CyberSecurity MALAYSIA

MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

KAAPAGAM EDUCATION

CYBERSECURITY AWARENESS FOR ALL USERS

With all the news stories about hackers, botnets, and breaches involving personal information, it's easy for the security message to sound over-used and tired. It's easy for people to say, "It won't happen here." Yet, studies and surveys repeatedly show that: the human factor (what employees do or don't do) is the biggest threat to information systems and assets. Until we address the human issue, technology alone cannot secure your organization. Humans will remain as the weakest link in the Security Chain.

This High-impact security awareness training addresses these issues. It ensures that your users are aware that they are a target; it motivates and changes behavior by teaching them how to use technology securely and ensures your organization remains compliant. In addition, by teaching your users the indicators of compromise and how to report incidents, you go beyond just prevention and begin developing human sensors, creating a far more resilient organization.

This training is an INTERACTIVE story board with 100% LIVE HACKING Demo based workshop for All users who use Internet, Computer, Mobile Phones, and Social Media. NO Technical Jargons – Suitable for ALL.

> "Humans will remain as the weakest link in the Security Chain"

OBJECTIVE

1. Understand the Basics of Security and Attack Lifecycle;
2. Understand the Latest Attacks in the wild with Live Demos instead of boring slides;
3. Understand the importance of Strong and Unique passwords;
4. Understand the importance of Strong and Unique passwords;
5. Understand Email and Messaging App Attacks and its Security;
6. Understand Wireless Attacks and Dangers of Free Wifi spots and how to be vigilant; and
7. Understand the Mobile devices Security.

OUTCOME

1. Attendees will learn basics of Security and understand about Vulnerabilities and how defense technologies like Anti-Virus, Firewall work;
2. Attendees will understand how all the Latest Attacks are carried out with DEMOS. This will help the attendees to be more aware on the current threats and Risk;
3. Attendees will learn on how hackers manipulate and turn their mind and data against them for a successful attack;
4. Attendees will also learn on different social engineering attacks including Facebook based attacks with DEMOS and Best practices on how to be aware and secure from these attacks;
5. Attendees will learn on importance of Strong Passwords and how wrong password usage opens up for data theft resulting in Identity theft and compromise with DEMOS;
6. Attendees will also learn the best practices for Password and how to create and remember Strong passwords without sticking the passwords on the Monitor or keyboard;
7. Attendees will learn on attacks via EMAIL and Messaging applications with DEMOS. Attendees will also learn best practices for Email and Messaging software's and how to distinguish spam and phishing emails from the genuine;
8. Attendees learn on how Hackers compromise devices thru WiFi with DEMOS and how to secure office and personal devices from Hackers;
9. Attendees will learn the necessity of Security on Mobile devices and how hackers hack your mobile devices and a sample Android Malware with DEMOs; and
10. Attendees will also learn the security best practices for the mobile devices.

AGENDA

Session 1 : Introduction : Anatomy of an Attack

- What is Security, Vulnerabilities & O-Days
- Attack life Cycle & How much hacker makes by selling your passwords and data?
- Different Attack Vectors, Threats Vs. Risks, Exploit Basics
- Why Perimeter defenses are failing?
- Why Anti-Virus is not enough?

Session 2: Latest Attack Trends : 100% Demo

- Mobile Malwares
- Web Attacks
- Business Email Compromise (BEC)
- Ransomware
- Advanced Persistent Threat
- Malvertising
- Identity Theft

Session 3 : Social Engineering Attacks : 100% Demo

- Drive by Download Attack with Java
- USB / File attachment Attacks
- Phone Call & Sweet Talking
- Facebook and social Media based attacks
- Best Practices for Safer Social Media Usage for Adults and Kids

Session 4 : Password Management & Privacy

- What is strong Password ? Why password must be changed at least once in 90 days?
- Why you should not use same password in more than 1 web application?
- Best Practices for Password Management & Privacy

Session 5 : Email & Messaging Security

- Email Spoofing
- Phishing
- Disposable Emails
- WhatsApp, Telegram and similar Messaging Systems security
- Best Practices for Email Security
- Best Practices for Messaging Software

Session 6 : Wireless Attacks : 100% Demo

- Why Public Wifi and Free hotspots are dangerous?
- Sniffing and MiTM attacks on Wifi
- How to secure office and house Wifi

Session 7 : Mobile Security

- Jail Breaking & Rooting : Why its disaster?
- Do you need Antivirus on a Mobile device?
- How hackers hack your phone and control it?
- Security best practices for Mobile

GET IN TOUCH

☎ 03 - 8800 7999

✉ training@cybersecurity.my

⌂ www.cyberguru.my

TRAINER

Mr. Clement Arul

Chief Executive Officer,
Kaapagam Technologies Sdn Bhd

- Mr. Clement Arul is a two-time recipient of Cyber Security Professional of the Year in 2017 and 2014 as well as a three-time Regional Award winner of Cyber Security Professional of the Year Asia and APAC in 2020, 2019 and 2017.
- A Principal Technology Architect, Security Professional and an Evangelist with Twenty Two (22) years of IT experience in Cyber Security, Ethical Hacking, Cyber Security Framework, Security Risk & Governance, Big Data, IoT, Systems Analysis, Design, Development, Secure Coding, Implementation, Digital Forensics and Project Management.
- Founder and CEO of Kaapagam Technologies Sdn. Bhd. and Kaapagam Education Services Sdn. Bhd. Also, Founder and Chief Technology Officer of Vigilant Asia (M) Sdn. Bhd.
- He has contributed to National Cyber Security Framework and many more national initiatives and now working with few ASEAN governments in developing and implementing National Cyber Security Frameworks. He was also part of the Secure Implementation of Nigerian ID system Project in 2019 as the prime security expert consultant.
- Presented in more than 120 public conferences and Talks in last Year and more than 600+ in last 5 Years across ASEAN
- Chief Architect for KALAM – IT Security Collaboration Platform : An MOHE Award Winning Platform
- Chief Architect for VALARI : Common Criteria Certified (the only) Malaysian Web Application Firewall
- Chief Architect for SOC 2.0 – A Regional Managed Detection and Response Platform for SME
- Security Consultant for many Multi-National and Leading IT Companies and Agencies in ASEAN Region
- Specializes in Payment Gateway Hacking, Application Security & Penetration Testing, Big Data & IoT Security.
- Issued 100+ Web Vulnerability Disclosure Documents in last 4 years on Vulnerabilities discovered in Government, Corporate, Banks, Online Payment Gateways and e-Shopping websites in ASEAN.
- Provide Penetration Testing, Vulnerability Assessments, Security Consultations, Security Frameworks, Disaster Recovery & Business Continuity, and Security Audit Services for Customers in APAC Region.
- Conduct Workshops across ASEAN region on Penetration Test, Mobile Security, IoT Security, Forensics Investigations, Secure Programming, Disaster Recovery, Incident Handling, Business Data Analytics, and many more.
- Created a Security Awareness Certification under KALAM and have trained and certified 5300 people across ASEAN including Singapore, Malaysia, Laos, Cambodia, Indonesia in the last year.
- Delivered Security Awareness Talk on Social Media & Cyber Attacks & Defences for public in THR Raaga Malaysia FM Radio: For the entire Nation
- Delivered 13 capsules (days) on various cyber security awareness topics and DO's and Dont's for general public : Nationwide Indian Audience on ASTRO Malaysia Vanavil TV.