SAFE BROWSING GUIDELINES FOR SOCIAL NETWORKING SITES

Online communities have existed since the invention of the internet. First there were bulletin boards and email lists, which gave people around the world opportunities to connect, to communicate and to share information about particular subjects.

Today, social networking websites have greatly expanded the range of possible interactions, allowing you to share messages, pictures, files and even up-to-the-minute information about what you are doing and where you are. These functions are not new or unique – any of these actions can also be performed via the internet without joining a social networking site.

Remember that social networking sites are owned by private businesses, and that they make their money by collecting data about individuals and selling that data on, particularly to third party advertisers.

If you work with sensitive information and topics, and are interested in using social networking services, it is important to be very aware of the privacy and security issues that they raise.

Before you use any social networking site it is important to understand how they make you vulnerable, and then take steps to protect yourself and the people you work with.

SOCIAL NETWORKING PLATFORMS

SOCIAL NETWORKING PLATFORMS

These social networking security guides aim to help you navigate the privacy and security settings of a few popular social networking platforms, with a view toward making them *more* secure Specifically, step-by step guides are provided for Facebook and Twitter, and some general guidelines are provided for YouTube and Flickr.

These social networking websites are the most popular and widely used social networking tools.

Government crackdowns will target these sites first and block them, and the companies will cave into government pressures and censor when necessary.

If they are not blocked, they are actively monitored by numerous governments who collect user metadata and make requests for private information about individuals of interest, often including human rights defenders.
Note, in this regard, that companies managing social networking servers have access to **all your information**, including your private data and password.

Other similar sites may be popular in different regions, so you way wish to explore other options.

1. it provide connection over **SSL** (like http*s*) for all uses of the site, rather than just during login? Are there no problems related to encryption, such as problems related to encryption certificates?
2. Read the End User Licence Agreement and Privacy Policy or Data Use Policy carefully. How are your content and personal data treated? With whom are they shared? For a useful add-on which helps users undestand the Terms of Service of many popular sites, see **Terms of Service; Didn't Read**.
3. What privacy options are provided for users? Can you choose to share your videos securely with a small number of individuals, or are they all public by default?
4. Do you know the **geographical location of the servers**, under which territorial jurisdiction they fall or where the company is registered? Are you aware of how this information relates to the privacy and security of your email activity and information? Will the site's owners hand over information if they receive a governmental request to do so?

FACEBOOK

Facebook is the world's most popular social networking site. It can be and has been used widely by human rights advocates in order to build networks, communicate, organise and publicise events or issues. However, it is also a potentially rich source of information for those opposed to the activities of rights advocates. Therefore, knowledge of the different account and privacy settings available is extremely important.

PRIVACY SETTINGS AND TOOLS

Step 1. To edit your **Facebook** *Privacy Settings*, **click** on the small arrow beside *Home* in the top right-hand corner and select *Settings*.

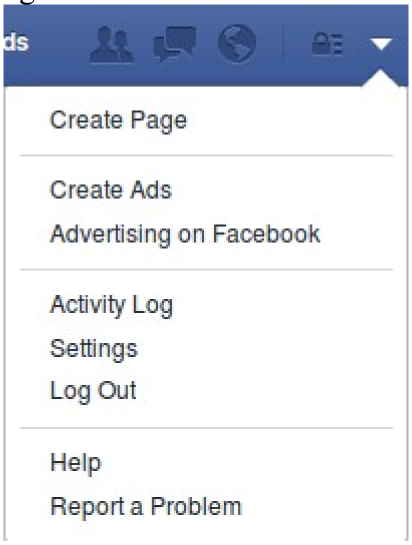


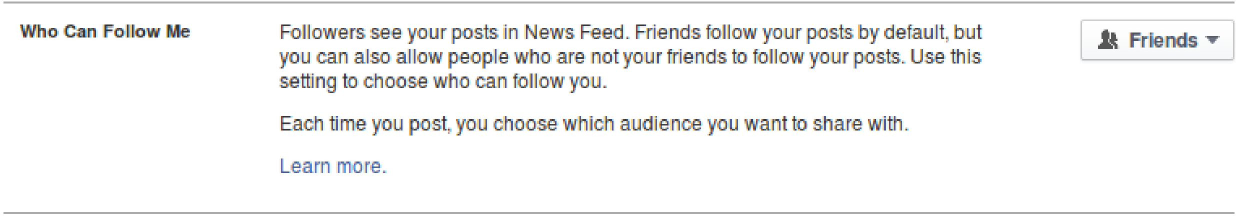
Figure 1: Options

FOLLOWERS

Facebook gives you the option of allowing people to subscribe to your news feed, without being friends. Be aware however, that if you allow others to subscribe to your news feed, then some of your data is available for them and others in their network to see. The safest option is not to allow people to subscribe to your news feed.

Step 16. Click on *Followers* from the menu on the left.

Step 17. Ensure that *Friends* is **selected**.



Who Can Follow Me

Followers see your posts in News Feed. Friends follow your posts by default, but you can also allow people who are not your friends to follow your posts. Use this setting to choose who can follow you.

Each time you post, you choose which audience you want to share with.

Learn more.

Fig. 18: Follower settings

ADVERTISING SETTINGS

Advertising is fundamentally important to social networking companies, as it is their source of revenue. There will always be advertisements on social networking sites such as **Facebook**, though we can make them less personal, which is the right move in terms of information security and privacy.

Note that changes made to this setting are not recorded by **Facebook**, but are rather stored in your browser. Unfortunately, you must **repeat** this process for every browser, app and device you use to connect to **Facebook**.

.

YOUTUBE

YouTube is a service, owned by **Google**, that allows you to upload and share video content. It has become popular among human rights defenders as a platform for carrying out campaigns and sharing evidence of human rights abuses, among other uses. **YouTube** is great for making your video available to its billions of users. However, if the people at Google find the content of your video objectionable, they will delete it. Google also collects users' metadata *en masse*, and may

YOUTUBE TIPS

- Never post a video of any individual without their consent. And even with their consent, try to think of any possible repercussions before posting it.
- When you navigate to **YouTube**, do so by typing "https://www.youtube.com" into your browser's address bar (or by using a bookmark to this Web address). This will ensure that the communication between your browser and **YouTube** is protected by **Secure Socket Layer** (SSL) encryption. To avoid having to do this each time you connect, we recommend using **Firefox** with the **HTTPS Everywhere**add-on.
- For more privacy, try creating a new, anonymous **Google** account that you access only through the **Tor Browser**. If you upload videos to **YouTube** this way, your location and other identifying information will be hidden from **Google**. Unfortunately, it is sometimes difficult to watch videos on **YouTube** with the **Tor Browser**. If you find this to be the case, you might have to rely on a combination of techniques to protect your privacy. The **Firefox** Web browser, various security add-ons and a separate **Google** would be a good place to start.
- When uploading a sensitive video from an Android device, consider using the Guardian Project's InformaCam, which gives you some control over your video's metadata and—when used in conjunction with **Orbot**—helps you send it through the Tor network.
- Make use of **YouTube**'s **face-blurring** option for videos in which people may not wish to be identified, such as those taken at protests. Read more **here**.
- Always keep a back-up copy of any video you share via **YouTube**.
- Use the *private* setting in order to share video with specific individuals only.

ALTERNATIVES TO YOUTUBE

If you do not wish to associate your videos with your **Google profile**, there are a number of alternatives, such as **Vimeo**. Vimeo is frequented by a smaller community of users than **YouTube**. Like **YouTube**, it facilitates connection over **SSL**, and gives users numerous privacy options and control of creative commons licenses for their videos. Other similar sites may be popular in different regions, so you way wish to explore other options. Before choosing one you should consider the following points:

1. Does it provide connection over **SSL** for all uses of the site, rather than just during login? Are there no problems related to encryption, such as problems related to encryption certificates?
2. Read the End User Licence Agreement and Privacy Policy or Data Use Policy carefully. How are your content and personal data treated? With whom are they shared?
3. What privacy options are provided for users? Can you choose to share your videos securely with a small number of individuals, or are they all public by default?
4. If you will upload sensitive images, such as footage of a protest, does the site facilitate protection of those you have filmed, such as through face-blurring?
5. Do you know the **geographical location of the servers**, under which territorial jurisdiction they fall or where the company is registered? Are you aware of how this information relates to the privacy and security of your email activity and information? Will the site's owners hand over information if they receive a governmental request to do so?

BASIC SECURITY FOR WINDOWS

Security refers to providing a protection system to computer system resources such as CPU, memory, disk, software programs and most importantly data/information stored in the computer system. If a computer program is run by an unauthorized user, then he/she may cause severe damage to computer or data stored in it. So a computer system must be protected against unauthorized access, malicious access to system memory, viruses, worms etc. We're going to discuss following topics in this chapter.

- Authentication
- One Time passwords
- Program Threats
- System Threats
- Computer Security Classifications

Authentication

Authentication refers to identifying each user of the system and associating the executing programs with those users. It is the responsibility of the Operating System to create a protection system which ensures that a user who is running a particular program is authentic. Operating Systems generally identifies/authenticates users using following three ways −

- **Username / Password** − User need to enter a registered username and password with Operating system to login into the system.
- **User card/key** − User need to punch card in card slot, or enter key generated by key generator in option provided by operating system to login into the system.
- **User attribute - fingerprint/ eye retina pattern/ signature** − User need to pass his/her attribute via designated input device used by operating system to login into the system.

One Time passwords

One-time passwords provide additional security along with normal authentication. In One-Time Password system, a unique password is required every time user tries to login into the system. Once a one-time password is used, then it cannot be used again. One-time password are implemented in various ways.

- **Random numbers** − Users are provided cards having numbers printed along with corresponding alphabets. System asks for numbers corresponding to few alphabets randomly chosen.
- **Secret key** − User are provided a hardware device which can create a secret id mapped with user id. System asks for such secret id which is to be generated every time prior to login.
- **Network password** − Some commercial applications send one-time passwords to user on registered mobile/ email which is required to be entered prior to login.

Program Threats

Operating system's processes and kernel do the designated task as instructed. If a user program made these process do malicious tasks, then it is known as **Program Threats**. One of the common example of program threat is a program installed in a computer which can store and send user credentials via network to some hacker. Following is the list of some well-known program threats.

- **Trojan Horse** − Such program traps user login credentials and stores them to send to malicious user who can later on login to computer and can access system resources.
- **Trap Door** − If a program which is designed to work as required, have a security hole in its code and perform illegal action without knowledge of user then it is called to have a trap door.

- **Logic Bomb** − Logic bomb is a situation when a program misbehaves only when certain conditions met otherwise it works as a genuine program. It is harder to detect.
- **Virus** − Virus as name suggest can replicate themselves on computer system. They are highly dangerous and can modify/delete user files, crash systems. A virus is generatlly a small code embedded in a program. As user accesses the program, the virus starts getting embedded in other files/ programs and can make system unusable for user

System Threats

System threats refers to misuse of system services and network connections to put user in trouble. System threats can be used to launch program threats on a complete network called as program attack. System threats creates such an environment that operating system resources/ user files are misused. Following is the list of some well-known system threats.

- **Worm** − Worm is a process which can choked down a system performance by using system resources to extreme levels. A Worm process generates its multiple copies where each copy uses system resources, prevents all other processes to get required resources. Worms processes can even shut down an entire network.
- **Port Scanning** − Port scanning is a mechanism or means by which a hacker can detects system vulnerabilities to make an attack on the system.
- **Denial of Service** − Denial of service attacks normally prevents user to make legitimate use of the system. For example, a user may not be able to use internet if denial of service attacks browser's content settings.

INTRODUCTION

Microsoft Windows is the world's most used consumer operating system.
Windows is considered a standard in many office environments, as is some other Microsoft software such as Microsoft Office. Some common and specialised software is only available for Windows.

The popularity of Windows also makes it a target for malware. The majority of new malware targets vulnerabilities and insecure user practices on the Windows operating system.

Windows is a closed-source operating system. This means that the source code of the system cannot be reviewed or verified by users or the security community. The security guarantees made by Microsoft can only be taken at face value as they cannot be independently audited.

This guide provides some tips on how to secure your Windows operating system and it has been written on Windows 10. Most instructions also apply to Windows 7 or 8.1, however the exact appearance or titles may be slightly different. Where significant differences for earlier versions exist we have provided version-specific sections.

1. ALTERNATIVES TO WINDOWS

Many people may not even know that there are alternatives to Windows. There are two major alternative operating system choices. Mac is a line of computers manufactured exclusively by Apple and running their own operating system called Mac OS X. Then there is the UNIX-like family of operating systems, of which GNU/Linux is the most well-known. These are free and open source operating systems which can be distributed freely and with source code which can be independently audited or modified by anyone. There are many 'flavours' of GNU/Linux, some popular ones include Ubuntu, Debian, Fedora, and Mint. GNU/Linux can run on most computers which operate Microsoft Windows.

2. PRIVACY-ENHANCING SETTINGS

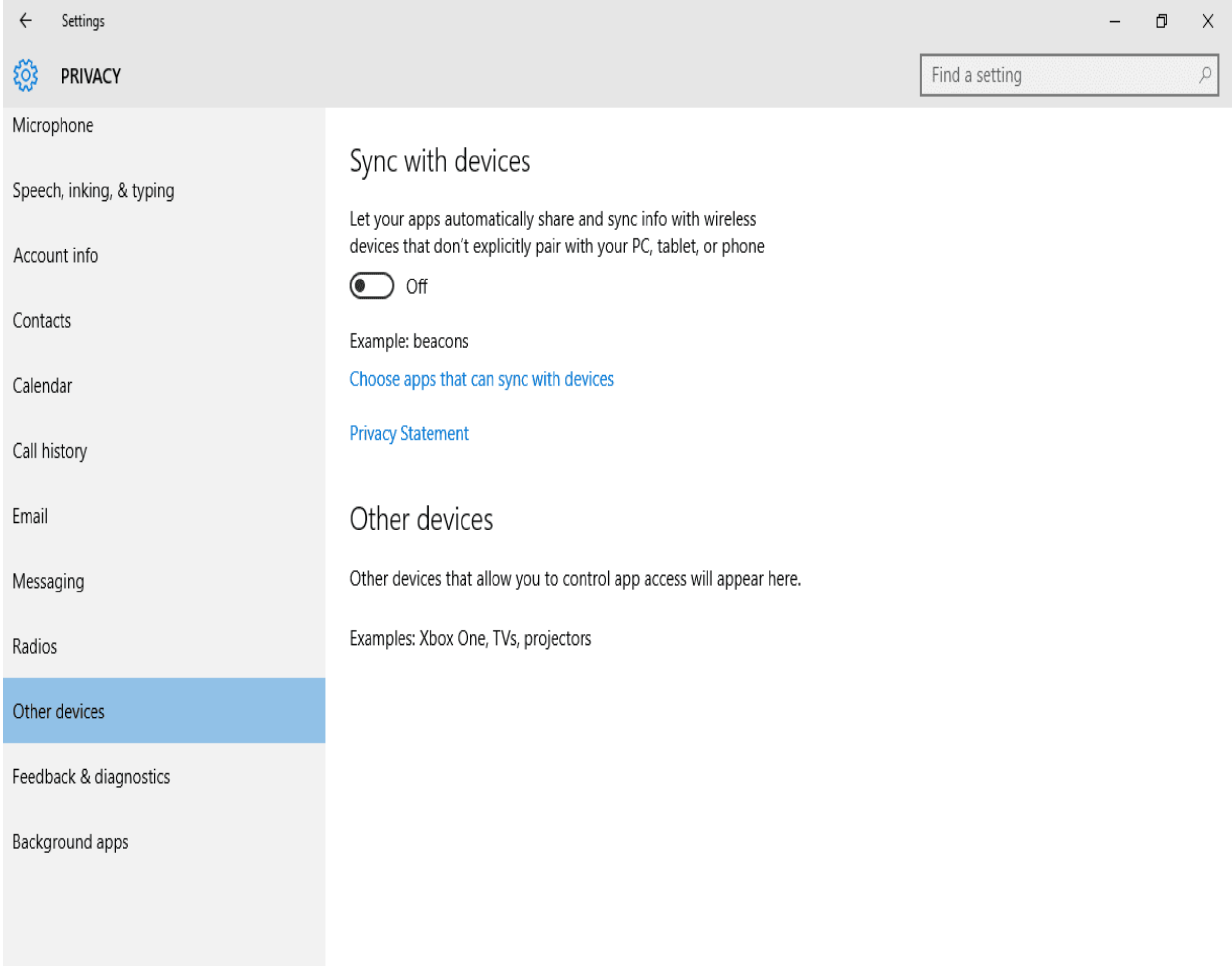
Windows communicates information from your computer back to Microsoft and other servers which can violate the privacy of the user. To limit (though not eliminate) these communications, there are some configuration options you can select. The process will be different if you are installing a new copy of Windows on a computer or if you are working on a computer with Windows already installed.

HOW TO SELECT PRIVACY-PROTECTING OPTIONS WHEN INSTALLING WINDOWS

Step 1. While installing Windows you will be asked to accept Express Settings which contain the most invasive Microsoft-selected settings to send personal data to the company and its advertising partners.

Instead of accepting Express Settings, click [Customise settings].

Note: You may make your own decisions on each of the below options based on your own comfort level trading privacy and functionality. Below are our suggestions for the best privacy and security.



Sync with devices

Let your apps automatically share and sync info with wireless devices that don't explicitly pair with your PC, tablet, or phone

Off

Example: beacons

Choose apps that can sync with devices

Privacy Statement

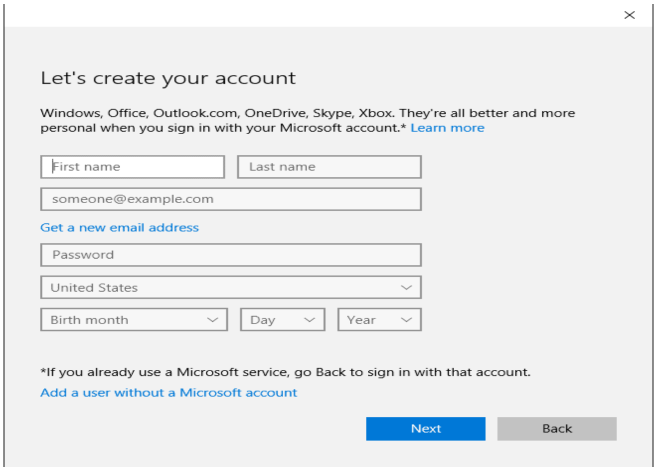
Other devices

Other devices that allow you to control app access will appear here.

Examples: Xbox One, TVs, projectors

USER ACCOUNT PASSWORD

Password-protecting your and all other user accounts and using unique user accounts for each person accessing the computer are basic security requirements.
Click the [Add a user without a Microsoft account] link through the following window.



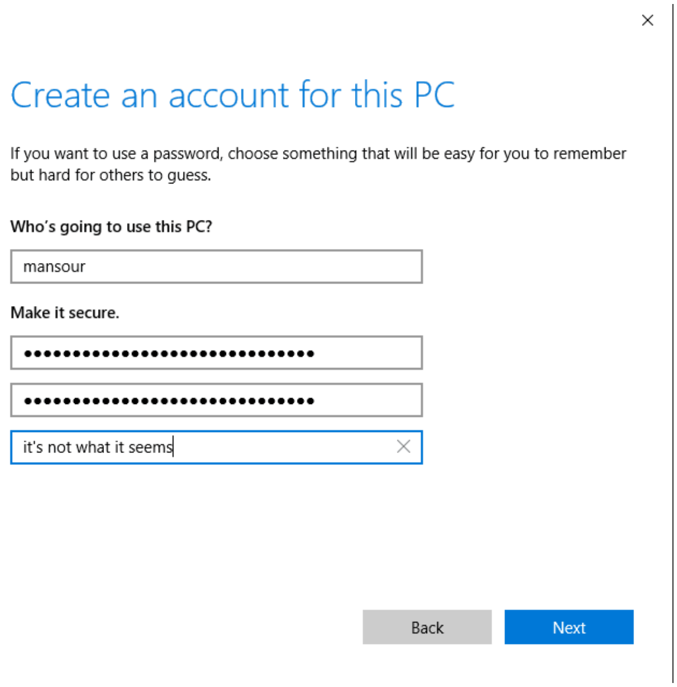
Let's create your account

Windows, Office, Outlook.com, OneDrive, Skype, Xbox. They're all better and more personal when you sign in with your Microsoft account.* Learn more

*If you already use a Microsoft service, go Back to sign in with that account.

Figure 4: Adding a user without a Microsoft account

Step 6. Type the user name for the new account under the Who's going to use this PC? section.



Create an account for this PC

If you want to use a password, choose something that will be easy for you to remember but hard for others to guess.

Who's going to use this PC?

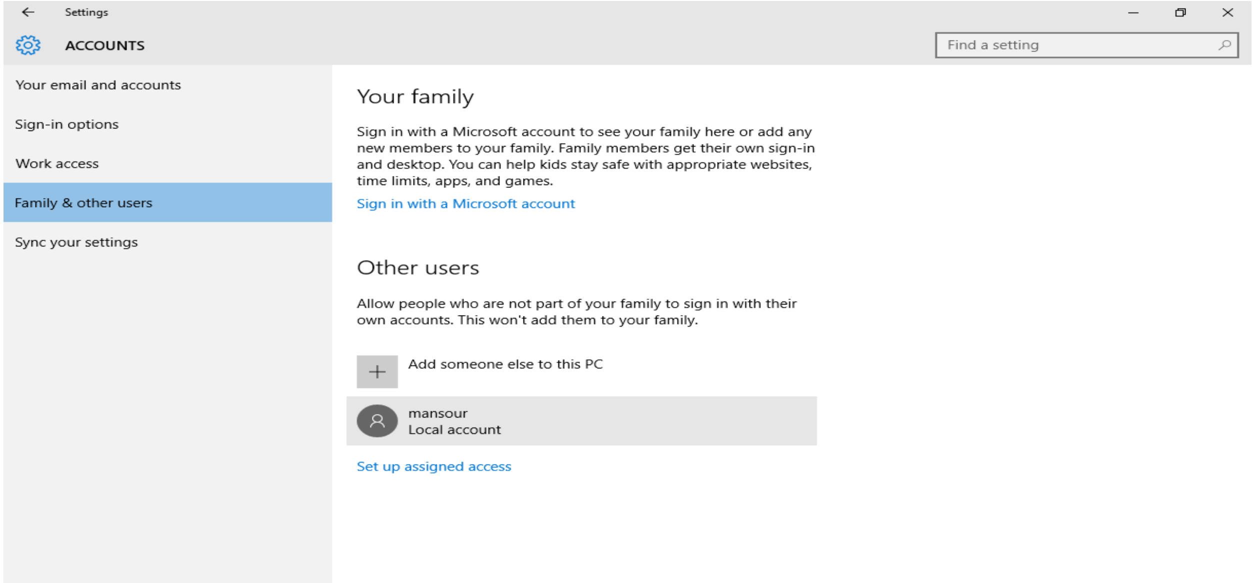
mansour

Make it secure.

••••••••••••••••••••••••••••••

••••••••••••••••••••••••••••••

it's not what it seems



Your family

Sign in with a Microsoft account to see your family here or add any new members to your family. Family members get their own sign-in and desktop. You can help kids stay safe with appropriate websites, time limits, apps, and games.

Sign in with a Microsoft account

Other users

Allow people who are not part of your family to sign in with their own accounts. This won't add them to your family.

Add someone else to this PC

mansour
Local account

Set up assigned access

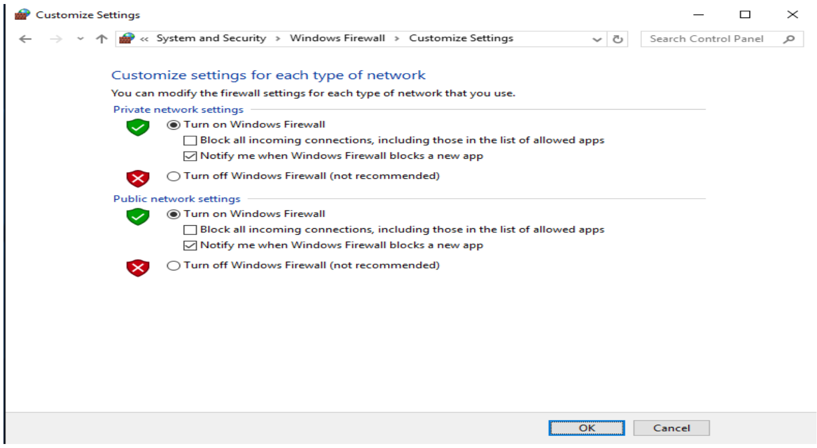
Figure 6: New user account created

SCREEN LOCK

To prevent third parties from physically accessing your computer, you should be able to lock access to your machine when you are not working on it and the screen should automatically lock itself after a period of inactivity. The sections below explain how you can do so.

WINDOWS FIREWALL

Ensuring that your system's firewall is turned on at all times is essential, as it is designed to protect your operating system from unauthorised access to your computer through the Internet based on a set of predetermined security rules.



Customize Settings
« System and Security › Windows Firewall › Customize Settings
Search Control Panel
OK
Cancel

Customize settings for each type of network

You can modify the firewall settings for each type of network that you use.

Private network settings

● Turn on Windows Firewall
□ Block all incoming connections, including those in the list of allowed apps
☑ Notify me when Windows Firewall blocks a new app
○ Turn off Windows Firewall (not recommended)

Public network settings

● Turn on Windows Firewall
□ Block all incoming connections, including those in the list of allowed apps
☑ Notify me when Windows Firewall blocks a new app
○ Turn off Windows Firewall (not recommended)

Figure 3: Turning the Windows Firewall on

Step 4. Select the [Turn on Windows Firewall] option under Public network settings (if it's not already selected).

REMOVING BLOATWARE

Many PC manufacturers include additional software with Windows when you purchase a new computer. These manufacturers are paid by the software vendors to include this software and the bundled software may not benefit and may even harm the interest of the consumer. One high profile case was the Superfish adware pre-installed on Lenovo computers which actively broke internet security processes in order to serve advertisements to users.

Such software is known as bloatware: software which bloats your computer. Best practice is to install a fresh copy of Windows on a new computer using a disk provided by Microsoft, however this may often be impractical or expensive. The next best option is to uninstall the extra software that comes with your computer.

Click the Start button and search for Add or Remove Programs.

Step 2. Review your installed programs. If you have a new computer this will be simpler than if you have been using it for long with many additional software installed. Look for programs you do not recognise and especially for programs not made by Microsoft. If you do not recognise a program try to research it online to understand its function and reputation. Also beware of software without a publisher name, meaning the software is not signed by a recognised software company.

Step 3. If you identify programs you would like to remove, click on it then click Uninstall and follow the program-specific uninstallation instructions.

4. AVOIDING MALWARE ON WINDOWS

HOW TO VIEW HIDDEN AND OPERATING SYSTEM FILES

Some malware hides itself as well as your documents as hidden files then creates shortcuts with names identical to your original documents which, when opened, redirect to the virus file and infects your computer. This is a particularly common attack on removable flash drives. To improve your ability to recognise infected file, you may change Windows settings to view hidden and operating system files.

Step 1. Open the File Explorer .

Step 2. Click the View menu tab and then click Options

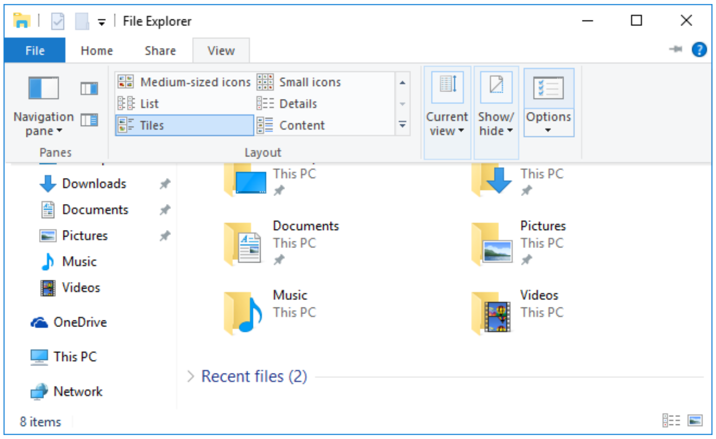


Figure 1: Windows 10 File Explorer View tab

WINDOWS FULL-DISK ENCRYPTION WITH BITLOCKER

Having a password to login to your Windows computer account is good first step but not enough to protect the files stored on this account. An attacker with physical access to the computer can read user files unless they are encrypted. BitLocker is built-in full disk encryption software offered by Microsoft in Windows 7 Enterprise, Windows 8 Pro, and most versions of Windows 10 (excluding Home version). Bitlocket can encrypt entire system disk of the computer, additional hard disks or partitions, and removable storage media.

Important: Steps below will help you encrypt your files. Without the correct password there will be no way to recover those files. Make a secure backup of your files before encrypting the files. Follow the below steps mindfully. Maintain a copy of your recovery key in a safe location (see below).

5.1. HOW TO ENCRYPT THE HARD DRIVE CONTAINING YOUR OPERATING SYSTEM

Step 1. Open This PC in the File Explorer, right-click your Local Disk (C:) and click Turn BitLocker on.

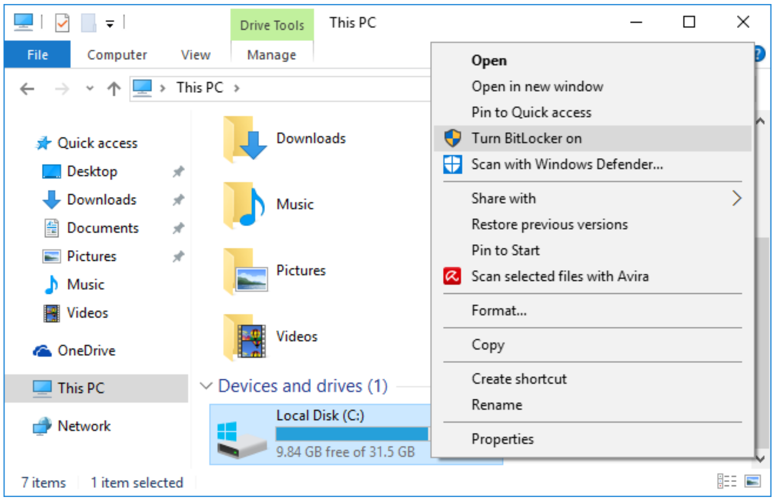


Figure 1: Right-click menu on system drive on Windows computer with BitLocker

Note: If you cannot find Turn BitLocker on in the menu above maybe you using a version of Windows which does not offer BitLocker. Consider upgrading your copy of Windows. Or see section 5.2. Alternatives to BitLocker below.

Note: in this example we assume that your Windows operating system is installed on drive C:

Important: If you see an error message This device can't use a Trusted Platform Module go to section In case of error "This device can't use a Trusted Platform Module" below.

INTRODUCTION TO MOBILE PHONES

Smartphones are one of the most empowering technologies to which most people in the world have access. At the same time, they are bristling with sensors, nearly always within arms reach and usually connected to some network or another. In short, they face most of the security challenges we associate with computers, plus a number of additional threats related to portability, ubiquity, insecure network architecture, location tracking, media capture and other such considerations.

OPERATING SYSTEMS

Most smartphones run one of two operating systems: Google's Android or Apple's iOS. Android devices are sold by many different companies. Their software is often modified by their manufacturers and by service providers who hope — and sometimes require — that their owners will rely on (and pay for) access to their mobile phone networks. iOS works only on Apple devices and makes it much more difficult to run applications that have not been approved by Apple.

The reliability of operating system updates is one of the most important considerations when buying an Android smartphone. Some cheaper models do not provide access to updates that are needed to fix important security flaws. This could leave you vulnerable to malware or other attacks.

BRANDED AND LOCKED SMARTPHONES

Smartphones are often sold locked to a specific carrier or mobile network operator. This means that the specific smart phone will only work with that company's SIM card. Mobile network operators often customise the operating system and install additional software on locked smartphones. They may also disable some functionality. This could leave you with apps on your smartphone that you cannot uninstall or prevent from accessing your information, including your contacts and storage.

For these reasons, it is usually safer to buy an unlocked smartphone that is not locked to a particular mobile provider. Unfortunately, these are often more expensive.

BASIC SECURITY SETUP

Smartphones have a number of settings that can help you manage the security of the device. It is important to pay attention to how your smartphone is set up. The Tool Guide below suggests a few specific Android settings and applications:

INSTALLING, EVALUATING AND UPDATING APPLICATIONS

The easiest — and typically the safest — way to install new software on your smartphone is to use Google's Play store for Android or Apple's App Store for iOS devices. Sign in from your device and you can download and install applications.

You can find Android apps in various places online, but you should generally avoid installing them. Some of these apps contain malware. You can learn more about malware in the Tactics Guide on how to Protect your device from malware and phishing attacks.

For experienced Android users, and for those who are unable or unwilling to rely on Google's Play Store,

Even "official" apps sometimes behave poorly. On Android devices, each application must ask your permission before it will be permitted to do certain things.

Remember to keep all of your apps up-to-date and to uninstall apps that you no longer use. App developers sometimes sell their apps to other people. A new owner could alter an app that you have already installed and push a malicious update.

MOBILITY AND THE VULNERABILITY OF INFORMATION

The mobile phones we carry around with us often contain sensitive information. Call logs, browser histories, text and voice messages, address books, calendars, photos and other useful functions can become liabilities if the device on which they are stored is lost or stolen. It is important to be aware of the sensitive information on your mobile phone as well as the online data to which it grants automatic access. These data have the potential to endanger not only the device's owner, but everyone who appears in their address book, inbox or photo album.

Once you have thought through the possible risks and familiarised yourself with the privacy and security features supported by your device, you can start putting safeguards in place.

STORING INFORMATION ON YOUR SMARTPHONE

Modern smartphones have a lot of room to store data. Depending on the device, however, it may be quite easy for anyone with physical access to extract that information.

DEVICE AND DATA ENCRYPTION

Recent iOS devices have strong encryption turned on by default, as long as you set a strong passcode. Android supports device encryption as well, and you should enable it if you can. Remember to back up the contents of your smartphone before turning on full disc encryption in case there is a problem while the phone is encrypting itself.

When you turn on an encrypted phone and enter your passcode, it allows you to access and modify the content on it.

As usual, there are trade-offs. If you believe you might need the ability to make an emergency call on short notice, for example, it might be worth taking the risk of leaving your phone powered on and just locking the screen.

RECORDING PASSWORDS SAFELY

You can store most of your passphrases in a single, encrypted file on an Android device by installing a FOSS tool called KeePassDroid. This app allow you to remember a single, strong master passphrase and use it to lookup your other passphrases. This, in turn, makes it possible to choose strong, unique passphrases, for all of your accounts, without having to memorise them. KeePassDroid also provides a random password generator you can use when creating new accounts.

There is a similar tool for iOS devices called MiniKeePass.

BEST PRACTICES FOR PHYSICAL PHONE SECURITY

Restricting physical access to your mobile phone is the first line of defence for the information it contains. You should keep it on you at all times, except where doing so presents a specific security risk. This applies to SIM cards and flash memory cards, as well. Even if you are concerned about malware or advanced surveillance, it may be safer to remove the battery and keep the device with you rather than leaving it unattended.

In addition to turning on encryption and keeping your phone nearby, below are a some additional steps you can take to maintain the physical security of your mobile device and limit the damage if it is lost or stolen.

GENERAL STEPS

- Always set a strong screen lock code and avoid sharing it with others. If you are using a basic phone that came with a default lock code, change it.

- Avoid storing sensitive information, including phone numbers, on a SIM card, as they cannot be encrypted.

- Regularly backup important data from your phone on your computer or on an external storage device. Store these backups securely as described in How to protect the sensitive files on your computer. Having a backup will help you remember what information is on your phone and make it easier for you to restore it to its factory settings in an emergency.

- Phone numbers are often linked to important accounts, and it is sometimes possible for an attacker to take over your phone number to gain access to those accounts or to impersonate you. Some mobile network providers allow you to set a PIN or password on your account to prevent unauthorised people from making changes to your account or stealing your phone number. You should take advantage of this feature if it is available.

- If you are concerned about malware, consider placing a small, removable sticker over your phone's cameras.

STEPS RELATED TO LOSS AND THEFT

Mobile phones have a 15-digit International Mobile Equipment Identity (IMEI) number that helps identify them on mobile networks. Changing SIM cards does not change your IMEI. This number is often printed behind the battery, and most phones will display it in their Settings or if you dial *#06#. Make a note of this number, as it could help you prove that you are the owner if your phone is stolen.

Consider the advantages and disadvantages of registering your phone with your service provider. If you report a registered phone stolen, your service provider can usually disable it. However, registering your phone may associate it more strongly with your actual identity.

Most Android phones and iPhones have a built-in anti-theft or "Find my Phone" feature that allows you to track or disable your phone if it is stolen. There are also third party tools that do the same thing. These tools involve trade-offs, but if you trust those who operate the service (and the quality of their software), you might want to enable one and practice using it.

STEPS TO TAKE WHEN GIVING YOUR DEVICE TO SOMEONE ELSE

When disposing of, giving away or selling a phone, make sure you do not also hand over the information stored on its SIM card or on a flash memory card. These storage devices may contain information even if they are expired or no longer working. Dispose of SIM cards by physically destroying them. Remove and keep (or destroy) flash memory cards. The best way to protect data on the phone itself is make sure it is encrypted and then reset the device to its "factory settings."

Try to use trusted phone dealers and repair shops. This reduces the vulnerability of your information when getting second-hand hand phones or having your phone repaired. If you think someone might have the access, resources or motivation to target you by pre-installing malware on your device before you buy it, consider choosing an authorised phone dealer at random.

Remove your SIM card and flash memory cards if you take your phone to a repair shop to be serviced.

ABOUT THE INTERCEPTION OF PHONE CALLS AND TEXT MESSAGES

Mobile networks are typically private networks run by commercial entities. Sometimes your service provider owns the mobile network infrastructure and sometimes it resells mobile service that it rents from another company. SMS text messages are sent unencrypted, and phone calls are either unencrypted or weakly encrypted. Neither are encrypted in a way that would protect them from the network itself. As a result, both your service provider and the owner of the cell towers you are using have unlimited access to your calls, text messages and location. In many cases, the local government has the same access, even in places where it does not own the infrastructure itself.

COMMUNICATING OVER THE INTERNET ON YOUR MOBILE PHONE

As discussed in our Tactics guides on how to keep your online communication private and on how to remain anonymous and bypass censorship on the Internet, sending information to and receiving data from the Internet can leave traces that identify who you are, where you are and what you are doing. Nevertheless, some Android and iOS tools that rely on the Internet to communicate are far safer than using the mobile network to place a voice call or send an SMS text message.

USING SECURE MESSAGING APPS

As mentioned above, phone calls and SMS text messages are quite insecure. Voice over IP (VoIP) is a way of making voice calls using an Internet connection rather than a mobile phone network. Text communication can also be sent over the Internet, and there are a number of modern messaging apps that use encryption to do both securely.

Below are some criteria that you might consider when choosing a mobile messenger app:

- What do digital security experts say about it?
- Is it Free and Open Source Software?
- Does it support end-to-end encryption one-on-one communication?
- Does it support end-to-end encrypted group text communication?
- Does it support end-to-end encrypted group voice communication?
- Are file transfers end-to-end encrypted?

- Can you set your messages to "self destruct?"
- Will it work over a low bandwidth network connection?
- Who are the developers, and do you trust them?
- Who operates the server and what information do they claim to store about your calls and messages?
- Does it work on
- Can you use the same account on multiple devices?
- Does it work on all major operating systems?
- Does it allow you to register with an email or a username, rather than an phone number, so that you can separate your contact information from your actual identity?
- Can you use it without giving it access to the list of contacts on your device?
- Can you use it on a mobile device that is not a phone?
- Can you or someone you trust run your own server and use it to communicate?

SENDING AND RECEIVING EMAIL ON YOUR SMARTPHONE

If you choose to access a potentially sensitive email account on a mobile device, you should make sure that device encryption is enabled, as discussed in the basic Security for Android guide. (Recent iPhones should have it turned on by default as long as you set a strong passcode.) This will not protect your emails in transit but it will prevent someone who finds or steals your device from reading them. You might also want to read the Tactics Guides on how to keep your online communication private.

The above guide covers GPG email encryption on Windows, Mac and Linux computers. There are ways to send and receive encrypted email on Android devices, as well, but they come with trade-offs. (There are currently no free GPG encryption tools for iOS.)

Most security experts advise against storing your private encryption key anywhere but on your primary computer. (To say nothing of carrying it around in your pocket.) And you will need that private key to read encrypted emails on your mobile device. Android devices are more secure than they used to be, however, and your private key is itself be protected by a strong passphrase. As such, if you must send and receive sensitive email on your Android device — and if switching to a secure mobile messaging app is not an option — you might want to install GPG on it.

To do so, you will need to:

- Install and configure a GPG and key management app like OpenKeychain;
- Copy your encrypted private key to the device; and
- Install and configure an email app, like K-9 Mail, that works with OpenKeychain.

BEYOND CALLS AND MESSAGES

Mobile phones are full featured computing devices, complete with their own operating systems and downloadable applications that provide various services to the user. Much of what you can do on a computer, you can now do on a smartphone. And, of course, there are plenty of things you can do on a smartphone that you cannot do on a computer.

BROWSING THE WEB ON YOUR MOBILE PHONE

While some basic mobile phones still lack Internet connectivity, this is increasingly rare. If you use the Web browser on your Android device to visit potentially sensitive websites, consider installing a virtual private network (VPN) or Orbot, which is the Android version of the Tor Browser.

GENERAL PURPOSE BEST PRACTICES FOR MOBILE PHONES

- Only connect your phone to a computer if you are sure it is free of malware. See our Tactics Guide on how to protect your computer from malware and phishing attacks.
- Just as you would when using a computer, be wary when connecting to a WiFi access point that does not ask for a password.
- Disable WiFi, Bluetooth, and Near Field Communication (NFC) when you are not using them. Switch them on only when they are required and use them only on trusted networks and when interacting with trusted devices. Transfer data using a cable connection when possible.
- Observe your phone's behaviour and functioning. Look out for unknown programmes and running processes, strange messages and unstable operation. If you don't know or use some of the features and applications on your phone, disable or uninstall them if you can.

SECURITY-RELATED SETTINGS FOR ANDROID

ACCESS TO YOUR PHONE

Enable Lock SIM card, found under Settings -> Personal -> Security -> Set up SIM card lock. This will mean that you must enter a PIN number in order to unlock your SIM card each time your phone is switched on, with out the PIN no phone calls can be made.

DEVICE ENCRYPTION

If your device uses Android version 4.0 or newer, you should turn on device encryption. This can be done in Settings -> Personal -> Security -> Encryption. Before you can utilise device

NETWORK SETTINGS

Turn off Wi-Fi and Bluetooth by default. Ensure that Tethering and Portable Hotspots, under Wireless and Network Settings, are switched off when not in use. Settings -> Wireless &

LOCATION SETTINGS

Switch off Wireless and GPS location (under Location Services) and mobile data (this can be found under Settings -> Personal -> Location).

CALLER IDENTITY

If you want to hide your caller-ID, go to Phone Dialler -> settings -> Additional Settings -> Caller ID -> hide number.

SOFTWARE UPDATES

To ensure that you phone remains secure it is strongly recommended to keep your software updated. There are two types of updates that need to be checked:

APPS FOR ANDROID

RECOMMENDED ANDROID APPS

We have a number of Tools Guides for Android apps that we recommend installing on your device. These guides will walk you through installing, configuring and using the apps on your Android Devices.

- APG
- ChatSecure
- K-9 Mail and APG
- KeePassDroid
- Obscuracam
- Orbot
- Orweb

ADDITIONAL ANDROID APPS FOR NON-ROOTED DEVICES

- Applock
- Avira
- Cerberus
- Firefox
- Notecipher
- OpenVPN for Android
- Panic Button
- Psiphon3
- Spideroak
- Surespot

Adopted from: **https://securityinabox.org/en/guide/basic-security/windows/**

Which is licensed under a Creative Commons Attribution-Share Alike 3.0 Unported License.

iOS Security

How to Encrypt Your iPhone

If you have an iPhone 3GS or later, an iPod touch 3rd generation or later, or any iPad, you can protect the contents of your device using encryption. That means that if someone gets physical access to your device, they will also need your passcode to decrypt what's stored on it, including contacts, instant messages or texts, call logs, and email.

In fact, most modern Apple devices encrypt their contents by default, with various levels of protection. But to protect against someone obtaining your data by physically stealing your device, you need to tie that encryption to a passphrase or code that only you know. See below for instructions on how to do this.

On devices running iOS 4–iOS 7:

1. Open the General settings and choose Passcode (or iTouch & Passcode).
2. Follow the prompts to create a passcode.

On device running iOS 8-iOS 11:

1. Open the Settings app
2. Tap Touch ID & Passcode
3. Follow the prompts to create a passcode.

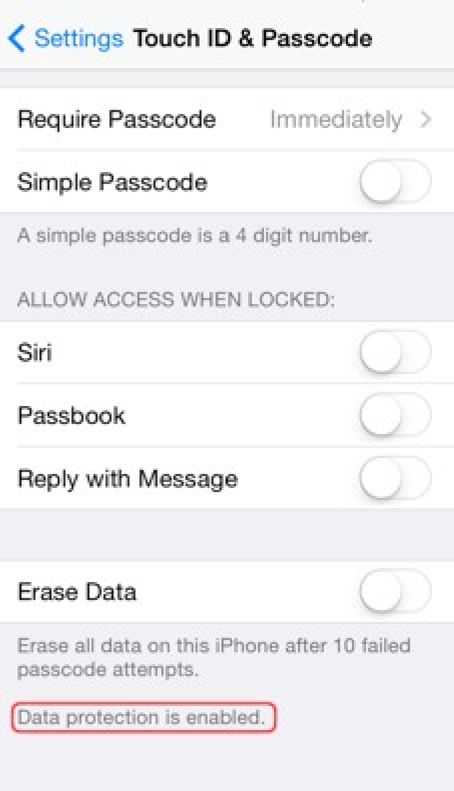
If your device is running iOS 8, disable Simple Passcode to create a code that is longer than 4 digits. With the release of iOS 9, Apple defaulted to a 6-digit passcode.

If you choose a passcode that's all-numeric, you will get a numeric keypad when you need to unlock your phone, which may be easier than typing a set of letters and symbols on a tiny virtual keyboard. However, we suggest choosing a passcode that's alphanumeric, and longer than 6 characters because it's simply harder to crack, even if Apple's hardware is designed to slow down password-cracking tools.

To customize your passcode, select "Passcode Options" and "Custom Alphanumeric Code." If you want to customize an existing passcode, select “Change Passcode” and then “Passcode Options.” You should also set the “Require passcode” option to “Immediately,” so that your device isn't unlocked when you are not using it.

Once you've set a passcode, scroll down to the bottom of the Passcode settings page. You should see a message that says “Data protection is enabled.” This means that the device's encryption is now tied to your passcode, and that most data on your phone will need that code to unlock it.

How to Encrypt Your iPhone 1



< Settings Touch ID & Passcode

Require Passcode Immediately >

Simple Passcode ○

A simple passcode is a 4 digit number.

ALLOW ACCESS WHEN LOCKED:

Siri ○

Passbook ○

Reply with Message ○

Erase Data ○

Erase all data on this iPhone after 10 failed passcode attempts.

Data protection is enabled.

Here are some other iOS features you should think about using if you're dealing with private data:

- iTunes has an option to backup your device onto your computer. iTunes doesn't encrypt your backups by default. If you choose the “Encrypt backup” option on the Summary tab of your device in iTunes, iTunes will backup more confidential information (such as Wi-Fi passwords and email passwords), but will encrypt it all before saving it onto your computer. Be sure to keep the password you use here safe: restoring from backups is a rare event, but extra painful if you cannot remember the password to unlock the backup in an emergency.
- If you back up to Apple's iCloud, you should use a long passphrase to protect the data, and keep that passphrase safe. While Apple encrypts most data in its backups, it may be

possible for the company to obtain access for law enforcement purposes since Apple also controls the keys used for iCloud encryption.

- If you turn on data protection as described above, you will also be able to delete your data on your device securely and quickly. In the Touch ID & Passcode settings, you can set your device to erase all its data after 10 failed passcode attempts. If you do this be sure your phone is backed up in case someone purposefully enters your passcode incorrectly.
- According to Apple's old Law Enforcement Guide, "Apple can extract certain categories of active data from passcode locked iOS devices. Specifically, the user generated active files on an iOS device that are contained in Apple's native apps and for which the data is not encrypted using the passcode ("user generated active files"), can be extracted and provided to law enforcement on external media. Apple can perform this data extraction process on iOS devices running iOS 4 or more recent versions of iOS. Please note the only categories of user generated active files that can be provided to law enforcement, pursuant to a valid search warrant, are: SMS, photos, videos, contacts, audio recording, and call history. Apple cannot provide: email, calendar entries, or any third-party App data."

The above information applies only to iOS devices running versions of iOS prior to 8.0.

- Now, Apple states that "For all devices running iOS 8.0 and later versions, Apple is unable to perform an iOS device data extraction as the data typically sought by law enforcement is encrypted, and Apple does not possess the encryption key."

REMEMBER: While Apple will be unable to extract data directly off a phone, if the device is set to sync with iCloud, or backup to a computer, much of the same data will indeed be accessible to law enforcement. Under most circumstances, iOS encryption is only effective when a device has been fully powered down (or freshly-rebooted, without being unlocked). Some attackers might be able to take valuable data from your device's memory when it's turned on. (They might even be able to take the data when it has just been turned off). Keep this in mind and, if possible, try to make sure your device is powered off (or rebooted and not unlocked) if you believe it's likely to be seized or stolen. At the time this guide was published, a few companies claimed they were able to break the passcodes of iPhones for law enforcement, but details surrounding these claims are unclear.

- If you are concerned about your device getting lost or stolen, you can also set up your Apple device so that it can be erased remotely, using the "Find My iPhone" feature. Note that this will allow Apple to remotely request the location of your device at any time. You should balance the benefit of deleting data if you lose control of your device, with the risk of revealing your own position. (Mobile phones transmit this information to telephone companies as a matter of course; Wi-Fi devices like iPads and the iPod Touch do not.)

Adopted from:https://ssd.eff.org/en/module/how-encrypt-your-iphone

Further Reading/ Viewing:
https://www.youtube.com/watch?v=SKBR1CaP80U
https://www.youtube.com/watch?v=k2kpCvLunXk
https://www.youtube.com/watch?v=TPA9IiRqLNY
https://www.youtube.com/watch?v=QSwQhuAdDxM
https://www.zerofox.com/social-media-security/
https://searchsecurity.techtarget.com/feature/Social-Media-Security
https://www.bullguard.com/bullguard-security-center/internet-security/social-media-dangers/social-media-security-abc.aspx

Further Reading/Viewing:
https://fraudwatchinternational.com/social-media/social-media-security-best-practices/
https://blog.hootsuite.com/social-media-security-for-business/
https://www.adweek.com/digital/5-social-media-threats/
https://www.youtube.com/watch?v=G5aBp2FlpBw
https://www.youtube.com/watch?v=W726-whX33c

Adopted from: https://securityinabox.org/en/guide/social-networking/web/

Adopted from:https://ssd.eff.org/en/module/how-encrypt-your-iphone