What to do if you clicked a link

step by step

First: take a breath.
This happens to very smart, very careful people every single day.
Clicking a suspicious link is not a moral failure — it's a human response to a message that was carefully engineered to look real.
What matters now is what you do next.

1 STOP

Do not enter any passwords, credit card numbers, bank account information, or your Social Security number on any page that opened after clicking.

---

2 DISCONNECT

Turn off your WiFi or unplug the internet cable. This stops any software from downloading in the background.

---

3 CALL SOMEONE YOU TRUST

A family member, a neighbor, or anyone who is comfortable with computers. Tell them what happened. Let them help you from here.

4 CALL YOUR BANK

If you entered any financial information — your card number, your bank login, your account number — call your bank right now. The number is on the back of your card.
Say:
"I may have entered my information on a scam website. What should I do?" They will take it from there

---

5 CHANGE YOUR PASSWORDS

If you entered any passwords, change them as soon as you're safely back online — ideally with a family member helping.

---

6 REPORT IT

When you're ready - report at reportfraud.ftc.gov.
You are not in trouble. You did nothing wrong.
Reporting helps protect the next person.
You handled this. That took courage.

Go to genguard365.com any time you need us.