



Doh!!! I Clicked the Link. Now What?

First, breathe. Clicking a link is rarely the emergency. What you typed next is what matters.

START HERE: Did you type anything after clicking?

A password, a card number, your Social Security number, a login.

If you only looked, and typed nothing: close the page and skip to Step 4. You are very likely fine.

If you typed something in: work through Steps 1 to 4 now, in order.

1. Stop and disconnect.

Do not enter anything else. Close the page.

On a computer: if you were prompted to download or install anything, turn off the Wi-Fi or unplug the network cable now. This stops anything mid-download.

On a phone: close the browser tab or app. You do not need to turn the phone off.

2. Change the password you typed. Right away.

Use a different device than the one you clicked on: your phone if you clicked on the computer, or the other way around.

Change it for that account, and for any other account where you use the same password. This is the single most important step.

3. Gave card or bank details? Call your bank.

Use the number printed on the back of your card or on your statement. Not a number from the text, the email, or the website you just clicked.

Tell them what happened. They can freeze the card, watch for charges, and send a new one.

4. Expect a follow-up, and ignore it.

Scammers know when someone has taken the bait. Within days you may get a call or email from a “fraud department,” a “recovery service,” or “tech support” offering to fix it or get your money back.

That is the same scam wearing a different hat. Real help never arrives uninvited. Hang up.

You are not in trouble, and you are not alone.

This happens to careful, capable people every single day. The people who get hurt are the ones who stay quiet. Tell someone you trust today.

To report it: Louisiana Attorney General, or the FTC at reportfraud.ftc.gov.
