Forbes New Phishing Schemes To Watch Out For

Alex Vakulov Contributor

Oct 25, 2024

Close up of hands tying. Getty

When it comes to cybercrime, phishing is one of the biggest threats—and for good reason. It is a gateway for different types of malware (including ransomware) and plays a key role in data theft and identity fraud schemes.

For cybercriminals, the appeal of phishing attacks lies in their profitability and simplicity. They are relatively easy to pull off, especially if the fake email is crafted to trigger the right emotional response from the recipient.

Here are some of the most common phishing schemes that cybercriminals use to trick unsuspecting victims:

- Exploiting fears around elections, the pandemic or other significant events.
- Sending fraudulent emails about changes to salaries or updates to banking agreements.
- Capitalizing on the buzz around popular TV shows and blockbuster movies.
- Taking advantage of the excitement surrounding major sports events.
- Tempting victims with discounts, fake giveaways, and offers for easy loans.
- Exploiting shipping services by sending messages that prompt targets to check delivery statuses or pay taxes.
- Scamming people with fake travel booking services that promise deals but deliver nothing.
- Preying on the popularity of dating apps to trick users into revealing personal information.
- Sending fraudulent emails encouraging users to sign up for popular cloud storage or streaming services or to renew subscriptions

The list shows how closely scammers track trends and adapt their tactics to fit what is popular. While this flexibility is vital to effective fraud, the right tactics are just as important for a successful phishing campaign.

Hackers Are Pushing the Boundaries

Automated defenses against phishing attacks are constantly improving to tackle new threats. Secure email gateways (SEGs) successfully filter out most suspicious messages, and many antivirus tools can block content that matches known phishing patterns. However, fraudsters are always finding ways to bypass these protections. Here are some tactics they use to stay ahead of cybersecurity experts.

Using Google Docs Comments as a Vehicle for Phishing Links

In 2022, criminals adopted a phishing technique that exploits Google Docs' commenting feature. They create a document, add a comment with a harmful URL, and tag the victim with an "@" mention. This triggers an email notification prompting the victim to respond.

Since the message appears to come from Google, security tools often miss it. Moreover, the notification shows only the sender's name, making it easy for attackers to impersonate trusted contacts. Clicking the link leads to a site that aims to steal sensitive information.

Google Forms Exploited to Conceal Malicious Links

Similar to the previous tactic, this phishing scheme exploits a trusted Google service. The attacker creates a Google Form survey with a phishing link embedded in a response option, using lures like "Pending Refund."

The attacker adds the target's email, sending an invitation to complete the survey. Because it is sent by Google, security filters overlook it, and the victim is likely to engage, risking malware or the exposure of personal data.

Cloud Platforms Exploited as Hubs for Credential Phishing

Fraudsters are increasingly using popular cloud services to host malicious files, adding a false sense of legitimacy that fools even cautious users. In one scam, phishers upload a decoy PDF to Google Drive, claiming it contains important information. When the victim clicks "Access Document," they are led to a fake login page for their Office 365 password. Next, a pop-up asks for Outlook credentials.

After providing their email and password, the victim can view the PDF, which is actually a legitimate marketing report. All pages are hosted on Google Cloud Storage, making it difficult to detect the scam.

Phishing Protection Tips

Stay alert and follow these simple dos and don'ts to guard against phishing:

- Avoid clicking links in emails- Do not open attachments from unknown senders.
- Ensure login pages use HTTPS, not HTTP, before entering credentials.
- If you must click an emailed link, check for typos in the URL.
- Look for spelling or grammar errors in messages claiming to be from trusted brands.
- Be wary of emails with urgent deadlines.
- Limit personal info on social media to avoid giving phishers clues for targeted attacks.