Lost Or Stolen Business Device? Here's What To Do Next

By Krislyn McDonnell

General Best Practices

Preparing yourself and your devices before they are stolen is the fastest way to avert potential breaches. Consider:

- Keeping a “Find My” app turned on for all devices. This is the best way to locate and remote wipe devices.

- Making sure your devices are secured behind individualized pin codes, fingerprints, or Face ID. This will slow down thieves trying to access your device.

- Mandate strong, individualized passwords for all accounts, including email and banking apps. Encourage the use of a trusted password manager to automate password creation. This will help limit the scope of any breach.

- When a device is stolen, act quickly. The faster the response, the more effective the following steps are likely to be. If the thief turns the device off, or removes a battery, it won’t be possible to remotely wipe the device.
- Back up the data on ALL business devices—including smartphones and tablets—so they can be remotely wiped if necessary following loss or theft

Learn how to back up business devices in the case of loss or theft.

Android Devices

Here is what Android users should do in case of device theft.

- First, locate the device. Have the owner go to android.com/find and sign into the Google Account associated with the account.
- If more than one device is associated with the account, choose the one you're looking for from the list at the top of the screen. The lost/stolen device will receive a notification, so you should act quickly.
- On the map screen, you'll be shown information about the phone's location. Remember this is approximate and may be neither precise nor accurate. If the device can't be found, you'll see its last known location (if available).
- If the device has certainly been stolen, click "Enable lock & erase" to erase your device. But be careful. After you erase your device, Find My Device will no longer work, so make sure you are certain.
- If you believe your phone is just lost, and not stolen, there are a few options. "Lock" will lock the device behind a PIN, pattern, or password. If there's no lock in place, you can set one. To help someone return the device, you can also add a message or phone number to the lock screen.

An important note: *If you happen to find the device after it's erased, you'll likely need the associated Google Account password to use it again.*

iOS Devices

Here is what iOS users should do in case of device theft.

- The device owner will need to sign into icloud.com/find or use the Find My app on another Apple device.
- Next, locate the missing device. Select the one you're searching for to view its location on a map.
- You'll be presented with a few options here. "Mark As Lost" will remotely lock the device, allow you to display a custom message with contact information on the missing device's lock screen, and track the device's location. If Apple Pay is enabled, the ability to make payments using Apple Pay on that device will be suspended for as long as the device is in Lost Mode.

- If you're certain the device has been stolen, select "Erase your device." When erased remotely, all information is deleted and the user will no longer be able to locate it with the Find My app or Find iPhone on iCloud.com. Make sure the phone is not recoverable before taking this step.

Device Theft Wrap-Up

After you have protected your most sensitive information with the steps above, take just a few more steps to fully wrap the crisis up.

- Report the lost or stolen device to local law enforcement. Law enforcement might request the serial number of your device. This can often be found on the original packaging.

- Report your stolen device to your wireless carrier. They will disable your account to prevent calls, texts, and data use by the thief. If you have insurance through your carrier, this is the time to begin filing a claim as well.

- Ensure the responsible user changes *all* passwords, including Google and Apple accounts. After a device is stolen, one can never be certain of how far the breach has penetrated.

- Alert your banking providers to the potential breach and monitor your bank accounts and credit cards for suspicious activity. If you see any, get ahead of the issue and cancel and replace all of your bank cards. This will prevent the financial breach from affecting multiple accounts.

A stolen device is a headache, but it doesn't have to be a disaster for your business. If you have a plan in place for a worst-case scenario, you'll be able to act quickly and confidently. Most importantly, make sure all devices are properly backed up in advance of any incident.