



Educate
Engage
Inspire



Presented by

**NORTHROP
GRUMMAN**

In partnership with



Module 3

Principles of cyber security

cybertairan.csiro.au



Learning objectives

- Participants will gain an understanding of basic cyber security concepts
The CIA triad
People, processes, and technologies that relate to CIA
- Participants will understand the differences between a threat and a vulnerability
Threats, vulnerabilities, and exploits
Risk and vulnerability severity
- Participants will become familiar with basic threat types and countermeasures
Overview of major threat categories
How attackers exploit infected computers
Best practices for threat prevention
- Participants will understand fundamental user security processes
Identification, Authentication, Authorisation, and Accounting
Proper password configuration

Section 1

The CIA triad

The CIA Triad

The 3 goals of information security are to maintain:

- Information **confidentiality**

Making sure only approved users have access to data.

- Information **integrity**

***Data Integrity:** assurance that information has not been tampered with or corrupted between the source and the end user.*

***Source Integrity:** assurance that the sender of the information is who it is supposed to be.*

- Information **availability**

Ensuring data is accessible by approved users when needed

People, Processes, and Technology (PPT)

- Protecting the CIA Triad is about more than just technology.
- PPT is a holistic approach to securing an organisation's information.



The CIA Triad —Tech tools of the trade

- Confidentiality
 - *Encryption — passwords, encryption keys*
 - *User access control — controlling which users have access to networks and what level of access each user has.*
- Integrity
 - *Encryption*
 - *User access control*
 - *File permissions — customisable settings that only allow certain users to view and edit files.*
 - *Version control systems/backups*
- Availability
 - *Offsite data storage/backups*
 - *Redundant architecture (hardware and software)*

Section 2

Threats and vulnerabilities

Important cyber security definitions

- Threat

An attacker or piece of malware that desires and/or is able to cause harm to a target.

- Vulnerability

Flaw in an environment that an attacker can use to harm the target.

- Exploit

The method by which an attacker can use a vulnerability.

- Risk

The potential that a threat will exploit a vulnerability.

Risks — probability and impact

The risk of a cybersecurity attack depends on two factors:

- **Probability**
 - *How much motivation does an attacker have to try to exploit my system?*
 - *How securely have I protected my system?*
- **Impact**
 - *How damaging is a potential attack on my system?*
 - *Types of impact: financial; health and safety; personal; service interruption.*

Risk Matrix

| | | Impact | | | | |
|-------------|-------------|---------|--------|----------|--------|---------|
| | | Trivial | Minor | Moderate | Major | Extreme |
| Probability | Rare | Low | Low | Low | Medium | Medium |
| | Unlikely | Low | Low | Medium | Medium | Medium |
| | Moderate | Low | Medium | Medium | Medium | High |
| | Likely | Medium | Medium | Medium | High | High |
| | Very likely | Medium | Medium | High | High | High |

Source: http://2.bp.blogspot.com/-xSHY5tsTvVY/Tzqi_kSorfl/AAAAAAAAABDo/cR71Da7qCQY/s1600/ProbabilityAndImpactMatrix.png

Risk assessment — target breach

Case: Attackers breached Target's network through a heating and air conditioning (HVAC) company and point-of-sale systems to steal 40 million credit card numbers.

Likelihood: Likely

- Attackers knew that Target has a massive network with many potential holes and that they could gain a wealth of information.
- Network was not fully secured; HVAC company had open access to it.

Impact: Major

- Loss of financial information could have major impact on Target's customers.
- Breach was a huge embarrassment to Target and could have led to a decrease in future sales.

Risk Matrix

| | | Impact | | | | |
|-------------|-------------|---------|--------|----------|--------|---------|
| | | Trivial | Minor | Moderate | Major | Extreme |
| Probability | Rare | Low | Low | Low | Medium | Medium |
| | Unlikely | Low | Low | Medium | Medium | Medium |
| | Moderate | Low | Medium | Medium | Medium | High |
| | Likely | Medium | Medium | Medium | High | High |
| | Very likely | Medium | Medium | High | High | High |

Source: http://2.bp.blogspot.com/-xSHY5tsTvVY/Tzqi_kSorfl/AAAAAAAAABDo/cR71Da7qCQY/s1600/ProbabilityAndImpactMatrix.png

Section 3

Cyber threats and countermeasures

Physical threats

- Dumpster Diving

Thieves sift through garbage for receipts with credit card information, medical forms with social security numbers, or other documents with PII.

- Shoulder Surfing

By looking over your shoulder as you type, thieves can glean passwords, account information, and other sensitive information.

Simple, but often overlooked threats.

Cyber hygiene

Basic personal practices that keep computers and data safe:

- Lock your computer when in public areas.
- Shield your keyboard when you type in passwords.
- Do not let strangers use your computer.
- Keep sensitive information in secure places.
- Update regularly.

Mobile devices

Portable or handheld devices that have data or can connect to another device which has data.



Mobile device threats

Risk

- Easily stolen and lost
- Often not encrypted
- Targets of malware, tools for attackers
- Can be compromised via wireless
- Applications collect information

Fix

- Guard your devices
- Set a strong passcode
- Use anti-malware and updates
- Avoid using open networks
- Customise security settings

Online threats

- **Social engineering**

Manipulating people into giving up personal information.

- **Phishing**

Fraud attempts perpetrated by random attackers against a wide number of users.

Attempts to manipulate people into giving up PII via phone/SMS/email.

- **Spear-phishing**

Fraud attempts targeted at specific people based on their membership or affiliation with the target.

E.g. Fraudulent emails sent to specific Accounts Payable employees with fake invoices from regularly used companies.

How to spot phishing emails

- Spoofed email address
- Poor quality logos or graphics
- All caps or strange formatting
- Spelling errors or typos
- Asks for personally identifying information
- Executable attachment or link to a website
- Informal or unprofessional language
- Signed by a department, not an individual
- Doesn't contain unsubscribe options or privacy statements

From: "Membership Reminder" <insect2@psbbcmovi.onmicrosoft.com>
Subject: Netflix: Your Subscription Ended 7728333781
Date: 15 June 2020 at 6:40:35 am AEST
To:

NETFLIX

Something went wrong.

We weren't able to complete your last payment for your netflix subscription, there was an error with the active payment method.

Please go to your subscription's payment methods to change the active payment method.

[Update Payment](#)

We are here to help if you need it. Visit the help center for more info or contact us.

—Your friend at netflix

Questions? Call 1-866-579-7172

This account email has been sent to as part of your Netflix membership. To change your email preferences at any time, please visit the Communication Settings page for your account.

Please do not reply to this email, as we are unable to respond from this email address. If you need help or would like to contact us

Malware — what is it?

Malicious software = malware

Software designed and written to:

- Steal information
- Spy on users
- Gain control of computers

Categorised by:

- How it spreads
- What it does

Types:

- Viruses/worms
- Trojan horses
- Zombies and botnets
- Keyloggers
- Backdoors
- Logic/time bombs
- Spyware

Malware — what is it?

Viruses

- Can infect and spread, but need human assistance People download infected email attachments, shared files, spoof links, etc.

E.g. ILOVEYOU virus

Worms

- Can infect and spread without human assistance.

E.g. Sasser worm

Trojan horses

- Program with a hidden malicious function.
E.g. It looks like something you want but it does something you do not want.
- Can cause computer crashes and be used by attackers to gain remote access to your system or steal information.

Zombies

- Also known as bots
- Compromised computers under the control of an attacker.
- Make it possible for someone else to control your computer from anywhere in the world.

Botnets

- A collection of compromised computers (zombies) under the control of an attacker.
- Attackers pool the computing power of all of the zombie machines to launch huge spam attacks or to bring down websites through Distributed Denial of Service (DDoS) attacks.
- DDoS attacks direct massive amounts of communication requests and traffic to websites in attempt to overwhelm their servers.

Keyloggers

- Tracks users' keystrokes, obtains passwords and other personal information.
- Especially dangerous because they track everything a user does, not just what they do on an unprotected internet browser.

Backdoors

- An entry point into a program without all the normal, built-in security checks.
- Programmers sometimes install backdoors when they develop programs so that they can manipulate a program's code more easily during troubleshooting and testing.
- Sometimes they forget to close them.
- Attackers use malware like viruses, worms, and Trojan horses to install backdoors on the computers they infect.

Logic/time bombs

- Malware designed to lie dormant until a specific logical condition is met.

E.g. A particular person logs in

A specific date or time

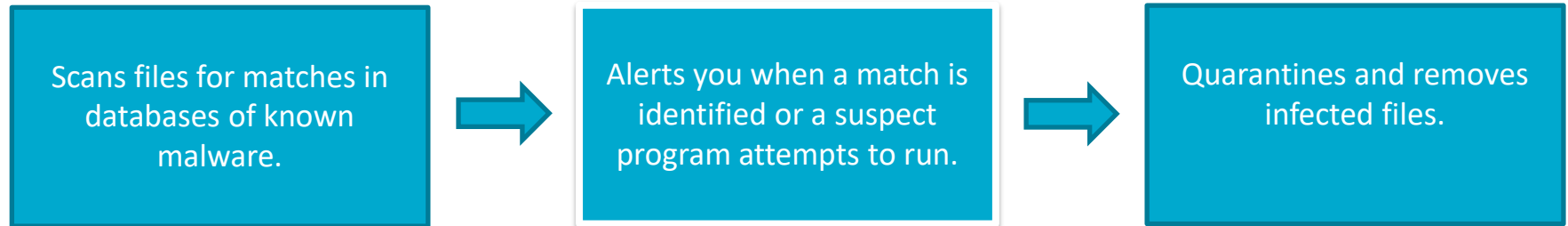
A message is received

Spyware

- Collects information about you, without your knowledge or consent.

Keyloggers are a type of spyware.

Anti-malware software (traditional)



- This type of anti-malware software (using database scanning) does not protect against new, unknown and bespoke malware.
- New protection software which utilises Artificial Intelligence to detect unusual activity and alert the user is now becoming more popular.

Section 4

Basic cyber security techniques

Basic cyber security techniques

- **Identification**

Providing user identity to a system.

- **Authentication**

Verifying the user identity.

- **Authorisation**

Determining whether a user is allowed to access certain resources.

- **Accountability**

Holding users responsible for their actions on a system.

Identification and authentication

Uses encryption to ensure that a user is who they say they are.

Methods

- Passwords
- Physical 'keys'
E.g. Key chains, swipe cards.
- Biometrics
E.g. Fingerprints, retina scanning.

Threats

- Brute force cracking
Test every possible combination of letters, numbers, and characters until the password is found.
- Dictionary cracking
Test words and combinations of words found in the dictionary or from a slightly shorter list of words known to be commonly used in passwords.

Authorisation

Uses tools to control access to a resource.

Methods

- File permissions
- Account management
- Sharing settings

Threats

- Insider threats
Disgruntled or inexperienced employees that have high-level access may cause intentional or accidental harm to a system.
- Elevation of privilege
Attacker is able to enter the system as a low-level user, but is able to attain high-level access.

Methods covered in detail in later modules.

Accountability

Holds users responsible for their actions on a system.

Methods

- System monitoring
- Audit logs

Threats

- Denial of Service
Attack overwhelms audit logs with excessive or very large log entries, causing the system to run slowly or not at all.
- Disclosure of confidential information
Attacker is able to gather confidential or personally identifiable information from log files.

Methods covered in detail in later modules.

Section 5

Passwords

Passwords

1234 is **NOT** a good password. Let's look at ways to improve this:

CLOUDS

Complex • Lengthy • Only yours • Unique • Different • Short term

Complex

Total combinations of passwords consisting of 8 characters:

- Numbers only: 100 million
- + Lower case: 2.8 trillion
- + Upper case: 210 trillion
- + Symbols: 7.2 quadrillion

Always use a combination of the following:

- Numbers
- Upper and lower case letters
- Symbols (% # * & ! : { " > |)

Old password:

1234

New password:

Pa123!

Passwords

Lengthy

Brute force attacks can run 4 billion calculations per second or more.

- <6 characters Cracked within 3 minutes
- 7 characters Cracked within 5 hours
- 8 characters Cracked within 3 weeks
- 9 characters Cracked within 5 years
- 10 characters Cracked within 526 years

Aim for a lengthy password (10 or more characters).

Old password:
Pa123!

New password:
Password123!

Only yours

Do not share your password with ANYONE.

Unique

Do not use words found in the dictionary.

Fend off dictionary cracking attacks by using passphrases.

Where's the beef?
Wh D@ B33f?

becomes
WhD@B33f?

Passwords

Different

Use different passwords for each login.

E.g. Gmail and Facebook

73 per cent of people do not. This means if one of your passwords is discovered, all of your passwords are discovered.

Example 1

Base password: Ronald123!

Site: Gmail

Site password: GMA

Base password + site password = Ronald123!GMA

Example 2

Base password: Ronald123!

Site: Facebook

Site password: FAC

Base password + site password = Ronald123!FAC

Old password:
Password123!

New passwords:
Ronald123!GMA
Ronald123!FAC

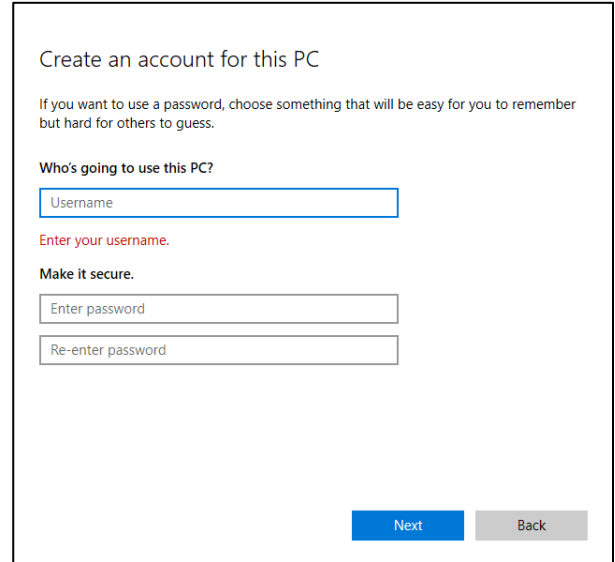
Passwords

Short Term

The longer you keep a password the longer attackers have to try and crack it.

Changing your passwords regularly can help foil cracking attempts as they happen.

It's best to change your passwords at least every few months.

A screenshot of a Windows account creation window. The title is "Create an account for this PC". Below the title is a message: "If you want to use a password, choose something that will be easy for you to remember but hard for others to guess." The next section is "Who's going to use this PC?" with a text input field containing the placeholder "Username". Below this is a red error message: "Enter your username." The next section is "Make it secure." with two text input fields: "Enter password" and "Re-enter password". At the bottom right are two buttons: "Next" (blue) and "Back" (grey).

Create an account for this PC

If you want to use a password, choose something that will be easy for you to remember but hard for others to guess.

Who's going to use this PC?

Username

Enter your username.

Make it secure.

Enter password

Re-enter password

Next Back

Building strong passwords

NOT names

Do not use any personal information in your password.

This can be easily found out by other means.

Name

Birthday

Pet's name

Mother's maiden name

Hometown

Remember CLOUDS

Complex

Lengthy

Only yours

Unique

Different

Short term

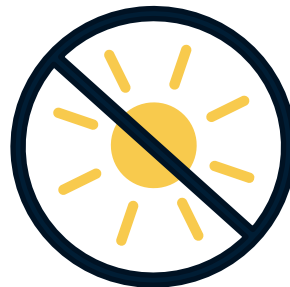


Not SUN

Simple

User ID

Names



Old passwords:

Ronald123!GMA

Ronald123!FAC

New passwords:

WhD@B33f?GMA

WhD@B33f?FAC

Gold standard

Consider using a password manager.

Risks

- All passwords in one place.
- If master password is compromised, all compromised.

Benefits

- No need to remember 30+ different passwords.
- Can auto-generate very strong passwords.

When considering a password manager:

- Make master password is VERY strong (CLOUDS, aim for 18+ characters).
- Enable Two-Factor Authentication.
- Research history of the password manager.

Independent security audits?

Any previous breaches?

Old passwords:

WhD@B33f?GMA

WhD@B33f?FAC

New passwords:

S&hcBBJ9&^b2vucw02n

NAKC8e92^@hn&bsk))_