



# Device Theft & Physical Access

## *Recovering from Lost or Stolen Devices*

Device theft or physical access incidents occur when a phone, laptop, tablet, or other digital device is lost, stolen, or accessed without your permission, creating risk that stored data, saved logins, or linked accounts may be exposed.

This includes:

- Stolen or lost smartphones
- Stolen laptops or tablets
- Devices taken from cars, homes, or workplaces
- Unauthorized physical access by someone you know
- Borrowed devices that were not returned or were accessed improperly

You did nothing wrong, but speed matters.

If the theft involved violence, stalking, or immediate danger, call 911.

## Device Theft – Do This First

### Prioritize Personal Safety

- Do not attempt to recover the device yourself, even if tracking shows its location.
- Do not confront a suspected thief
- If theft just occurred or you feel unsafe, call 911
- Your safety is more important than any device.

### Secure Accounts Immediately (From Another Device)

Email is the master key to most accounts.

Using a trusted device:

- Change passwords for:
  - Email accounts
  - Apple ID / Google account
  - Banking and payment apps
  - Social media and messaging apps
- Log out of all active sessions
- Update recovery email and phone numbers
- If passwords were reused, change them everywhere.

### Locate, Lock, or Wipe the Device (If Possible)

If the device was lost and not stolen, use official device-tracking tools to locate the device:





- Apple devices: Find My
- Android devices: Find My Device
- Windows laptops: Find My Device (if enabled)

If recovery is unlikely:

- Lock the device
- Display a contact message (if safe)
  - Only display contact information that does not expose your home address or sensitive details.
- Remote wipe the device if sensitive data is present
- Wiping protects your data but usually makes recovery impossible.

## Notify Key Providers

### Mobile Carrier (For Phones)

- Report the device as stolen
- Suspend or transfer service
- Request a SIM block or new SIM
  - Blocking or replacing a SIM can prevent service misuse after device theft.
  - Consider protecting the carrier account itself.
- Ask about IMEI blacklisting
- This helps prevent SIM swapping and call/text interception.

### Employer, School, or Organization (If Applicable)

- If the device had:
  - Work email
  - School access
  - Internal systems or a reputable VPN
- Notify them immediately so they can:
  - Revoke access
  - Secure organizational data
  - Document the incident

## Preserve Evidence & Document the Theft

Create a record with:

- Device make, model, and serial number
- Date, time, and location of loss/theft
- Any suspicious activity noticed afterward
- Police report number (if filed)

This documentation supports insurance claims, disputes, and investigations.





## Watch for Follow-On Risks

After device theft, criminals may attempt:

- Account takeovers
- Financial fraud
- Identity theft
- Social media impersonation
- Stalking using location data

Monitor closely for:

- Login alerts
- Password reset emails
- Unauthorized transactions
- New devices added to accounts

## Report the Theft

- Law Enforcement
  - File a police report (even if recovery is unlikely)
  - Use non-emergency lines unless danger is present
- Ohio Resources
  - Ohio Attorney General – Consumer Protection & Identity Theft
  - <https://www.ohioattorneygeneral.gov>
  - Hotline: 800-282-0515
- Geauga County
  - Geauga County Sheriff's Office
  - <https://www.geaugasheriff.org>
  - Call 911 if threats, stalking, or immediate danger occur

A police report can help with account disputes and insurance.

## Recovery – Ongoing Protection

- Continue monitoring accounts for several weeks
- Expect increased scam attempts
- Replace the device securely
- Restore data only from trusted backups
- Re-enable device tracking on replacements

## How to Reduce Harm After Device Theft

- Act quickly, delays increase risk
- Email security comes first
- Assume saved logins may be exposed





- Document everything
- Ask for help early if unsure

