Start Here: Your 7-Day Digital Safety Plan

Welcome to Click Giraffe

Welcome to Click Giraffe.

This member guide is designed to help you take the first practical steps toward a safer digital life.

You do not need to be technical.
You do not need to fix everything at once.
You do not need to understand every security term.

The goal is simple:

Take one small, useful step each day for seven days.

By the end of this plan, you will have improved the safety of your email account, passwords, phone, banking apps, home Wi-Fi, backups, and family scam-prevention habits.

Before You Begin

Digital safety can feel overwhelming because everything seems connected:

Email.
Phones.
Banking apps.
Passwords.
Wi-Fi.
Cloud storage.
Online shopping.
Social media.
Family devices.
AI tools.
Scam messages.

The best way to begin is not to panic.

The best way is to follow a simple order.

This 7-day plan focuses on the areas that matter most for everyday people, families, retirees, freelancers, and home-office users.

What This Plan Will Help You Do

This plan will help you:

- Protect your main email account.
- Reduce password reuse.
- Turn on multi-factor authentication.
- Secure your phone.
- Review banking and payment app safety.
- Improve home Wi-Fi security.
- Back up important files.
- Create a family scam-verification habit.

This plan is educational and self-service.

It does not include live support, emergency response, account recovery, device repair, malware removal, remote access, legal advice, financial advice, or professional incident response.

Day 1: Secure Your Main Email Account

Your main email account is one of the most important accounts you own.

If someone gets into your email, they may be able to reset passwords for your bank, cloud storage, shopping accounts, social media, phone account, or other services.

Today's goal

Make your main email account harder to break into.

Do this today

[ ] Confirm that your email password is unique.
[ ] Turn on multi-factor authentication.
[ ] Review your recovery email address.
[ ] Review your recovery phone number.
[ ] Remove recovery options you no longer use.
[ ] Check recent sign-in activity if your provider allows it.
[ ] Sign out of devices you do not recognize.

Important reminder

Do not share email verification codes with anyone.

A real company should not ask you to read them a login code, password reset code, or MFA code over the phone.

If you only do one thing today

Turn on multi-factor authentication for your main email account.

Day 2: Start Fixing Your Passwords

Reused passwords are dangerous.

If one website is breached and you used the same password somewhere else, criminals may try that password on your email, bank, shopping accounts, or social media.

Today's goal

Start replacing reused passwords with unique ones.

Do this today

[ ] Make a short list of your most important accounts.
[ ] Start with email, banking, Apple ID, Google account, Microsoft account, Amazon, PayPal, phone carrier, cloud storage, and social media.
[ ] Identify which passwords are reused.
[ ] Change at least three important reused passwords.
[ ] Consider using a reputable password manager.
[ ] Do not store passwords in plain notes, email drafts, text messages, or unsecured spreadsheets.

Good password manager options

Common reputable options include:

- Bitwarden
- Keeper
- 1Password
- Proton Pass
- NordPass

- RoboForm

Choose the tool you are most likely to keep using consistently.

If you only do one thing today

Change the password for your main email account if it is reused anywhere else.

Day 3: Turn On Multi-Factor Authentication

Multi-factor authentication, often called MFA or two-step verification, adds another layer of protection.

Even if someone knows your password, MFA can make it much harder for them to access your account.

Today's goal

Turn on MFA for your most important accounts.

Do this today

[ ] Turn on MFA for your main email account.
[ ] Turn on MFA for your bank accounts.
[ ] Turn on MFA for Apple ID, Google, or Microsoft accounts.
[ ] Turn on MFA for PayPal, Amazon, and social media.
[ ] Save backup codes in a safe place.
[ ] Do not share MFA codes with anyone.

MFA options

Common MFA options include:

- Authentication apps
- Passkeys
- Text-message codes
- Hardware security keys

Text-message codes are better than no MFA, but authentication apps, passkeys, or hardware security keys are usually stronger.

If you only do one thing today

Turn on MFA for your email and banking accounts.

Day 4: Secure Your Phone

Your phone is more than a phone.

It may contain your email, banking apps, photos, messages, password manager, MFA codes, payment apps, and private conversations.

Today’s goal

Make your phone harder to misuse if it is lost, stolen, or accessed by someone else.

Do this today

[ ] Use a screen lock.
[ ] Avoid simple PINs like 1234, 1111, or your birth year.
[ ] Update your phone operating system.
[ ] Update your apps.
[ ] Remove apps you no longer use.
[ ] Review app permissions.
[ ] Turn on Find My iPhone or Find My Device.
[ ] Back up important photos and contacts.
[ ] Protect your mobile carrier account with a strong password and account PIN if available.

Important reminder

Your phone number may be used to reset other accounts.

That means your phone carrier account also matters.

If you only do one thing today

Make sure your phone has a strong screen lock and is fully updated.

Day 5: Review Banking and Payment App Safety

Financial scams often rely on urgency, fear, or confusion.

Scammers may pressure you to send money through Zelle, Venmo, Cash App, PayPal, gift cards, wire transfers, or cryptocurrency.

Today's goal

Make financial accounts safer and reduce the chance of rushed payments.

Do this today

[ ] Use unique passwords for banking and payment apps.
[ ] Turn on MFA for financial accounts.
[ ] Turn on transaction alerts.
[ ] Review recent activity.
[ ] Remove old payment methods you no longer use.
[ ] Do not click banking links from text messages.
[ ] Use the official banking app or type the website directly.
[ ] Never share bank verification codes with anyone.

Slow-down rule

If someone says you must send money immediately, stop.

Call the person, bank, or company using a number you already trust.

Do not use the number in the suspicious message.

If you only do one thing today

Turn on transaction alerts for your main bank and payment accounts.

Day 6: Check Your Home Wi-Fi and Backups

Your home network connects your phones, computers, printers, smart TVs, cameras, tablets, and smart-home devices.

Your backups protect you if a device is lost, damaged, stolen, infected, or accidentally erased.

Today's goal

Improve your home technology foundation.

Do this today: Wi-Fi

[ ] Make sure your Wi-Fi password is strong.
[ ] Change the default router admin password if it is still unchanged.
[ ] Use WPA2 or WPA3 security if available.
[ ] Update router firmware if you know how to do it safely.
[ ] Create a guest network for visitors if your router supports it.
[ ] Consider replacing very old routers that no longer receive updates.

Do this today: backups

[ ] Identify your most important files.
[ ] Make sure important files are not stored only on one device.
[ ] Back up important photos and documents.
[ ] Protect cloud storage accounts with MFA.
[ ] Test that you can recover at least one file.

Good backup options

Common options include:

- iCloud
- Google Drive
- OneDrive
- Dropbox
- IDrive
- Backblaze

Cloud sync is useful, but it is not always the same as a true backup.

If you only do one thing today

Make sure your most important photos, documents, and records exist in more than one place.

Day 7: Create a Family Scam-Safety Plan

Scams are easier to prevent when families have simple rules before something happens.

This is especially important when helping older relatives, teenagers, or anyone who may be pressured by urgent messages.

Today's goal

Create a simple household plan for suspicious messages and money requests.

Do this today

[ ] Choose one trusted family contact for technology questions.
[ ] Create a family verification phrase.
[ ] Agree not to send money based only on a text, email, or unexpected call.
[ ] Make a list of critical accounts.
[ ] Review scam warning signs together.
[ ] Discuss what to do if someone clicks a suspicious link.
[ ] Decide who can help if someone is locked out of an account.
[ ] Keep recovery information in a safe, legal, and trusted place.

Family verification phrase

A verification phrase is a private phrase known only to trusted family members.

If someone calls or texts claiming to be a relative in an emergency, ask for the phrase before taking action.

Example:

"What was the name of our first family dog?"

Choose something that is easy for family members to remember but hard for a stranger to guess from social media.

Important reminder

Do not shame someone for falling for a scam.

Scammers are professionals. The goal is to slow down, verify, and respond quickly.

If you only do one thing today

Create a family rule: no urgent money transfers without voice or in-person verification through a trusted contact method.

Your 7-Day Completion Summary

Use this page to track your progress.

[ ] Day 1: I reviewed and protected my main email account.
[ ] Day 2: I started replacing reused passwords.
[ ] Day 3: I turned on MFA for key accounts.
[ ] Day 4: I secured and updated my phone.
[ ] Day 5: I reviewed banking and payment app safety.
[ ] Day 6: I checked Wi-Fi and backup basics.
[ ] Day 7: I created a family scam-safety plan.

What to Do Next

After completing this 7-day plan, continue with the Click Giraffe member library.

Recommended next resources:

1. How to Recognize Scam Emails and Texts.
2. How to Secure Your Main Email Account.
3. Password Manager Starter Guide.
4. MFA Starter Guide.
5. What to Do If You Clicked Something Suspicious.
6. Protecting Older Relatives from Scams.

You do not need to complete everything at once.

Digital safety improves through repeated small habits.

Simple Rules to Remember

Protect your email first.
Use unique passwords.
Turn on MFA.
Slow down before clicking.
Never share verification codes.
Keep your phone locked and updated.

Back up important files.
Verify urgent money requests.
Do not let fear rush your decisions.
Ask for help before sending money or sharing sensitive information.

Click Giraffe Reminder

Click Giraffe is a self-service digital safety membership.

It provides educational guides, checklists, tutorials, monthly scam alerts, and practical resources.

It does not provide live technical support, emergency support, remote access, device repair, account recovery, malware removal, legal advice, financial advice, medical advice, managed IT services, or guaranteed remediation.

If you are facing fraud, stolen money, identity theft, a compromised account, or an urgent incident, contact the relevant provider, financial institution, law enforcement agency, or qualified professional.