Norton Consumer Cyber Safety Pulse Report: Phishing for New Bait on Social Media

2022-07-26

Year-long analysis from Norton Labs finds nearly three-quarters of phishing sites imitate Facebook

TEMPE, Ariz., July 26, 2022 /PRNewswire/ -- NortonLifeLock's global research team, Norton Labs, today published its quarterly Consumer Cyber Safety Pulse Report, detailing the top consumer cybersecurity insights and takeaways from April through June 2022. Leveraging the company's global threat telemetry, the analysis includes new findings on how cybercriminals are using social media phishing attacks to steal people's private information.

Norton Labs analyzed a full year of phishing attacks on the top social media platforms, and while plenty of fake login pages designed to trick victims into inputting their login credentials were found, the diversity and complexity of lures went far beyond that one technique.

"Threat actors use social media for phishing attacks because it's a low-effort and high return way to target billions of people around the world," said Darren Shou, head of technology, NortonLifeLock. "As social media is intertwined in our daily lives, it's key to know how to spot the signs of a scam, and keep a sharp eye on where requests for your information are coming from. Even better, consider strong, multi-layered security that can be on the lookout for you."

Norton Labs uncovered the top tactics cybercriminals use to get victims to reveal personal information, and while classic login phishing pages are still the most common ploy, cybercriminals are finding new ways to deceive social media users. Tactics include account lockouts – making it seem that a victim's account has been locked luring victims to reveal login credentials or install malware on the promise of increasing follower count; and verified badge scams – prompting users to login to obtain, or not to lose, their verified status on the platform.

Another phishing campaign tactic aims to intercept temporary codes to break into profiles with two-factor authentication enabled. These tokens are generally tied to the victim's device and allow the scammer to perform privileged operations such as modifying personal details or login credentials.

This quarter, Norton also found that it's never too early for scammers to take advantage of the back-to-school season. As school-aged children enjoy their summer, cybercriminals are already at work, using the back-to-school time to inspire a variety of financial scams, such as bogus offers of scholarships and financial aid.

By the Numbers

From April through June 2022, Norton thwarted over 900 million threats, or around 10 million threats per day. Norton blocked:

- 22.6 million phishing attempts
- 103.7 million file threats
- 302 thousand mobile threats
- 78 thousand ransomware attacks

For more information and Cyber Safety guidance, visit the Norton Internet Security Center .

About NortonLifeLock Inc.
NortonLifeLock Inc. (NASDAQ: NLOK) is a global leader in consumer Cyber Safety, protecting and empowering people to live their digital lives safely. We are the consumer's trusted ally in an increasingly complex and connected world. Learn more about how we're transforming Cyber Safety at www.NortonLifeLock.com.

Jenna Torluemke	Audra Proctor
NortonLifeLock Inc.	Edelman for NortonLifeLock Inc.
Jenna.Torluemke@nortonlifelock.com	Audra.Proctor@edelman.com

View original content to download multimedia:https://www.prnewswire.com/news-releases/norton-consumer-cyber-safety-pulse-report-phishing-for-new-bait-on-social-media-301592846.html

SOURCE NortonLifeLock Inc.