## Forms response chart. Question title: Does your Password:. Number of responses: 14 responses.

## Forms response chart. Question title: Have you familiarised yourself with:. Number of responses: 13 responses.

## Forms response chart. Question title: Do you have 2 Factor Authentication?. Number of responses: 14 responses.

## Forms response chart. Question title: How do you store Passwords/Keys?. Number of responses: 14 responses.

## Forms response chart. Question title: Do you have an up-to-date Antivirus?. Number of responses: 14 responses.

## Forms response chart. Question title: How often do you update your passwords?. Number of responses: 14 responses.

## Forms response chart. Question title: Do you use a unique password for each Account/Device?. Number of responses: 14 responses.

## Forms response chart. Question title: Are your projects backed up?. Number of responses: 14 responses.

## Summary

All participants are familiar with at least 1 type of cyber attack with the most recognised being Phishing Scams and Scam Calls with ~92% confident they could identify them. The least understood of all these attacks was on Insider Threats and DDoSing (distributed denial of service attacks) with an alarmingly low 46% and 61.5% recognition rate respectively.

The password security measures of including numbers, capital letters, and special characters into their personal passwords is used effectively by most people who participated in the survey. The only thing that could use improving is the number of characters in the passwords, which could be increased to diminish the likelihood of an effective brute force attack. On a positive note, everyone surveyed answered that they are using a 2FA where applicable.

Less than half of respondents use a password manager, with 15% relying on sticky notes and ~35% using a notes application. The most common way that people store their passwords is just remembering the passwords without having them written down.

Additionally, a third never update their passwords. 15% surveyed don’t have an up-to-date antivirus program.

All respondents have a backup of their projects in some form, whether over cloud or on an external drive.

Training in the Identification, Prevention and Recovery of the following security threats is provided:

* Ransomware
* Phishing Scams
* Scam Calls
* Insider Threats
* DDoS Attacks
* Other Malware

Identification: Telltale signs of scams, and detection of viruses through Antivirus

Prevention: familiarity with Password Policy, Firewalls, 2 factor authentication

Recovery: Project Back Ups, Deletion of Malware, Reporting

Antivirus must be kept up to date (auto-update).

# Identification

## Antivirus

Approved antivirus is to be installed and kept up to date, and should commence regular automated scans.

## Scams

* Don’t click links in emails
* Verify sender address
* Check Caller Id
* Suspicious formatting/grammar

# Prevention

## Password Policy

Passwords must include:

* At least 12 characters
* Special characters
* Capital letters
* Numbers

Passwords must be stored with an approved password manager. Passwords must not to be recorded as physical copy (sticky notes) or as a non-protected note file.

Passwords must be updated every six months through the Password Manager.

Each account/Device Password must be unique.

Biometrics/2FA to be used where supported.

## Workspace Practices

Unattended computers must be locked. Additionally, Devices must be shut down at the end of the day. If using an unlocked (public) computer ensure signed out of browsers etc.

Any External drive is to be scanned before use.

# Recovery

## Back Up

All projects must be backed up online (cloud, repository) and on an external drive.

An online Back up should be made at the end of each day, and a copy of all work saved to an external hard drive each week. Hard drive should then be disconnected from computer.

# Resources

<https://www.passwordmonster.com/>

Check strength of password against brute force attacks. Identifies what makes your password a *good* password.

<https://www.cyber.gov.au/threats>

Articles detailing threat types. Covers identification, prevention and how to report.