LEARN ABOUT BASIC CYBER SECURITY

What is cybersecurity about?

Cybersecurity is the practice of protecting organisation's systems, networks, and programs from digital attacks from hackers, to prevent access to sensitive information.

What are hackers?

Hackers are people who want to gain access to companies internal systems to:

•access, change, or destroy sensitive information
•extorting money from users via ransomware;
• want to interrupt the normal business process

For your information

One size of hacking does not fit all.... because digital attacks can have a consequence from mild to severe impact.

There are different maturity levels for the types of attacks.

Difference Between Cybersecurity and Information Security

Cybersecurity pertains to any technology infrastructure in the cyberspace including computers and network devices, home automation, smart devices, driverless cars and drones.

Information Security

Information security is about protecting the privacy of information in digital or any other format such as paper. Even though most digital information is found in cyberspace; there are instances like digital information created on a stand-alone computer that was never connected to a network which make it on the information security list.

Another example is a USB storage device contains digital information and is in cyberspace when connected to a networked computer, but not when removed from that computer.

There are different types of hackers

- Black Hats - Ones to watch out for with bad intentions
- Grey Hats - Have loopholes which may not be ethical but not illegal
- White Hackers - Organisational ethical hackers from above hats

White, gray and black hat comparison

WHITE HAT

Considered the good guys because they follow the rules when it comes to hacking into systems without permission and obeying responsible disclosure laws

GRAY HAT

May have good intentions, but might not disclose flaws for immediate fixes

.....

Prioritize their own perception of right versus wrong over what the law might say

BLACK HAT

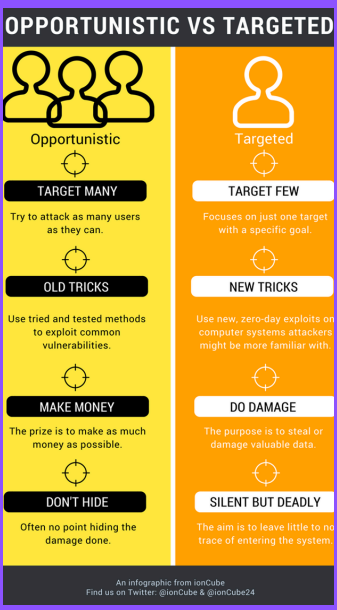
Considered cybercriminals; they don't lose sleep over whether or not something is illegal or wrong

.....

Exploit security flaws for personal or political gain—or for fun

Difference between Targeted Attacks vs Opportunistic Attacks from Hackers

- A targeted attack means this was done on purpose to get something such as confidential files or sensitive information
- An opportunistic hack means the hackers do not have a specific target but prefer to have as many victims as possible, to gain as much from the hack



What is the Essential 8?

The Essential Eight was designed to protect organisations' internet-connected information technology networks from harm. Not originally for enterprise purposes, this quickly caught on.

However, there are different other types of mitigation strategies to defend unique cyber threats.

Australian Government
Australian Signals Directorate

ACSC
Australian Cyber Security Centre

Who created the Essential 8 framework?

A Canberra government- based company named Australian Signals Directorate (ASD) developed strategies to protect cyber security incidents to prevent cybercrimes and threats, in partnership with Australian Cyber Security Centre (ACSC) in 2017.

This framework is only used in Australia as a baseline and the Essential 8 is basically a safeguard and resilience for cyber threats

yooralla

Prevents attacks

- Application control
- Patch applications
- Configure Microsoft Office macros
- User application hardening

Limits extent of attacks

- Restrict admin privileges
- Patch operating systems
- Multi-factor authentification

Recovers data and system availability

- Daily backups

NIST Framework vs Essential 8 Differences

The NIST Cyber Security framework (CSF) also known as National Institute of Standards and Technology was first coined in the United States. The framework addresses the lack of standards in organisation's cybersecurity awareness; and educate them on how to manage and reduce cybersecurity risks for improvements.

Essential 8 focuses on the prevention of cyber security threats, while the NIST CSF focuses on a holistic approach to cyber security, including prevention, detection, response and recovery.

Capability	Description
Identify	What processes and assets need protection?
Protect	Implement appropriate safeguards to ensure protection of the enterprise's assets
Detect	Implement appropriate mechanisms to identify the occurrence of cybersecurity incidents
Respond	Develop techniques to contain the impacts of cybersecurity events
Recover	Implement the appropriate processes to restore capabilities and services impaired due to cybersecurity events

Why & How of Essential 8 Framework

1. Assess organisation current compliance landscape for improvements
2. Design your findings
3. Operate on the findings
4. Implement the findings

Reporting Incidents

If have you have any questions, you can call or write to Australian Signal Directorate on

1300 CYBER1 (1300 292 371)

Postal address

PO Box 5076
KINGSTON ACT 2604

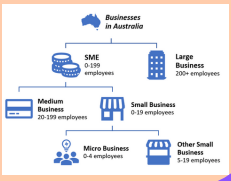
References

The Growing Need for Cybersecurity - Tarrant County College (tccd.edu)
https://guillaumejacquart.medium.com/targeted-and-opportunistic-attacks-292e6db587b9
https://www.nist.gov/itl/smallbusinesscyber/nist-cybersecurity-framework-0
The Essential 8 and why you should consider them? | by Fellow Human | Medium
The Ultimate Guide To The Essential Eight - Stanfield IT
Case Study: Implementing the Essential 8 in an Australian SME Engineering Business (powerbits.com.au)
Multi-Factor Authentication - ACSC Essential 8 (connectwise.com)

MYTHS & FACTS

Myths

- Cybersecurity is only for experts
- Cybersecurity is only for corporate large organisations
- Cybersecurity is too expensive
- Antivirus software and firewalls are the only line of cyber defence
- Viruses are the biggest cyber threat of all time
- Cybersecurity only refers to computers and devices



Facts

- Small to medium businesses that do not have a cybersecurity strategy do not shut down and lose money in the process more than large corporations

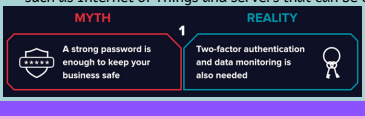
- Many businesses are turning to cyber insurance policies to protect themselves in a worst-case scenario, but this isn't always as straightforward as it sounds. It can require a lot of paperwork and the costs can be very high, depending on your industry, risk levels and current cyber security plan.

In fact, as of March 2022, only 1 in 5 small to medium business in Australia had a cyber insurance policy in place

- Even if your computer or devices has some line of defence such as antivirus software it does not completely protect your computer/devices

- Viruses have a small impact compared to other cybersecurity risks, and they can be a big nuisance but overall can resolved quickly compared to e.g. zero day threats.

- Cybersecurity can happen on computers and devices, but there are other things such as Internet of Things and servers that can be exploited.



Resources

Please see here if you wish to do the ACSC Essential 8 Self Assessment Guide

Please go to link here to get the official Australian Cyber Security Centre (ACSC)/Australian Signals Directorate (ASD) template for your business

8 cyber security professionals share their essential reads | by Threat Intel | Threat Intel | Medium

For all the cyber security definitions, go to this link here

yooralla