Scam Alert: AT&T Data Breach

May 22, 2024

McLennan Community College (MCC) received reports of a text message scam, appearing to be from Mario Leal, Chief Information Technology Officer (CITO).

The text message targets employees and asks you to confirm if you received the message. An example has been provided below.

Sample Fraudulent Text

Hello [employee name], please give me a quick response when you get this message. Thanks

Mario Leal

Chief Information & Technology Officer

McLennan Community College

If you respond to the initial text, you may receive the following message:

I'm in a meeting right now, I have a task that I want you to handle for me right now. Are you available?

AT&T Data Breach

AT&T announced 73 million current and former customers had their personal information stolen in an AT&T data breach. Account data includes: customer's full name, email address, mailing address, phone number, social Security number, date of birth and AT&T account number and passcode.

The breach appears to be from 2019 or earlier. AT&T is unsure if the information came from AT&T or one of its vendors. The data leak first came to light in 2021, as hackers claimed they had stolen customer data and would put the information up for sale. In March 2024, the stolen personal information was discovered on the dark web, according to the creator of Have I Been Pwned.

If you are an AT&T customer and worried about your data, see What is AT&T doing for the 73 million accounts breached?

Scam Text Messages & Phishing

Data breaches, such as AT&T, puts individual's information out, open to the public. Scammers use this information to create phishing (scam) emails or smishing (scam) texts.

Many users are aware of the dangers of responding to suspicious emails. With text messages, users let their guard down and usually respond more quickly. Here are a few signs of smishing texts:

- Tone of the message conveys a sense of urgency
- Strange or abrupt business request
- Phone number is spoofed - looks like it is coming from someone you know or trust
- Claims to be from a colleague, family member or friend, but does not sound like them

Remember to protect your identity and Recognize Phishing.

What to do now?

If you receive this or a similar scam, **DO NOT** respond or click on any links. You may contact Tech Support if you have any questions or need to report an issue.

Revision #2
Created 12 December 2024 19:02:55 by Laura J. Crapps
Updated 26 February 2025 03:35:37 by Laura J. Crapps