

6. Incident Playbooks

- [6.1 How to Use These Playbooks](#)
- [6.1 Account Compromise](#)
- [6.3 Personal Data Incidents](#)
- [6.4 Device Incidents](#)

6.1 How to Use These Playbooks

When you discover a security incident:

1. **Don't panic** - Take a breath; most incidents are recoverable if you act systematically
2. **Find the right playbook** - Match your situation to one of the scenarios below
3. **Follow the steps in order** - Steps are prioritized by urgency and importance
4. **Document everything** - Keep notes on what happened, when, what you did, who you spoke to
5. **Ask for help** - If you're overwhelmed, ask a tech-savvy friend or professional

6.1 Account Compromise

Compromised Email Account

Signs your email might be compromised:

- Can't log in / password doesn't work
- Emails you didn't send in your sent folder
- New forwarding rules or filters you didn't create
- Password reset emails you didn't request
 - Even assuming the reset email is not a phishing attempt, this is not necessarily a major warning sign, but if you received a password reset email for a website or service and then lose access to that service it is possible someone used that email to reset your password
- Contacts reporting spam from you

Step 1: Regain Control if Locked Out (IMMEDIATELY)

- Go to the email provider's recovery page
- Use your recovery email or phone number to reset your password
- If recovery fails, contact provider support immediately
 - Gmail: <https://support.google.com/mail/answer/8253>
 - Yahoo/AOL: <https://vzmmemberservices.secure.force.com/?fc=aolhelpus>
 - Outlook/Hotmail: <https://account.live.com/password/reset>
- Change password to a strong, unique password (20+ characters)
- Store new password in your password manager
- Remove ALL authorized devices from account settings
- Re-add only your trusted devices

Step 2: Update Security Settings (Within Minutes)

- Verify recovery email and phone number are correct
- Update security questions (if applicable) with new answers
- Enable MFA if not already enabled
- If MFA is already enabled, remove all MFA devices and re-add only yours
- Save new recovery codes in password manager

Step 3: Damage control (Within Hours)

- Check for and remove any email forwarding rules you didn't create
- Review sent folder for emails you didn't send

- Review recently deleted emails
- Check for auto-replies or vacation responders you didn't set
- Alert contacts immediately if spam / phishing was sent from your account
- Review inbox filters and labels for suspicious rules
- Check for password reset emails from other services
 - If found, secure those accounts immediately (see relevant sections below)

Step 4: Additional Actions

- Monitor account daily for 1 week for suspicious activity
- If sensitive information was accessed, consider notifying affected parties (contacts and calendar invites often contain sensitive information)

Compromised Password Manager

This is the worst-case scenario. Act fast!

Signs your password manager is compromised:

- Can't log in with your master password
- Unauthorized devices in account settings
- Notifications of success password changes you didn't initiate
- Unfamiliar new entries or missing entries in your vault

Step 1: Regain Control (IMMEDIATELY)

- If you can still log in
 - Change master password
 - Remove ALL authorized devices
 - Re-add only your trusted devices
- If locked out and recovery is available
 - Use your password manager's account recovery process
 - Follow provider's emergency access procedures
 - Once recovered, change master password
- If locked out with no recovery
 - Create new password manager account

Step 2: Reset All Passwords In Your Vault (IMMEDIATELY - this takes time)

Assume every account in your vault is compromised. Work through tiers in order. For EACH account changed:

1. Change password to new unique password
2. Remove all authorized devices
3. Enable or verify MFA

4. Check recent activity
5. Verify security questions and recovery settings
6. Check for account-specific issues (email forwarding, profile changes, etc)

Tier 1 - Immediately

- Password manager account itself (if recovered)
- Recovery email addresses
- All other email accounts

Tier 2 - Within 1 Hour

- Banks and credit unions
- Investment accounts
- PayPal, Venmo, payment processors
- Credit card accounts

Tier 3 - Within 4 Hours

- Cloud storage (Google Drive, iCloud, OneDrive, Dropbox, etc)
- Medical portals
- Social media accounts (Facebook, Twitter, LinkedIn, etc)

Tier 4 - Within 12 Hours

- Shopping sites (Amazon, eBay, etc)
- Gaming accounts (Steam, Xbox, Discord)
- Streaming services (Netflix, Hulu, AppleTV, etc)

Tier 5 - Within 24 Hours

- Everything else

Step 3: Additional Actions

- Monitor all financial accounts daily for 1 week
- Review credit reports for unauthorized activity
- Consider placing fraud alert on credit reports
- Document which accounts were in vault when compromised
- File police report if identity theft or financial fraud occurred

Compromised Financial Account

(Bank, credit union, credit card, investment account, etc)

Signs of compromise:

- Unauthorized transactions
- Can't log in / password doesn't work
- Alerts about new devices or locations
- New accounts or cards you didn't open
- Unexpected credit inquiries

Step 1: Regain Control (IMMEDIATELY)

- Call the fraud number on the back of your card
- Ask them to:
 - Freeze the account
 - Document the compromise
 - Issue new cards
 - Enable enhanced monitoring
- Report known unauthorized transactions and explain you will call back after a full review
- If you cannot log in, reset the password using recovery options
- Once logged in, change the password to a strong, unique password
- Store new password in your password manager
- Remove ALL authorized devices from account settings
- Re-add only your trusted devices

Step 2: Update Security Settings (Within Minutes)

- Verify recovery email and phone number are correct
- Update security questions (if applicable) with new answers
- Enable MFA if not already enabled
- If MFA is already enabled, remove all MFA devices and re-add only yours
- Save new recovery codes in password manager
- Verify linked external accounts
- Review authorized card users

Step 3: Damage Control (Within Hours)

- Review all recent transactions (go back 90 days)
- Document every transaction you didn't make
- Check for, document, and correct where possible:
 - New accounts opened in your name
 - Credit applications you didn't submit
 - Changed account settings (address, email, phone)
 - New beneficiaries or authorized users
- For payment apps (Venmo, Paypal, etc) review sent messages for phishing attempts
- Call the fraud line back and report all unauthorized activity

Additional steps:

- File a police report (required for most fraud disputes)

- Place fraud alert on credit reports with all three bureaus:
 - Equifax: 888-766-0008
 - Experian: 888-397-3742
 - TransUnion: 800-680-7289
- Monitor credit reports monthly for 6 months
- Consider credit freeze if multiple accounts were affected
- Monitor affected financial accounts daily for 2 weeks

Compromised Social Media Account

(Facebook, Twitter/X, Instagram, LinkedIn, forums, etc)

Signs of compromise:

- Can't log in / password doesn't work
- Posts you didn't make
- Messages sent from your account
- New friends or followers you didn't send
- Profile information changed
- Friends reporting spam from you

Step 1: Regain Control (IMMEDIATELY)

- Use platform-specific recovery:
 - Facebook: facebook.com/hacked
 - Instagram: help.instagram.com
 - Twitter/X: help.twitter.com
 - LinkedIn: linkedin.com/help
- Reset password using recovery email or phone
- Once logged in, change the password to a strong, unique password
- Store new password in your password manager
- Remove ALL authorized devices from account settings
- Re-add only your trusted devices
- If you cannot recover your account:
 - Create new account and notify contacts
 - Ask friends to unfriend/unfollow compromised account

Step 2: Update Security Settings (Within Minutes)

- Verify recovery email and phone number are correct
- Update security questions (if applicable) with new answers
- Enable MFA if not already enabled
- If MFA is already enabled, remove all MFA devices and re-add only yours
- Save new recovery codes in password manager
- Check for connected accounts (e.g., "Sign in with Facebook" to other services)

- Revoke access to third-party apps you don't use

Step 3: Damage Control (Within Hours)

- Alert friends/contacts if spam was posted or sent
- Post a public message explaining the compromise
- Message close contacts directly
- Review and delete posts you didn't make
- Review and delete messages sent from your account
- Check friend/follower lists for accounts you didn't add
- Remove suspicious connections
- Review profile information and undo any changes
- Check privacy settings
- Review tagged photos and posts

Step 4: Additional Actions

- Monitor account daily for 1 week for new suspicious activity
- Report the compromise to the platform
- If personal information was exposed, consider notifying affected individuals

Compromised Cloud Storage Account

(Google Drive, OneDrive, iCloud, Dropbox, etc)

Signs of compromise:

- Can't log in / password doesn't work
- Files you didn't upload or share
- Sharing notifications you didn't create
- New devices accessing your files
- Unusual storage usage

Step 1: Regain Control (IMMEDIATELY)

- Reset password using recovery email or phone
- Change password to strong, unique password
- Store new password in password manager
- Remove ALL authorized devices and active sessions
- Re-add only your trusted devices

Step 2: Update Security Settings (Within Minutes)

- Verify recovery email and phone number
- Update security questions if available
- Enable or verify MFA

- Save recovery codes in password manager
- Revoke access to ALL third-party apps
- Re-authorize only apps you actively use

Step 3: Damage Control (Within Hours)

- Review all shared files and folders and remove unauthorized users
- Remove public sharing links you didn't create
- Review recently accessed files for sensitive data exposure
- Check for files you didn't upload and delete them
 - If you must open them to verify, download and perform a virus scan first!
- Review deleted files folder for files you didn't delete
- Check activity log for unauthorized downloads
- If sensitive files were accessed:
 - Note which files (financial docs, passwords, personal info)
 - Determine what actions to take based on exposure (change passwords, notify affected parties)

Step 4: Additional Actions

- Download audit log if available (Google and Microsoft offer this, but availability varies by account type and region)
- Monitor account daily for 1 week
- If sensitive data was exposed, take appropriate action:
 - Financial documents - monitor accounts, consider credit freeze
 - Passwords - change affected passwords
 - Personal identification - consider identity theft protection
- Review all devices with cloud app installed

Compromised Shopping Account

(Amazon, eBay, Etsy, etc)

Signs of compromise:

- Unauthorized orders
- Can't log in / password doesn't work
- New payment methods you didn't add
- Changed shipping address
- Gift cards purchased without your knowledge

Step 1: Regain Control (IMMEDIATELY)

- Reset password using recovery email or phone
- Change password to strong, unique password

- Store new password in password manager
- Remove ALL authorized devices
- Re-add only your trusted devices

Step 2: Update Security Settings (Within Minutes)

- Verify recovery email and phone number
- Update security questions if available
- Enable or verify two-step verification
- Save recovery codes in password manager

Step 3: Damage Control (Within Hours)

- Review ALL orders (including cancelled orders)
- Cancel any unauthorized pending orders
- Contact seller to cancel shipped unauthorized orders
- Report unauthorized orders to platform
- Review and remove unauthorized payment methods
- Check for unauthorized gift card purchases or balances
- Verify shipping addresses and remove unauthorized addresses
- Review account balance or store credit for unauthorized changes
- Check wish lists and shopping lists for changes
- Review seller account for unauthorized listings (if you have one)

Step 4: Additional Actions

- Dispute unauthorized charges with credit card company
- Monitor payment methods for unauthorized charges
- File police report if fraud amount is significant
- Contact platform customer service to document compromise

If Any Other Account is Compromised

Signs of compromise:

- Unauthorized transactions
- Can't log in / password doesn't work
- Alerts about new devices or locations
- Alerts about personal information updates
- Account information changes you didn't make
- Notifications about password changes you didn't initiate

Step 1: Regain Control (IMMEDIATELY)

- Use the site's password recovery to reset password

- Change password to strong, unique password
- Store new password in password manager
- Remove ALL authorized devices and active sessions
- Re-add only your trusted devices

Step 2: Update Security Settings (Within Minutes)

- Verify recovery email and phone number
- Update security questions if available
- Enable or verify two-step verification
- Save recovery codes in password manager
- Revoke access to all third-party apps (if applicable)
- Re-authorize only apps you actively use (if applicable)

Step 3: Damage Control (Within Hours)

- Review recent account activity for unauthorized actions:
 - Purchases or transactions
 - Posts, messages, or comments
 - Profile or account information changes
 - Privacy setting changes
 - Friend/connection requests sent
- Undo unauthorized changes
- Delete unauthorized content
- Alert contacts if spam/phishing was sent from your account
- Review any sensitive data that may have been accessed
- Check for linked accounts ("Sign in with..." connections)

Step 4: Additional Actions

- Report the compromise to the service provider
- Monitor account daily for 1 week for suspicious activity
- Review connected services, secure any that use this account for login
- If financial loss occurred, file police report (also review Compromised Financial Account playbook)
- Document the incident for your records
- Consider whether any legal/regulatory notifications are required

6.3 Personal Data Incidents

Identity Theft

Signs of identity theft:

- Accounts or loans you didn't open appearing on credit report
- Calls or mail from debt collectors about debts you don't owe
- IRS notification of multiple tax returns filed in your name
- Medical bills for services you didn't receive
- Mail or email about accounts you didn't create
- Missing mail or bills
- Denied credit unexpectedly
- Unauthorized withdrawals from bank accounts

Step 1: Contain the Damage (IMMEDIATELY)

- Place fraud alert on credit reports (call ONE bureau, they notify the others)
 - Equifax: 1-888-766-0008
 - Experian: 1-888-397-3742
 - TransUnion: 1-800-680-7289
 - Fraud alert lasts 1 year, requires creditors to verify your identity
- File FTC Identity Theft Affidavit
 - Go to <https://www.identitytheft.gov>
 - Click “get started” – you’ll be guided through a series of questions, have ready:
 - Personal information (name, address, SSN, DOB)
 - Details about the identity theft (what happened, when discovered)
 - Information about fraudulent accounts (account numbers, companies, amounts)
 - Any evidence you have (emails, bills, credit reports)
 - Review and submit
 - Download and print multiple copies (keep one safe as a backup)
 - This will be used for police reports and to legally contest any action taken against you on account of the identity theft
- Get your credit reports
 - Request from all three bureaus immediately
 - Go to annualcreditreport.com (or one of your financial accounts)
 - Or request from the bureau you called for fraud alert
 - Review for accounts and inquiries you don't recognize
- File police report
 - Contact local police department

- Bring FTC Identity Theft Report
- Request a copy of the police report
- You'll need this for disputing fraudulent accounts

Step 2: Close Fraudulent Accounts (Within 24-48 Hours)

- For each fraudulent account found
 - Contact the fraud department of the company
 - Explain you're an identity theft victim
 - Provide your Identity Theft Report
 - Request the account be closed
 - Request fraudulent charges be removed
 - Ask for written confirmation
- For fraudulent credit cards or loans
 - Request investigation
 - Provide police report and FTC Identity Theft Report
 - Follow company's fraud dispute process

Step 3: Secure Your Legitimate Accounts (Within 48 Hours)

- Change passwords on all financial accounts
- Enable MFA on all accounts
- Review recent activity on all accounts
- Close accounts that were compromised

Step 4: Additional Actions

- Consider a credit freeze
 - More protective than fraud alert
 - Blocks new accounts from being opened
 - Free at all three bureaus
 - You can temporarily lift when applying for credit
- Ongoing monitoring (6-12 months)
 - Review credit reports every 3 months
 - Monitor bank and credit card statements weekly
 - Watch for new collection calls or letters
 - Keep detailed records of all actions taken
 - Follow up on dispute resolutions
- If tax fraud occurred
 - Contact IRS Identity Protection Specialized Unit: 1-800-908-4490
 - File Form 14039 (Identity Theft Affidavit)
- If medical identity theft
 - Contact your health insurance company
 - Request copies of medical records to review
 - Dispute incorrect information with providers

Lost or Stolen Wallet or Purse

What's at risk:

- Credit/debit cards
- Driver's license or ID
- Social Security card (if you carry it - you shouldn't)
- Insurance cards
- Other identification documents

Step 1: Immediate Containment (IMMEDIATELY)

- Cancel all cards:
 - Call fraud departments for all credit and debit cards in wallet
 - Request new cards with new numbers
 - Note the date/time you report each card
- Place fraud alert on credit reports (if ID was in wallet):
 - Call one credit bureau (see Identity Theft section above)
- Check accounts for unauthorized charges
 - Review all recent transactions
 - Report unauthorized charges immediately

Step 2: Replace Documents (Within 24-48 Hours)

- Driver's license/ID: Contact your state DMV to report and replace
- Social Security card: Contact SSA (don't carry SSN card in future)
- Insurance cards: Contact providers for replacements
- Other cards: Library, gym, membership cards - contact to cancel/replace

Step 3: Monitoring

- Monitor all financial accounts daily for 2 weeks
- Review credit reports monthly for 3 months
- Watch for fraudulent account openings
- Save all documentation of reported theft

Sent Money to a Scammer

Common scenarios:

- Wire transfer to scammer
- Gift cards purchased and codes given
- Cryptocurrency sent
- Payment app (Venmo, PayPal, Zelle) transfer

- Credit card payment to fake website

Step 1: Try to Stop the Payment (IMMEDIATELY)

Document everything:

- How scammer contacted you
- What they claimed
- Timeline of events
- Amount lost
- All communications

For wire transfers:

- Contact your bank (fraud department)
- Request wire transfer recall
- Most effective within 24 hours
- Provide details: amount, date, receiving bank

For credit/debit card charges:

- Contact card issuer fraud department
- Request transaction be blocked or reversed
- File dispute/chargeback
- Request new card number

For payment apps (Venmo, PayPal, Zelle):

- Contact app support
- Report unauthorized transaction
- Request cancellation/reversal
- Note: Zelle transfers are usually instant and irreversible

For gift cards:

- Contact gift card company (number on card)
- Provide card numbers and receipt
- Request freeze/cancellation
- Success rate is low but worth trying immediately

For cryptocurrency:

- Generally irreversible
- Report to exchange if applicable
- Document transaction details

Step 2: Report the Fraud (Within 24 Hours)

- File FTC report <https://reportfraud.ftc.gov>
 - Creates official record
 - Helps track scam patterns
- File police report:
 - Needed for most theft claims
 - Helps with bank/credit card disputes
 - Bring all documentation

Step 3: Protect Against Further Loss (Within 24 Hours)

- Place fraud alert on credit reports if you gave personal information
- Monitor accounts daily for additional unauthorized charges

Gave Out Personal Information

Follow this playbook if you gave out high risk, personal information via email or to a caller in a conversation you did not initiate.

High Risk Personal Information:

- Passwords or PINs
- Bank account numbers including any credit card data (number, CVV)
- Social Security number or date of birth
- Any answer you use in a security question

Step 1: Immediate Actions (Based on What You Shared)

- Passwords or PINs: Follow the appropriate account compromise playbook above
- Bank account numbers or any credit card data: Contact fraud department on back of card, or call banking institution to stop any unauthorized pending transactions and have new card or account issued
- Social security number or date of birth: Monitor credit report for any queries or new accounts and follow the Identity Theft playbook if anything shows up; consider a credit freeze regardless by calling one of the three credit bureaus (see Identity Theft playbook)
- Any answer you use in a security question: Change the security question in all sites where it was used

Step 2: Monitor accounts daily for 2 weeks

If you see anything unusual, follow the appropriate playbook

Clicked a Phishing Link or Opened Suspicious Attachment

Your next steps are based on what you did, based on risk.

Low Risk

- If you ONLY clicked the link and did not enter any information or download any files, close the browser and clear your browser cache.
- If you downloaded any files, and especially if you opened the file, delete the files and run a full virus scan (see Malware or Virus infection playbook below).

High Risk

- If you entered a password, follow the playbook for the appropriate type of compromised account above
- If you entered any other personal information, follow the playbook for Gave out Personal Information based on the type of data you entered

Received Notice of Data Breach

This is when a company notifies you your data was exposed.

Common notification sources:

- Email from company
- Letter in mail
- News article about breach
- Notification from HavelBeenPwned.com

Step 1: Verify Notification is Legitimate (IMMEDIATELY)

Beware of phishing! Don't click links in breach notification emails, instead, verify using one of the following:

- Go directly to company's website (type URL yourself)
- Look for official breach notification page
- Verify through news sources
- Call company using official phone number

Step 2: Understand What Was Exposed (Within 24 Hours)

Read the notification carefully:

- What specific data was compromised?
- When did the breach occur?
- What is the company doing?
- What services are they offering (credit monitoring, etc.)?

Step 3: Take Action Based on Data Exposed (Within 48 Hours)

If passwords were exposed: Follow the playbook for the type of compromised account above

If email address only: Not much you can do here, just understand you will likely start receiving a lot of spam and potentially phishing attempts, so be extra vigilant in the coming weeks and months.

If Social Security number or financial data:

- Place fraud alert on credit reports (see Identity Theft section)
- Consider a credit freeze
- Monitor credit reports monthly for 12 months
- Enroll in credit monitoring if offered (only California requires this be offered at the time of this writing, but many companies will offer anyway in a show of goodwill)
- Review financial statements going back to the date of the breach (US law requires you are notified, but the timeline for notification is somewhat of a gray area)

If medical information:

- Watch for fraudulent medical bills
- Contact health insurance if fraudulent claims appear
- Monitor credit reports monthly for 12 months

Step 4: Accept Company's Offer (If Valuable)

Many companies offer:

- Free credit monitoring (usually 1-2 years)
- Identity theft protection
- Credit freeze assistance

Evaluate the offer:

- Is credit monitoring included? (worth it)
- How long is coverage? (longer is better)
- Do you have to pay anything? (should be free)
- Read terms carefully before accepting

Step 5: Additional Actions

Document the breach:

- Save notification letter/email
- Screenshot relevant information
- Note what data was exposed

Monitor relevant accounts based on exposure and consider legal action if negligence was involved.

Ongoing monitoring:

- Check credit reports every 3 months for 1 year
- Monitor financial accounts for suspicious activity
- Watch for targeted phishing using your data
- Stay alert for identity theft signs

SIM Swap Attack

Signs of SIM swap:

- Phone suddenly has no service/signal
- Can't make calls or send texts (even after reboot)
- Notifications of password resets you didn't request
- Unusual account activity alerts stop arriving
- Carrier confirms your number was ported to new SIM

Step 1: Regain Control of Phone Number (IMMEDIATELY)

Contact your mobile carrier:

- Call from a different phone or use online chat
- Verify account activity and report unauthorized SIM swap if the agent determined your SIM card was ported
- Verify your identity (have account PIN ready)
- Request your number be restored to your SIM
- Ask them to lock your account with additional verification

Step 2: Secure Accounts That Use Phone for 2FA (Within 1 Hour)

Attackers may have targeted accounts using SMS for two-factor authentication. Verify recent logins to new devices in the following priority:

- Email accounts (especially recovery emails)
- Financial accounts (banks, investment, PayPal)
- Cryptocurrency exchanges
- Social media accounts
- Any other account using SMS for authentication

If there was an unauthorized login, for each account:

- Remove any new authorized devices that aren't yours
- Change password (from trusted device)
- Remove SMS as 2FA if possible and replace with authenticator app or hardware key
- Check recent activity for and perform damage control (see relevant playbook in Account Compromise above)
- Enable login alerts if not already enabled

6.4 Device Incidents

Ransomware Infection

Signs of ransomware

- Files suddenly encrypted with unfamiliar extensions (.locked, .cerber, etc.)
- Ransom note demanding payment for decryption
- Desktop wallpaper changed to ransom message
- Unable to open files (photos, documents, etc.)
- Pop-up demanding Bitcoin payment

Step 1: Isolate the Infection (IMMEDIATELY)

- Disconnect from network
 - Do NOT shut down the computer (some ransomware encrypts more on reboot)
- Unplug ethernet cable
- Turn off WiFi
- Disconnect external and network drives
 - Unplug any external hard drives, thumb drives, etc
 - Log out of any cloud accounts you have connected on your computer
- Identify the ransomware variant
 - Take a photo of ransom note with phone
 - Note the file extensions (.locky, .cerber, etc.)
 - Visit ID Ransomware <https://id-ransomware.malwarehunterteam.com> to identify variant

Step 2: Assess and Report (Within 1 Hour)

Do NOT pay the ransom, there is no guarantee of file recovery and this funds criminal activity

- Report to law enforcement (FBI) <https://ic3.gov>
- Check if free decryption is available from ID Ransomware
- Check what protections and warranties your antivirus solution offers
- Additional potentially free options:
 - <https://nomoreransom.org>
 - <https://kaspersky.com>

Step 3: Recovery Options

If decryption is available from your assessment, follow the instructions. This differs by type of ransomware and who is providing instruction, so I cannot be more specific than that.

If no decryption is available AND you have backups then performing a clean reinstall of your operating system is the way to go. Again, I cannot be more specific as there are too many variables. If you aren't sure how to do this, ask a technical friend or visit somewhere that services computers (Microcenter, Best Buy, Apple Store, etc).

If no decryption is available and you DON'T have backups, I'm sorry, you're pretty screwed. From a clean computer, go through all your accounts and remove that computer as an authorized device. Under no circumstances should you boot this computer and connect to anything until it is clean. Keep an eye on the decryption assistance sites above, there may be something in the future that can help, or seek assistance from a professional service.

Malware or Virus Infection (Not Ransomware)

Signs of malware infection:

- Computer running extremely slowly
- Unexpected pop-ups or ads
- Browser homepage changed without permission
- Programs opening automatically
- Antivirus disabled or won't update
- Strange network activity
- New toolbars in browser
- Files disappearing or appearing
- Excessive hard drive activity when idle

Step 1: Isolate The Infection (IMMEDIATELY)

- Disconnect from internet (unplug ethernet, disable WiFi), and log out of cloud accounts

Step 2: Scan and Remove (Within 1 Hour)

- Run a full scan using your installed antivirus software
- If this fixes the issue, reconnect to the internet and continue to step 3
 - Note that removing the virus will not restore settings which the virus changed, so you may need to follow steps 1 through 3 multiple times until the malware is removed and settings "stick"
- If this does not fix the issue, boot the computer into safe mode
 - For Windows: Restart, hold Shift, select Troubleshoot > Advanced > Startup Settings > Safe Mode
 - For Mac: Restart, hold Shift key

- Run full antivirus scan with your installed antivirus
- If you do not have an antivirus and are running Windows, use Windows Defender Offline Scan
 - Settings > search for “virus and threat protection” > click “scan options” > choose “Microsoft Defender Anti-Virus (offline scan)” > click “Scan now”
- If you do not have an antivirus and are using a Mac, you can look for a free scanner from Sophos, Kaspersky, Malwarebytes, or BitDefender
 - The options to run these vary, so follow the instructions
- If this fixes the issue, reconnect your cloud accounts and continue to step 3
- If this does not fix the issue it is probably time to seek help from a technical friend or professional services

Step 3: Check for Damage (Within 24 Hours)

- Review your installed software and remove anything you didn’t install (Windows will show you the date installed so you can use that as a guide for when the malware behavior started)
 - Start > add or remove programs
- Review browser extensions and remove anything suspicious
 - Browser settings > Extensions (varies by browser)
- Check browser homepage and search engine settings, restore as needed
 - Browser settings > Homepage (varies by browser)
 - Browser settings > Search engine (varies by browser)
- Check startup programs for unfamiliar entries
 - Windows: Settings > Apps > Startup
 - Mac: System settings > General > Login Items & Extensions

Step 4: Additional Actions

- Update operating system and all software
- Determine how infection occurred:
 - Downloaded software from untrusted source?
 - Opened email attachment?
 - Clicked suspicious link?
- Monitor accounts for any suspicious activity for a couple weeks

If infection cannot be cleaned, contact your antivirus provider. Even if you don’t pay for the service they may still offer help.

The worst-case scenario, make sure your backups are working and perform a clean reinstall of your operating system. If unsure how to do this, talk to a technical friend or seek professional services.

Gave Remote Access to Your Computer

Common scenarios:

- Tech support scammer asked you to install remote access software
- Downloaded and ran software that gave attacker control
- Allowed access via TeamViewer, AnyDesk, LogMeIn, etc.

Step 1: Cut Off Access (IMMEDIATELY)

- Disconnect from internet (unplug ethernet cable or turn off WiFi) to stop access
- Close remote access software, force close if necessary
 - Windows: Ctrl+Alt+Delete > Task Manager > End suspicious processes
 - Mac: Command+Option+Esc > Force Quit suspicious apps
- Close any software they installed or opened
- Uninstall any software they installed, booting into safe mode if necessary (safe mode prevents most malware from running)
 - For Windows: Restart, hold Shift, select Troubleshoot > Advanced > Startup Settings > Safe Mode
 - For Mac: Restart, hold Shift key
- Uninstall remote access software:
 - Windows: Settings > Apps > Find TeamViewer/AnyDesk/etc. > Uninstall
 - Mac: Drag application to Trash, empty Trash

Step 2: Scan for Malware (Within 30 minutes)

- See Malware or Virus Infection playbook above
- If you see anything that looks like it may be encrypting your files refer to Ransomware Infection playbook

Step 3: Additional Actions

- Consider what the attacker accessed
- Follow the appropriate playbook if any sensitive information was accessed
- Monitor accounts daily for a week

What To Do If Your Phone or Computer Is Lost or Stolen

Act quickly, the sooner you respond, the better your chances of recovery or protecting your data.

Step 1: Protect Your Data (IMMEDIATELY)

Use Find My Device (see Mobile Device Hardening or Physical Security section) to:

- Locate your device
- Play a sound (if nearby)
- Lock it remotely with a message to call you at another number

Suspend services and force logouts:

If you had an authenticator app on your phone, you may lose MFA access, so you may need to use another device where the authenticator app is install or the recovery codes form your password manager.

- Call your carrier (for phones) to suspend service (prevents calls and data charges)
- Disable payment methods on device
 - Apple Pay: iCloud > Devices > remove the lost device from the list
 - Google Pay: pay.google.com
 - Samsung Pay: <https://v3.account.samsung.com/dashboard/> > Devices
- Force active device logout for all accounts (prevents someone who gains access from accessing any of your data)

Step 2: Erase and File Reports (Within 12 Hours)

If stolen or otherwise not recoverable:

- Erase it remotely (see Mobile Device Hardening or Physical Security section)
- File a police report (needed for insurance claims)
- File insurance claim (if insured against theft) with the insurer (your mobile carrier, Apple, etc)

Step 3: Recovery

If device is recovered, before using:

- Inspect for physical tampering (opened, different SIM)
- Check for new apps you didn't install
- Review recently accessed files and folders
- Check settings for changes:
 - New accounts logged in
 - Developer options enabled (Android)
 - Unknown device profiles (iPhone)
 - New email forwarding rules
 - VPN or proxy configurations
 - Accessibility permissions changes

If suspicious changes found, factory reset the device and proceed as if setting up a new device.