If a Scammer Got Your Money or Your Computer

What to do, in order, and why each step matters

You are not the first person this has happened to, and you will not be the last. Scammers do this all day and they are good at it. Nothing here is your fault. Work down the list in order and tick each box as you go. If you only manage the first two steps today, that is still worth a great deal.

Speed is the whole game

A transfer can sometimes be stopped, and a password can sometimes be changed in time, but only if you move now. The first hour matters more than the first week. Do not tidy up, do not ring anyone back, and do not wait to see what happens.

1 Stop the connection right now

- Pull the internet cable out, or switch the Wi-Fi off on the computer.
- If somebody is on your screen, switch the router off at the wall as well.
- Hold the power button down until the computer turns off. Leave it off.
- Do not click anything else, and do not ring the caller back.

WHY THIS MATTERS

While the connection is open they can watch your screen, open your files and read what you type. Cutting the connection is the one thing that stops them mid-sentence. It does not undo what they have already seen, which is what step two is for.

2 Stop the money

- Ring the bank, the card company or the payment app.
- Use the number printed on the back of your card, never one a caller gave you.
- Ask them to freeze the card or account, and to recall anything sent today.
- Ask for a dispute on anything you did not authorise, and write the case number down.

WHY THIS MATTERS

Money can sometimes be pulled back if it is caught quickly, and the bank can put a stop on the account while you sort out what happened. The number on your card reaches your real bank. A number from a caller reaches the thief.

3 Change your passwords from a clean device

- Use your phone, or another computer that the scammer never touched.
- Change your main email password first, and then your bank.
- Change every account that used the same password, and never reuse it again.
- Switch on two-step sign-in wherever you are offered it.

WHY THIS MATTERS

A password changed on a computer they can still see is a password they simply read as you type it. Email comes first because whoever controls your email can reset the password on almost everything else you own.

4 Have the computer checked before you use it again

- Leave the computer switched off until somebody has looked at it.
- No banking, shopping or email logins on it in the meantime.
- Ask for the remote-access software and any odd start-up items to be removed.
- Ask what was exposed, so you know what else needs changing.

WHY THIS MATTERS

Programs that let somebody back in often survive a restart and do not show up as an obvious icon. A proper check is how you find out what was taken and what still needs changing, instead of guessing.

Who to ring, and where to report it

Every number and address below is the organisation's own published one.

Your bank or card company
The number on the back of your card, or in the bank app.
Ask for the fraud line. Say: unauthorised access, or a transfer I did not make.

FBI – Internet Crime Complaint Center
ic3.gov
Online form. File it even if you doubt it will go anywhere.

FTC – Report Fraud
reportfraud.ftc.gov • 1-877-382-4357
Federal Trade Commission. Most scam reports belong here.

Identity theft
identitytheft.gov • 1-877-438-4338
If your details were used to open anything, this builds the official record.

CISA – Report
cisa.gov/report • 1-888-282-0870
Cybersecurity and Infrastructure Security Agency. The computer side.

Missouri Attorney General – Consumer Protection
ago.mo.gov • 1-800-392-8222
Your state consumer protection office. They take scam complaints.

Your local police
The non-emergency number, not 911.
Worth doing for the report number. It helps with the bank and the insurer.

Never ring a number a caller gave you, even if it looks like the bank's number on your screen, and never install anything because somebody on the phone asked you to. If a number here looks wrong, go to the website and read it there yourself.

Ozark Computer Clinic
Need A Geek? We Can Help!
573.693.PCrx (7279)
2935 Bagnell Dam Blvd., Suite 213, Lake Ozark, MO 65049
Open Monday, Wednesday and Friday, 12:00 PM to 5:00 PM
support@ozarkcomputerclinic.com • Bring the computer and its charger.

Your notes

Times, names, case numbers, anything the bank or the police asked you for.

Take your time. One box at a time is still progress.