One unsecure password cost Colonial Pipeline $4.4 million: Here's how you can stay safe

Tuesday 29 June, 2021

What was the Colonial Pipeline hack?

The Colonial Pipeline, operated by Colonial Pipeline Company, is the largest pipeline system for refined oil products in the U.S.

On the 29th of April 2021, a cyber-criminal gang hacked their systems, causing one of America's most important fuel distribution companies to go offline. This disrupted supplies for several days, causing fuel shortages. The pipeline carries 45% of the East Coast's supply of diesel, petrol, and jet fuel, meaning the cyber-attack had major repercussions on a national level.

The cyber criminals demanded $4.4 million in ransom to rectify the impact of the attack, which Colonial Pipeline CEO, Joseph Blount, authorised to prevent any further damage.

He told the Wall Street Journal, "It was the right thing to do for the country. I didn't make it lightly. I will admit that I wasn't comfortable seeing money go out the door to people like this."

Once Colonial Pipeline had made the payment using cryptocurrency, they received a decryption tool from the hackers, allowing them to unlock the systems and data that had been compromised. Whilst they were able to restore their functionality, their systems didn't start immediately, and they suffered severe financial loss, as well as distrust for the company.

How did the Colonial Pipeline hack happen?

The hack occurred because of **just one compromised password**. Charles Carmakal, Senior Vice President at cyber security firm, Mandiant, confirmed that hackers gained entry to Colonial Pipeline's systems through a virtual private network (VPN) account, which allows employees to access the company's computer network remotely.

The account that they gained access from was no longer in use, but the right measures hadn't been taken to close the account down, meaning hackers could still use it to infiltrate the company's network. The account's password has since been found on the dark web, making it accessible to cyber criminals across the globe.

Lots still isn't known about how the attack occurred, such as how hackers deciphered the right username or how exactly the password was obtained. By what cyber security experts do know is that the right security measures were not in place to protect the company's data, and without this, they were extremely susceptible to a cyber-attack.

It's important to note that cyber criminals won't just target large corporations. They know that smaller businesses are less likely to invest in the right security measures, and, therefore, see them as an easy target. As such, it's essential to have the right security measures in place, no matter how large or small your business.

How can I protect my passwords from cyber criminals?

IT and cyber security experts, Netstar, share their views on how to keep your passwords secure.

There are several methods of protection you can use to combat the risk of password compromise. We've outlined below some key recommendations that would have prevented the Colonial Pipeline attack. Despite the size of Colonial Pipeline, these methods are recommended to businesses of all sizes.

Multi-factor authentication

Cyber security experts have emphasised Colonial Pipeline's failure to introduce multi-factor authentication as a key cause of the attack.

Multi-factor authentication adds an extra layer of protection to standard passwords, based on the premise that a username and password alone is not sufficient to protect from cybercrime.

Media:

netstar

Related Sectors:

Business & Finance :: Computing & Telecoms :: Construction & Property :: Consumer Technology :: Manufacturing, Engineering & Energy :: Media & Marketing ::

Related Keywords:

IT Support :: IT Support London :: Technology :: Cyber Security :: Technology Consulting :: IT Consulting :: Service Desk :: IT Projects :: 24/7 IT Support ::

Scan Me:

It requires users to verify their identity at least twice before being granted access to a device, application, or system. This usually consists of:

- Something they know (e.g. their password)
- Something they have (e.g. authenticating via a mobile app)
- Something they are (e.g. a fingerprint)

For example, employees will input their login credentials and then be asked to authenticate their identity again via a corresponding mobile app. This helps to confirm that the person logging on to the account is the person they say they are, blocking cyber criminals from gaining access to confidential data.

Dark web monitoring

The Colonial Pipeline hack saw important passwords readily available to hackers on the dark web. The dark web is the World Wide Web content that exists on darknets, often used for illegal activity. Once login details are on the dark web, they can be sold to cyber criminals who can use them maliciously to launch a cyber-attack.

Dark web monitoring will continually search the dark web in the background as you continue to work as normal. It will then alert you if any login details associated with your company are discovered. Your IT partner can then help you to remediate risk immediately, preventing a cyber-attack.

Password managers

Weak passwords that are used across multiple different accounts is a common security risk for businesses. The problem is, it's impossible to remember a complex password for each of your individual accounts.

A password manager is an online tool that securely stores login information for every different account, system, and application. All the data within a password manager is encrypted, meaning it's protected from cyber criminals. You can then use a password manager to login to accounts automatically, without needing to remember each individual password.

A secure leaving process

A crucial mistake for Colonial Pipeline was that they didn't have a secure process in place for staff who had left the company. The account that was hacked was that of an ex-employee, so should never have been accessible in the first place.

It's important to ensure that when an employee leaves, any business-critical data is migrated elsewhere, their accounts are closed, and all their access to company accounts is revoked. This can be carried out easily by your IT support partner.Enter your email to sign up for the CNN Meanwhile in America Newsletter.

The next steps…

If you're worried your current cyber security setup isn't equipped to protect against cyber-attack, it's time to switch IT partners. You can contact technology and cyber security provider, Netstar, today to speak to an expert about how to get the security strategy you deserve.

Top of Form

Company Contact:

Netstar Uk Ltd.

T. 02071010544
E. srobson@netstar.co.uk
W. https://www.netstar.co.uk/

View Online

Additional Assets:

Newsroom: Visit our Newsroom for all the latest stories:
https://www.netstar.pressat.co.uk