Fix Three Common Accounting Firm Data Vulnerabilities

ENCYRO

Fix Three Common Accounting Firm Data Vulnerabilities

Use these step-by-step guides to protect your business from data thieves

Brought to you by:

Encyro Community Resource Division

CONTENTS

Encrypt Your Devices

Why Encrypt Your Devices?

- Password protection is not enough – the thief can simply connect the stolen computer's hard drive to a different computer and read all data on the hard drive.

- Lost or stolen devices, if encrypted, are not considered a data breach in most states.

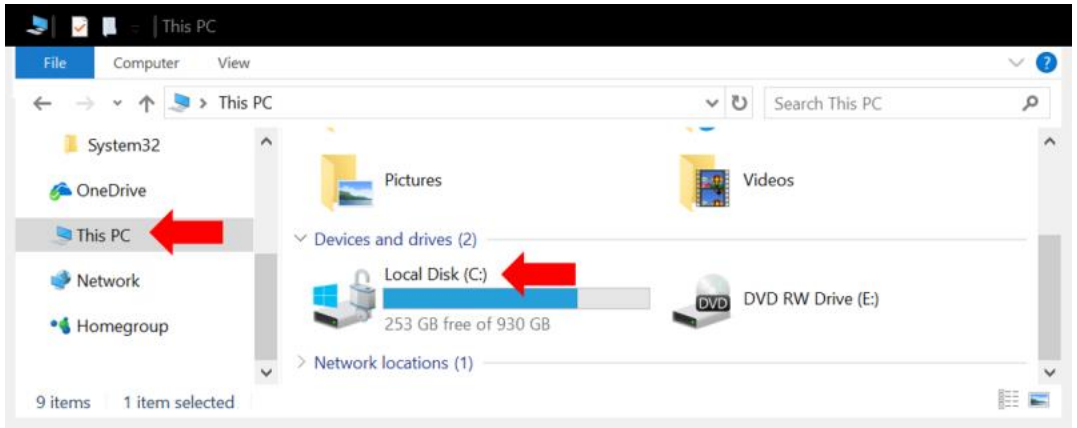
Encrypt PCs
(Windows 7, Windows 10)

- If you have the Ultimate, Pro or Enterprise version of Windows (typically comes with business PCs), you can use BitLocker.
- Once enabled, BitLocker will protect your drive but you will be able to access all your data as before.
- If your version of Windows does not have BitLocker, you may:
  - Upgrade Windows to Pro (not free)
  - Use third party tool: VeraCrypt (free) – See page 11

NOTE: Even if you are buying a new PC with a version of Windows that has BitLocker, you will still need to protect the data on your old computers.

Encrypt PCs Using BitLocker
(Windows 7, Windows 10)

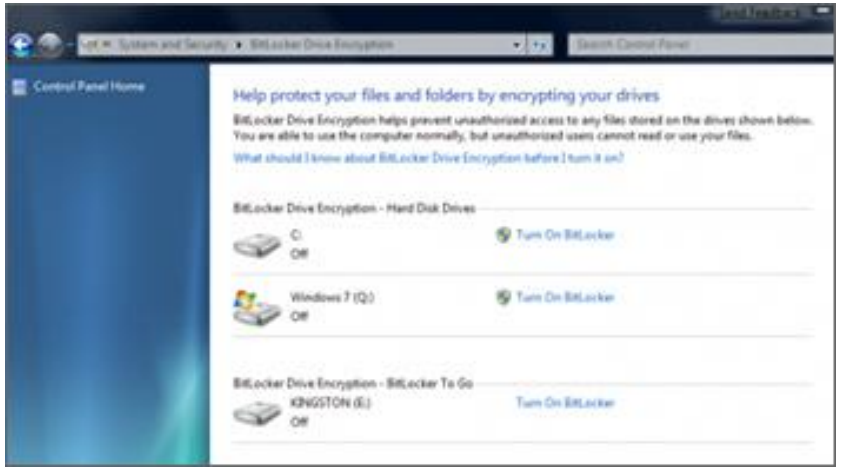
- **Step 1 (Windows 10):** Check if your PC has BitLocker.
  - From a Folder Explorer, click “This PC”. Then right click on the primary drive (typically “c:”) and select “Turn on BitLocker”



If there is no option named “Turn on BitLocker” or “Manage BitLocker,” then your version of Windows likely does not have BitLocker. Skip to page 11 for VeraCrypt instructions.

Step 1: Go to BitLocker

- **Step 1 (Windows 7):** Check if your PC has BitLocker.
  - Go to **Control Panel,** then select **System and Security** and look for **BitLocker.** If found click it and you should see a link to “Turn on BitLocker” next to each listed data drive.



If you do not find the BitLocker setting, then your version of Windows likely does not have BitLocker. Skip to page 11 for VeraCrypt instructions.

Step 2. Choose How to Unlock

- **Step 2:** Choose how to unlock your drive
  - When you click on “Turn on BitLocker”, the BitLocker wizard will start. It will ask you to choose how to unlock your drive, from the following options:
    - **Password:** (Recommended) You will enter a password that you can use to access the encrypted data on this or any other computer you may connect this drive to.
    - USB/Smartcard: A USB storage drive or smartcard will be needed each time. Not recommended, because the USB key or SmartCard may be accidentally left in the PC and stolen along with it.
  - **Unlock automatically on this PC** (May not be offered in Windows 7): If offered, select this.

NOTE: If your computer does not have a TPM module, you will not be allowed to proceed with BitLocker. To enable BitLocker without a TPM, see https://www.encyro.com/blog/how-to-turn-on-bitlocker-in-windows-10/

Step 3: Recovery Key

- **Step 3:** Save your recovery key
  - In case you forget your password, you will need this recovery key.
  - Save it away from your PC (so it is not stolen along with your PC).
  - Save at two or more places:
    - Print and store in a safe deposit box (or a trusted person's home).
    - Save to your Microsoft Account (if option offered in the BitLocker wizard)
    - Save to a file and copy it to your secure client portal account, or other secure cloud storage.

Windows will now encrypt the drive.

NOTE: Windows 7 may offer to save the recovery key after completing the encryption.

Encrypt PC Using VeraCrypt

- VeraCrypt is free and can be a good security alternative if your PC does not have BitLocker.
  - Once encrypted, you can still access all your data as before, without any extra steps other than entering a password at PC startup time.
- Two key differences from BitLocker:
  - You will need an external USB drive or writable DVD drive to create a recovery disk that is required during VeraCrypt setup.
  - Certain Windows OS updates may **not** work automatically after VeraCrypt encryption is enabled.

Step 1: Download and Install

- Visit https://www.veracrypt.fr/en/Downloads.html to download the version
- Run the downloaded .exe file to install VeraCrypt on your computer.

Step 2: Setup encryption

- Open the installed VeraCrypt application.
- Go to the top menu bar option *System* and select *Encrypt System Partition/Drive*
- Follow the wizard that opens – you will be required to
  - Create a recovery disk (on an external USB drive at least 8GB in size or a DVD).
  - Create a boot time password. This needs to be entered each time you restart your computer.

Step 3: Encrypt and reboot

- Let VeraCrypt finish encrypting your disk
- Then reboot and ensure that your boot time password works as expected.

Encrypt Mac

- Apple Mac OS offers FileVault 2 for full disk encryption
  - Available on Mac OS X Lion and newer
  - On a Mac OS X Panther and newer (but older than Mac OS X Lion) FileVault can be used to encrypt the home directory.

Step 1: Go to FileVault

- Choose Apple menu, then select System Preferences, and then click Security & Privacy.
- Click the FileVault tab.
- Click the Lock (in bottom left) and enter an administrator account password.
- You should now be able to access the option to “Turn on FileVault”

Step 2: Turn On

- Click “Turn on FileVault”
  - If there are other user accounts on this Mac, they have to enter their passwords as well. (Their data will also be encrypted.)
  - Any new users created after FileVault is enabled will automatically have access.

Step 3: Recovery Key

- You need the recovery key if you forget your password.
  - Save it to at least two places.
  - Save it away from the computer so that it cannot be stolen with the computer.

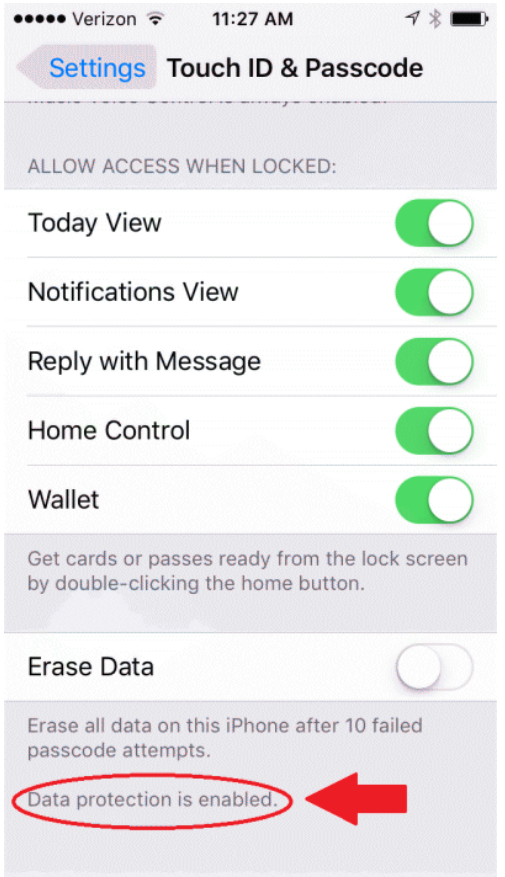
  - Options
    - Connect to iCloud account (offered on OS X Yosemite and later)
    - Save with Apple (offered on OS X Mavericks and newer) and select security questions
    - Save to a file and copy to your client portal or other secure cloud storage
    - Print and place in a safe deposit box (or a trusted person's home)

Your computer will encrypt the disk in the background.

Encrypt iPhones (and iOS devices)

- To enable encryption on an iPhone, you simply need to turn on a **passcode**.
  - Each time you turn on your device screen, you will be required to enter that passcode, or login using your fingerprint (on Touch ID devices), or your face (on iPhone X).
  - If already done, you will see “Data Protection is Enabled” under your Touch ID/Face ID and Passcode settings

- Also turn on **remote wipe**, to help erase data in case of device theft or loss.



Step 1: Go to Passcode Setting

- Go to Settings and tap the following option
  - On devices with Touch ID (fingerprint reader): Touch ID & Passcode.
  - On devices without Touch ID: Passcode.
  - On iPhone X: Face ID & Passcode.

Step 2: Choose a Passcode

- Tap on “Turn Passcode On”
- Enter a six-digit passcode.
  - You may optionally tap **Passcode Options** use a custom alphanumeric code.
- Ensure that
  - **Require passcode** is set to “Immediately”
  - (Optional) **Erase data** option is set to automatically erase data after 10 failed passcode attempts

Step 3: Enable Remote Wipe

- Go to Settings and then tap your name. The tap iCloud.
  - On older versions of iOS, tap Settings and then iCloud.
- Scroll to the bottom and tap “Find My iPhone.”
- Turn on Find My iPhone and Send Last Location.

Enabling “Find My iPhone” automatically enables remote data wipe.

Encrypt Android Devices

- Many newer models (e.g. Google Pixel) are encrypted by default.
- NOTES
  - On certain versions of Android, once encrypted, if the device reboots (such as for an automatic update at night), functions such as alarms and receiving calls will NOT work until you enter your passcode.
  - Set aside down-time: Device may restart several times during encryption and may not be usable for an hour or more.
- Enable the screen lock to enable encryption (using PIN, pattern, or password)
- Set the device to require screen lock
- Enable remote wipe by setting “Allow Remote Lock and Erase” to on

Step 1: Enable Screen Lock

- Open the Settings app (denoted by a gear icon)
- Tap Security or Security & Location.
- Tap Screen lock.
  - Choose your screen lock option: Pattern, PIN, or Password.

If you have a device older than Android 4.4: see https://support.google.com/nexus/answer/2844831?hl=en

Step 2: Require Screen Lock

- When setting your screen lock, the settings app will ask you to "**further protect this device**" by requiring your PIN, pattern, or password when your device starts.
  - Select Require to start device.
  - Tap Continue.

[The first time that you choose this setting, it will encrypt your device. This may take time.]

- Set your PIN, pattern, or password. Follow the on-screen steps.

Step 3: Enable Remote Wipe

- Go to Settings, then Security and Location (or Google, then Security) and Find my Device. Turn on “Remotely locate this device” and “Allow remote lock and erase.”
- Go to Settings, Security and Location (or just Location) and turn on “location”
- In a web browser, got play.google.com/settings and under “Visibility” select your required device. Ensure that it is set to visible.

Encrypt Your Email

Send Encrypted Email

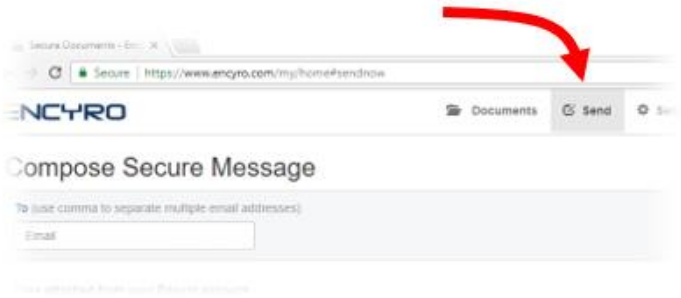
- You may use a free Encyro account to send encrypted messages or files to any email address.

- The recipient does not need an Encyro account. They simply click a link to access a secure webpage with their message.
  - The message and files expire for security reasons.

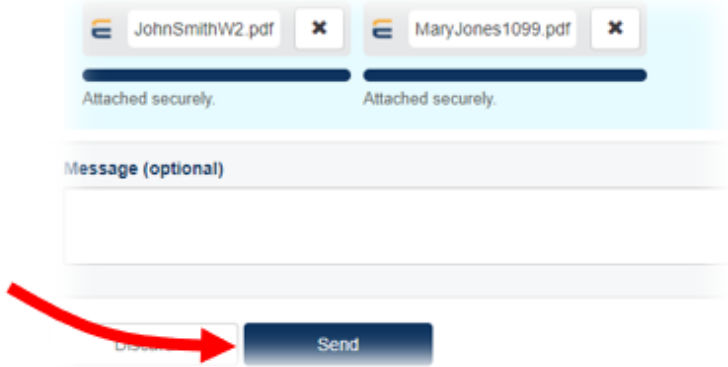
Send: Step by Step

- **Step 1:** In a web browser, go to https://www.encyro.com/account/register/ and create a free account.

- **Step 2:** Go to the Send tab. Compose your message. Attach files if needed.



- **Step 3:** Click the Send button. Messages and files are sent with bank-level encryption.



Receive Encrypted from Clients

- With **Encyro Pro** (free 30 day trial), you can receive securely from any client without asking them to create an Encyro account.
  - You receive an “upload page” where clients can easily upload files or messages to you
- **Alternatively:** If you do not wish to sign up for Encyro Pro, your clients can use a *free* Encyro account to send you messages and files.
  - When you send them a message from your free account, your client will have the option to reply by creating a free account.

Receive: Step by Step

- **Step 1:** Go to https://www.encyro.com/account/register/ and sign up for a Pro account.
  - If you already signed up for a free account, simply login and go to the Settings tab. Click “Change Membership Type” and click “Start Trial” to switch to the Pro membership.
- **Step 2:** Click the top menu tab “My Upload Page”. In the setting called “Upload Page URL” enter your business name without spaces or another name you wish to use. Click “Check and Create”
  - Optional: Add your full name, business logo and photo.
  - Optional: Choose one of the many available designs for your upload page.
- **Step 3:** Scroll down to the bottom to section “Visit Upload Page.” Copy the upload page web address shown. Email this link to any client and they can upload messages or files securely to you by visiting that link.

Remote Backup Your Data

Why Remote Backup

- Ransomware or other malware can make your computer unusable.
  - Ransomware can disable access to all data on your PC and asks you to pay a ransom amount (several hundred to thousands of US dollars). Paying the ransom does not guarantee that data access will be restored.
  - Ransomware typically infects the computer and any connected local backup drives at the same time – so a remote backup is needed.

- Remote backups also protect you against disasters (flooding, fire, earthquakes, etc.) and theft.
  - Remote backups also protect against hardware malfunctions much like local backups.
  - Remote backups may not be always be more expensive than local backups when you consider the time cost of connecting/managing backup drives in addition to the purchase price of backup drives.

Step 1: Choose a Provider

- Many alternatives: CrashPlan, Carbonite, Blackblaze, iDrive, Acronis, and others

Low cost options (not affiliated with Encyro)

- CrashPlan:
  - Business-friendly controls such as creating multiple staff accounts
  - Low price per computer, unlimited storage
  - Backup only computers (no servers or NAS storage)
- For solo accountants: Carbonite
  - Cheaper than CrashPlan per computer if used as an individual
  - No staff accounts or organization level controls (upgraded plans offer business options).

Step 2: Install backup client

- Once you have selected a provider, you will need to install their backup software on your PC.
- After installation, the software will ask you to
  - Select folders to backup – make sure all folders where business data is stored are selected
  - Select your encryption option – most providers offer to manage your encryption keys automatically, or manage your own encryption keys.
    - If you manage your own encryption key, those keys are not sent to the backup provider's cloud servers but you must backup and securely store the encryption key.

Step 3: Run Backup

- An initial backup will take time, possibly multiple days.
- Subsequent backups will be fast because only new data will be backed up.
  - Most backup clients will allow you to choose between continuous backup or scheduled backup times.
- **Verify that you can access the backup.**

Brought to you by:

Encyro Community Resource Division

ENCYRO

Making Data Security Easy for You

info@encyro.com