NOW & NEXT

Cybersecurity & Privacy Alert

JANUARY 7, 2022

New York Attorney General urges vigilance against "credential stuffing" hacks

By Jason C. Kravitz and Jenny L. Holmes

Why a new report from the New York AG means you should review your cybersecurity plans.

What's the Impact?

/ A new report from the New York Attorney General details cyberattacks affecting over one million accounts, particularly impacting the restaurant and retail industries

/ Businesses are encouraged to implement additional cybersecurity protocols

/ Experienced cybersecurity attorneys can audit your current incident response plan and recommend additional risk mitigation measures

Earlier this week, New York Attorney General Letitia James released a report summarizing the findings of a broad investigation into so-called "credential stuffing" that revealed more than 1.1 million online accounts have been compromised in cyberattacks at seventeen prominent companies. The report explains that the attacks involve repeated, automated attempts to access online accounts using usernames and passwords stolen from other online services and also offers suggestions for how businesses can protect themselves.

Credential stuffing has become a popular form of cyberattack. Most websites and apps use passwords to validate a user's identity. Because it is common for people to reuse the same passwords across multiple online services, hackers who come into possession of a user's password for one site/app can attempt to use the same password to access other online accounts linked to that user. According to the report, there are more than 15 billion stolen login credentials being circulated across the internet—giving rise to an extraordinary number of opportunities for hackers to exploit using bots or other automated mechanisms.

The AG's investigation was proactive and involved the review of thousands of dark web posts that contained customer login credentials that attackers purportedly had tested in a credential stuffing attack. From these posts, the investigators determined that customer accounts at seventeen well-known online retailers, restaurant chains, and food delivery services appeared to have been compromised in credential stuffing attacks and proceeded to warn those seventeen companies.

Preventing credential stuffing attacks

Businesses must be vigilant about protecting their customers' data, and the first step should be to review existing cybersecurity incident response plans to ensure they adequately address the threats discussed in this report. Attorneys with expertise in cybersecurity and data privacy can support an audit of your current protocols and help guide implementation of the recommended safeguards against credential stuffing attacks, including employing bot-detection technology, multi-factor authentication, and password-less authentication.

The Nixon Peabody Cybersecurity & Privacy Team will continue to monitor developments and keep you informed about best practices to protect your business.

For more information on the content of this alert, please contact your Nixon Peabody attorney or:

Jason C. Kravitz
617.345.1318
jkravitz@nixonpeabody.com

Jenny L. Holmes
585-263-1494
jholmes@nixonpeabody.com