
AiSP
Association of
Information Security Professionals
AiSP x ASPRI
CAAP Awareness Workshop: Managing Cyber Risks in a Digital Workplace
In collaboration with ASPRI
Speaker: Tony Low, CAAP Co-Chair
12 October 2020
Royalty-free image for Microsoft O365 subscribers.

Agenda

1. Digital tools: Email, Cloud Storage, App and Smart Devices

2. Is Your Password Secure?

3. Social Engineering: Phishing, Fraud and Business Loss

About AiSP

Started in 2008, the **Association of Information Security Professionals** (AiSP) is an independent cybersecurity membership-based association focusing on **developing, supporting** and **enhancing industry technical competence and management expertise to the integrity, status and interests of Information Security Professionals in Singapore**.

Programmes and Initiatives

ADVANCE
- Body of Knowledge
- CREST Singapore Chapter
- Cybersecurity Awareness & Advisory Programme
- Ladies in Cyber
- Student Volunteer Recognition Programme

CONNECT
- Academic Partnership Programme
- Corporate Sponsorship Programme
- Corporate Sponsorship Programme Plus
- International & Regional Collaboration

EXCEL
- AiSP Validated Information Security Professional Certification
- Qualified Information Security Professionals
- The Cybersecurity Awards

Cybersecurity Awareness & Advisory Programme (CAAP)

Targeted for Singapore SMEs, the CAAP aims to **drive digital security awareness and readiness**. Supported by CSA, our CAAP operating committee focuses on:

1. Enhance security awareness and training
2. Create cohesive security knowledge resources
3. Offer security solutions and services support

The three thrusts are driven by the respective working groups of credible and passionate infosec professionals, supported by AiSP secretariat. We are looking for more companies to tap on CAAP and also, partners and professionals to support the cybersecurity ecosystem.

AiSP Association of Information Security Professionals | CAAP

Cybersecurity Awareness & Advisory Programme (CAAP)

CyberSecurity Awareness

as integral part of

SME Business Owner Fundamentals

CyberSecurity Awareness

Body-of-Knowledge

for Business Owners and Individuals

Self-Sustainable Support Ecosystem

For SME 's

- ✓Outreach
- ✓Knowledge
- ✓Solutions

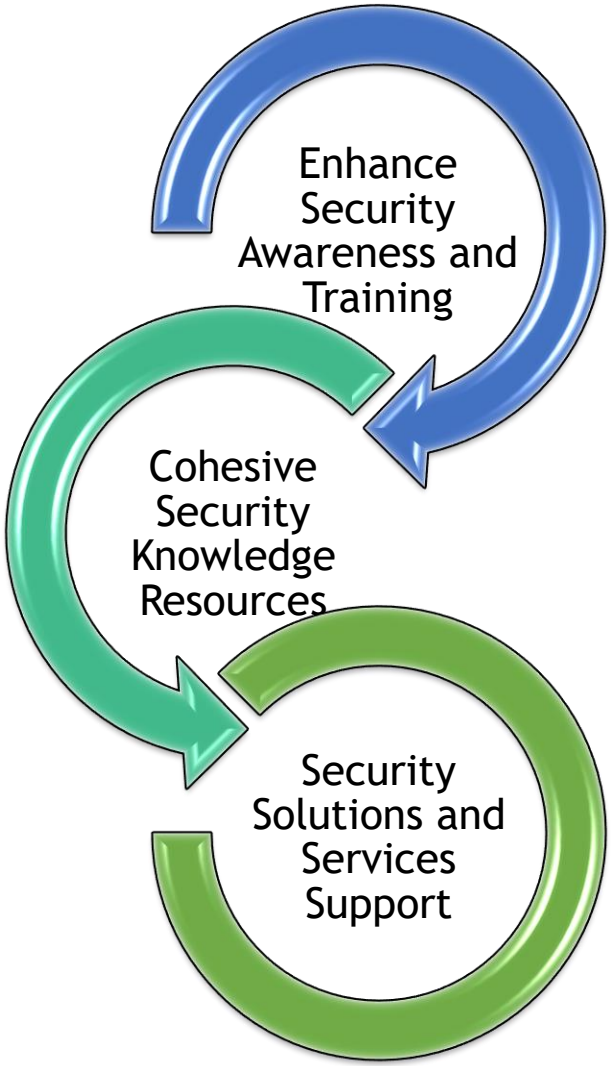
Create a common starting point and guided journey For SME Owners and Individuals To achieve Cyber Security Awareness through Collaboration

Cybersecurity Awareness & Advisory Programme (CAAP)

SME Cyber Safe PORTAL
- Create a Online Sitemap for Businesses & Individuals in terms of Cyber Awareness Maturity Journey

BOK
- Establish a Cyber Security Body of Knowledge (BOK) for Businesses and Individuals

Knowledge Management
- Build and Maintain Cyber Awareness Workshops Curriculum with Leverage on through Collaboration (e.g. SingCert, PDPA)



General Cyber Awareness Workshops
- Collaborated with Associations
- Targeted at Business Owners and Individuals

Focus Groups
- Concise group for Feedback and Consultation to update for General Cyber Awareness w

Emergency Advisory Workshops
- Ecosystem Collaboration to outreach in times of large cyber outbreaks

Cyber Awareness Fundamental
- *Online or Instructor-Led Training based on Cyber Security Body of Knowledge (BOK)*

Cyber Security Site Map
- Provide intuitive guide to match Cyber Concerns and Issues to Security Solutions & Services

Grants and Program Support
- Provide Linkage to Key Grants and Schemes e.g. Start Digital GoDigital/ PSG

SME Vendor Ecosystem
- Ease of access to relevant vendors and solutions
- Promote vendor participation in SME solutions and services

www.smecybersafe.sg

CAAP – Awareness & FGD Workshops

The CAAP workshops serve the following objectives:

A. Awareness workshop

Companies may not be aware of cyber risks in their digital transformation or when they want to embark on digital initiatives. The awareness workshop by various speakers give a macro view of what companies and their staff should be aware of, and what they can do to mitigate risks.

B. Focus Group Discussion (FGD) workshop

Companies that attended the Awareness workshop, may have done some checks at their workplaces on potential cyber risks. Armed with this newly-found knowledge, they want to take the next steps to be cyber-ready for their business needs. The closed-door workshop is by invitation only to attendees from (A), for them to clarify on how they want to address their cyber risks.

CAAP - Body of Knowledge for SME Business Owners

Module 1: Understanding the Digital Business Landscape

Module 2: Understanding the Digital Transformation Journey

- Module 2.1: Improving Productivity
- Module 2.2: Expanding Business Online
- Module 2.3: Emerging IT Technologies and their impact to cybersecurity cloud (IaaS, PaaS, SaaS)
- Module 2.4: Mobility and Internet of Things

Module 3: Understanding Risk and Threats to Business

- Module 3.1 Asset Identification and Risk Assessment
- Module 3.2: Cyber Attacks (Phishing, DDoS, Ransomware)
- Module 3.3: Social Engineering (E-Commerce fraud, Tech support fraud

Module 4: Securing the Business

- Module 4.1: Handling data securely
- Module 4.2: Cyber hygiene (updating IT assets and implementing cybersecurity measures)
- Module 4.3: Protection of Customer Data

Module 5: Understanding Business Obligations

- Module 5.1: PDPA
- Module 5.2: Cybersecurity Act
- Module 5.3: Computer Misuse Act
- Module 5.4: Regulatory Requirements
- Module 5.5: Contractual Obligation & Liabilities

Module 6: Incident Handling / Reporting

About the Speaker

Who Am I?

- 15+ Years in Consulting and Architecture – with focus on Financial institution
- Digital Strategist
- Challenging the *#norm*
- Passion in mentoring and giving back

Tony Low

tony.low@aisp.sg
LinkedIn: https://www.linkedin.com/in/tonylowsg/

AiSP
Association of
Information Security Professionals

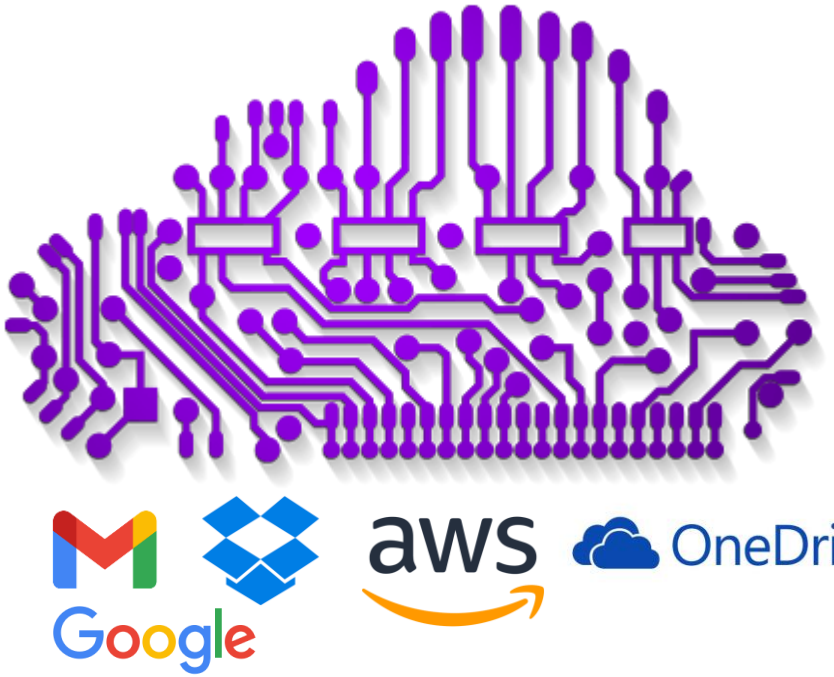
Digital tools: Email, Cloud Storage, App and Smart Devices

Royalty-free image for Microsoft O365 subscribers.

What are they?

Cloud Services:

- Every business and individual is a user of cloud services and the COVID pandemic has only accelerated the adoption



Digital Services:

- Entire user experience are conducted online via a platform (phone, computer, others)

Why are the benefits?

1. **Cloud Storage Can Save Costs**
    - Self service
    - No Need to manage complicated storage capacity and devices
    - Can be expanded on demand
    - Data Tiering for Cost Savings
2. **Data Redundancy and Replication**
    - Data redundancy is included where the same files is replicated to many servers / data center automatically increasing data durability
    - automatically provided as part of their infrastructure
    - Can be accessed anywhere
3. **Ransomware/Malware Protection**
    - Data store in cloud will required additional credentials for access
    - Provides a copy of your critical / important data / information in the event of an attack

What are the risk?

- Data privacy
- Lack of control
- Shared servers
- Insider threats
- Compliance violations

AiSP
Association of
Information Security Professionals

Is Your Password Secure?

Royalty-free image for Microsoft O365 subscribers.

An Overview - Password

- Why do we need Password
- Creating a Strong Password
- Common Password Attacked
- Helping passwords better protect you

Creating a Strong Password

- Do not choose a password with successive keyboard strokes - “qwerty”, “12345”
- Do not use your personal information as password - Name, birthday, mobile number
- Do not write down your password on post it and leave it exposed
- Do not use the same password for **EVERYTHING**

Common password attacks

1. Brute force attacks
2. Dictionary
3. Social Engineering

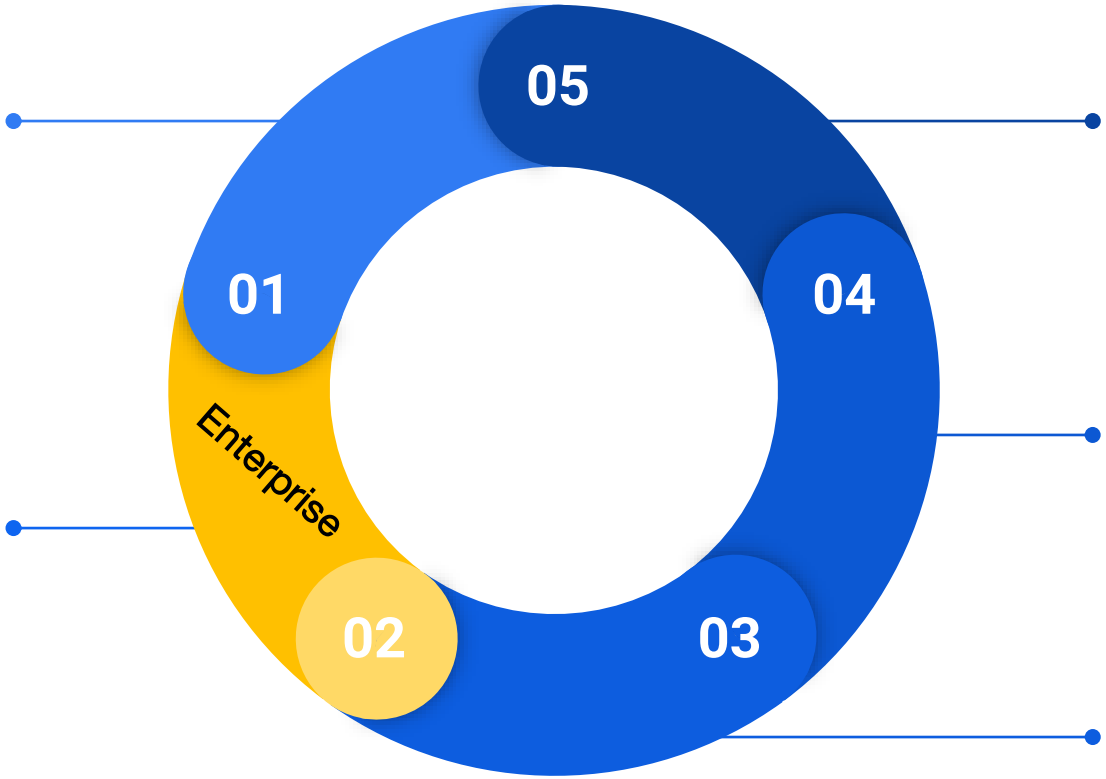
Helping passwords better protect you

Use a different password for each important service

Prevent stolen password to be reuse in your important services. Have a set of passwords that you used for work and personal

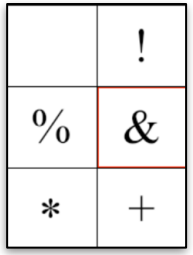
Using Single-Sign-On / 3rd Party Systems

Help to reduce the number of password



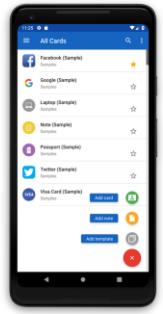
Make your password hard to guess

Include special characters and mix caps, minimum password length



Keep your password somewhere safe

Using a password vault to store your passwords



Set a recovery option

Make sure that password can be reset including 2FA enabled accounts

AiSP
Association of
Information Security Professionals

Social Engineering: Phishing, Fraud and Business Loss

Royalty-free image for Microsoft O365 subscribers.

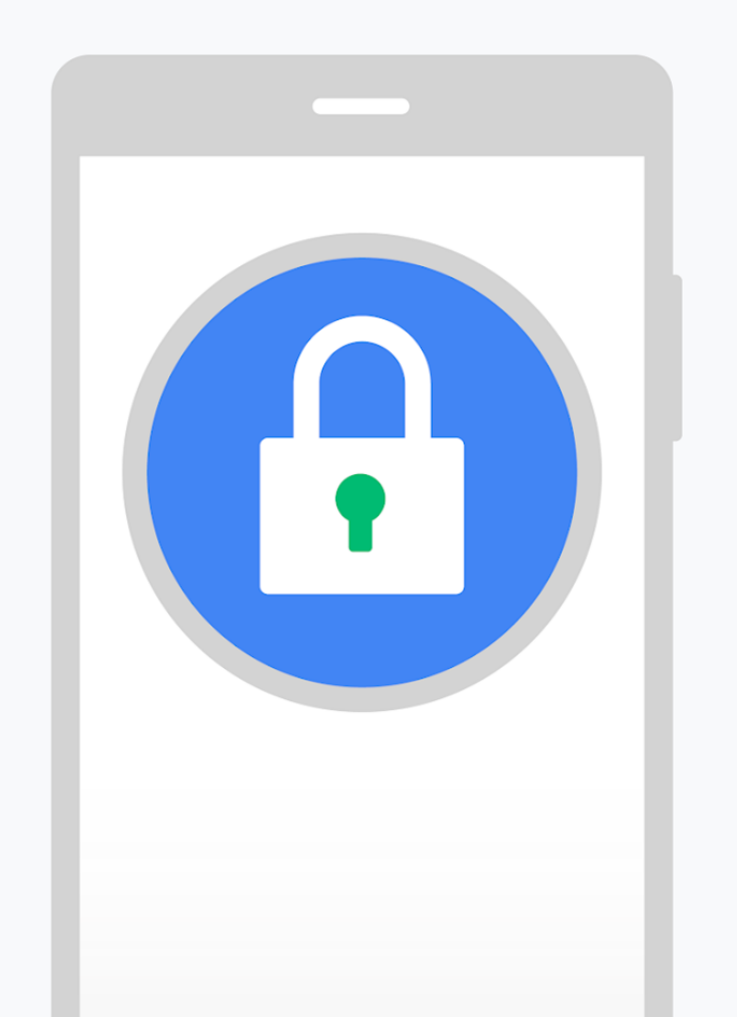
What is social engineering?

Social engineering occurs when someone develops personal relationships and uses those relationships as a tool to gain access to protected information or material.

- Social engineering also happens when the perpetrator uses such covert data collection methods as the following:
- Eavesdropping on conversations, radio traffic and phone calls.
- Peering over one's shoulder to view passwords.
- Reading confidential documents left out in the open on a desk or at a workstation.

How it’s done? An Example: Stealing passwords

- Friending: Gaining the trust of his target and either tricks or convinces the target to click on links or attachments that contain malware.
- Impersonation: taking identity of a friend or coworker and asking for a favor over the phone, or by email or instant messaging.
- Caller ID spoofing: causing the victim’s caller ID to display an authentic phone number, convincing the victim that the caller is legitimate.
- Email spoofing: using a forged email address that appears to come from a legitimate sender



Phishing

Phishing: via email or chat; the phisher poses as a employee or a legitimate company's representative to gain sensitive or protected information that should not be available to outsiders.

Phone phishing: direct phone contact; the caller claims to be a employee or a legitimate company's representative and has the victim provide sensitive information that should not be available to outsiders.

Identifying a Phone Phishing Attempt

The phisher might even know the right lingo - do not confirm anything they say.

They might say something along the lines of:

- I'm at the airport and really rushed; I just need you to give me this number.
- My corporate email is down; can you just send it to my personal gmail instead?
- I have his/her number, but I just can't find it right now and I'm in a hurry.
- I met with him/her the other day but I can't find their business card.
- I lost my phone with my contacts; can you give me the number for _____?
- Please transfer me to _____. They're expecting my call. Hurry, it's urgent.

If you think you've been targeted for phishing:

1. Notify your supervisor ASAP
2. Change your passwords
3. Scan your computer for virus
4. Verify if there is any identify theft
5. File a report to PDPC
6. Protect yourself against future phishing