How Your Phone Number is Exposed: Phone Number Leaks

Your phone number counts as personal data, and you don't just want anyone out on the internet to have it.

While they might still come to your door, when was the last time you used a phone book? Maybe you never have. The internet has replaced the white pages of yore, but there are good reasons why you don't want your number listed. Phone numbers are one of the most overlooked pieces of personal data. But as we increasingly rely on smartphones for communication and online transactions, you should understand how your phone number can be exposed on the web. Sometimes your phone number is leaked in a data breach, other times you might have revealed it on social media, for example. What steps can you take to safeguard your privacy?

How to see if your phone number is exposed

The easiest way to see if and where your phone number is revealed online is to do a web search of your name and phone number. While it might not crawl through every digital nook and cranny your number could exist, it will give you an idea if you, for instance, ever tweeted out your number or if it is publicly available on an old employer's website.

Why your phone number could be exposed

There are many reasons why your phone number could be released on the internet. Some of these situations you can control, like if you published your number on a public resume, and others are caused by issues like data leaks and hackings:

- Your phone number is linked to your social media or other online account.
- You entered your information for a free trial, contest, or other online form, and then your phone number was published.
- You provided your phone number for a product you purchased, loyalty points, or discounts from online retailers.
- Your phone number was lost in a data breach and bad actors posted it online.

How to keep your phone number safe

Here are some ways you can work to keep your phone number out of the baddies' hands:

1. PAY ATTENTION TO DATA BREACHES

Nowadays, data breaches have become a widespread problem and millions of people worldwide are impacted every year. When an organization is hit with a breach, cybercriminals might gain access to the phone numbers of

consumers. This exposes your phone number to bad actors who might misuse it for malicious purposes. Follow these steps to mitigate the risk:

- Regularly monitor trusted news outlets and cybersecurity websites to stay informed about recent breaches that might impact you.
- Enable multi-factor authentication (MFA) for every account that permits it to add an extra layer of security beyond your password. If an account doesn't have MFA, think about using an alternative that does.
- Consider using a virtual phone number for online accounts instead of your primary phone number. There are free options available.

2. CENSOR PUBLIC ONLINE LISTINGS

Phone numbers are often collected and published on various online platforms, directories, and social media websites. These listings often work as the internet version of phone books, but the entire world has access to your number instead of just your home city. Public listings make your number easily accessible to anyone, including scammers and telemarketers. You can minimize your exposure:

- Audit your social media profiles and ensure that your phone number is not publicly visible. Review your privacy settings.
- Regularly review online directories by conducting web searches for your phone number. Request the removal of your number from listings.
- Be extremely wary about sharing your phone number online, even when signing up for services or discounts.

3. AVOID BAD APPS

Some mobile applications and websites require you to provide a phone number to create an account or verify your identity. Importantly, not all platforms prioritize user privacy, and your phone number can be exploited. To protect yourself:

- Research the reputation and security measures of apps and websites before providing your phone number.
- Read the Terms of Service to see what an app does with your data.
- Be mindful of app permissions – only grant access to necessary functions. A solitaire app doesn't need your phone number to work, for example.

4. STAMP OUT SIM CARD SWAPPING

SIM card swapping is a scam used to gain access to your phone number. A scammer will try to trick your wireless provider into transferring your number to a new SIM card under their control. To give scammers the slip:

- Contact your mobile service provider to enable SIM card lock or PIN code protection to restrict unauthorized SIM card usage.
- Regularly check your phone's network connectivity and be wary of sudden signal loss or service disruptions.
- If you notice any unusual charges on your bill or weird phone activity, contact your wireless provider immediately.

5. DON'T ANSWER CALLER ID SPOOFING AND "VISHING" ATTACKS

Cybercriminals can use technology to manipulate the Caller ID information displayed on your phone, which will make it appear as if they are calling from an area code you know or a number you recognize. This technique is commonly used in so-called "vishing" (voice phishing) attacks, where scammers impersonate legitimate entities, like banks, to steal your money or sensitive information. Leave the hackers hanging:

- Be cautious when receiving calls from unknown numbers, even if the Caller ID appears legitimate. You can always let the call go to voicemail and see what the message says.
- Legitimate organizations including banks, the IRS, and social media platforms will **never** call you up to ask for sensitive information, like passwords or bank account numbers, over the phone.
- Look into call-blocking services that identify and block known spammy or fraudulent numbers.

Your phone number is personal data

While dozens of your friends and family have your phone number, it is important to remember that your private phone number is valuable personal data and should be treated as such. Companies pay millions of dollars to know your number and other info! By protecting your phone number, you can reduce the risk of identity theft, phishing, and other scams. You also make it harder for telemarketers and robocalls to reach you. The peace of mind you'll have by keeping your phone number private is well worth the effort.
