

SOCIALCO-LAB DIGITAL SAFETY SERIES

Computer Security Alert Response Packet

A church leadership resource for recognizing fake security alerts, responding safely, and protecting ministry teams from urgent digital scams.

Purpose

This packet equips church leaders, administrators, and ministry teams with a calm response protocol for fake browser-based security alerts. These alerts often look official, but they are designed to create fear, urgency, and compliance.

Core Principle

Most digital scams are not attacks on the computer first. They are attempts to influence the person using the computer. The target is attention, trust, and decision-making.

How to Recognize a Fake Security Alert

- It claims the computer is locked, infected, disabled, or being monitored.
- It tells the user to call a phone number immediately.
- It uses urgent language about fraud, stolen data, or permanent damage.
- It appears inside Safari, Pinterest, Facebook, email, or another website.
- It combines official-sounding company names in ways that do not match real Apple language.

Important truth: Apple does not send virus warnings through web pages, and Apple does not ask users to call phone numbers from browser popups.

Immediate Response Protocol

1. Do Not Interact

Do not click buttons. Do not select authorize. Do not call the phone number.

2. Force Quit Safari

Press Command + Option + Escape, select Safari, then click Force Quit.

3. Reopen Safely

Hold the Shift key while opening Safari to prevent the same page from reopening.

4. Clear Website Data

Safari, Settings, Privacy, Manage Website Data, Remove All.

5. Check Notifications

Safari, Settings, Websites, Notifications. Remove anything unfamiliar.

6. Restart the Mac

Restart normally after clearing browser data and notification permissions.

Never Do These Things

Never call a number from a popup.

Never allow remote access from a stranger.

Never enter passwords or financial information.

When to Ask for Help

- The user clicked a button on the alert.
- The user called the phone number.
- The user downloaded anything from the page.
- The user gave someone remote access to the computer.
- The screen will not close after force quitting the browser.

One rule to remember:

If a message creates urgency and tells you to call someone, stop and verify first.

Church Leadership Tech Safety Protocol

Digital discernment is now part of leadership responsibility. Leaders should pause, verify, and respond calmly when digital threats appear.

Common Threats to Leadership

- **Fake security alerts:** Popups claiming a device is infected or locked.
- **Phishing emails:** Messages pretending to be from banks, Apple, Microsoft, staff, or church members.
- **Impersonation requests:** Messages that appear to be from leadership asking for money, gift cards, passwords, or urgent confidential action.
- **Malicious links:** Links from social platforms, emails, ads, or search results that redirect to deceptive pages.

Leadership Communication Protocol

- Remain calm.
- Do not act under pressure.
- Contact a designated trusted person.
- Take a screenshot if possible.
- Do not attempt to fix the issue by calling unknown support numbers.

Recommended Support Structure

- Identify one trusted technical contact.
- Identify one backup contact.
- Teach staff and leaders this instruction: call before acting.
- Review this protocol during onboarding and annual leadership training.

Reassurance

Most browser-based alerts are deceptive prompts, not confirmed system breaches. When handled correctly, the risk is contained and the user can return to work safely.