‘What is the government doing’ Retrieved from - <https://www.industry.gov.au/data-and-publications/australias-tech-future/cyber-security/what-is-the-government-doing-in-cyber-security> viewed on 30/04/2020

 ©2020 [ISBuzz News](https://www.informationsecuritybuzz.com/), ‘evolution of cybersecurity’ Retrieved from - <https://www.informationsecuritybuzz.com/articles/the-evolution-of-cybersecurity/> viewed on 30/04/2020

©2020 Synopsys, ‘What is cyber security’ retrieved from - <https://www.synopsys.com/glossary/what-is-cyber-security.html> viewed on 30/04/2020

**CYBER SECURITY**

Cyber security, also known as IT security, is a part of technology that focuses on the protection of computers, programs, dad and networks from unauthorised (malicious) or unintended access, destruction or change. Many government agencies, such as: corporations, the army, hospitals, institutions that have to do with financials, and many other groups often collect, store and process important information on their operating systems or networks. For the protection of this data, many have developed a software that is designed to help protect data and information. As the internet has become an integral part of today’s world, this type of software is imperative for many. A computer that does not have the appropriate security controls can be infected with malicious entities called a virus and thus any type of information can be accessed and vulnerable. For example, a number of infected web pages and websites can be seen every day that infects computers and allows hackers to gain illegal access to other computer systems, compromising your data.

There are many types of sub-domains of cyber security such as:

**Application Security** – involves implementing various defences within all software and services used within an organisation against a wide range of threats. It requires designing secure application architectures, writing code for security and implementing strong data input validation. This helps minimise the likelihood of unauthorised access or modification to applications.

**Identity Management and Data Security -** Identity management includes frameworks, processes, and activities that enables authentication and authorization of legitimate individuals to information systems within an organisation. Data security involves implementing strong information storage mechanisms that ensure security of data at rest and in transit.

**Network Security -** involves implementing both hardware and software mechanisms to protect the network and infrastructure from unauthorised access, disruptions, and misuse. Effective [network security](https://www.synopsys.com/software-integrity/managed-services/network-security-testing.html) helps protect organisational assets against multiple external and internal threats.

[**Mobile Security**](https://www.synopsys.com/software-integrity/managed-services/mobile-application-security-testing.html) - refers to protecting both organizational and personal information stored on mobile devices like cell phones, laptops, tablets, etc. from various threats such as unauthorized access, device loss or theft, malware, etc.

[**Cloud security**](https://www.synopsys.com/software-integrity/solutions/by-security-need/cloud-security.html) - relates to designing secure cloud architectures and applications for organization using various cloud service providers such as AWS, Google, Azure, Rackspace, etc. Effective architecture and environment configuration ensure protection against various threats.

**DR&BC** - deals with processes, monitoring, alerts and plans that help organizations prepare for keeping business critical systems online during and after any kind of a disaster as well as resuming lost operations and systems after an incident.

**User Education** - formally [training individuals regarding topics on computer security](https://securitylearning.synopsys.com/) is essential in raising awareness about industry best practices, organizational procedures and policies as well as monitoring and reporting malicious activities.

Right now, cyber security is in its upmost importance, especially due to the pandemic. There is now even more traffic across the internet, therefore making even more people susceptible to being targeted by malicious individuals. While the state of cyber security is quite strong, there is always a way to continuingly upgrade encryption and other methods to minimise the chance of danger. It is also important for those who go onto the internet on a daily basis to be weary of what is deemed suspicious and unsafe. This not only help you understand what dangers are really out on the internet, but also save you a lot of hassle if you ever find yourself in a situation where you have to deal with, for example, a trojan. In the next three years, major corporations such as google or Microsoft will continually invest into cyber security so that their businesses are not at risk, while other companies do the same and also give their software out for consumers, so they too don’t lose out.

For us in Australia, the government has been committed to mitigate cyber security risks and reduce any risks to Australia’s national security. They have been actively implementing a ‘Cyber Security Strategy’ that has the investment of more than 230 million across five themes of action, including: national cyber partnership, stronger cyber defences, global responsibility and influence, growth and innovation and a cyber smart nation. This, if done correctly, will allow Australia to greatly benefit and result in a less susceptible system where we can deal with threats more easily. Reactive approaches to defences are no longer a feasible situation as our internet culture grows, so this development will be a positive one. From the outside appearance of cyber security, many will not notice a difference. However, internally, there will be many changes that will help many more individuals be safer when doing things with their devices. Protocols will be improved and methods of stopping threats will be improved. These must be continuously improved to stop hackers from accessing important information. As cyber security will never grow redundant, the only thing that will grow old is the different methods in protecting a system. This, in turn, will also allow for more job opportunities in many corporations as it is so crucial.

In our daily lives, we might not notice a difference as everything is done in the background. Although, this can save us from many situations where our important data is vulnerable; methods of encryption can be updated so that we will not have to panic about our data being stolen. Once again, it is also important that everyone knows what is truly out on the internet so that these instances can be mitigated. Family member or friends too will also not notice what has changed, unless they have knowledge on this type of topic. As technology grows and develops, so does the security of the systems, otherwise everyone would be more open to attacks. So, the best thing that you can do is make sure you know what is dangerous and how it can affect you if you do run into trouble online. As cyber security grows more prevalent in todays society, so does the importance of understanding how far these programs can help you.