

Security Emergency Response Playbook

I Think I've Been Hacked. Now What?

Security incidents are confusing on purpose.

Scammers, malware, account thieves, and fake support operations all benefit when you are rushed, scared, and clicking without a plan. This playbook gives you an order of operations so you can stop the damage, protect the accounts that matter most, and recover from something you can trust.

The Grumpy Sysadmin

Version: August 2026

How to Use This Playbook

This guide is for ordinary Windows users dealing with a suspected security incident: a hacked account, strange sign-in, malware warning, scam call, unexpected remote access, suspicious transaction, stolen session, ransomware alert, or a computer that suddenly can't be trusted.

You don't need to know exactly what happened before you start. You do need to avoid making the situation worse. Work in this order: observe, contain, protect critical accounts, investigate the scope, recover, verify, and document.

Grumpy Rule: *The first goal isn't to explain every mystery. The first goal is to stop the mystery from getting access to anything else.*

The Six Questions to Answer

- What did I actually observe?
- Which device or account may be affected?
- Is the problem still active?
- What can the affected device/account still reach?
- Which accounts or data matter most if credentials were exposed?
- What would make me trust this device or account again?

Table of Contents

- 1. First Five Minutes: Facts Before Fixes
- 2. Contain the Device or Account
- 3. Protect the Accounts That Control Everything Else
- 4. Hacked Email or Social Media Account
- 5. Microsoft, Google, or Apple Account Compromise
- 6. Password Manager and MFA Emergency
- 7. Malware, Fake Support, and Remote Access
- 8. Suspicious Financial Activity and Identity Exposure
- 9. Ransomware and Destructive Malware
- 10. Decide Whether the Computer Can Be Trusted
- 11. Rebuild and Recover in the Right Order
- 12. Tell the Right People - and No One Else
- 13. Incident Documentation and Worksheets
- 14. After the Emergency: Close the Door You Came Through
- 15. Final Verification

1. First Five Minutes: Facts Before Fixes

A security incident often begins with incomplete information. Maybe you received a login alert. Maybe a browser suddenly opened a fake virus warning. Maybe a contact says you sent a message you never sent. Maybe your bank called about a charge. Resist the urge to perform ten unrelated fixes at once.

Grumpy Rule: Random activity feels productive during a security incident. So did rearranging the deck chairs on the Titanic.

Write Down the Trigger

Initial Observation	Done
Exact message/alert or symptom	☐
Approximate time noticed	☐
Device involved	☐
Account involved	☐
Whether money or personal information may be involved	☐
Whether anyone had remote access	☐
Whether software was installed	☐
Whether files changed, disappeared, or became unreadable	☐

Take screenshots or photos when useful. Don't repeatedly interact with suspicious pop-ups or messages just to collect more evidence.

Don't Trust Contact Information Inside the Alert

If a pop-up, email, text message, or caller tells you to contact "support," don't use the number or link they provided until you independently verify it. Open the official app, use a known website, or use contact information printed on a bank card or statement.

Grumpy Rule: The person yelling "CALL THIS NUMBER NOW" doesn't get to choose the number you trust.

2. Contain the Device or Account

Containment is about reducing what the suspected compromise can still reach while you figure out what happened.

If Malware or Active Intrusion Is Suspected

1. Disconnect Ethernet.
2. Disconnect Wi-Fi.
3. Disconnect external backup drives if ransomware/destructive malware is possible.
4. Don't plug clean backup drives into the suspected machine.
5. Use a separate trusted phone, tablet, or computer for account recovery and password changes.
6. For a company-owned device, contact the organization's IT/security team and follow its process.

When should you power the computer off?

If destructive activity is continuing and you can't reliably isolate the system from the network, shutting it down may be the most practical way to stop further damage. If the system belongs to a business, is part of a legal/insurance investigation, or professional forensic help is involved, follow that incident-response guidance before altering evidence.

If the Problem Appears Account-Only

A strange sign-in doesn't automatically mean the computer itself is infected. If the incident is limited to an online account and you have a known-clean device, begin with the account recovery path while still watching for signs that the original device or browser was the source.

3. Protect the Accounts That Control Everything Else

Not all accounts have an equal blast radius. Primary email, password managers, and Apple/Google/Microsoft platform accounts can unlock or reset many other services.

Grumpy Rule: Protect the keys before you start polishing the doorknobs.

Recommended Triage Order

1. Primary email account
2. Password manager
3. Microsoft / Google / Apple main account
4. Banking and payment accounts
5. Cloud storage
6. Social media and messaging
7. Shopping accounts with stored payment information
8. Everything else

From a Trusted Device

Critical Account Recovery	Done
Change the password if the account is compromised or the password may have been exposed	☐
Use a unique password not reused elsewhere	☐
Turn on or repair MFA	☐
Sign out unknown or all other sessions where appropriate	☐
Review trusted devices	☐
Review recovery email and phone information	☐
Review connected apps / third-party access	☐
Save fresh recovery codes where the service provides them	☐

4. Hacked Email or Social Media Account

Common signs include a password change you didn't make, an unfamiliar sign-in, messages you didn't send, contacts receiving scam links from you, or being locked out of the account.

If You Can Still Sign In

1. Change the password from a trusted device.
2. Turn on MFA.
3. Sign out other devices/sessions.
4. Review recovery information.
5. Check email forwarding rules, filters, signatures, and automatic replies.
6. Review sent/deleted folders or social messages/posts for activity you did not create.
7. Review connected apps and revoke anything unfamiliar.
8. Warn contacts if the account sent scams, links, or pleas for money.

If You Can't Sign In

Use the provider's official account-recovery process from a clean device. Don't pay someone who contacts you claiming they can recover the account. If the provider offers recovery codes, trusted contacts, security keys, or identity-verification steps, follow those official procedures.

Grumpy Rule: *The person who stole your account isn't going to return it because you found a second scammer with a nicer website.*

Email Deserves Extra Attention

Email is often the recovery channel for everything else. Check forwarding rules and recovery addresses carefully. An attacker can change your password, then leave a forwarding rule behind to keep receiving password-reset messages after you think the problem is fixed.