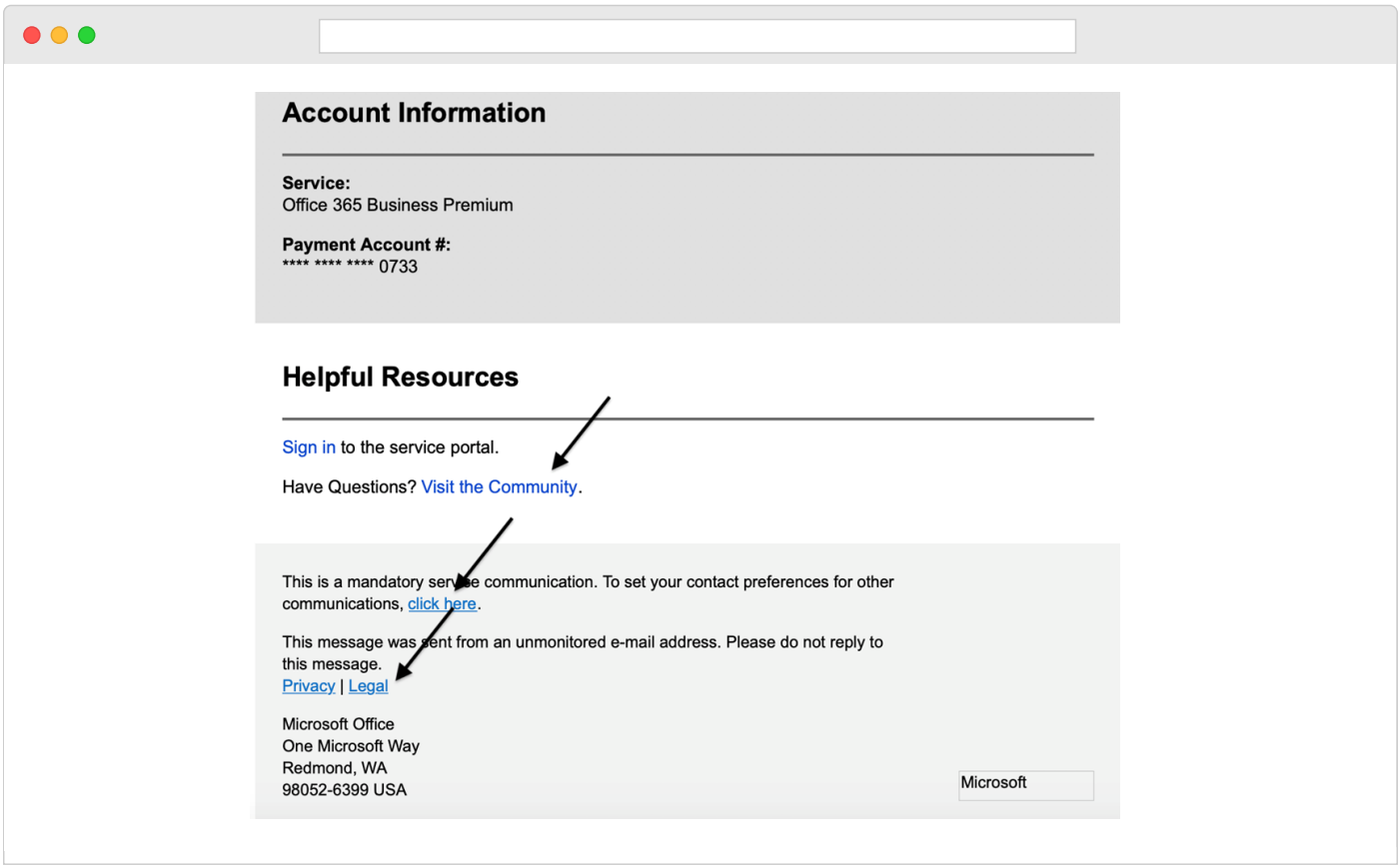
Example:

Original URL: **https://vadesecure.com**

Shortened URL: **https://bit.ly/2P9wh7n**

Concealing the URL in a QR code is a method of bypassing both URL blacklists and algorithms that can detect images and objects but cannot extract hidden URLs. The phishing URL behind the QR code typically directs a user to a Bitcoin website where they are instructed to make their ransom payment.

URL stuffing is a method of including numerous legitimate URLs in an email in addition to the phishing URL. Often, the phishing URL will be the final URL in the email. The hope, for the hacker, is that the email filter will render the email safe after identifying a handful of legitimate URLs from trusted brands.



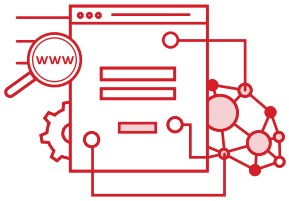
Legitimate Microsoft URLs

How can I spot a phishing URL?

Hover over all URLs in the email to see where they lead. Authoritative brands typically use short, clean URL structures without excess characters. If you click the URL, make sure the URL on the resulting landing page is the URL you expected. Or when in doubt, type the brand's website directly into your browser.

HOW VADE SECURE BLOCKS ADVANCED THREATS

Vade Secure's anti-phishing technology uses artificial intelligence to block targeted attacks at the time of delivery and the time of click.

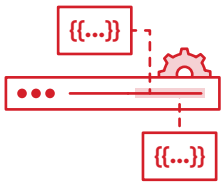


Feature analysis

Supervised machine learning models explore the email content, including meta data, HTML, and attachments, scanning for known phishing URLs, domains, and signatures. This initial scan, which analyzes 47 features of an email, is done at the time of delivery.

Time-of-click analysis

To protect from URL redirects, shorteners, and time-bombing techniques that might have bypassed the initial scan, unsupervised machine learning models also scan the URL at the time of click, following the URL to the ultimate webpage and analyzing the webpage.



Token randomization

To protect from sleeper pages and dynamic links, URL tokens are randomly replaced while the AI engine scans the URL for malicious content. During this process, the tokens will not trigger tracking of the user or action on the URL.

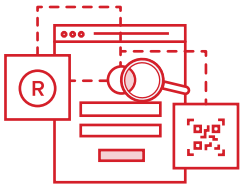


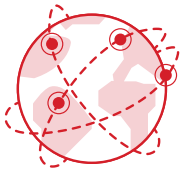
Image and object detection

Deep Learning models with Computer Vision analyze images within the email, including logos from the top 30 impersonated brands, to identify any changes a hacker might have made to bypass signature-matching technology.

The Computer Vision models are also trained to recognize QR codes, which are common in sextortion emails and which conceal URLs within the image. The Computer Vision models extract the URLs and analyze them to render a verdict.

Mobile rendering analysis

To protect from phishing attacks that are designed specifically to take advantage of mobile users, algorithms explore webpages across 30 device-browser combinations to identify threats that are visible only on mobile devices.



Regional page exploration

Webpages are explored from four zones to identify phishing pages that are displayed only when accessed in a certain region. Page exploration covers the North America, South America, Europe, and Asia.

Continuous, adaptive phishing protection

The best defense against phishing is a combination of user training and anti-phishing technology. The better trained a user is, the more likely they are to report suspicious emails. Training should occur not only during formal security awareness training but also when a user clicks on a phishing link, which provides context and connects the incident to the training.

Phishing attacks are always evolving, and new threats are discovered daily. Vade Secure's machine learning models are continually trained with new threat data generated by user reports from our customers, from phishing URLs reported to IsItPhishing.AI, and through 24/7 analysis of the more than 600 million mailboxes protected by Vade Secure. As new threats are discovered and analyzed, the models are revised and updated to identify and block the latest threats.

To learn more about Vade Secure's anti-phishing technology, visit:

vadesecure.com/en/solutions/anti-phishing

Vade Secure
Predictive Email Defense