Facebook: A Top Launching Pad For Phishing Attacks

By Lindsey O'Donnell

Published: 2020-10-20 · Archived: 2026-04-05 15:24:39 UTC

Amazon, Apple, Netflix, Facebook and WhatsApp are top brands leveraged by cybercriminals in phishing and fraud attacks – including a recent strike on a half-million Facebook users.

Facebook has been a top cybercriminal favorite in phishing attacks so far this year, with recent research shedding light on 4.5 million phishing attempts that have leveraged the social media platform between April and September 2020.

Behind Facebook, messenger app WhatsApp is the second-top platform leveraged by attackers (with 3.7 million phishing attempts), followed by Amazon (3.3 million attempts), Apple (3.1 million attempts) and Netflix (2.7 million attempts).

Google's offerings (including YouTube, Gmail and Google Drive) took sixth position, with 1.5 million phishing attempts altogether according to a Tuesday analysis released by Kaspersky.

Of note, many of these targeted web services are also frequently accessed by employees of small and medium businesses while working — potentially opening up risks for sensitive corporate data, researchers warned.

"We can't imagine our daily lives, and work, without different web services, including social media, messenger apps and file-sharing platforms," said Tatyana Sidorina, security expert at Kaspersky, in a statement. "However, it is important for any organization to understand where threats may come from, and what technology and awareness measures are needed to prevent them. Businesses also need to provide their employees with comfortable use of services they require, so it is crucial to get the balance right."

Facebook's incredible user base — with more than 2.7 billion monthly active users as of the second quarter of 2020 – makes it an attractive brand for cybercriminals to tap into. The social-media giant's access to a slew of private data, such as private messages, is another reason why attackers are leveraging Facebook.

In fact, just this week a report shed light on a Facebook phishing campaign that hit at least 450,000 victims. The attack sent Facebook users a link via Messenger that appeared to be a YouTube video. However, when victims clicked on the link, they were redirected to multiple websites and ultimately led to a Facebook phishing page. The attackers were then able to collect victims' Facebook credentials.

Previous cybercriminals have also targeted Facebook over the years with new tricky tactics, including reproducing a social login prompt in a "very realistic format" inside an HTML block, and targeting Facebook's ad platform for years in an attack that siphoned $4 million from users' advertising accounts.

Most used services	Most commonly blocked services	Top services, by phishing attempts
YouTube	**Facebook**	**Facebook**
Facebook	Twitter	WhatsApp
Google Drive	Pinterest	Amazon (all services)
Gmail	Instagram	Apple (all services, including iCloud)
WhatsApp	LinkedIn	Netflix

Credit: Kaspersky

Facebook is also one of the most-used services by corporate employees, with Kaspersky finding that YouTube and Facebook are the top two services that employees at small and medium businesses access on their corporate devices (Google Drive, Gmail and WhatsApp follow closely behind).

“With the two lists sharing many of the services, these results only confirm the trend that popular applications have become valuable platforms for fraudsters’ malicious actions,” according to researchers.

On the other side of the coin, the social-media platform is also a top blocked application by corporate companies. Other top blocked applications include Twitter, Pinterest, Instagram and LinkedIn.

Researchers also noted that messengers, file-sharing or mail services are not commonly blocked, “likely because they are often used for working purposes as well as for personal needs.” These products — including Google’s services (Gmail and Google Drive) — are often still leveraged in targeted attacks by cybercriminals.

These statistics, which were obtained for the period between April and September using Kaspersky’s distributed antivirus network (the Kaspersky Security Network, or KSN), consist of depersonalized metadata which is voluntarily provided by KSN participants among Kaspersky customers, a spokesperson told Threatpost.

Researchers said that moving forward, companies should keep an eye out for emerging popular brands – like the TikTok short-form video application – with big user bases that scammers will inevitably flock to for phishing attacks and other malicious purposes.

“While organizations can have different priorities and permissions for what web services can be used by their employees, it is important for organizations to understand all of the relevant threats they could face and how they can infiltrate corporate endpoints,” according to researchers. “Once a web service becomes popular, it is likely that it will become a more attractive target amongst scammers.”

Source: https://threatpost.com/facebook-launching-pad-phishing-attacks/160351/