COVID-19
WORK FROM HOME SECURITY POLICY

trufla
TECHNOLOGY

Section 01
APPROVED COMMUNICATIONS CHANNELS

Trufla has approved the following channels and tools to use for communications while working from home.

External:

Approved tools to use when communicating with clients are as follows:

- Telax or related phone systems
- Secure Trufla email accounts
- Zoom for B2B meetings

Internal:

- Telax or approved phone systems
- Telax Chat, Slack Chat, Teams Chat
- Zoom Video Conferencing, Teams Video Conferencing
- Intranet and MicroSoft OneDrive (through your work account for file access and file sharing

Section 02
EQUIPMENT

It is important that every employee have the proper work from home equipment needed to do their work to the same standard as the work they would be doing in the office. Equipement needed is as follows:

1. High speed internet
2. Desktop or laptop with the latest anti-virus software
3. Secure router with wifi password protection

Section 03
SECURITY AND PRIVACY STANDARDS

It is important that we do our due diligence to protect the security and privacy of the company and of our clients. In order to do that, we must adhere to the privacy and security protocols as stated below:

SECURTY REQUIREMENTS

- **Anti-virus software:** Please click here for the full list of anti-viral and malware software approved by corporate. (Link to branded Excel Sheet). It is mandatory to have the most up-to-date antivirus software on your computer in order to continue to work from home.
- **Start with cybersecurity basics:** Keep your security software up to date. Use passwords on all your devices and apps. Make sure the passwords are long, strong and unique: at least 12 characters that are a mix of numbers, symbols and capital and lowercase letters.
- **Keep an eye on your laptop:** If you're using a laptop, make sure it is password-protected, locked and secure. Never leave it unattended – like in a vehicle or at a public charging station.
- **Always secure your workstation:** Never leave your workstation unlocked when unattended.
- **Securely store sensitive iles:** When there's a legitimate business need to transfer confidential information from office to home, keep it out of sight and under lock and key. If you don't have a file cabinet at home, use a locked room. For more tips, read about physical security.
- **Dispose of sensitive data securely:** Don't just throw it in the trash or recycling bin. Shred it. Paperwork you no longer need can be treasure to identity thieves if it includes personal information about customers or employees.
- **Block the sight lines:** If you are working around other people, pay attention to your sight lines. If someone is behind you, they can see everything you are typing. Furthermore, someone with the right observational skills (like a cybercriminal) could easily watch what you are doing and identify confidential information. And keep your devices with you; in the time it takes you to use a restroom, your device could be quickly compromised by a threat actor with a USB stick that types pre-programmed sequences at 1000 words per minute. On a personal level, this is something you should do while keying in your ATM PIN as well.
- **Lock your doors:** If you bring your work computer home or tend to work remotely, confidential corporate information could be at risk. Don't subject yourself to the stress of a stolen work computer or harm your company by letting its data out into the wild.
- **Never leave your devices or laptop in the car:** Never leave your work computers or devices in a vehicle. It's a best practice to keep work laptops and devices on your person at all times while on the road. And the trunk of your car is not any safer. There may be criminals watching the parking lot from afar, waiting for their next victim. Putting valuables in the trunk may make life a little bit easier in the short-term - but why take that chance?
- **Don't use random thumb drives:** A classic hacking technique is to drop a number of large capacity thumb drives near the company you are hoping to attack. The chances that an unwitting employee will pick up the thumb drive and use it are surprisingly high. A. Never use a thumb drive if you don't know where it came from and do not continue to use one if you have plugged it into a system for whose safety you cannot honestly vouch.
- **Use a usb data blocker when charging up at a public phone charging station:** If you need to charge your phone and the only option is an unknown USB port, a wise measure is to protect it with a USB data blocker to prevent data exchange and guard against malware. This type of USB protection allows the device to connect to power without exposing the data pins inside your device; it connects the power leads, but not the data ones.

ROUTER SECURITY

If your Wi-Fi network isn't secured properly (has a public IP address, no unique Wi-Fi password, etc.), you could be letting anyone with a wireless-enabled device gain access. You might not be worried about someone using your wireless connection, but the real risk is exposing sensitive information you send and receive — your emails, banking information, and maybe even your smart home's daily schedule — to cybercriminals.

Manufacturers know how important it is to make their products user-friendly. Most routers come with instructions that are easy to set up and configure. Apps are replacing bulky user manuals and web interfaces that walk users through the set-up process. While using apps has made setting up routers easier for customers, the router may not be completely secure.

Here are a few things to consider before setting up the router.

Password Security

All routers come with a preset password. It's important to change the password setting from the default to help secure your WIFI, even if your alphanumeric default password looks beyond complicated to hack, here's why:

Router manufacturers often put the brand name or model of the router in the SSID. If you got a router from your internet service provider, the ISP might change that SSID when to show their own name instead of the manufacturer. If you bought the router yourself, its SSID will probably identify the manufacturer or even the model of the router.

A hacker can use the information that appears in the SSID to look up the default username and password for the router with little effort.

Here are some tips to help really secure your router:

- Change the SSID so that it doesn't give away the router brand or model.
- Don't choose an identifier that includes your name, address, or telephone number.
- Don't use any other personal information in the name. So, "10BullLane," "JBDecker Network," and "Homenet-12281975" are all bad ideas.
- Avoid making political statements, don't use offensive language, and don't provoke hackers with challenges in your SSID. Just make it bland.
- Creating a new, complex, unique password for your wireless router is easy.

It should only take a couple of minutes. Specific instructions vary from one router to another, but the basic idea is this:

1. All wireless routers have a numerical address. If you've lost the instructions, you can probably find yours by searching online for your router's model number.
2. In Security Settings, create a name for the router, and a password, and then select a type of encryption, like WAP2. Do not name your router something that can easily be associated with you, such as your last name.
3. Make sure you choose a complex password that you can remember, but one that's not easy to guess.

- Make a complicated router password
- If you give visitors the password, make your password a random sequence of letters, numbers and special characters, mixing uppercase and lowercase so no one could ever remember it. Fortunately, once a password is successfully entered into a device, it is not visible, so the people you give it to won't be able to read it off to tell someone else. Ideally, the password should be 20 characters long, but if you find that tiring, you could get away with 12 characters.
- Of course, it will be impossible for you to remember the password, so you will have to store it somewhere. You can keep it in a hidden file on your computer or write it in a notepad that you keep in a locked drawer.
- Change the password frequently. There is no hard and fast rule about how often you should change the router password. However, you should change it on a regular basis. Memorizing a new email or online banking password can be annoying because you have to log in all the time But because wifi routers typically only require you log in once to be allowed indefinite access, changing a wifi password is less of a nuisance. Make changing the router password part of your monthly routine. Remember to update the note you kept of the password.

4. Don't forget to save the updated information when prompted. Your router is now secured against roaming cybercriminals.

Beware of Phishing Scams

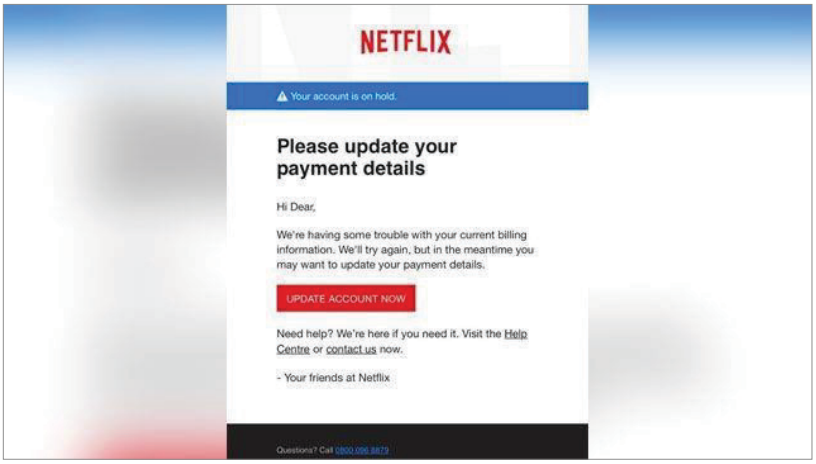
Phishing attacks are widely recognized as the top cause of data breaches. Hackers can easily send seemingly legitimate, deceptive emails with malicious links and attachments. Once an employee clicks on this malicious link, a hacker is able to gain access to the employer's device.

Phishing emails and text messages may look like they're from a company you know or trust. They may look like they're from a bank, a credit card company, a social networking site, an online payment website or app, or an online store.

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may :

- say they've noticed some suspicious activity or log-in attempts
- claim there's a problem with your account or your payment information
- say you must confirm some personal information
- include a fake invoice
- want you to click on a link to make a payment
- say you're eligible to register for a government refund
- offer a coupon for free stuff

Here's a real world example of a phishing email:



Imagine you saw this in your inbox. Do you see any signs that it's a scam? Let's take a look.

- The email looks like it's from a company you may know and trust: Netflix. It even uses a Netflix logo and header.
- The email says your account is on hold because of a billing problem.
- The email has a generic greeting, "Hi Dear." If you have an account with the business, it probably wouldn't use a generic greeting like this.
- The email invites you to click on a link to update your payment details.

While, at a glance, this email might look real, it's not. The scammers who send emails like this one do not have anything to do with the companies they pretend to be. Phishing emails can have real consequences for people who give scammers their information. And they can harm the reputation of the companies they're spoofing.

What to Do If You Suspect A Phishing Attack

1. If you get an email or a text message that asks you to click on a link or open an attachment, answer this question: Do I have an account with the company or know the person that contacted me?
2. If the answer is "No," it could be a phishing scam.
3. Do not open the email, or click on any links. Report the email directly to IT.

How to Recognize if You Have Been Breached

You may have been already been breached but not know it yet because you don't know the signs. Here's what you should watch out for. If you think you've been breached please contact IT right away.

Physical workspace:

1. Things out of place such as note pad, devices and/or documents
2. Doors or file containers originally locked but now unlocked

Online - while on browsers:

1. You receive ransomware messages that's a complete screen take over, requesting a fee be paid to unlock your computer.
2. You receive a fake antivirus message: Usually a pop-up message that mimics an antivirus product and claims to have found several viruses on your computer.
3. Your browsers restarted without warning or prompting
4. You have unwanted browser toolbars
    - Be mindful of toolbars you have on your web browser that you do not use or recognize. Ask IT to inspect it.
    - Your internet searches are redirected.
    - Many people are unaware of this, but hackers earn money for having people's web browsers redirected to websites they never searched in order to get that website more clicks.
    - You see frequent, random popups.
    - You receive continuous spamming of random popup adds.
5. Your friends receive social media invitations from you that you didn't send
6. Your online password isn't working
7. You observe unexpected software installs: Unknown and unexpected software downloads are a big tell that you've been hacked.
8. Your online account is missing money: If this does occur, it tends to be a lofty amount of funds taken.
9. You've been notified by someone you've been hacked: Tends to be an email from a Third-party address that is unrecognizable.
10. You observe strange network traffic patterns
11. Receive a notification from your Antivirus program you've been compromised

Emails:

1. You can check if personal emails have been hacked or compromised by visiting the link: https://haveibeenpwned.com/. This tool is a great tool to utilize in making sure your email accounts are hack free!

Desktop:

1. Errors in Applications and System event logs: When using different programs, you receive error messages you've never seen before.
2. Your mouse moves between programs and makes selections: If your mouse pointer moves and starts making selections that enables programs, this would be a big indication you've been breached.
3. Antimalware, Task Manager or Registry Editor is disabled: Antivirus software that has been disabled and not done by yourself can be an indication something could be wrong especially if you cannot access your Task Manager.

How and When to Update Your Computer Programs

It's important to recognize which programs require updates, and which may be a type of malware. Below is a detailed guide on the various common types of updates, and how to install them on your computer. Please refer to the appendix for a full manual on update.

See Appendix A for full details on how and when to update your computer programs.

Section 04
REMOTE TECH SUPPORT

For any issues relating to your work computer, or work software, please submit a ticket to IT. The company is not responsible for damages or performance issues on your personal work devise.

If you suspect you've been hacked, or compromised, please send an email to IT and your team lead right away.

Section 05
INTERNAL CULTURE GUIDE

While we're working remotely, and it may seem a bit odd, we want to keep our culture alive! Please engage on our #general channel in Teams, and let us know what we can do to help keep things fun and connected.

Appendix A

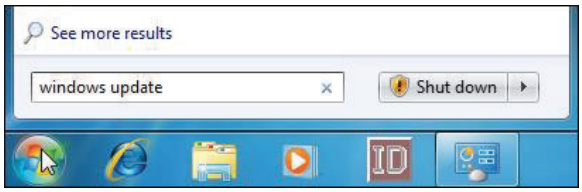
HOW AND WHEN TO UPDATE YOUR COMPUTER PROGRAMS

Contents:

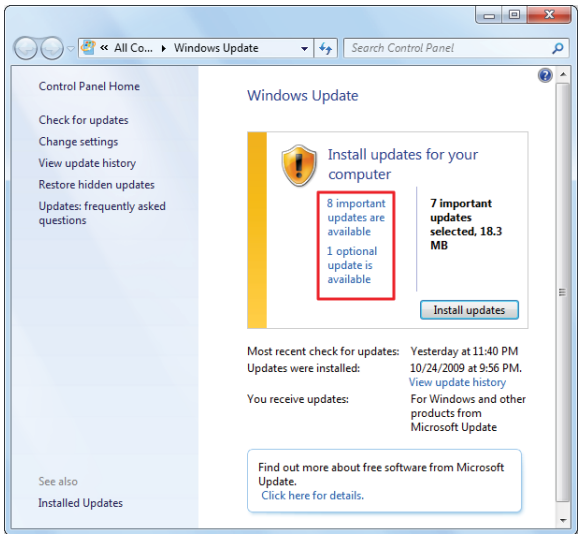
- Windows 7 Update
- Windows 8 And 10 Update
- Third-Party Apps Update
- How To Know If The Website Is Safe
- Using The USB Key

WINDOWS 7 UPDATE

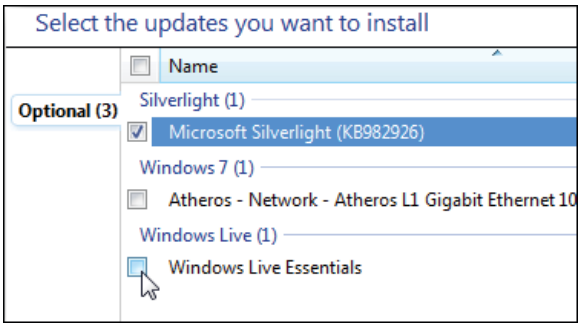
To access Windows Updates, just hit Start, type “Windows Update,” and then hit Enter.



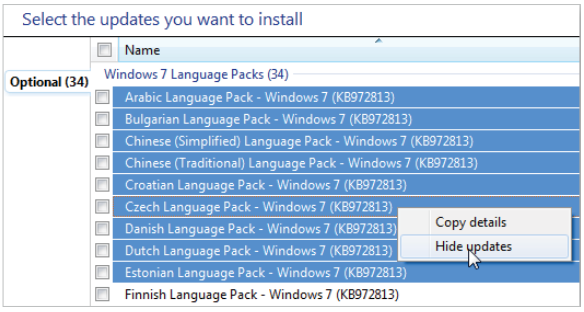
Windows Update divides updates into “important” and “optional.” Important updates are selected for download and installation by default. Optional updates are not selected. To control what updates Windows installs, click the relevant link.



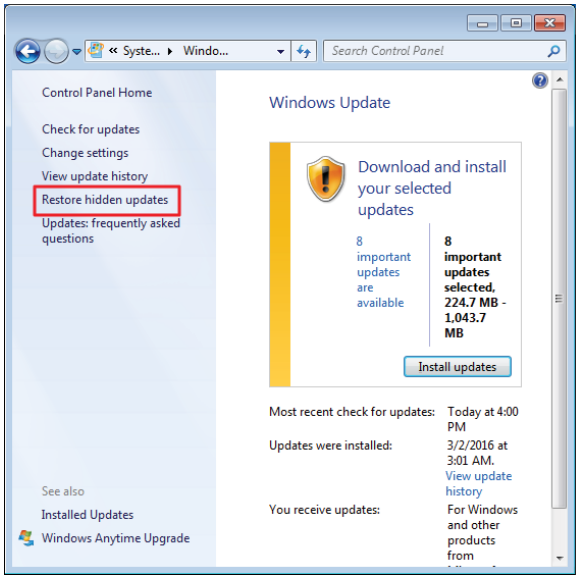
The window that opens allows you to select each update you want to install.



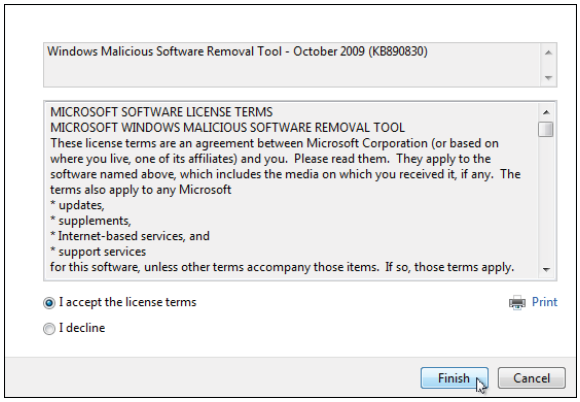
If you have updates on the list that you know you won’t ever install and would like to stop seeing them, right-click one or more updates and then choose “Hide updates” from the context menu.



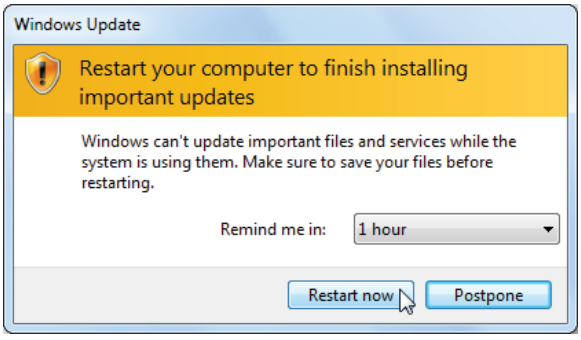
If you want to see your hidden updates again, return to the main Windows Update screen and click the “Restore hidden updates” link.



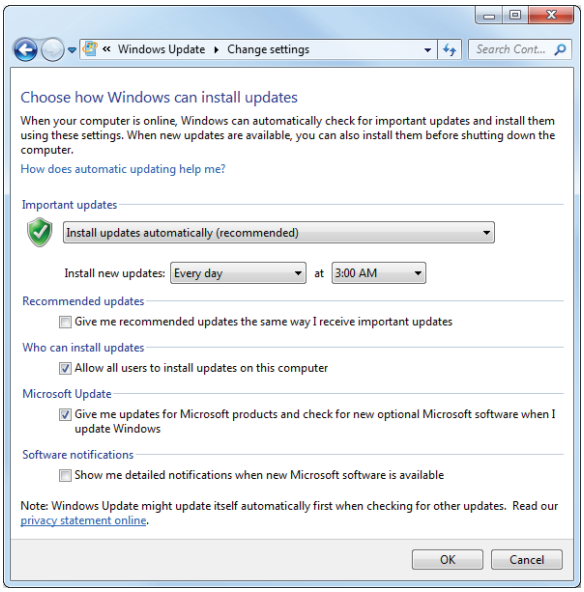
When you return the main Windows Update window and click the “Install updates” button, all the important and optional updates you’ve selected are downloaded and installed. Some updates will require that you agree to an EULA before the installation can proceed, but you’ll be able to agree to all necessary EULAs before the real updating process begins so that you don’t have to hang around and watch the entire installation happen.



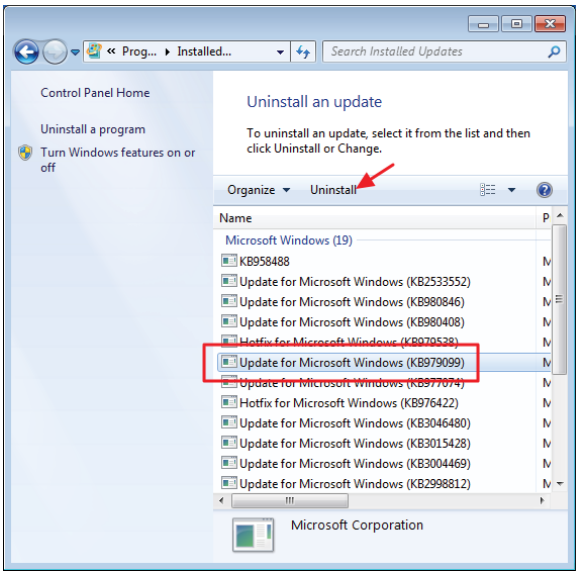
Some updates will require a system restart, but you’ll have the option to postpone the restart for a few hours or until you reboot manually.



Windows 7 also allows you to change some settings governing how Windows installs updates. You can have Windows automatically check for and install new important updates, turn automatic updating off altogether, or have Windows check for updates, but notify you before downloading them. Other options let you control whether recommended updates are installed along with important updates, what users can install updates, and whether other Microsoft products than Windows are updated, too.

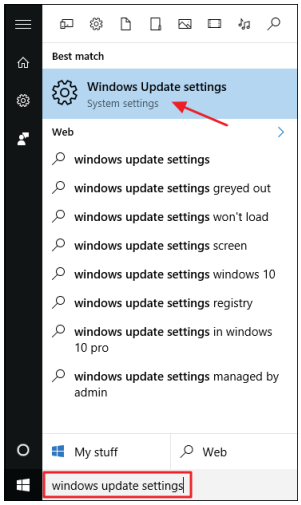


To uninstall updates in Windows 7, head to Control Panel > Uninstall a Program, and then click "View installed updates." Select an update and then click the "Uninstall" button. Again, do your research and make sure other people are reporting similar problems with the update and make sure you create a system restore point or back up your computer before you uninstall any updates.

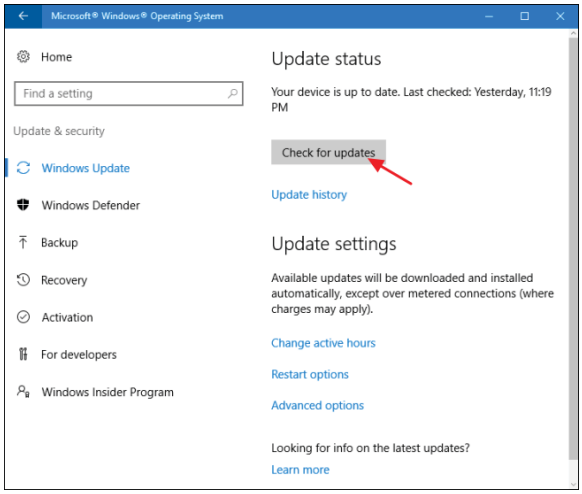


WINDOWS 8 AND 10 UPDATE

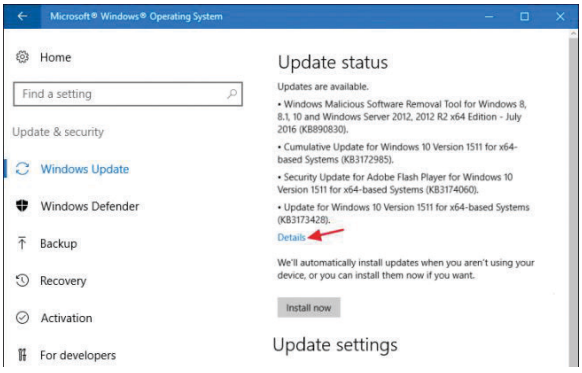
To access it, just hit Start, type “windows update” and then click the result.



The Windows Update window is sparse compared to what it used to be but is still useful for finding out the status of updates and configuring a few options. Since Windows downloads and installs updates automatically, you’re most likely to see a simple screen letting you know that your device is up to date and when Windows last checked for updates. If you want to check for updates immediately, you can click the “Check for updates” button and Windows will let you know if it finds anything. Even if you don’t bother checking updates manually, any updates that are available will be downloaded and installed sooner rather than later.

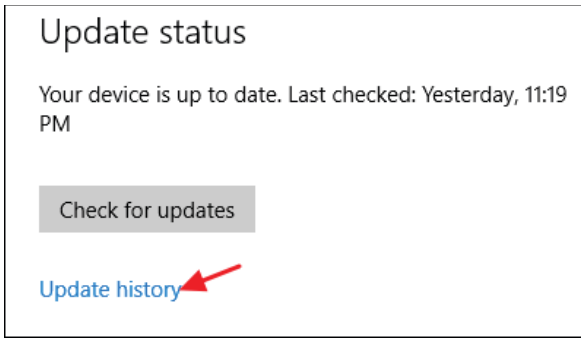


If there are available updates that have not yet been downloaded or installed, they’ll show up on the Windows Update screen. If you’d like to see more information about the available updates, click the “Details” link. The details page shows you pretty much the same information about each update that the main screen displays, but does add the status of each update so you can see whether it’s waiting to be downloaded or has been downloaded but is waiting for installation.

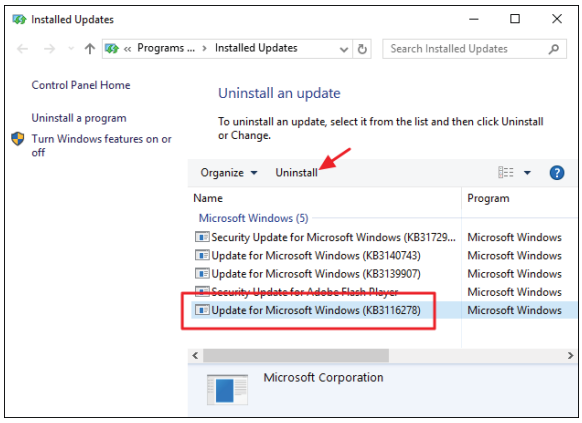


Back on the main page, you can also select the “Update history” link to see details about your recent history of updates.

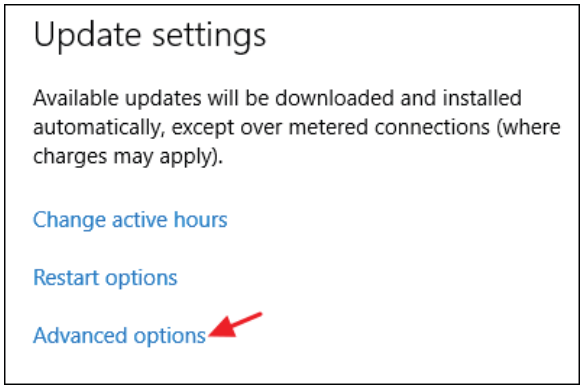
The history shows each update, whether it was installed successfully or not, and when it happened. The history screen has two options for helping you recover from a bad update. The “Recovery options” link takes you to the standard Windows recovery options screen, where you can reset the PC or boot in recovery mode. If you want to uninstall one or more particular updates, hit the “Uninstall updates” link instead.



To uninstall updates: In the Installed Updates control panel window, you can uninstall any update by selecting it and then clicking the Uninstall button. This can be useful if you’ve installed a problematic update, but it’s something you should take care when using. Do your research and make sure other people are reporting similar problems with the update and make sure you create a system restore point or back up your computer before you uninstall any updates. After you uninstall the update, you’ll also want to take steps to block that update in the future, if possible.

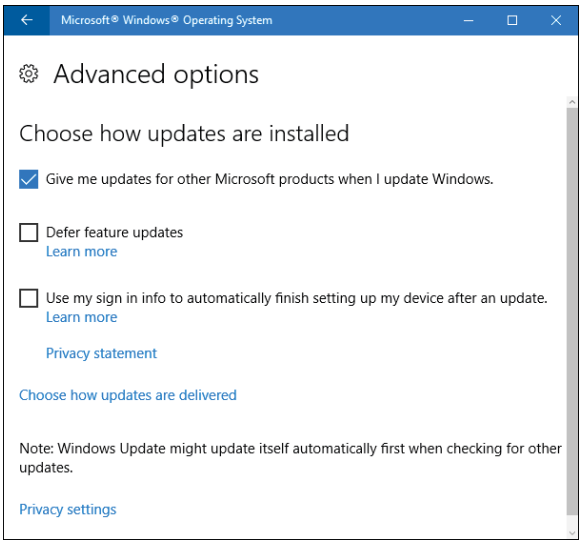


There also a few options you can set governing how Windows Update works. On the main Windows Update screen, the “Change active hours” link lets you set specific hours when Windows Update can restart your computer and the “Restart options” link lets you temporarily override the active hours you’ve set up. To find additional options, click the “Advanced Options” link.



The Advanced Options page offers several options. The “Give me updates for other Microsoft products when I update Windows” option is pretty self-explanatory and is useful if you’re using Microsoft Office or other Microsoft apps. You can also have Windows automatically sign in for you to finish installing an update if it needs to restart while applying the update.

The option to defer feature updates is an interesting one and is only available on Windows 10 Pro, Enterprise, and Education editions. By default, Windows downloads and installs all updates automatically, including security updates and new features. If you select the “Defer upgrades” option, Windows still downloads and installs security updates automatically, but holds off on downloading other types of updates for, as Microsoft puts it, “several months.” How long it actually defers these upgrades is not clear.



THIRD-PARTY APPS UPDATE

Keeping Windows updated is important, but it doesn't end there. You want to make sure your other apps are updated as well. Aside from bug fixes and new features, updating your apps ensures that you fix the inevitable security flaws that pop up in common third-party apps like Adobe Flash, Java, and so on. The hassle with keeping third-party apps updated is that different products require you to check for and perform updates in different ways.

Some Apps Have a Built-In Updater :

Some third-party apps, like those provided by Apple, have built-in updaters that automatically check for new updates and notify you so that you can download and install them.

Security software is especially important to keep updated, and most have automatic updaters for that reason. Still, it's essential to check up on them once in a while–like before you run a manual scan–just to make sure. As an example, Windows Defender gets regular updates for virus definitions through Windows Updates but still offers the ability to check for updates manually when you open it up.

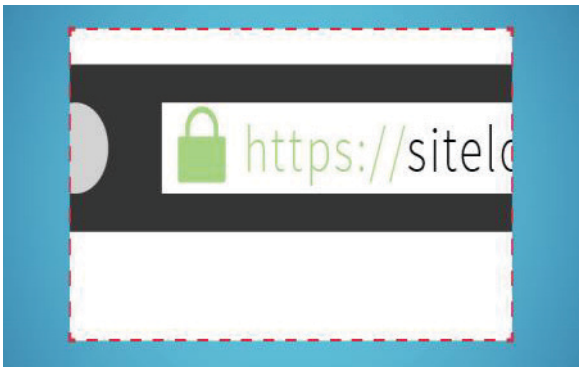
For Other Apps:

Some other third-party apps, unfortunately, offer no built-in updating features at all, requiring you to go to the product web site to download updates or new versions yourself.

HOW TO KNOW IF THE WEBSITE IS SAFE

Every website owner should take responsibility for ensuring the safety of its visitors, but unfortunately, some websites just aren't secure. An unsafe website can spread malware, steal your information, send spam, and more. To protect yourself and your personal information, it's important to know that a website takes your safety seriously – but how can you tell? Look for these five signs that a website is safe:

1. Look for the "S" in HTTPS



If HTTPS sounds familiar, it should – many URLs begin with "https" instead of just "http" to indicate that they are encrypted. This security is provided by an SSL certificate, which protects sensitive information entered into that site as it travels from the site to a server. Without an SSL certificate, that information is exposed and easily accessible by cybercriminals. It's important to note that HTTPS isn't the only thing a website can – or should do – to protect its visitors, but it's a good sign that the website owner cares about your safety. Whether you're logging in, making a payment, or just entering your email address, check that the URL starts with "https."

2. Check for a Website Privacy Policy

A website's privacy policy should clearly communicate how your data is collected, used, and protected by the website. Nearly all websites will have one, as they are required by data privacy laws in countries like Australia and Canada, and even stricter rules have been introduced in the EU. A privacy policy indicates that the website owner cares about complying with these laws and ensuring that their website is safe. Be sure to look for one, and read it over, before giving your information to a website.

3. Find Their Contact Information

If finding a website's contact information makes that site seem more trustworthy to you, you're not alone. A survey of website visitors found that 44 percent of respondents will leave a website that lacks a phone number or other contact information. Ideally, a safe website will clearly display an email address, a phone number, a physical address if they have one, return policy if applicable, and social media accounts. These won't necessarily provide protection, but they indicate that there's likely someone you can reach out to if you need assistance.

4. Verify Their Trust Seal

If you see an icon with the words "Secure" or "Verified," it's likely a trust seal. A trust seal indicates that the website works with a security partner. These seals are often an indicator that a site has HTTPS security, but they can also indicate other safety features, like the date since the site's last malware scan.

Although 79 percent of online shoppers expect to see a trust seal, the presence of the seal isn't enough. It's also important to verify that the badge is legitimate. Fortunately, it's easy to do – simply click the badge and see if it takes you to a verification page. This confirms that the site is working with that particular security firm. It doesn't hurt to do your own research on the company supplying the badge, too!

If a trust seal is legitimate, clicking on it will take you to a page that verifies the authenticity of that seal. As an example, SiteLock's verification page looks like this.

5. Know the Signs of Website Malware

Even if a website has an SSL certificate, a privacy policy, contact information, and a trust badge, it may still not be safe if it is infected with malware. But how do you know if a website is infected with malware? Look for the signs of these common attacks:

- **Defacements.** This attack is easily spotted: cybercriminals replace a site's content with their name, logo, and/or ideological imagery.
- **Suspicious pop ups.** Be cautious of pop ups that make outlandish claims – they are likely trying to entice you to click and accidentally download malware.
- **Malvertising.** Some malicious ads are easy to catch. They typically appear unprofessional, contain spelling/grammar errors, promote "miracle" cures or celebrity scandals, or feature products that don't match your browsing history. It's important to note that legitimate ads can also be injected with malware, so exercise caution when clicking.
- **Phishing kits.** Phishing kits are websites that imitate commonly visited sites, like banking websites, in order to trick users into handing over sensitive information. They may appear legitimate, but spelling and grammar errors will give them away.
- **Malicious redirects.** If you type in a URL and are redirected to another site – especially one that looks suspicious – you have been affected by a malicious redirect. They are often used in conjunction with phishing kits.
- **SEO spam.** The appearance of unusual links on a site, often in the comments section, is a sure sign of SEO spam.
- **Search engine warnings.** Some popular search engines will scan websites for malware, and place a warning on that site if it is definitely infected with malware.

It's unfortunate that not every website is trustworthy and secure, but don't let that keep you from going online – just do it safely! Simply being able to recognize a safe website can go a long way to help protect your personal data. A legitimate trust seal, "https," a privacy policy, and contact information are all good signs that a website is safe!

USING THE USB KEY

What Can a "Bad" USB Stick Do?

A malicious device can install malware such as backdoor Trojans, information stealers and much more. They can install browser hijackers that will redirect you to the hacker's website of choice, which could host more malware, or inject adware, spyware or greyware onto your computer. While the ramifications of these threats can range from annoying to devastating, you can stay protected from these threats.

Staying Protected is Easier Than You Think

- Don't plug unknown flash drives into your computer- this is one of the most important pieces of advice you should follow. This is a tactic used in social engineering, where the attacker relies on the curiosity of people. If you see a USB stick lying out in open, public places, do NOT plug it into your computer to see what's on it.
- Use secure USB drives. Some newer models have safety features such as fingerprint authentication that help protect the device from hackers.
- Don't use the same flash drives for home and work computers, as you could run the risk of cross contaminating your computers.
- Be careful where you purchase your USB drives from, as some shady third party manufacturers are known to manufacture these devices with malware on them. Always buy your flash drives from reputable, well known manufacturers as well as sellers.
- Keep the software on your computer up to date. No one likes to do them, but software updates are crucial to the security of your computer, as they patch known vulnerabilities.
- Make sure to keep your Internet security software up to date. In the event you accidentally use a device that contains malware, you're protected. If you don't have Internet security software, you should get it, as it can protect you from a host of issues other than just USB malware.

So What Should I Do to Be Safe?

- If you are not sure about the USB key, try to avoid using USB key as much as possible
- Always scan it once you plug it to the computer
- Never unplug USB key unless you safely eject it: How?
  - Click on the USB icon in the taskbar. If you don't see it, click on the up arrow to show all items in the taskbar.
  - A small window will appear above this, listing all the devices plugged in via USB. Find the device you want to eject and click on it.
  - Once Windows has safely dismounted the USB flash drive, you'll see the following confirmation screen open. You may safely remove your drive now.

Appendix B

ANTIVIRUS SOFTWARE PRODUCTS COMPARISON CHART

Contents:

- Norton
- Kaspersky
- Trend Micro
- Free Versions

Cost	Paid Version	# of Devices Protected	Anti-Spyware, Antivirus, Malware & Ransomware Protection	PC Cloud Backup‡‡, 4	Firewall for PC or Mac	Password Manager	100% Virus Protection Guarantee	Parental Control	Protection for Online Payments	Secures Privacy on Social Media	Secure VPN	SafeCam for PC	Support Hours including Live Chat	Secures Mobile Devices
	Norton													
$29.99/yr for 1st year	Norton AntiVirus Plus	1 PC or Mac	P	2GB	P	P	P	x			Not Available	Not Available	24 hours a day, 7 days a week	
$39.99/yr for 1st year	Norton 360 Standard	Protection for 1 PC, 1 Mac® or 1 smartphone or tablet	P	10GB	P	P	P	x			1 PC, 1 Mac or 1 smartphone or tablet	P	24 hours a day, 7 days a week	
$49.99/yr for 1st year	Norton 360 Deluxe	Protection for up to 5 PCs, Mac®, smartphones or tablets	P	50GB	P	P	P	P			Up to 5 PCs, Mac, smartphones or tablets	P	24 hours a day, 7 days a week	
$54.99/yr for 1st year	Norton 360 Premium	protection fPr up to 10 PCs, Mac®, smartphones or tablets.	P	75GB	P	P	P	P			Up to 10 PCs, Macs, smartphones or tablets	P	24 hours a day, 7 days a week	
	Kaspersky													
$29.99/yr	Kaspersky AntiVirus	3 to 10 PC's or Mac's, tablets and Android Smartphones	P		x	x							9AM - 8PM ET Monday to Friday	
$39.99/yr	Kaspersky Internet Security	3 to 10 PC's or Mac's, tablets and Android Smartphones	P		P	x	P	x	P		x	x	9AM - 8PM ET Monday to Friday	P
$49.99/yr	Kaspersky Total Security	5 to 10 PC's or Mac's, tablets and Android Smartphones	P		P	P	P	x	P		x	P	9AM - 8PM ET Monday to Friday	P
$53.99/yr	Kaspersky Security Cloud Personal	Pesonal Account up to 5 devices	P	P	P	x	P	x	P		P	P	9AM - 8PM ET Monday to Friday	x
$89.99/yr	Kaspersky Security Cloud Family	Family account up to 20	P	P	P	P	P	P			P	P	9AM - 8PM ET Monday to Friday	x

Cost	Paid Version	# of Devices Protected	Anti-Spyware, Antivirus, Malware & Ransomware Protection	PC Cloud Backup‡‡, 4	Firewall for PC or Mac	Password Manager	100% Virus Protection Guarantee	Parental Control	Protection for Online Payments	Secures Privacy on Social Media	Secure VPN	SafeCam for PC	Support Hours including Live Chat	Secures Mobile Devices
	Trend Micro													
$29.95/yr	Trend Micro Antivirus & Security	1 PC	P						P				online chat only	x
39.95/yr	Trend Micro Internet Security	Protection for 3 PC's	P			x		P	P	P			No Phone number, no hours posted - online chat only	x
39.95/yr	Trend Micro Maximum Security	Protection for up to 10 devices	P			P		P	P	P			No Phone number, no hours posted - online chat only	P
	Free Versions													
Free	Kaspersky Security Cloud Free	1 device (PC, Mac, Android or IOS)	P			x					x		1-866-328-5700 (Toll Free) Mon-Sunday 9am-10pm EST	
Free	Kaspersky Security Cloud Personal	3-5 devices (PC, Mac, Android or IOS)	P			P					P		1-866-328-5700 (Toll Free) Mon-Sunday 9am-10pm EST	
Free	Kaspersky Security Cloud Family	20 devices (PC, Mac, Android or IOS)	P			P					P	P	1-866-328-5700 (Toll Free) Mon-Sunday 9am-10pm EST	
Free	Avast Free Antivirus	available for PC's and Mac's	P	P	x	P		x	x	x	x	x	No Phone number, no hours posted - online chat only	x
Free	Bitdefender Antivirus Free	available for 1 PC only	P		x	x		x	x	x	x	x	No support	x
Free	Windows Defender Antivirus Free	protection for all PC's running windows 10	P	P	P	P		P					Onlie support only	x