Computers and Stuff.

Sam Houliston.

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

How cyber criminals use social engineering

Social engineering is nothing new. It's a tool of psychological manipulation that's been used since the dawn of man. Why? To influence people into taking action that might not be in their best interest. Sometimes it's fairly harmless, like a child sweet-talking its parent in order to get an ice cream. (I'm a victim of this one.) Many times, however, social engineering is used for nefarious purposes.

There are classic examples of social engineering at play throughout human history. Confidence tricks were first used by charmers in the 19th century to con people into trusting others with their valuables. (They should not have trusted…the charmers made off with the goods.) Psychological manipulation, otherwise known as propaganda, influenced droves of people during World War II to go out and buy war bonds. And advertising subtly hints that you're not pretty enough until you buy this product.

Social engineering taps into the human psyche by exploiting powerful emotions such as fear, urgency, curiosity, sympathy, or the strongest feels of them all: the desire for free stuff. Which is why cyber criminals have caught on.

Cyber crooks use this dangerous weapon to get at the weakest link: us. They know that the easiest way to penetrate a system is to go after the user, not the computer. "Attacking the human element has always been a favourite," says Jean-Phillip Taggart, Senior Security Researcher at Malwarebytes. "Why use some hard technical flaw to acquire a password when you can simply ask the user for it?"

In fact, psychological cyber attacks are on the rise. "We are seeing an increase of blended attacks that rely on a combination of social engineering and malicious software," says Taggart.

For example, a popular social engineering tactic is the technical support scam. An alert pop-up will appear on the screen that tells the user he is infected and needs to download a malware application. The user, fearful of infection, will download the fake antivirus or anti-malware application that is instead a vehicle for delivering malware.

So how are the criminals distributing their social engineering schemes? Here are some of the most prevalent forms of social engineering today.

Clickbait:

"Huge snake eats man alive!" Have I got your attention? What if I posted a link to a video of the ordeal? You just might be tempted to click, especially because many legitimate articles and other pieces of content use similarly eye-catching headlines to get people to look at their stuff. Cyber criminals get this, and they exploit it.

A particularly popular approach is to capitalize on the innately human desire to crane one's neck to see an accident on the side of the road. So beware of links to overly graphic terrorist attack images, natural disasters, and other tragedies.

Watering hole attacks:

One of the things cyber criminals do best is collect information about their targets. Browsing habits tell a lot about a person, which is why that ad for cat sweaters keeps popping up in your Facebook feed. Cyber criminals use this information the go after the sites most visited by their target group. Once they discover a particular website is popular with their targets, they infect the site itself with malware. For example, hackers knew the iPhone Dev SDK forum was visited frequently by Facebook, Apple, and other developers. They compromised the website, set up an exploit, and ended up infecting a lot of people.

Social networking attacks:

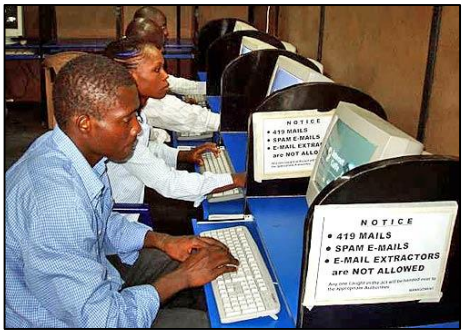
Social networking attacks can be particularly dangerous because criminals mess with your mind in two ways. First, they make digs at your personal information. Cyber criminals know that one of the biggest vulnerabilities people have is their self-image, people are worried about what others think of them. Second, they make their messages appear to come from a friend.

This two-pronged approach can be accomplished in one attack. You might receive a message from your ex-boyfriend that says, "lol, is this your new profile pic?" (with a picture of a walrus).

The picture has a link. You click on it, because what the heck, ex-boyfriend?! And would you look at that…you're infected with malware.

Ransomware.

Ransomware is nasty business. It's also social engineering at its finest/worst. Ransomware is a type of malware that holds your files or part of your system ransom. In order to return access, you have to pay cyber criminals. People who want their precious data back might pay up right away. But for those who need additional scare tactics, cyber criminals have come up with law enforcement scams that make it appear as though the Federal Police or Taxation Department are contacting you to claim that you've done something illegal.



Even worse, some cyber criminals will stoop to the level of claiming they found child pornography on your computer—and then display a piece of child pornography. So, they say, pay up and we'll make it go away. Users, naturally, tend to panic when faced with a message about child pornography that seems to come from law enforcement. This gross tactic has even lead, in an extreme case, to a user committing suicide.

Phishing/spear phishing.

If your dad has ever fallen for the old Nigerian prince tale, then guess what? He was phished. Phishing is a form of social engineering that relies on fooling people into handing over money or data through email. Bad guys accomplish this by sending a generic message out to a huge mass of people that might say something like, "You won $1 million! Click here for your reward!" Sadly, there are those that still fall for this.

However, in recent years cyber criminals have upped their phishing game with more sophistication. Spear phishing emails are crafted in order to make someone believe they're from a legitimate source. The messages might appear to come from banks or businesses and could include full names, usernames, and other personal info. Crooks know that if you get an email that looks like it's from your medical provider and it's talking about a surgery you had last year, you will likely believe it.

So how can you fend of these psychological attacks? Here are a few tried and true methods:

- Equip yourself with antivirus, anti-malware, and anti-exploit security programs. These can fight off malware attacks from a technical standpoint.
- Anonymize your data by using the privacy features of your browser. It's also a good idea to clear cookies every once in a while.
- Lock down privacy settings on social media accounts. Make sure you're making information available only to those you wish to have it.
- Use the right software and hardware systems. If you just use your computer to surf the web, you probably don't need a powerful processor or the Adobe suite. Every piece of software you put on your computer has potential vulnerabilities, the more you have, the greater your surface of attack is on a particular machine.
- Finally, and most importantly, use common sense. A healthy dose of scepticism goes a long way. Verify information. Contact the claimed source. Trust your gut feeling, if it feels too good to be true, it probably is. If it feels slightly off, it probably is. Stop and think about what is being asked of you.

I sat opposite an Indian lady on the train today, she shut her eyes and stopped breathing. I thought she was dead, until I saw the red spot on her forehead and realised she was just on standby.

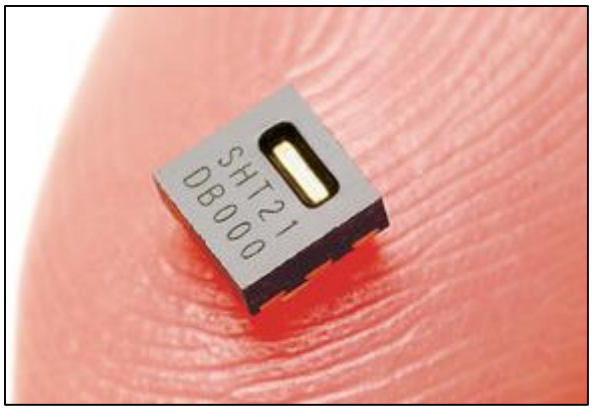
The Internet of things.

Some thirty years ago, the personal computer revolution began — and no other technology has evolved more quickly. Now there a new revolution, often referred to as the Internet of Things. Here's what you need to know about it.

The term Internet of Things (IoT) made little sense to me when I first heard it. I thought: "Oh no! Not another meaningless tech-industry marketing term — like Web 2.0." But then I visited my pool-supply store and the sales person asked me whether I wanted to connect my pool pump to the Internet. As you might expect, my first reaction was: "Why?" I left the store a bit bewildered and spent the next several months looking into the topic of new Internet-connected devices. What I've discovered took me by surprise.

The Internet of Things extends far beyond just attaching your thermostat (or pool pump) to the Internet. In the broader sense, IoT could encompass any instance in which objects or

organisms (including people) are fitted with sensors that collect and transfer data over a computer network. No human-to-human or human-to-computer interaction is required.
IoT isn't driven simply by convenience; the ultimate goal is collecting and processing large amounts of data in real time. More than fifty years of technology discovery and development has brought us to this point. For example, with nanotechnology we can now build data-collecting sensors that measure in billionths of an inch. These tiny devices are described as nano-electromechanical systems — or the somewhat larger microelectromechanical systems (MEMS).



Right, a tiny MEMS humidity and temperature sensor from Sensirion.

These data sensors are so inexpensive and so tiny they can be placed everywhere: in cars, homes, clothes — and even in our bodies. That potential flood of data collection would easily overwhelm our current IPv4 Internet-addressing scheme which is why we're moving to the more-capable IPv6. This newer addressing system uses 128 bits, an address space so large that each person on earth could be given a few Octillion (10 to the power of 27) IP addresses and there would still be a lot of addresses left over. In short, it will be nearly impossible to run out of IPv6 addresses.

With many ways to collect data, we also need ways to move the information to the computers that will process it. In the past, this connection was via Ethernet cabling. But now we live a mobile world. Advances in Wi-Fi and cellular transmission rates now make it more practical to move mountains of data wirelessly and if GPS is added to a sensor, we can know exactly where the data came from.

Data processing has also grown exponentially over recent years. Massive server farms and cloud-storage facilities make real-time processing of huge amounts of data — popularly called Big Data — cheap and practical. (Cloud storage is about a tenth the cost of local storage.) And all this "Big Data" is now stored in "Data Lakes," where it might reside for years or even decades to come.

Currently, hard drives still do the heavy lifting in data storage but tech companies are working on new forms of computer memory (RAM) and data storage. For example, Carbon nano tubes could increase storage in our devices up to a thousandfold — while using less electricity. It's quite possible that in the next five to 10 years, your smartphone might have 10TB of RAM/disk storage and a month of battery life.

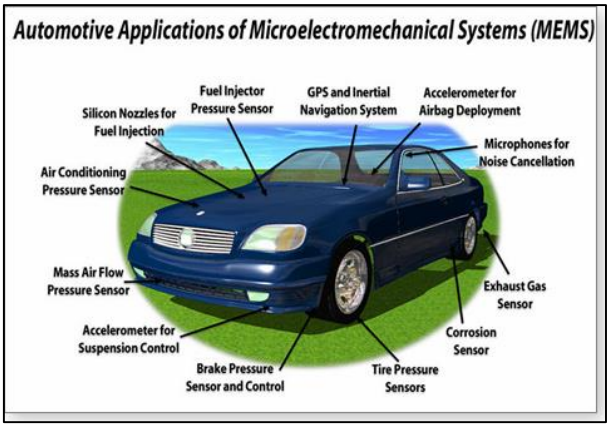
And what becomes of all this collected information? Businesses use sophisticated data analytics to process it — outwardly to "make our lives better," but mostly to make a profit. For

the most part, the information is cleaned, sorted, and combined with other data to build models of our online behaviour. That information is then used essentially to convince us to purchase products and services.

Connecting everything to the Internet.

What does the Internet of Things offer us today? It's far more than you might realize. You might be familiar with products such as the Nest thermostats and smoke alarms; or wearables such as Fitbit devices that monitor heath and exercise. But IoT is rapidly expanding into more prosaic things; for example, I found a BBQ propane-tank sensor that will notify you that it needs refilling or that you forgot to turn off your gas stove. And then there's that pool pump I mentioned that can be monitored and controlled via a smartphone app. Parking spaces can be fitted with IoT sensors; as you enter a parking garage, you can be notified ahead of getting to it where an open space is located. Power companies are using IoT in appliances and solar systems to manage and track energy usage.

And that's just the consumer side. Things get really interesting when you look at IoT for the business-to-business (B2B) market. Farming, automotive, security, and heath care are taking advantage of Internet connectivity. In farming, for example, cameras have been mounted on booms attached to tractors. As the machines are driven though the fields, the cameras take images of each plant and also record its GPS location. An on-board computer system processes the images in real time and determines whether a particular plant needs a shot of fertilizer, pesticide, or water, or is doing fine. The health of the plant is recorded and archived (again, Big Data) so that farmers can make year-over-year comparisons.



Many newer cars already have Wi-Fi and Bluetooth connectivity built in. Your next new car will most likely have at least four high-definition (HD) cameras, a hundred or so performance sensors, and a cellular data-service plan, not for you, but for the automobile manufacturer to keep tabs on the car. You and millions of other drivers will be "testing consumers," so manufacturers can produce better cars. But they'll also be able to monitor wear and tear on individual vehicles. In theory, they could use GPS data to tell you, via your onboard navigation/information system, that it's time to change the oil — and here's the location of the nearest dealer.

Onboard cameras and computers can now prevent unsafe lane changes, assist in emergency braking, and help with parking. The videos from the cameras can be stored, so should you have an accident, the images can be downloaded and used for any follow-up investigation.

IoT is rapidly finding its way into security. For example, retail stores that suffer heavy losses to shoplifters might install wireless cameras. Though some are visible, others are hidden. That mannequin could actually be watching you. These connected cameras can capture the face of anyone who enters the store; they then immediately compare that information against a list of known shoplifters. If there's a match, the store's security staff can then track the person's movements throughout the store. IoT, Big Data, and cloud storage let stores share a common database of known shoplifters. Someone caught stealing at the local department store will be recognized and watched at the nearby home-improvement store. The next time you enter a store, check out your image on a conspicuously placed, high-definition screen; it's there to remind you that you're being watched.

In health care, IoT-equipped pacemakers monitor heart rhythm. If a pacemaker detects an abnormal rhythm, it can notify a doctor, dispatch emergency-medical personnel and initiate treatment. Moreover, if the device is equipped with GPS, it can send out your exact location. IoT is assisting with pain management and neurological diseases. I was recently told that doctors have imbedded Windows 10 computers into patients. Using wireless connections and the Internet, doctors can remotely manage pain or, in the case of those with neurological diseases, send software updates that help patients cope with their illness.

The dark side of ubiquitous IoT applications.

We are a well aware of security on our phones and computers. But the concept of billions of devices connected to the Web raises real concerns over hacking, privacy, and personal security. For example, there was an uproar when it was shown that smart TVs might be capable of sending private conversations back to Web servers. And it was recently shown that hackers could take control of cars remotely. Anything attached to the Internet is a potential target.

Potentially more difficult, will be finding a balance between security and privacy. For many, having your neighbour record your comings and goings and sending that data to police computers is unacceptable. But if you've been the victim of a burglary, you might think it's okay. And will you be comfortable knowing that your car's manufacturer, and possibly your insurance company, can track your driving habits?

Again, one of the foundations of IoT is targeted marketing. Not too long ago, a woman who was still in high school began receiving drugstore ads targeting pregnant women. The woman's father (angrily) asked the chain store that sent out the ads why; he was told that, thanks to Big Data, it knew his daughter was pregnant. I'm sure that's not the way we'd want to learn about a loved one's private matters.

When I was in the pub I heard a couple of plonkers saying that they wouldn't feel safe on an aircraft if they knew the pilot was a woman. What a pair of sexists. I mean, it's not as if she'd have to reverse the thing!

Beware the Apple!

'Error 53' fury mounts as an Apple software update threatens to kill your iPhone 6. It's the message that spells doom and will render your handset worthless if it's been repaired by a third party. But there's no warning and no fix.

Thousands of iPhone 6 users claim they have been left holding almost worthless phones because Apple's latest operating system permanently disables the handset if it detects that a repair has been carried out by a non-Apple technician. Relatively few people outside the tech world are aware of the so-called "error 53" problem, but if it happens to you you'll know about it. And according to one specialist journalist, it "will kill your iPhone".

The issue appears to affect handsets where the home button, which has touch ID fingerprint recognition built-in, has been repaired by a "non-official" company or individual. It has also reportedly affected customers whose phone has been damaged but who have been able to carry on using it without the need for a repair.

But the problem only comes to light when the latest version of Apple's iPhone software, iOS 9, is installed. Indeed, the phone may have been working perfectly for weeks or months since a repair or being damaged. After installation a growing number of people have watched in horror as their phone, which may well have cost them $500-plus, is rendered useless. Any photos or other data held on the handset is lost – and irretrievable.

Tech experts claim Apple knows all about the problem but has done nothing to warn users that their phone will be "bricked" (ie, rendered as technologically useful as a brick) if they install the iOS upgrade

A journalist dropped his iPhone while covering the refugee crisis and had to use a local repair shop. He says this happened to his phone a few weeks ago after he upgraded his software. He had previously had his handset repaired while on an assignment in Macedonia. Because he desperately needed it for work he got it fixed at a local shop, as there are no Apple stores in Macedonia. They repaired the screen and home button, and it worked perfectly. He thought no more about it until he was sent the standard notification by Apple inviting him to install the latest software. He accepted the upgrade, but within seconds the phone was displaying “error 53” and was, in effect, dead. When he took it to an Apple store in London, staff told him there was nothing they could do and that his phone was now junk.

The whole thing is extraordinary. How can a company deliberately make their own products useless with an upgrade and not warn their own customers about it? Outside of the big industrialised nations, Apple stores are few and far between and damaged phones can only be brought back to life by small third-party repairers. If you Google “iPhone 6” and “error 53” you will find no shortage of people reporting that they have been left with a phone that now only functions as a very expensive paperweight.

Could Apple’s move, which appears to be designed to squeeze out independent repairers, contravene competition rules? Car manufacturers, for example, are not allowed to insist that buyers only get their car serviced by them.

When pressed for more information about the error, few, if any Apple employees could offer an explanation. There was no part they would replace, no software fix, and no way to access the phone’s memory. The fix was a new iPhone. Though still largely a mystery to most, error 53 is the result of a hardware failure somewhere within the home button assembly.

AND! Here's the reply from Apple

If you see error 53 or can't update or restore your iPhone or iPad, follow these steps to get help updating or restoring your iPhone or iPad.

If your iOS device has Touch ID, iOS checks that the Touch ID sensor matches your device's other components during an update or restore. This check keeps your device and the iOS features related to Touch ID secure. When iOS finds an unidentified or unexpected Touch ID module, the check fails. For example, an unauthorized or faulty screen replacement could cause the check to fail.

If the check on Touch ID fails, your update won't finish. You'll see a Connect to iTunes screen on your device or a message like this in iTunes on your computer: The iPhone [device name] could not be restored. An unknown error occurred (53).

Follow these steps.

- Make sure that you have the latest version of iTunes.
- Force restart your device.
- Try to restore your device again.
- If you still see error 53 when you try to restore your device, contact Apple Support. If the restore won't finish and you see a different error code, learn what to do.

If the screen on your iPhone or iPad was replaced at an Apple Service Center, Apple Store, or Apple Authorized Service Provider, contact Apple Support. If the screen or any other part on your iPhone or iPad was replaced somewhere else, contact Apple Support about pricing information for out-of-warranty repairs.

So – if you've got an iPhone 6 and it needs repair, be warned!! We can see the lawyers sharpening their pencils now, look out for a rather large class action law case developing here!!! tb.

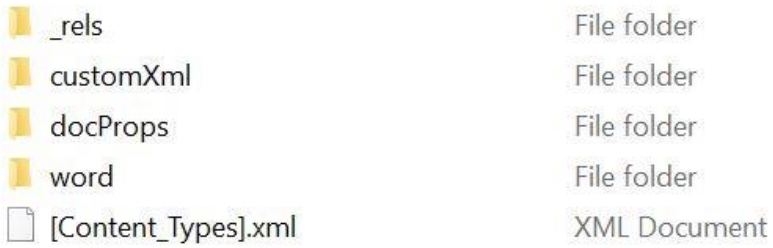
File Extensions.

File extensions are a type of metadata added to the end of computer file names to indicate to the operating system what format the file is in. It is by this mechanism that Windows knows to open File.txt with Notepad, File.doc with Microsoft Word and to attempt to launch File.exe as an application.

Changing the file extension on a file can render the operating system unable to open the file. Many modern operating systems hide file extensions from the end user by default for this very

reason. Although in most instances changing file extensions is not recommended, there are situations where renaming extensions can yield interesting results. From Word 2007 and forward, for example, Microsoft introduced the .docx format. The .docx format is essentially a .zip file filled with XML-based documents and the media (pictures) embedded in the Word document. Armed with that knowledge, you could rapidly extract all the images embedded in a Word document by simply opening windows explorer, copying the ***file.docx*** file, then pasting it as a copy. Rename this copy file to ***file.zip***.

We copied and renamed this file as Page4.zip. When you open Page4.zip you find the following:



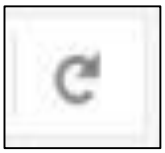
Click on the “word” directory and you get this:

Then when you click on “media” it opens up all the pics in this page and you can copy the lot.

Refresh!

In order to speed up web browsing, web browsers (Internet Explorer, Firefiox, Chrome, Opera etc) are designed to download web pages and store them locally on your computer's hard drive in an area called the "cache". Browser cache (also know as Internet cache) contains records of every item you have viewed or downloaded while Internet surfing. So when you visit the same page for a second time, the browser speeds up display time by loading the page locally from cache instead of downloading everything again.

Although storing Internet cache makes web browsing faster as it usually takes your computer less time to display a web page when it can open the entire page from your local Temporary Internet Files folder, you sometimes want to overrule the Internet cache, for example to see any changes made to a webpage since you first looked at it. This is called a "Refresh" and using Windows there are several ways of doing it. (It's easier on an Apple machine, just press the Apple key and R together).



On machines running Windows XP, Vista, Win 7, Win 8 or Win 8.1 you can either press the F5 key or click the little arrowed circle thing at the top of your browser window. Both of these commands work most of the time but they are not guaranteed to do a complete cache refresh and they could just load the cache again (which is why you have to sometimes hit them a few times to make them work). What you should do if using one of the above versions of Windows is do a "Force Cache Refresh" by holding down the Ctrl key and pressing F5.

But then along came Windows 10.

If you hit the F5 key under Win 10 you now get a search page??? You can still click on the little arrowed circle thing at the top of your page but once again, that's not guaranteed to work. Another way is to right click anywhere on your page, except on a pic, this will open another window where you'll find the little arrowed thing or the word Refresh (depending on which browser you're using) but this is also not guaranteed to work either.

In Windows 10 (and probably in all versions to follow) to do a complete refresh (a "Force Cache Refresh") you now do what Appleites do, hold down the Ctrl key and press the R key.

IOS 9 Problems.

Some people have found that they can no longer open links to web pages from within an email on their iPad or iPhone. This is commonly thought of as an IOS 9.3 problem, but it seems that the problem may have started with IOS 9.2.1

This link seems to explain what's going on.

Below is an explanation of this article in what I hope are simple terms:

In IOS 9.3, and also IOS 9.2.1, there is a new feature app developers can use called Universal Links. WWW.Booking.com have made use of this feature, but in doing so supplied a much bigger list of links than Apple expected. IOS cannot cope with such a big list of links and fails, leading to a general inability to open links to web addresses. My wife's iPad has booking.com installed and she has the problem. My iPad does not have booking.com installed and I do not have the problem.

I think booking.com have made their list smaller now, but it seems that iPads already affected will remain affected. Apple need to come up with a fix. I think they realise this, although they don't appear to be saying much as far as I've noticed.

There seems to be some ways to make the problem go away (now that booking.com has a smaller list of links) but they involve uninstalling booking.com and re-installing it, as well as doing other things to make everything start working again.

Even if the problem is resolved in this way, the iPad or iPhone remains vulnerable to the same problem if some app other than booking.com comes along with a really big list of links.

I don't feel inclined to suggest an uninstall / reinstall of booking.com if it contains a lot of material relevant to upcoming trips. Hopefully the next release of IOS will resolve the problem.

Hope this makes sense.


It's windy today!
No, it's Thursday!
So am I!
Let's have a beer!