Windows 10 & Security
November 7, 2016

Tell Your Relatives: No, Microsoft Won’t Call You About Your Computer

“Hi, I’m from Microsoft and we’ve noticed your computer has a lot of viruses.” This is how the Microsoft tech support scam starts. By the end, the victim has probably paid hundreds of dollars and had their computer infected.

This cold-calling telephone scam has been going on since 2008, but shows no sign of going away. If you have any relatives who might fall for it, be sure to let them know Microsoft won’t actually call them.

This scam isn’t just for Windows PCs. A new scam offers “Mac Technical Support” that works in a similar way, demanding access via a remote-desktop tool and requiring payment to fix non-existent problems.

How It Works

If you stay on the line — and you shouldn’t — the scammers will attempt to demonstrate that they have information about what’s wrong with your computer. They’ll ask you to look at parts of Windows that generally aren’t accessible to average users. For example, they’ll ask you to look at your Event Viewer, Prefetch folder, and MSConfig utility. Average Windows users aren’t familiar with these system utilities, and the scammers will attempt to deceive them.

For example, a scammer will tell you to open the Event Viewer and verify that errors are present. The Event Viewer lists a variety of status messages for many different things in Windows, and errors are often completely innocuous. Scammers will inform you that these errors are proof of viruses.

Scammers will often direct you to the C:\Windows\Prefetch folder as well, telling you that each file in the Prefetch folder is a virus. These are actually harmless files that are used to speed up application launch times, but they have confusing looking names.

Scammers also like directing users to MSConfig, telling them that each stopped services on the Services tab represents a problem. To a less knowledgeable user, this might seem logical. In reality, Windows normally starts and stops services as needed. It’s normal for system services to be stopped.

If It Happens To You...

- Treat any unsolicited phone call as a probable scam, even if it supposedly comes from a firm you trust. Microsoft does not call Windows users; it distributes security fixes only via Windows Update.
- Never reveal sensitive information, such as a credit card number, to any unsolicited caller.
- Do not visit a Web site, install software, re-configure Windows, or follow any other instructions at the insistence of any unsolicited caller.
- Do not purchase any software or services
- Ask if there is a fee or subscription associated with the "service" -- if there is, hang up
- Never give control of your computer to a third party unless you can confirm that it's a legitimate representative of a computer support team with whom you are already a customer
- Write down the caller's name, company, and contact information. It may very well be fake, but at least you'll have something to give to the police or other authorities.
- If you fall for a fake tech support scam and later realize your mistake, treat the incident as a serious security breach. Immediately change all of your passwords. Uninstall any software that you installed at the caller's behest. Disable remote access if you enabled it.

- Monitor your bank and credit card accounts closely and consider closing them if you detect any unauthorized transactions.

Ransomware

A new type of malware is showing up in email messages and it is very important that you understand what it is and how it gets installed on your computer. Ransomware is a type of malware that tries to extort money from you. One of the nastiest examples, CryptoLocker, takes your files hostage and holds them for ransom, forcing you to pay hundreds of dollars to regain access.

CryptoLocker starts encrypting your personal files as soon as it gains access to your system, preventing access to the files without knowing the encryption key. CryptoLocker then displays a message informing you that your files have been locked with encryption and that you have just a few days to pay up. If you pay them $300, they'll hand you the encryption key and you can recover your files.

This type of malware is another good example of why backups are essential. You should regularly back up files to an external hard drive or a remote file storage server. If all your files are on your computer, malware that infects your computer could encrypt them all and restrict access — or even delete them entirely. If you have files on a shared drive and the malware gets access to the files on that drive, they are all encrypted. No one will be able to get access to the files.

Aside from using a proper backup strategy, you can avoid ransomware in the same way you avoid other forms of malware. CryptoLocker has been verified to arrive through email attachments.

- Do not open email attachments.

- Use a good antivirus product that will attempt to stop ransomware in its tracks. Antivirus programs are never perfect and you could be infected even if you run one, but it's an important layer of defense.

- Avoid running suspicious files. Ransomware can arrive in .zip files attached to emails, from illicit websites containing pirated software, or anywhere else that malware comes from. Be alert and exercise caution over the files you download and run.

- Keep your software updated.

How To Tell If That Pop-Up Window Is Offering You A Rogue Anti-Malware Product

Rogue anti-malware products are a bane for every Internet user, especially those who have little or no technical know-how. This section examines these scareware scams: how they work, how to spot them and how to prevent them from infecting your computer.

Rogue anti-malware products are among the most persistent and annoying types of malware. Often called "scareware," rogues are usually do-nothing computer programs that mimic legitimate security software. They've plagued Internet users since at least 2005 and in some instances, have been linked to spyware infections. Some rogue distributors have even stolen the credit card numbers of users who have paid for their fraudulent applications.

Distributors of rogue anti-malware also release clones of these products, sometimes on a daily basis. This is done to avoid detection by security software vendors and users alike, and can be accomplished as simply as changing the product name on the graphic interface. Unfortunately, many of these rogues have legitimate-sounding names and look like the real thing

Like most rogues, this non-functional piece of software uses scare tactics to frighten users into purchasing it. A “your computer is infected!” pop-up appears, which links to a shopping cart to purchase the phony product. After it’s purchased, the scareware often appears to scan and remove a dozen or so phony viruses from a user PC.

At best, purchasing rogue anti-malware software is a waste of money. At worse, it may result in a purchaser’s credit card information stolen and sold on the Internet black market. Some rogues even install malware that steals personal information from a PC, connects the PC to a botnet and leaves it accessible to scammers for other malicious uses.

Spotify wasn't just serving up tunes over the last few days (Nov. 6, 2016)

The streaming music company confirmed that some listeners on the free version of its service saw "questionable website pop-ups" that continually opened up a device's browser. The company, which counts about 70 million people as users of its commercial-driven free service, confirmed the problem in a response to a user complaint on its community site.

The problem is called "malvertising" -- aggressive or ill-intentioned ads that, like malware, take control of some functions of your computer. Some users complained of actual malware getting installed on their computers.

Spotify blamed a single ad and said it has shut that ad down. "We will continue to monitor the situation," it said.

3 Reasons Hackers Love Your Small Business Infographic

1. **Hackers Prey on the Weak**
   - Small businesses are often less equipped to protect against an attack and dedicate fewer resources to fighting cybercrime

2. Hackers love internal access
   - 77% of all employees leave their computers unattended
   - Stealing credentials from key employees allows hackers to send email that looks legitimate to other companies they want to attack by disguising the email to look like it’s coming from a business partner.
   - Disgruntled formal employees pose internal threats, stealing trade secrets and data, and increasingly use Internet cloud services to hack companies by gaining remote access to corporate networks.
   - One of the country’s large scale breaches was hacked by gaining entry through a HVAC technician who had access.

3. Hackers love what small business have to offer
   - 95% of credit card breaches that Visa Inc. discovers are from its smallest business customers
   - Intellectual property
   - Personally identifiable information

Things You Should NEVER Share Online

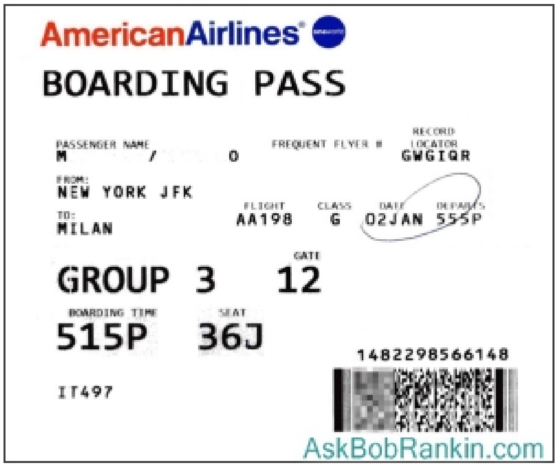
Two major trends are in conflict on the Internet. “Security” is big these days; it’s more important than ever to protect yourself against ever-increasing cyberthreats. “Sharing” is equally big, thanks to companies like Facebook and Twitter which make money when you share your thoughts, experiences, and other life-stuff with strangers. But security and sharing do not mix well. Here's what you need to know...

Are You Over-Sharing?

Look at airline boarding passes as an example. People excited about going on vacation often post pictures of their boarding passes on social media. (I guess they fear their “friends” won’t believe them without proof.) Unfortunately, those boarding passes may contain all the information an identity thief needs.

Delta Airlines’ boarding passes include the E-Ticket number, booking reference, frequent flyer number and even how many bags you have checked in. Go to Delta’s site and you’ll find the “manage existing trips” option. All you need to login there is the passenger’s name and E-ticket number or booking reference. That allows anyone with that info to change your seating assignment, change the date of your return flight, or even cancel your tickets. That's just one example; most airlines have the same type of barcodes and online passenger portals.

In some cases, the barcode on an airline ticket contains also the passenger’s phone number, date of birth, frequent flyer number, payment information, passport data, names of others in your party, and where you'll be staying upon arrival. Few passengers realize that, so even the security-conscious fail to cover it when taking a photo. Barcode readers are cheap, and many cybercrooks have them.



AmericanAirlines

BOARDING PASS

PASSENGER NAME
M / O

FREQUENT FLYER #

RECORD LOCATOR
GWGIQR

FROM:
NEW YORK JFK

TO:
MILAN

FLIGHT	CLASS	DATE	DEPARTS
AA198	G	02JAN	555P

GROUP 3

GATE
12

BOARDING TIME	SEAT
515P	36J

1482298566148

IT497

AskBobRankin.com

Tickets to concerts and other events should not be posted online until after you have used them. Tickets bear all the info necessary to create useable counterfeits. Many people have been disappointed at the box office to learn their tickets have already been used. Of course, you should never post a picture of a check online.

You should never tell the world that you are or soon will be on vacation or away on business. You might as well put a sign on your lawn that reads, “Nobody home, rob this house.” Use private messages to inform people who really need to know that you’ll be away for two weeks. Wait until you get home to share vacation photos and anecdotes with everyone.

Is Your Slip Exposed?

Going on a date to someplace expensive? Muggers would love to know that. Throwing a bridal shower where there will be a heap of expensive gifts? A home invasion is possible if you post the place and time online weeks in advance. Your social life is full of opportunities to get ripped off, or even physically harmed. Don’t share it with strangers.

Linking one of your social networks to another may prove embarrassing, at the least. When you link a Facebook account to a LinkedIn account, suddenly your professional colleagues know your personal life. One guy got fired this way; he called in sick at work and then bragged on Facebook about putting one over on the boss. His boss saw that and fired him.

Parents and grandparents love to post pictures of children, and they rarely consider the long-term effects on their offspring. A recent story making the rounds tells of an 18-year-old Austrian girl who is suing her parents because they refuse to take down 500+ "potty pics" and other embarrassing baby photos posted on Facebook.

Aside from causing possible embarrassment, a photo can reveal sensitive info about kids, and enables a creep to recognize a child. Mentioning the child’s name enables a creep to say, “Hey, Jenny, Grandpa So-and-So sent me to take you to his house.” Don’t mention anything about children on social media that can help perverts find and trick them. Remember, they’re kids, who trust easily.

More Facebook Faux Pas

I am constantly amazed by Facebook users who share their phone numbers and even home addresses with everyone. Ditto for users who leave location services enabled on Facebook or Twitter. I had to tell one single mom, via Twitter direct message, that her phone was broadcasting the street address of her home to the whole world. She had a major panic attack.

Facebook reports that 40 percent of its users leave their entire profiles open to the public. That means everything you post is available to 1.2 billion people! Take the time to get familiar with Facebook’s privacy settings and lock down your profile. Then be careful to make “friends” only of people who are friends in real life. The rest are strangers, and you don’t know what they might do with your personal info.

Even close friends and spouses should not have your passwords. Breakups happen, and before they happen someone often sneaks a peek at someone else’s social media accounts. Facebook has become a divorce attorney’s best friend, saving thousands of dollars on private investigators.

Cloud Storage and your privacy – more revelations

Anyone who uses email or cloud storage should be worried about some news stories of last few days. They show how email hosts and cloud storage is regularly snooped on by law enforcement who also act to keep it secret.

This isn't targeted court orders against specific people. This is bulk tapping of messages from any least one major online provider.

On a slightly better note, one company shows how to deal with privacy intrusive court orders and still be entirely within the law.

Yahoo 'hoovers' email for the US Government

Reuters has discovered that Yahoo created software to allow the US Government (NSA and FBI) to copy all incoming messages or attachments which had certain words or phrases.

This was bulk collection and copying of personal messages in way not seen before.

According to experts, it's the first known example of a broad range and real time check of messages according to certain key words or phrases.

You'd hope that the scanning of messages was for some anti-terror or other high importance crime but there's no way of knowing that.

While this action was only for incoming emails, it could easily be extended to documents and images saved on cloud storage.

Transparency Reports

You'd be naïve to think that Yahoo was the only participant in this program. Both Microsoft and Google have denied any involvement but, if they did, they would be forbidden from saying so.

It's worth noting the Yahoo's own 'Transparency Report' saying nothing about this major intrusion on customer privacy.

Unfortunately, none of these reports from any company can be taken at face value. Even if the company honestly wants to be fully transparent to their customers, the company can be legally prevented from telling customers what they are passing to a government.

Signal shows how it should be done

The best way to handle government intrusion on customer data is simple – don't store any customer data!

That's what sensible companies do like Open Whisper Systems (OWS), makers of the well-respected Signal messaging app.

The US government served a subpoena on OWS to hand over information they had about two customers. Subscriber details, addresses, telephone numbers, email addresses, method of payment, browser history, IP addresses, server logs etc. They wanted everything Signal/OWS had related to two phone numbers.

Signal complied with everything they had – which was very little. The time the account was created and the last time the user connected to the service. That's it.

By design, OWS/Signal keeps very little information about their users. None of the messages are retained, not even a 'call log' of when, where and who exchange messages on their system.

We're NOT saying you shouldn't use cloud storage for email and documents. It's far too useful to totally ignore. But everyone should consider the downside of cloud storage. Emails, documents, images on OneDrive, Google Drive, Dropbox etc are 'owned' by those companies which can read your information and pass it onto others.

The news of the last few days confirms what we already knew. Sometimes the companies are legally forced to hand over customer data and forbidden from telling customers that it's happening. We know that Microsoft has read customers emails for their own self-interest.

Adobe Flash Zero Day Exploits

There have been recent Flash Zero Day exploits that are being used to allow an attacker to take control of the affected computer. The Adobe Flash Player continues to be the favorite browser plugin threat actors have been focusing on this year. The recent zero-day exploit that was used in targeted attacks is now part of mainstream exploit kits. Because Flash has been such a hot target this year, it is recommended to uninstall it from your computer.

Below are instructions on how to uninstall Flash. This needs to be done immediately!

1. Click on the Start button
2. Click on Control Panel
3. Click on Uninstall A Program
4. Click on the Adobe Flash Player program
    - There will probably be a version number beside the name, i.e., 19 Active X and/or 19 NPAPI) You will need to uninstall all Adobe Flash programs
5. Click on the Uninstall button at the top of the list
6. Click on the Uninstall button on the Adobe Flash Player dialog box that displays
    - You may get an error telling you that you will have to close a program before it can complete the uninstall (i.e., Firefox, Internet Explorer.) Leave the dialog box on the screen, but close the program that is running in the background.
7. Close the Control Panel windows when you have finished uninstalling the toolbar

Microsoft Silverlight is another program that has known security issues that Microsoft isn’t going to correct. Follow the steps above to uninstall that program as well.

Windows 10 collects too much user data, lacks security says watchdog

Microsoft has been told to reduce the data Windows 10 collects about users and tighten up the OS security or risk facing sanction for breaching data protection rules.

By Nick Heath | July 21, 2016, 6:13 AM PST

Windows 10 is insecure and surreptitiously collects excessive data about what users do on their computer, according to a French authority.

Microsoft's flagship OS violates the French data protection act, according to the country's Chair of the National Data Protection Commission (CNIL), which highlighted the "seriousness of the breaches".

Microsoft has three months to change how Windows 10 collects data about users in order to comply with the act. If Windows 10 still doesn't comply after this point the company could be fined up to €150,000.

Windows 10 breaches user privacy in several areas, according to CNIL, which says the data the OS collects about users is "excessive".

Windows 10 transmits user data back to Microsoft by default, with users of Home and Pro versions only able to reduce data collection to the "Basic" level. On this setting, Windows 10 collects information about security settings, quality-related info (such as crashes and hangs), and application compatibility. Users of Enterprise, Education, and IoT core editions are able to reduce the data collection further, to what Microsoft calls the "Security" level.

Given Microsoft says that the data collected at the "Security" level is the bare minimum necessary to keep Windows machines "protected with the latest security updates", the collection of any data above and beyond this is not needed, the CNIL says in its formal notice.

"It is apparent that some of these data are not directly necessary for the operating system to work," it states.

"Most of the data included in the basic level are not essential for the system to operate so collecting such data is excessive with respect to this purpose."

Windows 10 also breaches the act in how it associates an advertising ID with each user, the watchdog said. This unique identifier allows a profile to be built of which apps are used and how.

Microsoft doesn't "validly obtain users' consent" for associating them with this ID, CNIL said, due to the way the ID is activated by default when the operating system is installed.

Windows 10 also downloads advertising cookies to users' machines without informing them or seeking permission, according to CNIL.

The authority also takes issue with how Microsoft handles Windows 10 user data, questioning why it is being transferred out of the EU under the terms of Safe Harbor, the data-sharing agreement declared "invalid" by the European Court of Justice in October.

Windows 10 does not ensure security

Beyond its data privacy failings, the CNIL also criticised Windows 10 for the poor security of allowing Windows users to log in using a four-figure PIN.

Windows 10 users who have associated their Microsoft account with a Windows 10 machine can then log into that machine using a PIN.

CNIL described this four-figure PIN as a "weak password" and said Windows did not lock the account after 20 attempts to guess the PIN — only requiring a reboot after five unsuccessful attempts.

These failings mean Windows 10 does "not ensure the security of confidentiality of the data that can be accessed using the PIN on the user's computer", it states.

CNIL is also concerned that logging in using the PIN automatically authenticates that device to connect to all of the online services linked to the associated Microsoft account — providing access to email and information about "store purchases and the payment instruments and devices used".

Addressing CNIL's concerns, Microsoft VP and deputy general counsel David Heiner committed the company to working with the authority over the next three months.

"We built strong privacy protections into Windows 10, and we welcome feedback as we continually work to enhance those protections. We will work closely with the CNIL over the next few months to understand the agency's concerns fully and to work toward solutions that it will find acceptable," he said.

Heiner said Microsoft would also work towards conducting transatlantic data transfers under the terms of the newly agreed Privacy Shield agreement.

Windows 10 Anniversary Update: Watch out for these nasty surprises

A major update to Windows 10 is being rolled out. These are the gotchas that are catching out early users.

By Nick Heath | August 8, 2016, 9:28 AM PST

Windows 10 users are getting the first major update to the operating system in just under a year, with the release of the Anniversary Update.

But alongside the new features and fixes are some more unwelcome changes, ranging from less control for users to frozen machines.

Here are the main gotchas to look out for, as well as some fixes.

Frozen computers and broken systems

When you update software there is always risk that something will break, and that's exactly what seems to be happening for some who have received the Windows 10 Anniversary Update.

The most common complaint seems to be that the update causes the computer to lock-up soon after loading the desktop.

In response to the problem, Microsoft has been advising users to run Windows 10's Maintenance Troubleshooter and if that doesn't work, to perform a clean boot of the system.

Meanwhile, users are reporting the most reliable fix has been to roll back to an earlier build of Windows 10.

Another repeated complaint is that Microsoft's virtual assistant Cortana is missing from the Task Bar, replaced instead with a search box. In affected systems, Cortana also seems to be disabled inside the Edge web browser.

Some users of Avast and McAfee anti-virus - both widely used products - are also reporting problems after the upgrade, as are gamers trying to use Xbox One controllers.

Cortana is more difficult to get rid of

If you're not a fan of Microsoft's virtual assistant Cortana then prepare to dislike the Anniversary Update.

Following the update, it is no longer possible to turn off Cortana from the virtual assistant's in-built Settings menu.

Instead, if users want to ditch Cortana they will need access to specific admin tools or to edit the registry.

Users can also minimise the information that Cortana collects, although this does require altering various settings.

Harder for admins to block ads

Another less welcome change is that Windows 10 Pro users lose the ability to use admin tools to block ads.

Prior to the update, admins could edit Group Policy settings to stop ads for apps showing in the Start menu and on the lock screen.

However, Windows 10 Pro users will lose that ability, and, following the update, disabling these ads via Group Policy settings will only be available to those running Windows 10 Enterprise, Windows 10 Pro Education, or Windows 10 Education editions.

Individual users should be able to turn off many of these ads by disabling Windows 10 tips, tricks, and suggestions and Windows Store suggestions in the Settings app, however.

Following the Windows 10 Anniversary Update, new installs of Windows 10 will show double the number of ads for Windows Store apps in the Start Menu. Some users have also reported a possible increase in the number of ads shown on the lock screen following the update.

Take control of your privacy in Windows 10

Where do you draw the line on personal privacy? The right options are different for everyone. In this guide, I show you which privacy settings help you create the right balance of privacy and convenience in Windows 10.

By Ed Bott for The Ed Bott Report | September 19, 2016 -- 10:45 GMT (03:45 PDT) | Topic: Windows 10

Over the past year, I've read countless "privacy guides" for Windows 10. Most are well-intentioned, but they invariably take a simplistic approach to privacy: Just turn off every switch in the Privacy section of the Settings app.

If you do that, you're not understanding the privacy landscape, which encompasses far more than just those settings. You're also missing some important additional steps.

Windows 10 is a mix of software and services. With every session, a Windows 10 device exchanges a great deal of information with Microsoft's servers. That's neither unusual nor alarming. Microsoft's chief rivals, Google and Apple, are also blending services into their software, with the goal of making your life easier and making that software more reliable.

So are other tech companies that you don't think of as software companies: Amazon, with the Echo. Tesla, with its self-updating, software-driven cars. Your thermostat and your home security system.

There's something profoundly satisfying about a service that anticipates your every move, reminding you when to leave for an appointment to arrive on time, or to pick up flowers for your anniversary tomorrow. Your digital personal assistant, whether it's Siri or Cortana or Alexa or Google, needs to be able to see your calendar and contacts to make that magic happen.

But when that sort of personal attention goes too far, it "crosses the creepy line," to use a phrase that Eric Schmidt probably regrets uttering when he was Google's CEO.

The thing about that line is that it's drawn in a different place for everyone. I know people who are thrilled at the idea that their PC or mobile device is so familiar with their actions that it can anticipate what they'll do next. I know others who would like to build a virtual Faraday cage around their computing hardware so that none of their personal details can escape.

Both of those viewpoints, and everything in between, are perfectly valid. That's why the software and services we use are loaded with switches and dials designed to help you take control of their potential privacy impact.

In this post, I'll walk you through the big privacy questions for Windows 10, with enough context to help you decide which settings are right for you.

Note that this guide assumes you are using Windows 10 on a personal PC or one in your small business. If you are in an enterprise setting, or if you are in a regulated industry, you should seek professional assistance to ensure that you're meeting proper standards.

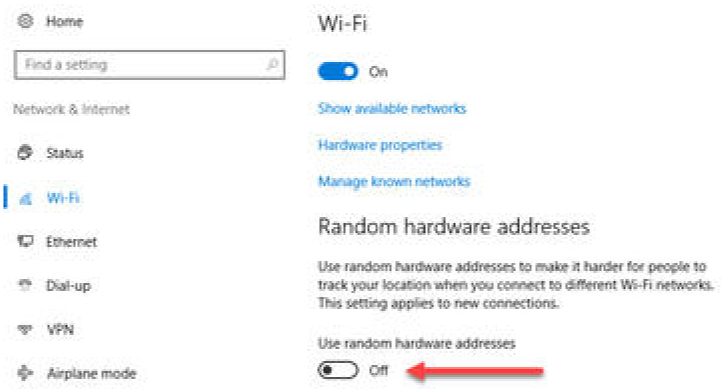
Let's start with the part of your PC that has the biggest impact on your personal privacy.

The network

No one knows more about your online identity than your Internet service provider. Every packet you send or receive from anywhere online goes through their servers. When you travel and connect to Wi-Fi networks that are under the control of others, the owners of those networks can see every connection you make and can intercept their contents.

Regardless of the platform you use, that's why it's important you use encrypted connections for any kind of sensitive communications. Using a virtual private network whenever possible is an excellent best practice.

Windows 10 does offer one obscure option that can help protect third parties from tracking your movements based on your connections to Wi-Fi networks. (Note that this feature requires support from your Wi-Fi adapter, so if you don't see this option, the most likely explanation is that your hardware doesn't support it.) Under Settings > Network & Internet > Wi-Fi, turn the **Use random hardware addresses** setting to On.



Wi-Fi

On

Random hardware addresses

Use random hardware addresses to make it harder for people to track your location when you connect to different Wi-Fi networks. This setting applies to new connections.

Use random hardware addresses

Off

Use this option to prevent unwanted location tracking

That step keeps third parties from matching your Wi-Fi adapter's hardware address with your personal information, making it more difficult to track your location.

The browser

Countless third-party ad networks and analytics companies use cookies and other tracking technology to record your movements around the web and to correlate your online activities with your offline identity.

The result is a digital fingerprint that can be extraordinarily detailed and, unfortunately, outside of your ability to change.

Ad-blocking software can also provide some privacy protection as a side-effect of performing its basic function. Here, too, watch out for close ties between some ad-blocking add-ins and the third-party trackers they supposedly protect you from.

Note that none of these steps is unique to Windows 10. Anti-tracking software is typically a browser add-in and works with most popular browsers.

The operating system

With those two big, platform-independent factors out of the way, we can now turn to Windows 10 itself. When you use a Windows 10 device, it is capable of sharing the following types of information with Microsoft's servers:

Your location

Windows 10 can determine your location to help with actions like automatically setting your current time zone. It can also record a location history on a per-device basis. Go to Settings > Privacy > Location to control the following:

- Location on/off   Use the master switch at the top of this page to disable all location features for all users of the current device.
- Location service on/off   If location is on for Windows, you can still turn it off for your user account here.
- General location   This allows you to set a city, zip code, or region so that apps can deliver relevant content.
- Default location   Click **Set default** to open the Maps app and specify the location you want Windows to use when a more precise location is not available.
- Location history   Click **Clear** to erase the saved history for a Windows 10 device.

If location is on, a list at the bottom of the Settings > Privacy > Location page allows you to disable access to that data on a per-app basis.

Your input

If you enable Cortana, Windows 10 uploads some info from your devices, such as your calendar, contacts, and location and browsing history, so that Cortana can make personalized recommendations. If you don't want any accounts on your PC to use Cortana, follow the steps in this article to disable the feature completely: **Turn off Cortana completely**.

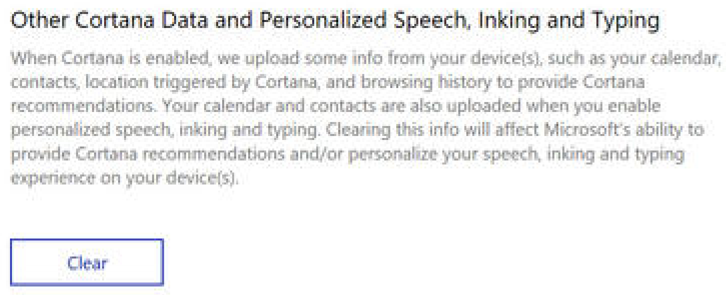
Windows 10 uses some feedback from the way you type, write, and speak to improve performance for you and as a way to improve the overall platform. This isn't keystroke logging; rather, the operating system uses a very small amount of information. A separate feature uses your speech and writing history to make better suggestions in Windows and Cortana.

You can control this collection with two sets of controls:

Under Settings > Privacy > General, click **Info about how I write** and turn it off so that your typos aren't used to improve things like the built-in spell checker.

Under Settings > Privacy > Speech, inking, & typing, under the Getting to know you heading, click **Stop getting to know me** to turn off personalization.

To clear previously saved information associated with your Microsoft account, click the first link under the **Manage cloud info** heading. That takes you to this Bing Personalization page, which includes this prominent button:



Other Cortana Data and Personalized Speech, Inking and Typing

When Cortana is enabled, we upload some info from your device(s), such as your calendar, contacts, location triggered by Cortana, and browsing history to provide Cortana recommendations. Your calendar and contacts are also uploaded when you enable personalized speech, inking and typing. Clearing this info will affect Microsoft's ability to provide Cortana recommendations and/or personalize your speech, inking and typing experience on your device(s).

This online option lets you erase information Windows 10 previously saved

Click Clear to remove that saved information from the cloud.

Files and settings

When you sign in with a Microsoft account, you have the option to save files to the cloud using OneDrive. Windows 10 also syncs some settings to OneDrive, allowing you to have the same desktop background, saved passwords, and other personalized settings when you sign in with that account on multiple PCs.

If you use a local account, of course, none of your settings are synced. If you use a Microsoft account, you can turn off syncing completely or remove certain settings from the sync list by going to Settings > Accounts > Sync Your Settings.

OneDrive is an opt-in service. If you don't sign in, it does nothing. You can't save files to OneDrive accidentally, and no files are uploaded without your explicit permission, which you can revoke any time. To disable OneDrive for all users on your PC, follow these instructions: **Shut down OneDrive completely**.

Telemetry

Microsoft, like all modern software companies, uses feedback from its installed base to identify problems and improve performance. In Windows 10, this feedback mechanism produces diagnostics data (aka *telemetry*) that is uploaded to Microsoft at regular intervals. The data is anonymized and is not used to create a profile of you.

If you want more information about how telemetry works, see **Windows 10 telemetry secrets: Where, when, and why Microsoft collects your data**.

The default telemetry setting for all consumer and small business versions of Windows 10 is Full, which means that the uploaded data also includes details (also anonymized) about app usage. If you are concerned about possible inadvertent leakage of personal information, I recommend that you go to Settings > Privacy > Feedback & diagnostics and change the **Diagnostic and usage data** setting to Basic.

The apps

Although the number of subcategories under the Privacy heading in Settings seems daunting, most of them govern access to your information by Windows Store apps. That set of apps includes those that are preinstalled (Mail, Calendar, Groove Music, Photos, and so on) as well as those you acquire from the Store.

Most of the categories offer a single on-off switch at the top, which you can use to disable all access to that feature by all apps. If you leave the feature enabled, you can use a list of apps at the bottom of the page to enable or disable access on a per-app basis.

This capability works the same with the following categories: Camera, Microphone, Notifications, Account Info, Call History, and Radios. The Other Devices category lets apps automatically share and sync info with wireless devices that aren't explicitly paired with your PC. Use the Background Apps category to specify which apps are allowed to work in the background.

If Location is enabled, you have the option to disable location access on a per-app basis and to disable Geofencing.

The Contacts, Calendar, Email, and Messaging categories allow you to control which apps can have access to these features. If you want to share content from an app using email or messaging, this option has to be on for that app. Note that Mail and Calendar, People, and Phone always have access to your contacts; Mail and Calendar are always allowed to access and send email and always have access to your calendar.

Finally, one horribly misunderstood setting is available under Settings > Privacy > General. Advertising ID controls whether Microsoft serves personalized ads to ad-supported apps. If you turn this option off, you still get ads, but they're not personalized. In any case, your information is not shared with advertisers.

Beware what’s inside an Office document

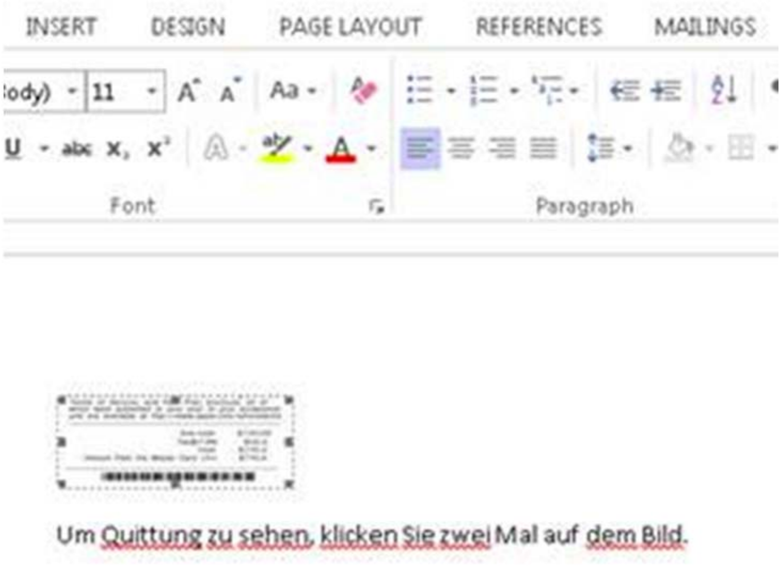
Microsoft has released details of a new way Office documents can be used to infect your computer. The documents can contain disguised OLE objects which are the real danger.

We've often said that 'new' Office documents (.docx .xlsx etc) are safer than their .doc etc predecessors. That's because the new '.???x' files won't run VBA code.

But hackers are always looking for ways to trick us and they've found one by adding a OLE object which carries the virus.   It takes more steps to run the virus code but people still fall for it.

Here's how this particular trick works and then we'll look at what should make you wary about opening emails or documents like this.

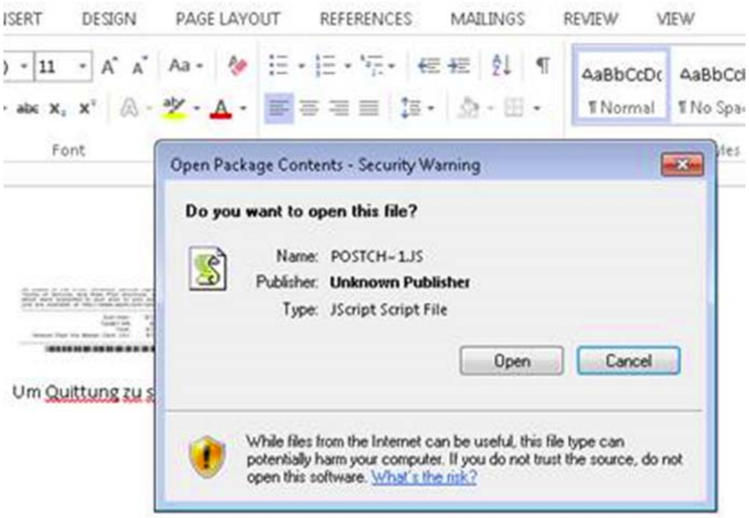
In this case, a document arrives via email that pretends to be an invoice. Open the .docx document and you'll see an innocent looking 'picture' in the document with a note in German "*"To see a receipt, click twice on the screen.*"



Um Quittung zu sehen, klicken Sie zwei Mal auf dem Bild.

Source: Microsoft plus our cropping

Double-click on the item and you'll get a security warning.



Um Quittung zu s

Open Package Contents - Security Warning

Do you want to open this file?

Name: POSTCH~1.JS
Publisher: Unknown Publisher
Type: JScript Script File

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open this software. What's the risk?

Source: Microsoft plus our cropping

The Javascript .js file is given an innocent looking name but the result is the same … an infected computer. The Microsoft post goes into some detail about what Trojan:JS/Certor.A does. It has its own root certificate which looks very sincere but allows the hackers to track even your 'secure' HTTPS traffic.

It changes your proxy server settings so that all your web browsing goes via a hackers computer for snooping. The virus also installs Tor software to hide the hackers computers.

What to look for

There are a few 'red flags' that should alert any wary computer user:

- A bland, almost blank email with no details but an attachment.
- Yes, the attachment is a .docx file but otherwise the message has all the hallmarks of a scam email.
- Open the document but instead of opening fully in Word, use the Outlook preview pane.
- In the document there's nothing but a request to open yet another item. That's very unusual so – red flag!
- Clicking on the object triggers a security warning – BIG red flag!!!!!!!!
- More tech savvy users will see that it's Javascript code inside a Word document. That's not common or likely.
- Happily, this particular virus is known and should be caught by any decent anti-virus software or spam filter.

But the best defence is you … the wary computer user.

Is Windows 10 right for you? Here are some of the reasons you might not want to upgrade.

1. You're worried about privacy

By default Windows 10 collects more data than many users are comfortable with. This includes information about how Windows and Windows apps are used, what you type, your contacts, your location, calendar appointments and more. If the virtual assistant Cortana is enabled, this data extends to web browsing history, voice commands and even more information about your activity.

Users of Home and Pro versions of Windows 10 can only reduce this data collection to the "Basic" level. On this setting, Windows 10 collects information about security settings, quality-related info (such as crashes and hangs), and application compatibility. Microsoft describes this information as being essential for maintaining and improving the quality of Windows 10 and says that only "anonymous identifiers" are transmitted.

However, questions remain about the information that Windows 10 sends back to Microsoft, even when you turn the data gathering settings down a minimum. Tech website Arstechnica found that even with the virtual assistant Cortana disabled, Windows 10 sends a request to www.bing.com that appears to contain a random machine ID that persists across reboots. Similarly, even when Microsoft OneDrive cloud storage was disabled and Windows 10 was not tied to a Microsoft account, the OS still seemed to be sending information to a server connected to OneDrive. While Microsoft stressed there is no query or search data being sent, Arstechnica queried the inclusion of a machine ID.

ZDNet's Ed Bott has said the very basic telemetry data collected by Microsoft is anonymized and doesn't reveal anything more than very high-level information along the lines of an unidentified Windows 10 user ran a particular app for half an hour.

However, for some users, even the gathering of anonymized usage data is more than they're willing to put up with.

2. It might cause pain for older machines

Windows 10 can run on a computer with relatively modest specs, working on many older PCs that shipped with Windows 7. But just because you can run Windows 10 on paper, you may not be able to in practice.

While the Get Windows 10 app that schedules the upgrade from Windows 7 or 8.x should check your system compatibility, some users that pass this test complain the upgrade still fails or devices don't work properly.

As Microsoft states: "The upgradability of a device includes factors beyond the system specification."

Microsoft gives you the option to rollback your machine to its previous OS, but there are reports from multiple people who claim the upgrade left their machine virtually unusable. In these cases either the rollback feature didn't work or it did work but the earlier OS is no longer stable, with previously working programs crashing.

If the upgrade process completes successfully, missing driver and firmware support has also caused difficulties for some Windows 10 users. Those affected cite problems such as monitors not working at their native resolution. Some of the Intel integrated graphics chips used in older laptops are also incompatible with Windows 10, though Windows 10 should warn of this fact.

These problems don't seem to affect the majority of upgraders, but it's worth being aware they exist, particularly if upgrading an older machine.

On a less serious level, upgrading to Windows 10 may not break your machine but it could mess with your settings. Microsoft has come under fire for Windows 10 changing users' default settings in a number of areas, such as swapping the default browser to its own Microsoft Edge.

3. Less control over updates

Windows 10's update process happens both more frequently and less obviously, with Windows Home and Pro users automatically receiving updates when they're available.

Windows Home users have less control over how long they can postpone updates for, and less easily-available information about what changes these updates will make.

The lack of control that Home users have over when updates are applied led to a group of users petitioning Microsoft to let them delay and refuse these downloads. Their reasoning was that since forced updates can crash machines, for instance via bad firmware or driver updates, all users need control over how updates are applied.

Another core concern for some users when it comes to Windows 10's frequent updates is the amount of data downloaded, with updates often weighing in at hundreds of megabytes. However, Windows 10 does allow users to block all but essential updates by toggling on 'metered connection' in the WiFi settings.

4. You don't like the new look

As much as Windows 10 has won people over by bringing back elements of the classic Windows desktop and Start menu — anyone fresh from Windows 7 will need to adjust to Windows 10's new look.

Unlike Windows 7, Windows 10's Start Menu takes up far more room, thanks to a menu full of tiles that is bolted onto the side. While most users should be able to quickly adjust to these cosmetic and layout changes, other alterations may grate more. Perhaps the most controversial tweak to the Start Menu is the inclusion of adverts for apps in the Windows Store. These promoted apps are tiles that link to the Windows Store or to apps that have been automatically installed on your PC by Microsoft. With the latest Anniversary Update, the number of these promoted apps will double, from five to 10.

And while it can be argued that Windows 10 is arguably easier to navigate, with its search function built directly into the Taskbar, the new OS introduces some significant changes that may confuse new users.

Whereas Windows 7 allowed users to adjust their system settings using the Control Panel, Windows 10 has both the Control Panel and Settings pages — with some configuration options exclusive to one or the other. This mix and match approach has been described as disorientating by some users.

5. Missing features

Windows 10 may add many new features — the virtual assistant Cortana, the new Edge browser — but it also lacks some key elements of earlier Windows operating systems.

Perhaps the biggest omission are the placeholders for Microsoft's OneDrive cloud storage service. In Windows 8.1, placeholders, also called smart files, let users see all of the files stored in the OneDrive service, whether those files were stored on the device or not. This feature was removed from Windows 10. Microsoft appears to be working on reintroducing placeholders, although there is still uncertainty about when they will be brought back.

Windows Media Center, the software for TV, music and movie playback is also gone from Windows, so if you are particularly attached, and not willing to mess around with an unofficial version, you may want to pass on the upgrade.