




**crowley
core**

CYBER SECURITY AWARENES S

**Protecting yourself against
Cyber Attacks and Scams**

Good afternoon guests and welcome to our presentation on Cyber Security Awareness - Protecting Yourself against Cyber Attacks and Scams

What is Cyber Security?



- Practice of defending
 - Computers
 - Servers
 - Mobile Devices
 - Electronic Systems
 - Networks and Data
- Types of attacks
 - Identity Theft
 - Ransomware
 - Scams
 - Data Breach

- So, what is Cybersecurity and why is it important?
- According to Kaspersky (A global Cybersecurity and Anti-virus company), “Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks and data from **malicious attacks**”
- So, for everyday people, what is a malicious attack? A malicious attack could comprise of some of the following:

- **Identity Theft** is when a cybercriminal gains access to your personal information to steal money or gain other benefits. They can create fake identity documents in your name to get loans and benefits or apply for real identity documents in your name, but with another person's photograph. Passports and driver licences to name a couple.
 - **Ransomware** is a common and dangerous type of malware. It works by locking up or encrypting your files so you can no longer access them. A ransom, usually in the form of cryptocurrency, is demanded to restore access to the files. Cybercriminals might also demand a ransom to prevent your data and information from being leaked or sold online on the dark web.
 - **Scams** are a common way that cybercriminals compromise your online accounts. The scammer's goal is to trick you into paying money or giving away your personal information. They will use email, text messages, phone calls or social media, and often pretend to be a person or organisation you trust.
 - A **data breach** occurs when sensitive or personal information is accessed, disclosed or exposed to unauthorised people. This may be by accident, or the result of a security breach. For example, when an email with personal information is sent to the wrong person, or a computer system is hacked and personal information is stolen.
- So, why is Cybersecurity important? Basically to prevent these types of intrusions and inconveniences to our lives. More and more systems and businesses require information and access to that information to be digital, which means the security to those systems are critical.
 - In the next slides, I'll touch on some of these attacks, what to look out for and how to protect yourself.

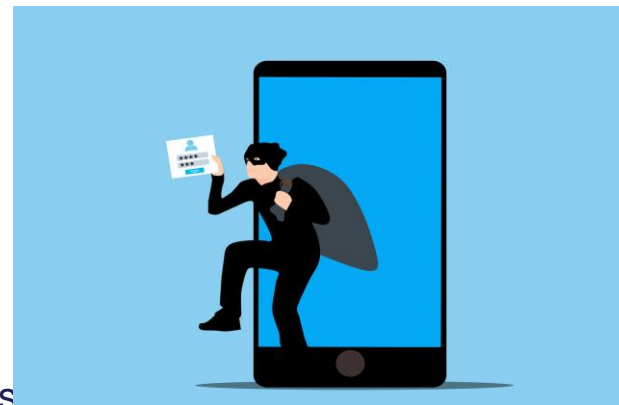
Reference

<https://www.kaspersky.com.au/resource-center/definitions/what-is-cyber-security> – Accessed 14/09/2023

<https://www.cyber.gov.au> – Accessed 19/09/2023

Identity Theft

- Financial and emotional consequences can be devastating
- What information do attackers target?
 - Name
 - Date of Birth
 - Drivers Licence Number
 - Medicare Card Number
 - Other personal information
- What is that you can look out for:
 - Check your bank statements
 - You may receive receipts for products purchased
 - You may be going for a loan and have been refused credit



- **Identity Theft** is one of the most complex and inconvenient attacks that can happen to someone. The financial and emotional consequences can be devastating for victims. Once your identity has been stolen it can be difficult to recover and you may have problems for years to come.
- What information do attackers target?
 - Name
 - Date of Birth
 - Drivers Licence Number
 - Medicare Card Number
 - Other personal information
- What is that you can look out for:
 - Periodically, check your bank statements to see if there are any unusual transactions
 - You may receive receipts for products you have never purchased, from stores you've never visited
 - You may be going for a loan and have been refused credit due to debts you have not incurred yourself

Identity Theft

- So here are some of the ways to protect yourself and your family
 - Limit what you share online **publicly**
 - Set all of your social media accounts to **“Private”**
 - Don't accept “friend” requests from strangers
 - Don't believe that email you received from the bank, have a careful look at it, what is it asking for?
 - For online and social media accounts, use strong passwords and **DON'T** reuse passwords
 - If you are worried your identity information has been compromised, you could use services such as IDCare



- So here are some of the ways to protect yourself and your family
 - Social media is a common source of easily obtained information.

- Limit what you share online **publicly**, such as your birthday, photos of your house and street name, and pictures of your children or grandchildren in their school uniform, sometimes we use these details as security questions on accounts.
- Set all of your social media accounts to “Private”, you only want your friends and family to share your memories.
- One of the rules I strictly follow especially on Linked-In and Facebook, is don’t accept “friend” requests from strangers (someone you haven’t met) or even accounts of people you know who don’t have images of themselves. The account might be legitimate, it’s better to ask them in person before accepting it.
- Don’t believe that email you received from the bank, well at least not straight away, have a careful look at it, what is it asking for? Is it asking for credentials or personal information, does it have a link to reset passwords? These are common tricks cybercriminals use to try and get this information. A bank will not be asking for this information in an email (They already have it). If you’re ever unsure about an email, get another family member to check the email or contact your bank directly using phone numbers on their website (Not from a number on the email)
- For online accounts and social media accounts, use strong passwords or passphrases and **DON’T** reuse passwords, because if one account is somehow compromised, and you use the same password they could get access to other accounts.
- If you are worried your identity information has been compromised, you could visit organisations such as IDCare <https://www.idcare.org/support-services/individual-support-services> or find other information at <https://www.cyber.gov.au>

Ransomware

- <https://player.vimeo.com/video/749391524>



- Please watch this short video about Ransomware from the Australian Cyber dot Gov website.
- The main takeaways from the video are:

- Don't click on any suspicious links in emails or on social media
- Don't open emails from unknown sources
- Keep regular backups of your devices
- If you are infected with Ransomware, don't pay any ransom demands. There is no guarantee you will get your data back.

• Ransomware

- Ask help from a professional.
- Step 1: Record Important Details
- Step 2: Turn off the infected devices
- Step 3: Disconnect your other devices
- Step 4: Change your important passwords




- If you are the victim of a ransomware attack. What should you do?
- It is important to record details about the ransomware attack to help you:
 - ask for help from a professional
 - make an insurance, bank or legal claim that may follow after the attack

- make a report to the relevant Australian authorities through the link on the Australian Cyber Security Center (ACSC) website [ReportCyber](#)
- tell your family, colleagues or authorities that there has been an issue.

- **Step 1: Record Important Details**
 - If files have a new file extension, what it is called
 - A ransom note and the name of the attacker group if they disclose it. This is helpful for the authorities and the professionals trying to help you.
- **Step 2: Turn off the infected devices**
 - As soon as you have recorded details about the ransomware attack, turn off the infected device by holding down the power button or unplugging it from the wall. For most people, this is the best way to stop the ransomware from spreading.
- **Step 3: Disconnect your other devices**
 - Ransomware can spread across networks. If there are other devices on your network, you should turn them off too. Start with the devices that are most important to you. Important devices typically include things like Network Attached Storage (NAS) devices, servers, computers, phones, tablets and any other devices that store valuable information.
- **Step 4: Change your important passwords**
 - Cloud storage accounts
 - Email accounts
 - Bank accounts
 - Business accounts
- I have put a link in the notes to visit a website for information on recovery after a ransomware attack,
- go to this link: <https://www.cyber.gov.au/report-and-recover/recover-from/ransomware>

• Scams

- Types of Scams
 - Phishing
 - Malware
 - Remote Access
 - Hacking



- So, we have already talked about a couple of scams such as Ransomware and Identity Theft, other types of scams include:
 - **Phishing** - When scammers trick you into giving away your personal details, for example by luring you to click on malicious links or attachments that look legitimate. Scammers may impersonate your bank or a government department, and ask you to give out information such as your account number, password, or credit card numbers.
 - **Malware** – When scammers trick you into installing software that can give them access to your files

- **Remote Access** – A little different to Malware in this requires you being tricked into giving the scammer remote access to your computer.
- **Hacking** – Where cybercriminals exploit security vulnerabilities in your devices or networks and gain access to your data



- So, what are some of the things scammers do to try and trick you
 - They use **Authority**, they may send you an email claiming to be from your bank or a government department (such as the ATO)

- They use **Urgency and Emotion**, they make the message appear that you have limited time to act and stop something nefarious from happening. An example might be, that you receive an email supposedly from your bank, that states there has been some suspicious activity on your account, you must click the link and “Log” into your account immediately or your account will be frozen. This tactic is used to elicit fear in the hopes you will act immediately.
- **Reward/Incentive** is another scam that has been around for a long time and I think most people here will know that if you receive an offer or deal that seems too good to be true then it probably is!
- Another common tactic for scammers is using **Current Events** to scam people. Using current news stories and events can make their claims seem more real. There was an increase in scam-related attempts during the COVID pandemic and the floods in Lismore.

Scams

- What to look out for
 - Were you expecting it?
 - Check the following:
 - Senders address
 - Spelling and grammar
 - Contain suspicious attachment



- OK, so hopefully I haven't scared too many people in here 😊, what should we look out for so we don't become the victims of these types of scams.....
- If you receive an email or text message claiming to be from your bank or other business you may deal with take notice of the following,

- **Were you expecting it?** One of the first questions I ask myself when I receive an email like this is “Was I expecting it?” If I receive an email from my bank (or Paypal) “out of the blue”, I like to ask myself this question, as it sets me up to proceed with caution.
- If I’m unsure, then I would be checking the following:
 - **The sender’s address** – this could be close in name to the legitimate business, but check spelling, and if unsure, check previous emails from that provider
 - **What sort of greeting does it have?** I would suggest if you are a customer, then it shouldn’t have a generic greeting such as Sir/Ma’am, Greetings customer
 - **If it has a link** when I hover my mouse over the link, where is it actually taking me?
 - **How is the grammar?** Poor grammar and bad spelling are indications of scams.
 - **Does it contain a suspicious attachment?** – A common scam that has suspicious attachments is parcel delivery scams or emails from Toll providers with “Fines attached” or “Invoice 765fc21”. Definitely do not open or download these attachments.
- In most cases, it’s better to be safe than sorry, you could check with someone else if you’re not sure of a message you receive, or just mark them as “Junk” or delete them. You can always follow up with the bank directly if you are concerned.
- Also to note, these scams don’t always happen via e-mail or SMS, a lot of scammers will call potential victims, so if you receive an unsolicited phone call from someone claiming to be from Telstra, Microsoft or your bank and you weren’t expecting it, good chance it is a scam.

Cues – Triggers to look out for

Errors
Spelling,
Grammar and
Punctuation

Visual Presentation
Low quality
images and
poor layouts

Language/content
Greetings,
signature and
formality

From: Order Confirmation [mailto:no-reply@discontcomputers.com]
Sent: Thursday, December 01, 2016 11:50 PM
To: Doe, Jane (Fed) <jane.doe@nist.gov>
Subject: Jane Doe Your order has been processed

[Click Here To Read Files](#)

Dear Sir,
Please find attached our first order as agreed with my boss.
Waiting for your OC and proforma.
Thank you in advance.
Regards

Here are some examples of what to look for:

- The top one is the header of an email, as you can see the senders address has a spelling mistake (Instead of “Discount Computers, it says Discont Computers”, something a real company wouldn’t allow to get passed onto the public.

- Visual Presentation is another trigger to look out for.
- And an example of a generic greeting where the language doesn't seem right.
- Remember just be cautious and if it doesn't feel right, have it checked by someone else, ignore or delete it.

• Data Breaches

- Generally affecting companies
- Often Targeted attacks
- It's your personal information they are after
- The Privacy Act 1988 makes some companies responsible for communicating breaches to customers affected



- Lastly, I will briefly discuss Data Breaches.
- Generally this will be a breach of a company where you might have data or personal information stored, such as an online shopping site.

- As discussed before, some of the organisations you have accounts with will have a lot of your personal details, details you required to upload to them as part of the sign-in process.
- Some of this information could be drivers licences, birth certificates, utility bills or credit card details.
- In Australia, if any organization or agency who is covered by the Privacy Act (Privacy Act 1988) and they have a data breach, they are responsible for contacting affected individuals.

• Medibank and Optus data breach






- On 22 September 2022, **Optus** became the victim of a cyber-attack that resulted in the disclosure of their customers' personal information.
- Estimates that up to 9.8 million Australians could have their data compromised due to the attack
- 2.8 million severely impacted.

- On 13 October 2022, one of Australia's largest medical insurers, **Medibank**, announced it had suffered a cyberattack
- Personal details of 9.7 million customers in Australia.



- Two recent newsworthy breaches were the Optus and Medibank ones last year.
- Up to 9.8 million Optus and 9.7 million Medibank customers could have their data compromised due to the attack.

• Good Password Practices

		
Secure	Change	Store
<p>Create a passphrase using:</p> <ul style="list-style-type: none">• A combination of different words• Capitals and lowercase letters• Numbers• A symbol <p>For example: ILikeChocolate2022! A password like this would take approximately 5 quadrillion years to crack. Check my password</p>	<p>When it is time to change your password:</p> <ul style="list-style-type: none">• Randomise it as much as possible• Don't just simply change a number at the end.• It needs to be unique and different from all your other passwords	<ul style="list-style-type: none">• Don't use a Word Document or a sticky note to remember all your passwords.• Use a password manager• Don't share your password with anyone (this includes other staff members)

- Lastly, I would like to touch on Good Password Practices. This has been something that has evolved and changed over time. The advice may have changed over time about what is a secure password, but the message is still the same, a good strong password is always advisable to keep your data and information safe.

- One of the issues for people when creating passwords are they either make it easy for them to remember, i.e. **Password1, your date of birth, etc.** When this happens, people often use the same password on multiple accounts which we have learnt is not safe.
- One of the more recent changes to password advice is to create what is called a passphrase. So instead of creating a simple password like **Password1** or a difficult password such as **Qwerty25!!\$06** a passphrase will be a combination of easy to remember words put together, like the example in the slide, **ILikeChocolate2022!** Making the first letter of each word a capital letter, or **Frogs-Eat-Daffodils2** adding a common separator in between each word, which could be any symbol such as **#** or **\$**, etc.
- The best advice I can offer for passwords are:
 - Sign up for a Password manager and let it handle your passwords for accounts. You just have to create one strong password for access and when you sign up to any account you can add it to the password manager and it is secure. There are many password managers out there to choose from, the one I use is Bitwarden and I went with that option because I believe it is safe and I can also access passwords on my computer and Phone which not all password managers can do.
 - I suggest researching your options.

Key Takeaways

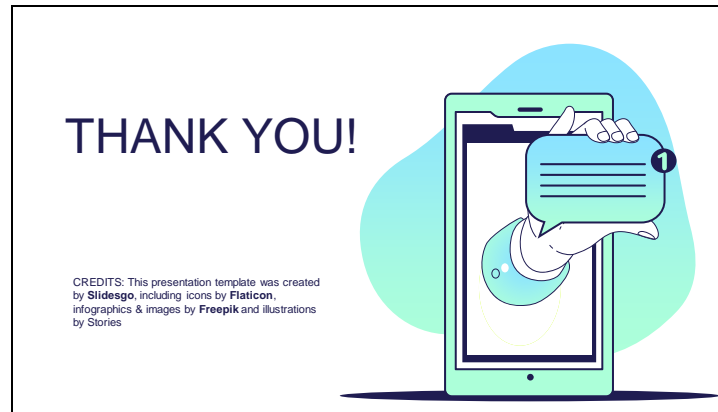
- Be aware and vigilant before opening emails or clicking on links.
- Look for the phishing cues/triggers
- Limit what you share online **publicly**
- Keep regular backups of your devices
- Stop, Think, Act
- Have good password practices



So, hopefully, I have been able to share some of the knowledge and tools you need to stay safe online, the information can seem scary and overwhelming, but using this knowledge to be cautious and to trust your own instincts can keep you safe and allow you to enjoy what technology can offer.

So I'll just recap some of the key takeaways

- Be aware and vigilant before opening emails or clicking on links.
- Look for the phishing cues/triggers
- Limit what you share online **publicly**
- Keep regular backups of your devices
- Stop and Think before acting on an unsolicited email or text message. Don't let the message rush you into a decision you might regret.
- And lastly, have good password practices, use a password manager or create passphrases to keep your accounts and information secure.



I'd like to thank you for your patience and time today, hopefully, the information was helpful. I will include some of the resources in the PDF for Anne to distribute.

Thank You very much and enjoy the rest of your day.

Resources

- <https://www.cyber.gov.au>
- <https://www.idcare.org>
- <https://www.oaic.gov.au/privacy/your-privacy-rights/data-breaches/Identity-fraud>
- <https://www.ncoa.org/article/how-older-adults-can-improve-their-personal-cyber-security>
- <https://bitwarden.com/>
- <https://www.esafety.gov.au/>