

- 1.1. 6. Securing Windows 10 devices -

Computer attacks continue to increase in number and severity each year.

Whether it's to steal your valuable personal data or hold it for ransom, appropriate your computing resources and bandwidth, or use your PC as a pathway into a bigger target with whom you do business, there are plenty of actors with bad intent.

Securing your computer: A defense-in-depth strategy

A multidimensional threat landscape requires a multilayered approach to protecting your PC and your network.

The big-picture goal is to secure your device, secure your data, secure your identity, and block malware.

On a home or small business network, those layers of security include the following:

- Use a hardware router to protect your broadband connection. This is an essential part of physical security, even if your network consists of a single PC.
- Enable a software firewall, and keep it turned on. You can use Windows Firewall, which is included with Windows 10, or a third-party firewall such as those included with security suites.
- Use biometric sign-in. Biometric sign-in using a fingerprint reader or facial recognition with Windows Hello offers much more than convenience. Because biometric sign-in is linked to a specific device, it provides effective two-factor authentication. If you don't have the necessary hardware, use a PIN or picture password for sign-in—both of which can be more secure than a traditional password.
- Set up standard user accounts, and keep User Account Control enabled. Standard accounts help to prevent (or at least minimize) the damage that an untrained user can do by installing untrusted programs. User Account Control (UAC) helps in this regard by restricting access to administrative tasks and virtualizing registry and file-system changes.
- Keep Windows and vulnerable programs up to date. Windows Update handles this chore for Windows, Office, and other Microsoft programs. You're on your own for third-party programs.
- Use an antimalware program, and keep it up to date. Windows Defender, which is included with Windows 10, provides antimalware protection, but many third-party solutions are also available.
- Protect yourself from threats in email messages. At a minimum, your email solution should block or quarantine executable files and other potentially dangerous attachments. In addition, effective antispam features can block scripts and prevent phishing attempts.

- Use parental controls to keep kids safe. If you have children who use your computer, family safety features in Windows can help you keep them away from security threats and keep them from wandering into unsafe territory online by restricting their computer activities in other ways.

The most important protective layer—and the one that's most easily overlooked—is user education and self-control.

Everyone who uses a computer must have the discipline to read and evaluate security warnings when they're presented and to allow the installation only of software that is known to be safe.

Although a user with a standard account can't install or run a program that wipes out the entire computer, he can still inflict enough damage on his own user profile to cause considerable inconvenience.

Countless successful malware attacks worldwide have proven that many users do not have adequate awareness of safe computing methods.

New security features in Windows 10

Because the bad guys are always upping their game, a hallmark of each new version of Windows is a number of new and improved security features.

Windows 10 is no exception.

Here we enumerate changes available in Windows 10.

Securing data

The increased mobility of PCs also increases the risk of theft.

Losing a computer is bad enough, but handing over all the data you've stored on the computer is by far the greater loss.

Windows 10 includes new features to ensure the thief can't get your data.

- Device encryption. On devices that support InstantGo, data on the operating system volume is encrypted by default. Formerly called Connected Standby, InstantGo is a Microsoft hardware specification that enables advanced power-management capabilities. Among other requirements, InstantGo devices must boot from a solid state drive. The encryption initially uses a clear key, but when a local administrator first signs in with a Microsoft account, the volume is automatically encrypted. A recovery key is available when you sign

in using that Microsoft account at <https://onedrive.com/recoverykey>; you'll need the key if you reinstall the operating system or move the drive to a new PC.

- BitLocker Drive Encryption. BitLocker Drive Encryption offers similar (but stronger) whole-volume encryption, and on corporate networks it allows centralized management. In Windows 10, BitLocker encrypts drives more quickly than in previous Windows versions; additional speed comes from the new ability to encrypt only the part of a volume in use.

Securing identities

It seems like every week we hear about another data breach where millions of user names and passwords have been stolen.

There's a thriving market for this type of information because it enables the thieves to sign in anywhere using your credentials.

Furthermore, because many people use the same password for different accounts, criminals can often use the stolen information to gain unauthorized access into a theft victim's other accounts.

Windows 10 marks the beginning of the end of passwords.

With Windows 10, enterprise-grade two-factor authentication is built in.

After enrolling a device with an authentication service, the device itself becomes one factor; the second factor is a PIN or a biometric, such as a fingerprint, facial recognition, or an iris scan.

After Windows Hello signs you in, it enables sign-in to networks and web services.

Windows Hello supports Microsoft accounts, Active Directory and Azure Active Directory (Azure AD) accounts, and any identity provider that supports the Fast ID Online (FIDO) v2.0 standard.

Your biometric data remains securely stored in your computer's TPM; it's not sent over the network.

With this combination of authentication methods, an attacker who has a trove of user names and passwords is stymied.

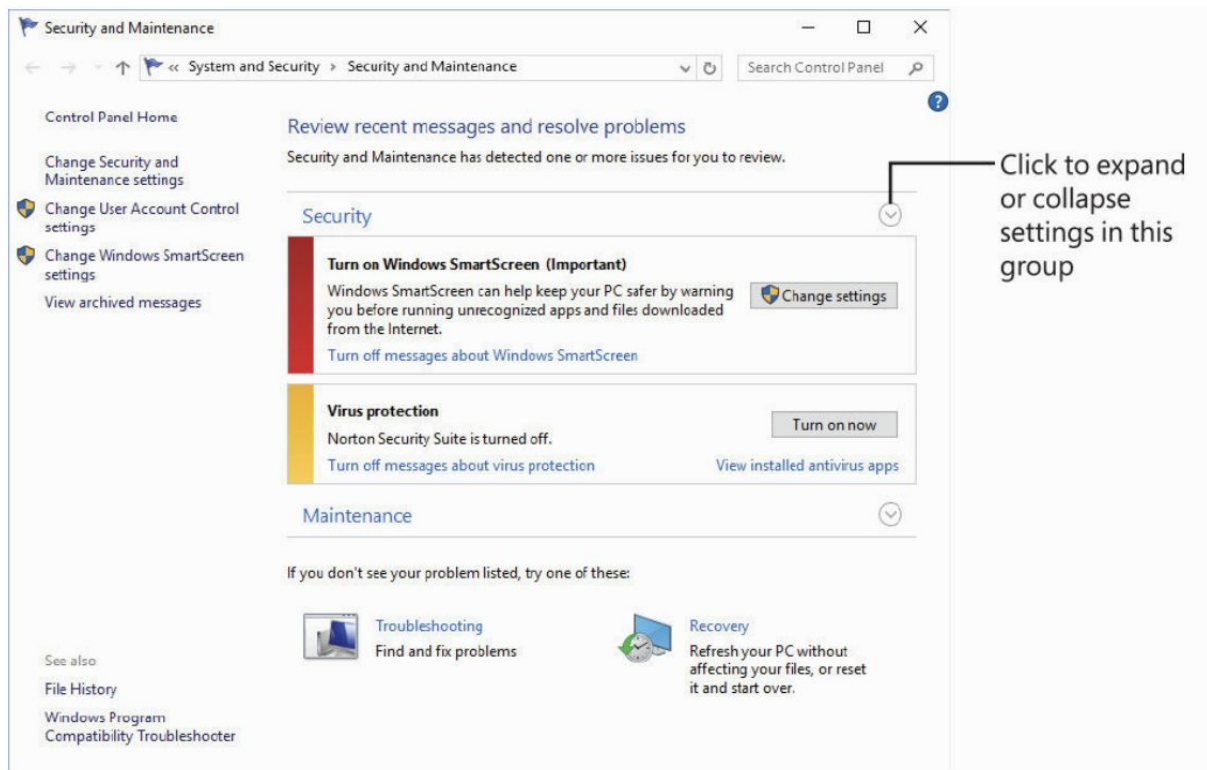
To unlock your encrypted information (and, by extension, gain the ability to sign in to your web services), he needs the enrolled device.

And a thief who steals your computer needs your PIN or biometric data.

Active Directory, Azure Active Directory, and Microsoft accounts support this new form of credentials; other services are sure to follow.

Monitoring your computer's security

In Windows 10, security-related options are available in one location when you go to Control Panel > System And Security > Security And Maintenance, shown in the following figure:



The Security section in "Security And Maintenance" provides at-a-glance information about your security settings.

Items that need your attention have a red or yellow bar, as shown in the previous figure.

A red bar identifies important items that need immediate attention, such as detection of a virus or spyware or that no firewall is enabled.

A yellow bar denotes informational messages about suboptimal, but less critical, settings or status.

Next to the bar appear explanatory text and buttons you can use to correct the problem (or configure "Security And Maintenance" so that it won't bother you).

"Security And Maintenance" is designed to work with third-party firewall, antivirus, and antispyware programs, as well as with the programs built in to Windows (Windows Firewall and Windows Defender).

Staying on top of security updates

Perhaps the most important step in keeping your system secure is to be sure you stay current with updates to Windows and other programs.

Microsoft issues frequent updates that provide replacements for installed device drivers as well as fixes to code that has been found to be faulty.

Some updates provide new features or enhanced performance, while others patch security holes.

To install updates automatically, Windows uses Windows Update, accessible via Settings > Update & Security > Windows Update.

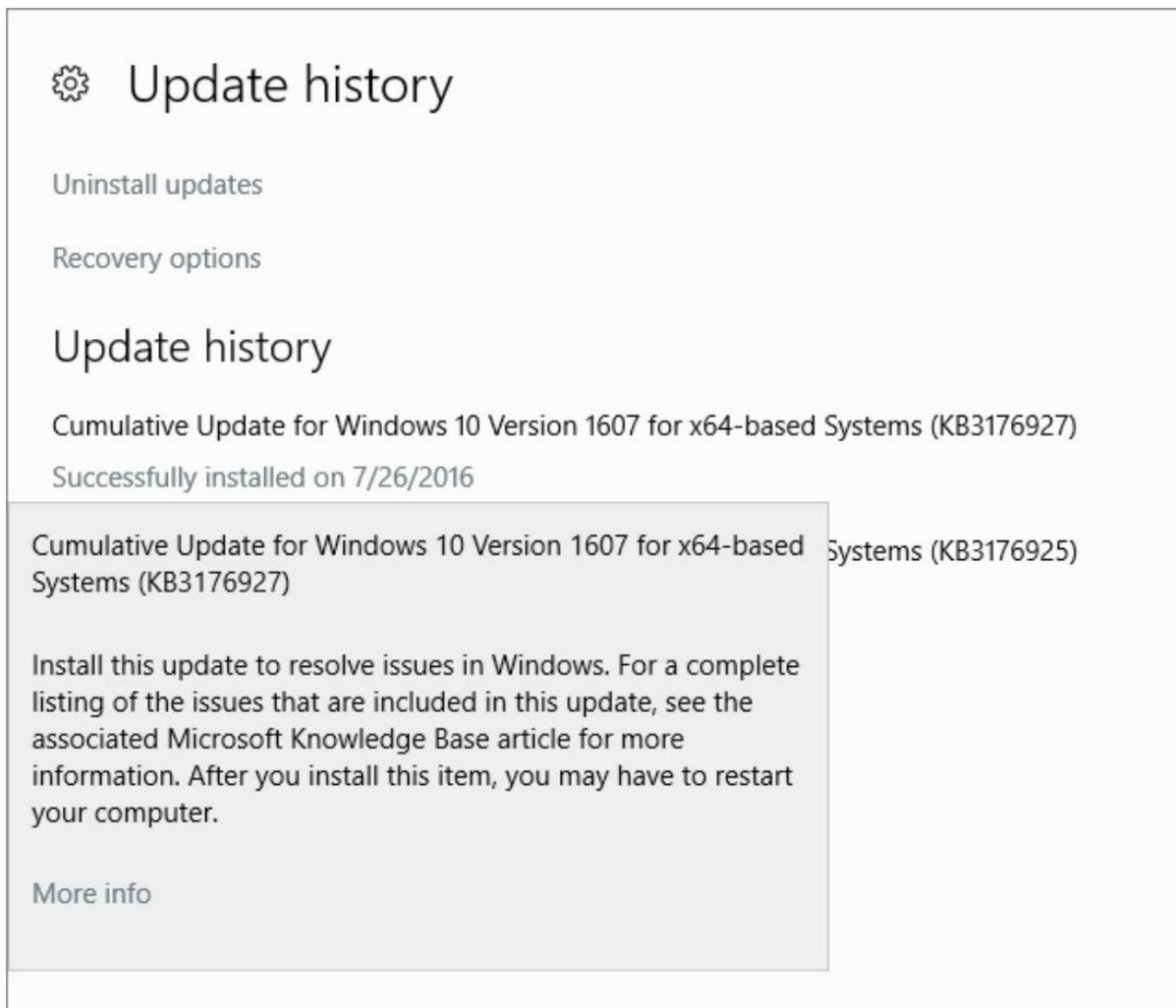
You might be interested in knowing more about current security threats, including those addressed by Windows Update: what, exactly, is the threat? How serious is it? What workarounds are available?


The Microsoft Security Response Center publishes detailed information, in the form of security bulletins, about the threat and the response.

Each cumulative update has its own Knowledge Base (KB) article, identified by a seven-digit KB number.

To see the KB number for an installed update, click Update History.

Click the installation link below any item for a brief description of it, and then click "More Info" to go to the associated KB article.



 **Update history**

Uninstall updates

Recovery options

Update history

Cumulative Update for Windows 10 Version 1607 for x64-based Systems (KB3176927)

Successfully installed on 7/26/2016

Cumulative Update for Windows 10 Version 1607 for x64-based Systems (KB3176925)
Systems (KB3176927)

Install this update to resolve issues in Windows. For a complete listing of the issues that are included in this update, see the associated Microsoft Knowledge Base article for more information. After you install this item, you may have to restart your computer.

More info

That KB article, in turn, might contain a list of security updates and other fixes that are new in that cumulative update, each of which has its own KB article for additional information.

You can open any KB article directly by using the URL format <https://support.microsoft.com/kb/nnnnnnn/> and replacing nnnnnnn with the seven-digit number following “KB.”

Each security bulletin includes a rating of the threat’s severity.

These are the four ratings that are used, listed in order of severity (with the most severe first):

- **Critical.** A critical vulnerability can lead to code execution with no user interaction.
- **Important.** An important vulnerability is one that can be exploited to compromise the confidentiality or integrity of your data or to cause a denial-of-service attack.
- **Moderate.** A moderate vulnerability is one that’s usually mitigated by default settings and authentication requirements. In other words, you’d have to go a bit out of your way for one of these to damage your system or your data.

- Low. A vulnerability identified as low usually requires extensive interaction or an unusual configuration to cause damage.

Blocking intruders with Windows Firewall

Typically, the first line of defense in securing your computer is to protect it from attacks by outsiders.

Once your computer is connected to the internet, it becomes just another node on a huge global network.

A firewall provides a barrier between your computer and the network to which it's connected by preventing the entry of unwanted traffic while allowing transparent passage to authorized connections.

Using a firewall is simple, essential, and often overlooked.

You'll want to be sure that all network connections are protected by a firewall.

You might be comforted by the knowledge that your portable computer is protected by a corporate firewall when you're at work and that you use a firewalled broadband connection at home.

But what about the public hotspots you use when you travel?

And it makes sense to run a firewall on your computer even when you're behind a residential router or corporate firewall.

Other people on your network might not be as vigilant as you are about defending against viruses, so if someone brings in a portable computer infected with a worm and connects it to the network, you're toast—unless your network connection has its own firewall protection.

Windows includes a two-way, stateful-inspection, packet-filtering firewall called, cleverly enough, Windows Firewall.

Windows Firewall is enabled by default for all connections, and it begins protecting your computer as it boots.

The following actions take place by default:

- The firewall blocks all inbound traffic, with the exception of traffic sent in response to a request sent by your computer and unsolicited traffic that has been explicitly allowed by creating a rule.
- All outgoing traffic is allowed unless it matches a configured rule.

Using Windows Firewall with different network types

Windows Firewall maintains a separate profile (that is, a complete collection of settings, including rules for various programs, services, and ports) for each of three network types:

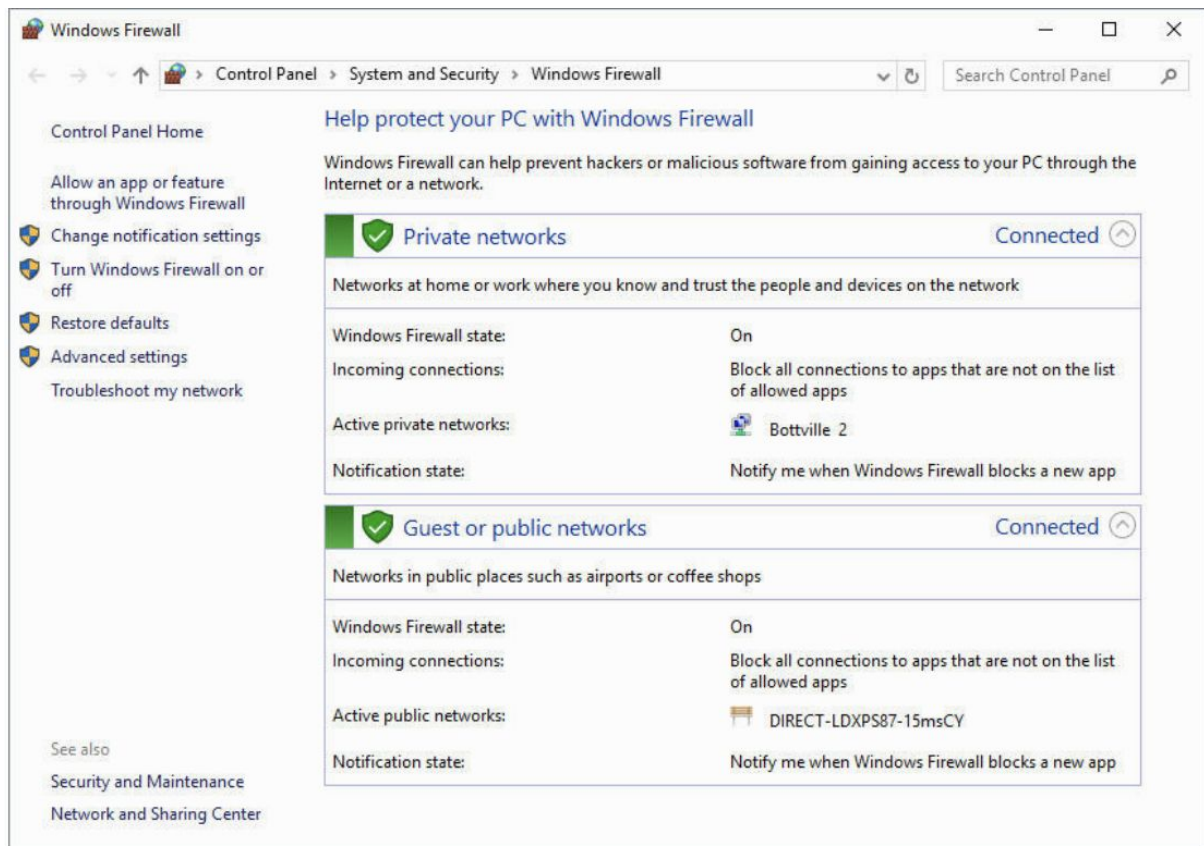
- Domain. Used when your computer is joined to an Active Directory domain. In this environment, firewall settings are typically (but not necessarily) controlled by a network administrator.
- Private. Used when your computer is connected to a home or work network in a workgroup configuration.
- Guest or public. Used when your computer is connected to a network in a public location, such as an airport or a library. It's common—indeed, recommended—to have fewer allowed programs and more restrictions when you use a public network.

Managing Windows Firewall

Windows Firewall is a Control Panel application that provides a simple interface for monitoring firewall status and performing routine tasks, such as allowing a program through the firewall or blocking all incoming connections.

To open Windows Firewall, type firewall in the search box or in Control Panel.

Click Windows Firewall to display a window similar to the one shown in the following figure:

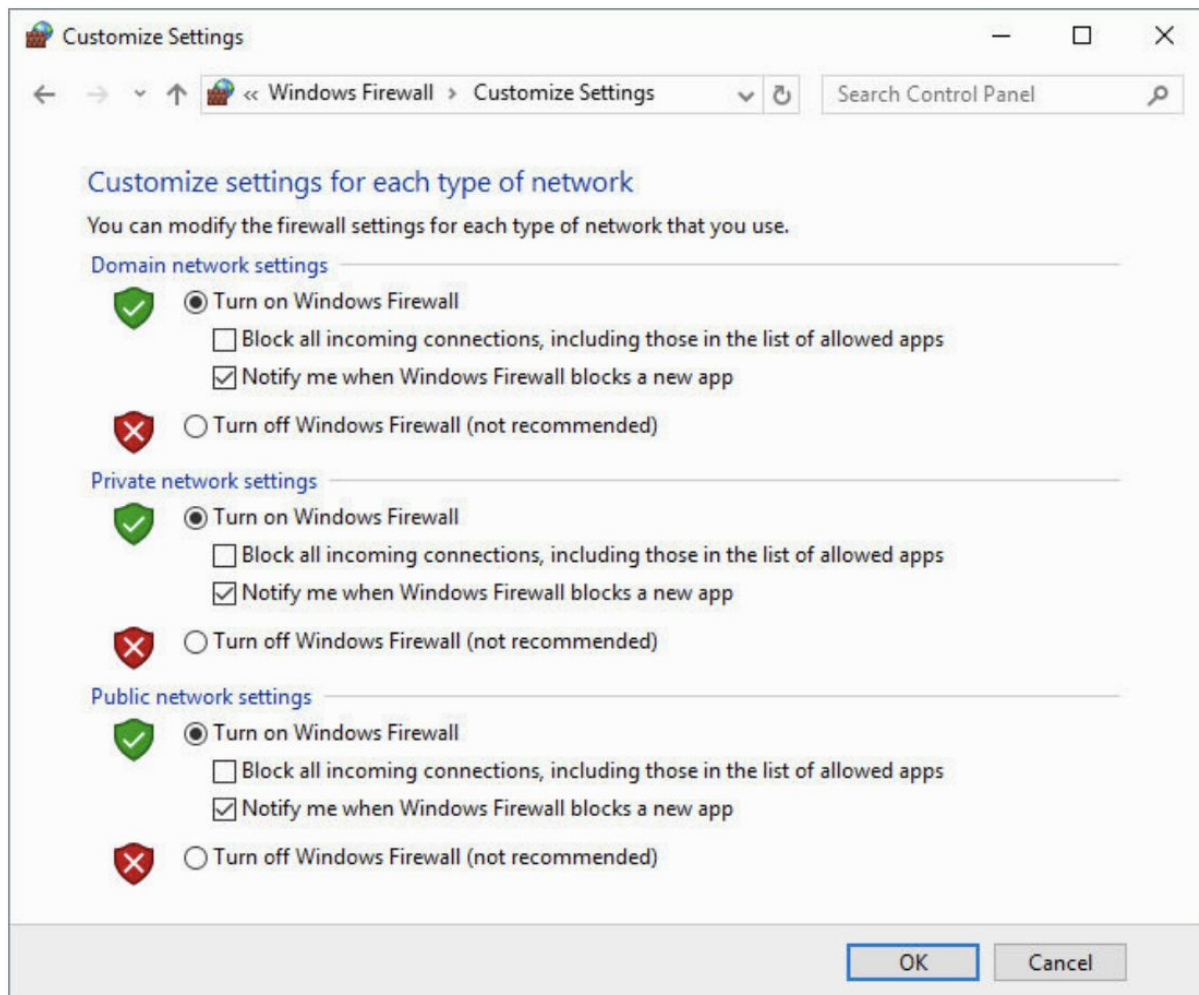


Enabling or disabling Windows Firewall

The main Windows Firewall application, shown in the previous figure, is little more than a status window and launch pad for making various firewall settings.

The first setting of interest is to enable or disable Windows Firewall.

To do that, click "Turn Windows Firewall On" or "Off" to open the screen shown in the next figure:



From here, you can enable (turn on) or disable (turn off) Windows Firewall for each network type.

In general, the only reason to turn off Windows Firewall is for brief (and extremely cautious) troubleshooting purposes, or if you have installed a third-party firewall that you plan to use instead of Windows Firewall.

Most compatible third-party programs perform this task as part of their installation.

As you'll discover throughout Windows Firewall, domain network settings are available only on computers that are joined to a domain.

You can make settings for all network types—even those to which you're not currently connected.

Settings for the domain profile, however, are often locked down by the network administrator using Group Policy.

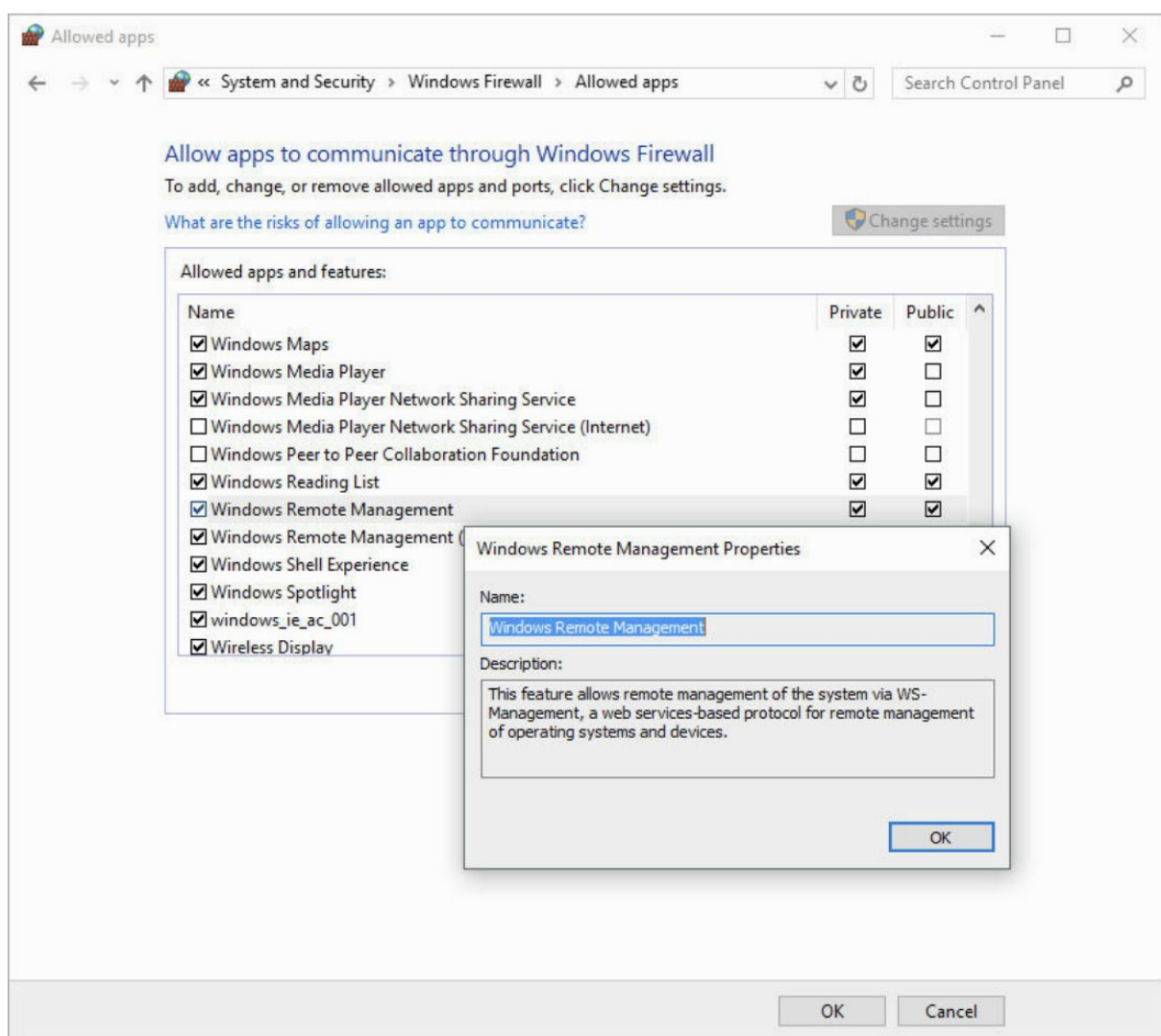
Allowing connections through the firewall

In some situations, you want to allow other computers to initiate a connection to your computer.

For example, you might use Remote Desktop, play multiplayer games, or chat via an instant messaging program; these types of programs typically require inbound connections so that others can contact you.

The simplest way to allow a connection for a program that does not create its own firewall rules is to click "Allow An App Or Feature Through Windows Firewall", a link in the left pane of the main Windows Firewall window.

The list of programs and features that initially appears in "Allowed Apps", shown in the next figure, depends on which programs and services are installed on your computer; you can add others.



In each of these cases, you enable a rule in Windows Firewall that pokes a small hole in the firewall and allows a certain type of traffic to pass through it.

Each rule of this type increases your security risk to some degree, so you should clear the check box for all programs you don't need.

If you're confident you won't ever need a particular program, you can select it and then click Remove.

Preventing unsafe actions with User Account Control

Widely scorned when it was introduced a decade ago as part of Windows Vista, User Account Control (UAC) intercedes whenever a user or program attempts to perform a system administrative task and asks for the consent of a computer administrator before commencing what could be risky business.

Since that rocky start, UAC has been tuned to become an effective security aid—without the annoyance factor that plagued the original implementation.

In Windows 10, user accounts you set up after the first one are standard (nonadministrator) accounts by default; although they can carry out all the usual daily computing tasks, they're prevented from performing potentially harmful operations.

These restrictions apply not just to the user; more importantly, they also apply to any programs launched by the user.

Even administrator accounts run as “protected administrator” accounts, which are allowed only standard-user privileges except when they need to perform administrative tasks: this is sometimes called Admin Approval Mode.

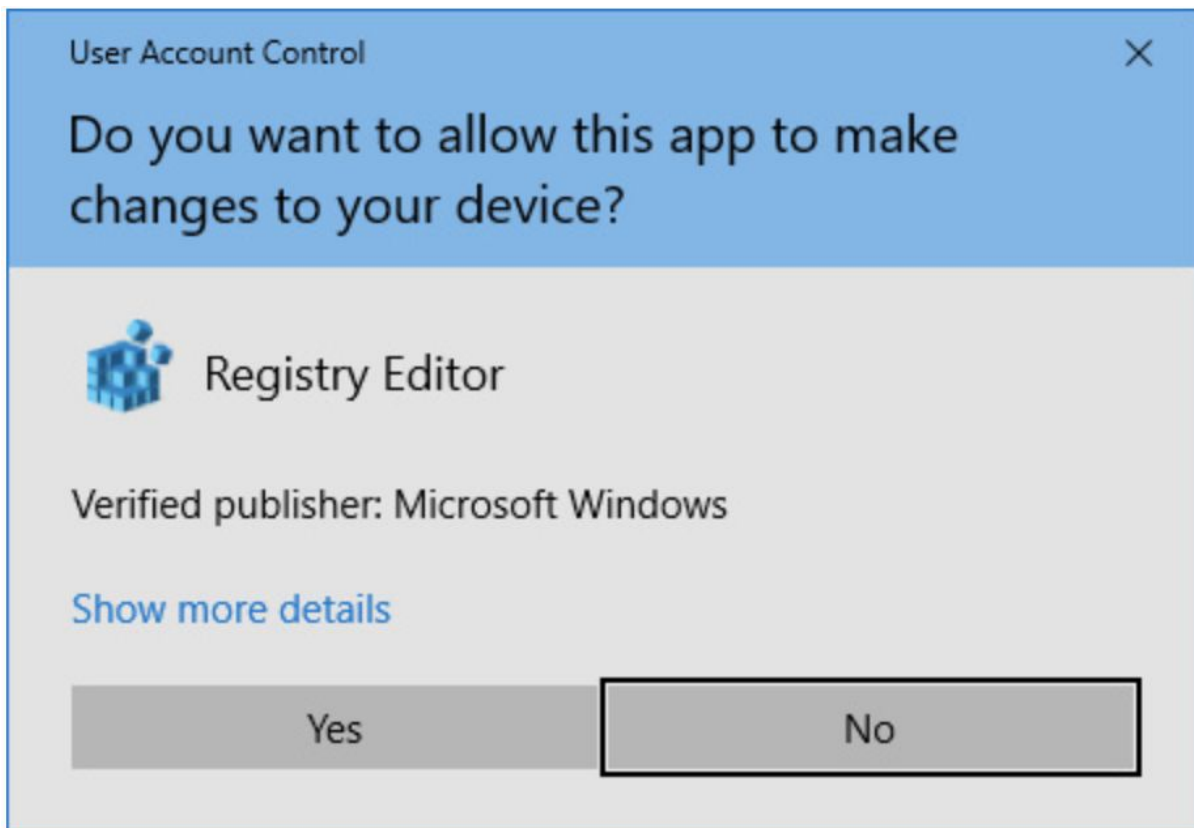
Most programs are written so that they don't require administrator privileges for performing everyday tasks.

Programs that truly need administrative access (such as utility programs that change computer settings) request elevation—and that's where UAC comes in.

Dealing with UAC prompts

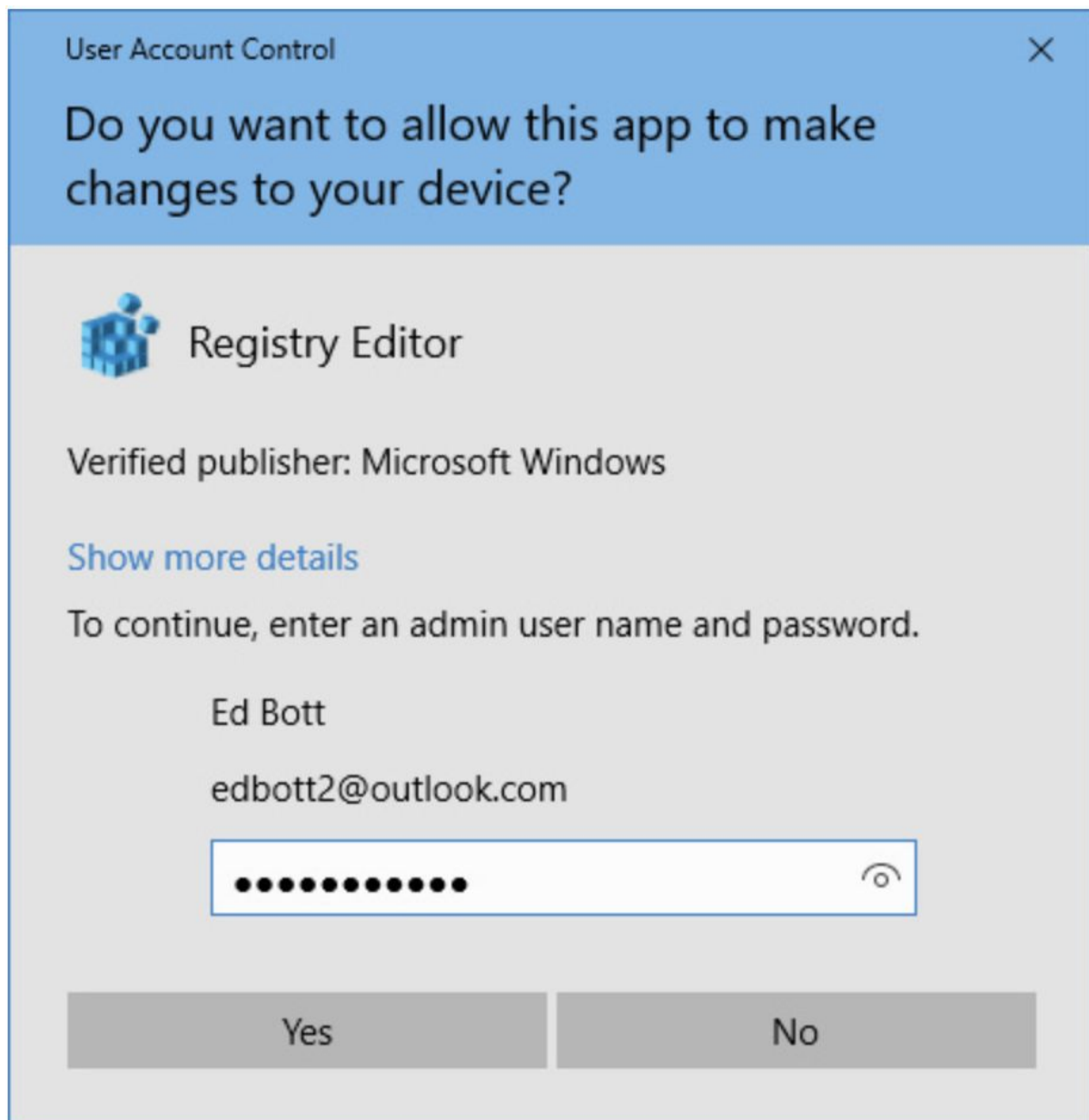
As an elevation-requesting application attempts to open, UAC evaluates the application and the request and then displays an appropriate prompt.

As an administrator, the most common prompt you're likely to see is the consent prompt, which is shown in the following figure:



Check the name of the program and the publisher, click "Yes" if you're confident that it's safe to proceed, and carry on.

If you use a standard account, any attempt to run a program that requires elevation displays the credentials prompt, which is shown in the next figure:

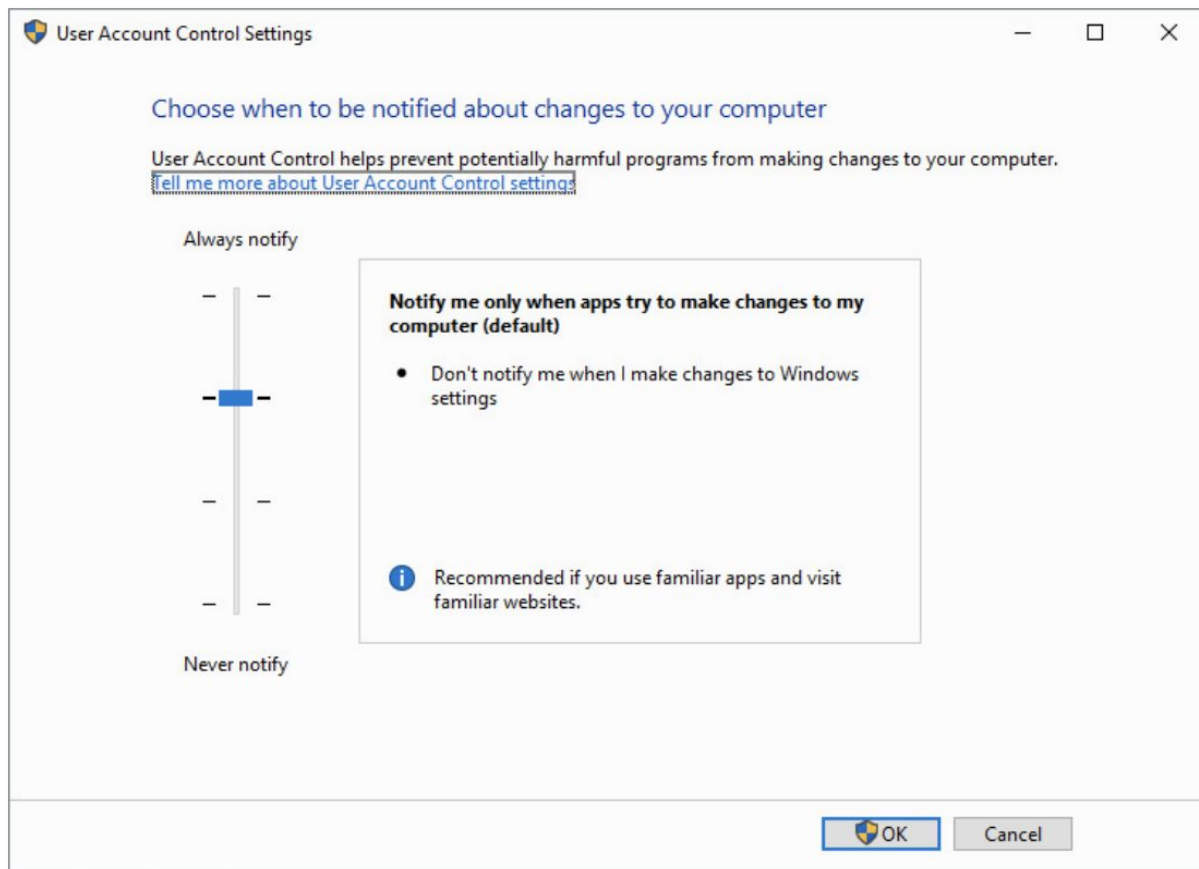


If the user is able to provide the credentials of an administrator (that is, user name and password, smart card, or biometric authentication, depending on how sign-in options are configured on the computer), the application opens using the administrator's access token.

Modifying UAC settings

To review your User Account Control options and make changes to the way it works, search for "uac" and then click "Change User Account Control Settings".

A window similar to the one shown in the next figure appears:



To make changes, move the slider to the position you want.

Be sure to take note of the advisory message in the bottom of the box as you move the slider.

Click OK when you're done—and then respond to the UAC prompt that appears!

Caution!

Don't forget that UAC is more than annoying prompts.

Only when UAC is enabled does an administrator run with a standard token.

Only when UAC is enabled does Internet Explorer run in a low-privilege Protected Mode.

Only when UAC is enabled does it warn you when a rogue application attempts to perform a task with system-wide impact.

And, of course, disabling UAC also disables file and registry virtualization, which can cause compatibility problems with applications that use fixes provided by the UAC feature.

For these reasons, we urge you not to select the bottom option in User Account Control Settings, which turns off UAC completely.

Encrypting information

Windows provides the following encryption tools for preventing the loss of confidential data:

- Encrypting File System (EFS) encodes your files so that even if someone is able to obtain the files, that person won't be able to read them. The files are readable only when you sign in to the computer using your user account.
- BitLocker Drive Encryption provides another layer of protection by encrypting entire hard-disk volumes. BitLocker reduces the risk of data being lost when a computer is stolen or when a hard disk is stolen and placed in another computer. A thief's standard approach in these situations is to boot into an alternate operating system and then try to retrieve data from the stolen computer or drive. With BitLocker, that type of offline attack is effectively neutered.
- BitLocker To Go extends BitLocker encryption to removable media, such as USB flash drives.

"Encrypting File System" and "BitLocker Drive Encryption" are not available in Windows 10 Home.

Encrypting a removable drive with "BitLocker To Go" requires that you be running Windows 10 Pro, Enterprise, or Education; the resulting encrypted drive can be opened and used on a device running Windows 10 Home (or, for that matter, any edition of Windows 7 or later).

Using the Encrypting File System

EFS ("Encrypting File System") provides a secure way to store your sensitive data.

Windows creates a randomly generated File Encryption Key (FEK) and then transparently encrypts the data, using this FEK, as the data is being written to disk.

Windows then encrypts the FEK using your public key.

Windows creates a personal encryption certificate with a public/private key pair for you the first time you use EFS.

The FEK, and therefore the data it encrypts, can be decrypted only with your certificate and its associated private key, which are available only when you sign in with your user account.

Designated data-recovery agents can also decrypt your data.

Other users who attempt to use your encrypted files receive an “access denied” message.

Even administrators and others who have permission to take ownership of files are unable to open your encrypted files.

You can encrypt individual files, folders, or entire drives.

You cannot, however, use EFS to encrypt the boot volume—the one with the Windows operating system files.

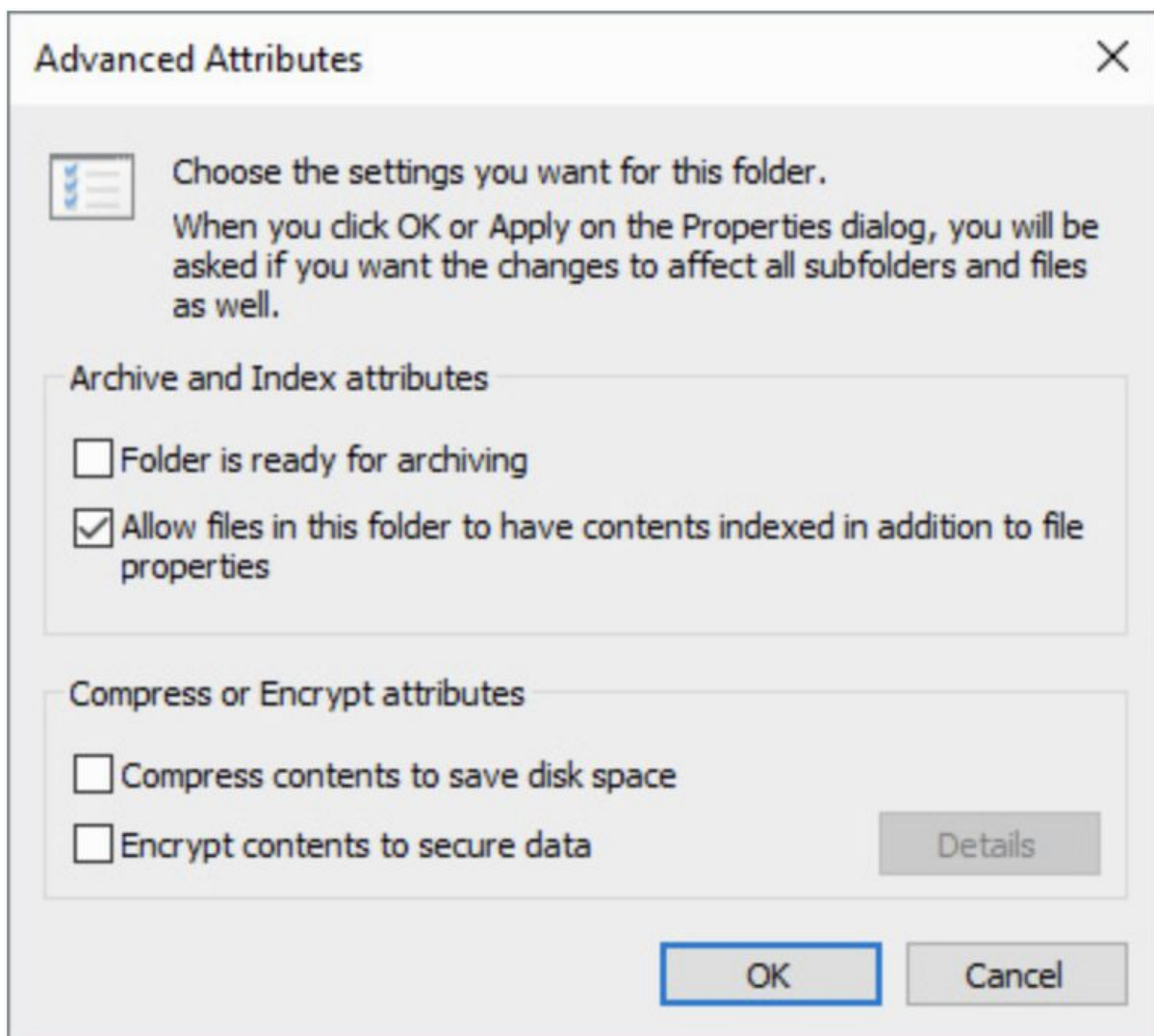
For that, you must use BitLocker.

We recommend you encrypt folders or drives instead of individual files.

When you encrypt a folder or drive, the files it contains are encrypted, and new files you create in or copy to that folder or drive are encrypted automatically.

To encrypt a folder, follow these steps:

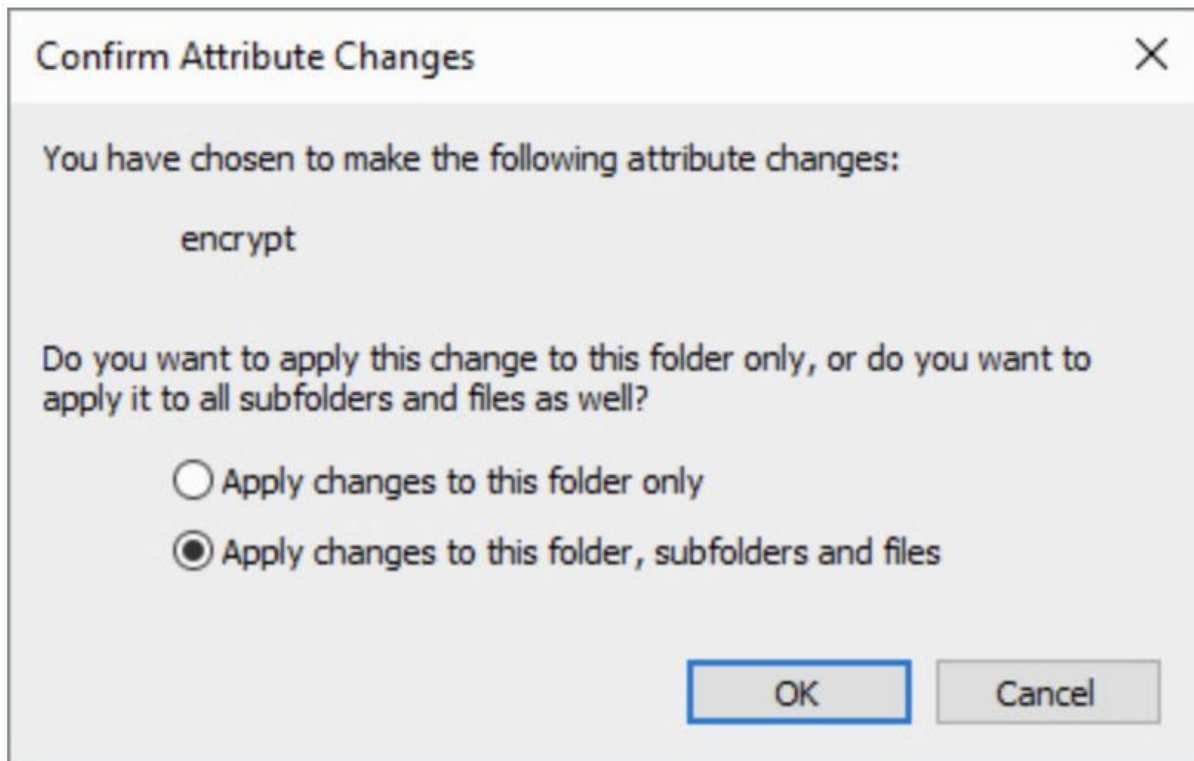
1. In File Explorer, right-click the folder, choose Properties, click the General tab, and then click Advanced, which displays the dialog box shown next.



If the properties dialog box doesn't have an Advanced button, the folder is not on an NTFS-formatted volume and you can't use EFS.

2. Select "Encrypt Contents To Secure Data". Note that you can't encrypt compressed files. If the files are already compressed, Windows clears the compressed attribute.

3. Click OK twice. If the folder contains any files or subfolders, Windows then displays a confirmation message:



After a file or folder has been encrypted, File Explorer displays its name in green.

This minor cosmetic detail is the only change you're likely to notice. Windows decrypts your files on the fly as you use them and reencrypts them when you save.

Caution!

Before you encrypt anything important, you should back up your file-recovery certificate and your personal encryption certificate (with their associated private keys), as well as the data-recovery-agent certificate, to a USB flash drive or to your OneDrive.

Store the flash drive in a secure location.

To do this, open User Accounts in Control Panel, and then click Manage Your File Encryption Certificates.

If you ever lose the certificate stored on your hard drive (because of a disk failure, for example), you can restore the backup copy and regain access to your files.

If you lose all copies of your certificate (and no data-recovery-agent certificates exist), you won't be able to use your encrypted files.

To the best of our knowledge, there's no practical way for anyone to access these encrypted files without the certificate.

If there were, it wouldn't be very good encryption.

Encrypting with BitLocker and BitLocker To Go

BitLocker Drive Encryption can be used to encrypt entire NTFS volumes, which provides excellent protection against data theft.

BitLocker can secure a drive against attacks that involve circumventing the operating system or removing the drive and placing it in another computer.

BitLocker provides the greatest protection on a computer that has TPM ("Trusted Platform Module") version 1.2 or later; on these systems, the TPM stores the key and ensures that a computer has not been tampered with while offline.

If your computer does not have a TPM, you can still use BitLocker on your operating system volume, but an administrator must first turn on the Group Policy option "Allow BitLocker without a compatible TPM."

In that configuration, you must supply the encryption key on a USB flash drive each time you start the computer or resume from hibernation.

Non-TPM systems do not get the system integrity check at startup.

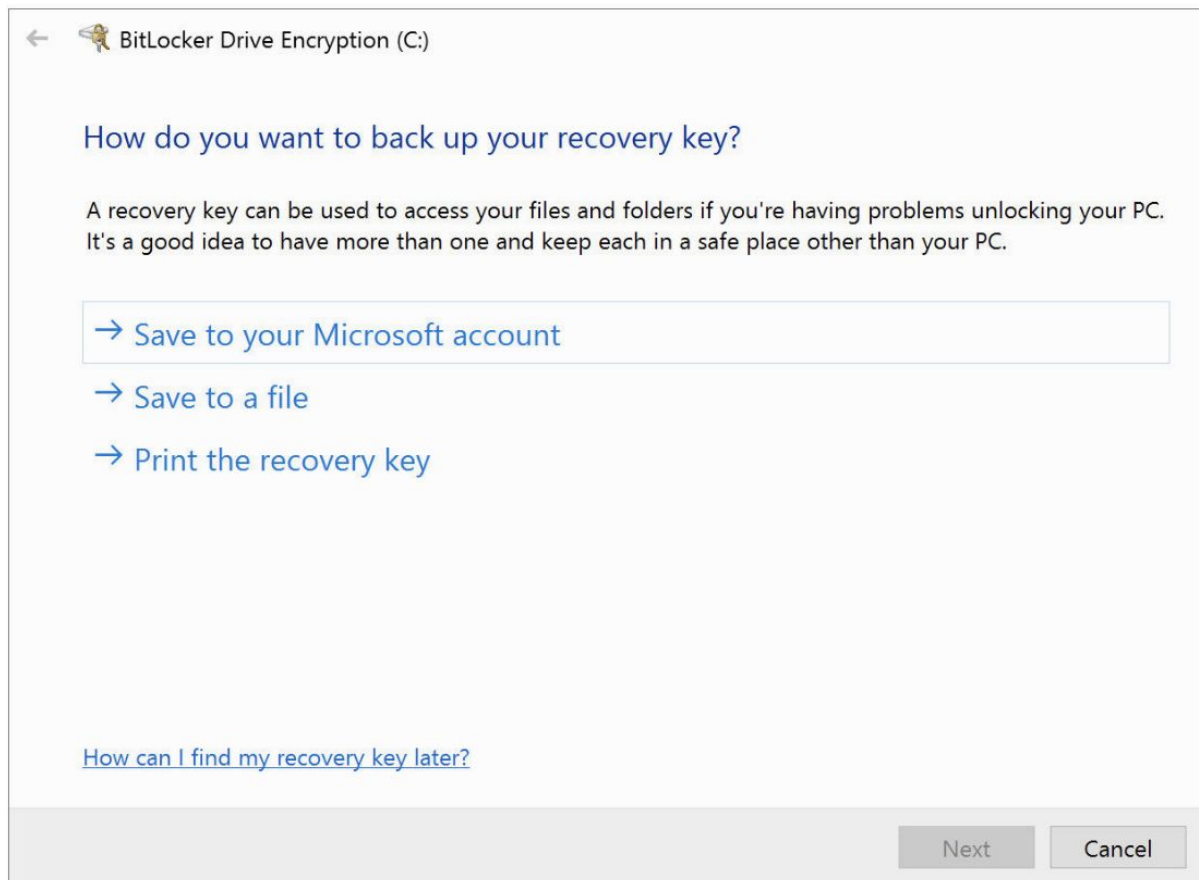
With BitLocker To Go, a feature introduced in Windows 7, you can encrypt the entire contents of a USB flash drive or other removable device.

If it's lost or stolen, the thief will be unable to access the data without the password.

To apply BitLocker Drive Encryption or BitLocker To Go, right-click the drive in File Explorer and then click Turn On BitLocker.

BitLocker asks how you want to unlock the encrypted drive—with a password, a smart card, or both.

After you have made your selections and confirmed your intentions, the software gives you the opportunity to save and print your recovery key, as shown in the next figure:



Your recovery key is a system-generated, 48-character, numeric backup password.

If you lose the password you assign to the encrypted disk, you can recover your data with the recovery key.

BitLocker offers to save that key in a plain text file; you should accept the offer and store the file in a secure location.

Clicking "Save To Your Microsoft Account" saves the recovery key on OneDrive, making it possible to recover from an encryption problem from anywhere, provided that you have an internet connection. To retrieve that key, go to <https://onedrive.com/recoverykey>.

With all preliminaries out of the way, BitLocker begins encrypting your media.

This process takes a few minutes, even if the disk is freshly formatted.

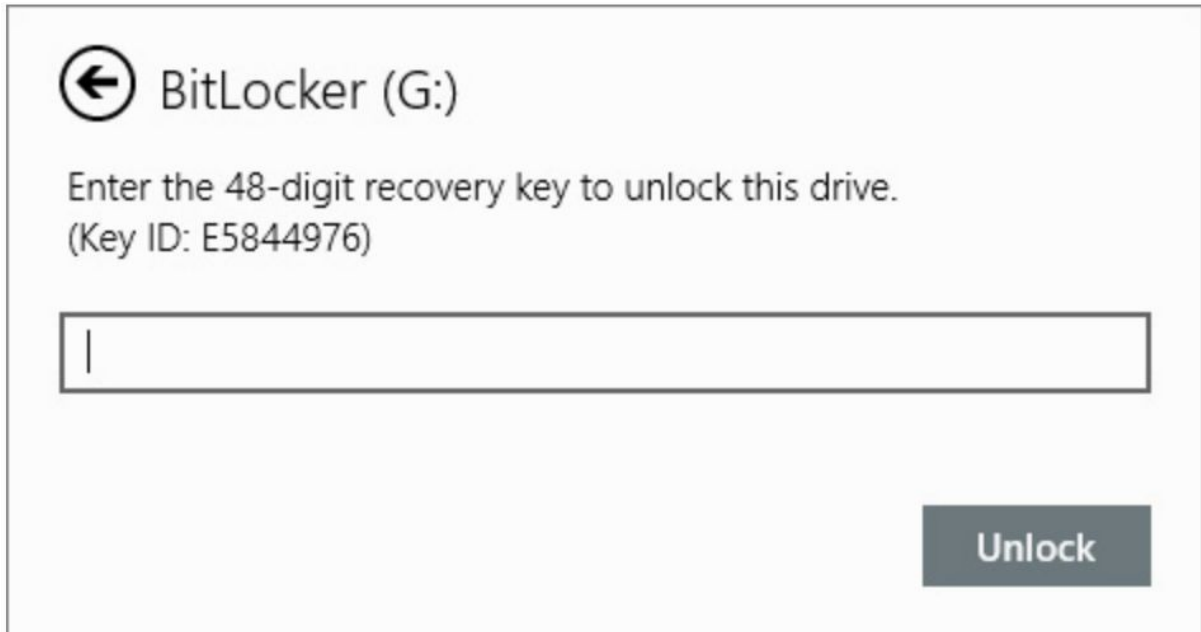
However, if you're in a hurry, you can opt to encrypt only the used space on the drive.

This choice can save you a considerable amount of time if your disk contains only a small number of files.

To read a BitLocker-encrypted removable disk, you need to unlock it by using whatever method you stipulated.

If you're prompted for a password you have lost or forgotten, click "More Options" and then click Enter Recovery Key.

In case you have several recovery-key text files, BitLocker To Go gives you the key's identification code:

A screenshot of the BitLocker (G:) recovery key entry dialog box. It features a circular arrow icon to the left of the title 'BitLocker (G:)'. Below the title, it says 'Enter the 48-digit recovery key to unlock this drive.' followed by '(Key ID: E5844976)'. There is a large rectangular text input field with a vertical cursor on the left. In the bottom right corner, there is a dark grey button with the word 'Unlock' in white text.

Find the entry on OneDrive (<https://onedrive.com/recoverykey>) or the text file whose name matches the identification code, and then enter the recovery key in the BitLocker dialog box.

You'll be granted temporary access to the files, which is good until you remove the disk or restart the computer.

At this point, you might want to change the password; go to Control Panel > System And Security > BitLocker Drive Encryption.

Select the encrypted removable drive and then click Change Password.

To remove BitLocker encryption from a disk, open BitLocker Drive Encryption in Control Panel and click Turn Off BitLocker.

The software will decrypt the disk; allow some time for this process.

Using Windows Defender to block malware

The best way to fight unwanted and malicious software is to keep it from being installed on any PC that's part of your network.

Over the years, malicious hackers have found various ways to install malware: floppy disks, document files, email attachments, instant messaging attachments, AutoPlay on USB flash drives, scripts, browser add-ons . . . and the list goes on.

Many of these transmission methods rely on social-engineering techniques designed to lure inattentive or unsophisticated users into opening an infected attachment, visiting an infected website, or otherwise falling into a trap.

Not satisfied with being able to pick off the inattentive and gullible, authors of hostile software are always on the lookout for techniques they can use to spread infections automatically.

Any program that tries to sneak onto your PC without your full knowledge and consent should be blocked.

An important layer in a basic PC protection strategy, therefore, is to use up-to-date antimalware software.

Into the breach steps Windows Defender, the antimalware program included in Windows 10.

Windows Defender runs as a system service and uses a scanning engine to compare files against a database of virus and spyware definitions.

It also uses heuristic analysis of the behavior of programs to flag suspicious activity from a file that isn't included in the list of known threats.

It scans each file you access in any way, including downloads from the internet and email attachments you receive.

This feature is called real-time protection—not to be confused with scheduled scans, which periodically inspect all files stored on your computer to root out malware.

Using Windows Defender

In general, you don't need to "use" Windows Defender at all.

As a system service, it works quietly in the background.

The only time you'll know it's there is if it finds an infected file; one or more notifications will pop up to alert you to the fact.

Nonetheless, you might want to poke around a bit.

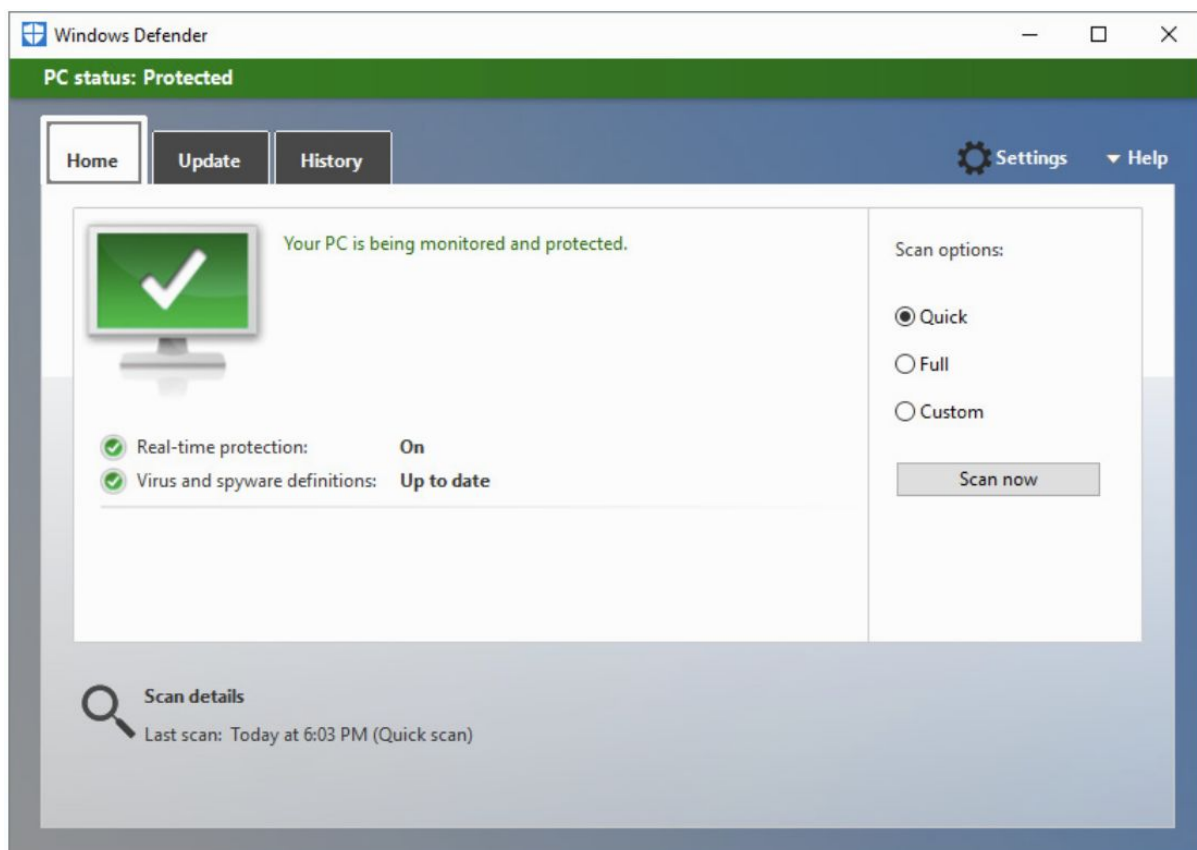
To start, go to Settings > Update & Security > Windows Defender, where you'll find the most common options.

Slide the Real-Time Protection switch to Off to temporarily disable protection (an option you should use only for short periods and only if you're certain you're not allowing malware to sneak onto your PC as a result of actions that would otherwise be blocked).

Two advanced options on this page are worth mentioning as well:

- In the Exclusions section, you can specify files, folders, file types (by extension), or processes you want Windows Defender to ignore. This option is especially useful for developers working with files that might otherwise trigger Windows Defender's alarms.
- Click Windows Defender Offline, an option that's new in Windows 10, to restart the computer and run the offline version of Windows Defender. This technique is useful for removing persistent infections that are able to evade real-time detection and removal.

For details about what Windows Defender has been doing recently, click Open Windows Defender, which runs the Windows Defender console, shown in the next figure:



The Home tab shows the current status and the results of the most recent scan.

This tab also tells you whether real-time protection is enabled.

Manually scanning for malware

The combination of real-time protection and periodic scheduled scanning is normally sufficient for identifying and resolving problems with malware and spyware.

However, if you suspect you've been infected, you can initiate a scan on demand.

To immediately scan for problems, on the Home tab (shown in the previous figure) under Scan Options, select the type of scan you want to perform and click Scan Now.

The Quick option kicks off a scan that checks only the places on your computer that malware and spyware are most likely to infect, and it's the recommended setting for frequent regular scans.

Choose Full if you suspect infection (or you just want reassurance that your system is clean) and want to inspect all running programs and the complete contents of all local volumes.

Click Custom if you want to restrict the scan to any combination of drives, folders, and files.

Dealing with detected threats

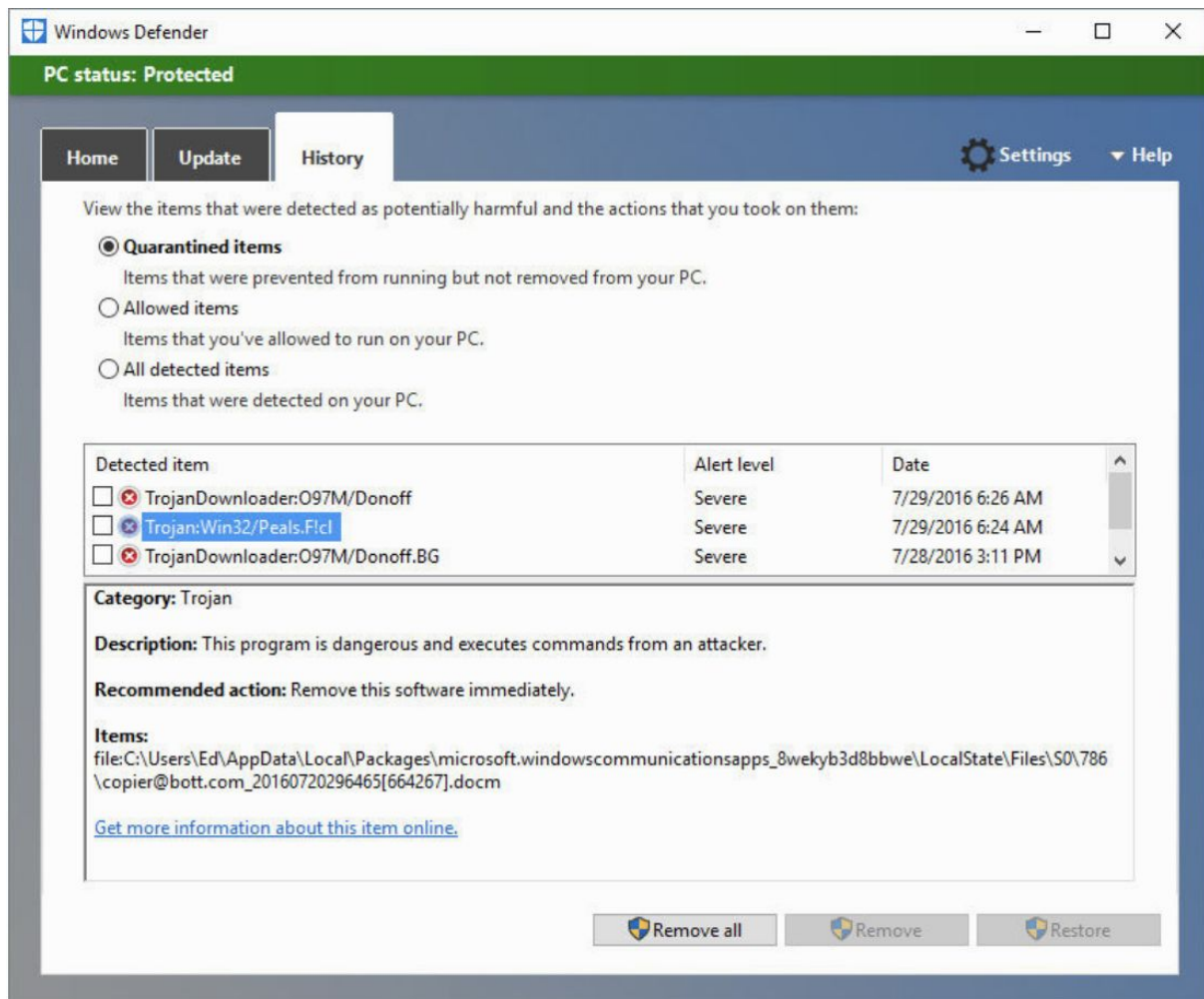
If Windows Defender detects the presence of malware or spyware as part of its real-time protection, it displays a banner and a notification in Action Center and, in most cases, resolves the problem without you lifting a finger.

To learn more about its findings, open Windows Defender and click the History tab.

Select Quarantined Items, and then click View Details.

As the following figure shows, Windows Defender shows the name, alert level, and detection date of the quarantined item or items.

In this case, the detected threats all arrived as attachments in email messages and had been shunted to the Junk folder, where the malicious code was blocked from execution:



Detected items are moved to a restricted folder (%ProgramData%\Microsoft\Windows Defender\Quarantine) whose permissions include a Deny access control entry that locks out the built-in Users and Everyone groups.

Executable files in this folder cannot be run, nor can the folder's contents be accessed from File Explorer.

Items moved here can be managed only from the Windows Defender console (preferred) or an elevated Command Prompt window.

Stopping unknown or malicious programs with SmartScreen

SmartScreen, which began as a feature in Internet Explorer in Windows 7, is used to identify programs that other users have run safely.

It does so by comparing a hash of a downloaded program with Microsoft's application-reputation database.

It also checks web content used by Windows Store apps.

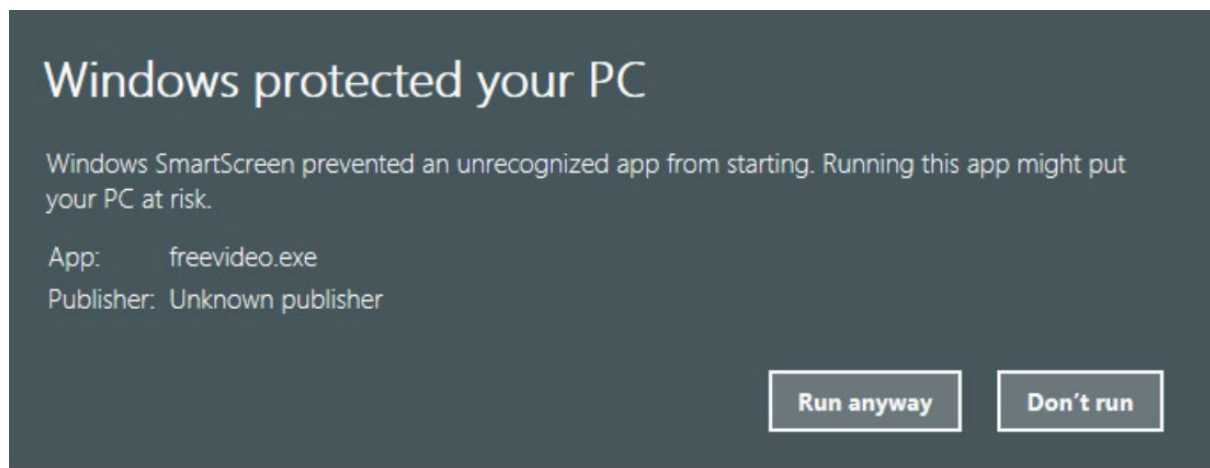
This reputation check occurs when you download a program using Microsoft Edge or Internet Explorer.

SmartScreen also kicks in when you attempt to run a program you downloaded from the internet—regardless of what browser you use.

Programs with a positive reputation run without any fuss.

Programs that are known to be bad or that have not yet developed a reputation are blocked.

A message similar to the one shown in the next figure appears:



If you're certain that a program is safe, you can override the block by clicking the Run Anyway button.

With default settings in place, you then need the approval of someone with an administrator account before the program runs.

Don't say you weren't warned.

You can turn SmartScreen protection off by going to Security And Maintenance and clicking Change Windows SmartScreen Settings.

- Vocabulary -

- ransom: extorsión / rescate.
- chore: tarea.
- to neuter: neutralizar / castrar.
- threat: amenaza.
- to hand over: entregar.

- Exercises - 1. 1. 6. Securing Windows 10 devices -

Open the following Google Document that you have created in a previous sub-unit:

"1. 1. Getting started with Windows 10 - Apellidos, Nombre"

being "Apellidos, Nombre" your Last Name and Name.

Inside this Google Document you are going to copy and answer all the "Exercises" of this sub-unit:

1. Which types of security threats do we face today?
2. Which solutions can you use in order to avoid those security threats?
3. How does Microsoft classify the threats in their KBs in order of severity?
4. How does the Windows Firewall handle inbound and outgoing traffic?
5. What is the User Account Control (UAC)?
6. Describe "Encrypting File System" (EFS).
7. In your Windows 10 virtual machine, add a new virtual hard drive of 5 GB.
Inside Windows 10, open the Disk Manager, and create one NTFS partition in this new virtual hard drive of 5 GB, and label it "ENCRYPTED". Create a folder named "Test" in this partition. Add some files to this "Test" folder. Use "Encrypting File System" to encrypt this "Test" folder.
8. How can you back up your file encryption certificate to a USB flash drive or to the cloud?
9. Explain BitLocker Drive Encryption and BitLocker To Go.
10. Use BitLocker Drive Encryption to encrypt the whole new "ENCRYPTED" partition (inside the new virtual hard drive of 5 GB). Save the back up recovery key to a file.
11. What is Windows Defender?
12. What is SmartScreen?