One Tech Tip: What to do if your personal info has been exposed in a data breach

July 12 2024, by Kelvin Chan

Data breaches like the most recent one involving AT&T customers are becoming an almost regular occurrence.

As more of our lives move online, our personal data like email
addresses, phone numbers, birthdates and even passcodes are becoming ever more vulnerable to theft or being mistakenly exposed.

In malicious breaches, cybercriminals can use stolen data to target people with phishing messages, or by taking out loans or credit cards in their name, a common and harmful type of identity theft.

Here are some tips to protect yourself.

**Be aware**

In the United States, there's no federal law compelling companies or organizations to notify individuals of data breaches, but it's standard practice for them to inform affected customers and often provide identity protection services, said Oren Arar, vice president of consumer privacy at cybersecurity company Malwarebytes.

The situation is better in the European Union, where the 27-nation bloc's privacy regulations require disclosure of certain types of breaches.

Even after a breach has been made public, cybersecurity experts say people need to remain vigilant. Be on guard for phishing and other social engineering attempts, in the form of emails or phone calls purporting to be from the hacked organization or someone offering help. Contact the company or organization involved to see if they can confirm it. But use their official website, smartphone app or social media channels—don't use links or contact details in any messages you've been sent.

Also consult the Federal Trade Commission's website for identity theft victims, identitytheft.gov, which provides step-by-step advice on how to recover from various scenarios.
Change your password

If your data has been exposed, the first thing you should do is change your password for the account involved.

Use a strong password including letters, numbers and symbols. The longer the better—some experts say it should be 16 characters. Make sure to add multifactor authentication, which adds a second layer of verification by requiring a code sent by text message or email, or inserting a USB authenticator key into your device.

And if you've been using the same or similar login information for multiple websites or online accounts, make sure to change it. The reason is that if hackers pilfer your password from one service, they can try it on your other accounts and easily get into all of them. If you find it too hard to memorize all your various credentials, consider a password manager.

"Just because your info shows up in a breach doesn't mean someone's stolen your identity or money. But it does mean you're at risk," said Arar. "That's why it's smart to watch your credit for new accounts, change any passwords that get leaked, use multifactor authentication, and have a separate 'junk' email for less important sign-ups."

Keep monitoring

Data breaches are rampant and it can be hard to keep track of them through individual notifications. There are online services that you can check, like Have I Been Pwned, a free website that shows if your email has been involved in a data breach.

Malwarebytes' Digital Footprint Portal does a similar job but it can also
check whether your info has been posted on the dark web.

"When public data breaches occur, cybercriminals gather as much data as possible so they can sell it on the dark web," said Darren Guccione, CEO of Keeper Security, which makes password protection software and offers a tool, BreachWatch, that scans the dark web to see if your personal information shows up there.

**Tell your bank and credit agencies**

If card payment numbers were stolen, inform your bank or credit card company, explaining that your card is at risk of fraud and asking them to alert you of any suspicious activity. They'll probably issue a new card right away. Some banking and credit card apps allow you to lock the account and freeze any transactions from the app.

You can also notify credit agencies—the three main ones are Equifax, Experian and TransUnion. They can freeze your credit, which restricts access to your credit report and makes it hard to open new accounts or issue a fraud alert, which will be a warning added to your credit report encouraging lenders to contact you before lending money.

**Take extra care after telco hacks**

Cybersecurity experts have warned that breaches that involve a telephone company, like the AT&T case, leave customers vulnerable to having their phone numbers stolen, or SIM swapped. Thieves could then use the hijacked number to access other accounts that use that number for multi-factor authentication through text messages.

To reduce that risk, AT&T advises also setting up a unique passcode that's needed to prevent significant account changes such as porting
phone numbers to another carrier. Also, delete phone bills, bank statements and other messages with personal info from your email account, so that if criminals gain access to your inbox, they won't be able to use that information to pass security checks.

© 2024 The Associated Press. All rights reserved. This material may not be published, broadcast, rewritten or redistributed without permission.

Citation: One Tech Tip: What to do if your personal info has been exposed in a data breach (2024, July 12) retrieved 18 July 2024 from https://techxplore.com/news/2024-07-tech-personal-info-exposed-breach.html