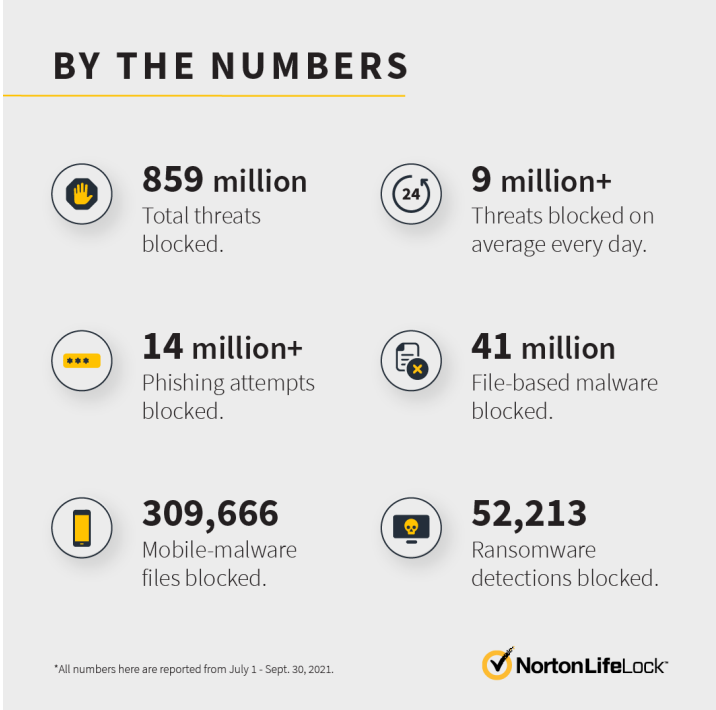
NortonLifeLock Consumer Cyber Safety Pulse Report
July 1 – September 30, 2021

SUMMARY & KEY FINDINGS

In October, NortonLifeLock's global research team, Norton Labs, published its third quarterly Consumer Cyber Safety Pulse Report, detailing the top consumer cybersecurity insights and takeaways from July 1 to September 30, 2021. Analyzing data from NortonLifeLock's threat telemetry, which blocks more than 9 million threats on average every day, the report provides a quarterly look at the top privacy, security and identity threats impacting consumers.

The latest findings show tech support scams, which often arrive as a pop-up alert convincingly disguised using the names and branding of major tech companies, have remained a top phishing threat and more recently surged to take the number one place. Attackers have leveraged the pandemic and consumers' increased reliance on devices to manage hybrid work schedules and family activities to successfully deploy tech support scams. These scams are expected to further proliferate in the upcoming holiday season, alongside shopping and charity-related phishing attacks[1].



Additional Norton Labs findings from this Consumer Cyber Safety Pulse Report include:

Virtual gaming goods have real value: Rare, in-game items are highly sought after and can be traded on real-world marketplaces. For example, RuneScape, a multiplayer online role-playing game touts a virtual blue "Party Hat," which was most recently valued at approximately $6,700. A new phishing campaign, specifically designed to obtain RuneScape players' login credentials and two-factor authentication information, was deployed with the intent to steal and sell such high value virtual items.

Fraudulent online banking pages are convincing: A punycode phishing campaign targeted Citibank customers with a near carbon copy of the real banking homepage to trick them into entering their credentials. For this type of phishing campaign, attackers host a fraudulent homepage using an internationalized domain name (IDN) to resemble the legitimate banking domain, in this case "citi.com." The fraudulent domain name was registered by the attackers in punycode as "xn--ct-njab.com," which web browsers convert and display as "cítí.com" in the address bar. Cybercriminals continue to find combinations of characters that are deceivingly close to high-profile targets, such as major banks.

[1] No one can prevent all cybercrime or identity theft.

Stolen gift cards are (almost) as good as cash: Gift cards are a prime target for attackers because they typically have lower security than credit cards and aren't tied to a specific person's name. Further, many gift cards are made by the same company with a 19-digit number and 4-digit PIN. Attackers use websites intended to check a gift card's balance to uncover valid card number and pin combinations, giving them full access to the funds.

Vaccine passports carry potential privacy and fraud concerns: Vaccine passports, or digital vaccination certificates, have raised questions of privacy, security and ethics. While vaccine passports can be a helpful tool in reducing the transmission of COVID-19 across borders and in high-risk environments (stadiums, travel, etc.), the passports also present two risks – if they're not designed with privacy in mind, they could create the potential for governments and private companies to invade the privacy of millions of people. Further, if security is not baked in, there's the potential for unvaccinated people to forge valid-looking passports that defeat the system.

Phishing attacks continue to reel in victims: As one of the most common online scams, phishing campaigns have existed for more than 20 years, manipulating and exploiting people's emotions to gain access to their information. Further, phishing kits are freely available, making it easier for hackers with little technical knowledge to launch a campaign and successfully access sensitive information that can be sold for monetary gain.

Hackers continue to target the Roman Catholic Church and the Vatican: Hackers, potentially operating out of China, have been targeting the Roman Catholic Church and the Vatican. In one case, researchers found targeted malware in files that appear to be legitimate, Vatican-related documents but infect the devices of users who access the documents. In a second instance, computers located in the Vatican were found to have malware installed. While this type of targeted attack is usually associated with large organizations, people belonging to special interest groups, dissidents or individuals with influential jobs may also be subject to similar attacks, and general consumers should stay vigilant against phishing campaigns and infected webpages.

Norton Labs issues these reports on a quarterly basis, with the next one expected in January 2022. 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.

ABOUT NORTON LABS

Norton Labs, formerly NortonLifeLock Research Group, is NortonLifeLock's global research organization and was formed to secure the world's computing devices and information through novel security and privacy paradigms.