

The bad news is over 70,000 current and former AT&T customers had important and personal information leaked to hackers. The even worse news? There isn't much those people can do about it. I'm talking with one of the foremost experts on cybersecurity and privacy about the leak, what anyone can learn from it, and what you can do to minimize the risk.

NOTE: I'm not going into much detail about how the leak happened or what the bad guys were able to get. This piece would probably run best with a quick reader or full-screen graphics with what AT&T is now saying. That will likely change

TRT 141
STD OUT

SUPER

0-8 Jamey Tucker/whatthetech.tv
27-36 Troy Hunt/havebeenpwned.com

ON-CAMERA TEASE:

What can victims of the ATT data leak do? You're not going to like the answer. Not many people will. I'm Jamey Tucker, coming up we'll talk to a privacy expert on what all of us should do right now.

ANCHOR INTRO

AT&T IS JUST THE LATEST COMPANY DEALING WITH A LEAK OF CUSTOMER'S PRIVATE INFORMATION. IT SEEMS TO HAPPEN EVERY FEW DAYS.

AND AS THE LEAKS BECOME MORE FREQUENT, CONSUMERS ARE WONDERING WHAT THEY CAN DO TO PROTECT THEMSELVES. OUR CONSUMER TECHNOLOGY REPORTER JAMEY TUCKER HAS SOME INSIGHT FROM AN EXPERT.

PACKAGE SCRIPT

Troy Hunt is one of the most respected names when it comes to privacy, passwords, and data leaks. I've talked about his website HavelBeenPwned.com many times as a resource for consumers to find out if their email and passwords have been compromised.

From his home in Australia, Hunt told me AT&T's data leak which included social security numbers, is more disturbing than many other data leaks. Then we've got names, phone numbers, physical addresses. That's really all of the building blocks for theft, unfortunately.

“We’re seeing headlines that it’s on the dark web. It’s not the dark web. It’s the clear web. It is somewhere you go on your normal browser. There will be thousands if not tens of thousands of people who now have all of this data” And there’s not much victims can do about it now.

We cannot go and change our date of birth, changing a social security number is an absolute nightmare. So we have to work on the fact that the data is out there and we’re never going to get it back.

Hunt says, most people don’t take steps to protect their data until they’re a victim. And it’s safe to say everyone has been in a data leak. So taking steps now is critical.

I can’t stop myself from being in data breaches. The only thing I can do is minimize the impact when I am.

Hunt says Identity theft and fraud protection is a good step toward protecting your privacy.

These are about \$100 a year. And good, strong, unique passwords for each account. That’s What the Tech? I’m Jamey Tucker

ANCHOR TAG

AT&T SAYS IT IS CONTACTING ALL CURRENT AND FORMER CUSTOMERS WHOSE INFORMATION WAS INCLUDED IN THE LINK. IT ALSO RESET THE PASSCODES OF THOSE ACCOUNTS.

WEB STORY

The recent data leak at AT&T is just the latest incident where the private information of millions of consumers was compromised and is now in the hands of cybercriminals.

AT&T on Monday confirmed the data leak of over 70,000 current and former AT&T customers.

The data includes Social Security Numbers and other personal information.

Web security consultant Troy Hunt, who also runs the website www.haveibeenpwned, said this data leak is worse than many others due to the wealth of information included.

“Social security numbers are a big part of identity verification,” Hunt said. “Then we’ve got names, phone numbers, physical addresses. That’s really all of the building blocks for theft, unfortunately”.

AT&T confirmed in a release Monday that the data has been released on the dark web but Hunt says, it’s much more accessible than that.

“We’re seeing headlines that it’s on the dark web. It’s not the dark web. It’s the clear web. It is somewhere you go on your normal browser. There will be thousands if not tens of thousands of people who now have all of this data”, Hunt explained.

Armed with all of that information, a cybercriminal would be well on their way to stealing the victims' identities. And there's not much victims can do about it now.

"We cannot go and change our date of birth," Hunt said. "Changing a social security number is an absolute nightmare, that's not going to happen for 70 million people. So we have to work on the fact that the data is out there and we're never going to be able to get it back."

One problem, Hunt says, is that most people don't take steps to protect their data until they become a victim. And it's safe to say everyone online has been in a data leak. We just don't know it.

So taking steps now is critical.

Hunt himself said his email address has been included in some 30 data leaks. "I live this stuff and I can't stop myself from being in data breaches. The only thing I can do is minimize the impact when I am."

What can that be? Hunt says identity theft and fraud protection services that alert people when there's a credit inquiry on their name, is a good step toward protecting your privacy. These are about \$100 a year.

"But I'm also conscious that this is not a panacea," cautions Hunt. "This is not going to necessarily notify me when someone has my username and password and they're trying to log into my email account."

To protect accounts that use email addresses and passwords to access Hunt, and other cybersecurity experts strongly recommend using strong and unique passwords for individual accounts, turning on multi-factor authentication, and a password manager.