I’m the assistant coordinator at TechMate and passionate about technology, I am also passionate about security and I can talk at length about security.
Focused on Digital Inclusion,

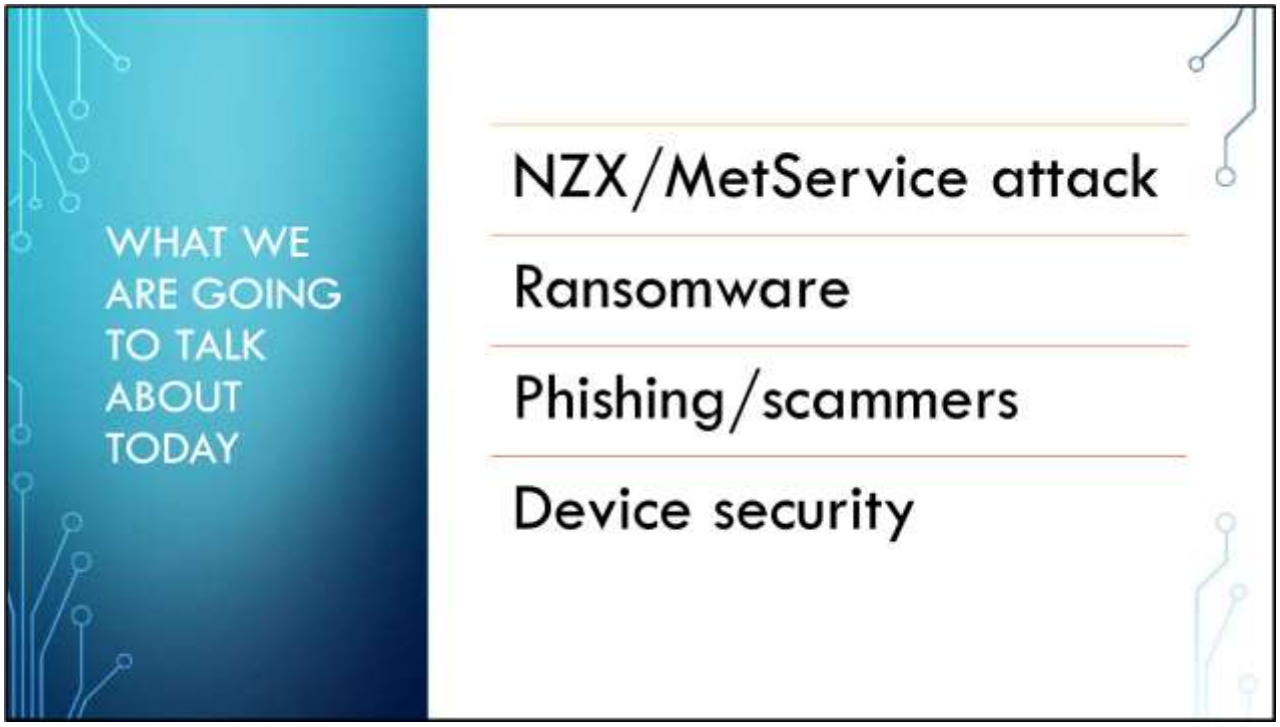
we do this by learning sessions, group sessions, low cost repairs, this sort of thing, low cost internet, kids IT club
Who trusts you?

It is not just about what the bad person can access from your accounts.

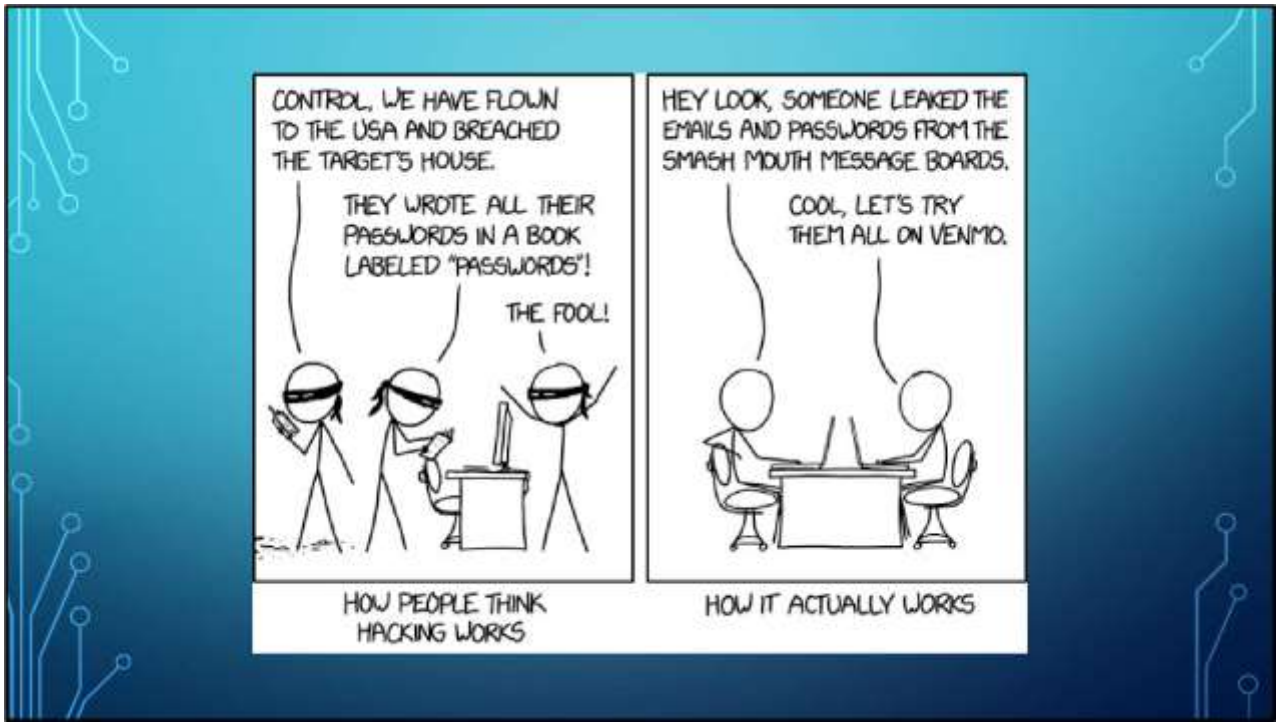
Think about all your friends and family, how many trust you?

How could this trust be exploited by somebody who is not you?

Would you like it if your computer was used as a staging post for really bad stuff?



In the first section of this talk, I thought it would be interesting to take real examples of bad stuff and examine what we can learn that can make us safer in the digital realm. In the second bit I will give you all a rundown of the security needs of different devices. To understand how to best protect ourselves online, we need to get some perspective.



75% of the time bad people are not interested in you specifically, They just want money.

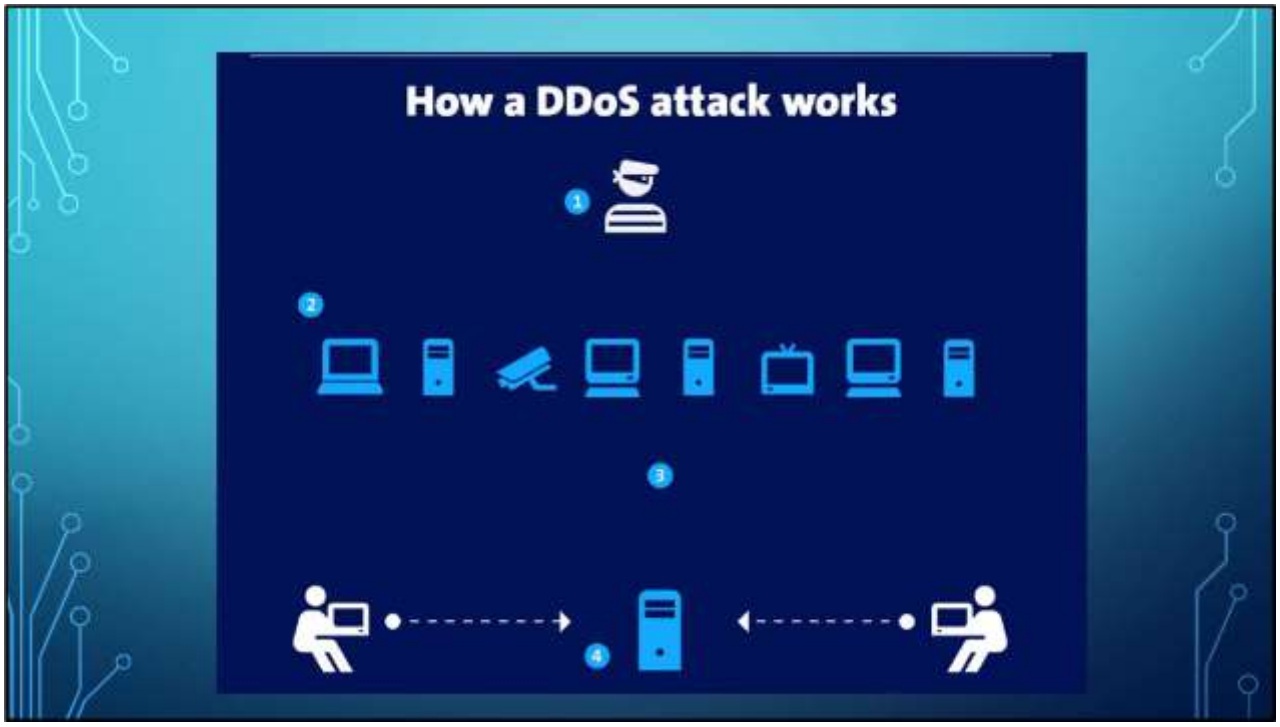
Ways bad people earn money from you: ransomware, selling your data (cards, passwords, accounts, pictures etc), leasing your computer out for bad things, just plain scamming you, pretending to be you to exploit your colleagues, friends and family.

So what did happen at NZX?

A couple of weeks ago, what appears to have happened is that an international crime organisation tried to ransom NZX into paying them to stop DDoSing the NZX server. NZX refused. It took NZX and their providers a long time to stop the attack.

To stop a huge DDoS attack without giving in to the ransom, it takes a lot of resources (most of the time these resources are special computers that are designed to filter bad information really quickly), I have no doubt that NZX spent a large some of money getting help for this.

So, what is a DDOS attack?



A DDoS (Distributed Denial of Service attack) is when a bad person/organisation uses a lot of devices/computers to more or less all send information to a computer or server at once, the end result of this is that the service/computer is overwhelmed and stops responding.

DDoS attacks are not really thought of as sophisticated attacks, they are crude, but effective. The source of one of the largest DDoS's in history was hacked security cameras and security camera recorders.

You might be thinking that you are not a large-cashed up target for a crime organisation, and you would be right, unless I am seriously misjudging you all.

That said…

A few years ago I was moderating an online community I frequent when I encountered a rude person wanting to push the rules and be an unpleasant human being, I didn't let him get away with his antics and I removed him from the community, I thought that was that.

A few minutes later I noticed my internet connection was being terrible, being a nerd, I tried to log into my router to see what was what, my router was unresponsive, as I work in IT I figured it wouldn't hurt to turn my router off and on again.

I did that and things worked again, I logged on to the online community to a message from the person I banned to the extent of "HAHA, I BLASTED YOU OFF THE INTERNET", to which I didn't respond. I honestly thought I just had some minor internet issues.

I looked into it and it turned out that yes, this delightful human being had followed some digital breadcrumbs I was stupid enough to lay down right to my address on the internet, and then used a service to blast me off the internet.

Realistically, If you are the target of a DDoS attack the best thing to do is to call your internet provider and let them deal with it.

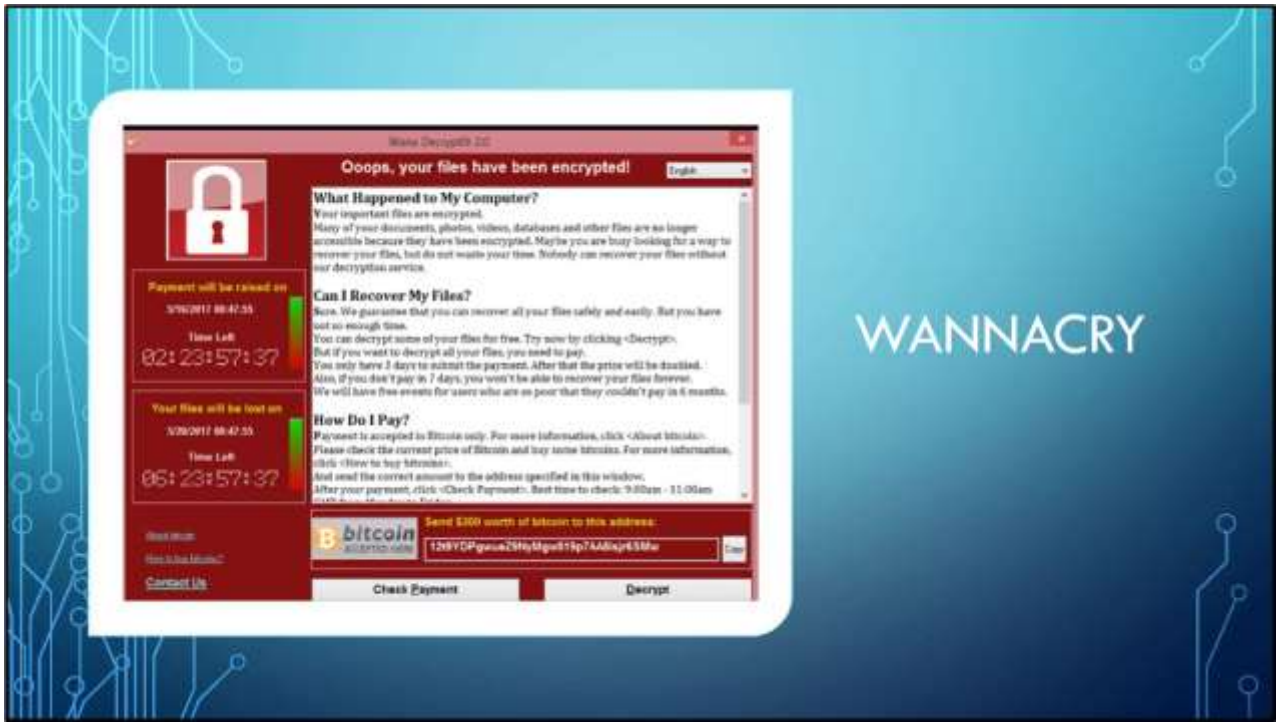
If you don’t want your computer to be used to do somebody else's bidding, the best thing you can do is make sure you update regularly. Bad people have lots of systems that automatically scan for things that are not updated so that they can take advantage of the bug and take your computer over without you knowing. These same systems also automatically check for easily guessable passwords.

Ransomware is the thing that keeps me up at night. Ransomware is a type of malware that encrypts computer data (i.e. scrambles the user's computer data into meaningless information) and proceeds to demand that affected users pay a decent some of money to unlock your data.

If you ever get hit with ransomware the accepted advice is not to pay the ransom, as the money you pay can end up with really bad people. Not to mention the fact that when you pay whomever, you validate their business model and they keep at it.

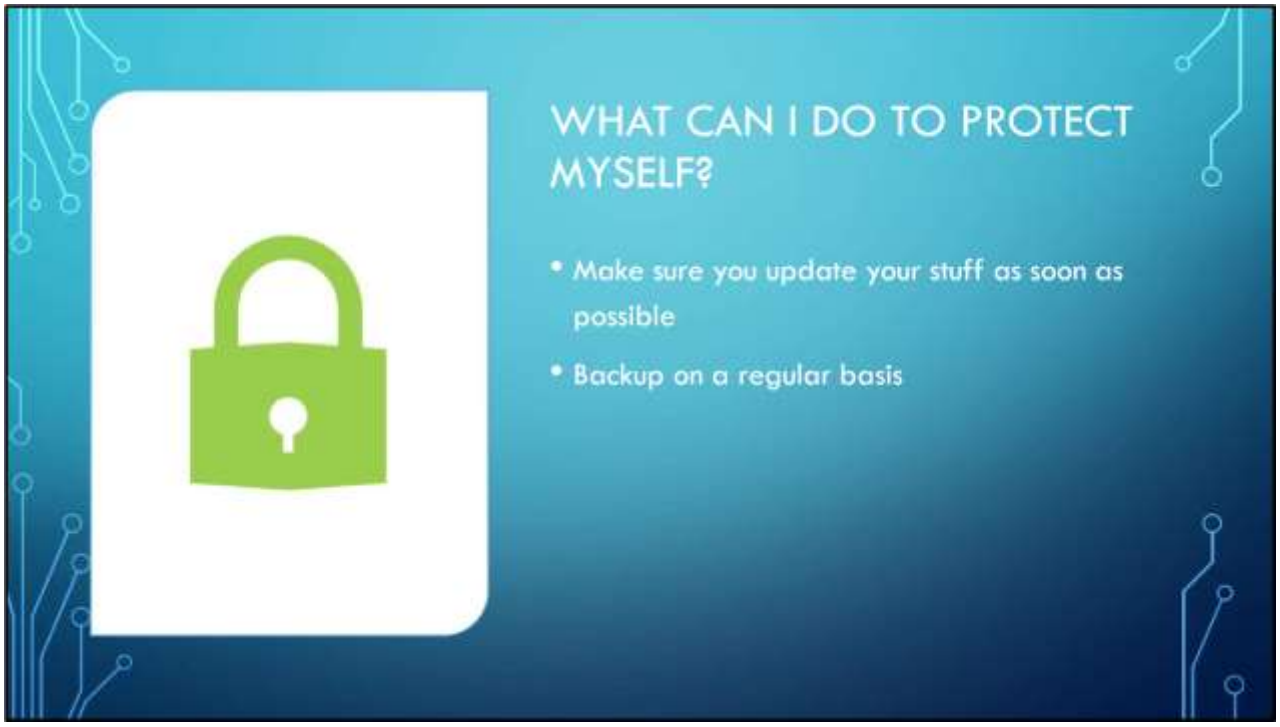
Ask has anybody been infected with ransomware?

The most well known piece of ransomware is called WannaCry.



WannaCry is a a piece of ransomware that came into prevalence in May 2017. Wannacry is notable because it was/is self executing, meaning it spread without user input. It demanded affected users to pay $300 within 3 days or $600 within a week before all of the affected computer's data is destroyed. It managed to find its way into the British health system and took many hospitals offline for a long period of time. WannaCry is estimated to have cost millions, if not billions of dollars in damages.

WannaCry used a exploit that had been fixed with updates six months prior to it’s release, it is more or less a worst case scenario for what can happen if you don’t update your software regularly.



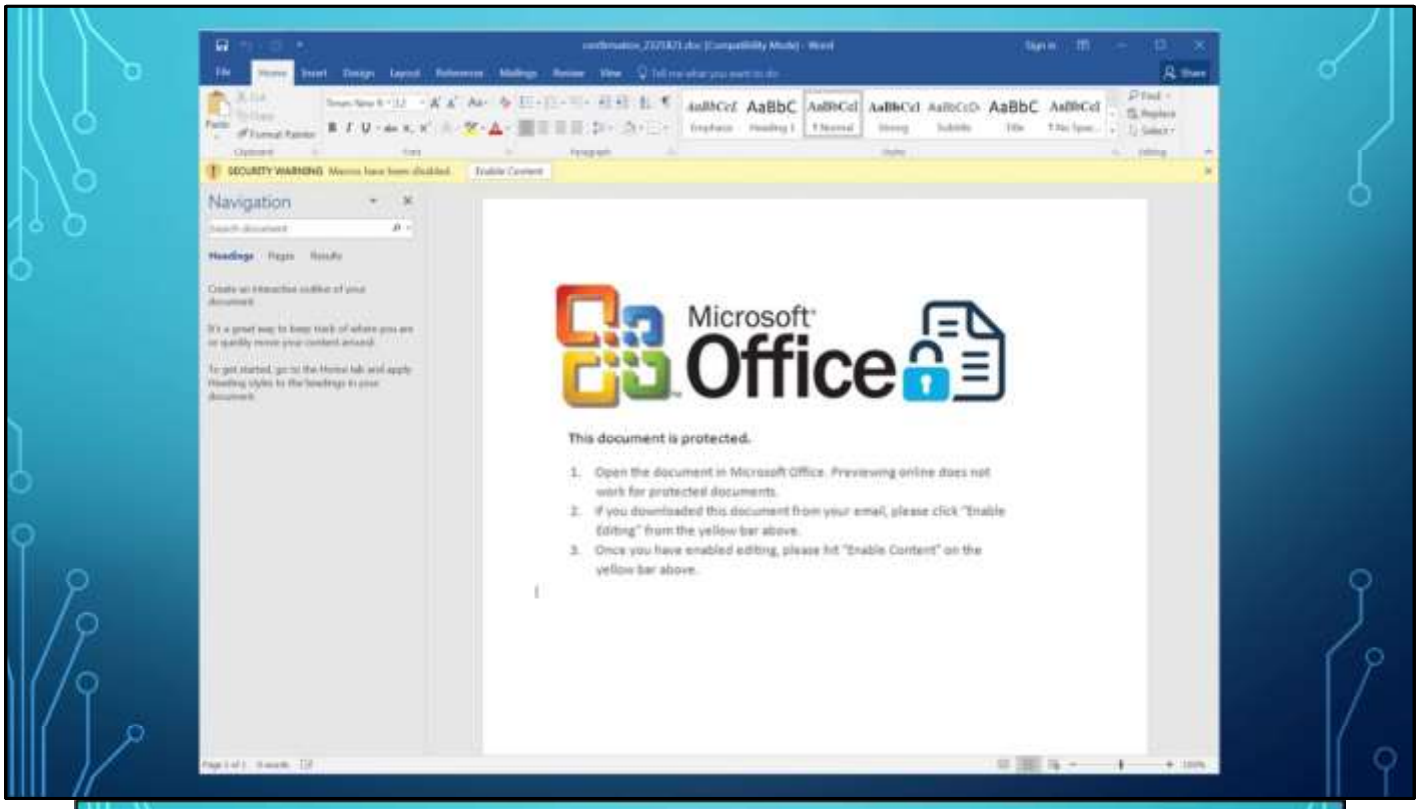
I know it is easy to put off updates as they are a pain in the rear, but often it is the easiest thing to do to prevent bad stuff from cropping up.
Ask Has anybody here had a “Tech support” call?

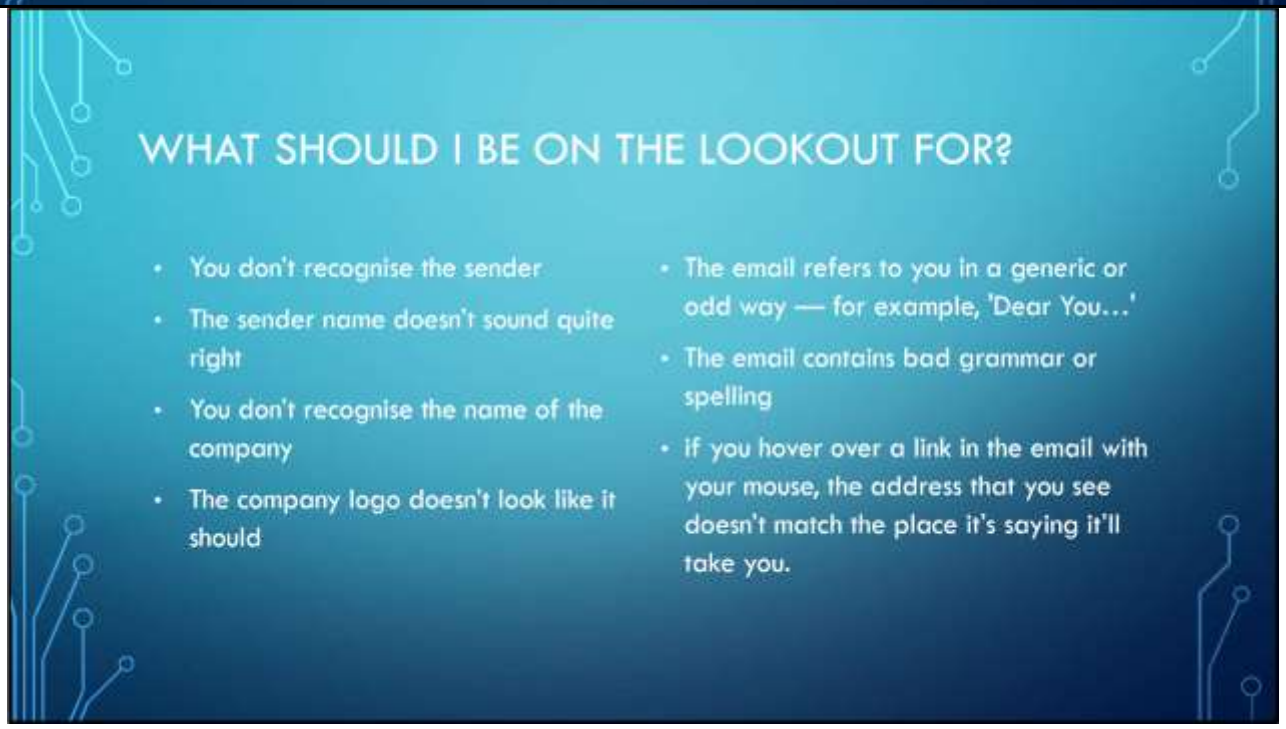
Tech support scams are as old as time. There has been an uptick in recent calls. The best thing to do if somebody calls up for tech support is just to end the call. If you are truly concerned then call up your provider with the number on your bills or in the phone book.

If you accidentally let them in, first of all, don't panic, secondly, call up your bank as soon as you can and let them know, they can then place a block on your accounts for a little while. Thirdly, call up your internet provider and let them know. In the handout I have given out there is the number for Netsafe, who are a great organisation that will not judge you for your moment of human.

These rules more or less apply to anything, don’t trust anything on the internet (at least initially). Don’t engage with somebody trying to antagonise you.


PHISHING





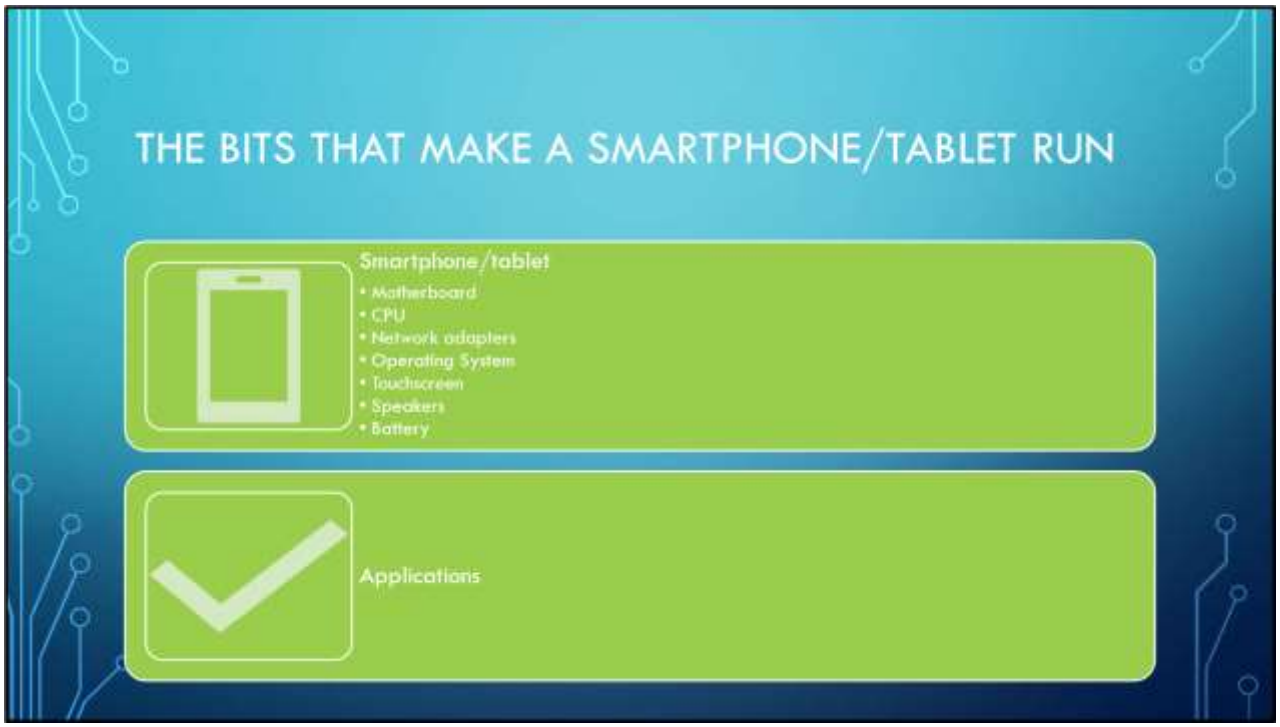
Spearphishing – targeted phishing. 18 This is a real phishing attempt. It evaded spam filters due to trickery In order to make the next couple of slides make sense, I think it is prudent to quickly go over emails. Note emails have a subject, a from field and a to field.

Same thing again, subject, from, to.

Phishing Not phishing Phishing If you see anything like this, close it, it is trying to trick you into running something nasty.


SECURITY NEEDS OF DIFFERENT DEVICES

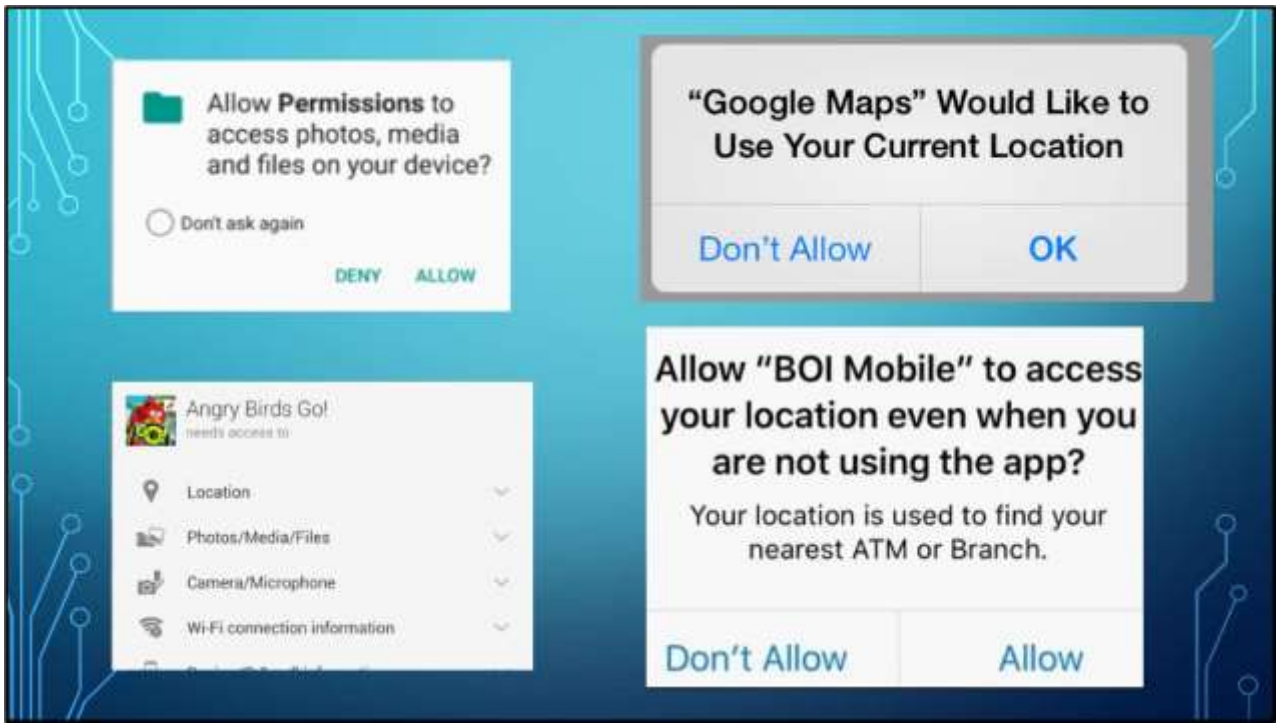
All these things need to speak to each other.



One thing about smartphones/tablets is that smartphones/tablets is that smart devices are designed from the ground up to run Android/iOS/whatever, in most instances everything

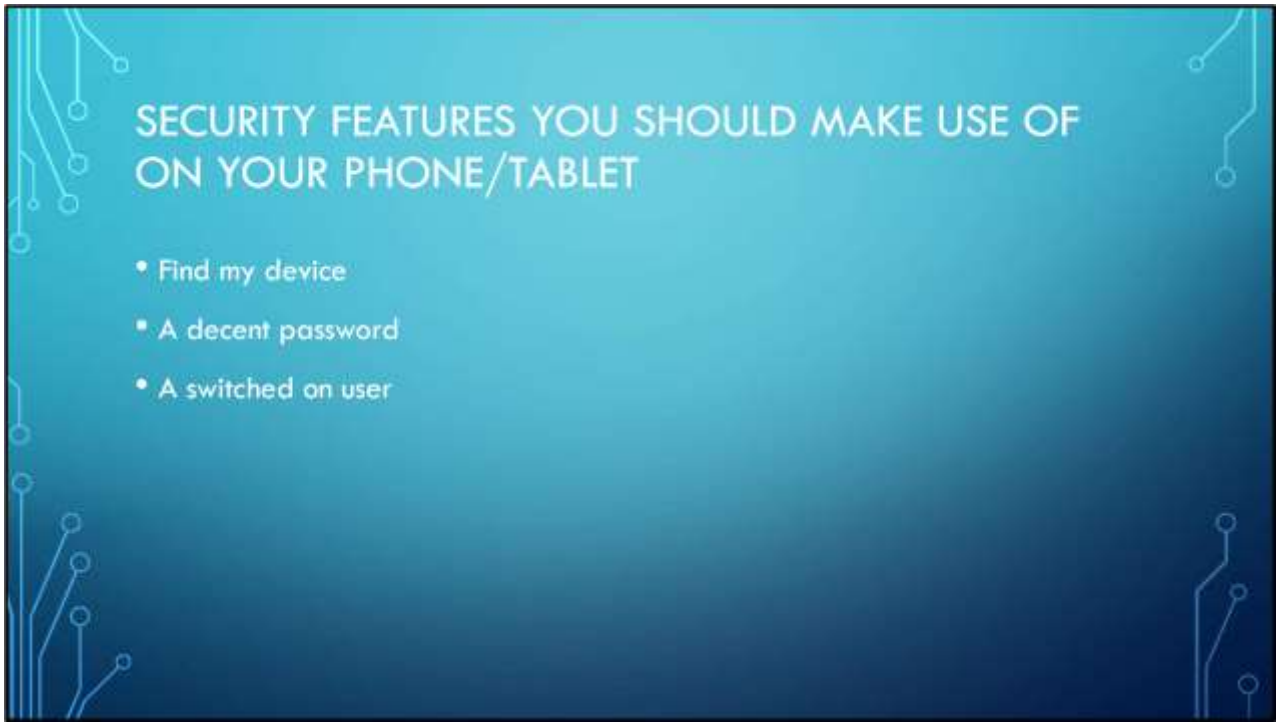
in a smartphone is manufactured with the intention of being in a smartdevice that runs Android/iOS/whatever.

Smart devices also have another thing going in their favour is that smart devices run apps in what is known as a sandbox, what this means is that well, apps can only make a mess in the sandbox.



Google and Apple both make sure that most nasty stuff doesn't get in your phone if you just use the Play Store/App store as the only place you download apps from. Most of the real danger comes from apps that are designed to steal your information. One of the best ways you can combat this is only give permission for stuff that you trust


SECURITY FEATURES YOU SHOULD HAVE ON YOUR COMPUTER
• Antivirus software (on Windows, Defender is a great inbuilt choice)
• Malwarebytes
• Adblocker (I recommend uBlock Origin)
• A password
• A suspicious user


SECURITY FEATURES YOU SHOULD MAKE USE OF ON YOUR PHONE/TABLET
• Find my device
• A decent password
• A switched on user

This means that if a bad person gets hold of your Facebook password, they don't have access to your bank, emails, etc

Yes, I know this is a pain, In a few minutes I will talk about some ways this can be made really easy.

This animation is a little old and some of those figures are now much smaller, but long passwords are very much better than shorter, more complex passwords

PASSWORD MANAGERS

By using a password manager, we can store a whole bunch of passwords easily and securely.

A password manager can be

- Analog (i.e a notebook)
- Digital (i.e Lastpass)

ANALOG PASSWORD MANAGERS

Easy to use and set up

No password to remember

Won't automatically generate your passwords for you

Won't fill in your passwords for you.

If you forget the book you can't log in

DIGITAL PASSWORD MANAGERS

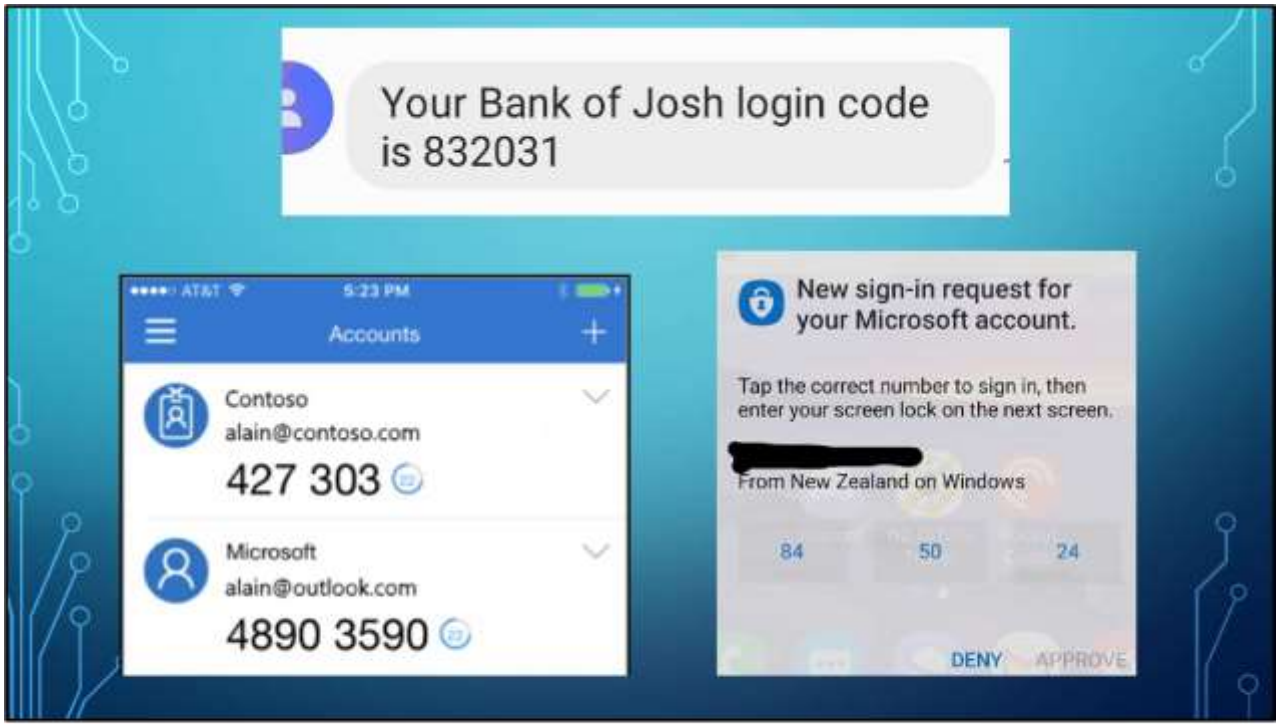
Slightly harder to set up and use

A password to remember

More secure than analog

Will automatically generate and fill your passwords in

With most digital password managers, you can easily log in to them anywhere in the world



Ask *who has seen the following?*

These are examples of 2FA.

Ask Does anybody know what 2FA is?

The idea behind two factor authentication is that if I am a bad person and I have your password, I still need something from you to get in to your account. Something you know (a passphrase) and something you have(a phone).

Instructions on how to enable 2FA for most services are on the handout