AASBCR®
AT&T, Ameritech, SBC
AND BELL SYSTEM
RETIREES

Your Voice for AT&T Retiree Benefits

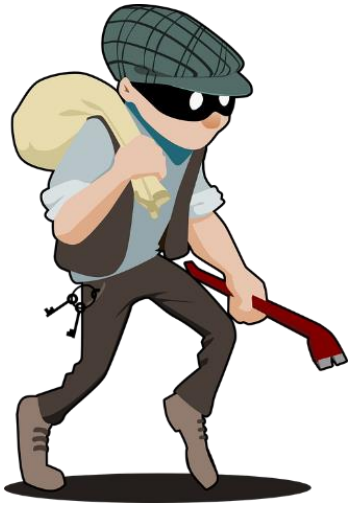
Join AASBCR® or **Make a Donation**

AT&T Data Breach — April 2024

Internet security bloggers report that about 50 million AT&T *customer* profiles obtained by a hacker in August of 2021 have been posted this past week on a website, where the data could be downloaded by anyone for free. The data was sorted by email address, and included name, address, phone, with Social Security number for most, and date of birth for some.

AT&T says it is not responsible for the breach – it must be some third party, they say.

AASBCR® is passing on this information because many of our retiree members were also customers of AT&T prior to 8/2021, so this data breach may include your information. For example, you may have had an AT&T landline or an AT&T Mobile account. In such cases, you would sign onto the account with your email and a password, which would then provide access to personal information in your account profile.



To see if your email was one of those captured by the hacker, go to https://haveibeenpwned.com/ and enter the email address.

Fortunately, passwords to AT&T accounts were NOT included in the breach. But, if the password you used on your breached AT&T account is one you also used for other accounts, it would be smart to change all those passwords to something else.

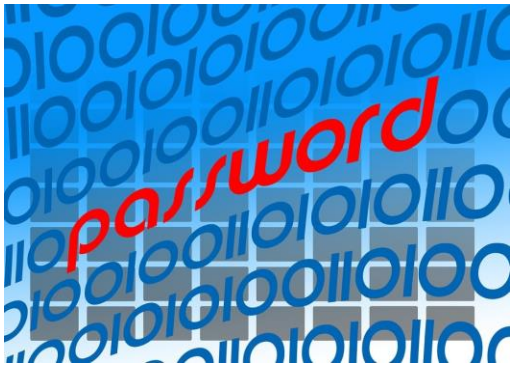
What is the Risk for You?

If a hacker has your email, you may get more emailed scam attempts. Don't open emails from unknown sources! Your hacked name, address, and phone number can also be used to send you unwanted paper mail or phoned offers or robocalls.

If a hacker has your social security number and date of birth, they may be able to apply for credit and make you liable when they don't pay it back. So be alert for scams.

If a hacker has your email and can figure out your password, perhaps from other breaches, they can access your accounts with merchants and associations, and perhaps make transactions.

More likely, they would sign on with your email and then enter “forgot password,” and change your password to their own. This would give them access to your profile, which may include a stored credit card number. They could then make transactions themselves, or sell that capability. Meanwhile, your access would be blocked.



You should replace any passwords that might have been part of breaches, use hard-to-guess passwords, and don’t re-use the same password for multiple accounts.

You can use a password manager software, or even a spreadsheet, to keep track of all your passwords.

Even better, see if you can change the username in the login process so it is something other than your old email address – either a new email address, or something else. If you can do this, it won’t matter if the hacker has your old email address.

The sources for this bulletin are internet security bloggers. AASBCR® has no way to verify the accuracy of the information they have published, but it seems accurate, and AT&T seems to believe it is true, so we pass it on to you.