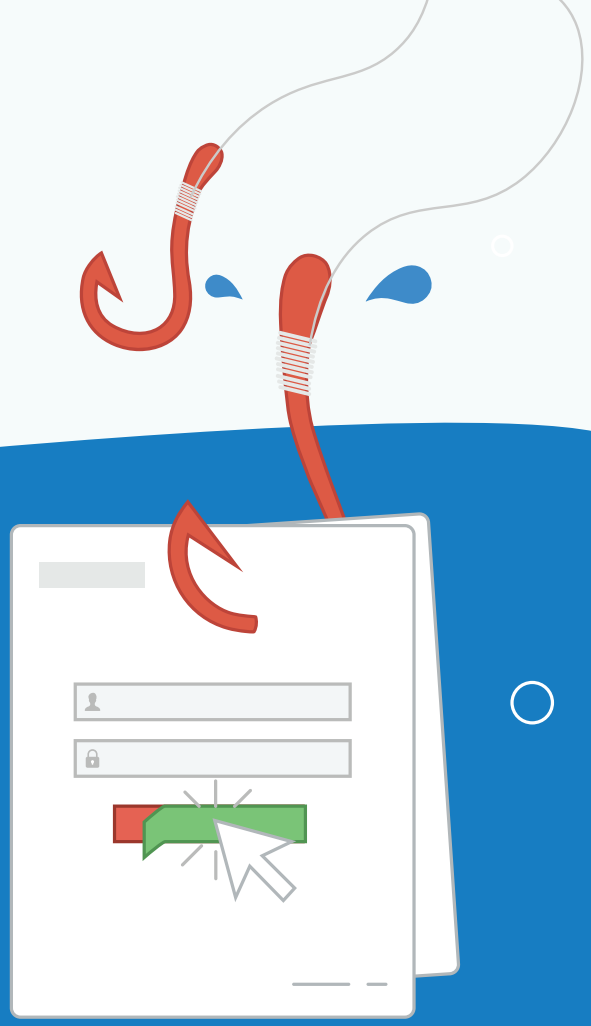
Phishers' Favorites

2019 Year-in-review



Vade Secure
Predictive Email Defense

www.vadesecure.com

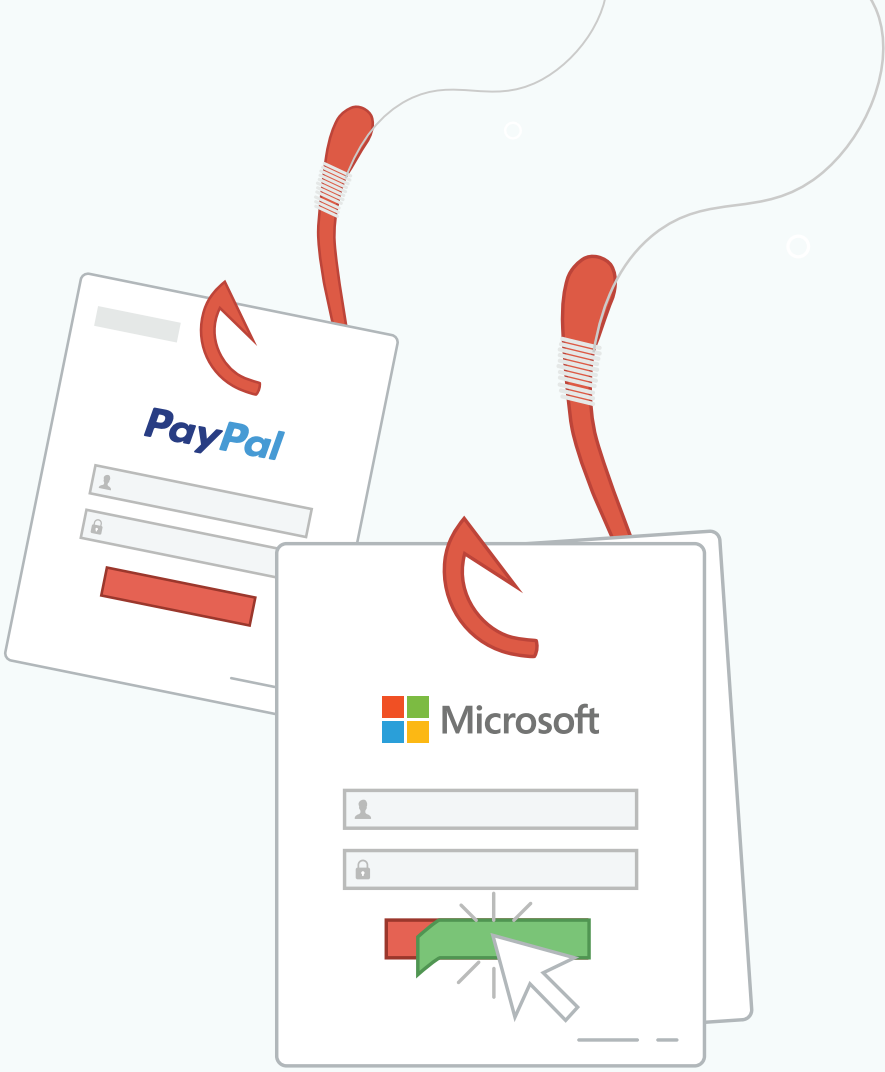
TABLE OF CONTENTS

Phishers' Favorites 2019 Year-in-review 3

- Microsoft and PayPal Are Phishers' Favorite Targets 3
- The 20 Most Impersonated Brands in Phishing Attacks 4
- The rise of Office 365 makes Microsoft the top target for corporate phishing 6
- PayPal emerges as a phishers' favorite 7
- Netflix is growing in popularity 9
- Social media phishing grows 11
- Financial services represents the most phishing URLs 13
- Sophisticated phishing emails replace sloppy attacks 14
- Timing is everything 18

Sophisticated phishing attacks require sophisticated defenses 20

PHISHERS' FAVORITES 2019 YEAR-IN-REVIEW



Microsoft and PayPal Are Phishers' Favorite Targets

Phishers' Favorites is Vade Secure's quarterly report highlighting the top 20 most impersonated brands in phishing attacks. Our inaugural year-in-review looks at the top 20 most impersonated brands of 2019 and explores key phishing trends from the year, including the role of Office 365 in Microsoft phishing, the rise of PayPal impersonation, and the sophisticated email attacks phishers are using to lure corporate email users.

Each quarter, Vade Secure's filter engine detects and analyzes tens of thousands of unique phishing URLs. Unique phishing URLs refers only to the number of URLs and not the volume of phishing emails received. Hackers will often send dozens or more phishing emails containing the same phishing URL.

The 20 Most Impersonated Brands in Phishing Attacks

For the second year in a row, Microsoft was the most impersonated brand of the year, with more than 64,000 unique phishing URLs detected in 2019. PayPal followed closely behind and even surpassed Microsoft in Q3 and Q4 2019, with more than 61,000 URLs for the year.

This shift in rankings marked a first since Vade Secure started publishing Phishers' Favorites in 2018. Microsoft ranked #1 for six straight quarters between 2018 and 2019. Netflix placed third in our annual ranking, with more than 43,000 phishing URLs, making it one of two cloud companies in the top 10.

The 20 Most Impersonated Brands in Phishing Attacks

#	Brand	Unique Phishing URLs	QoQ Growth
1	- Microsoft Category: Cloud	64,331	-11.9%
2	- PayPal Category: Financial Services	61,226	85.5%
3	- Netflix Category: Cloud	43,185	68.3%
4	- Facebook Category: Social Media	42,338	83.9%
5	↑1 Bank of America Category: Financial Services	19,800	34.0%
6	↑7 Apple Category: E-Commerce/Logistics	12,222	100.3%
7	↑21 CIBC Category: Financial Services	8,616	399.5%
8	↑3 Chase Category: Financial Services	7,075	-14.8%
9	↑1 DHL Category: E-Commerce/Logistics	7,030	-22.2%
10	↑17 Amazon Category: E-Commerce/Logistics	6,909	238.3%
11	↑9 Credit Agricole Category: Financial Services	6,010	49.4%
12	- Dropbox Category: Cloud	5,967	-27.4%
13	↓5 Docusign Category: Cloud	5,665	-48.7%
14	↑38 WhatsApp Category: Social Media	5,231	956.8%
15	↑47 Desjardins Category: Financial Services	4,540	1680.4%
16	↑1 Adobe Category: Cloud	4,191	-24.0%
17	↓2 Google Category: Cloud	4,076	-31.2%
18	↓13 Wells Fargo Category: Financial Services	3,941	-74.5%
19	↑5 Yahoo Category: Internet/Telco	3,841	22.7%
20	↓11 Orange Category: Internet/Telco	3,751	-59.6%

The rise of Office 365 makes Microsoft the top target for corporate phishing

Topping 200 million active users, including 485,000 businesses in the US and 102,000 in the UK, Office 365 is the #1 cloud-based email and productivity suite for businesses. This, coupled with the lucrativeness of the data businesses store in Office 365 applications, makes it an irresistible target for cybercriminals and the primary reason for the rise in Microsoft impersonation.

With a single username and password, a cybercriminal holds a skeleton key to Office 365, along with the freedom to spread through the system to conduct additional attacks. Also known as lateral phishing, multiphase attacks begin with a phishing email and progress to internal phishing and spear phishing attacks sent from a compromised Office 365 account.

Multiphase attacks are becoming increasingly common within Office 365 due to its numerous applications and the opportunities they present. Once a hacker has compromised an Office 365 email account, they no longer need to create elaborate phishing emails impersonating Microsoft—they simply impersonate the user whose account they have compromised.

200 million
active users

485,000
businesses in the US

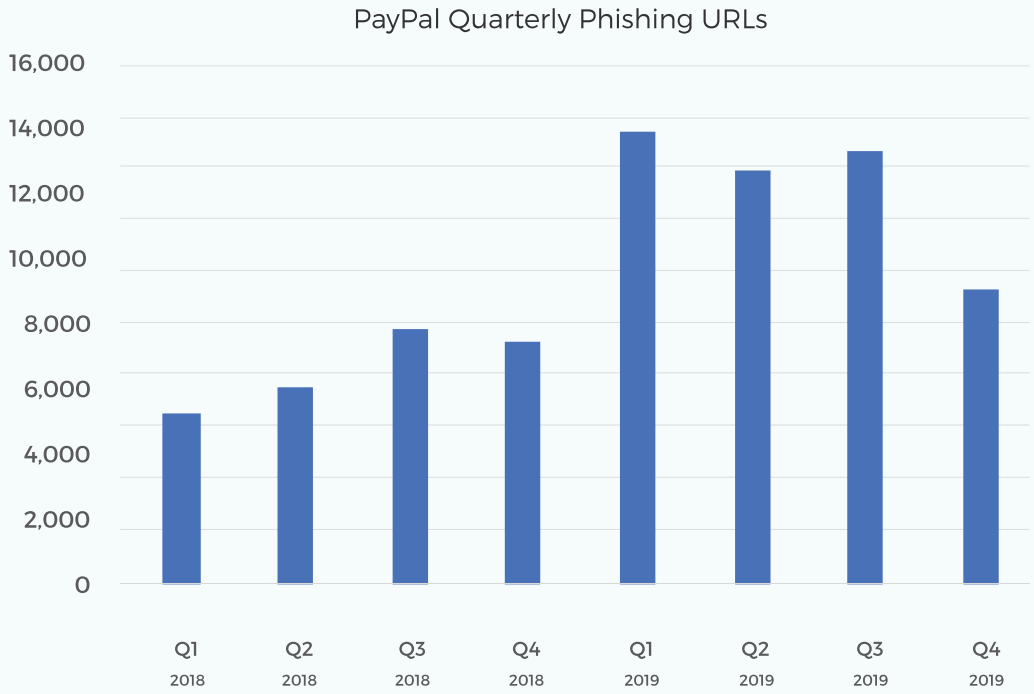
102,000
businesses in the UK

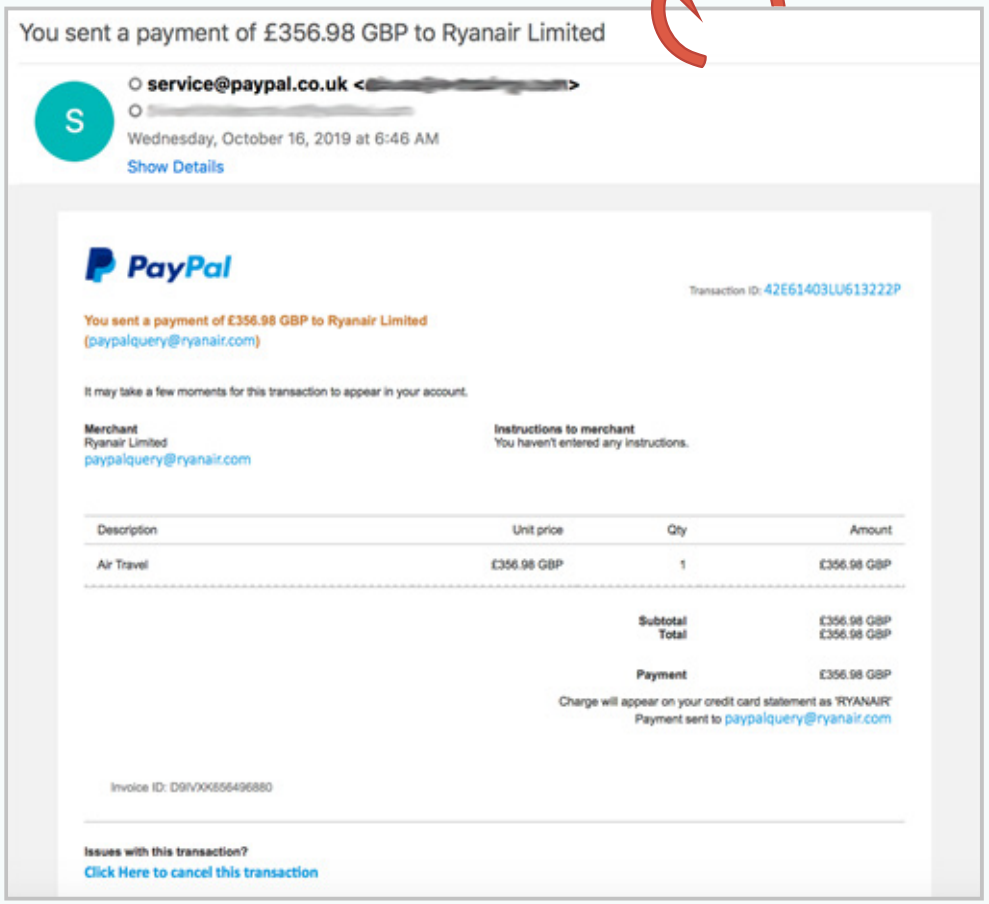
PayPal

PayPal emerges as a phishers' favorite

The rise of PayPal impersonation in 2019 coincided with the June announcement of the PayPal Commerce Platform, which connects retailers from around the globe to PayPal's 277 million active users. The PayPal Commerce platform provides end-to-end payment offerings, compliance support, and AI-based fraud protection. PayPal Commerce Platform also has high-profile partners, including several brands on the Phishers' Favorites top 20 list, including Facebook and Instagram.

The 61,226 unique PayPal phishing URLs detected in 2019 represent an 85.5 percent increase from 2018. In Q1 alone, Vade Secure detected 17,377 unique PayPal phishing URLs, edging off only slightly over the next three quarters. Unlike Microsoft phishing emails, PayPal phishing emails are more consumer oriented and bent toward creating financial anxiety.





In the example, the hacker has created a fake payment confirmation to induce panic in the user, who has made no such purchase. Eager to correct the issue and get their refund, the user has a strong motivation to click the phishing link, log in to a PayPal phishing page, and divulge their credentials.

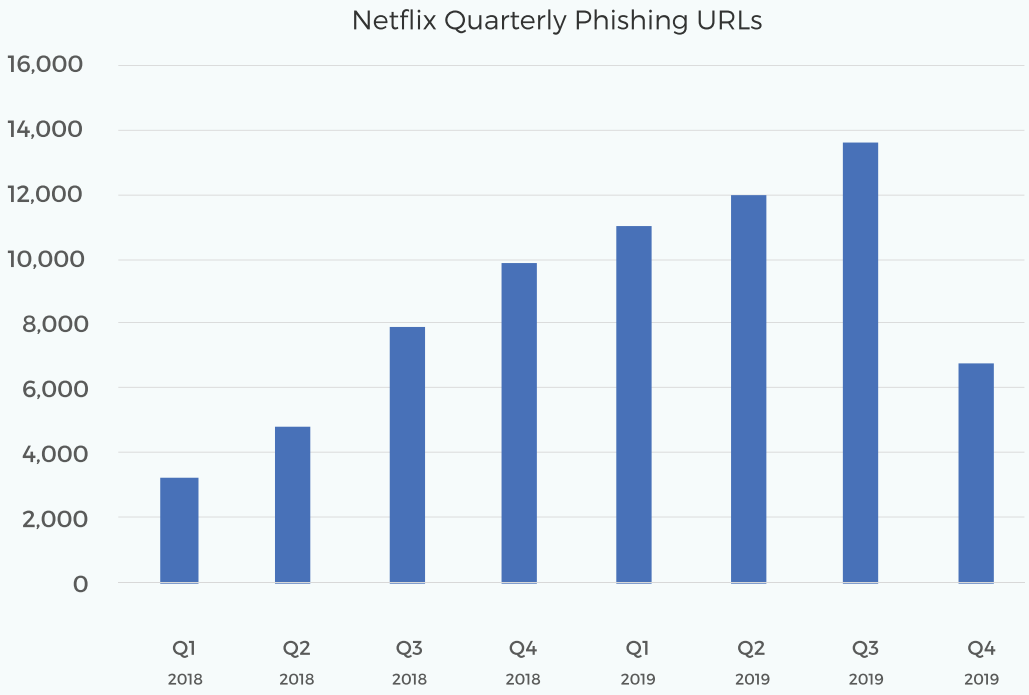
In Q2 2019, Vade Secure detected a phishing campaign targeting roughly 700,000 PayPal users and threatening legal action. With threatening subject lines and legal jargon, the phishing emails directed users to pay a fee to avoid prosecution for various infractions. While victims were told they could pay by mail or phone, they also had the option to pay via PayPal, the quickest and easiest option. With a phishing URL containing a series of redirects designed to fool email filters, users eventually landed on a PayPal phishing page.

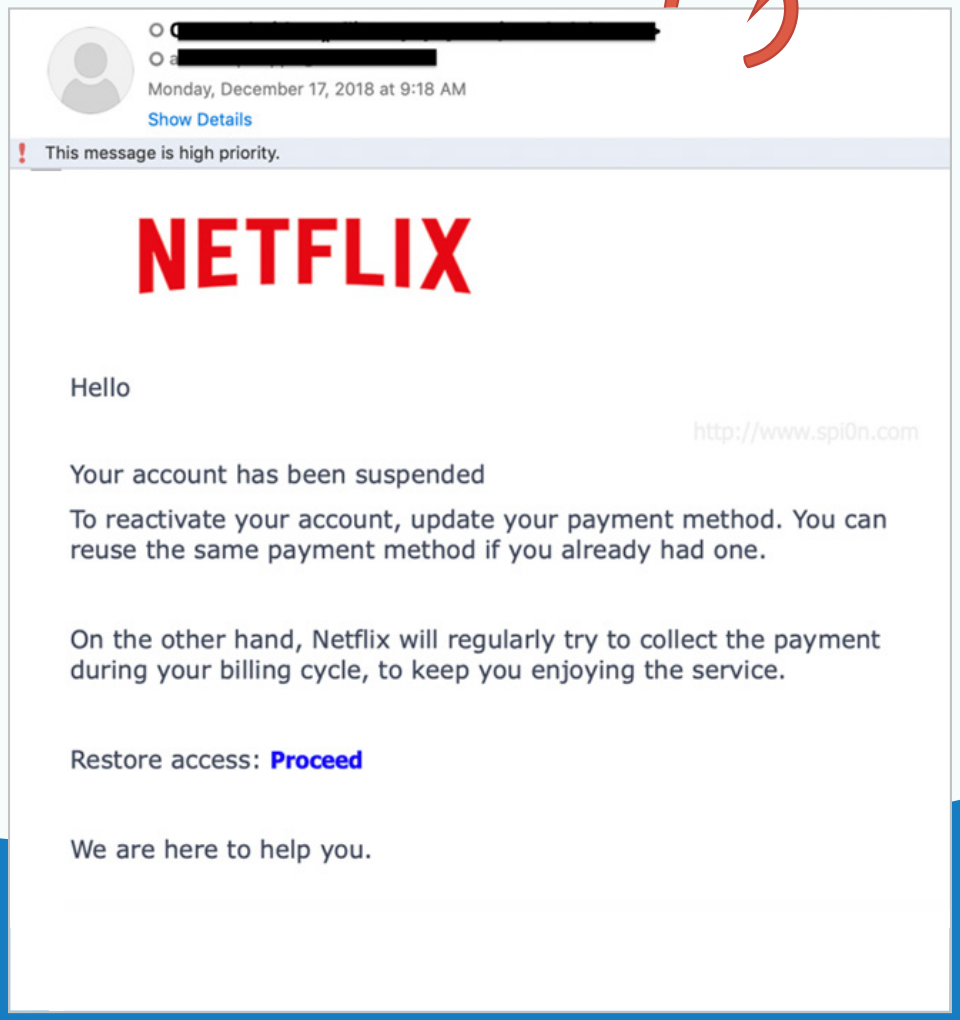
NETFLIX

Netflix is growing in popularity

Like Microsoft and PayPal, Netflix is a clear leader in its space. With 158 million subscribers and 5.5 million free-trial customers, Netflix is unmatched in the streaming wars. Vade Secure detected 43,185 unique Netflix phishing emails in 2019, up from 25,660 in 2018.

According to Netflix, in 2019, its original programming attracted more visitors and views than programming developed from outside studios. A constant stream of new releases makes Netflix subscribers eager to keep their accounts current. It also makes it an irresistible target to hackers looking to reach those visitors who are accustomed to receiving emails from Netflix, whether to alert them to new releases, send them payment reminders, or warn them of suspicious activity on their accounts.





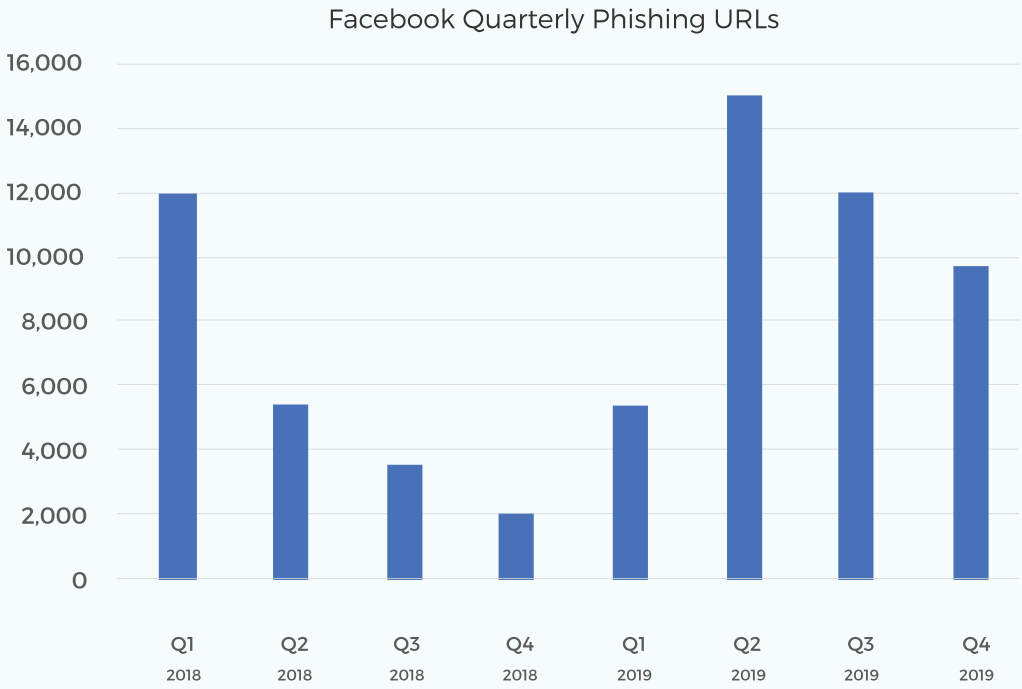
Suspicious activity alerts are a popular phishing tactic and especially popular and effective in Netflix phishing emails. While some viewers are excited to get home to continue streaming their favorite shows, others are anticipating the world premiere of a new season. If their accounts are locked or compromised in any way, there is a strong possibility they will let their guards down and react to a phishing email.

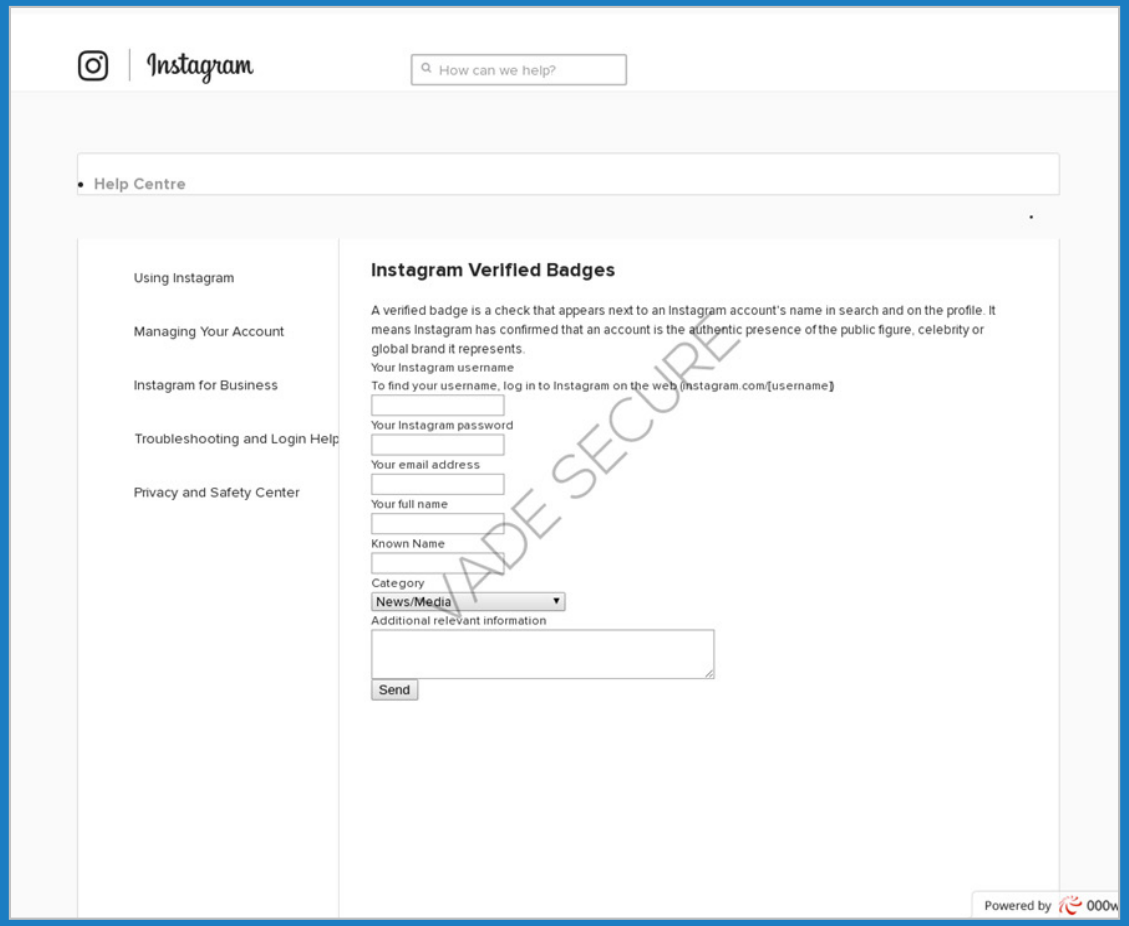
Despite a strong showing throughout 2019, Netflix phishing decreased by more than 50 percent in Q4, with only 6,758 phishing URLs detected. Whether Netflix phishing will continue to decrease may depend on whether Microsoft and PayPal phishing remain a lucrative enterprise. While Netflix beat subscriber expectations in Q4, pressure from competitors is growing. It will be interesting to see if Disney+ appears on our quarterly list sometime in the near future.

facebook

Social media phishing grows

Year-over-year, Facebook phishing spiked 358.8 percent, an alarming increase that could have roots in Facebook's own faulty data privacy practices. Facebook saw triple-digit phishing URL growth in Q1 and Q2, for a one-year tally of 42,338. Why the sudden rise in Facebook phishing? Facebook's difficulty protecting its users provided media fodder throughout 2019, and the lawsuits have not stopped. This gives hackers a reason to communicate regularly with Facebook users who are on high alert about data compromise.



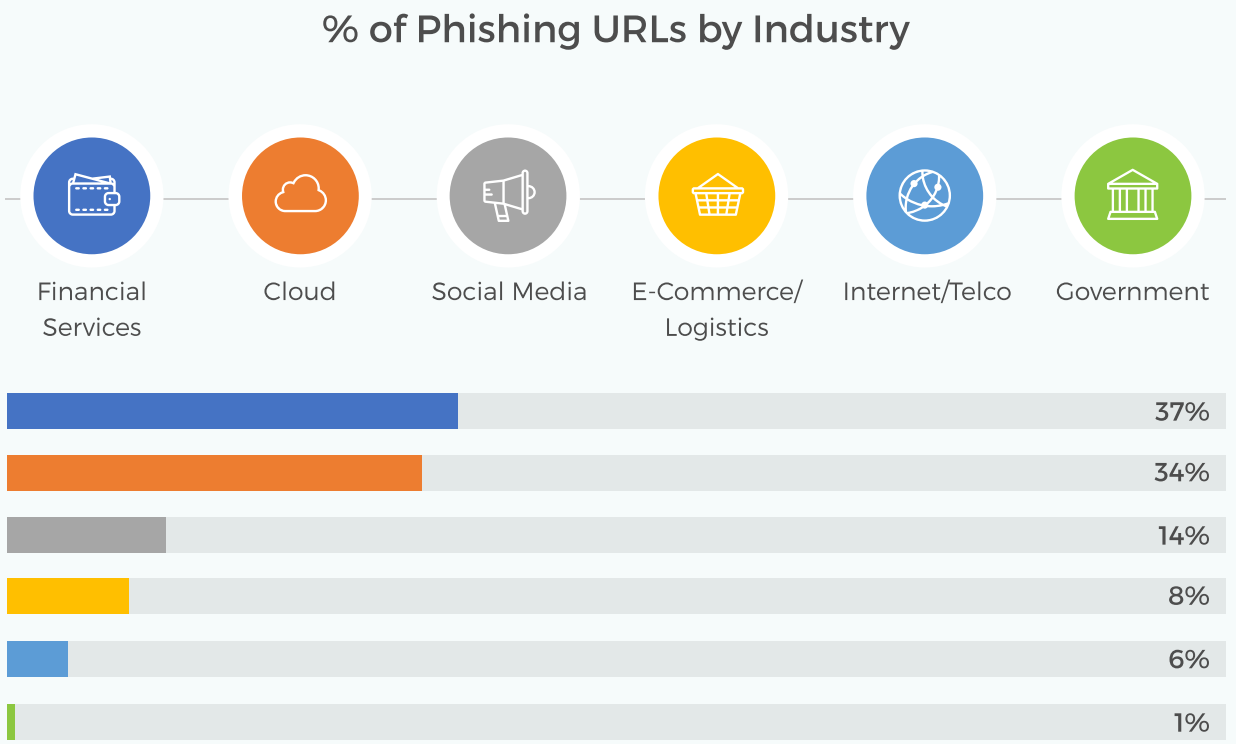


Additionally, with Facebook's universal login feature, Facebook Login, a hacker who is armed with a set of stolen user credentials can access all the user's associated applications, along with all the personal data contained in those applications. In November 2019, Facebook launched Facebook Pay, a competitors to PayPal and Apple Pay that connects a Facebook user's credit card to Facebook, Instagram, and WhatsApp applications; Facebook pages and businesses on Facebook Marketplace; and more.

Facebook isn't alone in being a favorite social media target. Although not in the top 20 of the year, both Instagram and WhatApp have seen an increase in phishing activity. WhatsApp jumped 63 spots to #5 in Q4, a 13,468 percent increase from Q3. Instagram jumped 16 spots to #13 in the same quarter. Overall, Instagram phishing grew 2,332 percent from 2018.

Financial services represents the most phishing URLs

With the high potential of direct financial payback, the financial services industry is impersonated more than any other, with ten financial services brands in the top 20, including Bank of America, CIBC, Chase, and Credit Agricole. The financial services industry represented 37 percent of all unique phishing URLs detected in 2019, for a total of 139,964. Bank of America, the ninth most impersonated brand of 2019, saw large gains in Q2 and Q3, with a slight drop-off in Q4.



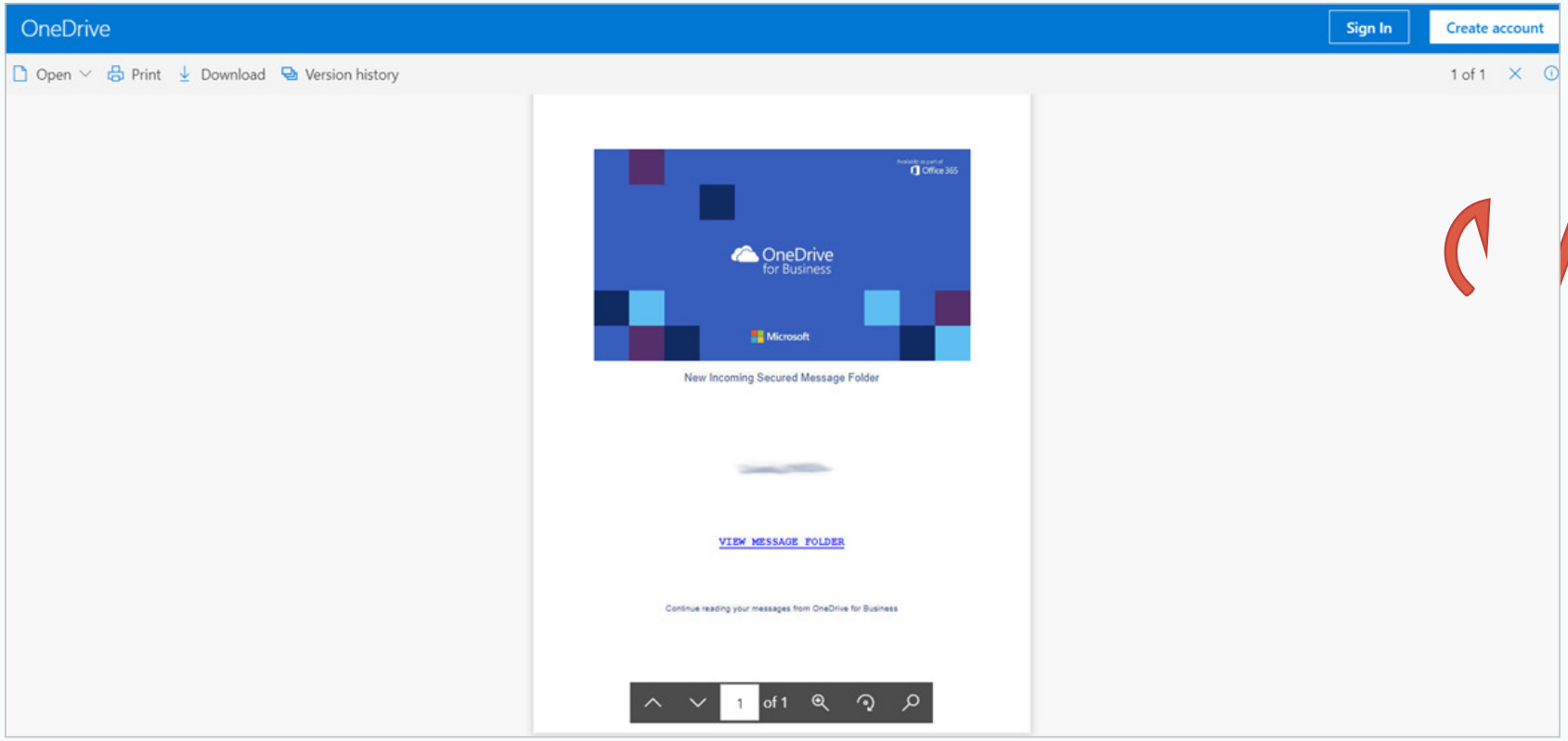
Although the trend in financial services remained largely consistent throughout the year, in Q4, Vade Secure detected a decrease in phishing URLs for Wall Street banks, including a 21 percent decrease in Bank of America phishing and 54 percent decrease for Wells Fargo. However, there was an increase in phishing attacks impersonating community banks, including a 470 percent increase for M&T Bank and a 54 percent increase for Dejardins.

The shift toward community banks is consistent with an overall shift in cyberattack targets in 2019. Throughout the year, SMBs were pummeled with ransomware attacks, many of them originating from phishing emails. From city governments to MSPs, SMBs with limited budgets and IT staff are easy targets compared to enterprises who can afford to spend millions on cybersecurity.

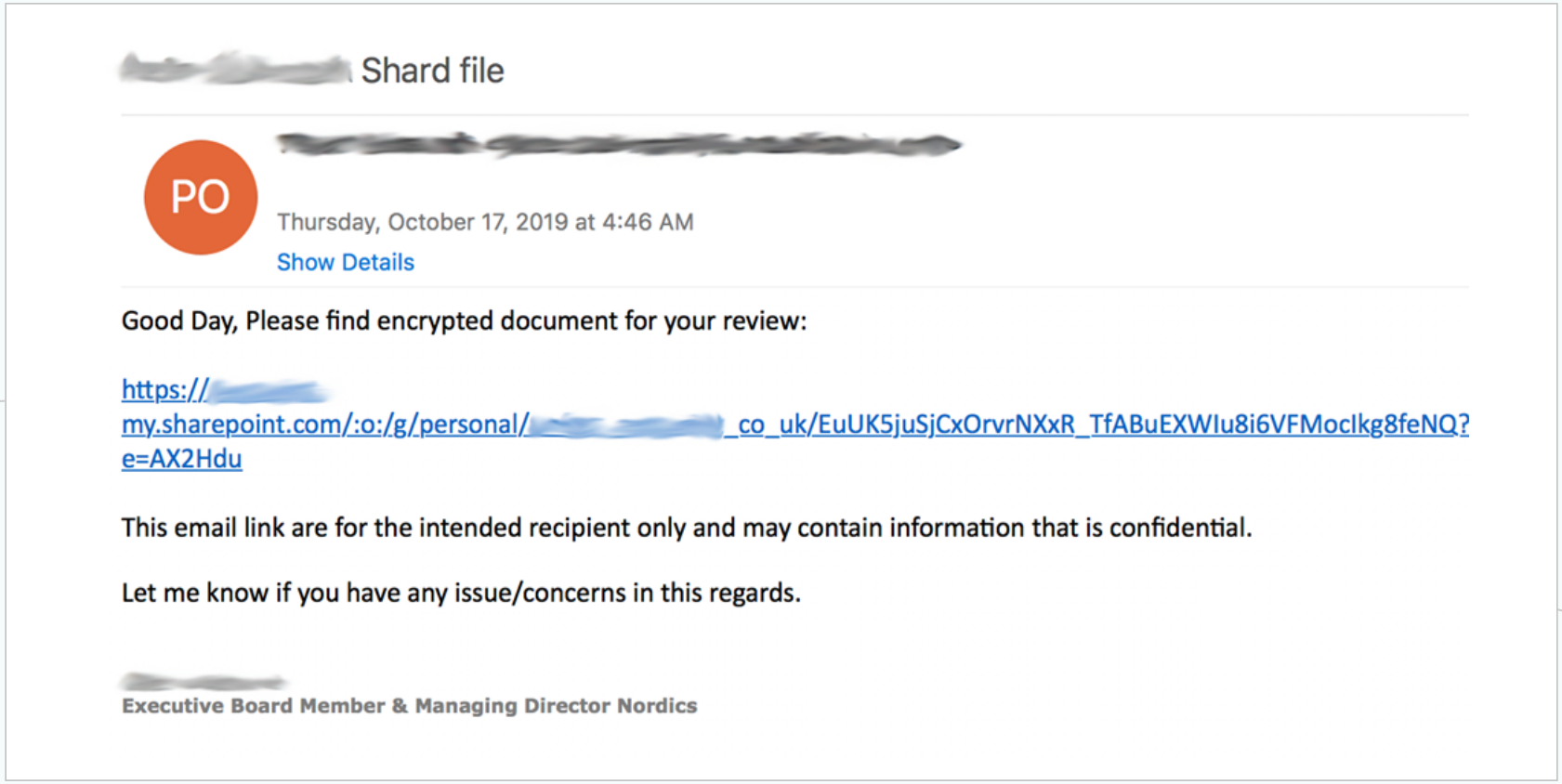
Sophisticated phishing emails replace sloppy attacks

In terms of technology prowess, amateur hour has passed. Today's phishers do not make the mistakes of their predecessors and are consistently honing their techniques to bypass detection. Microsoft phishing emails are particularly targeted and rightfully so: Office 365 features six applications, including SharePoint, Teams, and OneDrive, each serving a unique purpose and delivering custom alerts and notifications.

In 2019, Vade Secure detected a number of Microsoft phishing attacks that leveraged SharePoint and OneDrive notifications. While many of these notifications were fraudulent, some were sent via legitimate Office 365 accounts, making them nearly impossible for users to detect.
In the SharePoint example below, the phishing link is not in the email but in the shared file.



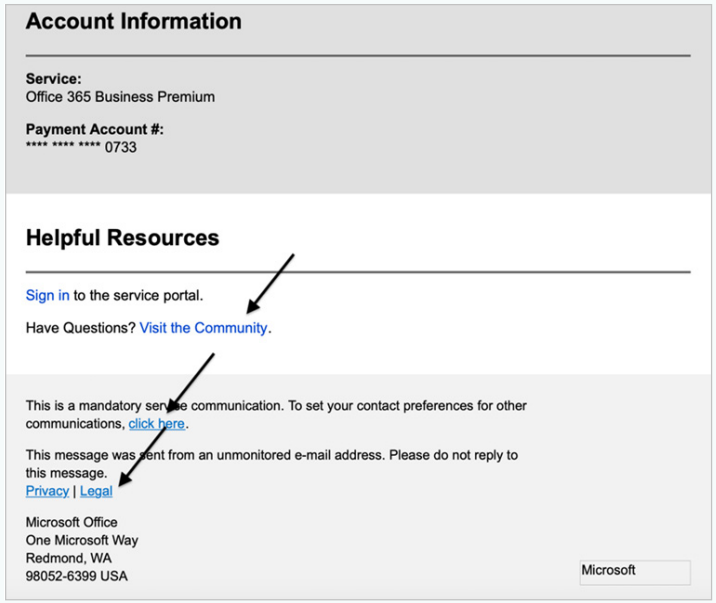
Fake OneDrive Notification



Legitimate SharePoint Notification from Compromised O365 Account

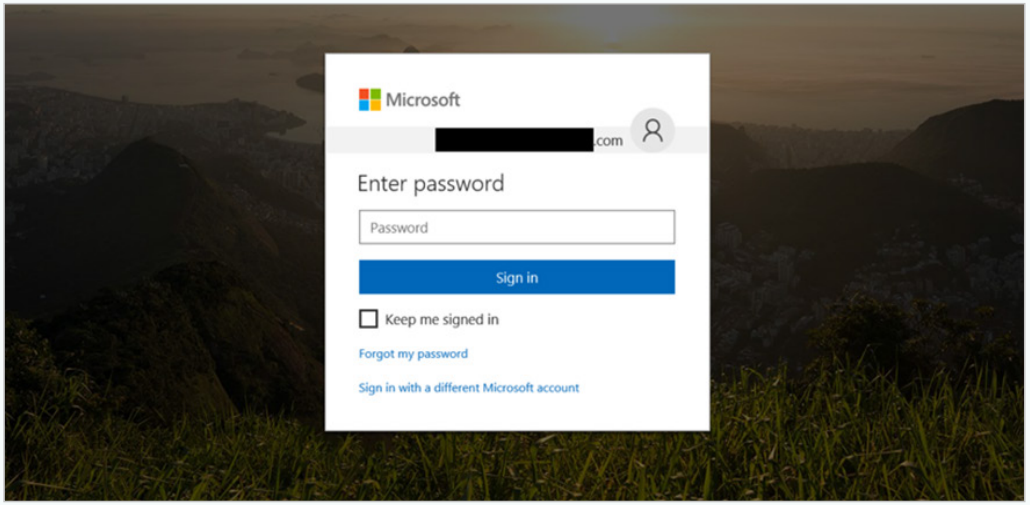
While the above examples point to new methods of user manipulation, the latest techniques used to manipulate email filters reveal that phishers have a clear understanding of the technologies designed to stop them.

Reputation- and signature-based email filters are scanning for known phishing URLs, but they will not recognize a new, unknown threat or phishing URL that has not yet been detected and blacklisted. In the below email, the phisher has included a number of clean links. Not only does it trick the email filter but also adds to the authenticity of the email in the eyes of the user.



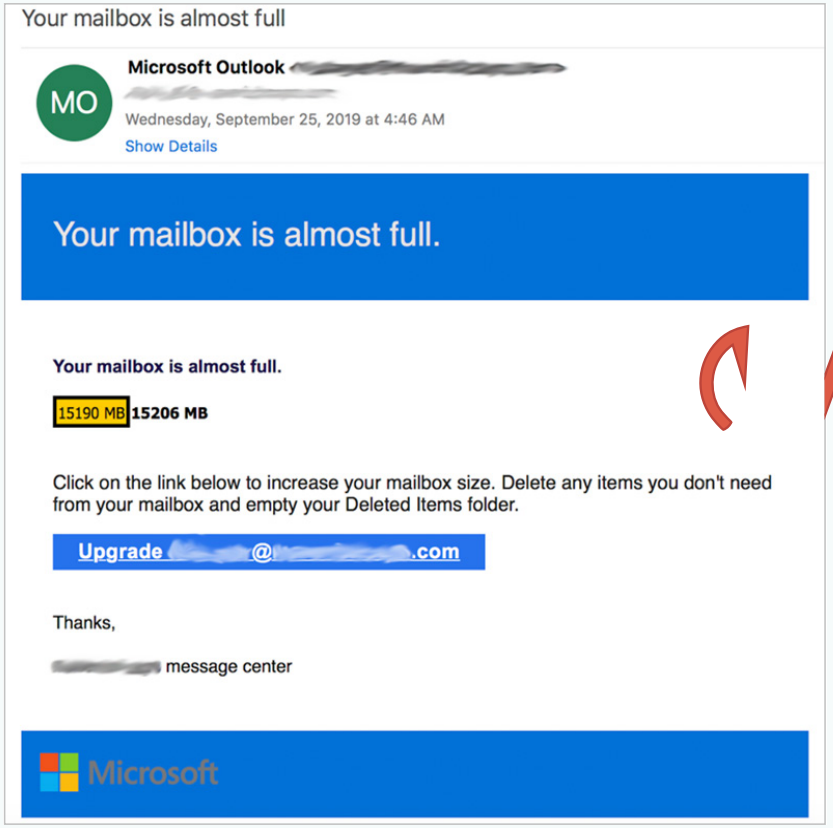
Office 365 phishing email with clean links

Phishing webpages are equally important to the success of an attack, both visually and technically. To bypass email filters, hackers mimic both the design of Office 365 login pages and the building blocks of the page: the CSS. In the example, the hacker has copied the CSS from the real Office 365 login page and used it to build their phishing page, making it unlikely that a user will recognize the deception.



Fake Office 365 login page

Like webpages, images are critical to the authenticity of brand impersonation, but they are more than visual proof for users. Beneath the surface of an image is a cryptographic hash that a filter can recognize if it was present in previously detected phishing emails. To bypass a filter, hackers distort the image slightly, changing the cryptographic hash and manipulating the email filter into classifying the email as unique.

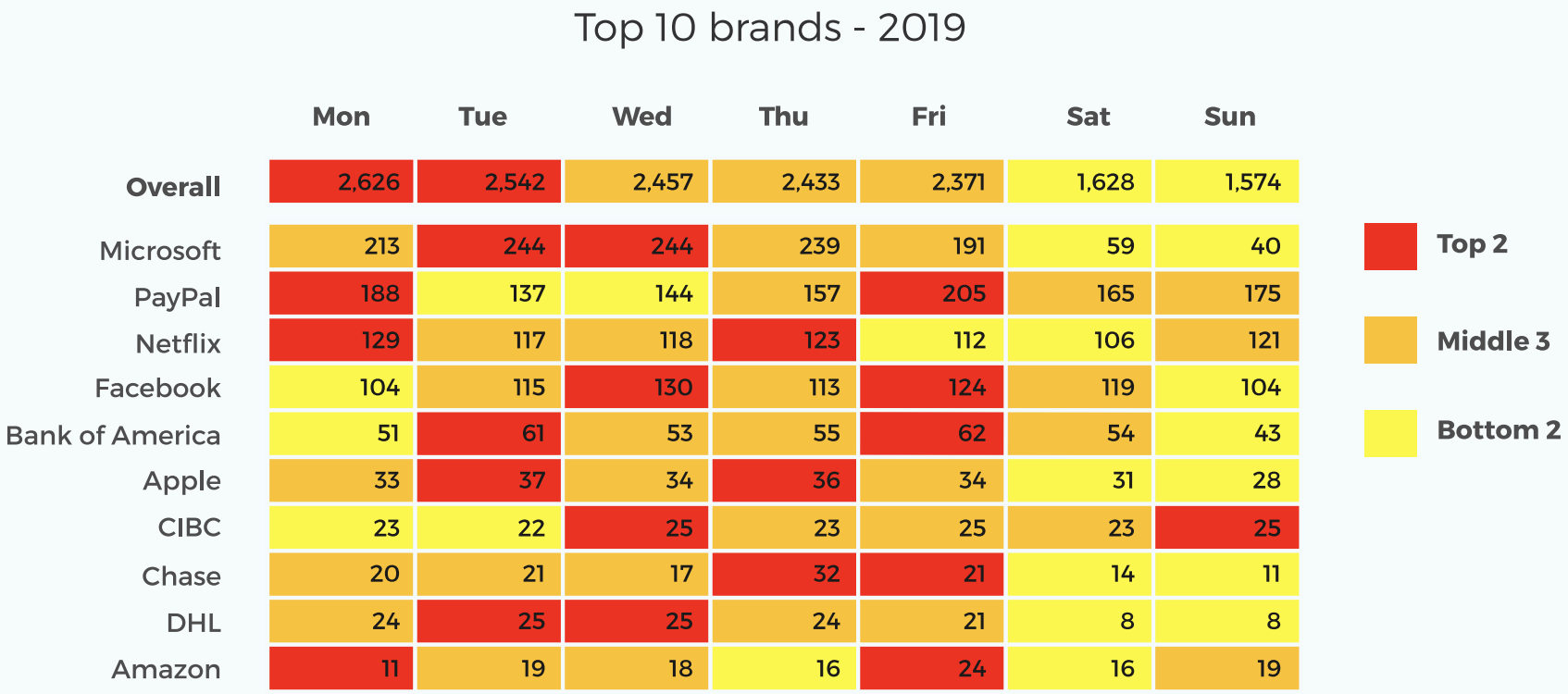


Gray Microsoft logo hidden by blue background

In the example, the hacker has placed a Microsoft logo with barely visible text on a blue background, a technique that would easily bypass a template matching algorithm, which is commonly used to detect images exactly matching the original.

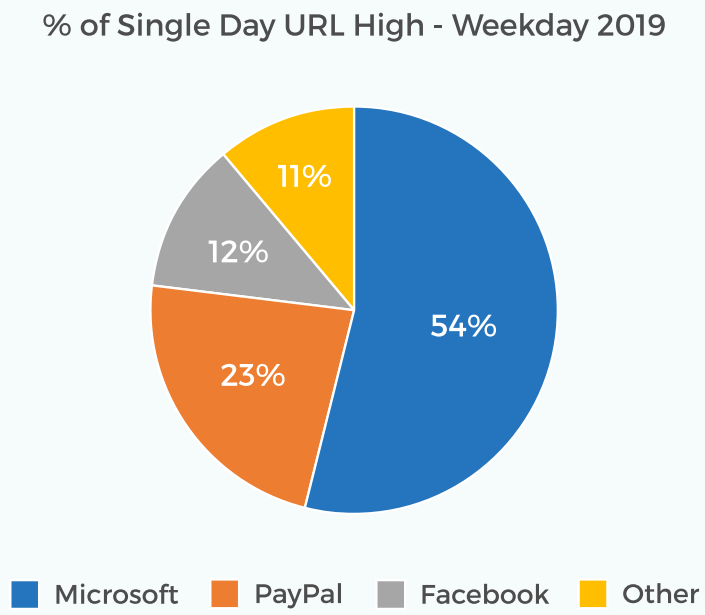
Timing is everything

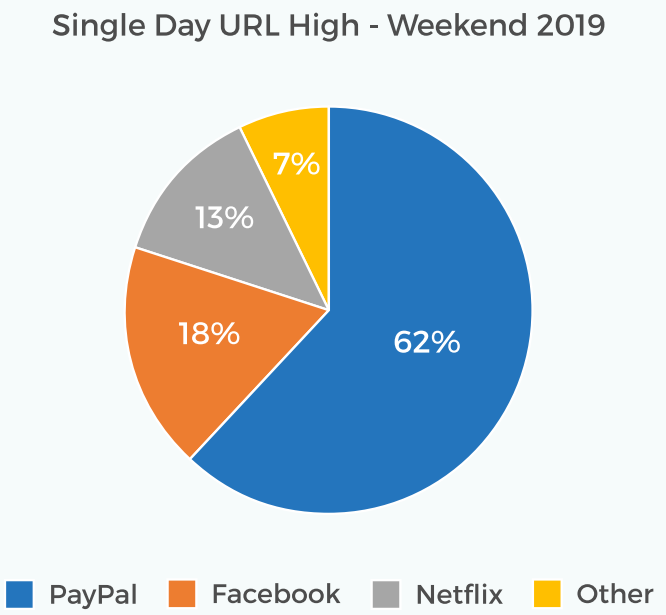
Among the 64,331 unique Microsoft phishing URLs detected by Vade Secure, most were detected on Tuesdays and Wednesdays. This pattern is strategic: Most business users return to work on Monday and encounter overflowing inboxes, making them less likely to read emails that are not business-critical. After digging out from the weekend, their inboxes are more focused by Tuesday and mid-week, giving them more time to read and respond to emails of other types.



Average # of phishing URLs per day in 2019

The overall trend of weekday phishing is not exclusive to Microsoft. In 2019, 79.5 percent of phishing emails were sent on weekdays, with Mondays and Tuesdays being the most high-traffic days for the top 10 brands. Q4 2019 saw a slight change in this trend, with Friday being the top day for phishing for three of seven top brands, including Facebook, Netflix, and Bank of America. Overall, Microsoft was the most impersonated on 54 percent of weekdays. PayPal is the weekend leader, being the most impersonated brand on 62 percent of weekends.





SOPHISTICATED PHISHING ATTACKS REQUIRE SOPHISTICATED DEFENSES

Phishing attacks are a daily occurrence. Whether they land in your junk folder or your inbox, the assaults are ongoing, growing in sophistication, and designed to bypass both advanced filters and trained users. Protect your business and your clients from dynamic phishing attacks with a combination of training, technology, and vigilance:

User training: Invest in phishing training that goes beyond the annual training session. Providing contextual training at the time the user clicks on a phishing link connects the event to the training, making it more memorable for the user.

AI-based Anti-Phishing Technology: AI-based anti-phishing technology exceeds reputation- and signature-based defenses. Unsupervised Learning algorithms learn to generalize based on the training dataset to recognize variances of known attacks. Deep Learning algorithms with Computer Vision are trained to recognize brand images, detecting even minute distortions to those images designed to evade detection.

Automated Phishing Remediation: Phishing emails that bypass a filter will not go unopened for long. Automated phishing remediation removes threats post-delivery, reducing manual investigation and response.

Multiphase Attack Protection: Spear phishing emails without links and unknown malware require additional technologies and capabilities in one solution. Unsupervised Learning algorithms detect rare events and anomalies, while Natural Language Processing detects malicious behaviors, such as flag words and phrases common to spear phishing.

Additional Resources

Evaluating Office 365 Email Security Solutions
Phishing Attacks: Advanced Techniques That Evade Detection
IsItPhishing.AI
Phishing IQ Test