NINJIO

Zoom Hack Analysis

Are your security credentials actually keeping you safe?

The use of digital communication and productivity tools is quickly becoming second nature for many employees. However, poor cybersecurity habits often come just as naturally, which makes these tools far more dangerous than they should be.

For example, earlier this year, the cybersecurity intelligence company Cyble discovered that it was remarkably easy and cheap to purchase more than 500,000 stolen Zoom credentials on a hacking forum. In most cases, it's likely that the passwords had been reused to open the compromised Zoom accounts – a reminder that bad cybersecurity hygiene can create easily exploitable vulnerabilities on a vast scale.

The mass theft of Zoom credentials is a cautionary tale for companies as the number of cyberattacks continues to surge, remote work remains the norm (and shows every sign of persisting in the post-COVID era), and employees continue to demonstrate a dangerous lack of cybersecurity awareness.

CARELESS CREDENTIALS LEAVE **COMPANIES EXPOSED TO CYBERTHREATS**

It's ironic that passwords, which are designed to keep employees and companies safe, are so frequently security liabilities instead of assets. According to a recent report by the Ponemon Institute, organizations cited credential theft as the most common cyberattack they've experienced over the past several months. Meanwhile, a survey conducted by Google and Harris found that more than half of Americans admit to using the same password for multiple accounts, while 13 percent use the same password for all of their accounts.

Beyond the fact that many of these passwords are common, rudimentary, and easily solved, the frequency of their use puts their owners at even graver risk. This is because cybercriminals compile and distribute extensive databases of passwords over time, which can then be tested across many different accounts to see which ones have been reused (i.e. what happened with many of the Zoom accounts). When hackers discover that a password works in one instance, they'll keep trying it to infiltrate as many of a victim's accounts as possible.

ADDRESSING THE CYBERSECURITY **AWARENESS DEFICIT**

Despite the fact that cyberattacks are on the rise and becoming far more costly every year, most people believe they're taking adequate steps to protect themselves and their organizations. For example, almost 70 percent of Americans say they would give themselves "an A or B when it comes to protecting their online accounts." But if this were the case, companies wouldn't cite credential theft and social engineering as the top cyberthreats they face.

While many forms of cybersecurity awareness require employees to make informed judgments in real time – such as spotting a phishing email or recognizing when something is wrong with a website they're visiting (such as a misspelling in the address bar or a missing encryption icon) – others are preemptive. Responsible password management falls in the latter category, which means employees can take action right now to make themselves and their companies far safer.

If employees know they're reusing passwords across multiple accounts or deploying simple passwords that can be broken, they have to take action immediately.

HOW TO ENSURE THAT YOUR **PASSWORDS ACTUALLY WORK**

Although credential theft is among the most pressing cyberthreats companies face, it can also be addressed in many different ways:

1.

Employees should only use passwords that are unique and complex. Hackers steal credentials which are either a) overused, b) too simple, or c) a combination of the two. The fix for this problem is simple: every account should have its own password, and each of those passwords should be sufficiently complex (i.e., "sPor23!@" instead of "12345678") to make them extremely difficult to crack.

2.

Use a password manager. According to McAfee, the average person has 23 online accounts that require a password. It would be difficult to keep track of 23 unique and complex passwords, which is a problem that password managers like LastPass and 1Password (which less than a quarter of Americans use) can solve instantly.

3.

Be careful with how and where you enter usernames, passwords, and other sensitive information. It's easy to forget how frequently we log in to bank accounts, company email inboxes, and other sensitive sites without even thinking. Employees should never enter passwords or other sensitive information when they're on networks they don't trust, and they should always use a VPN while on public WiFi.

One of the best ways to teach employees about the consequences of cyberattacks is to show them real-world examples of what can happen if they're careless online. This is why case studies like the leak of half a million Zoom credentials should serve as reminders that cybersecurity isn't an abstract concept – it's a way to keep our most sensitive information out of the wrong hands.

ABOUT NINJIO

NINJIO is a cybersecurity awareness training and simulated phishing company founded in 2015 that empowers individuals and organizations to become defenders against cyberthreats. The company's Hollywood-style content teaches organizations, employees, and families how not to get hacked. Today, NINJIO serves some of the largest companies in the world, and its methodology is responsible for changing the behavior of hundreds of thousands of people through engaging, emotionally-driven storytelling.