JUNE 2023

ALBION FINANCIAL GROUP

HAS YOUR CELL PHONE BEEN HACKED?

No matter what service provider you use, every cell phone number can be a target for hackers. And it takes remarkably little effort to wreak havoc to your online life.

WHY YOU NEED TO PROTECT YOUR PHONE NUMBER

Your cell phone number is a single point of failure.

Think about it. You use your cell phone number all the time. You use it when you sign up to sites and services, and sometimes you'll use it to log into an app or a game on your phone. Your phone number can be used to reset your account if you forget your password. And, you use it for two-factor authentication to securely login to your accounts.

If someone steals your phone number, they become you — for all intents and purposes. With your phone number, a hacker can start hijacking your accounts one by one by having a password reset sent to your phone. They can trick automated systems — like your bank — into thinking they're you when you call customer service. And worse, they can use your hijacked number to break into your work email and documents — potentially exposing your employer up to data theft.

Just think of every site and service that has your phone number. That's why you need to protect your phone number.

HOW DO HACKERS STEAL CELL PHONE NUMBERS?

It's easier than you might think. Phone numbers can be found anywhere – thanks in part to so many data breaches.

Often, hackers will find the cell phone number of their target floating around the internet (or from a phone bill in the garbage), and call up their carrier impersonating the customer. With a few simple questions answered — often little more than where a person lives or their date of birth, they ask the customer service representative to "port out" the phone number to a different carrier or a SIM card.

That's it. As soon as the "port out" completes, the phone number activates on an attacker's SIM card, and the hacker can send and receive messages and make calls as if they were the person they just hacked.

In most cases, the only sign that it happened is if the victim suddenly loses cell service for no apparent reason.

From there, it's as simple as initiating password resets on accounts associated with that phone number. Facebook, Gmail, Twitter — and more. A hacker can use your hijacked phone number to initiate wire fraud from your bank accounts, take over your social media accounts or maliciously delete all of your data.

In the worst cases, it can be difficult or impossible to get your phone number back — let alone the accounts that get broken into. Your best bet is to make sure it never happens in the first place.

COMMON WAYS YOUR DEVICES CAN BE HACKED

There are a few different ways that hackers can get into your device, such as:

- **Using a public Wi-Fi network that is not secure.** Hackers can easily access these networks and find your device if it is not properly protected.
- **Downloading apps that are not secure.** If you download an app from an untrustworthy source, it could contain malware that can infect your device.
- **Gaining access to your device through phishing scams.** Hackers will send you an email or text message that appears to be from a legitimate source, but is actually a scam. If you click on a link in the message, you could inadvertently give the hacker access to your device.
- **Losing your device or having it stolen.** If you do not have a password or other security measure in place, the hacker could easily gain access to all of your information.

WHAT YOU CAN DO TO PROTECT YOUR PHONE NUMBER

Just like you can apply two-factor authentication to your online accounts, you can add a secondary security code to your cell phone account, too.

You can either call up customer services or do it online. (Many feel more reassured by calling up and talking to someone.) You can ask customer service, for example, to set a secondary password on your account to ensure that only you — the account holder — can make any changes to the account or port out your number.

Every carrier handles secondary security codes differently. You may be limited in your password, passcode or passphrase, but try to make it more than four to six digits. And make sure you keep a backup of the code!

MORE WAYS TO STAY SAFE

- AT&T has a guide on how to set up extra security on your account.
- T-Mobile allows you to set up a customer passcode.
- Verizon explains how you can add a PIN to your account.
- Sprint also lets you add an account PIN for greater security.

If your carrier isn't listed, you might want to check if they employ a similar secondary security code to your account to prevent any abuse. And if they don't, maybe you should look into switching to a carrier that does.

CONTACT ALBION

If you receive a suspicious email, call or text claiming to be from Albion, let us know. We'll work with you to determine the legitimacy of any suspicious messages.

PHONE: (801) 487-3700

EMAIL: CYBERSECURITY@ALBIONFINANCIAL.COM

FOR MORE INFORMATION VISIT ALBIONFINANCIAL.COM/LEARNING-CENTER/CYBERSECURITY/

THANK YOU

WE DO NOT TAKE LIGHTLY THE TRUST YOU HAVE PLACED IN US.

Albion Financial Group is committed to maintaining the confidentiality, integrity and security of the personal information that is entrusted to us. Protecting our clients' identity is of the utmost importance. We will never send you an email asking for your account information.

We do not provide your personal information to mailing list vendors or solicitors and we regularly review the importance and methods of maintaining client confidentiality with our entire staff.

ALBION FINANCIAL GROUP