Phishers' Favorites

2020 Year-in-Review

vade

TABLE OF CONTENTS

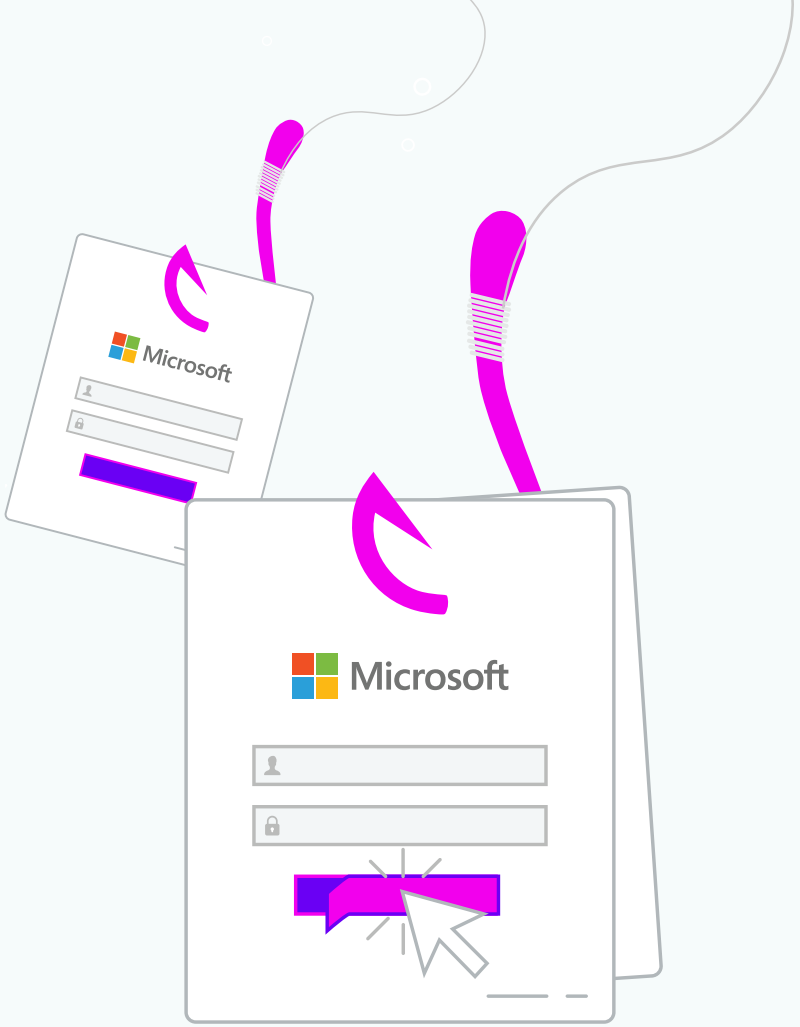
Phishers' Favorites 2020 Year-in-review 3

- Microsoft impersonation continues to dominate 3
- The 20 most impersonated brands in phishing attacks 4
- Phishers' Favorites 2020 - 20 Most Impersonated Brands 5
- Microsoft 365 remains the #1 target for phishing attacks 6
- Social media stays on target 7
- Cloud overtakes financial services as the most impersonated industry 9
- Current events drove phishing attack trends 11
- A late summer surge caused Microsoft phishing to soar 13

Sophisticated phishing attacks require sophisticated defenses 16

About Vade 17

PHISHERS' FAVORITES 2020 YEAR-IN-REVIEW



Microsoft impersonation continues to dominate

Phishers' Favorites is Vade's quarterly report highlighting the top 25 most impersonated brands in phishing attacks. Our year-in-review looks at the top 20 most impersonated brands of 2020 and explores key phishing trends from the year, including the continued dominance of Microsoft 365 phishing and the rise of new brands on the Phishers' Favorites list.

Each quarter, Vade'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, and sometimes hundreds or thousands, of phishing emails containing the same URL.

The 20 most impersonated brands in phishing attacks

Microsoft is the most impersonated brand of 2020, marking its third year in the top spot. Vade detected 39,621 unique Microsoft phishing URLs in 2020. Facebook came in at #2 on the list, up from #4 in 2019 with 14,876 unique phishing URLs.

Rounding out the top three is PayPal, which ranked at #2 in in 2019. Vade detected 11,841 unique PayPal phishing URLs in 2020. Unique phishing URLs overall were down for 2020, while the volume of phishing emails detected remained steady. What did not change were the top targets and the growing sophistication of attacks.

Microsoft

facebook

Phishers' Favorites 2020

#		Brand	Unique Phishing URLs
1	-	Microsoft Category: Cloud	39,621
2	↑2	Facebook Category: Social Media	14,876
3	↓1	PayPal Category: Financial Services	11,841
4	↑4	Chase Category: Financial Services	8,832
5	↑28	eBay Category: E-Commerce/Logistics	6,918
6	-	Rakuten Category: E-Commerce/Logistics	6,452
7	↓4	Netflix Category: Cloud	6,417
8	↑2	Amazon Category: E-Commerce/Logistics	6,063
9	↑5	WhatsApp Category: Social Media	5,322
10	↓1	DHL Category: E-Commerce/Logistics	4,403
11	-	Credit Agricole Category: Financial Services	4,317
12	↑6	Wells Fargo Category: Financial Services	4,265
13	↑3	Adobe Category: Cloud	4,171
14	↓9	Bank of America Category: Financial Services	4,042
15	↑2	Google Category: Cloud	3,317
16	↑8	Comcast Category: Internet/Telco	3,297
17	↓11	Apple Category: E-Commerce/Logistics	3,131
18	↑22	La Banque Postale Category: Financial Services	2,932
19	↑9	LinkedIn Category: Social Media	2,548
20	↓8	Dropbox Category: Cloud	2,427

Microsoft 365 remains the #1 target for phishing attacks

Microsoft 365's user base grew to 258 million in 2020, higher than expected and continuing its dominance in the business productivity software market. This growth was, in large part, spurred by the COVID-19 pandemic that swept the globe early in 2020. Microsoft reported 75 million active Microsoft Teams users in April 2020, up from 44 million in March 2020.

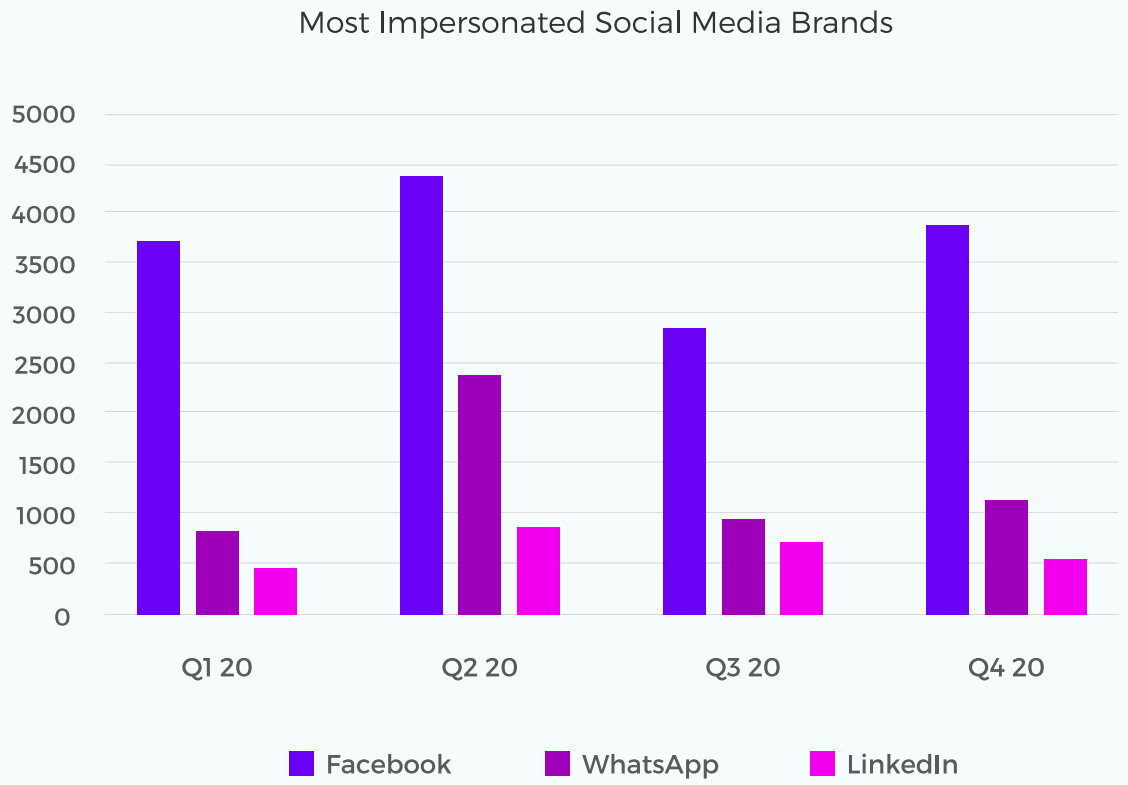
Microsoft has consistently remained at the top of our Phishers' Favorites quarterly reports, holding the #1 spot for seven quarters. With more than 90 percent share of the email market and authoring market, Microsoft 365's suite of applications is a rich source of data for cybercriminals to exploit.

Microsoft phishing attacks range from run-of-the mill password reset alerts to more personalized emails requesting colleagues to open OneDrive and SharePoint files. As we will see later on, many Microsoft phishing emails don't impersonate Microsoft at all. Instead, the emails impersonate another brand and include links to Microsoft 365 phishing pages, exploiting user trust in the Microsoft brand.

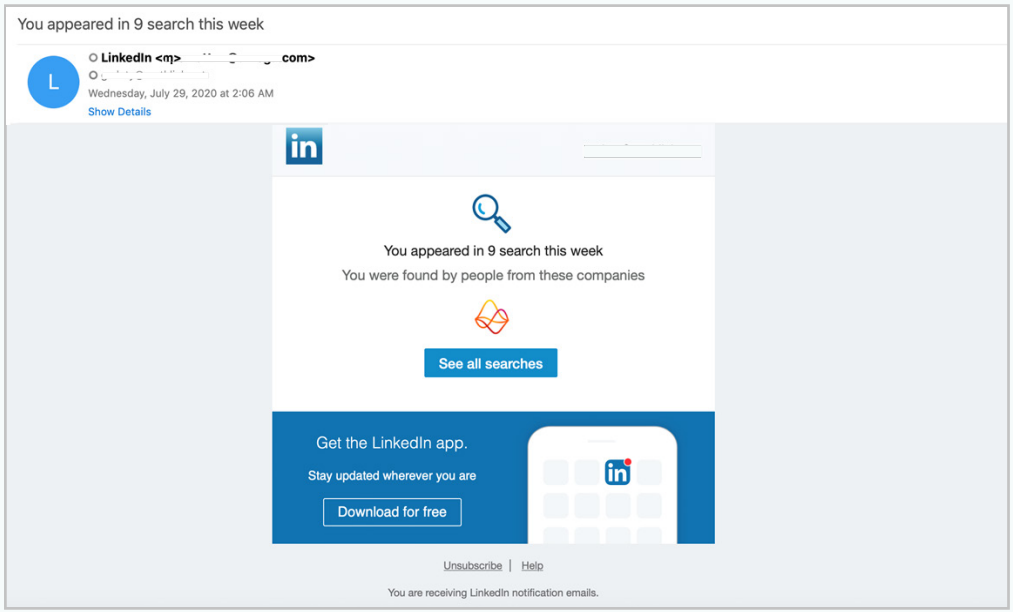
Social media stays on target

Interest in Facebook has been on the rise since 2018 when Vade first started tracking unique Facebook URLs. Facebook's first big leap came in Q2 2019 when unique Facebook phishing URLs grew more than 155 percent and remained steady through 2020. Q2 was the biggest month for Facebook phishing in 2020, with 2,868 unique URLs detected, for a total of 14,876 for the year.

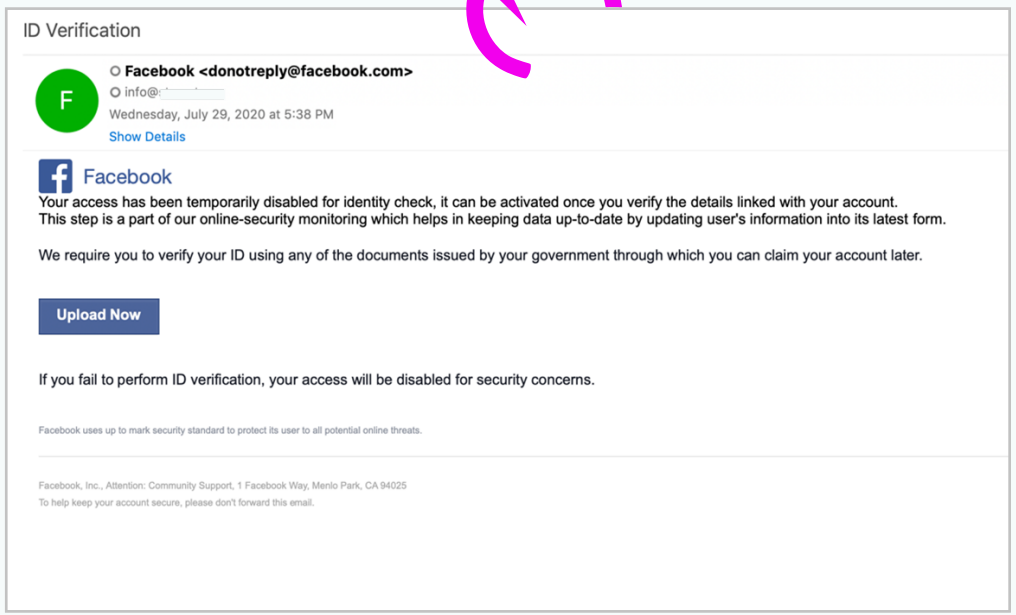
WhatsApp made its first appearance on the Phishers' Favorites list in Q1 2019 with a small number of phishing URLs detected. That changed drastically in Q4 2019, when Vade detected 5,029 unique WhatsApp phishing URLs for the quarter. Things slowed down for WhatsApp in Q1 2020 and then picked back up in Q2. The spike coincided with the COVID-19 pandemic, when social media brands in general saw a pickup in phishing.



Facebook and WhatsApp have a combined 4.7 billion users. Dominating the list of most impersonated social media brands, Facebook and WhatsApp offer not the bank account and credit card numbers of a large bank or financial institution, but a wealth of personal data to be harvested, sold, and exploited.



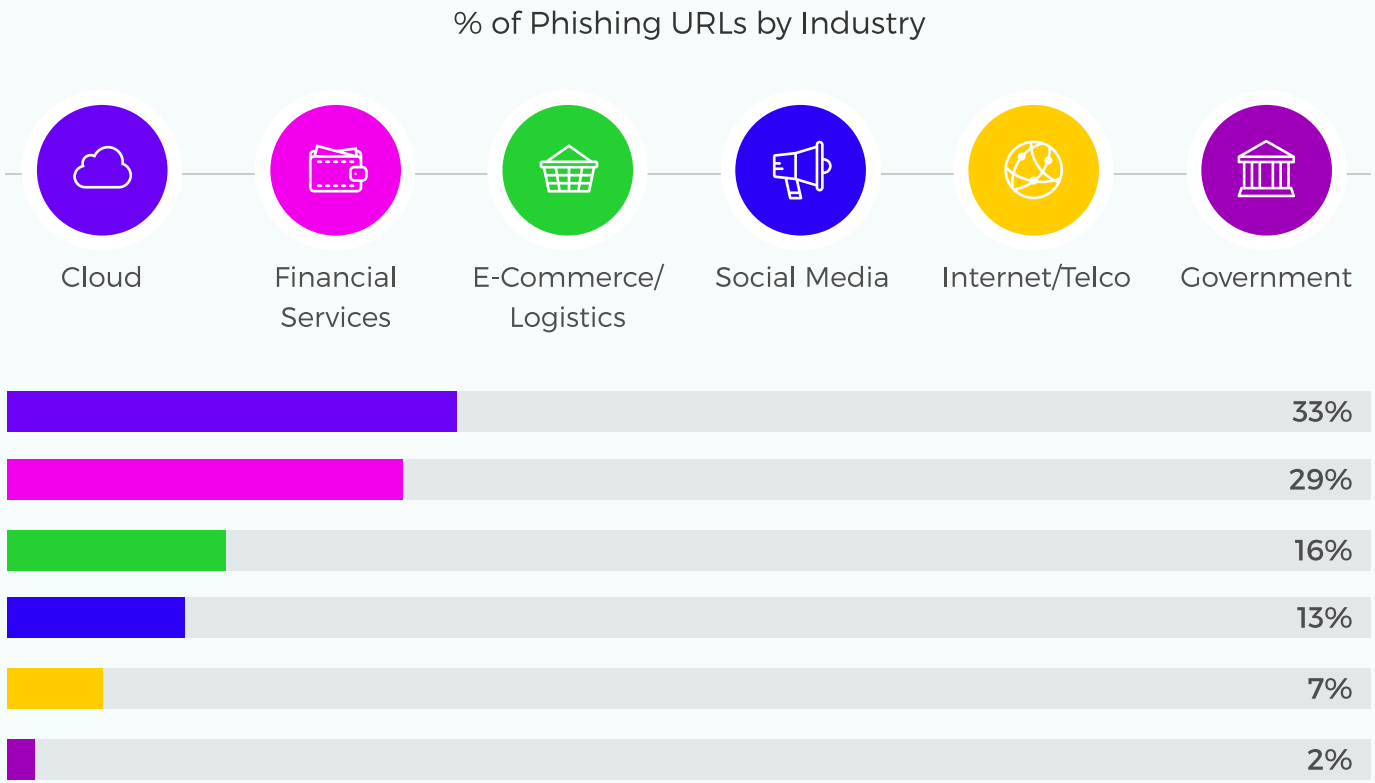
LinkedIn phishing email, July 2020



Facebook phishing email, July 2020

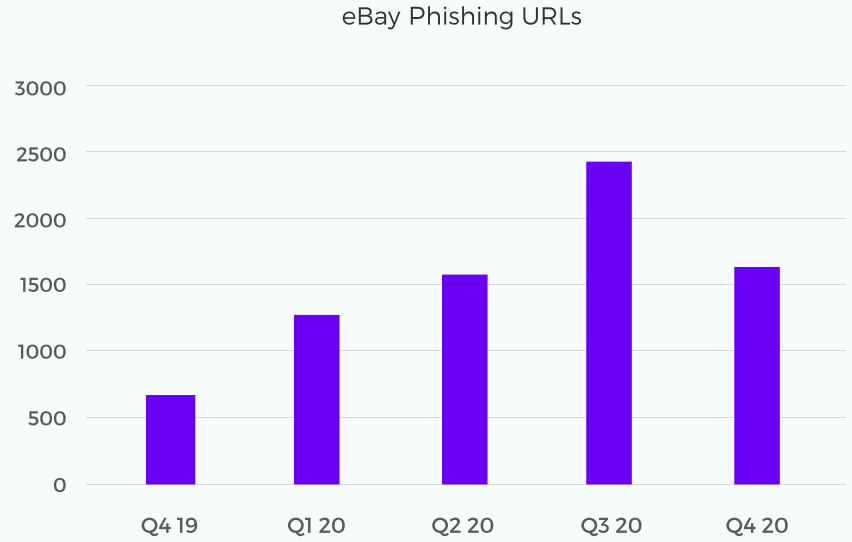
Cloud overtakes financial services as the most impersonated industry

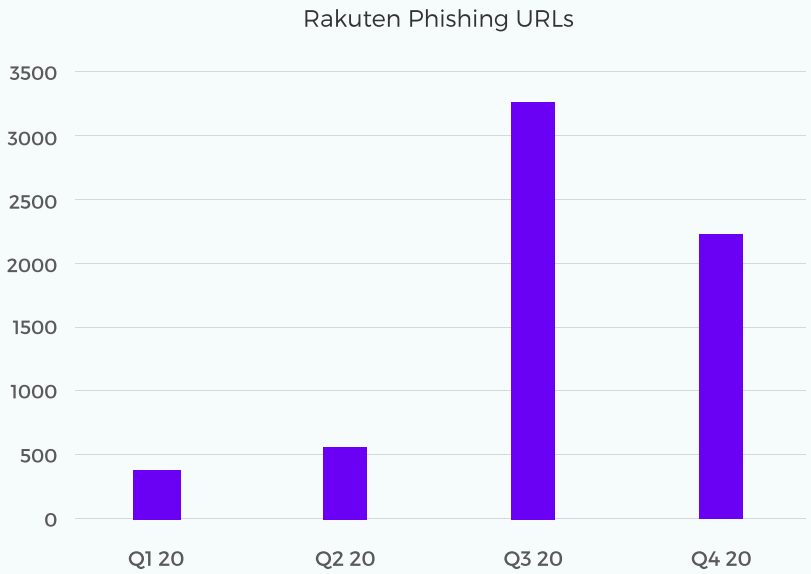
Financial services started out the year strong, representing 36.7 percent of unique phishing URLs in Q1. PayPal, which came in at #2 in 2019, dropped to the third spot. Chase, previously at #8, rose to the fourth spot in 2020, with 8,832 phishing URLs. Credit Agricole maintained its position at #11 in 2020 with 4,317 phishing URLs, followed by Wells Fargo, which rose six spots to #12 with 4,265 phishing URLs.



In an abrupt shift, phishing attacks impersonating financial services decreased in Q2 from 37 percent to 33 percent, while attacks on cloud services companies increased. In Q3, cloud phishing increased to 40.5 percent, up from 33 percent in Q2. Cloud remained strong for the remainder of the year, representing 33 percent of all unique phishing URLs detected in 2020. Microsoft, Netflix, Adobe, and Dropbox represented the most impersonated cloud services companies in the top 20. Both Google and Adobe saw growth in phishing URLs, moving up two and three spots respectively.

In another shift from 2019, e-commerce overtook social media as the third most impersonated industry. Like cloud services, e-commerce reached new heights in 2020 thanks to the shift to both mass teleworking and quarantine. eBay, which didn't make the top 20 list in 2019, jumped 28 spots to #5. eBay's rise began in Q1 with an 89 percent increase in phishing URLs over Q4 2019. eBay phishing peaked in Q3 with 2,424 URLs and 143 percent year-over-year (YoY) growth.



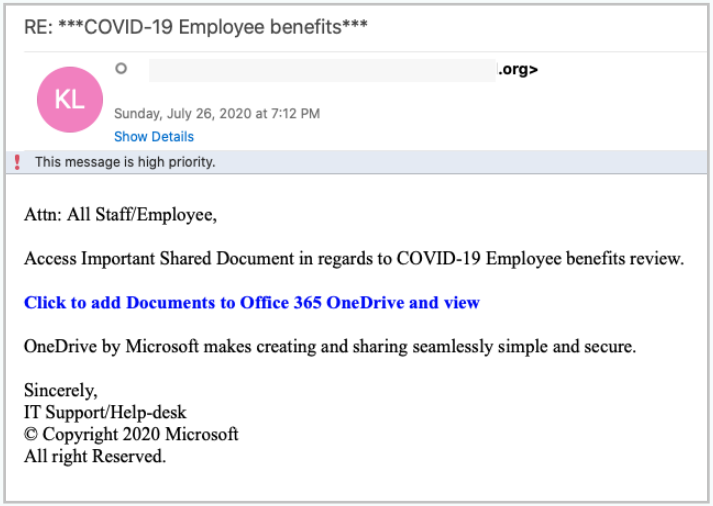


New to the list, Rakuten, a Japanese e-commerce company founded in 1997, first started making noise in Q3 2020 when unique Rakuten phishing URLs exploded by 485 percent, from 559 URLs in Q2 to 3,272 URLs in Q3. Things quieted down for Rakuten in Q4, with Rakuten phishing URLs decreasing 32 percent.

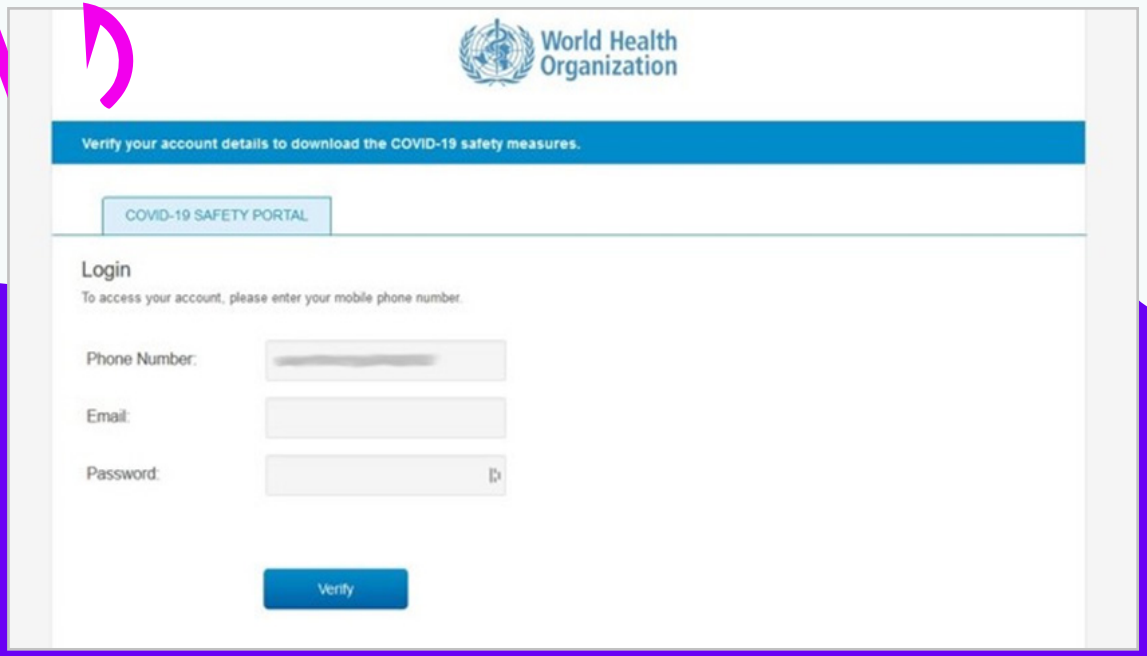
Current events drove phishing attack trends

The abrupt shift from financial services phishing to cloud services phishing came as COVID-19 changed the way we work around the world. Microsoft Teams active users exploded in Q3, Amazon Web Services (AWS) revenue grew 29 percent in both Q2 and Q3, and Google cloud revenue grew 45 percent in Q3. Around the same period, eBay phishing peaked and Rakuten phishing skyrocketed.

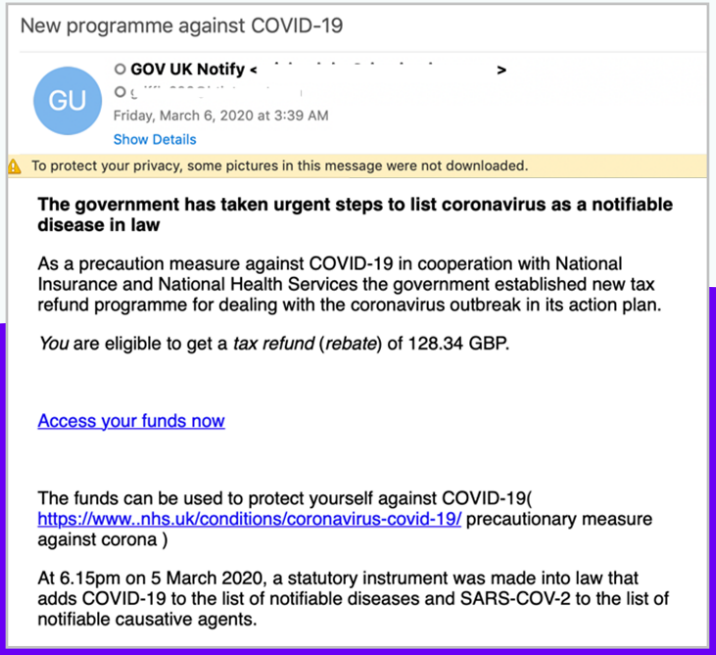
When COVID-19 forced businesses to shift to teleworking, cybercriminals went immediately to work, leading to a mass wave of COVID-19 themed phishing and spam emails. Capitalizing on fear, COVID-19 emails ranged from advertisements for facemasks and other personal protective equipment, to fake emails from human resources touting COVID-19 benefits, and finally to phishing emails impersonating health organizations, including the World Health Organization (WHO) and National Health Services.



COVID-19 HR phishing email



WHO phishing page



COVID-19 tax break refund phishing email

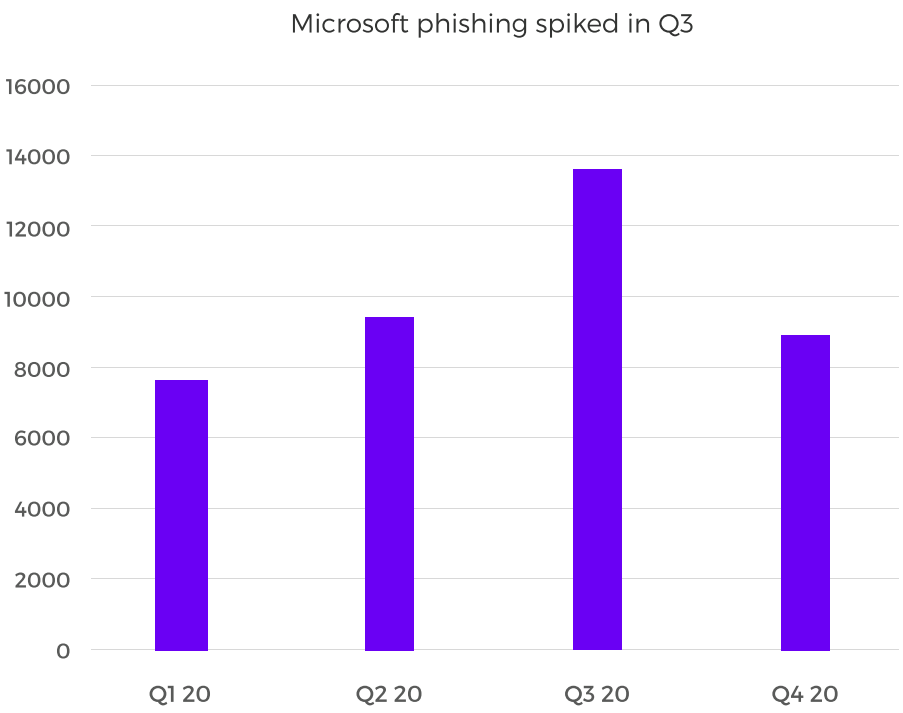
Black Friday is another current event that drove mass waves of malicious emails. In 2020, 10 to fifteen percent of Black Friday emails analyzed by Vade were malicious. Amazon spam and phishing emails were prevalent during the Black Friday wave. A global event, Black Friday spawned email threats ranging from fake sweepstakes and surprise rewards to emails that capitalized on Black Friday excitement in the subject line but featured an offer unrelated to the event itself.

Amazon phishing email (Italian)

Effuel spam email

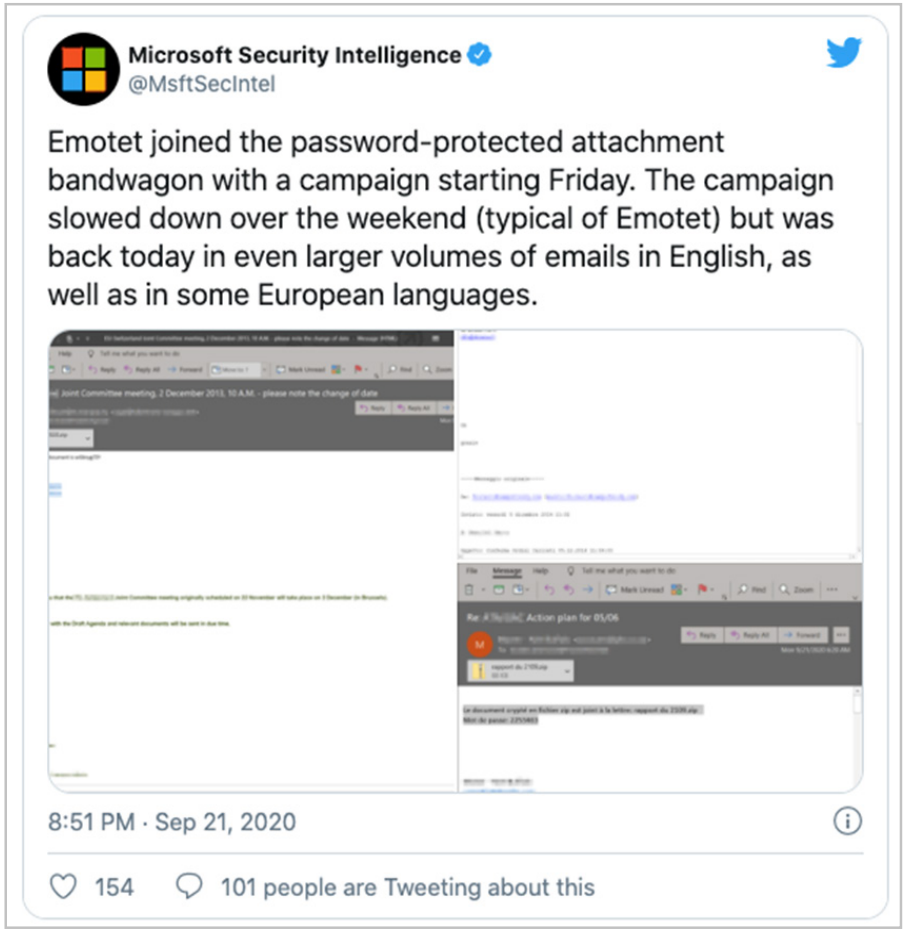
A late summer surge caused Microsoft phishing to soar

Microsoft saw steady levels of phishing URLs in the first half of the year, with 7,581 URLs in Q1 and 9,410 URLs in Q2. In early Q3, Microsoft phishing exploded to 13,617 phishing URLs, with a small surge of phishing in July followed by a burst in August and September. The single-day high during the wave occurred on September 24, when Vade detected 1,151 unique Microsoft phishing URLs.



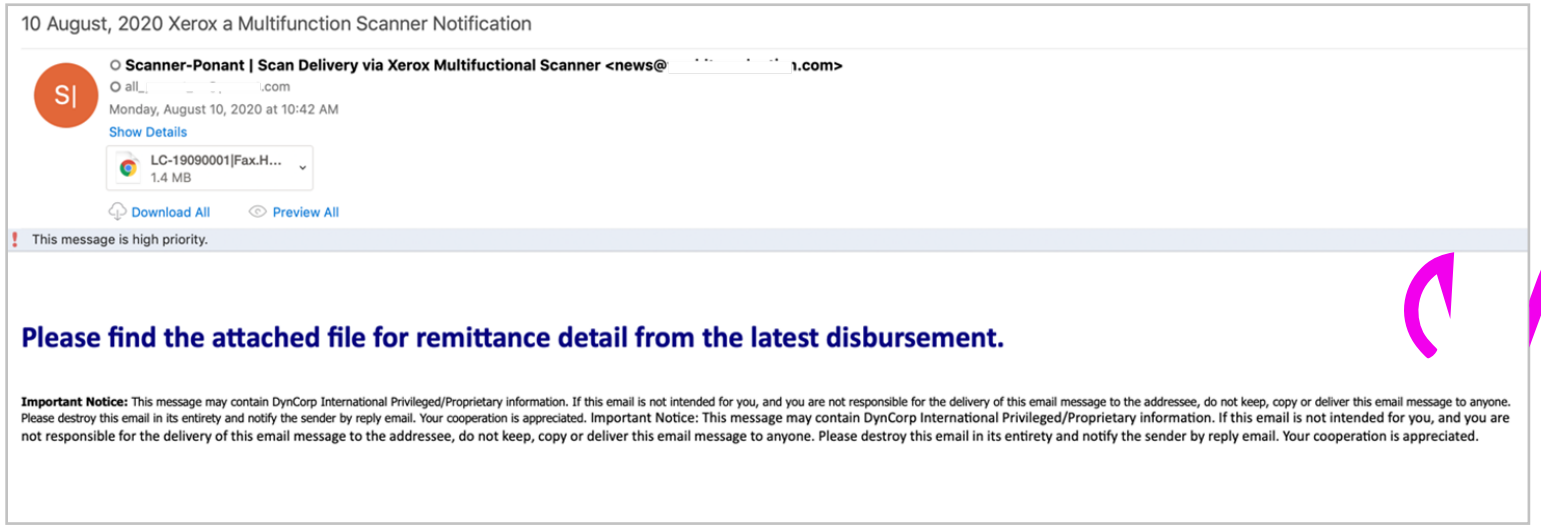
The wave coincided with a series of warnings about Emotet malware, a botnet that is a precursor to malware attacks. Emotet gangs had been on hiatus for months before reemerging in July, when Microsoft, along with cybersecurity organizations in France, Japan, and New Zealand, warned its users of Word documents featuring links and malicious macros that unleash Emotet.

Microsoft warned its users again in September about a new wave, followed by warnings from security organizations in Italy and the Netherlands. The new wave featured password-protected .ZIP files containing Emotet.

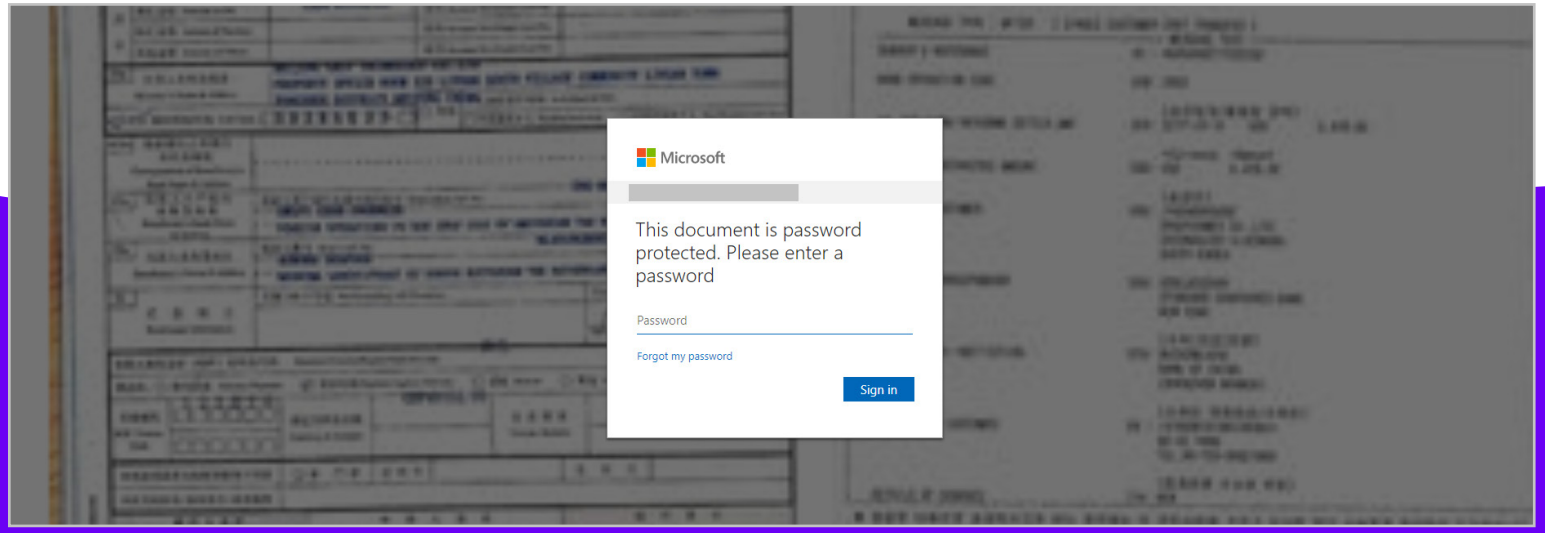


Microsoft phishing fell back to normal levels in Q4, with 9,013 unique phishing URLs detected. The Emotet wave cleverly exploited user trust in the Microsoft brand name. Microsoft Word is the most standard electronic document in use around the world. This visual cue brings with it perceived authenticity and an opportunity for cybercriminals to exploit it.

We saw this throughout 2020 with phishing emails that impersonated brands other than Microsoft yet featured links to Microsoft products, including Microsoft 365 and its applications. Many COVID-19 phishing emails, for example, impersonated health organizations but asked users to login to Microsoft 365 to retrieve files and special announcements. In the below example, the cybercriminal impersonates Dropbox and links to a prepopulated Microsoft form.



Xerox phishing email



Microsoft form

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 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.

ABOUT VADE

Vade helps MSPs and ISPs protect their users from advanced cyberthreats, such as phishing, spear phishing, malware, and ransomware. The company's predictive email defense solutions leverage artificial intelligence, fed by data from 1 billion mailboxes, to block targeted threats and new attacks from the first wave. In addition, real-time threat detection capabilities enable SOCs to instantly identify new threats and orchestrate coordinated responses. Vade's technology is available as a native, API-based offering for Microsoft 365 or as lightweight, extensible APIs for enterprise SOCs.