

# The Example family

Prepared October 16, 2026 · by Alex Sample, CISSP  
Version 1 · Review by October 16, 2027  
Keep this by your computer. Never write passwords in it.

QUESTIONS? CALL ALEX

**(555) 010-0199**

hello@example.com

## If something seems wrong

Do these in order. You will not get in trouble for stopping to check.

- 1** Stop. Do not click, do not call the number on the screen, and do not send money or codes.
- 2** If someone is on the phone with you, hang up. If a warning fills the screen, turn the device off.
- 3** If money may be involved, call your bank using the number below or the one on the back of your card.
- 4** Call your family helper, Casey Example, or call me at (555) 010-0199.
- 5** Write down what happened while you remember it: the time, what they said, and any phone number or website.

## Your important phone numbers

Use these numbers, not ones given to you in a call, text, email or pop-up.

| WHO                                             | PHONE NUMBER                                   | NOTES                                        |
|-------------------------------------------------|------------------------------------------------|----------------------------------------------|
| Sample Community Bank (checking and savings)    | <b>Use the number on the back of your card</b> | Joint account. Trusted contact added: Casey. |
| Example Rewards Visa card                       | <b>Use the number on the back of your card</b> | Card replaced October 3; new card ends 4821. |
| Example Wireless (cell phone company)           | <b>(555) 010-0165</b>                          | Or use the number on your bill               |
| Sample Health Plan (made up) (health insurance) | <b>(555) 010-0161</b>                          | Member services                              |
| Example Family Medicine (doctor)                | <b>(555) 010-0162</b>                          | Dr. Lee's office                             |
| Example Fiber (internet provider)               | <b>(555) 010-0163</b>                          | Internet and home Wi-Fi                      |
| Sample Pharmacy, Main Street (pharmacy)         | <b>(555) 010-0164</b>                          | Prescriptions                                |
| Casey Example (daughter)                        | <b>(555) 010-0131</b>                          | Family helper                                |
| Alex Sample, CISSP                              | <b>(555) 010-0199</b>                          | Monday to Friday, 9 a.m. to 5 p.m.           |
| Emergency                                       | <b>911</b>                                     | If you are in danger or being threatened     |

## STEP 1 OF 3

**Assess**

Where you stand today

## What happened

On September 30 a caller who said he was from Sample Community Bank's fraud department told Pat there was a suspicious charge, and asked her to read back a code sent to her phone. The code was really for her email account. Over the next two days the caller changed her email settings and tried to send a \$4,800 transfer, which the bank stopped.

### Step by step

|   | WHEN                   | WHAT HAPPENED                                                                                                                 |
|---|------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| 1 | Sept 30, about 10 a.m. | A caller says he is from the bank's fraud department and asks Pat to read back a code sent to her phone. She reads it to him. |
| 2 | Sept 30, 10:20 a.m.    | The caller signs in to Pat's email and adds a rule that hides messages from the bank.                                         |
| 3 | Oct 1, 3 p.m.          | Using Pat's email to reset the bank website password, the caller starts a \$4,800 transfer to an unknown account.             |
| 4 | Oct 2, 9 a.m.          | The bank's fraud team stops the transfer and calls Lee on the number they have on file.                                       |
| 5 | Oct 2, 1 p.m.          | Casey calls Example Security Partners. Email and bank sign-ins are secured the same afternoon.                                |

Keep this timeline. Your bank, the police or the FTC may ask for it.

## Your accounts and how they are protected

A second login step means a thief needs more than your password. This list has no passwords in it, on purpose.

| ACCOUNT     | SECOND LOGIN STEP      | NOTES                         |
|-------------|------------------------|-------------------------------|
| Email (Pat) | Authenticator app code | Forwarding rule removed Oct 2 |
| Email (Lee) | Authenticator app code |                               |

| ACCOUNT                 | SECOND LOGIN STEP      | NOTES                    |
|-------------------------|------------------------|--------------------------|
| Bank website            | Approve on your phone  | Sample Community Bank    |
| Apple ID                | Text message code      | Codes go to Pat's iPhone |
| Amazon                  | Authenticator app code |                          |
| Medicare (Medicare.gov) | Not turned on yet      | On the to-do list        |

## Your devices

How each one is set up today.

| DEVICE               | UNLOCKS WITH                 | UPDATES   | BACKUP                      |
|----------------------|------------------------------|-----------|-----------------------------|
| Pat's iPhone         | Face ID and 6-digit passcode | Automatic | Not yet (on the to-do list) |
| Lee's Windows laptop | PIN                          | Automatic | Weekly to an external drive |
| Family iPad          | Passcode                     | Automatic | Nightly to iCloud           |

## Your cell phone account

Your phone number is a key to your accounts, because login codes are sent to it. Thieves try to move phone numbers to their own phones.

|                           |                                                  |
|---------------------------|--------------------------------------------------|
| Cell phone company        | Example Wireless                                 |
| Your cell phone number    | (555) 010-0132                                   |
| Account number            | Ending in 7731                                   |
| To reach them             | (555) 010-0165, or dial 611 from your cell phone |
| Protection on your number | Number lock and account PIN are both set         |
| Your plan                 | Two lines, unlimited, about \$90 a month         |

- ☐ Your phone company will never call or text you to ask for your PIN or a code. If someone does, hang up.

- ☐ If your phone shows "No service" or "SOS only" for more than an hour at home, call the phone company from another phone, then call me.
- ☐ Before you change your plan, add a line, or trade in a phone, you can say "I need to think about it." Then call your family helper or me.
- ☐ Read your phone bill each month. Call about any new line, device or charge you did not ask for.

## STEP 2 OF 3

# Prioritize

What we fixed, and how to use it

## What we fixed

### Done

- ✓ Changed the email password and signed out every other device
- ✓ Removed mail forwarding rules the scammer added
- ✓ Turned on a second login step for email
- ✓ Turned on a second login step for bank and card accounts
- ✓ Set up a password manager and replaced reused passwords
- ✓ Reported the fraud to the bank's fraud department
- ✓ Froze credit at Equifax, Experian and TransUnion
- ✓ Filed a report with the Federal Trade Commission
- ✓ Filed a report with the FBI's Internet Crime Complaint Center
- ✓ Added a trusted contact at the bank
- ✓ Checked both laptops and phones for remote-access programs; none were found
- ✓ Agreed a family code word with Pat, Lee and Casey

### Still to do, most important first

- ☐ Set up the password manager on Lee's laptop (booked for October 22)
- ☐ Turn on automatic backup for Pat's iPhone
- ☐ Review the Visa statement together when it arrives in November

## Your password manager: Bitwarden

An app on your phone and a small shield button in your web browser. It remembers a different strong password for every account, so you do not have to.

- 1 Open Bitwarden (a blue shield icon).
- 2 Unlock it with your master password, or with your fingerprint or face if we turned that on.

- 3 To sign in to a website: click the shield button at the top of your browser, then click the login it shows. The name and password fill in.
- 4 To save a new account: click New, choose Login, and use the Generator to create the password. Click Save.
- 5 To look something up: open Bitwarden and type the website's name in the search box.

**Your master password is the one password to remember. Nobody can reset it for you, not Bitwarden and not me.**

Your emergency sheet is kept: in the fireproof box in the hall closet

If the password manager ever offers to fill in a password and then does not, stop. You may be on a fake copy of the website. Close it and call me.

## Your second login step

After your password, the website asks for one more thing that only you have. Here is how each kind works.

### | A code from Microsoft Authenticator

- 1 Sign in with your username and password as usual.
- 2 Open Microsoft Authenticator on your phone.
- 3 Find the name of the website in the list. Next to it is a six-digit code that changes every 30 seconds.
- 4 Type the code into the website before it changes. If it changes, just use the new one.

### | An approval request on your phone

- 1 Sign in with your username and password as usual.
- 2 Your phone shows a message asking whether you are trying to sign in.
- 3 Tap Yes only if you are signing in right now.
- 4 If the message appears when you are not signing in, tap No. Someone may have your password. Call me.

## A code sent by text message

- 1 Sign in with your username and password as usual.
- 2 Within a minute, a text message arrives with a short code, usually six numbers.
- 3 Type that code into the website or app you just opened.
- 4 If a code arrives when you were not signing in, do nothing with it and call me.

### About login codes and approvals

A code or an approval request is a second key to your account.

Type a code only into a website or app that you opened yourself.

Never read a code to anyone on the phone. Your bank will not ask for it, and neither will I.

If your phone asks you to approve a sign-in you did not start, tap No and call me.

If you lose your phone: your backup codes are kept with the emergency sheet in the fireproof box. Call me before you use them and I will walk you through it.

## How to spot a scam

One of these is a warning. Two or more is almost certainly a scam.

- ☐ Someone contacts you first, by phone, text, email or pop-up, about a problem you did not know you had.
- ☐ They say you must act right now, or something bad will happen.
- ☐ They ask you to keep it secret from your bank, your family or anyone else.
- ☐ They want payment by gift card, wire transfer, cryptocurrency, cash in the mail or a payment app.
- ☐ They ask for a code that was just sent to your phone or email.
- ☐ They ask to connect to your computer or phone, or to install a program so they can 'help'.
- ☐ They say they are from your bank, Microsoft, Apple, Medicare, Social Security, the IRS or the police.
- ☐ A message or pop-up tells you to call a phone number it gives you.

## | What to do every time

- 1 Stop. Real problems can wait ten minutes. Scams cannot.
- 2 Hang up or close the message. You are not being rude.
- 3 Look up the phone number yourself, on the back of your card or on a statement, and call that.
- 4 Never read a login code to anyone. Type it only into a website or app you opened yourself.
- 5 When in doubt, call your family helper or call me before you do anything else.

**Your family has a code word. It is not written here. Anyone who calls saying they are family and need money must say it. If they cannot, hang up.**

## How I help you from a distance

Sometimes I need to see your screen to help. These rules never change.

- 1 You call me, or we set a time. I do not connect without talking to you first.
- 2 The only program I use is Quick Assist (built into Windows). If anyone asks you to install a different one, it is not me.
- 3 You start the connection yourself and read me the code on your screen.
- 4 You can see everything I do. You can end the connection at any time by closing the window.
- 5 When we finish, I end the connection and remove the program.

**Banks, Microsoft, Apple, Medicare and the government never ask to connect to your computer.**

## STEP 3 OF 3

## Adjust

Keeping it current

## Your ten-minute monthly check

Pick a day, such as the first of the month, and tick these off.

- ☐ Read your bank and card statements. Call the bank about any charge you do not recognize.
- ☐ Install updates when your phone or computer offers them, then restart the device.
- ☐ Check that your backup ran this month.
- ☐ Delete emails and texts from senders you do not know, without tapping any links.
- ☐ Tell your family helper about anything that seemed odd, even if you handled it.

### Once a year

- ☐ Get your free credit reports at [AnnualCreditReport.com](https://AnnualCreditReport.com) and look for accounts you did not open.
- ☐ Ask your bank to confirm the trusted contact on your accounts.
- ☐ Go through this playbook with your family helper and with me, and print the new version.

### This playbook has a review date

Phone numbers, websites and scams change. Review this playbook by October 16, 2027.

Call me before then and we will go through it together and print a new version. Also call me if you get a new phone or computer, change banks, or move.

## Where to report fraud and get help

Call your bank first if money is involved. A report also strengthens a bank dispute.

| WHO                           | PHONE                 | WEBSITE                                                       | USE IT FOR                                       |
|-------------------------------|-----------------------|---------------------------------------------------------------|--------------------------------------------------|
| Federal Trade Commission      | <b>1-877-382-4357</b> | <a href="https://ReportFraud.ftc.gov">ReportFraud.ftc.gov</a> | Report any scam                                  |
| Identity theft recovery (FTC) | <b>1-877-438-4338</b> | <a href="https://IdentityTheft.gov">IdentityTheft.gov</a>     | Someone used your name or Social Security number |

| WHO                                           | PHONE                 | WEBSITE               | USE IT FOR                                                                                                    |
|-----------------------------------------------|-----------------------|-----------------------|---------------------------------------------------------------------------------------------------------------|
| FBI Internet Crime Complaint Center           |                       | ic3.gov               | Online fraud, especially if money was lost                                                                    |
| National Elder Fraud Hotline                  | <b>1-833-372-8311</b> |                       | Help for adults 60 and over, U.S. Department of Justice                                                       |
| AARP Fraud Watch Helpline                     | <b>1-877-908-3360</b> | aarp.org/fraud        | Talk to a trained volunteer                                                                                   |
| Equifax                                       | <b>1-888-298-0045</b> | equifax.com           | Freeze or unfreeze your credit                                                                                |
| Experian                                      | <b>1-888-397-3742</b> | experian.com          | Freeze or unfreeze your credit                                                                                |
| TransUnion                                    | <b>1-800-916-8800</b> | transunion.com        | Freeze or unfreeze your credit                                                                                |
| Social Security fraud line                    | <b>1-800-269-0271</b> | oig.ssa.gov           | Scams using Social Security's name                                                                            |
| Medicare                                      | <b>1-800-633-4227</b> | medicare.gov          | Medicare card or billing fraud                                                                                |
| IRS                                           | <b>1-800-829-1040</b> | irs.gov               | Check whether a letter or bill from the IRS is real                                                           |
| IRS identity theft line                       | <b>1-800-908-4490</b> | irs.gov/identitytheft | Someone filed a tax return in your name                                                                       |
| Treasury Inspector General (TIGTA)            | <b>1-800-366-4484</b> | tigta.gov             | Report someone pretending to be the IRS                                                                       |
| Arizona Attorney General, Consumer Protection | <b>602-542-5763</b>   | azag.gov/consumer     | Report a scam to the state. Also 520-628-6648 (Tucson)                                                        |
| Arizona Adult Protective Services             | <b>1-877-767-2385</b> | des.az.gov            | Someone is taking advantage of an older or vulnerable adult                                                   |
| Local police or sheriff, non-emergency        | <b>602-876-1011</b>   |                       | File a police report: city police inside city limits, county sheriff outside them. In an emergency, call 911. |
| Eldercare Locator                             | <b>1-800-677-1116</b> | eldercare.acl.gov     | Find local help for an older adult, including Adult Protective Services                                       |

Phone numbers last checked October 15, 2026.

## For your family helper

Casey Example, this page is for you.

- ☐ Be the first call. If something seems wrong, your relative should be able to reach you without feeling judged.
- ☐ Never ask for passwords by phone, text or email. If you need to help with an account, do it together, in person or on a video call.
- ☐ Agree on a family code word. Anyone who calls claiming to be family and asking for money must know it.
- ☐ Know where this playbook and the password manager's emergency sheet are kept.
- ☐ If money has left an account, the bank's fraud line comes first, then the reports listed in this playbook.

### How you will know it is really me

I never ask for your passwords. You type them yourself.

I never take gift cards, wire transfers or cryptocurrency.

I never call you out of the blue. If someone calls saying they are me, hang up and dial (555) 010-0199 yourself.

### Alex Sample, CISSP · Example Security Partners LLC

(555) 010-0199 · hello@example.com · example.com

Monday to Friday, 9 a.m. to 5 p.m.