CMIT Solutions®

QUICKTIPS

TUESDAY, JANUARY 24, 2023

5 Ways to Protect Your Online Information

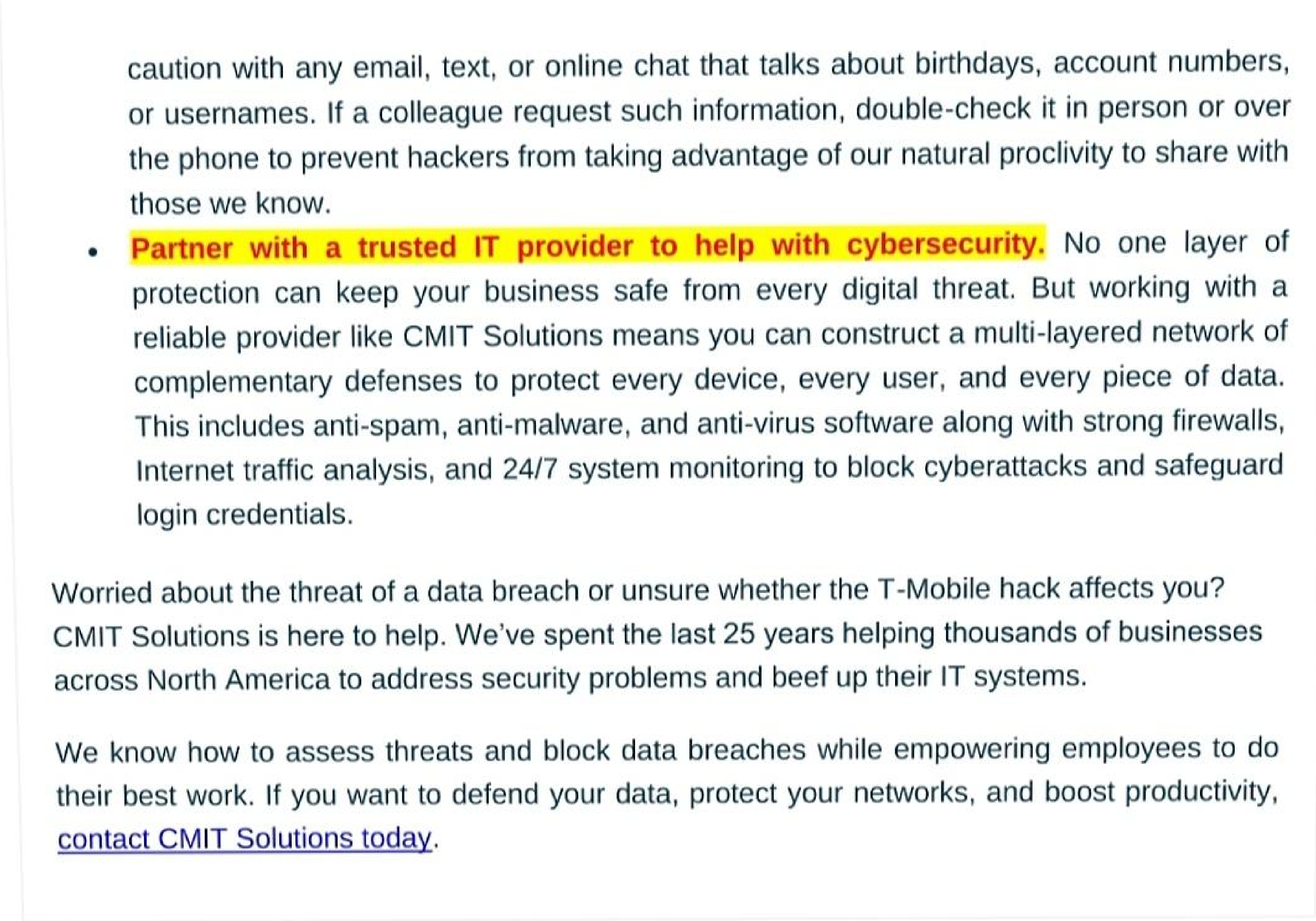
Another week, another data breach: **on Jan. 19, T-Mobile announced that the information of 37 million customers was stolen in a coordinated cyberattack**. The second-largest wireless carrier in the U.S. said that mobile phone numbers, customer names, and birth dates were stolen. Although not as sensitive as account numbers or passwords, the information could still be used for social engineering or phishing scams that try to steal further details.

Hackers stole the T-Mobile data by exploiting an API, or application programming interface. APIs allow two different software applications to transfer data back and forth. Experts haven't been able to pinpoint precisely how T-Mobile's information was stolen. But the company's track record points to a severe problem.

This is the fifth major privacy failure in the last five years for the company that once billed itself as the "Un-Carrier." In **2021**, T-Mobile reported a breach that compromised the data of 77 million people; in 2022, it agreed to pay a $500 million settlement to those affected. Now it could face similar action from regulators concerned about its ongoing security issues and consumers upset about another breach.

Understandably, T-Mobile customers—and anyone else worried about protecting their digital identities—want to know how to keep themselves safe now. **CMIT Solutions recommends the following five strategies to beef up online security and mitigate any potential problems that could stem from the T-Mobile breach:**

- **Enable multi-factor authentication (MFA) across all accounts.** MFA requires computer users and account holders to enter something they know (a username and password) with something they have (a one-time code delivered via text message or push notification sent through an app). Even though passwords weren't stolen in the T-Mobile breach, this extra layer of cybersecurity protection can go a long way toward protecting personal data stored in any account.
- **Know how to spot dangerous messages.** Typically, these arrive in the form of fake shipping updates, invitations to a shared document, or account details that need to be confirmed. But T-Mobile phone numbers, customer names, and birth dates could be used to target users with illicit phone calls or text messages that ask about mobile phone settings or monthly bills. You and your employees should learn how to identify these scams by looking out for suspicious sender addresses, strange copy or punctuation, or any kind of alert asking about a password. Cybersecurity training and education can help immensely in this area.
- **Never open attachments or click links in unfamiliar emails.** In addition to spotting suspicious messages, be extra cautious with PDFs, Word documents, or audio files attached to them—and the URLs included in the email. Anything that urges you to take caution should be considered a red flag. With web links, you can hover over the blue URL or right-click it to see whether the address spelled out in the email copy matches the actual destination. If you see long strings of nonsensical numbers or letters, DO NOT CLICK the link. Only open attachments if they're specific files you're expecting from a specific sender. NEVER test an unfamiliar attachment just to see what it is since one click can often execute a ransomware infection or install malware on your machine.
- **Don't share personal, financial, or medical information with any unknown source.** The next level of scams is called social engineering, typically defined as a method of warming up to users with personal entreaties or sensitive information. Use



caution with any email, text, or online chat that talks about birthdays, account numbers, or usernames. If a colleague request such information, double-check it in person or over the phone to prevent hackers from taking advantage of our natural proclivity to share with those we know.

- **Partner with a trusted IT provider to help with cybersecurity.** No one layer of protection can keep your business safe from every digital threat. But working with a reliable provider like CMIT Solutions means you can construct a multi-layered network of complementary defenses to protect every device, every user, and every piece of data. This includes anti-spam, anti-malware, and anti-virus software along with strong firewalls, Internet traffic analysis, and 24/7 system monitoring to block cyberattacks and safeguard login credentials.

Worried about the threat of a data breach or unsure whether the T-Mobile hack affects you? CMIT Solutions is here to help. We've spent the last 25 years helping thousands of businesses across North America to address security problems and beef up their IT systems.

We know how to assess threats and block data breaches while empowering employees to do their best work. If you want to defend your data, protect your networks, and boost productivity, contact CMIT Solutions today.