Gen Q3 Threat Report: Millions Fooled by "Scam-Yourself Attacks"

2024-11-19

Report Finds 614% Increase in Scams Where Cybercriminals Go After People's Desire to Learn about Technology and Problem-Solve, Supporting a Surge in Data Theft

TEMPE, Ariz. and PRAGUE, Nov. 19, 2024 /PRNewswire/ -- Gen™ (NASDAQ: GEN), a global leader in consumer Cyber Safety with a family of brands including Norton, Avast, LifeLock, Avira, AVG, ReputationDefender and CCleaner, today released the Q3/2024 Gen Threat Report. This quarter highlights cybercriminals' rapid adaptation to new tactics, including social engineering, AI and deepfake technologies, making scams much harder to spot and more dangerous than ever.

"In July through September, scams continued to dominate the threat landscape, while data-theft abusing malware and ransomware also increased rapidly," said Siggi Stefnisson, Cyber Safety CTO at Gen. "Our consistent focus is to empower people with the tools they need, such as the Norton Genie scam detector, so they can protect their digital lives as threats evolve."

A 614% Increase in Scam-Yourself Attacks
The Gen report highlights a 614% rise in "Scam-Yourself Attacks," where cybercriminals use social engineering, psychological manipulation tactics, to trick people into installing malware on their own devices. The term encompasses a variety of threats, including:

- **Fake Tutorials** – cybercriminals use video tutorials on platforms like YouTube to lure people into installing malware while pretending to provide a free download for a paid software.
- **ClickFix Scams** – under the guise of "fixing" a computer issue, a fake technical solution prompts people to copy a text into the command prompt, ultimately giving cybercriminals control of their system.
- **FakeCaptcha** – a fake CAPTCHA prompt that copies text of a dangerous code onto your clipboard and instructs the person to install this malicious content onto their device.
- **Fake Updates** – malware disguised as a necessary software update guides people to paste a malicious script into their system, giving attackers admin privileges.

Together, these Scam-Yourself Attacks form a broader web of deception that's catching millions of people off guard. Social engineering continues to be one of the most dangerous tools in the cybercriminal arsenal, underscoring the importance of security products to help detect and block malware before it's downloaded.

The Surge of Data theft using Data Stealing Malware and Ransomware

While scams have dominated the landscape, data stealing malware and ransomware are experiencing a resurgence. Data stealing malware activity, specifically information stealers, rose by 39% overall this quarter. The most popular information stealer, Lumma Stealer, increased its share by 1154%, using methods like the previously mentioned Fake YouTube Tutorials to make its way onto people's computers to collect sensitive

information including account credentials, crypto wallets and browser data.

Ransomware threats also increased, with a notable 100% rise in risk ratio, the potential risk per person. This quarter, the lead ransomware threat was led by Magniber, with outdated software – particularly Windows 7 – being the open door for ransomware actors.

Gen researchers collaborate with governments around the world to combat ransomware by providing free decryption tools for victims, and most recently released the Avast Mallox Ransomware Decryptor.

Mobile Threat Escalation: Data Stealing Malware Focusing on Identity and Financial Theft

Data stealing malware also increased on mobile devices in Q3/2024, with criminals having an eye toward identity theft. Spyware, software that gains access to sensitive data and can even screen-record, grew 166% in the quarter. In July through September, a new strain of spyware called NGate appeared, which siphons away victims' money by cloning bank card NFC data, which is used to withdraw money from physical ATMs or make contactless payments.

Banking malware – used mainly to collect banking credentials – increased by 60% quarter-over-quarter, led by the Rocinante malware with new strains such as TrickMo and Octo2 emerging.

A common denominator for the key mobile threats is their delivery via malicious SMS messages. Avast, a brand of Gen, continues to enhance its defenses against mobile-specific threats, knowing that proactive protection is critical as consumers rely more on mobile devices for personal and financial transactions. To stay safe, people should avoid clicking links in unsolicited SMS messages and ensure they have comprehensible mobile security software, such as Avast Mobile Security, to help protect them.

Norton Genie Insights: Real-Time Scam Defense in Action

As AI technologies advance, they're increasingly used by both cybercriminals and defenders. We continued to observe attackers leveraging AI-driven tactics to enhance social engineering campaigns—like generating realistic deepfakes and crafting highly tailored phishing emails and SMS messages —making scams harder to detect. Gen's AI-driven Norton Genie App adapts in real time to these advancements, empowering people with proactive, real-time threat detection against AI-enhanced deception.

Norton Genie telemetry data from 2024 highlights that after generic scams, smishing attempts –SMS messages pretending to be from banks, delivery services or government agencies, urging people to click a malicious link – are the most common scams seen by people (16.5%). Lottery scams – those where people are notified of "winnings" and prompted to share personal information or pay fees to claim a prize – came in second (12%), followed by general phishing emails and texts, package delivery scams (9.6%) and fake invoices (7.7%).

This real-time scam data helps Gen continuously refine its protections, ensuring its defenses adapt as quickly as the threats people are facing.

To read the full Q3/2024 Gen Threat Report, visit: https://www.gendigital.com/blog/insights/reports/threat-report-q3-2024

About Gen

Gen™ (NASDAQ: GEN) is a global company dedicated to powering Digital Freedom through its trusted Cyber

Safety brands, Norton, Avast, LifeLock, Avira, AVG, ReputationDefender and CCleaner. The Gen family of consumer brands is rooted in providing safety for the first digital generations. Now, Gen empowers people to live their digital lives safely, privately, and confidently today and for generations to come. Gen brings award-winning products and services in cybersecurity, online privacy and identity protection to nearly 500 million users in more than 150 countries. Learn more at GenDigital.com.

Brittany Posey-Thomas
Gen
Press@GenDigital.com

Courtney Rowles
Edelman for Gen
Courtney.Rowles@edelman.com

View original content to download multimedia:https://www.prnewswire.com/news-releases/gen-q3-threat-report-millions-fooled-by-scam-yourself-attacks-302309060.html

SOURCE Gen Digital Inc.