Computers and Stuff.

Report scams to the ACCC via www.scamwatch.gov.au or by calling 1300 795 995.

Windows Secrets
Everything Microsoft forgot to mention.

Master Macros in Microsoft Office.

Macros are an under-used feature of the Microsoft Office Suite – they are often spoken of in awe as though they are the biggest and badest thing you could ever imagine and are to be avoided at all costs. But that's not the case at all, used correctly they can be a very helpful tool.

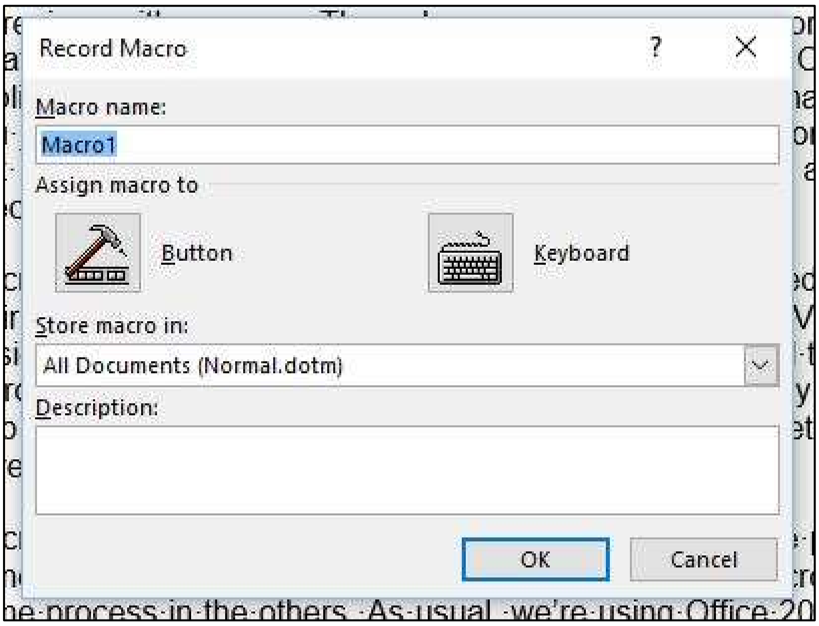
You can automate a host of time-consuming tasks using macros. For instance, do you find yourself running the same laborious and repetitive commands and tasks in Microsoft Word or Excel? There must be a better way, you say to yourself. And there is - with macros. Through a macro, you can record or create a series of commands and tasks in a Microsoft Office application. Then, whenever you want to run those commands, you just trigger the macro. You can create macros to automate just about anything in a program like Word or Excel -- apply special formatting, change the layout, insert objects.

Macros definitely sound intimidating if you've never ventured into their territory. They're stored as mini programs using the Visual Basic for Applications (VBA) language. But you don't need to be a programmer to use macros, you can record the macro by performing the various commands step by step then edit the macro to make any changes. Let's check out how to use macros to save time in Microsoft Office.

Macros are available in Word, Excel, and PowerPoint. The process for creating a macro is the same across all three applications so once you master macros in one program, you can use the same process in the others. As usual, we're using Office 2016 here, but the steps for creating, editing, and using macros are the same for the past few versions of Office.

Let's launch Word to kick things off.

Open any document with text. We'll try a relatively simple macro to start, one that I often use. I often give certain documents a specific font, point size, line spacing, and justification, and I can accomplish all those tasks in a single macro. Click on the View menu and then click on the Macros button. Select the option to Record Macro.



Macro name: Macro1

Store macro in: All Documents (Normal.dotm)

Description:

At the Record Macro window, type a name for your macro. The name can be up to 80 characters and can include letters and numbers but no symbols or spaces. The macro must also begin with a letter. Try to keep the macro name short so it's easier to use. In this case, I might create a name like RAMLayout. (You can assign a macro to a button or a keyboard shortcut, but we'll do that separately.)

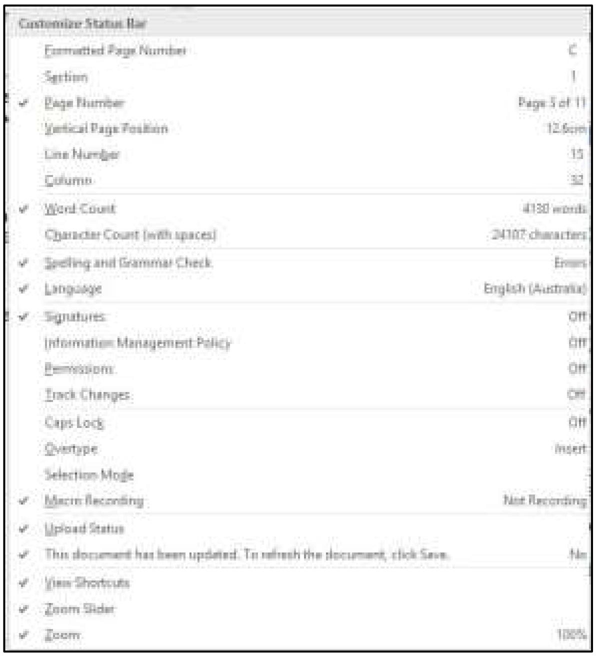
Type a description for your macro so you know exactly what it does. You can opt to store your macro in the default template for all documents or just your current document. Unless there's a reason you want to restrict the macro to your current document, keep this setting at All Documents. Click OK, and now the fun begins.

Select your entire document by pressing Ctrl+A. Now perform each of the following tasks one after another:

- Click on the Home menu.
- Change the font to Arial and the point size to 12.
- Click on the small arrow in the Paragraph section to access the Paragraph Settings window.
- Change the space for After to 0 points and the line spacing to Single.
- Finally, change the alignment to Justified.
- Click OK to close the Paragraph Settings window.
- Click anywhere in the document to turn off the selection and then make sure your cursor is at the top of the screen.
- Click on the View menu, select the Macros button, and click on the option to Stop Recording.

Now open a different document in Word, one without any of the formatting we used for the macro. Click on the View menu, select the Macros button, and click on View Macros. You should see your macro listed and selected. Click on the Run command, and the macro applies all the stored formatting and layout changes to your document.

Instead of going through the Macros button, you can click on the small macro recording button on the bottom status bar, the button to the right of the word count or page numbers. If it's not there, right click the status bar, the "Customize Status Bar" window (right) will open, click the box next to Macro Recording.



Customize Status Bar

	Formatted Page Number	C
	Section	1
✓	Page Number	Page 3 of 11
	Vertical Page Position	12.6cm
	Line Number	15
	Column	32
✓	Word Count	4130 words
	Character Count (with spaces)	24107 characters
✓	Spelling and Grammar Check	Errors
✓	Language	English (Australia)
✓	Signatures	Off
	Information Management Policy	Off
	Permissions	Off
	Track Changes	Off
	Caps Lock	Off
	Overtype	Insert
	Selection Mode	
✓	Macro Recording	Not Recording
✓	Upload Status	
✓	This document has been updated. To refresh the document, click Save.	No
✓	View Shortcuts	
✓	Zoom Slider	
✓	Zoom	100%

Going through the Macros menu to trigger a macro is a clumsy process, so put a macro the Quick Access toolbar. You can also assign a keyboard shortcut to a macro. Performing those actions in the Record Macro window is the easiest option but you can also do all that after the fact by customizing the Ribbon and customizing the Quick Access Toolbar. Follow these steps:

- Right-click on the Home Ribbon and click on the command to Customize the Ribbon.
- At the window to "Customize the Ribbon and keyboard shortcuts," make sure the Home Ribbon is selected in the right pane.
- Click on the New Group button. Make sure the new group is selected.
- Click on the Rename button and change the name to Macros.
- Click on the dropdown menu under "Choose commands from" in the left pane and change the view to Macros. You should see the two macros you created.
- Click on the first one in the list and then click on the Add button.
- Do the same for the second one. You can rename the Ribbon buttons for the macros and change their icons.
- Click on one of the macros and click on the Rename button. Type a new name for the macro button and select a different icon. Click OK.
- Do the same for the other macro. Buttons for your macros appear on the Home Ribbon.

Follow these directions to create a keyboard shortcut for each macro.

- Click on the Customize button next to Keyboard shortcuts at the bottom of the left pane.
- Under Categories in the Customize Keyboard window, scroll down the list and select Macros. Your two macros appear in the Macros window. Select one.

- Click in the Press new shortcut key field and press the keys on your keyboard that you want to use as the shortcut, for example, Ctrl+Shift+R. Make sure you don’t assign a shortcut that’s already used by a Windows or Office command.
- Click the Assign button.
- Do the same for the other macro.
- Close the Customize Keyboard window.
- Pressing one of the new keyboard shortcuts triggers the respective macro.
- At the window to “Customize the Ribbon and keyboard shortcuts,” change the selection to Quick Access toolbar.

You can now repeat the steps you used to add the macros to the Ribbon, this time adding them to the Quick Access Toolbar.

Finally, what if you want to edit the code for a macro to modify any elements? Even if you don’t know VBA, you can make certain changes and rename the macro.

Click on the View menu, select the Macros button, and click on the option to View Macros. Here you can delete a macro if you wish but we want to edit its code and change its name.

- Select the macro and click on Edit. The code for each macro appears.
- For the FullJustLayout macro we created, you can see lines of code for the font, point size, and other attributes.
- To change those, just replace the existing font name or point size with a different name or size. To change the name of the macro, look for the line of code at the beginning that says: Sub [the name of macro] ().
- Delete the existing name of the macro but don’t remove the Sub and () items.
- Type the new name for your macro.
- Press Ctrl+S when done to save the macro with your changes and the new name.
- Close the VBA window.

Editing or renaming a macro doesn’t affect any existing buttons or keyboard shortcuts. So you can run your edited macro from the Macros window, from the Ribbon, from the Quick Access Toolbar, or from your keyboard shortcuts.

Buyers' guide: choosing a smart speaker for your home.

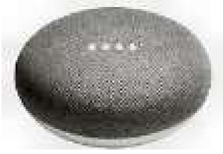
While Amazon pioneered the internet-connected speaker that responds to voice commands, it now has plenty of competition from other tech heavyweights. Even the original Amazon Echo has six Alexa-powered alternatives vying for your attention and dollars.

Digital assistants on these speakers — Amazon's Alexa, Google Assistant, Microsoft's Cortana and soon Apple's Siri — can play music, set timers and read off your calendar events. These speakers can also serve as a gateway to controlling other internet-connected appliances, such as smart lights, thermostats and even streaming video on TVs.

Here's a guide to choosing one for you or a loved one.

The Choices.

Amazon's $180 Echo (2nd Gen) is smaller and costs half what the original did at its 2014 debut. Variations range from the $85 Echo Dot, which has a lower-quality speaker, to the $495 Echo Show, which has a touch screen.



Google's speaker, the $165 Google Home, no longer challenges the main Echo on price. Bargain hunters can get the Google Home Mini for $65 or splurge for high-quality speakers in the $650 Google Home Max.

Apple. Early next year, Apple will compete at the high end with the $899 HomePod.

Microsoft. Microsoft's assistant appears on Invoke, a $185 speaker made by Samsung's Harman Kardon business. Samsung is also planning a speaker based on its own Bixby assistant, but there's no word yet on when.

Other manufacturers are also making speakers with Alexa or Google Assistant built-in.

The Smarts.

You can talk to Alexa, Google Assistant and Cortana as you would a friend. Ask any of them, "Do I need an umbrella today?" to get the forecast for rain. (Siri's capabilities on HomePod won't be fully known until it comes out.) Nonetheless, no single assistant does everything well. Alexa, for instance, won't let you set an alarm more than 24 hours out; its rivals do.

All three are learning. At first, Alexa was able to make calls only to other Alexa users. Now, it can dial regular phone numbers, too, for hands-free conversations. Google Assistant was the first to distinguish different voices, so it knows to play music on your playlist, not your teenager's. Alexa got that capability a few months ago. Cortana is still behind in many ways, but all three are racing to get better. Don't choose a device solely on what it can do today, as any small lead could be short-lived.

Favouritism.

Of course, each device will work best with its manufacturer's own services. Alexa, for instance, can read Kindle e-books in her computer-generated voice. If you just finished Chapter 23 on the Kindle e-reader or app, Alexa will continue with Chapter 24. You can also buy toilet paper and other items, on Amazon of course, with a voice command.

Cortana, meanwhile, can make calls using Microsoft's Skype service. When you set up Invoke, Microsoft's Outlook.com calendar is automatically linked; you have to add Google's yourself. Google Assistant can read only your Google calendar, not Apple's or Microsoft's. (Alexa is the only one to work with all three.) The assistants will work with many other services, though. Amazon is at the forefront in enabling third-party capabilities, so Alexa can call you an Uber ride or track progress on your Fitbit fitness tracker. Google and Microsoft are catching up. Meanwhile, Amazon and Microsoft have agreed to let their assistants summon each other; when that's enabled soon, Alexa can fulfil something Cortana can't do on its own.

Sound Quality.

These speakers can, of course, play music. If that's important, pay more for a quality device. Invoke is made by Harmon Kardon, experts in audio. Home Max and HomePod are also designed with sound quality in mind. As tempting as the $50 Echo Dot might be, Alexa sounds as though she's coming over a speaker phone, but if you already have good wireless speakers, you can pair them to the Dot with Bluetooth. You need Google's $35 Chromecast Audio device to pair other speakers with Home.

The three major assistants all work with Spotify. Alexa and Google Assistant work with Pandora as well, while Amazon and Google work with their own music services. Alexa also has Sirius XM.

Security and Privacy.

Expect your kids to mess around with the speaker, by asking an assistant to make fart noises, for instance. Parental controls are limited. Microsoft says it's still working on them. Google's controls are limited to its YouTube service. Amazon lets you set a PIN for ordering products by voice, but a lot remains unfiltered, including news that's not always pleasant.

Even among adults, there are security and privacy considerations.

These speakers are always listening, unless you hit a mute button. Companies insist that nothing is sent over the internet unless the device hears a key word, such as "Alexa" or "OK, Google." You can view your history of voice requests. Amazon and Google let you delete individual ones; with Microsoft, you can only delete your entire history.

Another consideration: If you're living in close quarters, a nosy neighbour could hear the assistant recite your doctor's appointment or upcoming travel plans.

Be Careful.

More people are getting voice-activated speakers and other smart devices for convenience and security, but doing so could also be giving hackers a key to their homes. Many devices from reputable manufacturers have safeguards built in, but those can't guarantee against hackers. Gadgets from startups and no-name brands may offer little or no protection.

Before buying one, here are some risks to assess:

Listening in.

Speakers with built-in microphones are increasingly popular. Devices such as Amazon's Echo and Google Home let people check the weather or their personal calendar with simple voice commands. Beyond that, many smart TVs and TV streaming devices now have voice-activated functions, often for playback controls and video search. Many newer toys also come with microphones, so kids can talk to them and get canned responses.

Many of these devices are constantly listening for your commands; when they receive them, they connect to corporate servers to carry them out. What if you're having private conversations at home? Are they getting sent over the internet, too? In some cases, sound recordings will only leave home when you trigger the device. You might have to speak a command phrase like "OK Google" or press a button to get the device's attention. Check before buying to make sure a product includes such safeguards.

Some gadgets go further. Smart speakers, for instance, typically have a mute button to disable the microphone completely. Amazon says its mute function involves disconnecting the circuit, so that hackers cannot override the intent.

But there's no easy way for consumers to verify manufacturer promises, such as Amazon's assertion that the Echo never transmits recordings to the cloud unless it's been activated. That's where it helps to stick with reputable brands, as their reputations are at stake if they're caught in a lie. Bigger companies can also quickly fix security holes that crop up.

Deeper Insights.

Missteps are still possible, even with reputable brands. One of the WikiLeaks disclosures alleged that the CIA commandeered some Samsung smart TVs as listening devices even when the TV appeared to be off. And beware of internet-connected toys, as manufacturers frequently rush their products to market, sometimes skimping on privacy features in the process.

One more catch: Voice commands sent over the internet are typically stored indefinitely to help manufacturers personalize their services (and, potentially, advertisements). These voice snippets may include music or conversations in the background. They can be sought in lawsuits and investigations. Reputable brands let you review and delete your voice history; be sure to do so regularly.

Watching You.

Online security cameras such as the Cam IQ, from Google sibling company Nest, let you check in on your pets or kids when you're not home. They also typically store video online, so you can see whether your housekeeper actually cleaned the kitchen last week. Some services routinely send video to online storage; others do so only when triggered by a sound or motion.
Again, reputable brands are likely to take security seriously, but no system is perfect.

If you want to be very careful, you might want to turn the camera to face the wall when you're home. You might also want to turn off the microphone, since it could capture background conversations. Or just unplug the camera altogether ... though you'll also have to remember to reconnect it when you leave. Along similar lines, consider covering up the front-facing camera on your laptop with opaque tape unless you need it

regularly for video chats. Laptops aren't supposed to send video unless you activate an app that needs it, but malware has been known to activate the camera remotely.

Digital Trails

Smart locks let you unlock doors with an app, so you can let in guests even when you're not home. Burglars might try to hack the system, though it's often easier for them to just break a window. Some rental properties are also turning to smart locks to control access. When you move out, the landlord can automatically disable your digital key. But these systems also let landlords track your whereabouts and those of your guests. If you create a guest key that's used daily, for instance, the landlord might suspect you have an unauthorized occupant. Even if you own the home, these keys can leave a digital trail. In a child-custody dispute, for instance, your ex might subpoena the records to learn that you've been staying out late on school nights.

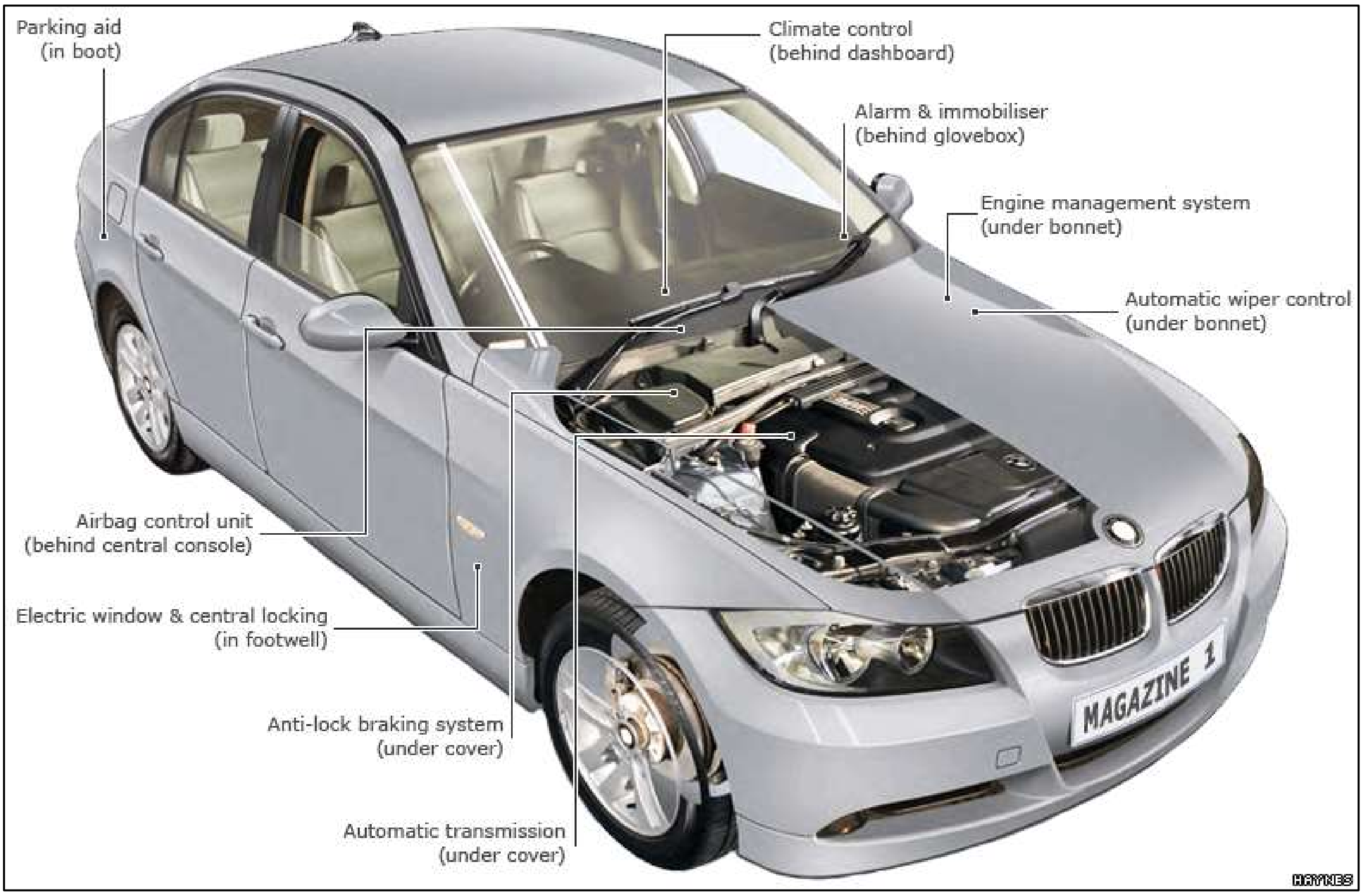
Here's how we can stop driverless cars from being hacked.

Once hackers get into your internet-connected car, they could disable the air bags, brakes, door locks and even steal the vehicle. That's the finding of researchers who recently uncovered a flaw in the way the different components of a connected car talk to each other. Their work follows several demonstrations of researchers remotely hacking into and taking control of cars, including one that led to a worldwide recall of one connected model of Jeep.

None of these hacks have yet been demonstrated with regular vehicles on the road, but they show how cyber security is becoming a big challenge to the car industry, especially as vehicles incorporate more and more driverless technology. It has even worried the UK government enough to release a set of guidelines for the sector. These emphasise the need for companies to work together to build resilient vehicles whose security can be managed throughout their lifetime. But what can actually be done to ensure that as cars effectively become computers on wheels they are kept safe from hackers?

There are three main reasons why cars are becoming vulnerable to cyber attacks, and these trends have also made security more challenging to design and test.

First, the different systems that make up a car are increasingly designed to work together to improve their efficiency and so they all need to be able to communicate, as well as being connected to a central control. Adding autonomous systems that make cars partly or fully self-driving means the vehicles also have to connect to other cars and infrastructure on the road. But this opens up what was traditionally a closed system to outside, possibly malicious influences. For example, we've seen demonstrations of attacks using cars' Bluetooth, WiFi and radio frequency (RF) on passive key entry systems, which all create possible entry points for hackers.

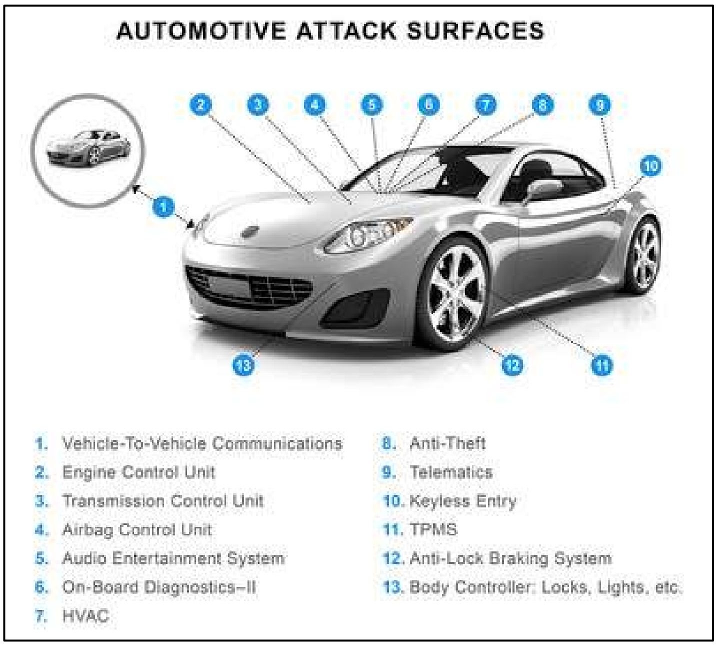

Parking aid (in boot)
Climate control (behind dashboard)
Alarm & immobiliser (behind glovebox)
Engine management system (under bonnet)
Automatic wiper control (under bonnet)
Airbag control unit (behind central console)
Electric window & central locking (in footwell)
Anti-lock braking system (under cover)
Automatic transmission (under cover)
MAGAZINE 1
HAYNES

Second, more features and functionality in cars means more software and more complexity. A single vehicle can now use millions of lines of code, put together in different ways in different components from different manufacturers. This makes it hard for security testers to know where to look, and hard for auditors to check a car complies with the rules. If the software recently used by Volkswagen to circumvent emissions limits had been a malicious virus, it may have taken months or years to find the problem.

Finally, the volume and variety of the data and content stored and used in a vehicle is ever increasing. For example, a car's multimedia GPS system could contain contact addresses, information about the driver's usual routes and, in the future, even financial data. Such a hoard of information would be very attractive to cyber criminals.

One of the best ways to protect connected cars from this growing threat is by building security into the design of the vehicles. This means, for example, ensuring that there are no conflicts, errors or misconfigurations in individual components. Fully assembled cars should be tested more rigorously to ensure the final product lives up against security hacks, using methods such as penetration testing, whereby systems are purposefully attacked to expose flaws. This in turn would mean better tools and standards that would force everyone in the industry to factor in security right from the start.

The next big challenge is likely to be designing vehicles that match security with safety. As self-driving technology evolves to use more artificial intelligence and deep learning techniques, we will be relying on yet more software to control our cars and make decisions on safety grounds like human drivers would. This will make it even more important that the cars are secure so that they also protect drivers' safety.


AUTOMOTIVE ATTACK SURFACES
1
2
3
4
5
6
7
8
9
10
11
12
13
1. Vehicle-To-Vehicle Communications
2. Engine Control Unit
3. Transmission Control Unit
4. Airbag Control Unit
5. Audio Entertainment System
6. On-Board Diagnostics–II
7. HVAC
8. Anti-Theft
9. Telematics
10. Keyless Entry
11. TPMS
12. Anti-Lock Braking System
13. Body Controller: Locks, Lights, etc.

Industry response.

The industry is slowly but steadily responding to the growing threat of cyber attacks. Aside from government regulations, the US Society of Automotive Engineers (SAE), has introduced its own set of guidelines that show how cyber security can be treated like other safety threats when designing a car. There are also efforts to make drivers more able to protect their vehicles, for example by warning them in car manuals against plugging in unknown devices.

In the longer run, the biggest challenge is simply getting the car industry to coordinate more. The sector is very competitive at every level, and companies rely on the latest autonomous and connected technologies to set themselves apart and win new customers.

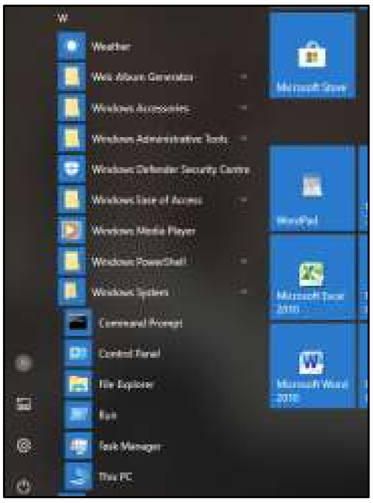
Unfortunately, this rivalry means that companies are reluctant to share intelligence about cyber threats and vulnerabilities or work together to develop more secure designs. To make cars truly secure we'll need to see the industry change gear.

A blonde walks into the CBA in George St, Sydney and asks for the loan officer. She says she's going to Europe on business for two weeks and needs to borrow $5,000. The bank officer tells her that the bank will need some kind of security for such a loan, so the woman hands over the keys to a new Rolls Royce that's parked on the street in front of the bank. Everything checks out, and the bank agrees to accept the car as collateral for the loan. An employee drives the

Rolls Royce into the bank's underground garage and parks it there. Two weeks later, the woman returns, repays the $5,000 and the interest, which comes to $15.41. The loan officer approaches her and says: "We are very happy to have had your business, and this transaction has worked out very nicely, but we're a little puzzled. While you were away, we checked out your accounts and found that you were a multi-millionaire. What puzzles us is why would you bother to borrow $5,000?" "Well' she said, "where else in Sydney can I park my car for two weeks for fifteen bucks?

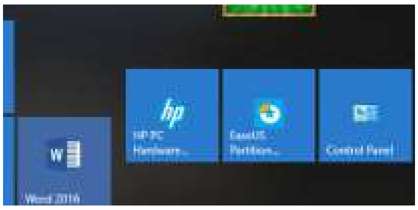
Control Panel.

Many Windows users have grown up with and have become accustomed to using MS's Control Panel. If there was a problem with your computer or you wanted to add or remove a device (add a printer or scanner etc) or change something, the first tool most went for was the Control Panel. You could look at the Control Pan two ways, either by Category or by Icon and it was/is a very handy tool. To access it all you had to do was click on "Start" down the bottom LHS of the screen and click it, but! - for some reason, MS thinks no-one wants it anymore and when they released the last couple of Windows 10 updates, they removed it from the Start button.



BUT – that's not the end of it. It's still there, you just have to know where it is and how to get it, and luckily, it's easy.

To get it back, Click START, then scroll down to the bottom of the Apps to the W heading, click on WINDOWS SYSTEM then RIGHT click CONTROL PANEL, then click PIN TO START. This will put it on the Start page.



If you want, you can also click on MORE, then click PIN TO TASKBAR which will put in on the taskbar at the bottom of your screen and either way make it available whenever you want it.

Any day on this side of the flower bed is a good day.

This page left blank.