AN IDENTITY THEFT RESOURCE CENTER

Resource Guide

When Your Phone or Computer Is **Hacked**

ITRC | IDENTITY THEFT RESOURCE CENTER

Contents

Introduction

Scammers and identity thieves (or "bad actors") are increasingly trying to get access to your devices. So many of us carry our devices everywhere that they've become an almost invisible extension of ourselves. You may not think about the fact that your phone, tablet or laptop is a gateway to your entire digital identity. Bad actors know this, which is why they target them as the ultimate launchpad for compromise. They access devices to steal money out of accounts, steal identity information to commit identity theft, or use your device to access more people and obtain their information.

The Identity Theft Resource Center (ITRC) created this guide because of the very real threat of identity compromise, identity theft and identity misuse due to devices being accessed without their owners' permission. Finding out your personal computer or smartphone has been hacked can be overwhelming and frightening. This guide is meant to give you a clear picture of how bad actors access your devices and basic information about how to detect them, what might happen once your device is accessed, how to remove the threat and how to protect your device.

How Bad Actors Steal Your Information

Bad actors primarily use four methods to get access to your accounts and devices: tricking you into giving them information through social engineering, forcing their way in using malicious software, exploiting systems and intercepting data.

PHISHING THROUGH SOCIAL ENGINEERING

Cybercriminals often impersonate a trusted entity (like a bank, tech company or government agency) to get you to share your sensitive information.

Phishing

You get an email, text message or pop-up about an "urgent problem" or letting you know you're eligible for or have won a "prize". You click the link in the message, which takes you to a website that is a near-exact copy of a legitimate login page for your bank, a retailer or other well-known company. The URL might look very similar (e.g., walmart-prizes.com instead of walmart.com). The site will ask you to type in your username and password (or credit card number, driver's license or other personal information), which is sent to a bad actor.

Vishing *(Video Phishing)*

You get a call from a spoofed phone number that looks like a legitimate company (like Apple, Microsoft or your bank). They create a high-pressure scenario ("There's been a fraudulent transaction on your account!") and convince you to provide your credit card number or login details over the phone, or ask you to install "security software" (which is actually malware) or remote access software on your device to help address the issue.

Smishing *(SMS Phishing)*

You get a text message that often includes a sense of urgency ("Your package delivery failed. Click here within 24 hours to update your address"). When you click the link, it either takes you to a phishing website or directly installs malware onto your phone.

MALWARE, VIRUSES AND SPYWARE

This software is designed to compromise your device and steal your information.

Malware, viruses and spyware can be installed when you, or someone who has access to your device, downloads an application, clicks a malicious link or attachment, or visits a compromised website. For example, you might download a free game that secretly installs a virus or spyware.

Three common types of malicious software are:

1 ***Keyloggers*** *(Type of Spyware)*

Once installed, this malicious program runs silently in the background of your computer or phone and records every single keypress you make—passwords, account numbers, emails and private messages. It periodically bundles this data and sends it back to a bad actor.

2 ***Remote Access Trojans*** *(RATs)*

This type of malware allows a bad actor to control your device remotely, including:

- Viewing your screen in real-time.
- Turning on your webcam or microphone.
- Accessing all your files, stored passwords and browsing history.
- Installing or uninstalling programs.

3 ***Information Stealers***

Malware that specifically searches your hard drive for specific information like financial data, cryptocurrency wallets, or stored login files and uploads them to a bad actor.

EXPLOITING SYSTEMS THROUGH ACCOUNT TAKEOVER AND SIM SWAP

These methods bypass the need to access your device directly.

Account Takeover *(ATO)*

ATO occurs when a bad actor gains control of one of your existing, legitimate accounts. They may have obtained your login details through phishing scams or an easy-to-crack or compromised password. ATO involving a cloud account like your Apple or Google ID, which is linked to your device's operating system, can give them control over your physical devices.

The bad actor gains the ability to:

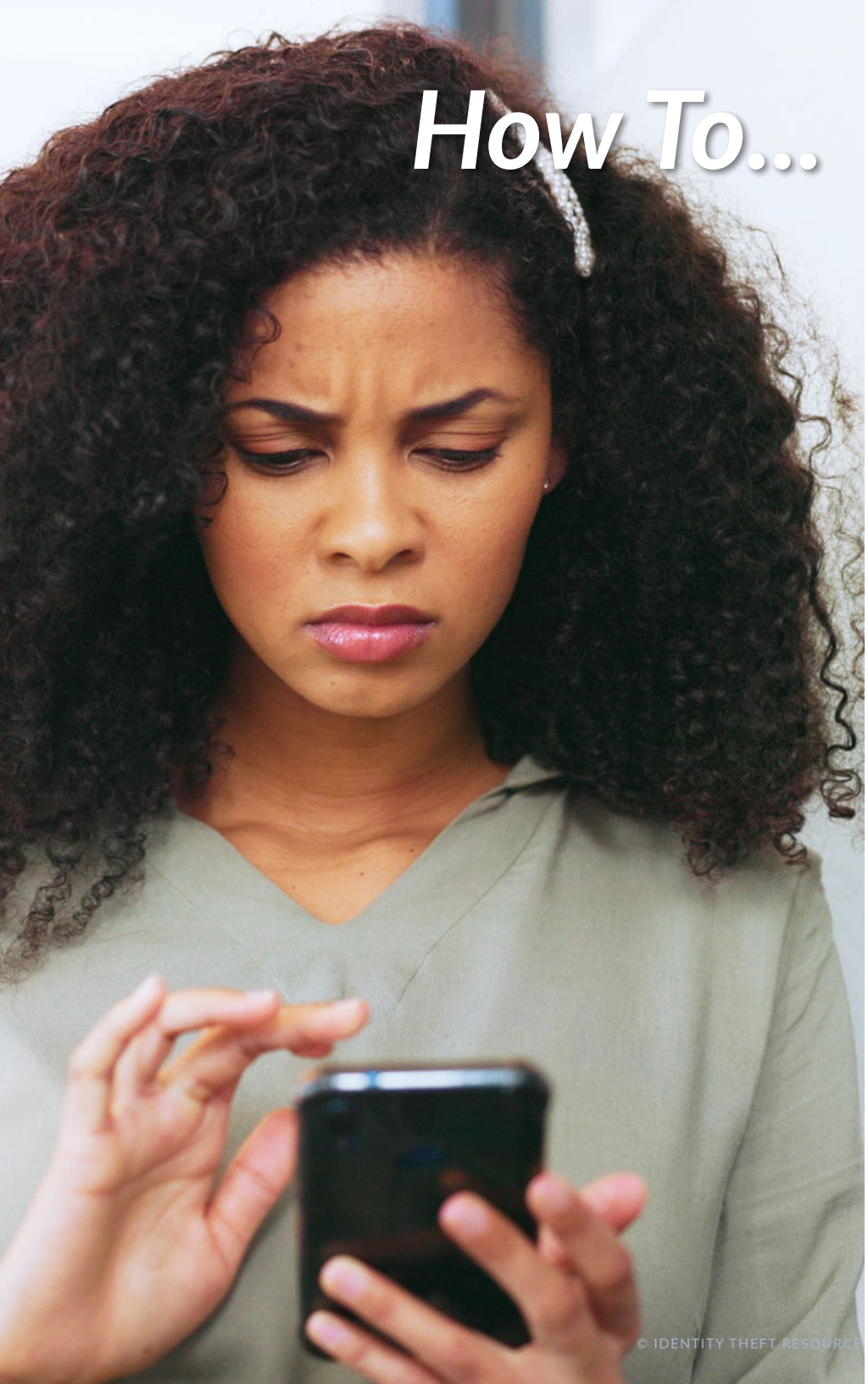
- Access your phone or computer as if they were you.
- Remotely lock the device.
- View data backups stored in the cloud, which include private messages, photos and app data.
- Reset passwords for other linked services, effectively locking you out of your digital accounts.

SIM Swap

In a SIM Swap, the bad actor contacts your mobile phone carrier (e.g., T-Mobile, Verizon) and pretends to be you, claiming your phone was lost or damaged and they need to activate your number on a new SIM card. If the carrier's employee goes along with it, the bad actor's new SIM card is activated, and your actual phone loses all service. The scammer now receives all your text messages and calls. If you use text messages for one-time passwords (OTPs) or Multi-Factor Authentication (MFA) codes, the bad actor will intercept these codes and use them to log into and take over your accounts.

DATA INTERCEPTION THROUGH UNSECURED NETWORKS

Bad actors will use unsecured connections, like public Wi-Fi or a spoofed Wi-Fi network set up by the bad actor themselves, to access your device and monitor your activity. They can steal any credentials you enter, like payment card numbers or usernames and passwords, and spread malware through pop-ups or exploit device vulnerabilities.



How To...

Detect A Hack Verse A Glitch

When your device starts acting suspiciously, it's natural to think that you've been hacked. Some activity that seems suspicious may actually have simple causes.

Slow Performance

HACK

The device is slow, even after restarting, because malware or spyware is running constantly in the background.

GLITCH

Too many open programs or tabs, low hard drive or storage space, outdated operating system, or an old battery.

Battery Draining Fast

HACK

A spyware app is secretly active, constantly monitoring and transmitting data to the bad actor.

GLITCH

The battery is old, or legitimate apps (like streaming video or navigation) are running in the background.

New Apps or Programs

HACK

You see an app you didn't download, and its name is often generic or misspelled (e.g., "Settings Pro").

GLITCH

You forgot you downloaded it, or the app was installed as part of an update for another legitimate program.

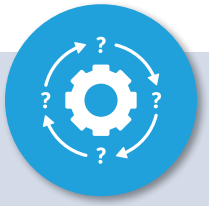
Weird Pop-Ups or Ads

HACK

Pop-ups appear aggressively outside your web browser, suggesting malware is installed.

GLITCH

They only appear while using specific, legitimate websites (which might just have bad advertising).



Unexplained Activity

HACK

The mouse moves or files are accessed when you're away from the keyboard, showing the bad actor has remote access.

GLITCH

A legitimate cloud sync service (like Dropbox or OneDrive) is running.

Account Lockouts

HACK

You receive a notification that your password or recovery details were changed from a location you don't recognize, and you can no longer log in.

GLITCH

You forgot your password, or you entered it incorrectly too many times.

Strange Dot or Light

HACK

An indicator light at the top of your phone stays on even though no microphone, camera, or app is being used, and the battery is fully charged.

GLITCH

You are actively using an app, or an app you opened is actively using, your microphone or camera, or your battery is low or dead.

SIGNS OF A POTENTIAL HACK

If you experience any of the following, the problem is likely due to a bad actor and not a simple glitch:

Unauthorized Account Changes

Your email address, phone number, or password on a finantcial account (or your Apple ID or Google Account) was changed, and you did not do it. This can happen because your device was hacked or because a bad actor was able to access your online account another way.

Remote Control

You witness files opening, settings changing or the cursor moving on its own without your input.

Suspicious Messages or Calls Sent to Contacts

Your friends or family tell you they received strange messages or links from your phone or email that you never sent. This can happen because your device was hacked or because a bad actor was able to access your account another way.

What Can Be Accessed By A Bad Actor

If a bad actor compromises your phone or computer, they are looking for easy access to accounts or personally identifiable information (PII) that can be used to commit identity theft. They can get this information using malware or by accessing apps, stored data files or pictures.

They are looking for:

- Passwords or Logins
- Credit Card or Bank Details
- Social Security Number (SSN)
- Documents and Photos (*Driver's License*, *Medical Records*, *Utility Bills*, *Tax Documents*)
- Text Messages or Emails
- Call History
- GPS Location
- Camera or Microphone
- Logged-In Applications
- Access to Logged-In Applications or Websites

The biggest vulnerability on both phones and computers is apps or websites that are actively logged in and don't require a password or biometrics to open. The most common apps or websites that stay logged in are social media, email and cloud storage.

For a bad actor, your actively logged-in device is a goldmine. They can post on social media, send malicious links via your email or messaging apps, or change security settings, passwords, and other account information without needing to take any extra steps.

What to Do When Hacked

Given the complexity of malware, antivirus/spyware/malware software may not be able to detect all forms. When you suspect someone is accessing your device, your priority is to cut off further access.

1 Disconnect and Change Passwords

Disconnect Immediately

This stops the malware from communicating with malicious servers.

Computer – Unplug the Ethernet cable or immediately turn off the Wi-Fi.

Phone – Turn off Wi-Fi and mobile data (an easy way to do this is to put the phone in "airplane mode").

Change Passwords and Enable MFA

+ Use a different, trusted device (e.g., a friend or family member's device, a separate computer) that you know is not compromised.
+ Change the passwords for any accounts you think may have been compromised.
+ If you haven't already, enable MFA, preferably using an authenticator app

2 Do a Simply Security Check

Review Logged-In Sessions

Go into the security settings of your accounts and review the list of devices logged in. Log out or revoke access for any device you don't recognize.

Disable Remote Access

Computer – Check the System Tray (Windows) or Menu Bar (Mac) for any unfamiliar icons related to remote desktop software (e.g., TeamViewer, AnyDesk) and uninstall them immediately.

Phone – Review permissions from the Privacy dashboard (Android) or use the Safety Check option (iPhone). Revoke access for any unfamiliar app (and review access for apps you know). Uninstall any apps that allow remote access to your phone.

3 *Information Stealers*

Because advanced malware can hide from and even disable antivirus software, the only way to guarantee the removal of an infection is a complete reset.

Computer – Perform a complete re-installation of the operating system.

Phone – Use the built-in option in the device settings on your Android phone or iPhone to perform a factory reset.

Restoring From A Backup

If you do not want to wipe your device completely, you can restore the information and apps on your device from a backup. If malware on your device was included, you will re-infect your device. To avoid this, you must be highly cautious about what data you bring back. When in doubt, consult a reputable professional.

Low-Risk Backups

Contacts, Calendar, Notes, Documents, Photos and Videos – When restoring documents, make sure they have been scanned by antivirus software. Do not restore application folders.

Moderate-Risk Backups

Application Data – It is safer to re-download apps and log in manually.

High-Risk Backups

System or Full-Image Backups *(includes operating system files and app data),* ***Executable Programs and Application Folders*** – These are most likely where malware and its hidden files are stored.

ON A COMPUTER

Windows or MacOS

1. Do not use the built-in system reset.
2. Back up personal, low-risk data and files to an external hard drive, USB flash drive or a cloud location. Avoid copying application data folders like AppData (Windows), Library (macOS) or Program Files. Scan your backup for malware.
3. Reinstall the operating system (OS) by choosing "Custom" (Windows) or manually transferring files (macOS).

ON A PHONE

Android or iOS

1. Factory-reset your Android phone or iPhone. When it restarts and prompts you to restore data from a backup (Google or iCloud), select "Set Up as New Device" or "Don't Copy Data."
2. Manually sign in to secured cloud services (Apple or Google). Sync only your contacts, calendar, notes and photos.
3. Re-download necessary apps. Go to the App Store or Google Play Store and manually re-download your necessary apps. Do not use an "App Restore" list.

Protect Your Information

Protecting your information involves creating layers of defense so that if one fails, others are there to help shore up your defenses. Physically securing your device, leveraging built-in device features, protecting your apps, and staying aware of common and new ways bad actors will try to exploit you make it very hard for a bad actor to access your device and personal information.

1 Control Physical Access to Your Device and Apps

- Use biometric authentication to unlock your device.
- Use a strong passcode for your device. If biometrics fail, a strong, unique and long password is the final barrier.

2 Use Built-In Security Features

- Automatic updates allow major systems, browsers and apps to push security patches automatically to close known security vulnerabilities.
- Using your browser settings, choose safe browsing options, which check websites against a list of known malicious, phishing, and malware sites and warn you or block access.
    - Look for the lock icon and https:// in the website address bar. The 'S' means the connection is encrypted. This isn't foolproof, as bad actors can create their own encrypted sites to capture your information.

3 Protect Access to Your Accounts Through Your Apps/Browser

- Use passkeys, biometric authentication, or strong, unique and long passwords combined with MFA for your apps or accounts.
- Log out of apps or websites, when possible, rather than leaving them logged in.

4 *Be Cautious About Unexpected Communications That Contain Links or Attachments*

- This is especially crucial if the communication threatens you, makes claimers that seem too good to be true or insists that you act immediately and not tell anyone.
- Go to the sender independently, through verified sources. Do not click on the link, call the number, respond directly or download the attachment in the message.

5 *Use Public WiFi Securely, If At All*

- A VPN is still the primary security tool for public Wi-Fi. It creates an encrypted "tunnel" between your device and a server operated by the VPN provider.

6 *Purchase Anti-Virus, Anti-Malware, Anti-Spyware Software If It Makes You More Comfortable*

- Newer Apple and Windows devices typically have a built-in software solution that works well to protect against malicious software, as long as you keep them up to date.
- Open platforms, like Android, create a higher risk because you can bypass traditional security settings. A reputable security app or software can provide an additional layer of scanning and protection.