FREE GUIDE FROM LEGACY SOLUTIONS ARCHITECTURE

The 72-Hour Bank Crash and Cyber Survival Guide

Simple steps to protect your money from hackers, outages and bank failures. About 10 minutes to start.

What just happened in Paraguay

In the first week of November 2026, Paraguay's central bank took over **Ueno Bank**, a digital bank that says it has close to 3 million customers in a country of about 6.5 million. The app, cards and transfers stopped and branches shut. Pensions paid through the bank were frozen.

It was not a hack. Euronews, Reuters, the Associated Press and others report that the central bank found the bank's capital had fallen below half of the legal minimum, after regulators found poorly documented loans and expenses booked as assets. Reports of a cyberattack are not supported. (Sources as reported 3 to 6 Nov 2026; the story is still developing.)

Why it matters to you, wherever you live

A hacked bank, a ransomware attack, a bad outage and a failed bank all feel the same to you: the app will not open, the card is declined, the transfer never lands. You get no warning for any of them.

Security people call it a **single point of failure**: one app, one bank, one card, one phone. If your salary lands there, your rent leaves from there and your savings sit there, one thing is holding up your whole life.

The aim of this guide is not to scare you. Nobody can promise your bank will never fail or never be attacked. You can make sure that if it happens, it is an inconvenience and not a disaster.

The 10-minute check: do this tonight

- [ ] **Map your money.** Where does your salary land? What leaves from where? Could you cope if that account was out of reach for two weeks?
- [ ] **Second bank, second card.** Open an account at a different bank, with a card on a different network if possible.
- [ ] **Cash buffer.** Keep a few days of cash somewhere safe at home (enough for food, transport, essentials).
- [ ] **Turn on alerts** for every transaction, in the bank's app.
- [ ] **Move off text-message codes.** Use an authenticator app for your bank and your email (page 2).
- [ ] **Write down** your bank's emergency number and your account details, and keep the list offline (paper or a locked file).
- [ ] **Look up your deposit guarantee**: how much is covered per person, per bank, and what is not.

PART 1

Stop getting hacked: the basics

Ten habits that stop most attacks on ordinary people. None needs special software.

1. **One password manager, a different password for every site.** Reusing passwords is how one leak becomes ten.
2. **Lock your email first.** Email resets every other account. Give it your strongest password and an authenticator app.
3. **Authenticator app or passkey, not text codes.** Text messages can be redirected (SIM swap). Switch on the app option for your bank, email and social accounts.
4. **Ask your phone company for a SIM-swap PIN or lock.** It stops someone taking over your number.
5. **Never approve a request you did not start.** Banks and apps send "approve this login" prompts. If you did not just try to log in, tap Deny and change your password.
6. **Your bank will never ask for your PIN, password or one-time code.** Not by phone, not by SMS, not by WhatsApp. If in doubt, hang up and call the number printed on your card.
7. **Do not click links in messages about your bank.** Type the bank's address yourself or use its official app.
8. **Keep your phone and apps updated.** Updates fix the holes attackers use.
9. **Check your statement weekly.** A small strange payment is often the test before a big one. Report it the same day.
10. **Use a low-limit card for online shopping** and keep your main account card for the shops you trust.

Red flags

- "Urgent: your account will be closed"
- A caller who knows your name and pressures you
- Asking you to install a screen-sharing app
- A "refund" you did not expect

If you are hacked

- Call your bank and freeze the card
- Change your email password first
- Switch on the authenticator app
- Report to the police and keep screenshots

PART 2

If your bank freezes: the first 72 hours

A calm plan, in order. Print it and keep a copy offline.

Hour 0 to 1	**Stay calm and confirm.** Check the central bank, regulator and the bank's official channels. Do not click links in messages. Do not give anyone your login. Write down what you were told and when.
Hour 1 to 24	**Cover the essentials.** Use your second account, second card and cash buffer for food, transport and urgent bills. List what must be paid in the next 14 days and from where. Ask employers to pay into your second account if salary is due.
Day 2	**Find your rights.** Look up the deposit guarantee: the amount, who pays, how long it takes and how to claim. Gather ID and account details. Expect that anything above the guarantee may be at risk.
Day 3	**Watch for scams and plan ahead.** Fraudsters move in fast after a bank failure with fake "recovery" calls, apps and links. Only claim through official channels. Then move salary and standing orders so you are not dependent on one bank again.

From survival plan to money plan

Level 1: this week

- A few days of cash
- Two banks, two cards
- Alerts and an authenticator app

Level 2: this month

- A written money map
- Savings spread so no bank holds more than its guarantee
- Offline copy of key details

Level 3: this year

- An emergency fund of 3 months of costs in two places
- Insurance and documents reviewed
- A yearly 15-minute re-check

If you run a business: ask the same question at a bigger size. If your bank, your email or your cloud login went dark tomorrow, how long could you keep trading? Who can pay staff? Who can invoice? Finding single points of failure before they find you is what we do at Legacy Solutions Architecture. Message us at **legacy-sa.co.za** and we will walk through it with you.

General education only, not financial, legal or investment advice. Rules and guarantees differ by country: check your own regulator. Paraguay facts as reported by Euronews, Reuters (via Al Jazeera), the Associated Press and Outlook India, 3 to 6 November 2026.