Norton Consumer Cyber Safety Pulse Report: Sneaky Ways Your Privacy and Security Could Be Compromised

2022-10-18

Privacy, phishing and scams – oh my. Here's what cybercriminals have been up to the past quarter.

TEMPE, Ariz. and PRAGUE, Oct. 18, 2022 /PRNewswire/ -- Norton Labs, the global research team at NortonLifeLock (NASDAQ: NLOK), today released its quarterly Consumer Cyber Safety Pulse Report, detailing the top consumer cybersecurity threats and insights from July through September 2022. Leveraging the company's global threat telemetry, the report includes an analysis of the most recent ways cybercriminals are putting privacy and security at risk.

Norton Labs analyzed recent attacks on top companies that were compromised through stolen login credentials. While these campaigns aimed to steal the information that could later be monetized against victims, the goal was to undermine the trusted technologies used to send automated emails, authentication codes, and an entire company's single sign-on.

"Cybercriminals have become experts at catching one-time codes used in most two-factor authentication and they know that by undermining the systems that send the codes, their efforts are even more effective," said Jeff Nathan, Technical Director and Researcher, NortonLifeLock. "Consumers should use FIDO U2F tokens everywhere they can as they aren't susceptible to these phishing attacks."

Cybercriminals are also turning to scam e-shops offering electronics, jewelry, clothes, and everything in between to lure victims. According to the FTC, there were 397,826 reports of online shopping fraud in 2021, totaling $392 million in losses. These sites often seem legitimate with polished storefronts, positive reviews, ties to social media accounts and more. However, once you place an order, you may receive a counterfeit item or nothing at all. Norton Labs warns shoppers to watch out for prices that may be too good to be true, be wary of sites that request unusual payment-processing methods and to beware of social media ads and unsolicited messages. Using a URL lookup tool like Norton Safe Web can also let shoppers know if a site is already known to be a malicious/scam domain.

Another alarming discovery from Norton Labs is that 80 percent of websites share search terms with advertisers either accidentally or deliberately. Trackers can gain information from website visits, such as a user's IP address, the website's content, domain and more. This offers third parties a user's search terms which can include sensitive information like medical concerns or family and legal situations. Advertisers may then use these characteristics to target ads in unexpected or potentially uncomfortable ways.

Behind the Data

From July through September 2022, Norton thwarted over 750 million threats, or around 8 million threats per day. Norton blocked:

- 25.2 million phishing attempts
- 103.7 million file threats
- 330 thousand mobile threats
- 63 thousand ransomware attacks
- Over 1 billion trackers and fingerprinting scripts blocked by Norton AntiTrack

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
NortonLifeLock Inc.
Jenna.Torluemke@nortonlifelock.com

Audra Proctor
Edelman for NortonLifeLock Inc.
Audra.Proctor@edelman.com

View original content to download multimedia:https://www.prnewswire.com/news-releases/norton-consumer-cyber-safety-pulse-report-sneaky-ways-your-privacy-and-security-could-be-compromised-301651475.html

SOURCE NortonLifeLock Inc.