ที่ วท 5410.0302/ว 52/2554

19 เมษายน 2554

เรื่อง ขอเรียนเชิญเข้าร่วมงานสัมมนา "Social Networking Security Conference 2011" และ "Mobile Computing Security Conference 2011"

เรียน นายแพทย์โพจิตร์ วราชิต
ปลัดกระทรวงสาธารณสุข
สำนักงานปลัดกระทรวงสาธารณสุข

สิ่งที่ส่งมาด้วย 1. เอกสารรายละเอียดงานสัมมนาฯ
2. ระเบียบกระทรวงการคลังฯ ที่ กค 0406.4/ว485

เนื่องด้วย เขตอุตสาหกรรมซอฟต์แวร์ประเทศไทย ศูนย์บริหารจัดการเทคโนโลยี ภายใต้สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ (สวทช.) โดยความร่วมมือกับ สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (Thailand Information Security Association - TISA) และ บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด (ACIS Professional Center) **กำหนดจัดงานสัมมนา "Social Networking Security Conference 2011" และ "Mobile Computing Security Conference 2011" ในวันที่ 28 – 29 มิถุนายน 2554 เวลา 08.30 – 18.00 น. ณ ห้องแกรนด์บอลรูม ขั้น 4 โรงแรมแกรนด์ มิลเลนเนียม สุขุมวิท กรุงเทพฯ** โดยมีวัตถุประสงค์สำคัญ เพื่อทราบถึงภัยใหม่ของสื่อเครือข่ายสังคมออนไลน์และมาตรการป้องกันด้านความมั่นคงปลอดภัยในการใช้งาน, รู้จักเครื่องมือในการวิเคราะห์ และสังเคราะห์ข้อมูลในสื่อสังคมออนไลน์, รับทราบความก้าวหน้าของเทคโนโลยีเครือข่ายไร้สายของอุปกรณ์ประเภทโทรศัพท์มือถือกับภัยสมัยใหม่อันร้ายกาจ เมื่อโทรศัพท์ได้กลายเป็นคอมพิวเตอร์ส่วนบุคคล ฯลฯ

ในการนี้ คณะผู้จัดงานฯ ขอเรียนเชิญท่านหรือผู้แทนของหน่วยงานของท่านเข้าร่วมการอบรมตามวัน เวลาและสถานที่ดังกล่าว กรุณากรอกแบบฟอร์มการลงทะเบียนเข้าร่วมสัมมนา และชำระค่าลงทะเบียนเพื่อรับส่วนลดภายในวันที่ **6 มิถุนายน 2554** โดยส่งแบบฟอร์มพร้อมเอกสารการชำระเงินมายังหมายเลขโทรสาร 0 2650 5776 ทั้งนี้ในการเข้าร่วมงานดังกล่าวสำหรับหน่วยงานภาครัฐสามารถเบิกค่าใช้จ่ายในการเข้าร่วมอบรมจากต้นสังกัดได้ตามระเบียบกระทรวงการคลัง ที่ กค 0406.4/ว485 เรื่อง การเบิกค่าใช้จ่ายในการฝึกอบรม ลงวันที่ 25 ธันวาคม 2552

จึงเรียนมาเพื่อโปรดพิจารณาเข้าร่วมงานสัมมนาดังกล่าว และหากท่านต้องการสอบถามรายละเอียดเพิ่มเติมสามารถติดต่อได้ที่ฝ่ายประสานงานโครงการฯ โทรศัพท์หมายเลข 0 2650 5771 คุณลัดดา ต่อ 108 คุณวราพงศ์ ต่อ 107 หรือ ลงทะเบียนในระบบออนไลน์ได้ที่ www.snsconference.com

ขอแสดงความนับถือ

(นายไพจิตร์ วราชิต)
ปลัดกระทรวงสาธารณสุข

(นายธนชาติ นุ่มนนท์)
ผู้อำนวยการ
เขตอุตสาหกรรมซอฟต์แวร์ประเทศไทย

(นางนันทพร มานะเมตร)
หัวหน้าฝ่ายบริหารทั่วไป
๒๖ W.A. ๒๕๕๔

เรียน นายแพทย์สาธารณสุขจังหวัดฯ
-เพื่อโปรดทราบ
-เห็นสมควรให้ กุณฑิตินันต์ ประชาสัมพันธ์

ศูนย์บริหารจัดการเทคโนโลยี
เขตอุตสาหกรรมซอฟต์แวร์ประเทศไทย
โทรศัพท์ 0 2583 9992 ต่อ 1420–1425 โทรสาร 0 2583 2884

ที่ กค 0406.4/ว485

กรมบัญชีกลาง
ถนนพระราม 6 กทม.10400

25 ธันวาคม 2552

เรื่อง ระเบียบกระทรวงการคลังว่าด้วยค่าใช้จ่ายในการฝึกอบรม การจัดงาน และการประชุมระหว่างประเทศ (ฉบับที่ 2) พ.ศ. 2552

เรียน ปลัดกระทรวง อธิบดี อธิการบดี เลขาธิการ ผู้อำนวยการ ผู้บัญชาการตำรวจแห่งชาติ ผู้ว่าราชการจังหวัด

ด้วยสำนักเลขาธิการคณะรัฐมนตรีแจ้งว่า ระเบียบกระทรวงการคลังว่าด้วยค่าใช้จ่ายในการฝึกอบรม การจัดงาน และการประชุมระหว่างประเทศ (ฉบับที่ 2) พ.ศ. 2552 ได้ประกาศในราชกิจจานุเบกษา ฉบับประกาศและงานทั่วไป เล่ม 126 ตอนพิเศษ 183 ง วันที่ 22 ธันวาคม พ.ศ. 2552 แล้ว

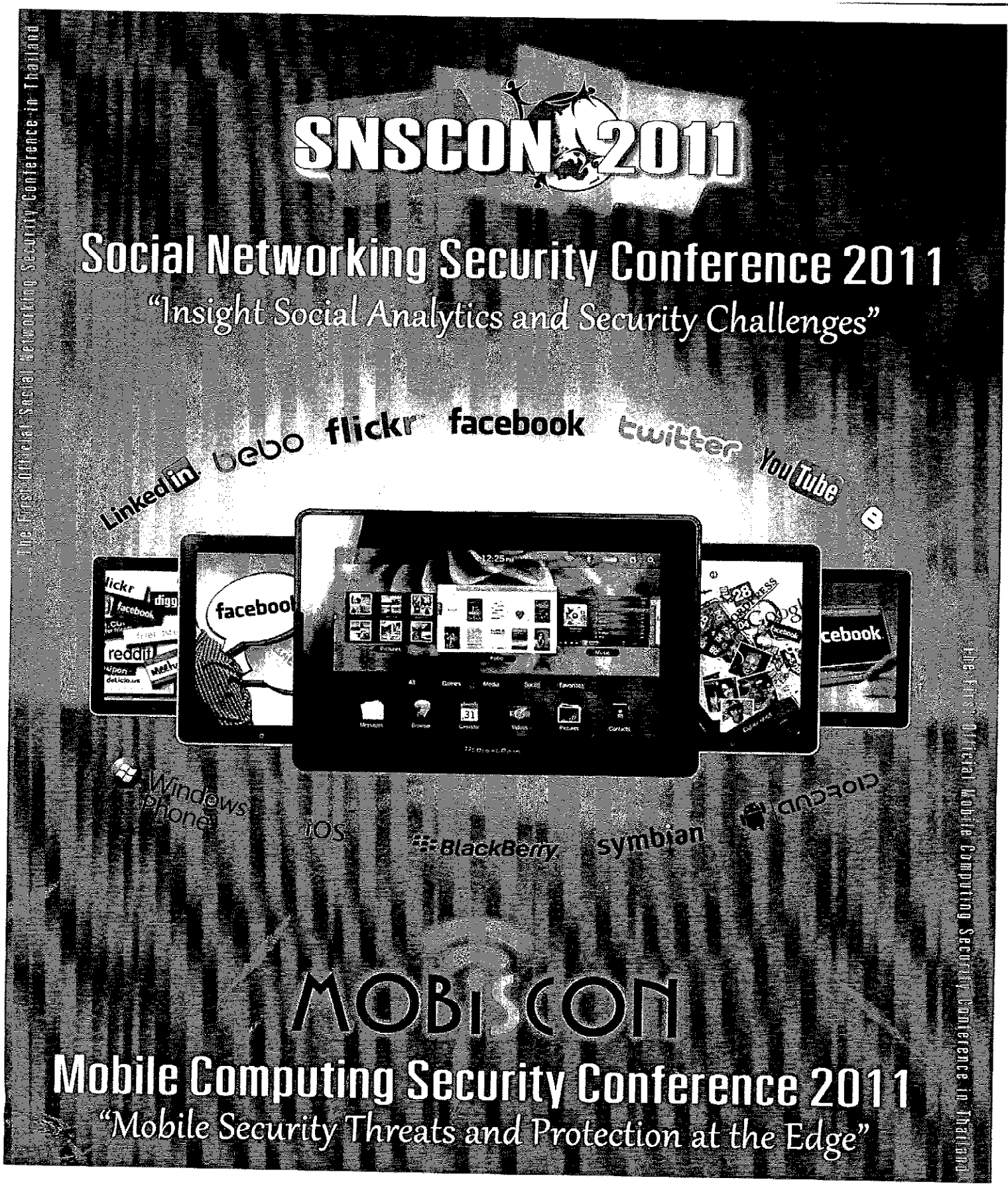
กรมบัญชีกลางขอเรียนว่า ได้นำระเบียบดังกล่าวลงในเว็บไซต์ www.cgd.go.th เรียบร้อยแล้ว

จึงเรียนมาเพื่อโปรดทราบ และแจ้งให้หน่วยงานในสังกัดทราบและถือปฏิบัติต่อไป

ขอแสดงความนับถือ

(นางสาวสุทธิรัตน์ รัตนโชติ)
รองอธิบดี ปฏิบัติราชการแทน
อธิบดีกรมบัญชีกลาง

สำนักกฎหมาย
กลุ่มงานกฎหมายและระเบียบด้านค่าใช้จ่ายในการบริหาร
โทร. 0-2273-9573
www.cgd.go.th

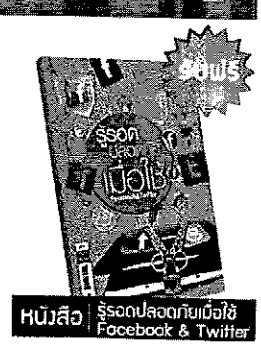


28th - 29th June 2011, Grand Millennium Sukhumvit, Bangkok

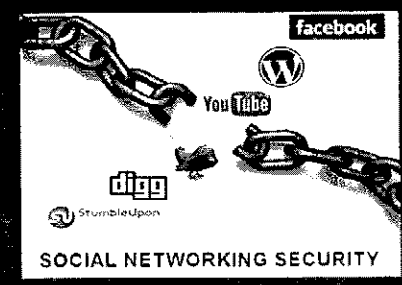
Platinum Sponsored

Organized by

www.snsconference.com



“SNSCON 2010 เป็นงานสัมมนาแรกของประเทศไทยด้านความมั่นคงปลอดภัยเครือข่ายสังคมออนไลน์ ที่ประสบความสำเร็จอย่างสูงในปี 2010 และสำหรับปี 2011 นี้ คณะผู้จัดงานฯภูมิใจนำเสนอ SNSCON 2011 โดยมีหัวข้อและเนื้อหาการสัมมนาซึ่งเป็นการต่อยอดองค์ความรู้มาจากงาน SNSCON 2010 โดยถือได้ว่า SNSCON 2011 เป็นงานสัมมนาภาคสองที่มีเนื้อหาทางด้านวิชาการที่เข้มข้นมากขึ้นและมีกรณีศึกษาที่ทันยุคทันสมัยจากผู้บริหารระดับสูงขององค์กรขนาดใหญ่ในประเทศไทยที่เกี่ยวกับความมั่นคงปลอดภัยเครือข่ายสังคมออนไลน์โดยเฉพาะ”



เครือข่ายสังคมออนไลน์ (Social Network)

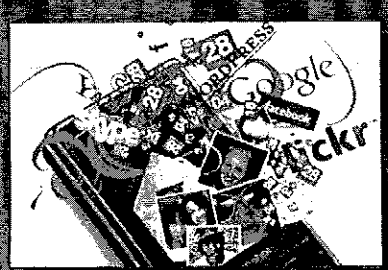
แม้จะมีคุณประโยชน์หลากหลายเพียงใดแต่ก็ยังคงมีโทษมากมายเช่นกัน หากเราใช้อย่างไม่รู้เท่าทันเหล่าอาชญากรไซเบอร์ เพราะผู้ไม่หวังดีสามารถใช้เครือข่ายสังคมออนไลน์เป็นที่แพร่กระจายของโปรแกรมมุ่งร้าย (MalWare) อาจสร้างความเสียหายให้กับตัวเราและองค์กร หากเราไม่มีความรู้เท่าทันที่จะระวังตัวและรู้วิธีป้องกันภัยคุกคามได้อย่างถูกต้องและเพียงพอในการใช้งานเครือข่ายสังคมออนไลน์ โดยข้อมูลส่วนตัวของเรา เช่น ชื่อ ที่อยู่ เบอร์โทรศัพท์และข้อมูลอื่น ๆ อาจจะไม่เป็นข้อมูลส่วนตัวอีกต่อไป จึงมีความจำเป็นอย่างยิ่งยวดที่เราควรจะรู้ว่าอะไรคือกลโกงหรือหลุมพลางในการใช้งานเครือข่ายสังคมออนไลน์วันนี้และอนาคตอันใกล้ที่ต้องพึงระวัง

ถึงเวลาแล้วหรือยัง

ที่เราจะต้องหันมาให้ความสนใจกับเรื่องการใช้งานเครือข่ายสังคมออนไลน์อย่างไรให้มีความมั่นคงปลอดภัยและปรับความคิดเสียใหม่ว่า เรื่องความมั่นคงปลอดภัยในการใช้งานเครือข่ายสังคมออนไลน์เป็นสิ่งจำเป็นที่ต้องรู้และทำความเข้าใจ ไม่ว่าจะเป็นการใช้งานส่วนตัวหรือการใช้งานในระดับองค์กรเราต้องรู้เท่าทันเล่ห์เหลี่ยมและกลโกงของเหล่ามิจฉาชีพ ซึ่งสามารถ Up-Trend รับชมและรับฟังได้จากวิทยากรรับเชิญและทีมวิทยากรผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยโดยเฉพาะในงานสัมมนา SNSCON 2011 เปิดรับโอกาสใหม่บนโลกสังคมออนไลน์อย่างมั่นใจได้ที่งาน SNSCON 2011 วันที่ 28 มิถุนายน 2554 โรงแรมแกรนด์ มิลเลนเนียม สุขุมวิท

5 เหตุผลที่ต้องเข้าฟังสัมมนา SNSCON2011 และ MOBISCON 2011 ในครั้งนี้

1. รับฟังวิสัยทัศน์และ Update Trend ล่าสุด จาก Security Guru ชั้นนำของเมืองไทย
2. รู้เท่าทัน เล่ห์เหลี่ยม และกลโกง ของเหล่ามิจฉาชีพ พร้อมรู้วิธีป้องกันภัยคุกคามได้อย่างถูกต้อง
3. เรียนรู้เทคนิคขั้นสูง ทำอย่างไรจะไม่ให้ตกเป็นเหยื่อ ผ่านการสาธิต “Live Hacking Demonstration”
4. สัมผัสประสบการณ์จริงในการถูกดักข้อมูลส่วนตัว “Live, Real-Time and Interactive – Get Hacked Experience Workshop”
5. รับ Best Practice สำหรับการป้องกันข้อมูลส่วนตัวของตนเองและองค์กรในการใช้ Social Network และ Smartphone อย่างได้ผล



“MOBISCON 2011 เป็นงานสัมมนาแรกของประเทศไทยด้านความมั่นคงปลอดภัยในการใช้งานสมาร์ทโฟนและอุปกรณ์สื่อสารไร้สายทั้งการใช้ส่วนตัวและใช้ในองค์กรให้รู้เท่าทันภัยร้ายยุคใหม่และมุมมองการป้องกันให้รอดพ้นปลอดภัยไม่ตกเป็นเหยื่อจากไลฟ์สไตล์ของตัวเราเอง ซึ่งผู้เข้าร่วมงานสัมมนาจะได้รับ Toolkit: Mobile Computing/Social Networking Security Policy Template จากงานวิจัยของสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA) เพื่อการบริหารจัดการด้านความมั่นคงปลอดภัยในการใช้งานโทรศัพท์สมาร์ทโฟนและอุปกรณ์สื่อสารไร้สายในองค์กรและรับฟรีหนังสือ รู้รอดปลอดภัยเมื่อใช้ Facebook/Twitter”

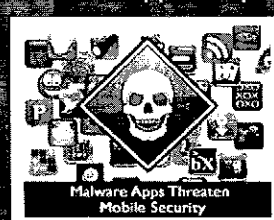
มหันตภัย “สมาร์ทโฟน” ยิ่งสมาร์ท...ยิ่งอันตราย

เป็นคำกล่าวที่ดูจะไม่ไกลเกินความเป็นจริงในปัจจุบันเพราะโทรศัพท์มือถือประเภทสมาร์ทโฟนแม้จะช่วยอำนวยความสะดวกให้เราได้มากเพียงใดแต่ก็มีภัยร้ายที่แอบแฝงมาด้วยจากความสามารถที่เพิ่มขึ้นทุกวันของสมาร์ทโฟนรุ่นใหม่ ๆ จากการใช้งานที่รู้เท่าไม่ถึงการณ์ อาจสร้างความเดือดร้อนให้กับความเป็นส่วนตัวของเราและอาจก่อให้เกิดความเสียหายในระดับองค์กรอีกด้วย สาเหตุที่ “สมาร์ทโฟน” ได้รับความนิยมเนื่องจากผู้ใช้สามารถออนไลน์ได้ทุกที่ทุกเวลาผ่านเครือข่าย EDGE, Wi-Fi และ 3G และสามารถใช้งานเครือข่ายสังคมออนไลน์ แชร์รูปภาพให้กับเพื่อนๆ และท่องเว็บไซต์..กราบหรือไม่ว่าในปัจจุบันเหล่ามิจฉาชีพหันมาเจาะระบบบุกรุกเครือข่ายขององค์กรผ่านทางสมาร์ทโฟน..รู้หรือไม่ว่ามีภัยคุกคามที่จะเกิดขึ้นหลังจากที่เราทำ Jailbreak กับโทรศัพท์ iPhone รวมทั้ง เราอาจถูกขโมยเงินออกจากบัญชีเพียงแค่เราใช้ Free Wi-Fi เมื่อใช้งานอินเทอร์เน็ตผ่านสมาร์ทโฟน

คุ้มค่าหรือไม่

ที่เราต้องจ่ายค่าเครื่องโทรศัพท์ราคาค่อนข้างสูงแล้วยังต้องเสียรู้และเสียเงินเพราะความไม่รู้เท่าทันภัย ถึงเวลาแล้วหรือยังที่คุณจะต้องให้ความสนใจกับการใช้งานโทรศัพท์มือถือสมาร์ทโฟนทั้งด้านบวกและลบ ป้องกันข้อมูลส่วนตัวบนโทรศัพท์มือถือ

รู้เท่าทันเล่ห์เหลี่ยมของเหล่ามิจฉาชีพจากวิทยากรผู้เชี่ยวชาญในงาน MOBISCON 2011 วันที่ 29 มิถุนายน 2554 ณ โรงแรมแกรนด์ มิลเลนเนียม สุขุมวิท กรุงเทพฯ



S1 SNSCON @WORKSHOP #1

Social Networking Security Policy and Technics for Securing Your Corporate

ระยะเวลา 1 วัน | รุ่นที่ 1 : 4 ก.ค. | รุ่นที่ 2 : 11 ก.ค.

หลักสูตรภาคปฏิบัติทางด้านเทคนิคและการพัฒนานโยบายด้าน Social Networking Security สำหรับองค์กร

เครือข่ายสังคมออนไลน์ (Social Network) ถึงแม้จะมีคุณประโยชน์หลากหลายเพียงใด แต่ก็มีมุมมืดบางมายเช่นกัน หากเราใช้อย่างไม่รู้เท่าทันแล้วอาชญากรไซเบอร์ เพราะเหล่ามิจฉาชีพและผู้ไม่หวังดีสามารถใช้เครือข่ายสังคมออนไลน์เป็นสื่อแพร่กระจายของโปรแกรมมุ่งร้าย (MalWare) ที่อาจสร้างความเสียหายให้กับองค์กรของเรา ซึ่งหากผู้ควบคุมดูแลระบบไม่มีความรู้เท่าทันที่จะระวังตัวหรือรู้วิธีป้องกันภัยคุกคามได้อย่างถูกต้องเพียงพอในการใช้งานเครือข่ายสังคมออนไลน์ โดยข้อมูลที่สำคัญขององค์กร เช่น ข้อมูลรายชื่อลูกค้า ข้อมูลทางการเงิน อาจจะไม่เป็นข้อมูลส่วนตัวอีกต่อไป จึงมีความจำเป็นอย่างยิ่งยวดที่บุคลากรในองค์กรควรตระหนักและควรจะรู้ว่า อะไรคือกลไก ในการใช้งานเครือข่ายสังคมออนไลน์วันนี้และอนาคตอันใกล้ที่ต้องพึงระวัง

สำหรับในองค์กร การห้ามใช้งานอาจไม่ใช่ทางออกที่ดีที่สุด วิธีใดเหมาะกับองค์กรของท่าน สามารถหาคำตอบและวิธีการป้องกันภัยจากการใช้เครือข่ายสังคมออนไลน์ได้จากเข้ารับการอบรมหลักสูตรภาคปฏิบัติ SNSCON @Workshop #1 ที่ได้รับการออกแบบมาสำหรับผู้บริหารและผู้ดูแลระบบในองค์กรได้เรียนรู้เทคนิคต่างๆ ในการป้องกันภัยที่อาจเกิดขึ้นจากการใช้งานเครือข่ายสังคมออนไลน์ในระดับองค์กร โดยมีเนื้อหาหลักสูตรดังต่อไปนี้

เนื้อหาที่น่าสนใจ

- The Latest Update สถานการณ์ล่าสุดการใช้งานเครือข่ายสังคมออนไลน์ในประเทศไทยและทั่วโลก
- รู้เท่าทันภัยมืดใหม่ๆ ที่แฝงมากับการใช้งานเครือข่ายสังคมออนไลน์ และกำลังคุกคามองค์กร
- เทคนิคใหม่ล่าสุดในการขโมยชื่อผู้ใช้และรหัสผ่าน Facebook/Twitter ด้วย SSLStrip Toolkit
- "ห้ามใช้" หรือ "ให้ใช้แต่ควบคุม" ทางออกที่ดีที่สุดขององค์กรคืออะไร?
- กำไม? ต้องมีนโยบายควบคุมการใช้งานเครือข่ายสังคมออนไลน์ภายในองค์กร
- "รูปแบบ" ของนโยบายควบคุมการใช้งานเครือข่ายสังคมออนไลน์ภายในองค์กรเป็นอย่างไร?
- เทคนิคการเขียนนโยบายควบคุมการใช้งานเครือข่ายสังคมออนไลน์ในองค์กร และต้นแบบแนวนโยบายฯ Security Policy Template
- "ถ้าผู้ใช้ไม่ตระหนักก็ไม่ให้ความร่วมมือ" จึงจำเป็นต้องรู้วิธีการสร้างความตระหนักในการใช้งานสังคมออนไลน์ซึ่งเป็นเรื่องสำคัญที่ผู้บริหารองค์กรจะมองข้ามไม่ได้
- การควบคุมการใช้งานเครือข่ายสังคมออนไลน์ด้วยเทคโนโลยีสมัยใหม่โดยไม่กระทบกับการทำงานของผู้ใช้งาน
- การตรวจสอบการใช้งานสื่อเครือข่ายสังคมออนไลน์ในองค์กร เรื่องบางเรื่องในองค์กรที่คุณไม่เคยรู้
- "เกิดเหตุแล้วใครรับผิดชอบ?" Update ร่าง พรบ. การกระทำผิดเกี่ยวกับคอมพิวเตอร์ ฉบับล่าสุด และประเด็นกฎหมายที่เกี่ยวข้องกับการใช้งานสื่อเครือข่ายสังคมออนไลน์ที่ผู้บริหารต้องรู้

SNSCON @WORKSHOP #2

Learning Social Networking Security for Protecting Yourself from Today Social Networking Threats

ระยะเวลา 1 วัน | รุ่นที่ 1 : 5 ก.ค. | รุ่นที่ 2 : 12 ก.ค.

หลักสูตรภาคปฏิบัติเพื่อเรียนรู้ภัยคุกคามและวิธีการป้องกันตนเองในการใช้เครือข่ายสังคมออนไลน์สำหรับผู้ใช้งานทั่วไป

เราคงจะปฏิเสธไม่ได้ว่าเครือข่ายสังคมออนไลน์หรือ Social Network ไม่ว่าจะเป็น Facebook หรือ Twitter รวมทั้ง YouTube, Multiply, Linkedin หรือ MySpace กำลังเป็นที่นิยมใช้กันอย่างมากในเวลานี้ ทั้งที่เพื่อใช้ทั้งเรื่องบันเทิง หรือ ใช้เพื่อการทำงานหรือการศึกษาหาข้อมูล จนทำให้ Social Network กลายเป็นชุมชนบนโลกออนไลน์ที่หากนับรวมกันแล้ว คาดว่ามีประชากรใน Social Network ทั้งหมดไม่น่าจะต่ำกว่า 1,000 ล้านคน (as of 31 March 2011)

เป็นเรื่องปกติที่ทุกสังคมย่อมมีทั้งคนดีและคนไม่ดี สังคมออนไลน์ก็เป็นเช่นนั้นเหมือนกัน มีคนจำนวนไม่มากนักที่รู้ว่าสังคมออนไลน์กลายเป็นสังคมเปิดที่เต็มไปด้วยภัยคุกคามในรูปแบบใหม่ที่หลายคนอาจจะเคยโดนหรือไม่เคยโดนหรืออาจจะเคยโดนแต่ไม่รู้ตัว จนทำให้บางคนต้องสูญเสียข้อมูล เสียทรัพย์ เสียชื่อเสียงหรืออาจเสียชีวิตเพราะการใช้งานสื่อเครือข่ายสังคมออนไลน์กันไปได้

หลักสูตรภาคปฏิบัติ SNSCON @Workshop #2 ได้รับการออกแบบมาสำหรับผู้ใช้งาน Social Network และผู้สนใจทั่วไปในการเรียนรู้ภัยคุกคามในรูปแบบต่างๆ ที่แฝงตัวมากับโปรแกรมประเภท Social Network เพื่อเป็นการป้องกันตนเองและครอบครัวจากภัยบนเครือข่ายสังคมออนไลน์

เนื้อหาที่น่าสนใจ

- หลอกว่ามาดี แต่จริงๆมาร้าย : Social Engineering Attack on Social Network (Fake Game/Fake Anti-Virus/Malicious Facebook Application)
- ล่อเหยื่อตกปลาออนไลน์ : Phishing Attack
- โค้ดร้ายฝังลึก : Cross Site Scripting Attack (XSS Attack)
- ถูกสวมรอยกันง่ายๆ เพียงเล่น Facebook อย่างไม่ระมัดระวัง : Cross Site Request Forgery Attack (CSRF Attack)
- หลอกให้คลิกแต่แอบซ่อนมีดไว้รอเชือด : Clickjacking or UI redressing Attack
- เล่น Facebook เพลินๆ กดไปกดมาระวังโดนหลอกล่อให้ไปเจอ Link ของผู้ไม่ประสงค์ดีเปิดรออยู่ : Drive-by Download Attack
- เทคนิคการจารกรรมข้อมูลขั้นสูงแบบต่อเนื่อง : APT (Advanced Persistent Threats) and MitB (Man-In-The-Browser Attack)
- ระวังโดนดักข้อมูลลับระหว่างทาง (เสร็จโจร) : Identity Theft (Man-in-The-Middle Attack) (SSL attack or Session Hijacking)
- บอกเพื่อนว่าเราอยู่ไหน (บอกโจรด้วยว่าเราไม่อยู่บ้าน) : GPS Location Exposed
- ระวังข้อมูลส่วนตัวหลุดรั่วขณะเล่น Facebook เพลินๆ : Privacy Exposed

S2

M1 MOBISCON @WORKSHOP #1

Smartphone and Media Tablets Security Policy and Technics for Securing Your Corporate

ระยะเวลา 1 วัน | รุ่นที่ 1 : 6 ก.ค. | รุ่นที่ 2 : 13 ก.ค.

หลักสูตรภาคปฏิบัติทางด้านเทคนิคและการพัฒนานโยบายด้าน Smartphone and Media Tablets Security สำหรับองค์กร

มหันตภัย "สมาร์ทโฟน" ยิ่งสมาร์ท ยิ่งอันตราย เป็นคำกล่าวที่ดูจะไม่ใกล้เกินความเป็นจริงในปัจจุบัน เพราะโทรศัพท์มือถือประเภทสมาร์ทโฟน แม้จะช่วยอำนวยความสะดวกให้เราได้มากเพียงใด แต่ก็มีภัยร้ายที่แอบแฝงมาด้วยจากความสามารถที่เพิ่มขึ้นทุกวันของสมาร์ทโฟนรุ่นใหม่ ๆ จากการใช้งานที่รู้เท่าไม่ถึงการณ์ อาจสร้างความเดือดร้อนให้กับความเป็นส่วนตัว และอาจก่อให้เกิดความเสียหายในระดับองค์กรอีกด้วย

สำหรับในองค์กรแล้ว...การห้ามใช้งาน Smartphone และ Media Tablets คงเป็นไปไม่ได้ แต่มีวิธีใดบ้างที่เหมาะกับองค์กรของท่าน สามารถหาคำตอบและวิธีการป้องกันภัยจากการใช้งานอุปกรณ์พกพาประเภท Smartphone และ Media Tablets ได้โดยเข้าร่วมการอบรมหลักสูตรภาคปฏิบัติ MOBISCON @Workshop #1 ที่ได้รับการออกแบบมา ให้กับผู้บริหาร นักพัฒนาแอพพลิเคชั่น และผู้ดูแลระบบในองค์กรได้เรียนรู้เทคนิคต่างๆ ในการป้องกันภัยที่อาจเกิดขึ้นจากการใช้ Smartphone และ Media Tablets ทั้งภายในและภายนอกองค์กร โดยมีเนื้อหาหลักสูตรดังต่อไปนี้

เนื้อหาที่น่าสนใจ

- The Latest Update กระแสสถานการณ์ล่าสุดการใช้งาน Smartphone/Media Tablets ในประเทศไทยและทั่วโลก
- รู้เท่าทันภัยมืดใหม่ๆ ที่แฝงตัวมากับการใช้งาน Smartphone/Media Tablets และกำลังคุกคามองค์กรโดยที่เราไม่รู้ตัว เช่น iPhone สามารถแปลงกายเป็น Personal Hotspot ในองค์กรโดยไม่ได้รับอนุญาต
- จุดอ่อนของแอพพลิเคชั่นบน Smartphone/Media Tablets ที่ผู้บริหาร และ นักพัฒนา Application ต้องรู้
- Smartphone/Media Tablets ใช้ในองค์กรได้แต่ต้องมีการควบคุม
- ผู้บริหารควรทำอย่างไรจึงจะ Balance ระหว่าง ความสะดวกสบายในการใช้งานของผู้ใช้กับเสถียรภาพและความมั่นคงปลอดภัยขององค์กร?
- นโยบายควบคุมการใช้งาน Smartphone/Media Tablets ที่ทุกองค์กรถามถึงเป็นอย่างไร?
- เทคนิคการเขียนนโยบายควบคุมการใช้งาน Smartphone/Media Tablets ในองค์กร พร้อม Security Policy Template สำหรับเป็นต้นแบบสำหรับเป็นต้นแบบในการเขียนนโยบาย
- "ถ้าผู้ใช้ไม่ตระหนักก็ไม่ให้ความร่วมมือ" จึงจำเป็นต้องรู้วิธีการสร้างความตระหนักในการใช้งาน Smartphone/Media Tablets ซึ่งเป็นเรื่องสำคัญที่ผู้บริหารองค์กรจะมองข้ามไม่ได้
- "ไม่ตระหนักก็ไม่ร่วมมือ" สร้างความตระหนักในการใช้งาน
- เทคนิคการควบคุมและตรวจสอบการใช้งาน Smartphone/Media Tablets ด้วยเทคโนโลยีสมัยใหม่ที่เราจำเป็นต้องรู้วันนี้

MOBISCON @WORKSHOP #2

Learning Smartphone and Media Tablets Security for Protecting Yourself from Today Mobile Computing Threats

ระยะเวลา 1 วัน | รุ่นที่ 1 : 7 ก.ค. | รุ่นที่ 2 : 14 ก.ค.

หลักสูตรภาคปฏิบัติเพื่อเรียนรู้ภัยคุกคามและวิธีการป้องกันตนเองในการใช้สมาร์ทโฟนสำหรับผู้ใช้งานทั่วไป

คงปฏิเสธไม่ได้ว่าคนไทยมีโทรศัพท์มือถือเป็นอุปกรณ์ข้างกายแทบทุกคน งานกลายเป็นอุปกรณ์ที่ขาดไม่ได้แล้วในชีวิตประจำวัน เพราะนอกจากจะใช้โทรศัพท์มือถือในการติดต่อประสานงานหรือใช้เพื่อติดต่อคนในครอบครัว หรือเพื่อนฝูงเหมือนเช่นในอดีตแล้ว แต่ด้วยคุณสมบัติโทรศัพท์มือถือรุ่นใหม่ๆ หรือที่เราเรียกว่าสมาร์ทโฟนนั้นมีความสามารถเทียบเคียงได้กับเครื่องคอมพิวเตอร์ ทำให้สามารถใช้งานได้อย่างรวดเร็วและเก็บบันทึกข้อมูลได้จำนวนมาก จึงสามารถนำไปใช้ประโยชน์ได้อย่างมากมาย

การที่จำนวนผู้ใช้งานโทรศัพท์มือถือมีจำนวนมากขึ้นนั้น อาจเป็นผลมาจากการที่ผู้ผลิตได้มีการพัฒนาเทคโนโลยีและแอพพลิเคชั่นประเภทต่างๆออกมามากมายเพื่ออำนวยความสะดวกให้แก่ผู้ใช้งาน ซึ่งหากมองในมุมของผู้ใช้งานแล้วย่อมเป็นเรื่องดีที่มีแอพพลิเคชั่นให้เลือกใช้จำนวนมาก แต่หารู้ไม่ว่าแอพพลิเคชั่นเหล่านั้นอาจนำภัยมาสู่ตัวท่านเหมือนกับพาโจรเข้ามาอยู่ในกระเป๋ากางเกงหรือกระเป๋าถือของคุณก็เดียว เนื่องจากพฤติกรรมการโหลดแอพพลิเคชั่นโดยไม่ระมัดระวังของผู้ใช้งานทั่วไป จึงทำให้ผู้ไม่ประสงค์ดีใช้เป็นช่องทางในการกระจายโปรแกรมนักสืบ (Spyware) โดยแฝงโปรแกรมเหล่านี้มากับโปรแกรมที่เราโหลดจากอินเตอร์เน็ต หรือส่งมาหลอกล่อให้เราเปิดผ่านทางอีเมล์หรือ Bluetooth ซึ่งหากโทรศัพท์มือถือของเราติดโปรแกรมนักสืบเหล่านั้นแล้วก็จะทำให้โทรศัพท์มือถือของเราไม่ได้เป็นของเราคนเดียวอีกต่อไป

ดังนั้นเราจึงควรเรียนรู้ภัยคุกคามรูปแบบต่างๆ ที่แฝงตัวมาจากการใช้งานอุปกรณ์พกพาทั้งโทรศัพท์มือถือและอุปกรณ์แท็บเล็ต โดยหลักสูตรภาคปฏิบัติ MOBISCON @Workshop #2 ที่ได้รับการออกแบบมาสำหรับการเรียนรู้รูปแบบของภัยคุกคามใหม่ๆ และวิธีการป้องกันตนเองและครอบครัวจากภัยที่อาจเกิดขึ้นจากการใช้อุปกรณ์พกพา โดยมีเนื้อหาหลักสูตรดังต่อไปนี้

เนื้อหาที่น่าสนใจ

- ภัยร้ายจากการใช้ iPhone, Blackberry, Android, Symbian และ iPad
- หลอกว่ามาดี แต่จริงๆมาร้าย : Social Engineering Attack on Mobile (Fake Game/Fake Anti-Virus/Malicious Facebook Application)
- เล่นมือถือเพลินๆ กดไปกดมาระวังโดนหลอกล่อให้ไปเจอ Link ของผู้ไม่ประสงค์ดีเปิดรออยู่ : Drive-by Download Attack
- บอกเพื่อนว่าเราอยู่ไหน (บอกโจรด้วยนะว่าเราไม่อยู่บ้าน) : Mobile GPS Location Exposed
- ล่อเหยื่อตกปลาบนมือถือเนียนสุดๆ : Phishing Attack (using URL Shorten Technics or sending fake email)
- จะเกิดอะไรขึ้นเมื่อ Hacker มายึดเครื่อง : Mobile Trojan
- ใช้ Net ฟรีระวังโดนดักข้อมูลลับ : Identity Theft
- ไวรัสบนมือถือมีจริงหรือไม่ ป้องกันอย่างไร : Mobile Antivirus

M2

SNSCON 2011 Registration Form แบบฟอร์มการลงทะเบียนเข้าร่วมสัมมนา MOBiCON

รายละเอียดผู้เข้าอบรมสัมมนา

ประเภทหน่วยงาน ☐ หน่วยงานรัฐ ☐ รัฐวิสาหกิจ ☐ เอกชน ☐ บุคคล ☐ อื่นๆ ระบุ ....

ชื่อผู้ลงทะเบียน .... นามสกุล .... ตำแหน่งงาน ....

แผนก/กอง/ศูนย์ .... ฝ่าย/กรม/สำนัก ....

กระทรวง/บริษัท/หน่วยงาน/สถาบัน ....

ที่อยู่ เลขที่ .... หมู่ที่ .... อาคาร/หมู่บ้าน .... ชั้น .... ห้อง ....

ตรอก/ซอย .... ถนน .... แขวง/ตำบล ....

เขต/อำเภอ .... จังหวัด .... รหัสไปรษณีย์ ....

โทรศัพท์ .... โทรสาร .... มือถือ .... อีเมล์ ....

ชื่อผู้ประสานงาน .... โทรศัพท์ ....

ต้องการออกใบเสร็จในนาม ☐ บุคคล ☐ องค์กร * กรณีที่อยู่ในการออกใบเสร็จรับเงิน ไม่ตรงกับรายละเอียดผู้เข้าสัมมนา กรุณากรอกข้อมูลด้านล่าง

....

....

ค่าธรรมเนียมการสมัคร

สัมมนา - Conference (28-29 มิถุนายน 2554) Ⓒ	สมัคร 1 ท่าน (ราคาปกติ)	สมัคร 3 ท่านขึ้นไป (ราคาพิเศษ/ท่าน)	สมัคร 5 ท่านขึ้นไป (ราคาพิเศษ/ท่าน)
ค่าธรรมเนียมการสมัคร (2 วัน)	8,900.00	8,500.00	7,500.00
ภาษีมูลค่าเพิ่ม 7%	623.00	595.00	525.00
รวมจำนวนเงิน	9,523.00	9,095.00	8,025.00

ภาคปฏิบัติ - Workshop S1 S2 M1 M2	สมัคร 1 ท่าน (ราคาปกติ)	สมัคร 3 ท่านขึ้นไป (ราคาพิเศษ/ท่าน)	สมัคร 5 ท่านขึ้นไป (ราคาพิเศษ/ท่าน)
ค่าธรรมเนียมการสมัคร (1 วัน)	3,900.00	3,500.00	2,500.00
ภาษีมูลค่าเพิ่ม 7%	273.00	245.00	175.00
รวมจำนวนเงิน	4,173.00	3,745.00	2,675.00

กรุณาเลือกประเภทการลงทะเบียน

รูปแบบการสมัคร ☐ สมัคร 1 ท่าน ☐ สมัคร 3 ท่านขึ้นไป ☐ สมัคร 5 ท่านขึ้นไป

Ⓒ สัมมนา (SNSCON2011 + MOBISCON2011) ☐ 28-29 มิถุนายน 2554

S1 ภาคปฏิบัติ SNSCON@1 (1 วัน) ☐ 4 ก.ค. 54 ☐ 11 ก.ค. 54

S2 ภาคปฏิบัติ SNSCON@2 (1 วัน) ☐ 5 ก.ค. 54 ☐ 12 ก.ค. 54

M1 ภาคปฏิบัติ MOBISCON@1 (1 วัน) ☐ 6 ก.ค. 54 ☐ 13 ก.ค. 54

M2 ภาคปฏิบัติ MOBISCON@2 (1 วัน) ☐ 7 ก.ค. 54 ☐ 14 ก.ค. 54

ส่วนลด

ต่อที่ 1 ลงทะเบียน สัมมนา 2 วัน	ต่อที่ 2 ลงทะเบียน สัมมนา + ปฏิบัติ	
รับส่วนลด **10%**	+ ลด **5%** ลงปฏิบัติเพิ่ม 1-2 หัวข้อ	+ ลด **10%** ลงปฏิบัติเพิ่ม 3-4 หัวข้อ

ส่วนลดดังกล่าวจะได้รับสิทธิ์เมื่อชำระค่าลงทะเบียนภายในวันที่ 6 มิถุนายน 2554

- ส่วนลดนี้สำหรับหน่วยงานเดียวกันเท่านั้น ให้สิทธิ์ต่อท่านไม่สามารถนำส่วนลดมารวมกันได้
- ผู้เข้าสัมมนาที่เคยลงทะเบียนในงานสัมมนาครั้งที่ผ่านมา รับส่วนลดเพิ่ม 10% (เฉพาะบุคคล)
- ผู้เข้าสัมมนาที่ลงทะเบียนปฏิบัติอย่างเดียวไม่ได้รับส่วนลดในส่วนสัมมนา 10%
- นักศึกษาระดับปริญญาตรี หรือระดับต่ำกว่า รับส่วนลดเพิ่ม 10%
- เพื่อความสะดวกในการลงทะเบียนโปรดชำระเงินก่อนวันงาน และงดการชำระเงินหน้างาน
- สิ้นสุดการรับลงทะเบียนและชำระค่าลงทะเบียน ภายในวันที่ 24 มิถุนายน 2554
- คูปองส่วนลดอื่นๆ ไม่สามารถนำมาใช้ร่วมกับส่วนลดดังกล่าวได้

วิธีการลงทะเบียน

1. กรอก "แบบฟอร์ม" (Registration Form) แล้วแฟกซ์มาที่ 0-2650-5776
2. ลงทะเบียนใน "ระบบอินเทอร์เน็ต" ได้ที่ www.snsconference.com
3. ติดต่อ โทรศัพท์ 02-650-5771 คุณลัดดา (ต่อ 108) , คุณวราพงศ์ (ต่อ 107)

วิธีการชำระเงิน

1 โดยการโอนเข้าบัญชี

ส่งเอกสารการลงทะเบียนพร้อมหลักฐานการโอนเงินโดยระบุชื่อผู้เข้าอบรม และสำเนาใบหักภาษี ณ ที่จ่าย (ถ้ามี) มาที่โทรสารหมายเลข 0-2650-5776 หรือ สแกนหลักฐานการโอนเงินมาที่ registration@snsconference.com

2 โดยการสั่งจ่ายเช็ค

นำส่งเช็คพร้อมใบหักภาษี ณ ที่จ่าย (ถ้ามี) มาที่ บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด

โอนเงินเข้าบัญชี/สั่งจ่ายเช็คในนาม

บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด

ธนาคารกรุงไทย สาขาการไฟฟ้านครหลวงเพลินจิต
เลขที่บัญชีกระแสรายวัน 092-6-00379-8

ธนาคารกสิกรไทย สาขาถนนหลังสวน
เลขที่บัญชีกระแสรายวัน 082-1-09135-7

สำหรับหน่วยงานที่ต้องการหักภาษี ณ ที่จ่าย กรุณาหักภาษีในนาม

บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด

เลขประจำตัวผู้เสียภาษี 3 0 3 0 8 4 5 2 4 5
2101 ชั้น 21 เลขที่ 62 อาคารเดอะมิลเลนเนีย
ถ.หลังสวน ลุมพินี ปทุมวัน กรุงเทพฯ 10330

CONFERENCE DESCRIPTION

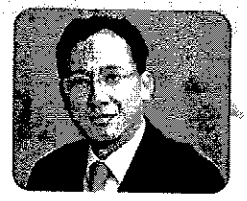
จากความสนใจ ของผู้เข้าร่วมงานสัมมนา Social Networking Security Conference 2010 ครั้งที่ 1 ซึ่งเป็นงานด้านความมั่นคงปลอดภัยสำหรับเครือข่ายสังคมออนไลน์งานแรกของโลกที่จัดขึ้นในประเทศไทย ได้ประสบความสำเร็จเกินความคาดหมายด้วยความร่วมมือทั้งหน่วยงานภาครัฐและเอกชน ตามที่มีเสียงเรียกร้องของผู้ร่วมงานและผู้ที่พลาดการสัมมนาในครั้งที่แล้วจึงทำให้เกิด Social Networking Security Conference 2011 (SNSCON 2011) ปีที่ 2 ในครั้งนี้ที่จัดขึ้นแบบ Dual Conference มาพร้อมกับงาน Mobile Computing Security Conference 2011 (MOBISCON 2011) ที่จัดขึ้นเป็นครั้งแรกในประเทศไทย

พิเศษสุด สำหรับการจัดสัมมนาในปีนี้ ทางคณะผู้จัดฯ จะนำเสนอในรูปแบบ Interactive Conference ซึ่งจะทำให้ทุกท่านได้ลงมือปฏิบัติจริงด้วยตัวท่านเอง ร่วมกับการฟังบรรยายการ Update ประโยชน์และภัยคุกคามจากการใช้งาน Social Network ที่กำลังมาแรงควบคู่กับเทคโนโลยีอันทันสมัยอย่าง Smartphone ที่ยิ่งสมาร์ทก็ยิ่งอันตราย ที่จะทำให้ทุกท่านได้รับความรู้อย่างเต็มอิ่มกับเนื้อหาสาระและเทคนิคดีๆ ที่ทีมงานทุกคนใช้เวลารวบรวมข้อมูลจากทั่วโลก รวมทั้งมุมมองและข้อคิดเห็นจากวิทยากรผู้ทรงคุณวุฒิทั้งในและต่างประเทศ พร้อมสัมผัสกับผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยจากสมาร์ทโฟนยักษ์ใหญ่ BlackBerry ตัวจริง เสียงจริงที่จะมาไขข้อข้องใจเรื่องความปลอดภัยที่เป็นประเด็นที่เกิดขึ้นทั่วโลกพร้อมทั้งอนาคตของเทคโนโลยีโทรศัพท์สมาร์ทโฟนให้ทุกท่านได้รับทราบใน SNSCON 2011 & MOBISCON 2011 งานนี้

ดร.รอม หิรัญพฤกษ์

นายกสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ
Thailand Information Security Association (TISA)

การใช้งานเครือข่ายสังคมออนไลน์ Social Network ขยายตัวอย่างรวดเร็ว จำนวนผู้ใช้ Facebook ทั่วโลกมีมากกว่า 620 ล้านคน รวมกันเทียบเท่าประเทศที่มีประชากรมากเป็นอันดับสามของโลก ในประเทศไทยมีผู้ใช้ Facebook มากกว่า 8 ล้านคน รวมถึงการเติบโตในการใช้งาน Smartphone ซึ่งผู้ใช้สามารถเข้าร่วมเป็นส่วนหนึ่งของเครือข่ายสังคมออนไลน์ได้ทุกที่ทุกเวลา เกิดการสร้างกลุ่มสังคมต่างๆ มากมายบนโลกออนไลน์ ความสมดุลของการรักษาข้อมูลความเป็นส่วนตัว (Privacy) พร้อมกับการ ใช้งานอย่างปลอดภัย (Security) เพื่อป้องกันความเสี่ยงจากภัยสมัยใหม่ (New Risk from New Threats) ที่เกิดขึ้นตามความก้าวหน้าของเทคโนโลยี จึงเป็นประเด็นสำคัญที่ต้องให้ความรู้ความเข้าใจในการใช้งานทั้งเพื่อส่วนตัว และในระดับองค์กร ตลอดจนผู้ใช้ต้องเข้าใจทั้งคุณประโยชน์และโทษ ของการใช้งาน Social Network และ Smartphone เพื่อใช้เทคโนโลยีให้เกิดประโยชน์สูงสุด และขณะเดียวกันก็ต้องรู้วิธีป้องกันภัยร้ายต่าง ๆ ที่นับวัน จะอยู่ใกล้ๆ เพียงแค่ปลายนิ้ว



รศ.ดร.รนชาติ นุ่มนนท์

ผู้อำนวยการ
เขตอุตสาหกรรมซอฟต์แวร์ประเทศไทย
Software Park Thailand

กระแสของโลกาภิวัฒน์และเทคโนโลยีได้ทำให้รูปแบบของการทำงานของหน่วยงาน และบุคลากรในองค์กรเปลี่ยนแปลงไป การเข้ามาของ Social Networks ในชีวิต ประจำวันของผู้คนและการนำมาประยุกต์ในองค์กร ทำให้เห็นว่าอนาคตคือ ความร่วมมือทางสังคม (The Future is Social) การสัมมนาในครั้งนี้จะเป็นประโยชน์ที่จะช่วยทำให้เราเห็นพลังความร่วมมือดังกล่าวโดยการนำเทคโนโลยี Social Network มาใช้ในธุรกิจ และให้ตระหนัก ถึงความปลอดภัยของระบบ Social Network

อ.ปริญญา หอมเอนก

ประธานและผู้ก่อตั้ง
บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด
ACIS Professional Center

เป็นประจำทุกปีที่ผมได้มีโอกาสเข้าร่วมงานสัมมนาด้าน Information Security ที่ใหญ่ที่สุดในโลก "RSA Conference 2011" ที่กรุงซานฟรานซิสโก โดยหัวข้อเด่นๆของงานในปีนี้เน้นไปที่ประเด็นที่เกี่ยวข้องกับ "Social Network Security" และ "Mobile Computing Security" โดยเฉพาะ ซึ่งงานวิจัยของ Gartner เรื่อง "Top 10 Strategic Technologies" ก็พบว่ามีเรื่องที่เกี่ยวกับ Social Network อยู่ใน Top 10 ถึง 2 เรื่อง ได้แก่ "Social Analytics" และ "Social Communication and Collaboration" รวมถึงเรื่องที่เกี่ยวกับ Smartphone ในหัวข้อ "Mobile Applications and Media Tablets" จึงเป็นการบ่งชี้แนวโน้มว่าทั่วโลกกำลังให้ความสำคัญกับเรื่องนี้เป็นอย่างมาก

สำหรับประเทศไทยมีการเติบโตของผู้ใช้งาน Facebook แบบก้าวกระโดด จากปลายปีที่แล้วประมาณห้าล้านคน มาปัจจุบันเข้าใกล้ 9 ล้านคน ซึ่งองค์กร ส่วนใหญ่ เริ่มใช้ Social Network เป็นกลยุทธ์ด้านการตลาดที่สำคัญ ดังนั้น Social Network และ Smartphone จึงเปรียบเสมือนขุมทรัพย์ที่เต็มไปด้วยข้อมูลอันมีค่า จึงไม่แปลกที่เหล่ามิจฉาชีพจะหันมาพุ่งเป้าโจมตี Social Network และ Smartphone ของผู้ใช้งานส่วนตัวและองค์กรโดยอาศัยเทคนิคใหม่ๆ ในการแพร่กระจายโปรแกรมมุ่งร้าย ซึ่งสามารถสร้างความเสียหายให้กับผู้ใช้งานตลอดจนครอบครัวและองค์กร หากผู้ใช้งานยังขาดความตระหนัก (Security Awareness) และไม่มีความระมัดระวังที่จะป้องกันภัยคุกคามอย่างเพียงพอ อีกทั้งยังขาดความรู้ความเข้าใจในกลโกงของมิจฉาชีพที่แฝงมากับ Facebook, Twitter หรือ อาจถูกส่งมาในรูปแบบ SMS และ MMS ผ่านทาง Smartphone

ผมคิดว่าถึงเวลาแล้วที่เราจะต้อง "ตระหนัก" ให้ความสำคัญกับเรื่องความมั่นคงปลอดภัยในการใช้งานเครือข่ายสังคมออนไลน์ และ Smartphone ไม่ว่าจะเป็นการใช้งานส่วนตัวหรือการใช้งานในระดับองค์กร โดยเฉพาะภัยร้ายใหม่ๆ ที่แฝงมากับการใช้งาน เพื่อให้รู้เท่าทันเล่ห์เหลี่ยมของเหล่ามิจฉาชีพ และรู้วิธีการป้องกันเพื่อไม่ให้เราตกเป็นเหยื่ออาชญากรรม Hi-Tech ที่นับวันจะสลับซับซ้อนมากขึ้นทุกที และยังมุ่งเป้ามาที่ผู้ใช้ตามบ้าน พนักงานออฟฟิศทั่วไป รวมถึง Generation Y ที่ส่วนใหญ่ ยังเป็นวัยรุ่น ตลอดจนนิสิตนักศึกษา ซึ่งเป็นอนาคตของชาติก็อยู่ในกลุ่มเสี่ยงเช่นกัน

ผมจึงขอ "Recommend" อย่างยิ่งที่ทุกท่านไม่ควรพลาดงานสัมมนาดี ๆ เช่นนี้ครับ

Gartner

RSA 2011 CONFERENCE
FEBRUARY 14 18 | SAN FRANCISCO

facebook
@1Thailand

onference Agenda)

MOBI CON

MOBISCON 2011 — DAY 2 : 29th JUNE 2011

08:45-09:00 **M-01**

Welcome Note :

- The Future of Mobile Application and Media Tablets
  อนาคตของแอพพลิเคชั่นบนมือถือและมีเดียแท็บเล็ต
  - รศ.ดร.ธนชาติ นุ่มนนท์
    ผู้อำนวยการเขตอุตสาหกรรมซอฟต์แวร์ประเทศไทย (Software Park Thailand)

09:00-10:00 **M-02**

Keynote Address :

- New and Update : The Top Ten Mobile, Tablets and Ubiquitous Computing Security Threats
  Update ภัยคุกคาม 10 อันดับของโทรศัพท์มือถือ แท็บเล็ต และเทคโนโลยียูบิคควิทัสคอมพิวติ้ง
- Smartphone is a new PC
  จะเกิดอะไรขึ้นเมื่อ Smartphone กลายเป็น PC
  - อ.ปริญญา หอมเอนก
    ITIL V3 Expert, CFE, CGEIT, CISSP, CSSLP, CISA, CISM, SSCP, SANS GIAC GCFW, CBCI IRCA ISMS Lead Auditor, ITSMS and BCMS Provisional Auditor, CobiT Certified Trainer
    ประธานและผู้ก่อตั้ง บริษัท เอซิส โปรเฟสชันนัล เซ็นเตอร์ จำกัด (ACIS)
    กรรมการและเลขานุการ สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA)

10:00-10:45 **M-03**

Case Study :

- Security Challenges for Smartphones
  กรณีศึกษา ภัยคุกคามด้านความปลอดภัยสำหรับสมาร์ทโฟน
  - Mr. Marcus Klische
    BlackBerry Security Advisor, Research in Motion Deutschland GmbH

10:45-11:15 พักรับประทานอาหารว่าง (Coffee Break)

11:15-12:00 **M-04**

- How to Use Mobile Device Securely in Your Organization and How to Protect from Corporate Mobile Computing Security Threats
  ประสบการณ์จริงของการใช้งานสมาร์ทโฟนอย่างปลอดภัยภายในองค์กร
  ผู้บริหารสารสนเทศระดับสูงรับมืออย่างไร?
  - อ.กำพล ศรรษรัตน์
    ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ
    สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.)

12:00-13:30 พักรับประทานอาหารกลางวัน (Lunch Break)

13:30-14:00 **M-05**

TISA Research :

- Using Mobile Application and Media Tablets in Corporate, Mobile Computing/ Social Network Security Policy Template developed by TISA
  ต้นแบบนโยบายในการใช้งานสมาร์ทโฟนและมีเดียแท็บเล็ตในองค์กร
  โดยสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ
  - อ.ไชยกร อภิวัฒโนกุล CSSP, GCFA, IRCA ISMS
    Chief Executive Officer, S-GENERATION (aka QUANTIC)
    กรรมการ สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA)

14:00-14:30 **M-06**

Live Demonstration :

- Top 7 Smartphone Attacks/Threats and How to Protect (Part I)
  เทคนิคการโจมตีสมาร์ทโฟน 7 อันดับที่กำลังเป็นที่นิยมของแฮกเกอร์และพร้อมทั้งวิธีรับมือ
  - Advanced Trojan Horse Attack – โทรจันใน โทรศัพท์มือถือ iPhone, Windows Phone และ Android ภาค 2 ยิ่ง Smart ยิ่ง อันตราย
  - QR Code Attack – หลุมพรางใหม่ที่ผู้บริโภคและนักการตลาด...ต้องระวัง
  - GSM Hack – เปิดโปงกระแสข่าวลือที่ว่าระบบ GSM ถูก Hack สำเร็จแล้ว

  นำเสนอโดย
  - อ.ปริญญา หอมเอนก
    ITIL V3 Expert, CFE, CGEIT, CISSP, CSSLP, CISA, CISM, SSCP, SANS GIAC GCFW, CBCI IRCA ISMS Lead Auditor, ITSMS and BCMS Provisional Auditor, CobiT Certified Trainer
    ประธานและผู้ก่อตั้ง บริษัท เอซิส โปรเฟสชันนัล เซ็นเตอร์ จำกัด (ACIS)
    กรรมการและเลขานุการ สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA)
  - อ.นิพนธ์ นาซิน
    ITIL V3 Expert, AMBCI, CSSLP, CISSP, CISA, CISM, SSCP,SANS GIAC GCFA, CompTIA Security+, IRCA BCMS, IRCA ITSMS, IRCA ISMS Auditor
    Senior Consulting Manager,Technology Risk Advisory Services (TRAS)
    Information Security Consulting Business Unit (ISCBU)
    บริษัท เอซิส โปรเฟสชันนัล เซ็นเตอร์ จำกัด (ACIS)
    กรรมการ สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA)
  - และ ทีม ACIS Technical Risk Advisory Service Team

14:30-15:00 พักรับประทานอาหารว่าง (Coffee Break)

15:00-16:00 **M-07**

Live Demonstration:

- Top 7 Smartphone Attacks/Threats and How to Protect (Part II)
  เทคนิคการโจมตีสมาร์ทโฟน 7 อันดับที่กำลังเป็นที่นิยมของแฮกเกอร์และพร้อมทั้งวิธีรับมือ
  - On-the-fly SSL Hacking in Wireless Environment – เสน Net มีชีวิตวิ่งโดนขุดข้อมูล!!! (Mobile Internet banking, Facebook/Twitter/Gmail/Hotmail Password Stealing when using Mobile Phone)
  - Internet Tethering Threat (Phone-As-Modem) : The New Corporate Security Threat "Welcome to my World" – ระวังพนักงานเชิญ Hacker มาเยี่ยมชมบริษัทฯ โดยไม่ตั้งใจ
  - New Mobile Security Threat: Fingerprint Oil (Smudge Attacks on Smartphone Touch Screens) – ข้อมูลลับหลุดเพราะรอยนิ้วมือ
  - Mobile O/S Threat : The Real-World Android Threats – ภัยคืบคลานมาพร้อมกับสมาร์ทโฟนบนระบบปฏิบัติการ Android

  นำเสนอโดย
  - อ.ปริญญา หอมเอนก
    ITIL V3 Expert, CFE, CGEIT, CISSP, CSSLP, CISA, CISM, SSCP, SANS GIAC GCFW, CBCI IRCA ISMS Lead Auditor, ITSMS and BCMS Provisional Auditor, CobiT Certified Trainer
    ประธานและผู้ก่อตั้ง บริษัท เอซิส โปรเฟสชันนัล เซ็นเตอร์ จำกัด (ACIS)
    กรรมการและเลขานุการ สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA)
  - อ.นิพนธ์ นาซิน
    ITIL V3 Expert, AMBCI, CSSLP, CISSP, CISA, CISM, SSCP,SANS GIAC GCFA, CompTIA Security+, IRCA BCMS, IRCA ITSMS, IRCA ISMS Auditor
    Senior Consulting Manager,Technology Risk Advisory Services (TRAS)
    Information Security Consulting Business Unit (ISCBU)
    บริษัท เอซิส โปรเฟสชันนัล เซ็นเตอร์ จำกัด (ACIS)
    กรรมการ สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA)
  - และ ทีม ACIS Technical Risk Advisory Service Team

16:00-16:30 **M-08**

Mobile Computing Threats :

- Live, Real-Time and Interactive "Get Hacked Experience" Workshop
  สัมผัสประสบการณ์จริงในการถูกดัก ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ทั้ง Facebook และ Twitter ทำให้แฮกเกอร์สามารถเจาะข้อมูลส่วนตัวของเราได้อย่างง่ายดาย

16:30 ถาม-ตอบ และ Lucky Draw Bold 9780 และ Torch 9800

ผู้รับผิดชอบโครงการ

- เขตอุตสาหกรรมซอฟต์แวร์ประเทศไทย (Software Park Thailand - SWPARK)
- สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (Thailand Information Security Association - TISA)
- บริษัท เอซิส โปรเฟสชันนัล เซ็นเตอร์ จำกัด (ACIS Professional Center - ACIS)

รูปแบบการจัดอบรม

เป็นการบรรยายประกอบการสาธิตและฝึกปฏิบัติ (Live-Show Demonstration and Hands-On Information Security Workshop/LAB)

สัมมนา SNSCON 2011 & MOBISCON 2011 เหมาะสำหรับ

- ผู้บริหารระดับสูงหรือผู้บริหารระบบสารสนเทศระดับสูง (Management: CEO, CFO, CTO, CSO, CIO)
- ผู้อำนวยการหรือผู้จัดการสายงานระบบสารสนเทศ (IT Director / IT Manager)
- ผู้บริหารและผู้ปฏิบัติงานด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร (Information Security Officer and Executive)
- ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT Officer / IT Practitioner)
- ผู้บริหาร หรือผู้จัดการระบบเครือข่ายระบบสารสนเทศขององค์กร (System / Network Administrator)
- ผู้บริหารด้านการตลาด, การประชาสัมพันธ์ และกาแฟลักษณ์องค์กร (Corporate / Private Marketers)
- ผู้ประกอบการหรือเจ้าของกิจการ ผู้บริหารโครงการหรือผู้บริหารหน่วยธุรกิจขององค์กร (Business Owner or Project Owner)
- บุคลากรผู้เกี่ยวข้องกับการใช้อินเทอร์เน็ตของหน่วยงานภาครัฐและเอกชน (IT User)
- ผู้ใช้งานอินเทอร์เน็ตและผู้ใช้โทรศัพท์สมาร์ทโฟน (General Internet & Smartphone Users)

สิ่งที่ท่านจะได้รับเมื่อเข้าสัมมนา

- เอกสารคู่มือประกอบการบรรยาย SNSCON 2011 & MOBISCON 2011
- ซีดี SNSCON 2011 & MOBISCON 2011 ใหม่ล่าสุดรวบรวมโปรแกรมใช้งานบน Social Networking และ Smartphone พร้อมโปรแกรมการป้องกันข้อมูลส่วนตัวและองค์กรเพื่อการใช้ Social Network ครั้งต่อไป ปลอดภัยห่างไกลจากแหล่งข้อมูลที่น่าเชื่อถือในระดับสากล
- ชุด "SNSCON 2011 & MOBISCON 2011 Seminar Kit" สำหรับผู้เข้าร่วมสัมมนาทุกท่าน
- ผู้เข้าร่วมสัมมนาจะได้รับใบวุฒิบัตรจาก เขตอุตสาหกรรมซอฟต์แวร์ประเทศไทย (Software Park Thailand), สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA), บริษัท เอซิส โปรเฟสชันนัล เซ็นเตอร์ จำกัด (ACIS Professional Center - ACIS)
- หนังสือ รู้รอดปลอดภัยเมื่อใช้ Facebook/Twitter

SNSCON 2011

โปรแกรมการสัมมนา (

DAY 1 : 28th JUNE 2011

SNSCON 2011

07:30-08:45 ลงทะเบียน

08:45-09:00 **S-01**

Welcome Notes :

- The Implication of Social Networking in TISA's Perspective
  เครือข่ายสังคมออนไลน์กับผลกระทบด้านความมั่นคงปลอดภัยในมุมมองของสมาคมความมั่นคงปลอดภัยสารสนเทศ
  - ดร.รอม หิรัญพฤกษ์
    นายกสมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA)

09:00-09:45 **S-02**

Keynote Address :

- Power of Social Collaboration and Business Technology Adoption
  เพิ่มพลังการสื่อสารให้กับองค์กรด้วยโซเชียลคอลลาโบเรชั่นจากกูรูระดับประเทศ
  - รศ.ดร.รนชาติ นุ่มนนท์
    ผู้อำนวยการเขตอุตสาหกรรมซอฟต์แวร์ประเทศไทย (Software Park Thailand)

09:45-10:30 **S-03**

Keynote Address :

- New and Update : The Top Ten Social Networking Security Threats and How to Protect
  "Update" ภัยจากเครือข่ายสังคมออนไลน์ 10 ประการและวิธีการรับมืออย่างได้ผล
- Next Generation Analytics & Social Analytics
  รู้จักกับ Next Generation และ Social Analytics เทคโนโลยีใหม่ที่ทั่วโลกกำลังจับตามอง
- Social Network as a New Platform
  จะเกิดอะไรขึ้นเมื่อเครือข่ายสังคมออนไลน์กลายเป็นแพล็ตฟอร์มใหม่ของโลกวันนี้
  - อ.ปริญญา หอมเอนก
    ITIL V3 Expert, CFE, CGEIT, CISSP, CSSLP, CISA, CISM, SSCP, SANS GIAC GCFW, CBCI IRCA ISMS Lead Auditor, ITSMS and BCMS Provisional Auditor, CobiT Certified Trainer
    ประธานและผู้ก่อตั้ง บริษัท เอซิล โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด (ACIS)
    กรรมการและเลขานุการ สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA)

10:30-11:00 พักรับประทานอาหารว่าง (Coffee Break)

11:00-12:00 **S-04**

Panel Session :

- Security Issues and Concerns on using Social Networking and Mobile Devices in Organization
  ประเด็นปัญหาที่ผู้บริหารควรระวังเมื่อพนักงานใช้เครือข่ายสังคมออนไลน์และอุปกรณ์แพกพาในองค์กรมากขึ้นทุกวัน
- Effectiveness of Security Policy Enforcement for using Social Networking and Mobile Devices
  ปัญหาและประสบการณ์จริงของการใช้งานเครือข่ายสังคมออนไลน์และสมาร์ทโฟนภายในองค์กร องค์กรชั้นนำรับมืออย่างไร ?

วิทยากรผู้ทรงคุณวุฒิร่วมเสวนา

- ดร.วิริยะ อุปัติศกุล์
  หัวหน้าคณะผู้บริหารด้านเทคนิค บริษัท กรุ อินเทอร์เน็ต จำกัด
- คุณศรกวี ปุรณโชติ
  ผู้ช่วยผู้จัดการสายงานพัฒนาระบบงานเทคโนโลยีสารสนเทศ ตลาดหลักทรัพย์แห่งประเทศไทย
- คุณเสนีย์ วัชรศิริธรรม CISA
  ผู้จัดการตรวจสอบเทคโนโลยีสารสนเทศ ธนาคารไทยพาณิชย์ จำกัด (มหาชน)
  อดีตนายกสมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ-ภาคพื้นกรุงเทพฯ (ISACA)
- คุณสุรางคณา วายุภาพ
  รองผู้อำนวยการ สำนักงานพัฒนารัฐกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
  ผู้อำนวยการ ฝ่ายกฎหมาย สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
- อ.สมหมาย ฟองน้ำทิพย์ CISSP, CISA, CISM
  กรรมการ สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA)
  เลขานุการ สมาคมผู้ตรวจสอบและควบคุมระบบสารสนเทศ-ภาคพื้นกรุงเทพฯ (ISACA)
- อ.ปริญญา หอมเอนก
  ITIL V3 Expert, CFE, CGEIT, CISSP, CSSLP, CISA, CISM, SSCP, SANS GIAC GCFW, CBCI IRCA ISMS Lead Auditor, ITSMS and BCMS Provisional Auditor, CobiT Certified Trainer
  ประธานและผู้ก่อตั้ง บริษัท เอซิล โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด (ACIS)
  กรรมการและเลขานุการ สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA)

ผู้ดำเนินการเสวนา

- อ.ไชยกร อภิวัฒโนกุล CISSP, GCFA, IRCA:ISMS
  Chief Executive Officer, S-GENERATION (pka. QUANTIQ)
  กรรมการ สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA)

12:00-13:30 พักรับประทานอาหารกลางวัน (Lunch Break)

ให้ผู้ร่วมสัมมนาที่ต้องการร่วมทดสอบกับทีมงาน นำโทรศัพท์มือถือสมาร์ทโฟน Notebook/Laptop และเตรียม Username, Password ที่ใช้สำหรับการทดสอบมาในวันสัมมนา

13:30-14:00 **S-05**

- Stopping Current Attacks and Enforcing Accepted User Policies with Next Generation Intelligence Firewall
  เทคนิคการรับมือกับการโจมตีของแฮกเกอร์กับศิลปะในการออกนโยบายเพื่อการป้องกันด้วยเทคโนโลยี Firewall อัจฉริยะ
  - Mr.Kevin Lai
    Security Specialist (ASEAN), McAfee Global Threat Intelligence (GTI)

14:00-14:30 **S-06**

- Social Technologies and their Security Concerns on Social Networking Collaboration
  วิธีการใช้เทคโนโลยีบน Social Network อย่างปลอดภัยที่ทุกคนควรรู้
  - Advanced Facebook/Twitter Technics for Internal Corporate Usage
    "เทคนิคการใช้ Facebook และ Twitter ขั้นสูงเพื่อให้เกิดประโยชน์สูงสุดแก่องค์กร"
    เมื่อองค์กรจำเป็นต้องใช้ Facebook และ Twitter ในเชิงกลยุทธ์ จึงจำเป็นที่จะต้องเรียนรู้เทคนิคการใช้และลดความเสี่ยงจากการใช้งาน Facebook และ Twitter ภายในองค์กร
  - Brand Promotion Technics on Social Network
    "สร้าง Brand บน Social Network อย่างไรให้รวดเร็วแต่ปลอดภัย"
    การประยุกต์ใช้เครือข่ายสังคมออนไลน์ เพื่อส่งเสริมและสร้างชื่อเสียงให้กับสินค้าและบริการขององค์กร
  - The Bright Side of "Social Web Analytics"
    "เทคนิคการใช้ประโยชน์จากการสืบเสาะหาข้อมูลเครือข่ายสังคมออนไลน์ขั้นเทพ"
    การเพิ่มความสามารถในการแข่งขัน โดยการวิเคราะห์และสืบเสาะหาข้อมูลบนเครือข่ายสังคมออนไลน์
  - Privacy Breach Problem on Social Networks and How to Protect
    "ความเป็นส่วนตัวบนเครือข่ายสังคมออนไลน์ ปัญหาโลกแตกที่ต้องติดตาม"
    ปัญหาเรื่องข้อมูลส่วนตัวรั่วไหลในเครือข่ายสังคมออนไลน์ร้ายแรงกว่าที่คิด และแนวทางในการป้องกัน
  - Lifestyle Hacking Protection
    "รู้ทันภัยร้ายใหม่ๆ กับพฤติกรรมคนรุ่นใหม่" ภัยร้ายอยู่ใกล้แค่เพียงปลายนิ้ว เมื่อผู้ใช้ Facebook/Twitter ก้าวล้ำโลดแล่นไปในเครือข่ายสังคมออนไลน์อย่างสนุกสนาน โดยขาดความระมัดระวัง เรียนรู้วิธีการสร้างเกราะป้องกันก่อนจะสาย

  นำเสนอโดย

  - อ.ปริญญา หอมเอนก
    ITIL V3 Expert, CFE, CGEIT, CISSP, CSSLP, CISA, CISM, SSCP, SANS GIAC GCFW, CBCI IRCA ISMS Lead Auditor, ITSMS and BCMS Provisional Auditor, CobiT Certified Trainer
    ประธานและผู้ก่อตั้ง บริษัท เอซิล โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด (ACIS)
    กรรมการและเลขานุการ สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA)

  - อ.นิพนธ์ นาชิน
    ITIL V3 Expert, AMBCI, CSSLP, CISSP, CISA, CISM, SSCP,SANS GIAC GCFA, CompTIA Security+, IRCA BCMS, IRCA ITSMS, IRCA ISMS Auditor
    Senior Consulting Manager,Technology Risk Advisory Services (TRAS)
    Information Security Consulting Business Unit (ISCBU)
    บริษัท เอซิล โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด (ACIS)
    กรรมการ สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA)

  - และ ทีม ACIS Technical Risk Advisory Service Team

14:30-15:00 พักรับประทานอาหารว่าง (Coffee Break)

15:00-16:00 **S-07**

Live Demonstration :

- Top Social Network Threats and How to Protect
  สาธิตเทคนิควิธีการขโมยข้อมูลบน Social Network พร้อมวิธีป้องกัน
  - APT (Advanced Persistent Threat) - การกลับมาอีกครั้งของสงครามม้าโทรจันหมัดเด็ดภัยร้ายล่าสุดที่คุณอาจตกเป็นเป้าหมายของมันโดยไม่รู้ตัว
  - Clickjacking - คลิ๊กไม่คิดมีสิทธิ์โดน "Hack"
  - Targeted Brand Attacks on Social Network and How to Combat - สร้างง่ายก็ทำลายง่าย ต้องระวังแบรนด์ของคุณให้ดี
  - Advanced Facebook/Twitter Username and Password Attack - ใช้ Social Network ใน Office ระวังเพื่อน Hack Account!
  - Advanced on-the-fly SSL Hacking - SSL/https ใครว่าปลอดภัย?

  นำเสนอโดย

  - อ.ปริญญา หอมเอนก
    ITIL V3 Expert, CFE, CGEIT, CISSP, CSSLP, CISA, CISM, SSCP, SANS GIAC GCFW, CBCI IRCA ISMS Lead Auditor, ITSMS and BCMS Provisional Auditor, CobiT Certified Trainer
    ประธานและผู้ก่อตั้ง บริษัท เอซิล โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด (ACIS)
    กรรมการและเลขานุการ สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA)

  - อ.นิพนธ์ นาชิน
    ITIL V3 Expert, AMBCI, CSSLP, CISSP, CISA, CISM, SSCP,SANS GIAC GCFA, CompTIA Security+, IRCA BCMS, IRCA ITSMS, IRCA ISMS Auditor
    Senior Consulting Manager,Technology Risk Advisory Services (TRAS)
    Information Security Consulting Business Unit (ISCBU)
    บริษัท เอซิล โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด (ACIS)
    กรรมการ สมาคมความมั่นคงปลอดภัยระบบสารสนเทศ (TISA)

  - และ ทีม ACIS Technical Risk Advisory Service Team

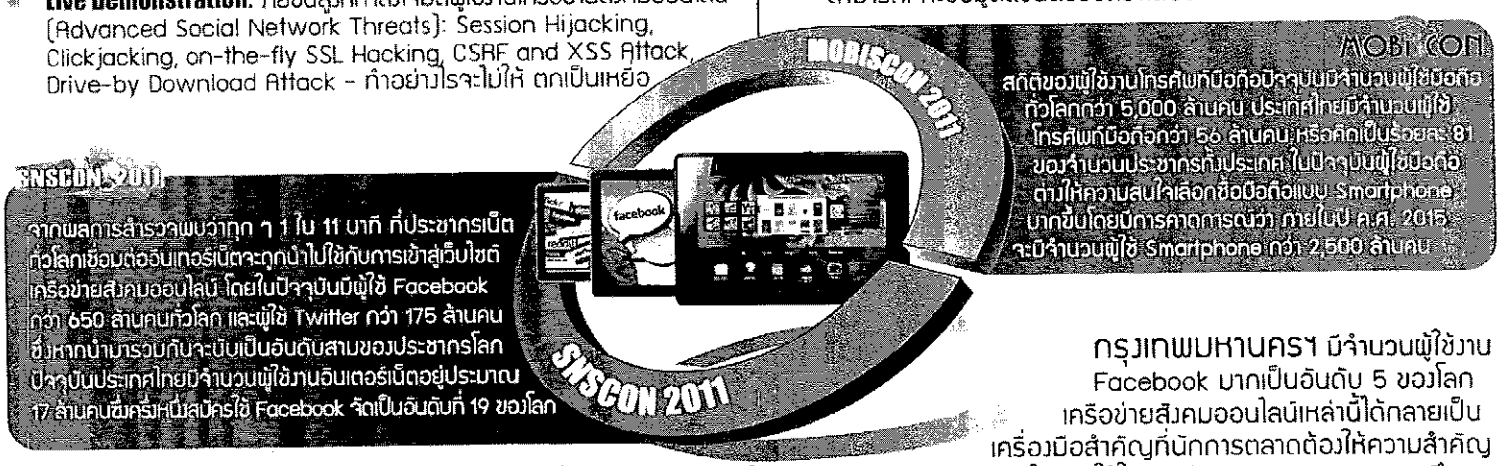
16:00-16:30 **S-08**

Social Network Threats using Facebook/Twitter :

- Live, Real-Time and Interactive "Get Hacked Experience" Workshop
  สัมผัสประสบการณ์จริงในการถูกดักข้อมูล ชื่อผู้ใช้ (Username) และ รหัสผ่าน (Password) ทั้ง Facebook และ Twitter ทำให้แฮกเกอร์สามารถเจาะข้อมูลส่วนตัวของเราได้อย่างง่ายดาย

CONFERENCE HIGHLIGHTS

- วิสัยทัศน์จาก Security Guru อะไรจะเกิดขึ้นเมื่อ "Social Network" กลายเป็น "New Platform"
- บทวิเคราะห์แนวโน้มล่าสุด "Social Network Technology Trends & Threats" จากงานสัมมนา RSA 2011 San Francisco, USA.
- ประเด็นร้อนเรื่องความมั่นคงปลอดภัยในการใช้งานเครือข่ายสังคมออนไลน์ในประเทศไทยและทั่วโลก
- คุณประโยชน์และด้านมืดของเครื่องมือสังเคราะห์ข้อมูล (Social Network Analytic Tools) จากเครือข่ายสังคมออนไลน์เพื่อชิงความได้เปรียบในการแข่งขัน
- เรียนรู้มาตรการด้านความมั่นคงปลอดภัยในการใช้งานเครือข่ายสังคมออนไลน์เพื่อป้องกันการใช้งานเครือข่ายสังคมออนไลน์ที่ไม่ถูกต้องในองค์กร
- เรียนรู้กลเม็ดเคล็ดลับในการใช้งาน Facebook, Twitter และ YouTube อย่างปลอดภัย
- เรียนรู้นโยบายในการบริหารจัดการความมั่นคงปลอดภัยในการใช้งานเครือข่ายสังคมออนไลน์ เพื่อการนำไปใช้ในองค์กรอย่างมีประสิทธิภาพ
- บทวิเคราะห์ New Hacking Technics วันนี้ เทคนิคการจารกรรมข้อมูลขั้นสูงแบบต่อเนื่อง (APT: Advanced Persistent Threats) และวิธีป้องกัน
- ไลฟ์สไตล์ที่ต้องพึงระวัง..เทคนิคการล่อลวงที่มากับเครือข่ายสังคมออนไลน์ที่คุณต้องรู้ (Advanced Social Engineering Techniques on Social Networks)
- กลโกงใหม่ๆใน Facebook และ Twitter ที่นักการตลาดต้องระวัง
- **Best Practice:** การป้องกันข้อมูลและความเป็นส่วนตัวในการใช้งานเครือข่ายสังคมออนไลน์อย่างได้ผลในทางปฏิบัติจริง
- **Case Study:** กรณีศึกษาจากผู้บริหารระดับสูงและผู้ตรวจสอบสารสนเทศจากภาครัฐและเอกชนเกี่ยวกับปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ในองค์กรและการป้องกัน
- **Success Story:** การบริหารจัดการและการป้องกันภัยใหม่ๆที่มากับการใช้งานเครือข่ายสังคมออนไลน์ในองค์กรจากวิทยากรรับเชิญผู้มากด้วยประสบการณ์
- **Live Demonstration:** ภัยขั้นสูงที่กำลังโจมตีผู้ใช้งานเครือข่ายสังคมออนไลน์ (Advanced Social Network Threats): Session Hijacking, Clickjacking, on-the-fly SSL Hacking, CSRF and XSS Attack, Drive-by Download Attack - ทำอย่างไรจะไม่ให้ ตกเป็นเหยื่อ
- วิเคราะห์แนวโน้มทิศทางความก้าวหน้าของเทคโนโลยีโทรศัพท์มือถือสมาร์ทโฟนและอุปกรณ์สื่อสารไร้สาย
- อะไรจะเกิดขึ้นเมื่อสมาร์ทโฟนได้กลายเป็นคอมพิวเตอร์ส่วนบุคคล (Smartphone is a new PC) เพื่อการใช้งานแบบเคลื่อนที่ไร้ขอบเขตในยุค Pervasive Computing แล้วความมั่นคงปลอดภัยจะอยู่ที่ไหน?
- บทวิเคราะห์ภัยใหม่ที่มากับโทรศัพท์มือถือและสมาร์ทโฟน Advanced Mobile Trojan Attack...แอบล้วงตับโดยการใช้โปรแกรมโทรจันในสมาร์ทโฟน...ยิ่งสมาร์ท...ยิ่งอันตราย
- เปิดโปงการแฮกระดับโลก "GSM Hacking" และการล้วงข้อมูลบนโทรศัพท์มือถือและสมาร์ทโฟน "บทสนทนาผ่านโทรศัพท์ GSM ของคุณจะไม่เป็นส่วนตัวอีกต่อไป"
- ใช้สมาร์ทโฟนเล่นอินเทอร์เน็ตฟรีระวังโดนดูดข้อมูลไม่รู้ตัว...รู้หรือไม่ว่าเรากำลังเชื่อมต่อสมาร์ทโฟนเข้ากับ Access Point ปลอม (Rouge AP)
- ภัยใหม่ล่าสุด "Internet Tethering Threat" จากการใช้สมาร์ทโฟนทำตัวเป็น Access Point ต่อเชื่อมกับเครือข่ายอินเทอร์เน็ต
- ไลฟ์สไตล์ที่ Gen-Y ต้องระวัง...หลุมพรางใหม่ "QR Code Attack"
- เรียนรู้มาตรการและนโยบายในการบริหารจัดการความมั่นคงปลอดภัยในการใช้งานโทรศัพท์มือถือและสมาร์ทโฟนในองค์กรจากงานวิจัยของ TISA พร้อมรับเอกสารต้นแบบนโยบาย "Mobile Computing/Social Network Security Policy Template for Corporate"
- เราจะป้องกันตนเองและองค์กรให้รอดพ้นและปลอดภัยจากภัยสมัยใหม่อันร้ายกาจที่มากับเครือข่ายสื่อสารไร้สายได้อย่างไรในอนาคต
- ม้าโทรจันตัวใหม่บน Blackberry, iPhone, Android และ Windows Phone ที่เราต้องระวัง
- ข้อมูลส่วนตัวอาจหลุดรั่วได้ง่าย ๆ เพียงเพราะรอยนิ้วมือบน Touch Screen ของโทรศัพท์มือถือ
- **Live, Real-Time and Interactive:** Get Hacked Experience Workshop - สัมผัสประสบการณ์จริงในการถูกดักข้อมูลส่วนตัว ได้แก่ ชื่อผู้ใช้ (Username) และ รหัสผ่าน (Password) จากการใช้งานโทรศัพท์มือถือและสมาร์ทโฟนโดยไม่ระวังและรู้เท่าไม่ถึงการณ์ทำให้แฮกเกอร์สามารถเจาะข้อมูลส่วนตัวของเราได้อย่างง่ายดาย



กรุงเทพมหานคร มีจำนวนผู้ใช้งาน Facebook มากเป็นอันดับ 5 ของโลก เครือข่ายสังคมออนไลน์เหล่านี้ได้กลายเป็นเครื่องมือสำคัญที่นักการตลาดต้องให้ความสำคัญไม่น้อยไปกว่าสื่ออื่น ๆ ปัจจุบันมีองค์กรชั้นนำมากมายที่ประสบความสำเร็จในการนำเครือข่ายสังคมออนไลน์มาใช้ในการส่งเสริมการตลาด เราควรศึกษา Case Study "กลยุทธ์การตลาดของแบรนด์ชั้นนำในการนำ Facebook/Twitter มาใช้" ว่ามีวิธีการอย่างไร และเขามาถึงจุดนี้ได้อย่างไร และเรื่องสำคัญที่มองข้ามไม่ได้เลยก็คือเรื่องความมั่นคงปลอดภัยในการใช้งานเครือข่ายสังคมออนไลน์และโทรศัพท์ประเภทสมาร์ทโฟนที่กำลังได้รับความนิยมอย่างสูง เพื่อให้เราสามารถใช้งานได้อย่างมั่นใจ และไม่ตกเป็นเหยื่อของเหล่ามิจฉาชีพ ไฮเทคที่นับวันจะเปลี่ยนรูปแบบการโจมตีจนเราตามแทบไม่ทัน

ในปีนี้งาน SNSCON 2011 และ MOBISCON 2011 คณะผู้จัดได้นำข้อมูลจากงาน RSA conference และทั่วโลกมา Update รวมทั้งวิเคราะห์แนวโน้มทิศทางและประเด็นร้อนเรื่องความมั่นคงปลอดภัยในการใช้งานเครือข่ายสังคมออนไลน์และสมาร์ทโฟน ซึ่งได้กลายเป็น "Hot Issue" สำหรับองค์กรต่างๆ ในเวลานี้และสมาคม TISA ได้ร่วมกันระดมสมองผู้เชี่ยวชาญจัดทำต้นแบบแนวนโยบายสำหรับการใช้งานเครือข่ายสังคมออนไลน์และอุปกรณ์สื่อสารไร้สายอย่างปลอดภัยและได้ผลอย่างเป็นรูปธรรม มาพร้อมกับคำตอบบทวิเคราะห์ "Social Network as a New Platform" และ "Smartphone is a new PC"

สมัครเข้าร่วมสัมมนา สามารถติดต่อได้ที่
บริษัท เอซิส โปรเฟสชั่นนัล เซ็นเตอร์ จำกัด
ติดต่อ คุณลัดดา (ต่อ 108), คุณวราพงศ์ (ต่อ 107)
โทรศัพท์: 02-650-5771, โทรสาร: 02 650 5776
E-mail: ladda.re@acisonline.net, varapong.ra@acisonline.net

Please visit us at :
www.snsconference.com
twitter.com/snsconference
facebook.com/snsconference