What data can be stolen if the phone or laptop is lost?

Losing a phone or laptop is bad enough, but what happens to your personal data in the lost phone or laptop?

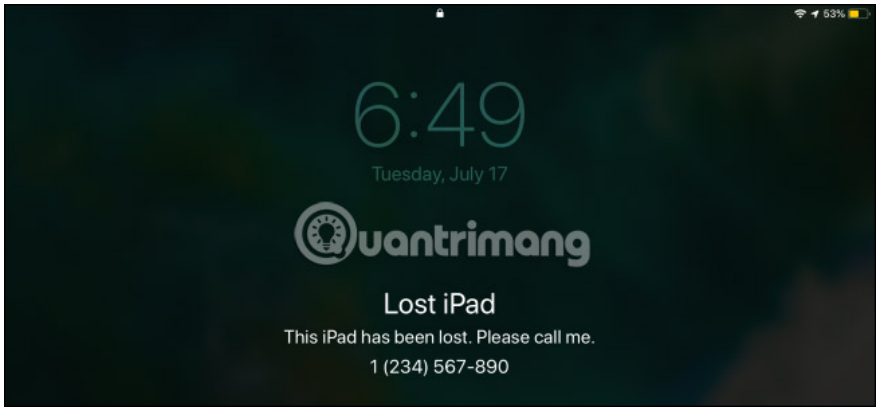
Losing a phone or laptop is bad enough, but what happens to your personal data in the lost phone or laptop? Can a thief use your stolen phone, tablet or laptop to access applications and files on the computer? That depends on the type of device you lost. And unfortunately, most Windows computers are not encrypted.

Thieves can always delete data on your device and continue using that device, unless you turn on something like **Activation Lock** on an iPhone or iPad, for example, but they can't get your personal data if memory of the device is encrypted.

iPhone and iPad

Apple's iPhone and iPad are securely encrypted by default. Thieves will not be able to unlock your phone without a passcode. Even if you usually sign in with the Touch ID or Face ID, your phone is still secured with a passcode.

Of course, if you install your iPhone or iPad so that they do not require a passcode or if you use an iPhone password that is easy to guess, like 1234 or 0000, the thief will be able to easily unlock it.



However, some types of personal information are still displayed, even if you have protected the device with a passcode. For example, thieves can see all incoming notifications on your phone without unlocking. With the default settings, this means that the thief will see the text message in the inbox, including messages containing the SMS verification code to access your account. You can hide sensitive notifications on the lock screen, but usually all display on your lock screen by default. Thieves can also answer incoming calls on your phone.

You can access the Apple Find My iPhone website to remotely locate your lost iPhone or iPad. To prevent thieves from using your device, put it in "Lost Mode". This will turn off all notifications and alerts on the device. **Lost Mode** also allows you to write a notification and it will appear on the phone or tablet. For example, you can ask anyone who finds it to return it and provide a phone number to contact you again.

1. Lock iPhone, iPad, Mac devices remotely when you lose your device

If you have abandoned the lost iPhone or iPad, you can and should delete the data remotely. Even if the device is offline, the data will still be deleted the next time it is online.

GrayKey may allow police departments and government agencies to ignore your passcode, but Apple is correcting this problem with USB Restricted Mode.

Android phone

Modern Android phones are also encrypted by default. Specifically, encryption is required by default starting with Android 7.0 Nougat, which was officially released in August 2016. As long as the phone you are using comes with Android Nougat or a newer Android version right from First, it is definitely encrypted.

1. How to root your Android Nougat phone with SuperSU

If your phone initially has an older version of Android and you have never turned on encryption, the phone's memory may not be encrypted and the thief may delete your data from the phone. Even if your phone is currently running Android 7.0 or higher, the phone may not be encrypted if it originally ran an older version of Android.

Of course, this encryption only helps if you are using a PIN or passphrase to protect your device. If you are not using a PIN or you are using an easy-to-guess password like 1234, a thief can still easily access your device.

Just like on iPhone, your Android phone will continue to display notifications on the lock screen. This can reveal sensitive text messages, unless you hide sensitive messages from your lock screen.

You can use Google's **Find My Device** feature to remotely locate your lost Android phone. This tool also allows you to lock the device to prevent thieves from seeing your message and remotely delete notifications to ensure your personal data is not disclosed.

Windows PC

Most Windows PCs cause problems if they are stolen. Windows 10 is still the only modern operating system that does not provide encryption for all users and Windows 7 and 8 are even worse. Your Windows PC storage is not encrypted, which means that anyone who steals your Windows device can access your personal files, by booting another operating system on it or taking the drive. internal disk, then insert it into another computer.

If you are using the Professional, Enterprise or Education version of Windows 7, 8 or 10, you can turn on the BitLocker encryption option to protect your device. If you are using these expensive versions of Windows and have set up BitLocker, your data will be secure (provided you have used a strong password).

You can check whether BitLocker is used on PC by going to **Control Panel> System and Security> BitLocker Drive Encryption** . (If you do not see this option, then you are using the Home version of Windows).

If you are using the Home version of Windows 7, 8 or 10, there is no way to use standard BitLocker encryption. Some new computers using Windows 8.1 or 10 have a special, limited version of BitLocker, originally called 'Device Encryption'. This feature automatically encrypts the memory of these operating systems, but only if you sign in with your Microsoft account and not a local user account. This encryption feature is not available on all

Windows 8.1 and 10 PCs, but only on computers with specific hardware.

You can check if the **Device Encryption** feature is available on PC by going to **Settings> System> About.** Look for the ' **Device Encryption** ' message. If you do not see this item, then your PC does not support.

If you are using a Home version of Windows, you can also try third-party encryption tools like VeraCrypt or pay $ 100 to upgrade from Home to Professional version and use BitLocker.

The bad news is, unless you've used BitLocker or you have this encryption feature built into Windows 10 PC, your computer's internal memory may not be encrypted and the files will be accessed by thieves. .

If your device runs Windows 10, you can use Microsoft's **Find My Device** tool to track it, provided that Find My Device is turned on the PC before you lose the device.

Microsoft should enable encryption by default for all users. Unfortunately, Microsoft did not do so and, among modern devices, Windows PC is the only device prone to data theft (unless BitLocker is enabled).

MacBook

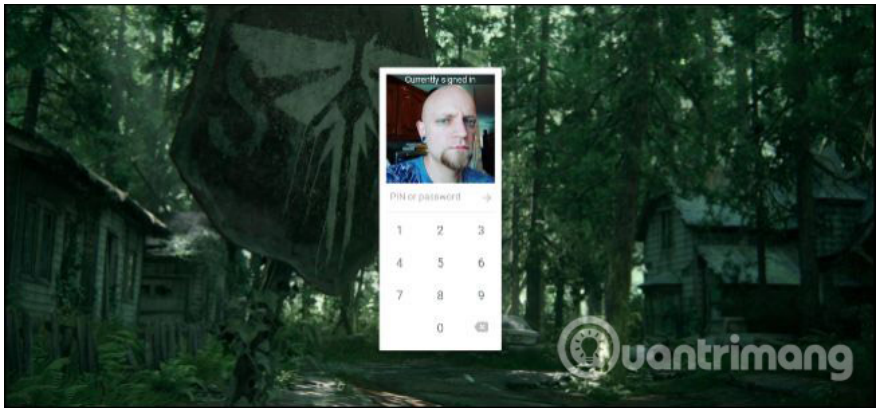
Apple has encrypted Mac storage by default with FileVault from OS X 10.10 Yosemite, released in 2014. Mac's internal drives are almost certainly encrypted with FileVault, preventing people from accessing your files otherwise know the Mac password.

You can check whether your Mac is encrypted by going to **Apple menu> System Preferences> System & Privacy> FileVault** .

Of course, this only works if your MacBook is secured with a password. If you use very weak, easy-to-guess passwords or automatic logon settings, thieves can easily access your MacBook.

If you have enabled Find My Mac, you can use Apple's **Find My iPhone** tool (the Mac also appears in it) to remotely lock and delete data from your Mac. The password you set when locking your Mac will even prevent a thief from being able to reset your Mac and use it.

Chromebook

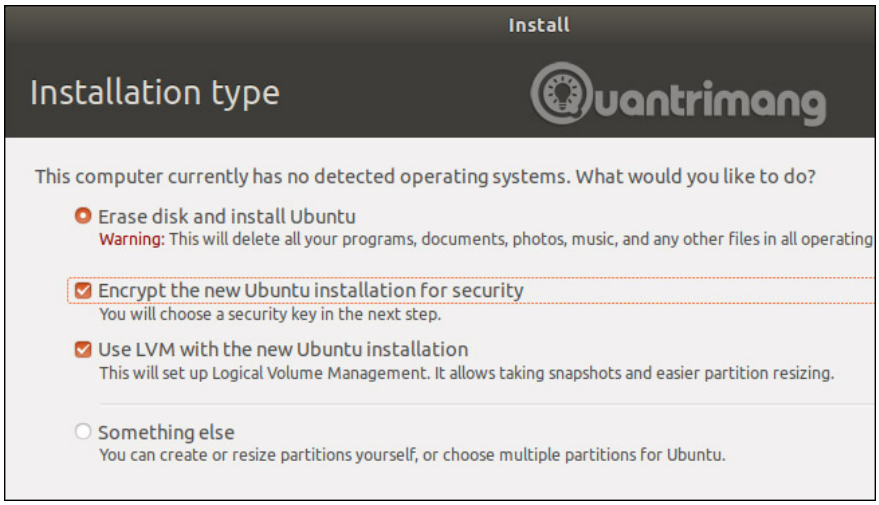


Chromebooks always have encrypted memory, so thieves will not be able to log in and access your data without the Google account password or PIN you use to unlock your Chromebook.

1. What Chromebooks have and can't do?

A thief can log in with another Google account, log in to a guest account or delete your Chromebook and set it up from scratch, but will not be able to access your personal data, of course under account conditions Your Google has a strong password.

Linux laptop



If you are running the Linux operating system on your laptop, whether the device is encrypted or not depends on the options you selected while installing the Linux distribution. Most modern Linux distributions, including Ubuntu, allow you to enable disk encryption during the installation process, and this encryption is secured with a normal Linux user account password or with a password. Special encryption that you type when starting the computer.

However, this encryption option is usually not enabled by default and it is not available in Ubuntu. If you do not enable this feature, your Linux system will not use encrypted memory.

Assuming you have enabled encryption while installing the Linux distribution, your data must be protected, provided you have used a hard-to-guess security password.

Laptops are more vulnerable to sleep when in sleep mode

Another thing to note about laptops: If your laptop is powered on, but in sleep mode, its encryption key is still stored in the memory of the laptop. Theoretically, an attacker could perform a "cold boot attack", quickly reset your device and boot another operating system from a USB drive, to get the encryption key from memory before it is deleted.

Most thieves don't even think of an attack like this, because it's quite complicated. However, if you are really worried about spies or government agencies, it is safer to turn off your laptop when you are not using it, instead of leaving it to sleep. You should turn off the laptop, when you are taking it to a public place or somewhere else you are worried it could be stolen. This will ensure the encryption key is not in memory.

See more:

1. Find smartphones, laptops lost accurately and effectively with Prey application
2. Let the laptop self-destroy data when lost
3. 5 types of data theft you should know to prevent