NordPass®

Blog / Digital Life /

# What Happens if I Use Two-factor Authentication and Lose My Phone?

2021-03-26 - 5 min read

Benjamin Scott

Most online accounts give you the option of setting up 2FA for an extra layer of security when logging in. Using your phone number as your 2FA verification is excellent – you receive a text or phone call to verify it’s you, and boom! You’re in. Except now you’ve lost your phone and can’t access any of your accounts. Don’t panic just yet; you still have some options, which we discuss below, along with some handy preventative measures.

Contents

Backup codes: the easy way to recover your account

Transfer your old phone number to a new phone

Have your verification code sent to your backup phone

Set up 2FA on two different devices

## Backup codes: the easy way to recover your account

When you set up 2FA on most sites, including Google, they provide you with a set of unique recovery codes, which are made up of random numbers and sometimes letters. Each backup code can be used once to log in to your account.

Tip: Save your backup codes offline

Please don’t save your recovery codes in the cloud – such as in your emails or notes. Your email account and devices can be hacked, lost, or stolen, and if you get locked out of your email account, you’ll lose access to your codes. Instead, use a USB stick, external disk drive, or encrypted password manager to store them securely. If you want to get more creative, you could store them on an old phone, Kindle or iPad that is factory-reset and set to offline mode for maximum security.

## Transfer your old phone number to a new phone

If you didn’t save your backup codes, and you’ve lost the phone that you use for 2FA – try calling your phone network to transfer your old number over to a new phone. You’ll need a new SIM card for that, and it could take a day or two for it to activate. But once you have your old number working again, you can receive 2FA verification codes as usual.

Tip: Erase your old phone remotely

If you’ve lost your phone, you should be able to remotely erase it if you’ve previously activated the feature in settings. Use Apple’s Find My Phone or Google’s Find My Device to view its location and delete its contents. The last thing you need is someone accessing your 2FA from your old phone and breaching all of your accounts.

## Have your verification code sent to your backup phone

When you set up 2-step verification, you may have been given the option to choose a backup phone in case you lose access to your main number. If you’ve done this on Google, for example, select “Try another way to sign in” and have your verification code sent to your backup phone.

Tip: Use a trusted family member or friend as a backup

You can add their number as a trusted backup source in case you lose access to your phone. Since a phone number is only part of the verification process for most accounts, it’s a good idea to use this method for your Apple ID, for example. Apple’s alternative recovery process is intentionally time-consuming to deter criminals. That’s why having a trusted friend receive your codes can be a massive relief during emergencies.

## Set up 2FA on two different devices

Having a secondary device with your 2FA is a great backup if you ever lose your primary phone. A whole barrage of authentication apps exists to help you with 2FA, like Authy and Google Authenticator. The latter lets you scan a unique QR code to verify it’s you. Take a picture of the QR code on a secondary device or, better yet, print it and store it in a secret location to use in dire situations.

## Contact customer service

Losing access to your 2FA isn’t the end of the world, which is why customer service departments are there to help. While proving your identity and going through recovery processes are difficult and time-consuming, your service may offer some quicker verification methods. Take your bank, for example. They may ask you to confirm your card details, unique security numbers, or address to help you get back into your account. Either way, forgetting passwords and losing devices is common, so it’s always worth a call before you give up.

## Use NordPass with biometric authentication

2-step authentication is a good security measure, but it’s not without its inconveniences. So it might be time to rethink your account security and opt for biometrics. Biometric authentication uses face, voice, or fingerprint recognition to help you access your accounts. The NordPass app can be set up with your Face ID or fingerprint to quickly access your encrypted vault of passwords. No longer are you bound to stashing physical copies of passwords – your details in NordPass are accessible from your phone or tablet, even when you’re offline.

**Even though you use 2FA, you still need a secure way of storing your passwords and codes, which is what NordPass is expertly designed to help you with.**

Subscribe

Share

Enter your email

Subscribe

NordPass®

Subscribe to NordPass news

Enter your email

Subscribe

PERSONAL

- Features
- Pricing
- How It Works
- Password Manager
- Terms of Service

BUSINESS

- Pricing
- Business
- Enterprise
- MSP
- Case Studies
- Whitepaper
- Terms of Service
- DPA

COMPANY

- About Us
- Press Area
- Careers
- Contact Us
- Help Center

RESOURCES

- Blog
- 200 Worst Passwords
- What is Digital Stress

TOOLS

- Username Generator
- Business Name Generator
- Password Generator
- Password Strength Checker
- Data Breach Scanner

BECOME A PARTNER

- Affiliate
- Influencers

PROMOTIONAL OFFERS

- Refer a Friend
- Student Discount

APPS

- Windows
- macOS
- Linux
- iOS
- Android
- Web Vault

EXTENSIONS

- Chrome
- Firefox

DISCOVER

- NordVPN
- NordLayer

Subscribe

Share

Enter your email

Subscribe

NordPass®

Privacy Policy

Subscribe

Share

Enter your email

Subscribe

NordPass®

Subscribe

Share

Enter your email

Subscribe