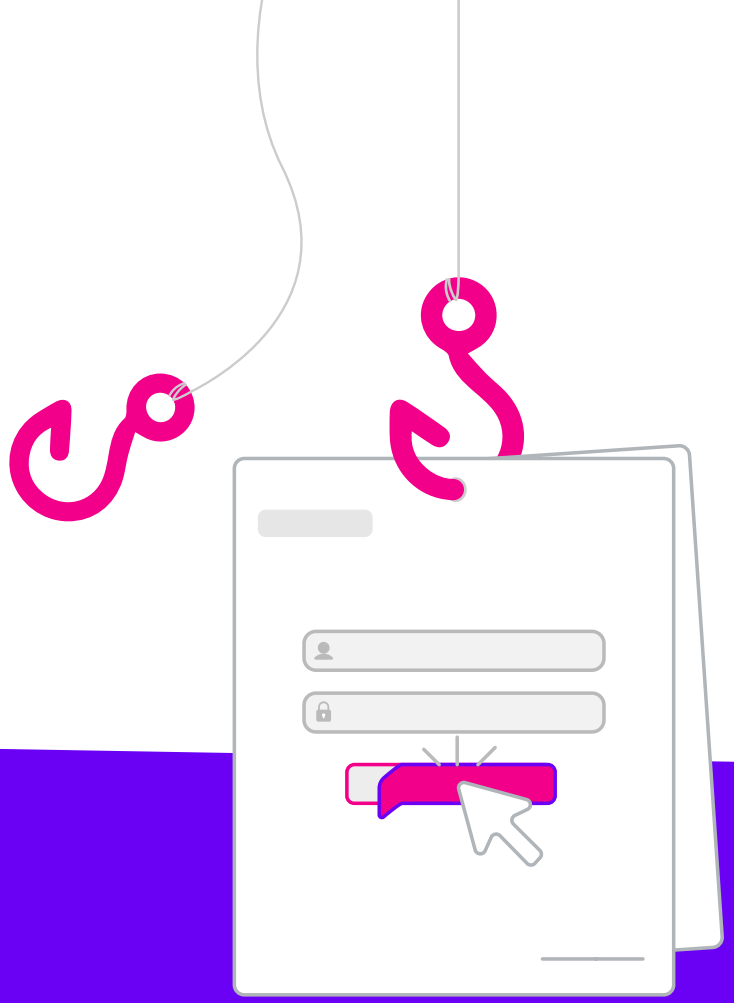
vade

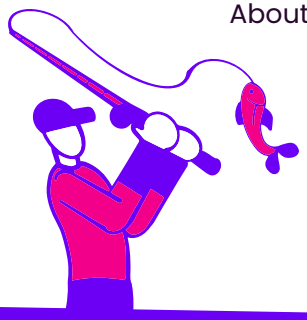


Phishers' Favorites

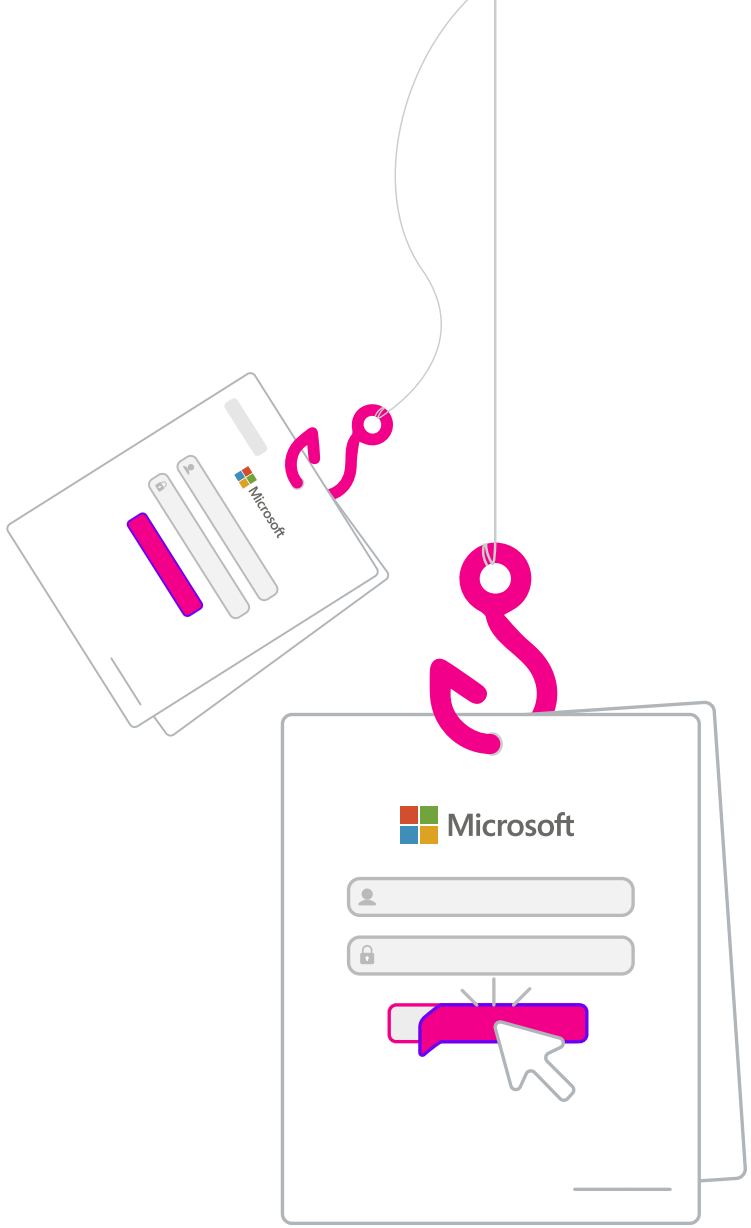
2021 Year-in-Review

www.vadesecure.com

TABLE OF CONTENTS



PHISHERS' FAVORITES YEAR-IN-REVIEW



The top 20 most impersonated brands in phishing attacks

Phishers' Favorites Year-in-Review is Vade's annual report highlighting the top 20 most impersonated brands in phishing attacks and exploring key phishing trends from the year.

For this report, Vade analyzed 184,977 phishing pages from January 1, 2021 to December 31, 2021. Cybercriminals often send dozens, and sometimes hundreds or thousands of phishing emails containing the same unique phishing URL, while a single domain can host thousands of unique URLs.

The top 20 most impersonated brands in phishing attacks

Facebook is the most impersonated brand of 2021, marking its first year at the top of the list and representing 14 percent of phishing pages. Microsoft, previously in the top spot, sits at #2 on this year's list and represented 13 percent of phishing pages. Microsoft remains the most impersonated brand in the corporate market.

Crédit Agricole, representing 13 percent of phishing pages, came in at #3 on the list, thanks to a large spike in unique phishing emails in H1 2021. WhatsApp, which has seen large fluctuations in phishing over the last two years, came in at #4, with 9 percent of phishing pages, followed by La Banque Postale at #5.

Phishers' Favorites 2021

The top 20 most impersonated brands in phishing attacks

#		Brand	Category
1	↑ 1	**Facebook**	Social Media
2	↓ 1	**Microsoft**	Cloud
3	↑ 8	**Crédit Agricole**	Financial Services
4	↑ 5	**WhatsApp**	Social Media
5	↑ 13	**La Banque Postale**	Financial Services
6	↑ 15	**Orange**	Internet/Telco
7	↑ 1	**Amazon**	E-Commerce / Logistics
8	↓ 4	**Chase**	Financial Services
9	↓ 6	**Comcast**	Internet/Telco
10	↓ 7	**PayPal**	Financial Services
11	↓ 1	**DHL**	E-Commerce / Logistics
12	↓ 5	**Netflix**	Cloud
13	↓ 1	**Wells Fargo**	Financial Services
14	↓ 8	**Rakuten**	E-Commerce / Logistics
15	↓ 2	**Adobe**	Cloud
16	↑ 7	**OVH**	Internet/Telecom
17	↑ 2	**LinkedIn**	Social Media
18	↑ 16	**MTB**	Financial Services
19	↓ 2	**Apple**	E-Commerce / Logistics
20	↑ 12	**Yahoo**	Internet/Telecom

Facebook is the #1 target for brand impersonation, as social phishing gains ground

Social media phishing has steadily increased over the last three years, with Facebook firmly in the lead. Facebook's dominance in the market directly correlates with its position on the Phisher's Favorites report.

With more than 2.8 billion active users and a slew of social brands under the new Meta name, including Instagram and WhatsApp, Facebook is a lucrative target for hackers looking to reach a wide audience.

Additionally, 2021 saw a string of high-profile ups and downs for Facebook, from its starring role in politically charged arguments about freedom of speech, to Facebook's rebranding to Meta, to its ongoing fight against misinformation. Cybercriminals are opportunists, and they have a strong preference for attacking brands during periods when the brand is top of mind with end users.

Facebook phishing runs the gamut from fake security alerts to password reset requests, each directing to a phishing page designed to steal user credentials.

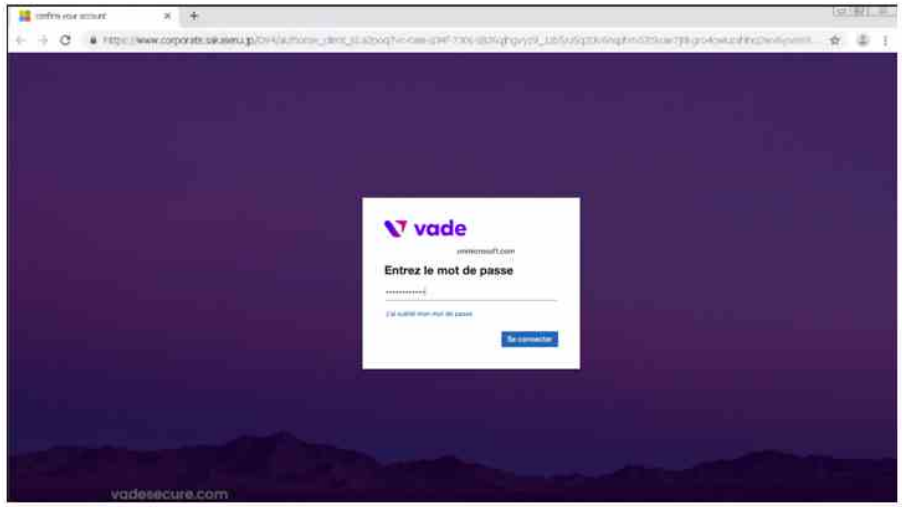
Microsoft phishing sophistication hit new levels

2021 saw a number of highly sophisticated attacks against Microsoft users. Unlike the phishing attacks of old, with little more than a Microsoft logo and phishing link, these attacks were highly automated and expertly targeted. As corporate users are more security aware than average consumers, cybercriminals have learned that it will take more than run-of-the-mill phishing emails to break through.

In late June, Vade detected a sophisticated Microsoft phishing attack in which corporate logos and background images were automatically rendered onto Microsoft 365 phishing pages. Highly targeted, the attack was designed to trigger only if the email reached the intended victim, which the hacker validated by sending an API call to Microsoft with the victim's email address. If unintended users clicked on the phishing link, they were directed to a safe webpage.

After confirming the victim's identify, the phishers made an HTTP post request for the logo and background image of the victim's corporate identity.

The hacker then redirected the victim to a custom Microsoft 365 login page featuring the corporate logo and background image of the corporate identity associated with the victim. Below is an example of the dynamic webpage, with Vade's branding to illustrate the resulting page.

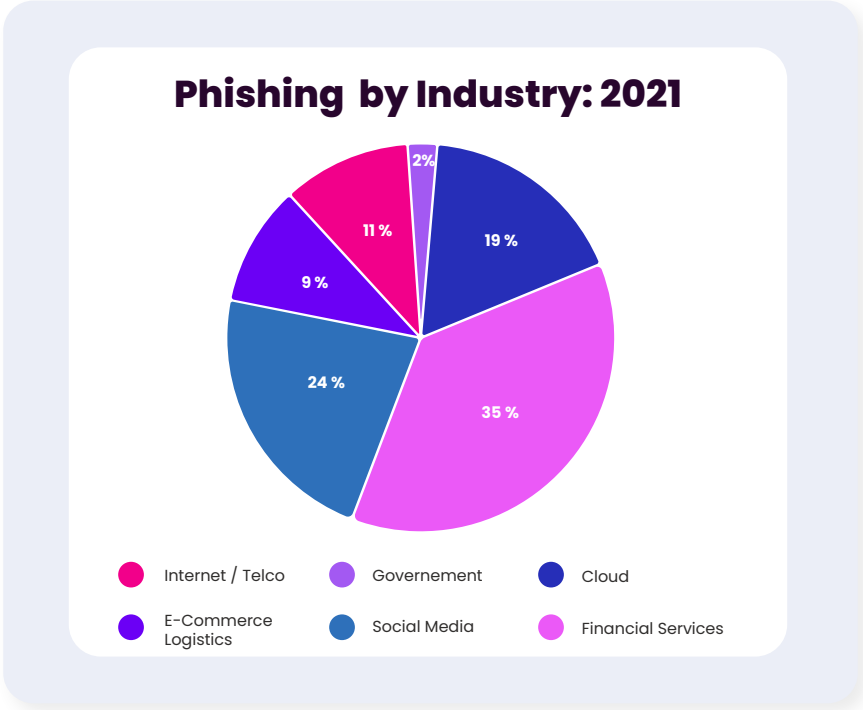


The above example reveals the level of sophistication that we are now seeing on a daily basis with phishing and demonstrates the progress that cybercriminals have made with automating their attacks.

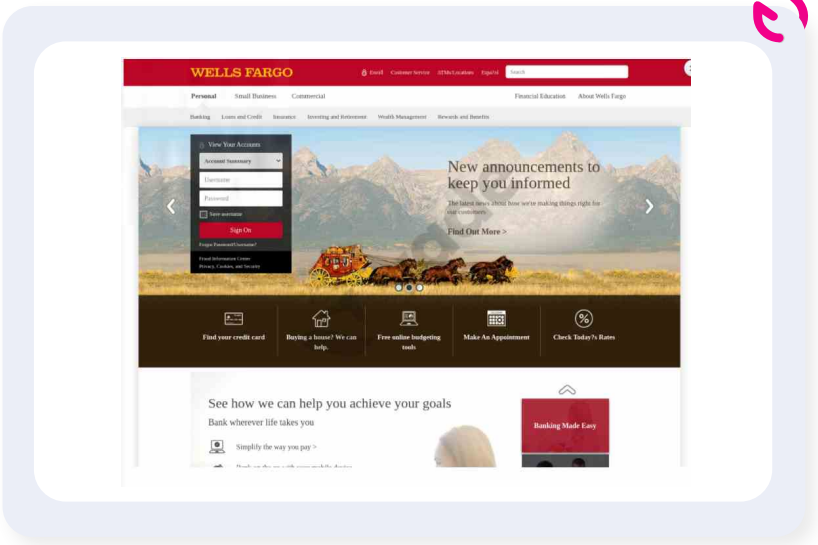
Combined with other Microsoft attacks throughout the year, including the Microsoft Exchange hack, this attack shows that Microsoft remains one of the top targets for cyberattacks and that those attacks are being launched by highly sophisticated, organized groups who do not rely on simple phishing emails and webpages.

Financial services overtakes cloud as the most impersonated industry

Financial services phishing dominated 2021, with cloud dropping to third place on the list of most impersonated industries of the year. Social media, the fourth most impersonated industry of 2020, jumped to the second spot in 2021, representing 24 percent of phishing pages. Cloud came in third, with 19 percent of phishing pages.



Financial services phishing started out strong in Q1, representing 24.5 percent of phishing pages. By Q3, financial services represented 36.3 percent of all phishing websites. For the year, financial services represented 35 percent of phishing pages and had six brands in the top 20, including Chase, PayPal, and Wells Fargo.



The trend toward financial services phishing began in Q1 2021 and continued through Q4. Growth in financial services phishing could be attributed to the impact of COVID-19 on the global economy.

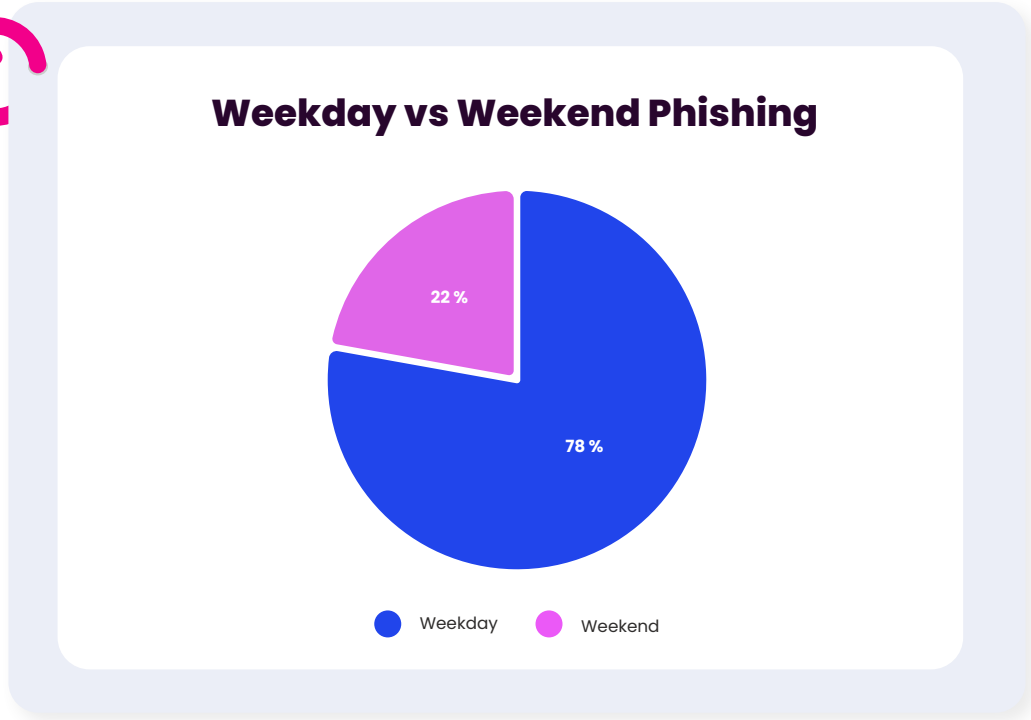
At the beginning of the crisis, businesses and citizens around the world took advantage of government-backed business loans and payment deferrals or “holidays” from consumer banks and credit unions. Crédit Agricole processed 211,000 applications for small to midsized business and small business and corporate loans, totaling €315 billion.

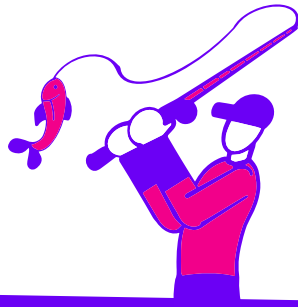
In February 2021, the bank announced a “return to normal,” with only 93,000 “payment holidays” out of 552,000 still active. As citizens returned to work, economies recovered, and payment moratoriums expired, those bills became due.

This is a significant weapon for phishers to wield against businesses and individual citizens who borrowed or deferred. Many businesses owners, hit hard by the pandemic, are still struggling with the consequences of lost business. As the pandemic rages on, the financial troubles resume, leaving millions of potential victims for phishers to exploit.

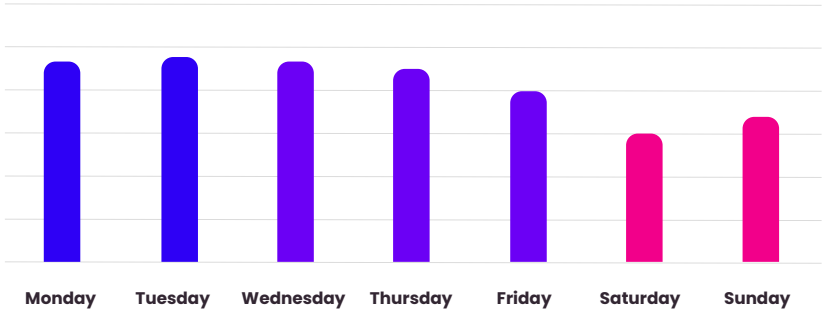
Mondays and Tuesdays were the top days for phishing

Weekdays were the most popular days for phishing in 2021. Overall, 78 percent of all phishing emails were sent on weekdays, while 22 percent were sent on weekends.



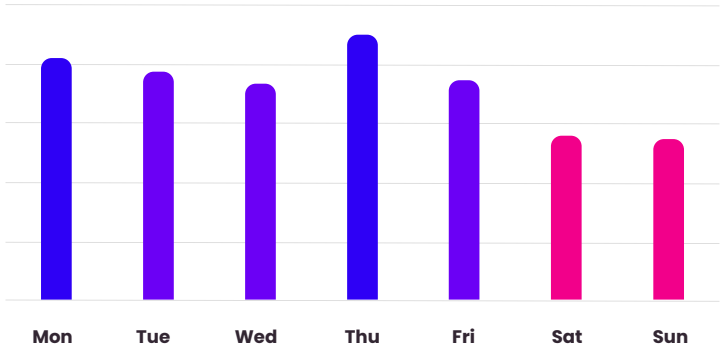


Phishing by Day of Week



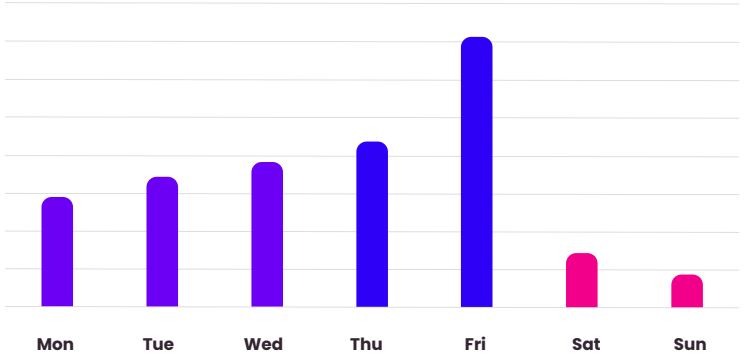
Tuesday was the top day for phishing in 2021, followed by Monday in second place, and Wednesday following closely behind.

Top Days for Facebook Phishing



While Microsoft phishing is considerably less frequent on weekends, Facebook phishing remains strong. This could be due to that fact that social media users are active on Facebook as well as personal email on weekends, while Microsoft users are less likely to interact with corporate Microsoft accounts, including Microsoft 365, on weekends.

Top Days for Microsoft Phishing



The spike in Friday phishing is a result of an August 2021 campaign that saw triple digit phishing URLs in a single day from 20 separate domains.

Phishers followed current events

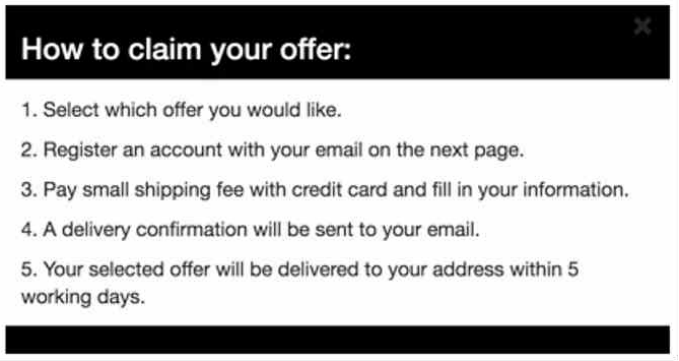
From sporting events, to holidays, to elections, current events capture the attention of users around the world. They present a prime opportunity for phishers to attack a wide pool of victims for whom the events are top of mind and are likely to respond to emails containing keywords and images associated with the event.

COVID-themed phishing

Now entering its third year, the pandemic continues to provide fodder for phishers looking to manipulate users' emotions. In Q2 2021, Vade detected 6.5 million COVID-themed emails targeting corporate email accounts. During that time period, 10 percent of all COVID-themed emails in the US and Europe were malicious.

In March, Vade detected 1 million fraudulent vaccine-related emails over the course of three days. Subject lines included in the campaign included *"Important Pfizer Vaccine Message for you, "Pfizer Vaccine Survey Response Needed," and "Pfizer COVID-19 Survey Response Confirmation".*

The campaigns used a series of evasive techniques to bypass detection, including inserting random noise into the text to trick email filters, use of remote images to conceal the text, and use of high-reputation domains to host the images or redirect to the final malicious website, including https://storage.googleapis.com. Users were then instructed to create an account and pay a shipping fee to claim their "prize".



Vaccine hesitancy also provided a perfect lure for phishers. COVID-19 vaccines have sparked high emotions in every corner of the world. Phishers' capitalized on the emotions of people on all sides of the argument, from those in favor of passports to those vehemently opposed to any mandate related to COVID vaccines.

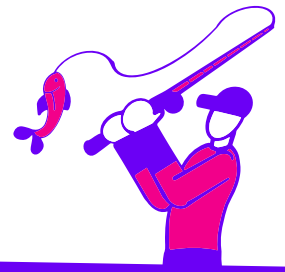
Tech support scams preyed on home workers

In March 2021, Vade detected a large wave of technical support scams featuring fake antivirus renewal invoices from Microsoft, McAfee, and Norton. From March to April, Vade detected more than 1 million tech support emails.

Unlike most phishing scams, the emails did not include links to phishing websites but included phone numbers that users were encouraged to call to either cancel or renew their subscriptions.

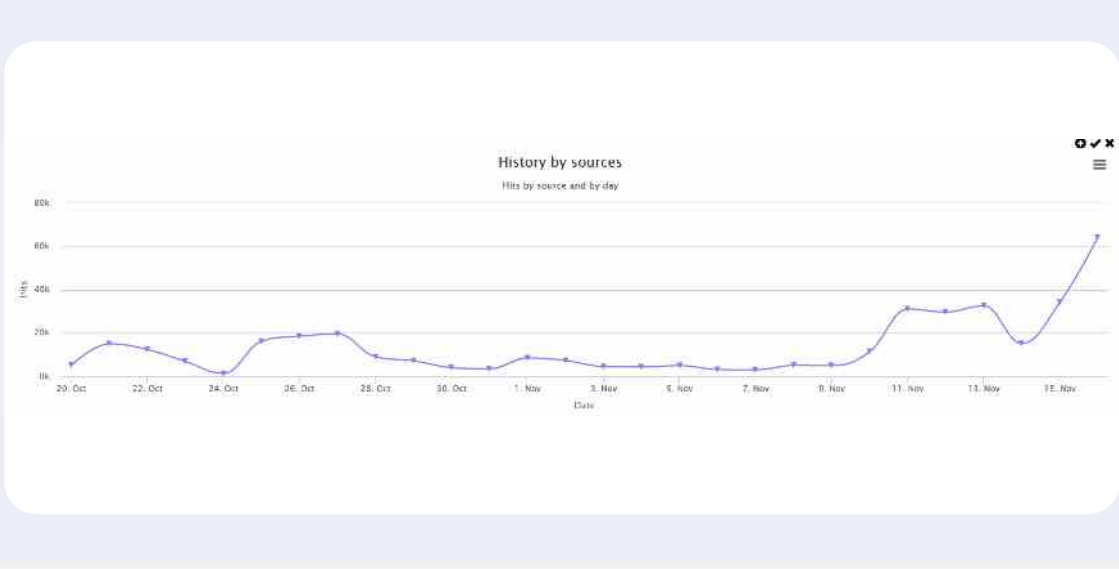
The goal of the scam is to lure the victim into a telephone conversation to avoid being charged for the antivirus subscription. During the phone call, the hacker convinces the victim to install AnyDesk remote access software on their computer.

The hacker then uses disguised script to convince the victim that their computer is infected with malware. To remove the malware, the victim must relinquish personal information. In the interim, the hacker can also download additional software onto the victim's computer.

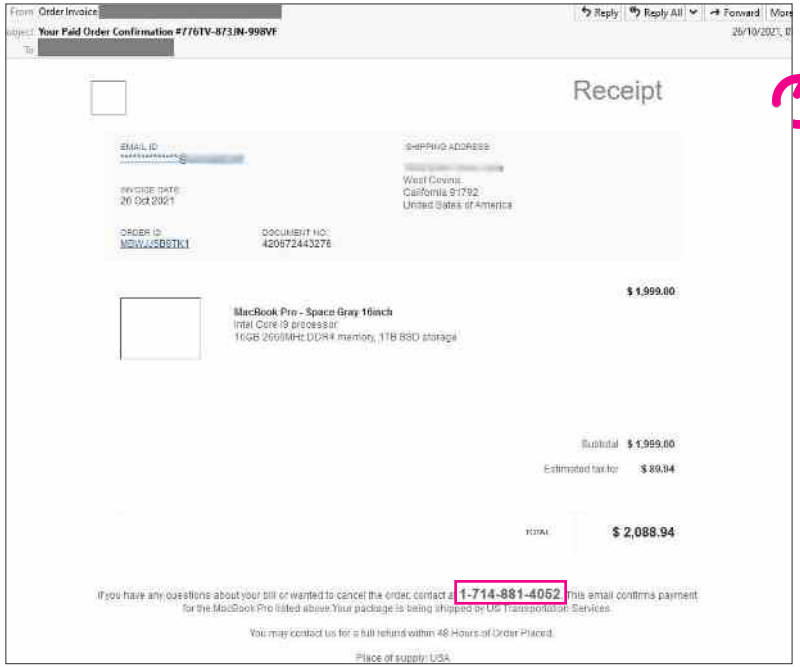


Tech support scams evolved into new forms

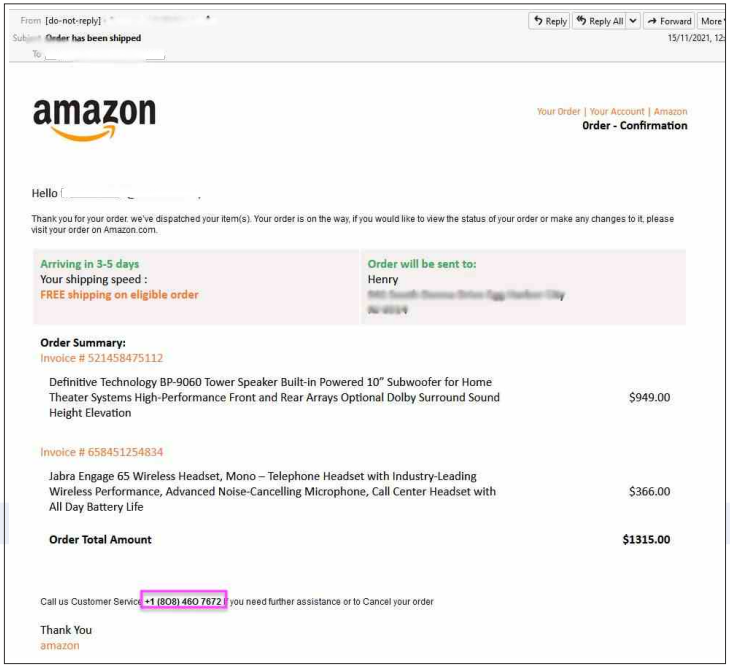
The tech support scam resurfaced later in the year in a another format during peak phishing season. In October, Vade began tracking Amazon and Apple phishing scams that used the same format as the tech support scams. By mid-November, two weeks before Black Friday, the phishing emails spiked, with a single-day high of 60,000 phishing emails.



Like the tech support scams, the phishing emails included a telephone number but no phishing links. This time, phishers used fake invoices for high-value purchases, including MacBooks and subwoofers.



Apple Impersonation



Amazon Impersonation

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.

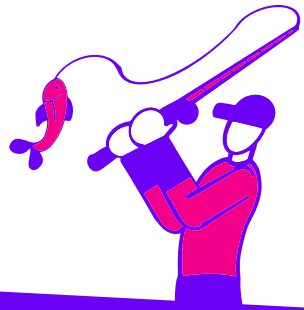
Automated Incident Response: Phishing emails that bypass a filter will not go unopened for long. Automated phishing incident response removes threats post-delivery, reducing manual investigation and response.

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 is a global cybersecurity company specializing in the development of threat detection and response technology with artificial intelligence. Vade's products and solutions protect consumers, businesses, and organizations from email-borne cyberattacks, including malware/ransomware, spear phishing/business email compromise, and phishing.

Founded in 2009, Vade protects more than 1 billion corporate and consumer mailboxes and serves the ISP, SMB, and MSP markets with award-winning products and solutions that help increase cybersecurity and maximize IT efficiency.



vade

Subscribe to our blog:

www.vadesecure.com/en/blog

Follow us :