Computers and Stuff.

Sam Houliston.

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

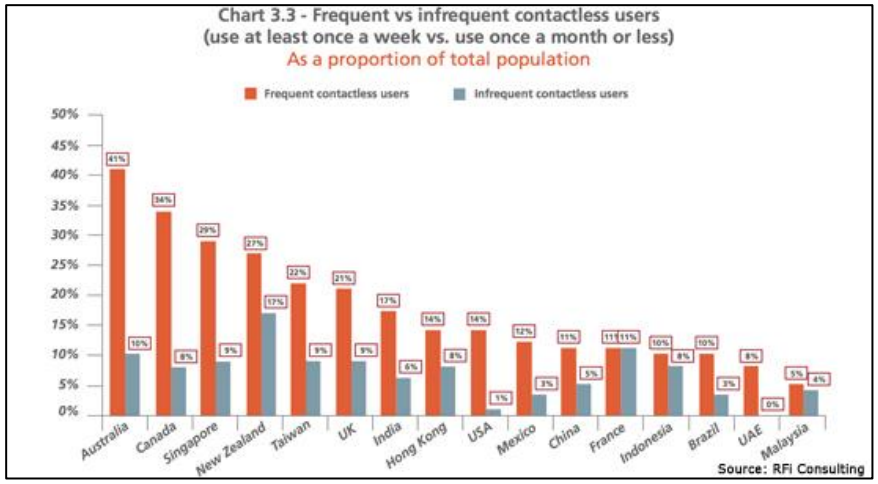
Four must-know secrets about Paywave.

THE NEWDAILY

Australians are the world's most prolific 'tap and go' payers, but the intricacies of the system still seem to concern some of us. Almost 60 per cent have used a contactless card at least once, and 41 per cent use them frequently, according to a new study published this week by banking research firm RFi Consulting. That's the highest rate in the world — and is much higher than in the UK and the US.

The technology allows customers to pay for purchases by tapping or hovering their cards over a terminal, without the need to insert the card or enter a PIN number. And we seem to love it. More than three quarters (76 per cent) of Australians said it was their favourite payment method, according to research published this week by Beyond Bank.

In that survey, most rated the experience highly. But there was still a sizeable number, about 20 per cent, that rated contactless payments between 1-5 out of 10. This could have something to do with security concerns. When asked about the current limit of $100 per transaction, a quarter of respondents told Beyond Bank it should be lower. Presumably they were concerned about theft.



Interestingly, the vast majority (82 per cent) agreed we are moving towards a cashless society. So let's allay some concerns, and perhaps reveal some secrets, about 'pay waving' before that future becomes reality.

1. 'Shields' are probably a waste of money.

You probably don't need one of these. A spokesman for Beyond Bank said there is a "lot of misinformation" about the security risks. It is a common misconception that thieves can 'clone' cards for later use. This is impossible because the computer chips in the cards send unique codes for each payment.

There is also a popular 'digital pickpocketing' theory that criminals can steal money simply by walking down the street with a special machine that charges nearby cards. Even if this technology exists, it would require thieves to receive the funds into an Australian bank account, making them easily trackable. Many companies are cashing in on these fears by selling 'protectors' or 'shields' that claim to prevent such attacks. The New Daily contacted several major banks to find out if these crimes had ever been reported to them. ANZ, Westpac and ME all said they had not received a single report of this happening in Australia. Ever. A spokesperson for regulator ASIC also said it had not seen any such incidents.

2. You can disable it.

You can ask for PIN-only. While 'digital pickpocketing' may be impossible, there is still the risk of the card itself being lost or stolen. Given the $100 transaction limit, quite a few illegal purchases could be racked up before a customer can cancel the card. The banks cover the cost of these crimes but some Australians may still feel uncomfortable carrying around the technology. No problem, many customers can request that their cards require a PIN for every purchase. For example, ANZ confirmed that it offers this service.

3. Beware of hidden payments.

Your account balance, or amount owing, could be out of date. It can often take days for contactless payments to be deducted from your account balance. As explained by an ME spokesperson, this is beyond both the customer and the bank's control: "This is dependent upon the merchant as they are required to settle their facility." Not seeing the full deductions can trick you into spending more than you can afford, so keep a close eye on all your pending transactions.

4. Watch out for fees.

Just because you're tapping-and-going doesn't mean you get to avoid those pesky fees charged by many merchants. The banks charge interchange fees of between 0.3 and 0.5 per cent on most credit card payments, which often get passed down from merchants to consumers. For many customers, paywaving is always processed as a credit transaction, even for debit cards. So, ask your merchant what they charge before opting for contactless.

For more paywave tips, check out the ASIC MoneySmart website.

Early aircraft throttles had a ball on the end of it, in order to go full throttle the pilot had to push the throttle all the way forward into the wall of the instrument panel. Hence "balls to the wall" for going very fast.

HDCP Error. (High-bandwidth Digital Content Protection)

Unbeknown to most consumers there's an anti-piracy protocol built right into the HDMI cable standard. Not only does it have a poor track record when it comes to piracy prevention it deteriorates the viewing experience for many people. This is how it works, why it spoils your TV viewing experience, and how you can fix it.

HDCP: DRM for the HDMI Age.

Digital Rights Management (DRM) protocols are protocols designed to protect content creators and distributors against piracy. Different companies and industries use different protocols, but the basic premise is the same. The DRM generally performs one of two tasks (or both) to prevent piracy:

a. it locks purchases to the purchase makers and,
b it locks content to authorized devices.

When you buy an album on iTunes and you can only listen to it on devices authorized by your account, you're experiencing DRM. When you buy an operating system or video game and they can only be installed on a single computer, you're experiencing DRM.

Content creators and distributors should be protected as it is expensive to create and distribute content and they should be compensated for that content. However, DRM typically makes life more difficult for honest paying consumers and in many cases, it can outright ruin the experience for those paying consumers. This is the kind of trouble you run into with games that require authorization servers to run, if the company goes under so does the authorization server and suddenly the game won't run.

In the case of the HDMI standard and digital video there's a DRM standard just like there is in other industries and that DRM standard causes headaches for regular consumers just trying to enjoy their televisions and engage in other legitimate activities.

HDMI's DRM protocol is known as High-bandwidth Digital Content Protection (HDCP). The protocol was developed by Intel and is used not just with HDMI but a variety of digital video standards like DisplayPort and Digital Visual Interface. It provides for an encrypted connection between a content outputting device (like a Blu-ray player, cable box, streaming stick like the Chromecast or Roku Stick) and a receiving device (an audio-video receiver in a media centre setup or the HDTV itself). HDCP is everywhere and is built into devices like Blu-ray players, cable boxes, satellite TV receivers and streaming video hardware like the Chromecast and Amazon Fire TV. It's also built into laptops and computer hardware, DVRs, and other modern HDMI devices.

Like other forms of DRM, such as the previously mentioned game authorization server, HDCP isn't without its problems and outright breaks the viewing experience for many consumers.

Blonde Interview. The executive was interviewing a young blonde for a position in his company. He wanted to find out something about her personality so he asked, "If you could have a conversation with any person, living or dead, who would you chose?" The blonde quickly responded, "The living one."

Where HDCP Breaks Down.

Although the underlying encryption and protocols are sophisticated and outside the scope of this article, the basic premise of how HDMI HDCP works is quite simple. There is a licensing body that issues licenses for HDCP devices. Each HDCP compliant device, like your Blu-ray player or Xbox, has a license and the ability to talk to the device it is outputting the signal to over the HDMI cable.

The outputting device says "Hey display! Are you HDCP compliant? Here is my license, show me your license!" and in turn the display (or other HDCP compliant device) returns with "I am! Here is my license!" When that process is working, it happens within a thousandth of a second and you, the consumer, never even notice. You power on your Blu-ray player or DVR, it shakes hands with your HDTV, and you live a happy life never knowing what HDCP even is. Unfortunately, however, there are a host of situations where HDCP gets in the way of consumers doing perfectly legal things with their devices and content. If any device in the chain is not HDCP compliant, the video stream will fail.

For example, if you have an older HDTV set that is not HDCP compliant then you cannot watch any HDCP compliant content on it. If you plug in your Blu-ray player, a Chromecast, or any other device that follows HDCP standards you'll either see a blank screen or you'll see an error message like "ERROR: NON-HDCP OUTPUT" or simply "HDCP ERROR."

So, if you want to turn that old monitor with integrated speakers into a cheap little video box with a Chromecast, there's a very good chance that the old monitor (despite having an HDMI port) is not HDCP compliant. You won't be streaming anything to it unless you want to dedicate a whole computer to the project.

Want to record your video game sessions or stream them live? It's hit or miss. Console makers are now better about recognizing that players want to record and stream their content but

HDCP is still problematic. The Sony Playstation lineup is a perfect example of this problem. While Sony did release an update in 2014 for the PlayStation 4 that unlocked HDCP lock while actually playing the game, they can't provide the same update for the PlayStation 3 because the HDCP output is locked at the chip level in the PS3. Their only advice is to buy a capture device that supports component cables and use those instead of HDMI.

Even when we're not actively watching TV or gaming, you could still find HDCP to be annoying and intrusive. There's nothing illegal or unethical about hooking a Blu-ray player up to an old TV, trying to recycle an old computer monitor into a little Chromecast-powered streaming station, recording and streaming your video game play, or trying to capture menus and screen shots to write tutorials and guides, but thanks to a flawed DRM protocol anyone who wants to any or all of those things is left in the dark.

So, can you fix this problem?

Absolutely no one should have to buy a new television set, upgrade their perfectly fine audio-video receiver, or otherwise spend significant piles of money to solve a problem that shouldn't exist in the first place, yet officially the only way to comply with HDCP is to buy a new HDCP-compliant device. The most absurd thing about the HDCP protection scheme is that there is no HDCP compliant way to circumvent it for legitimate use. There are zero methods endorsed or supported by the agency in charge of HDCP that help consumers in anyway if they have older equipment or a legitimate non-piracy need to interact in any way with an HDCP compliant device. To add further insult to injury, the HDCP standard has been compromised for years now and manufacturers continuing to pay for licenses and including it in their products has everything to do with not wanting to fight with the licensing agency and the anti-piracy lobby and very little to do with actually stopping piracy (or helping consumers). So what can you do to deal with the outdated and now compromised mess that is HDCP?

Short of buying a new television or giving up on your video game project the only way to deal with your HDCP compliance problem is to buy a cheap HDMI splitter that ignores HDCP requests. That's the secret media centre ingredient that has helped thousands of consumers.

One such device is the ViewHD 2-Port 1×2 Powered HDMI Splitter (Model: VHD-1X2MN3D) which you can buy from eBay for about US$25. There are a few of these on the market and unfortunately there is no consistency as to whether or not they will be HDMI compliant – the ViewHD model VHD-1X2MN3D is.

To use the splitter, simply put it between the device(s) giving you the HDCP error and the display device. For example, if you have a simple configuration like you just want to plug a Chromecast into an old monitor, you'd plug the Chromecast into "Input 1" on your HDMI splitter and use an HDMI cable to connect the splitter from "Output 1" to your display. If you have a new audio-video receiver that doesn't play nice with your old HDTV, plug all your HDMI devices into the receiver and then place the HDMI splitter between the receiver and the display.

You can imagine how absurd it is that the solution to a problem which shouldn't even exist is "buy an out-of-spec device that ignores the faulty protocol." Nonetheless, that's exactly the situation consumers find themselves in and thankfully, whether through poor or intentional design, there are products out there that get new media players talking to old HDTVs.

Energy-Efficient Batteries from Silicon in Diatomaceous Earth.

Researchers at the University of California have developed an inexpensive, energy-efficient way to create silicon-based anodes for lithium-ion batteries from the fossilized remains of single-celled algae called diatoms. The research could lead to the development of ultra-high capacity lithium-ion batteries for electric vehicles and portable electronics.

Lithium-ion batteries, the most popular rechargeable batteries in electric vehicles and personal electronics, have several major components including an anode, a cathode, and an electrolyte made of lithium salt dissolved in an organic solvent. While graphite is the material of choice for most anodes, its performance is a limiting factor in making better batteries and expanding their applications. Silicon, which can store about 10 times more energy, is being developed as an alternative anode material, but its production through the traditional method, called carbothermic reduction, is expensive and energy-intensive.

To change that, the UCR team turned to a cheap source of silicon, diatomaceous earth (DE), and a more efficient chemical process. DE is an abundant, silicon-rich sedimentary rock that is composed of the fossilized remains of diatoms deposited over millions of years. Using a process called magnesiothermic reduction, the group converted this low-cost source of Silicon Dioxide (SiO_2) to pure silicon nano-particles.

A significant finding in their research was the preservation of the diatom cell walls, structures known as frustules, creating a highly porous anode that allows easy access for the electrolyte. This research is the latest in a series of projects to create lithium-ion battery anodes from environmentally friendly materials. Previous research had focused on developing and testing anodes from portabella mushrooms and beach sand.

Batteries that power electric vehicles are expensive and need to be charged frequently, which causes anxiety for consumers and negatively impacts the sale of these vehicles. To improve the adoption of electric vehicles requires much better batteries. They believe diatomaceous earth, which is abundant and inexpensive, could be another sustainable source of silicon for battery anodes.

I bought the wife a hamster skin coat last week.
Took her to the fair last night, and it took me 3 hours to get her off the Ferris wheel.

New Zealand fibre uptake rate 10 times OECD average.

A "visionary" investment in fibre networks in New Zealand is propelling the country to the front of the OECD pack, network company Chorus told investors today.

Mark Ratcliffe, the Chief Executive of Chorus New Zealand, said the rate of fibre adoption in New Zealand is "comfortably" the fastest in the OECD and more than 10-times the OECD average. Chorus is a provider of telecommunications infrastructure throughout New Zealand. It is listed on the NZX stock exchange and is in the NZX 50 Index. It is the owner of the majority of telephone lines and exchange equipment in New Zealand and is also responsible for building approximately 70% of the new fibre optic Ultra-Fast Broadband network. It has received a government subsidy of $929 million to build the new fibre network.

The company was demerged from Telecom New Zealand in 2011 (now Spark), as a condition of winning the majority of the contracts for the Government's Ultra-Fast Broadband Initiative. By law, it cannot sell directly to consumers, instead it provides wholesale services to retailers.

2015 was the year that fibre went mass market in New Zealand, and that change has come about remarkably rapidly. Describing fibre as "the fourth utility", chairman Patrick Strange said, in contrast with New Zealand, Australia's fibre rollout was "awash in cost over-runs and red ink". British Telecom has been building out a fibre-to-the-cabinet network and Australia was now looking to do likewise, he said. "We completed our fibre-to-the-cabinet network in 2011, covering around 80 percent of the population."

Fibre use was taking off "massively", Ratcliffe said, outstripping the take-up of copper broadband at the same stage of availability. After four years of availability, copper broadband was used by about 8 percent of customers who could buy it, he said. Fibre adoption is already pushing 20 percent while availability was now "nudging ahead" of the OECD average. Ratcliffe said he had just returned from the Broadband World Forum in Europe and concluded they were not likely to catch up for "decades at least". Therefore, New Zealand needed to benchmark itself against the progressive broadband nations of Asia, not Europe and the US.

"We are the envy of many, they want to do what we are doing but haven't figured out how yet. I firmly believe that the fibre network we are building today will be a visionary investment that future generations will thank us for."

But it's not all good news!

While Chorus is clearly pleased with progress on the fibre rollout, it continues to struggle with regulation that has seen the price it can charge for legacy copper access, still the bulk of its revenue, slashed. "We are waiting on the final copper pricing decision from the Commerce Commission in December," Strange said. "The cost of this uncertainty is a cost to New Zealand. "That final price will have a significant bearing on our ability to fund ongoing investment in broadband."

Chorus has slashed costs, postponed non-essential maintenance and cancelled dividends while the regulatory issue is being settled.

How to beat ransomware:

Prevent, don't react.

Malwarebytes LABS

Picture this: You've spent the last few weeks working on a tribute video for a friend's 30th wedding anniversary. You collected photos and video clips and edited them together, laying over a soundtrack of their favourite songs. It was a real labour of love. When you finally finish the project, you go to copy the file onto a DVD and—what the?—a strange message pops up.

> "Unfortunately, the files on this computer have been encrypted. You have 96 hours to submit payment to receive the encryption key, otherwise your files will be permanently destroyed."

You've been hit with ransomware.

You didn't back up the anniversary video. In fact, you haven't backed up any of your files in months. What do you do? Unfortunately, when it comes to ransomware, once your files are encrypted, there's not much you can do—besides cut your losses or pay up. And even if you do pay up, there's a chance you won't get your files back, so you're out the files and your cash.

That's why it's so important to prevent ransomware attacks from happening in the first place.

Types of ransomware.

The first step in ransomware prevention is to recognize the different types of ransomware you can be hit with. Ransomware can range in seriousness from mildly off-putting to Cuban Missile Crisis severe.

Scareware.

Yes, it's called scareware, but in comparison to other types of ransomware, not so scary. Scareware includes rogue security software and tech support scams. You might receive a pop-up message claiming that a bajillion pieces of malware were discovered and the only way to get rid of them is to pay up. If you do nothing, you'll likely continue to be bombarded with pop-ups, but your files are essentially safe. A quick scan from your security software should be able to clear out these suckers. For simple instructions on how to clean an infected computer, check out our step-by-step guide later in this page. Remember, a legitimate antivirus or anti-malware program would not solicit customers in this way.

Screen lockers.

Upgrade to terror alert orange for these guys. When lock-screen ransomware gets on your computer, it means you're frozen out of your PC entirely. Upon starting up your computer, a full-size window will appear, often accompanied by an official-looking Government Justice Department seal saying illegal activity has been detected on your computer and you must pay a fine. In order to reclaim control of your PC, a full system restore might be in order. If that doesn't work, you can try running a scan from a bootable CD or USB drive. Remember, Governments will never freeze you out of your computer or demand payment for illegal activity.

If they suspect you of piracy, child pornography, or other cybercrimes, they would go through the appropriate legal channels.

Encrypting ransomware.

This is the truly nasty stuff. These are the guys who snatch up your files and encrypt them, demanding payment in order to decrypt and redeliver. The reason why this type of ransomware is so dangerous is because once cybercriminals get hold of your files, no security software or system restore can return them to you. Unless you pay the ransom—they're gone. And even if you do, there's no guarantee you can get those files back.

So what should you do about this kind of ransomware? Get out in front of it. "If any attack in the history of malware proves that you need protection in place before an attack happens, encrypting ransomware is it," says Adam Kujawa, Head of Intelligence at Malwarebytes. "It's too late once you get infected. Game over."

Ransomware prevention.

The first step in ransomware prevention is to invest in awesome cybersecurity. Start with an antivirus with active monitoring and layer on other applications that are specifically designed to thwart advanced malware attacks such as ransomware.

Next, as much as it may pain you, you need to create secure backups of your data on a regular basis. You can purchase USBs or an external hard drive where you can save new or updated files—just be sure to physically disconnect the devices from your computer after backing up, otherwise they can become infected with ransomware, too. Cloud storage is another option, but we recommend using a server with high-level encryption and multiple-factor authentication.

Finally, stay informed. One of the most common ways that computers are infected with ransomware is through social engineering. Educate yourself on how to detect phishing campaigns, suspicious websites, and other scams. And above all else, exercise common sense. If it seems suspect, it probably is.

10 easy steps to clean your infected computer.

Malwarebytes LABS

You log onto your computer and it takes forever to boot. When it finally does, a few unfamiliar applications litter your desktop, and your browser immediately sends you to an ad for hair loss products. Sounds like your PC has a problem with malware.

So what should you do? Before you flip out, try these simple steps to clean up your infected computer.

1. Computer acting suspect?

- Do a little digging and check for symptoms.
- Look for issues characteristic of a malware infection:
- Does your web browser freeze or become unresponsive?
- Do you get redirected to web pages other than the ones you are trying to visit?
- Are you bombarded with pop-up messages?
- Does your computer run slower than usual?
- Do you see new icons on your desktop that you don't recognize?
- Unfortunately, even if you see nothing wrong with your computer, there may be trouble brewing under the surface, sneaking around and screwing with your files undetected. So it's a safe bet to move on to Step 2 even if you can't find a symptom.

2. Use protection: Enter safe mode.

- Remove CDs and DVDs, and unplug USB drives from your computer. Then shut down.
- When you restart, press the F8 key repeatedly. This should bring up the Advanced Boot Options menu.
- Select Safe Mode with Networking and press Enter. Only the bare minimum programs and services are used in this mode. If any malware is programmed to automatically load when Windows starts, entering safe mode may block the attempt.

3. Back up your files, including documents, photos, and videos.

- Do not back up program files, as those are where infections like to hide. You can always download these programs again if files are lost.

4. Download an on-demand malware scanner such as Malwarebytes Anti-Malware.

- Follow set-up instructions and install the program.

5. Disconnect from the Internet. Then run a scan.

- If you truly believe you are infected, do not pass go, do not collect $100. Just go directly to the scan. If you do have an infection, your on-demand scanner should let you know that you in danger, girl. A list of scan results tells you what malware was found and removed.

6. **Restart your computer. After all, everyone deserves a second chance.**

7. **Confirm the results of your anti-malware scan by running a full scan with another malware detection program.**

   - Restart again if the program found additional infections.

8. **Update your operating system, browser, and applications.**

   - If there's an update available on any of your software, go ahead and do it. Some of the most dangerous forms of malware are delivered by "exploits" that take advantage of out-of-date software.

9. **Reset all of your passwords.**

   - Before being deleted, malware could have captured your passwords and forwarded them to hackers. Change each and every password you can think of, and make sure they're strong. None of this 1, 2, 3, 4, 5 business.

10. **If, after all of these steps, you're still having problems with a possible infection, feel free to post your question in the Malware public forum.**

We've said it before, but should probably say it again - keep your operating system software up to date - apply updates as soon as is reasonably possible. Not such an issue with Windows 10 which tends to annoy people by doing updates whether or not they want them, more of an issue with Win7/8 and IOS. An IOS bug fixed earlier this year corrected a security hole where hackers could access your stuff simply by sending you a message which you ignored. Not something Apple gave a lot of publicity to, considering that IOS is the operating system that runs iPhones and iPads. Frightening!!.

With Windows, change the option to suppress the file extension for known file types so that the extension is always shown. (Click HERE to see how to do that). A friend a while ago got a scam email supposedly from the NSW RTA advising of a traffic infringement, as described in the attached PDF it said. The attachment was called infringement.pdf.exe but it displayed as infringement.pdf - after attempting to open it ransomware set in. Free version of Malwarebyes removed the malware, there were backups of all encrypted files, so they were lucky that time.

I very quietly confided to my best friend that I was having an affair.
She turned to me and asked, "Are you having it catered?"

And that, my friend, is the sad definition of "OLD"!