OUCH! November 2026



Workforce Security and Risk Training

Locked Out of Your Account? How to Get Back In

A Password Reset That Went Nowhere

Nadia was rushing to catch a train when her phone suddenly stopped syncing with her email. She tried logging back in, but her password was rejected. She used "Forgot password," expecting a quick reset. Instead, the recovery code was sent to an old email address she had not used in years. She tried another option. The service offered to text a code to a phone number she no longer had.

Now worried, Nadia tried several more times. Nothing worked — she was locked out of her email account. What's worse, her email account was tied to banking alerts, shopping accounts, cloud storage, social media, and other password resets. Without access to that one account, pieces of her digital life began falling like dominoes.

Then she received a message claiming to be from "account support," offering to restore access if she paid a fee and provided personal information. Desperate to get her account back, she almost did what the message said, but instead realized that her account had been hacked and this was a scam. Nadia had secured her account with what she thought was a strong password. But she had overlooked one critical question: **If she ever lost access, could she actually get back in?**

Account Recovery: Your Digital Spare Key

Many online accounts have some type of recovery process. It is the backup plan for when you forget a password, lose a phone, replace a device, or get locked out, such as after suspicious activity. Recovery may rely on a backup email address, mobile number, recovery code, trusted device, security key, or another method you configured earlier.

The problem is that it is easy to set up these backup options once and forget about them. Years later, that backup email may be abandoned, the phone number may belong to someone else, or the recovery codes may be nowhere to be found. A strong password protects the front door. Good recovery planning makes sure you still have a safe way back inside.

Build Your Recovery Plan Before You Need It

1. Check Your Recovery Information

Start with your most important accounts, such as email, financial services, cloud storage, and your password manager. Open the security settings and review the recovery email addresses and phone numbers listed. Are they current? Do you still control them? If not, update them now.

`© SANS Institute 2026

2. Save Your Recovery Codes

Many services that use multi-factor authentication provide one-time backup or recovery codes. These codes can help you regain access if you lose your phone or cannot use your normal authentication method.

Save them somewhere secure, such as a password manager or password notebook that is stored securely.

3. Have More Than One Way Back In

Whenever possible, configure more than one recovery method. For example, you may have a backup email address plus recovery codes or a security key. Relying on only one device or phone number creates a single point of failure. If that method disappears, your access may disappear too.

4. Protect Your Recovery Email Account the Most

Many of your online accounts allow you to reset the password or recover the account by sending a recovery email to a personal email account. Make sure your primary email account is secure. As with all online accounts, apply basic cyber hygiene: protect your personal email with a long, unique password and multi-factor authentication. If a cybercriminal compromises your personal email that you use to recover your other accounts, they may be able to reset passwords and take over those other accounts.

5. Keep Recovery Information Private

Treat backup codes and recovery details like passwords. Never share them with someone who contacts you unexpectedly. Legitimate support personnel will never ask for your password, multi-factor authentication code, or backup recovery code.

6. Review Your Plan Once a Year

Phone numbers change. Email accounts get abandoned. Devices are replaced. Once a year, take a few minutes to review the recovery settings on your most important accounts. It can also help to maintain a secure list of your most important accounts so you can quickly review their recovery settings each year. Finally, consider giving a trusted family member access to essential recovery information in case of an emergency.

Account recovery is easy to ignore because everything works — until suddenly it does not. A lost phone, a forgotten password, a stolen device, or a hacked account can become a much bigger problem if your recovery options are outdated.

Guest Editor

Priya Saravanan is a Senior Security Consultant at UltraViolet Cyber with 7+ years of experience in offensive security. She specializes in web, API, mobile, and cloud penetration testing. She is the Vice President of the WiCyS Indianapolis Affiliate.



Resources

Stop Password Pain: Use a Reliable Password Manager: https://www.sans.org/newsletters/ouch/stop-password-pain-reliable-password-manager
The Power of the Passphrase: https://www.sans.org/newsletters/ouch/power-passphrase-why-longer-beats-smarter
How Cyber Criminals Steal Your Passwords: https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords

OUCH! Is published by SANS Security Awareness and distributed under the Creative Commons BY-NC-ND 4.0 license. You are free to share or distribute this newsletter as long as you do not sell or modify it. Editorial Board: Phil Hoffman, Leslie Ridout, Princess Young.

You can find more Ouch! On the following link: https://www.sans.org/newsletters/ouch