RAJAH & TANN TECHNOLOGIES

NOVUSDEMIA
Discover the Future of Learning

R&TCYBER
Safeguarding your Digital Assets

Essential Communications Security

With the rise of digitalisation, communication between people and businesses is no longer bound by time and geographical constraints. As more organisations adopt remote working commonly known as "work from home" as the new normal, email, teleconferencing and messaging have become the primary form of communication for work. However, this also leads to a rise of cyber-attacks relating to these forms of communication.

It is essential for employees to be informed of the potential threats and the impact of these attacks, to prevent and mitigate them before they potentially cause substantial damage to your organisation.

The Essential Communications Security (ECS) course is a collaborative effort between Rajah & Tann Technologies and Rajah & Tann Cybersecurity, which caters to all organisations to build awareness among all personnel in these vulnerable areas, namely Email Security, Teleconferencing Security and Messaging Security.

Course Objectives

This course aims to equip participants with the fundamental knowledge of potential threats, mitigation, and prevention measures of essential communications security, which will be supplemented with the use of interactive scenarios and case studies.

By the end of the course, participants will be able to:

- Learn the importance of being aware of email, teleconferencing and messaging attacks
- Understand the different types of email, teleconferencing and messaging attacks that can be encountered
- Understand the impact of these attacks on individuals and organisations
- Apply the instructed necessary mitigation and prevention methods

Course Details

Duration	:	**2 hours**
Modules	:	**3**
Delivery	:	**Online interactive course**
Suitable for	:	**All personnel**

**For more details on course fees and plan features, please contact us for more information.*

The course consists of post-module quizzes and a mandatory assessment which participants are required to pass to complete the course. A digital certificate of completion will be issued and is available for download upon successful course completion. Tracking and reporting of participants' progress are also available for corporate users. Content will be updated periodically to ensure recency with legislative and regulatory requirements and current digital trends.

Course Overview

Module 1: Email Security

Email is one of the most commonly used forms of communication for personal and work correspondence daily. Over the years, cyber attackers have devised ways to send malicious emails to trick unsuspecting individuals into launching highly damaging attacks on themselves or affiliated organisations. To prevent and mitigate such threats, it is important to be able to identify malicious emails and implement necessary measures to prevent or mitigate such attacks from occuring.

Lesson 1: Impact of Email Attacks

- Deliver malicious payloads to recipients
- Obtain sensitive information from recipients
- Trick recipients to perform fraudulent activities
- Damage reputation of the sender and/or organisation
- Breach of laws and/or regulations
- Resource wastage

Lesson 2: Common Types of Email Attacks

- Phishing
- Spam
- Accidental data leak emails
- Inappropriate emails

Lesson 3: Measures Against Email Attacks

- Measures against phishing emails sent to your business contacts and/or organisation
- Measures against accidental data leak emails
- Measures against inappropriate emails

Course Overview

Module 2: Teleconferencing Security

Teleconferencing has become the norm for organisations to communicate. With the use of teleconferencing apps, a meeting can be held online from any part of the world in real-time without the need for travel. However, cybercriminals have found ways to eavesdrop, hijack or disrupt web meetings for several reasons, including obtaining confidential information, for ransom, or even for their own amusement. Thus, it is important to learn how to prevent or tackle such situations when they occur.

Lesson 1: Impact of Teleconferencing Attacks

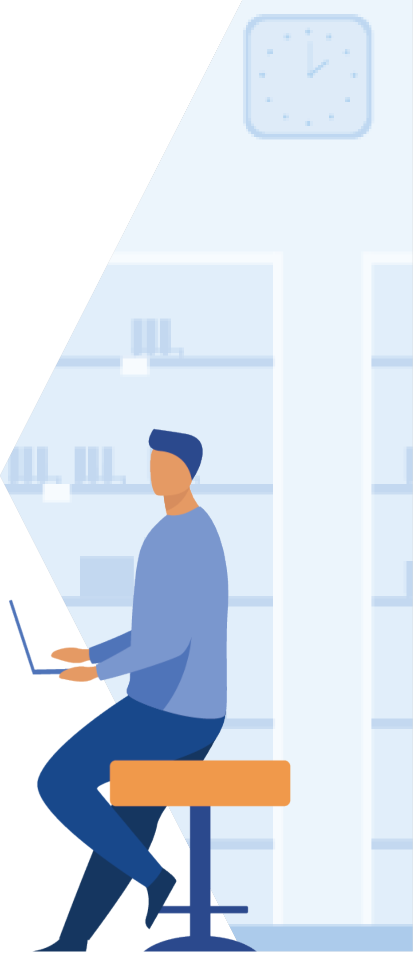
- Disruption by visual and/or audio interference
- Compromise via malicious files or links
- Trick recipients to perform fraudulent activities
- Disruption by visual and/or audio interference

Lesson 2: Common Types of Teleconferencing Attacks

- Unauthorised access
- Sabotage
- Infection of participants
- Data leakage

Lesson 3: Measures Against Teleconferencing Attacks

- Measures against unauthorised access
- Measures against sabotage
- Measures against infection of participants
- Measures against data leakage
- Data privacy
- Audit logging
- Teleconferencing Social Etiquette



Course Overview

Module 3: Messaging Security

Messaging has become the norm for communication in our everyday life. Before the introduction of smartphones, people used text messaging (SMS) to communicate with one another on mobile, while today it is more commonly used by service providers to send important notifications. In the recent years, instant messaging (IM) has revolutionised the way we communicate with messaging applications with features such as file sharing and group chats. Due to the instantaneous nature of messaging, users are susceptible to attacks such as phishing scams, malware and data leakage. Thus, it is key to understand the several measures users can take to protect themselves from such attacks.

Lesson 1: What is Messaging?

- Concepts of Messaging
- Common Features of Messaging Applications
- Superapps

Lesson 2: Types of Messaging Attacks

- Accidental Data Leakage
- Spoofing
- Malware Sharing
- Spam / Spim
- Malicious Spread of Information
- Unauthorised Access
- Botting
- Social Engineering

Lesson 3: Measures Against Messaging Attacks

- Security Setup
- App Usage
- Privacy Settings
- Other Measures

RAJAH & TANN TECHNOLOGIES NOVUSDEMIA Discover the Future of Learning R&TCYBER Safeguarding your Digital Assets

About the expert: Wong Onn Chee

- Chief Executive Officer, Rajah & Tann Cybersecurity
- Technical Director, Rajah & Tann Technologies
- CISSP, CISM, CISA, GCIH, CISSP-ISSAP, CDPSE, SABSA Chartered Architect, AVIP, CRISC

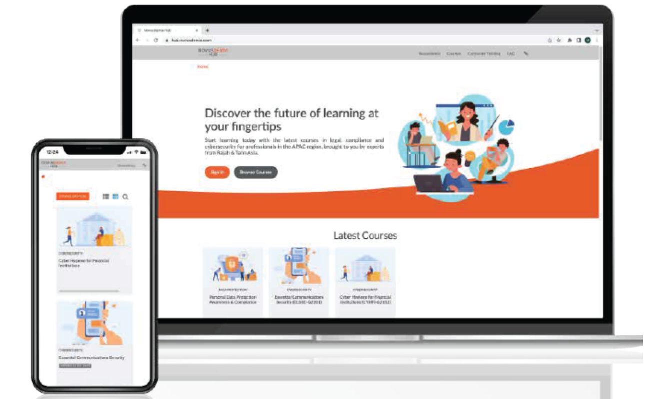
Wong Onn Chee has more than 21 years of experience in the cybersecurity field and has been involved in the security assessment and advisory of major nationwide IT systems in Singapore. His key areas of expertise include information leakage protection, web security and security strategy.

He is the current Chapter Leader of OWASP Singapore and a member of the working groups which developed Singapore's first standard on cloud security and technical reference on IoT Security.

About NOVUSDEMIA

Novusdemia is the training content development arm of Rajah & Tann Technologies that provides courses in legal, compliance and cybersecurity for professionals in the APAC region. Curated by highly experienced subject matter experts across Rajah & Tann Asia, Novusdemia courses are designed to offer top quality training through engaging interactive content and knowledge assessments for effective learning.

Novusdemia courses can be accessed on Novusdemia Hub, an online learning platform that provides a seamless learning experience without geographical or time restraints. Novusdemia Hub makes training accessible and manageable for organisations with features needed to deliver training quickly and effectively to every user, while keeping a pulse on progress and results to ensure compliance.



NOVUSDEMIA HUB

Log in to Novusdemia Hub at hub.novusdemia.com

For enquiries about the course and Novusdemia Hub, contact us at:

T: +65 6988 4903 E: contact novusdemia@rttechlaw.com www.novusdemia.com