

TECH FIX

I Shared My Phone Number. I Learned I Shouldn't Have.

Our personal tech columnist asked security researchers what they could find out about him from just his cellphone number. Quite a lot, it turns out.



By Brian X. Chen

Aug. 15, 2019

For most of our lives, we have been conditioned to share a piece of personal information without a moment's hesitation: our phone number.

We punch in our digits at the grocery store to get a member discount or at the pharmacy to pick up medication. When we sign up to use apps and websites, they often ask for our phone number to verify our identity.

This column will encourage a new exercise. Before you hand over your number, ask yourself: Is it worth the risk?

This question is crucial now that our primary phone numbers have shifted from landlines to mobile devices, our most intimate tools, which often live with us around the clock. Our mobile phone numbers have become permanently attached to us because we rarely change them, porting them from job to job and place to place.

At the same time, the string of digits has increasingly become connected to apps and online services that are hooked into our personal lives. And it can lead to information from our offline worlds, including where we live and more.

In fact, your phone number may have now become an even stronger identifier than your full name. I recently found this out firsthand when I asked Fyde, a mobile security firm in Palo Alto, Calif., to use my digits to demonstrate the potential risks of sharing a phone number.

Emre Tezisci, a security researcher at Fyde with a background in telecommunications, took on the task with gusto. He and I had never met or talked. He quickly plugged my cellphone number into a public records directory. Soon, he had a full dossier on me — including my name and birth date, my address, the property taxes I pay and the names of members of my family.

From there, it could have easily gotten worse. Mr. Tezisci could have used that information to try to answer security questions to break into my online accounts. Or he could have targeted my family and me with sophisticated phishing attacks. He and the other researchers at Fyde opted not to do so, since such attacks are illegal.

"If you want to give out your number, you are taking additional risk that you might not be aware of," said Sinan Eren, chief executive of Fyde. "Because of collisions in names due to the massive number of people online today, a phone number is a stronger identifier."

There is no simple solution to this. In some situations, giving your digits to institutions like your bank provides an extra layer of security. But in most cases, the potential dangers and annoyances of handing out your number outweigh the benefits, as you will read below.

How your phone number exposes you

It took only an hour for my cellphone number to expose my life.

All that Mr. Tezisci, the researcher, had to do was plug my number into White Pages Premium, an online database that charges \$5 a month for access to public records. He then did a thorough web search and followed a data trail — linking my name and address to information in other online background-checking tools and public records — to track down more details.

In an hour, this is what came up:

- My current home address, its square footage, the cost of the property and the taxes I pay on it.
- My past addresses from the last decade.
- The full names of my mother, father, sister and aunt.
- My past phone numbers, including the landline for my parents' home.
- Information about a property I previously owned, including its square footage and the mortgage taken out on it.

- My lack of a criminal record.

While Fyde declined to hack into my accounts using the obtained information and my number, the company warned that **there was plenty an attacker could do**:

- A hacker could try to reset my password for an online account by answering security questions like “What is your mother’s maiden name?” or “Which of the previous addresses did you live at?”
- An attacker could use the personal information linked to my phone number to trick a customer service representative for my phone carrier into porting my number onto a new SIM card, thus hijacking my digits — a practice called SIM swapping.
- A hijacker with control of my phone number could then break into my accounts if I had mechanisms in place to receive a security code in a text message when logging in to an online account.
- A scammer could also use my hijacked phone number to trick members of my family into sharing their passwords or sending money.
- A scammer could also target my phone number with phishing texts and robocalls.
- An intruder could use knowledge of my phone number to call my voice mail inbox and try to crack the personal identification number to listen to my messages.

Marketers could also take advantage:

- An ad tech agency could add my number to a detailed profile about me, linked to other information about my identity and web-browsing activities.
- If I signed up for an internet service with my phone number, a brand that bought my digits from an ad firm could upload them into an ad tech tool to correlate the number with my online profile and serve targeted ads.
- A shady marketing agency could add my number to a database to blast me with spam calls and text-messaged promotions.

When it’s wise to share your number (and when it’s not)

There are some situations when sharing your phone number is reasonable.

When you enter your user name and password to get into your online banking account, the bank may call or text you with a temporary code that you must enter before you can log in. This is a security mechanism known as two-factor verification. In this situation, your phone number is a useful extra factor to prove you are who you say you are.

“A phone number is a better identifier than just your name, but sometimes you want that,” said Simon Thorpe, director of product for Twilio, a communications company that works with phone carriers on combating robocalls.

But which companies should you trust with your phone number? Here’s where things get tricky.

Plenty of tech companies let you use your phone number to protect your accounts from unauthorized access. But even some legitimate brands like Facebook have been scrutinized for improper use of phone numbers.

Last year, a study by the tech blog Gizmodo found that after a Facebook user set up two-step verification with his phone number, advertisers that uploaded his digits into Facebook’s database could match them to his Facebook profile and serve targeted ads. Separately, some people complained this year that the social network allowed them to look up a person’s Facebook profile just by typing a phone number into its search bar.

What to Know About Ransomware Attacks

What are ransomware attacks? This form of cybercrime involves hackers breaking into computer networks and locking digital information until the victim pays for its release. Recent high-profile attacks have cast a spotlight on this rapidly expanding criminal industry, which is based primarily in Russia.

The company has removed the ability to find people’s profiles by entering their phone number, said Rochelle Nadhiri, a Facebook spokeswoman. She added that when a user set up two-step verification with a phone number, the company would not use the information to serve targeted ads.

But when large companies like Facebook abuse your digits, whom do you trust?

Unfortunately, there is no neat solution. It all involves work.

That includes first asking yourself whether the benefits of giving out your phone number outweigh the potential risks.

You might also want to set up a second phone number to cloak your personal digits altogether. You could share this second phone number with people and brands you don't entirely trust. Apps like Google Voice and Burner let you create a different number that you can use for calls and texts.

As for two-factor authentication, most tech companies offer other verification options. They include apps that generate temporary security codes or a physical security key that can be plugged in. Generally, those are safer to use than a phone number.

Here's a bonus piece of advice. If you have business cards with your personal number printed on them, shred them and order new ones with just your office line.

Eventually, I spoke to Mr. Tezisci about his experience tracking me. He said he was surprised by how easily a person could be targeted with a single set of numbers.

"I only spent an hour, and I was able to see all your addresses and all phone numbers," he told me. "I think that's scary, isn't it? And I selected the legal options. If I were a scammer, I would have gone for your relatives."

Brian X. Chen is the lead consumer technology writer. He reviews products and writes Tech Fix, a column about solving tech-related problems. Before joining The Times in 2011 he reported on Apple and the wireless industry for Wired. @bxchen

A version of this article appears in print on , Section B, Page 1 of the New York edition with the headline: Sharing Your Phone Number Can Open a Risky Portal to Your Life

Referenced in This Article

Protecting Your Accounts by Text or App

Dec. 22, 2017

Moving Your Number to Google Voice

Jan. 20, 2018

Protecting Your Internet Accounts Keeps Getting Easier. Here's How to Do It.

March 28, 2019

How Google's Physical Keys Will Protect Your Password

Jan. 20, 2018