

Passwords & Account Security: Keep Your Accounts Yours

Most accounts are taken through a reused password, a fake login page, a shared code or an unlocked phone. Close each of those doors, and know exactly what to do if an account is taken over.

25 min read · Content last verified 18 September 2026 · Reviewed by Shravya M

Free awareness guide. Not legal or financial advice. <https://www.shravyadigital.com/guides/passwords-account-security>

CONTENTS

1. Before you start
2. Chapter 1: How accounts really get taken
3. Chapter 2: A strong password is a long one
4. Chapter 3: One password per account
5. Chapter 4: Two-step verification
6. Chapter 5: Fake login pages
7. Chapter 6: Your phone is the master key
8. Chapter 7: If an account is taken over
9. Quick reference card

Before you start

This guide is the reading for **Course 4** of the Digital Safety Pathway. It takes about 25 minutes to read. It covers the habits that keep your email, banking, social media and WhatsApp accounts yours: strong passwords, two-step verification, spotting fake login pages, securing your phone, and what to do if an account is taken over.

All names and examples here are made up.

Chapter 1: How accounts really get taken

Most accounts aren't "hacked" by genius. They're taken in a few ordinary ways:

1. **A reused password.** One website you signed up to years ago leaks its password list. Criminals then try the same email and password on email, banking and shopping sites.
2. **A fake login page.** A message sends you to a page that looks exactly like the real one, and you type your password into it.
3. **A shared code.** Someone persuades you to read out an OTP or a verification code, which is the key to your account.
4. **An unlocked or infected phone,** which receives all your codes.

Every chapter in this guide closes one of these doors.

The rule: Your password, your codes and your phone are three keys. Guard all three.

Chapter 2: A strong password is a long one

What makes a password weak

- Anything someone could guess from your life: **your name, a family member's name, your date of birth, your mobile number, your vehicle number**, or your favourite team.
- Short words with a number stuck on the end, like Priya@123.
- Common patterns such as 12345678, password or qwerty.

What makes a password strong

Length. A long passphrase made of several unrelated words is much harder to guess than a short jumble, and easier to remember. For example (don't use this one): mango-bicycle-river-lantern.

- Aim for **at least four random words**, or a long phrase that means something only to you.
- Add a number or symbol if the site asks for one, but length matters most.

The rule: Long beats clever. Use a passphrase, not a password.

Chapter 3: One password per account

Why it matters

If you use the same password everywhere, one leak anywhere unlocks everything. Your **email** matters most of all, because it can reset the passwords of almost every other account.

How to manage many passwords

- A **password manager** (built into your phone or browser, or a well-known app) can create and remember a different strong password for every account. You then need to remember only one strong passphrase.
- If you don't use one, at least use **completely different passwords** for your email, your banking, and your main social media account.
- **Never tell anyone your password**, including people claiming to be from your bank, your employer's IT team, or the app itself.

The rule: Every important account gets its own password. Your email gets the best one.

Chapter 4: Two-step verification

What it is

Two-step verification (also called two-factor authentication or 2FA) means that logging in needs **something you know** (your password) **plus something you have** (a code on your phone, a prompt in an app, or a security key). A stolen password alone is then not enough.

How to use it well

- **Turn it on** for your email, social media, WhatsApp (two-step verification PIN) and any other account that offers it.
- An **authenticator app** or an in-app prompt is generally harder to steal than an SMS code, because it doesn't depend on your SIM.
- **Only approve a login prompt that you started.** If your phone asks "Is this you signing in?" and it isn't, say no and change your password.
- **Never share a verification code or OTP**, whoever asks and whatever they say it's for. A code you're asked to read out is the key to your account or your money.

The rule: Turn on two-step verification, and never give anyone the code.

Chapter 5: Fake login pages

What it looks like

Suresh gets an email: "Unusual sign-in detected. Verify your account within 24 hours or it will be suspended." The button opens a page with the right logo and colours. The address bar says `accounts-verify-login.help`.

Why it works

The page looks right, and the message creates urgency. Whatever you type goes to the criminal.

The check

- **Don't sign in from a link in a message.** Open the app, or type the website address yourself.
- **Read the web address.** The Ministry of Home Affairs' job-fraud advice on cybercrime.gov.in points out that fake addresses often differ by a small spelling change, like `companie.com` or `compaany.com` instead of `company.com`, or `.net` instead of `.com`.
- A **padlock icon** only means the connection is encrypted. It does **not** mean the site is genuine.

The rule: Sign in only from an app or an address you typed yourself.

Chapter 6: Your phone is the master key

Your phone receives your OTPs, holds your banking apps and opens your email. Protect it like a wallet with every card in it.

- **Lock screen:** use a PIN, pattern or fingerprint, and set the screen to lock quickly.
- **Updates:** install system and app updates; many fix security holes.
- **Apps:** install only from your phone's **official app store**, never from a file sent in a message.
- **Lost or stolen phone:** call your bank to block UPI and net banking on that number, get a duplicate SIM, file a police report, and block the phone through **Sanchar Saathi**. Our [Sanchar Saathi guide](#) walks through it.
- **Aadhaar biometric lock:** UIDAI lets Aadhaar holders with a **registered mobile number lock their biometrics** (fingerprint, iris, face) through the **myAadhaar** portal or the **mAadhaar** app, so no one can use them for Aadhaar authentication until you unlock them.
- **Infected device?** The government's **Cyber Swachhta Kendra** (csk.gov.in), run by CERT-In, offers free tools and advice for cleaning it.

The rule: Lock your phone, update it, and install apps only from the official store.

Chapter 7: If an account is taken over

Act quickly, from a device you know is safe.

1. **Change the password**, and the password of any other account that used the same one. Start with your email.
2. **Log out of all other sessions or devices**. Most apps have an option for this in their security settings. In WhatsApp, check **Linked Devices**.
3. **Turn on two-step verification** if it wasn't on.
4. **Check your recovery email and phone number** in the account's settings. Criminals often change them so they can take the account back later.
5. **Warn your contacts** not to trust messages or files sent from the account while it was taken over.
6. **If money is involved**, call **1930** or report at **cybercrime.gov.in**, and **tell your bank the same day**.

Warning: Anyone who contacts you offering to "recover" your account for a fee is running a second scam. Use only the app's own recovery process.

The rule: New password, log out everywhere, turn on two-step, check recovery details.

Quick reference card

1. **Passphrase:** four or more random words. Long beats clever.
2. **One password per account.** Your email gets the strongest.
3. **Use a password manager**, or at least keep email, bank and social media different.
4. **Turn on two-step verification** everywhere it's offered.
5. **Never share an OTP or verification code**, with anyone.
6. **Sign in only from the app or an address you typed.**
7. **Lock, update, and use the official app store** on your phone.
8. **Hacked?** Change password, log out everywhere, check recovery details, report to 1930 if money is involved.

Take the course for what you just read

Take the free 10-question assessment and pass with 8 or more. Every course you pass counts towards a Pathway Certificate issued by Shravya Digital, earned when you pass all five courses in the pathway: <https://digital.shravyaworld.org/courses/passwords-account-security>

Sources

Checked against these primary sources on 18 September 2026. Rules change: if something here looks out of date, trust the source.

- UIDAI FAQs: biometric lock and unlock (<https://uidai.gov.in/en/contact-support/have-any-question/925-faqs/aadhaar-online-services/biometric-lock-unlock.html>)
- Ministry of Home Affairs / I4C, "Is your job offer fake or real?" (lookalike addresses) (<https://cybercrime.gov.in/pdf/Job%20Fraud%20Brochure%20Final.pdf>)
- Cyber Swachhta Kendra (CERT-In) (<https://www.csk.gov.in/>)
- I4C advice on WhatsApp linked devices (PIB, 7 Aug 2026) (<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2295889>)
- National Cyber Crime Reporting Portal and helpline 1930 (<https://cybercrime.gov.in/>)