Latest Norton Consumer Cyber Safety Pulse Report Unveils Top Phishing Scams

2021-07-20

New Threats Observed Across Encrypted Chat Marketplaces, Online Cookies, and Vulnerable Gaming Drivers

TEMPE, Ariz.--(BUSINESS WIRE)-- NortonLifeLock's global research team Norton Labs today published its second quarterly Consumer Cyber Safety Pulse Report, detailing the top consumer cybersecurity insights and takeaways from April to June 2021. Leveraging the company's global threat telemetry, the analysis reveals the three most common phishing scams, in addition to new threats in encrypted chat marketplaces, online cookies, and vulnerable gaming drivers.

(Graphic: Business Wire)

Norton thwarted 23.7 million phishing attempts between April and June 2021, with tech support scams, survey scams and supplement scams ranking as the top types of phishing scams seen. These scams are specifically designed to trick unsuspecting consumers to share personal information or engage in behavior that puts their privacy at risk.

"Cybercriminals often take advantage of current events to make their scams more convincing," says Darren Shou, head of technology, NortonLifeLock. "As the world begins to open up, we anticipate scammers will pivot to tailor their phishing attempts to tie into themes like travel and back-to-school."

Over the past quarter, Norton blocked 909 million Cyber Safety threats in total, including 56 million file-based malware, 405,710 mobile-malware files, and 85,339 ransomware detections.

Additional findings from the report include:

- **Online tracking ecosystem is much larger and more sprawling than generally understood:** Amid intensifying privacy concerns and legislative action pushing for companies to limit the data they collect on online users, Norton discovered the online cookie ecosystem is much larger than previously understood. The analysis identified as many as 171,140 organizations that are involved in the creation and sharing of cookies, a figure that's 2.5x more than generally understood.
- **Encrypted chat app is doubling as illegal marketplace:** Cybercriminals are exploiting a popular chat app's encryption capabilities to sell illegal goods – everything from COVID-19 vaccines and personal information, to pirated software and fake IDs. Research also found cybercriminals are selling tools and services to facilitate cybercrime, such as distributed denial-of-service (DDoS) infrastructure.
- **Vulnerabilities in drivers expose new threat to gamers:** Cybercriminals are devising social engineering schemes that play into gamers' hyper-competitive spirits and trick gamers into installing compromised drivers on their PCs. This in turn infects their computer systems, which can lead to stolen personal information, account takeovers, and even loss of virtual gaming swag.

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.
(650) 527-6015
Jenna.Torluemke@nortonlifelock.com

Heaven Lampshire
Edelman for NortonLifeLock Inc.
(541) 852-7885
Heaven.Lampshire@edelman.com

Source: NortonLifeLock Inc.