CyberGuardLab

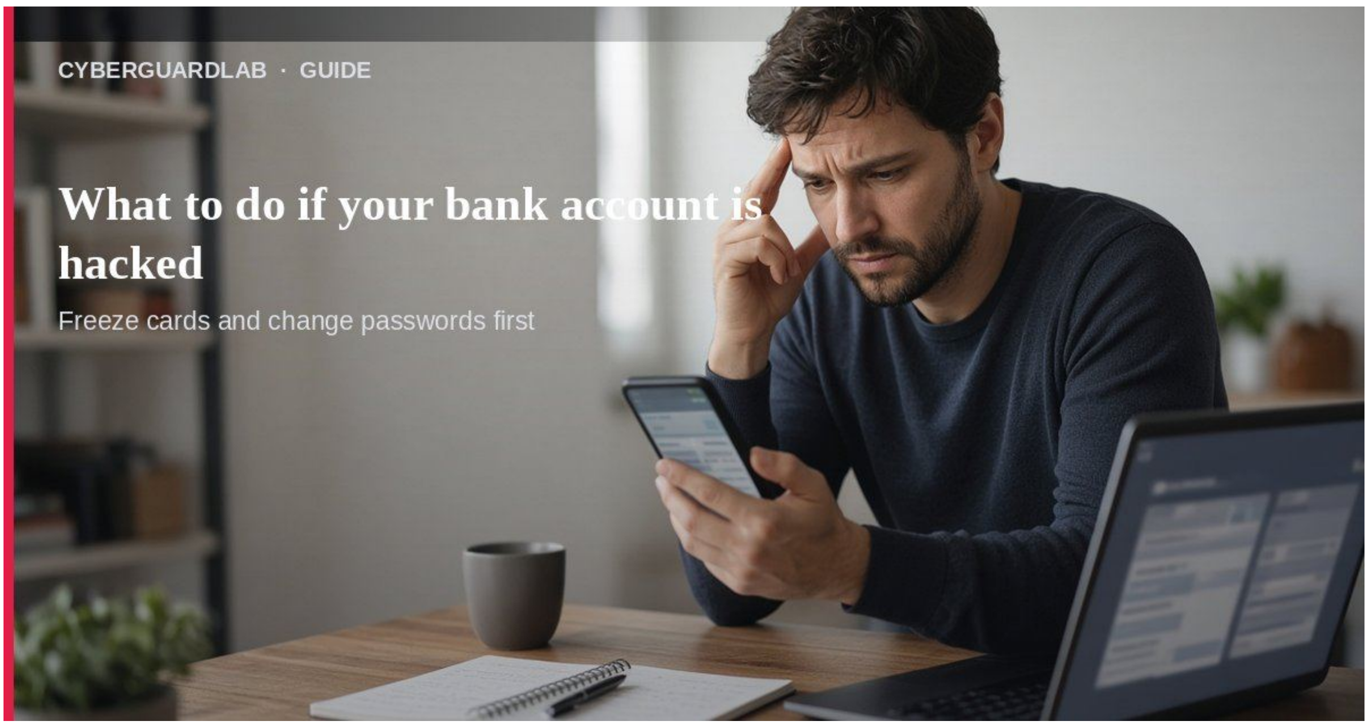
Household antivirus, explained

cyberguardlab.com

What to do if your bank account is hacked

https://cyberguardlab.com/blog/bank-account-hacked-first-hour

Independent US household comparison site. Not the vendor. Paid links below may earn a commission. Confirm first-year price, renewal, device limit, and refund terms at checkout.



If your checking or savings account looks compromised-or you get a call about "fraud on your bank account"-the first hour is about stopping transfers, contacting the real bank, and locking down sign-in. Per FTC consumer alerts, scammers often pretend to be your bank and tell you to move money to a "safe" account or to share verification codes. That is the scam. This guide focuses on bank account compromise and bank-fraud impersonation calls, not the separate credit card fraud first-hour path (cards often have stronger dispute rules than money you were tricked into sending from checking). You do not need to buy antivirus before you call the number on your statement or in your official banking app.

1. Two situations this page covers

* Unauthorized activity - Transfers, withdrawals, or new payees you did not start on checking/savings.
* Bank impersonation call - Someone claims fraud on your account and coaches you to "protect" funds by moving them, buying crypto, or reading codes from a text.

FTC: a call about fraud activity on your bank account could be a scammer. Treat the inbound call as hostile until you verify with the bank yourself.

2. First-hour checklist (do these in order)

* Do not move money to "protect it" - That is a common bank-impersonation trap. Real banks do not ask you to wire, crypto-send, or payment-app your balance to safety.
* Do not share verification codes or one-time passwords - Hang up if anyone asks for the code that just arrived on your phone.
* Call the bank using a number you already trust - Statement, back of a debit card, or the phone number inside your official banking app-not the number the caller gave you.
* Report the unauthorized activity - Ask the fraud desk to freeze or monitor the account, reverse what they can, and flag related accounts.
* Secure sign-in - Change online banking and email passwords, turn on 2FA for bank and email, and review recent devices/sessions.
* Watch for SIM swap - If codes stop arriving or your phone loses service suddenly, see SIM swap / stolen phone number and tell the bank.

3. Why checking/savings is different from cards

FTC guidance on scams notes that if you were tricked into transferring money yourself, bank accounts often have fewer protections than credit cards. Act fast, document every call, and ask the bank which dispute or claim process applies to ACH, Zelle-style sends, wires, or debit. For card-only incidents, use the dedicated credit card fraud first-hour guide.

4. After the first hour

* Follow FTC recovery steps for the payment method involved (What to do if you were scammed).

* Report at ReportFraud.ftc.gov.
* If Social Security numbers, driver's license data, or other personal info may be exposed, use IdentityTheft.gov.
* Check whether email or reused passwords show up in known breaches (check email data breach) and prefer a password manager over reused browser-saved passwords.
* Tell household members not to trust inbound "bank fraud" calls that demand money movement.

FAQ

What should I do first if my bank account is hacked?

Call the bank using a trusted number, stop further transfers, change passwords, and enable 2FA. Do not follow an inbound caller's "move your money" instructions.

The caller said they were fraud prevention-why hang up?

Because scammers spoof banks. FTC: get a call about fraud activity and it could be a scammer. You call the bank back on a known number.

Is this the same as credit card fraud?

No. This page is checking/savings compromise and bank-impersonation recovery. Card disputes belong on credit-card-fraud-first-hour.

Will antivirus fix unauthorized transfers?

Not by itself. The urgent work is the bank fraud desk, password/2FA lockdown, and refusing coached transfers. Defender is optional later if a device may also be infected - see Is Microsoft Defender enough?.

Where do I report it?

Your bank first, then ReportFraud.ftc.gov. Identity exposure: IdentityTheft.gov. Walkthrough: how to report a scam to the FTC.

If you still want a paid suite

First-hour bank recovery does not require paid antivirus. Microsoft Defender is a valid buy-nothing choice for many Windows households. What actually helps is calling the real bank, refusing "protect your money" transfers, and locking down passwords + 2FA. If the household later wants multi-device paid protection, use only these on-site paid links: TotalAV (paid link), Norton (paid link), Bitdefender (paid link), McAfee (paid link), Avast (paid link).

Sources

* Got a Call About Fraud Activity on Your Bank Account? It Could Be a Scammer (FTC)
* What to Do If You Were Scammed (FTC)
* ReportFraud.ftc.gov (FTC)
* IdentityTheft.gov

Also read

* What to do in the first hour of credit card fraud
* How to turn on 2FA for Gmail, Apple, and your bank
* What to do after a SIM swap or stolen phone number
* Password manager vs browser passwords
* How to check if your email is in a data breach
* How to report a scam to the FTC