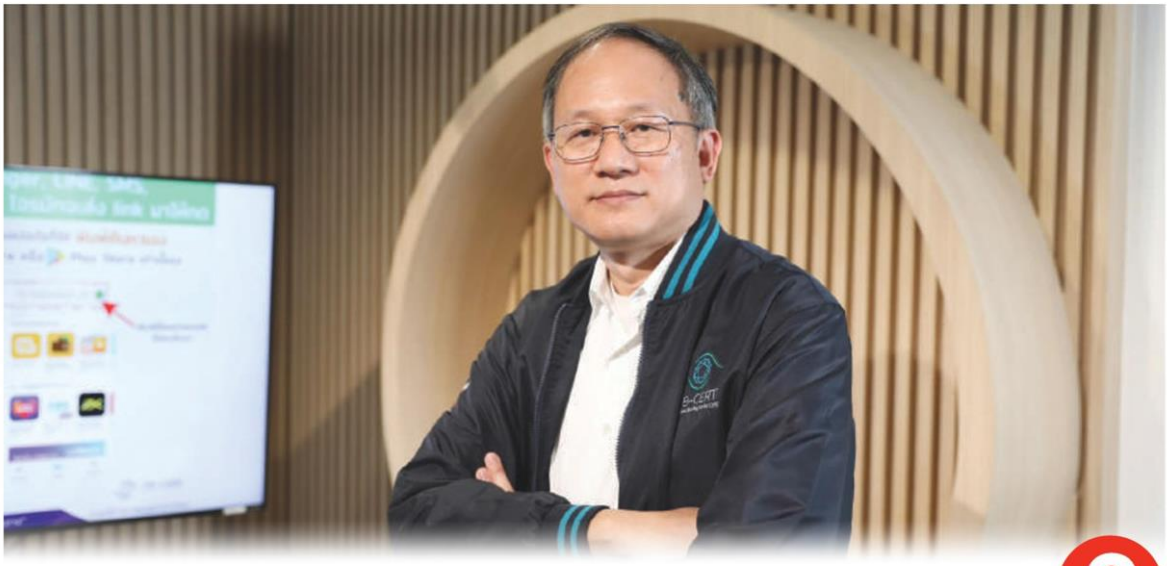
ผู้จัดการรายวัน 360°
Poo Jadkarn Daily 360 Degree
Circulation: 850,000
Ad Rate: 1,500

Section: iBusiness/iBusiness
วันที่: จันทร์ 13 กุมภาพันธ์ 2566
ปีที่: 15 ฉบับที่: 3887 หน้า: 1(ล่างซ้าย), 2
Col.Inch: 233.78 Ad Value: 350,670 PRValue (x3): 1,052,010 คลิป: สี่สี
หัวข้อข่าว: TB-CERT เปิดกลโกงภัยไซเบอร์



TB-CERT เปิดกลโกงภัยไซเบอร์ 2

TB-CERT เปิดกลโกงภัยไซเบอร์

ตลาดทุน-ตลาดเงิน

คงปฏิเสธไม่ได้ว่าในยุคปัจจุบันสิ่งที่เรียกว่า "ดิจิทัล" เข้ามามีความสำคัญในการใช้ชีวิตประจำวันของเราไม่น้อยเลยทีเดียวไม่ว่าจะเป็นการดูหนัง ฟังเพลง รับประทานอาหารไปจนถึงการทำธุรกรรมทางการเงินหรือดิจิทัล แบงก์กิ้ง ที่สร้างความสะดวกรวดเร็ว และทำได้ 24 ชั่วโมงไม่มีวันหยุด และเช่นกันที่ตามมาติดๆ ก็คือภัยทางไซเบอร์ที่เพิ่มจำนวนขึ้นมาอย่างต่อเนื่องและมีจำนวนความเสียหายที่สูงขึ้น ซึ่งในเรื่องดังกล่าว นายกิตติ โฆษะวิสุทธิ์ ผู้จัดการบริหารความมั่นคงปลอดภัยด้านสารสนเทศและความปลอดภัยไซเบอร์ ธนาคารกรุงเทพ จำกัด (มหาชน) (BBL) ในฐานะที่ปรึกษากิตติมศักดิ์ ศูนย์ประสานงานด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศภาคธนาคาร (TB-CERT) ให้ข้อมูล-ความรู้ความเข้าใจเกี่ยวกับภัยทางไซเบอร์ กลโกง ไปจนถึงข้อควรระวังดังต่อไปนี้

ภัยทางไซเบอร์ที่ต้องระมัดระวัง

อันดับหนึ่ง ก็คือ **Ransomware การถูกเรียกค่าไถ่ โดยตามสถิติแล้วเป้าหมายอันดับหนึ่งที่ประสบคือ อุตสาหกรรมการเงิน ก็คือการขโมยข้อมูลเพื่อนำไปเรียกค่าไถ่** ซึ่งวิธีนี้ต้องมีการกระตุ้นให้รีบจ่ายค่าตอบแทน หรือขู่ให้จ่าย อาทิ ขู่ว่าถ้าไม่จ่ายในระยะเวลาที่กำหนด จะนำข้อมูลไปขาย เพราะหากให้เวลานานองค์กรนั้นก็อาจจะสามารถแบ็กอัปเอาข้อมูลกลับมาได้เอง

อันดับ 2 **การขโมยตัวตนในโลกดิจิทัล Identity and Credential Theft ถ้าขโมยได้ก็จะปลอมเป็นตัวตนของคนคนนั้นได้** ซึ่งเป็นแนวโน้มที่น่าจับตามองเพราะมีแนวโน้มสูงขึ้น

อันดับ 3 **Social Enginerring(Phishing) การหลอกลวงยังเป็นเทคนิคที่ไม่ได้ใหม่ มีมานานแล้ว** แต่ยังคงใช้ได้ผล โดยเฉพาะช่วงโควิดที่ทำงานที่บ้าน Phishing Mail มีสูงมาก ช่วงแรกของโควิดเพิ่มขึ้นหลายเท่าตัว

อันดับ 4 **Vulnerability exploitation ช่องโหว่ระบบ**

ผู้จัดการรายวัน 360°
Poo Jadkarn Daily 360 Degree
Circulation: 850,000
Ad Rate: 1,500

Section: iBusiness/iBusiness
วันที่: จันทร์ 13 กุมภาพันธ์ 2566
ปีที่: 15 **ฉบับที่:** 3887 **หน้า:** 1(ล่างซ้าย), 2
Col.Inch: 233.78 **Ad Value:** 350,670 **PRValue (x3):** 1,052,010 **คลิป:** สี่สี
หัวข้อข่าว: TB-CERT เปิดกลโกงภัยไซเบอร์

นายกิตติ โฆษะวิสุทธิ์

คอมพิวเตอร์ไม่ว่าจะเป็นแบบไหนก็มักจะมีช่องโหว่ อัตราการพบช่องโหว่ที่มีความรุนแรง ไม่ว่าจะเป็น IOS แอนดรอย คนร้ายจะเข้าถึงระบบนั้นจากความบกพร่องนั้นที่ยังไม่ได้ถูกแก้ไข อันนี้ก็พบได้บ่อยโดยเฉพาะการใช้กลไกที่เรียกว่า Remote ที่สามารถเข้าไปถึงระบบงานได้เลยโดยอาศัยช่องโหว่ไม่ได้อาศัยการหลอกลวง

อันดับ 5 เป็นเรื่อง **3rd Party ในการให้บริการลูกค้า การติดต่อเชื่อมโยงไม่ได้มีแค่ผู้ให้กับผู้ใช้บริการ แต่ระบบงานหลังบ้านจะต้องเชื่อมโยงกับอื่นๆ** เช่น การเพย์เมนต์ โลจิสติกส์ กรณีที่หน่วยงานใดหน่วยงานหนึ่งมีความผิดพลาดแล้วถูกแฮกก็อาจจะเป็นช่องทางที่นำมาสู่อีกหน่วยงานหนึ่งได้เป็นซัปพลายเชนได้

วิธีการ-รูปแบบกรณีศึกษาการโจรกรรม

Case # 1 ขโมยรหัสลับ : มิจฉาชีพสุ่มส่งเมล SMS ให้กับหลายๆคนที่มี URL ไปที่ Phishing website ที่เตรียมไว้ เข้าไปที่หน้าเว็บไซต์ที่ทำเลียนแบบเป้าหมายต้องการหลอกเอาข้อมูล OTP ก็หลอกลวงโดยใช้หน้าเว็บไซต์ที่เลียนแบบมาเพื่อให้ได้ข้อมูลที่ต้องการ และ login เข้าระบบแล้วทำรายการในบัญชีของท่านได้เลย แต่ระบบนี้มีจุดอ่อนที่จะต้องรอให้เหยื่อ logon บน Phishing website ซึ่งไม่รู้เมื่อไหร่

Case # 2 Remote App แก๊ง Call Center ชวนคุยและชวนให้ทำตาม โดยอ้างมาจากหน่วยงานภาครัฐ เช่น ตำรวจ สรรพากร อื่นๆ โดยใช้ Chat หรือ SMS ส่ง Link ให้ cilck เพื่อลงโปรแกรมที่ใช้ควบคุมทางไกล เช่น Team Viewer ,AnyDesk หรือ RealVNC ซึ่งเป็นโปรแกรมจริงจาก Official Store จากนั้นก็เริ่มโปรแกรม remote control และขอให้ส่งโค้ด เพื่อให้เข้าควบคุมเครื่อง ซึ่งหน้าจอจะถูก mirror ไปให้มิจฉาชีพซึ่งจะล่อลวงให้เข้าระบบ Mobile app แล้วชวนคุย เพื่อให้มิจฉาชีพจะสามารถทำธุรกรรมโอนเงินไปสู่บัญชีม้าได้ โดยเจ้าของบัญชีไม่เห็นหน้าจอ

ทั้งนี้ ในกรณีดังกล่าวในส่วนของ Mobile app ของธนาคารต่างๆ นั้น ได้ป้องกันโดยสั่งหยุดทำงานของ Mobile Banking เมื่อพบการทำ screen mirroring หรือส่งหน้าจอสีดำไปให้แอป ที่ควบคุมทางไกล

Case #3 Accessibility Service Malware โดยมิจฉาชีพจะชวนคุยในไลน์ และชวนให้ลงโปรแกรม/แอปพลิเคชันหาคู่ปลอมเพื่อดูไลฟ์สด เมื่อเหยื่อคลิกเพื่อลงโปรแกรมซึ่งเป็นโปรแกรมจากนอก Official Store และให้คำยินยอมอื่นๆตามที่แอปฯร้องขอ โดยไม่รู้ว่ากำลังให้ความยินยอมเพื่อลงโปรแกรมที่จะเป็น Accesssibility service ซึ่งสามารถเข้าถึงการทำงานของเครื่องได้ เช่น ข้อมูลสำคัญ, การใช้งานบนหน้าจอ รวมถึงรหัสผ่าน OTP บนหน้าจอ จากนั้นมัลแวร์ทำการดักจับข้อมูลการเข้าใช้งานแอปพลิเคชันต่างๆ ในเครื่องรวมถึง PIN ในการใช้งาน โมบายแบงก์กิ้ง และมัลแวร์จะทำการรันโมบายแบงก์กิ้งและโอนเงินในบัญชีในช่วงที่เหยื่อไม่ได้ใช้งาน เพื่อไม่ให้รู้ถึงความเคลื่อนไหวขณะโอนเงิน

นายกิตติกล่าวว่า เราจะเห็นได้ว่ากลโกงที่มิจฉาชีพใช้

ผู้จัดการรายวัน 360°
Poo Jadkarn Daily 360 Degree
Circulation: 850,000
Ad Rate: 1,500

Section: iBusiness/iBusiness
วันที่: จันทร์ 13 กุมภาพันธ์ 2566
ปีที่: 15 **ฉบับที่:** 3887 **หน้า:** 1(ล่างซ้าย), 2
Col.Inch: 233.78 **Ad Value:** 350,670 **PRValue (x3):** 1,052,010 **คลิป:** สี่สี
หัวข้อข่าว: TB-CERT เปิดกลโกงภัยไซเบอร์

ก็มีการพัฒนาขึ้นนับแต่ Case # 1 ที่จะต้องมานั่งรอให้เหยื่อคลิกอีเมลที่ส่งไปซึ่งไม่รู้เมื่อไหร่ มาเป็นการใช้ Remote App ใช้ Sceen Mirroring ที่มีความซับซ้อนขึ้นและเห็นผลมากขึ้น ขณะที่ในCase # 3 นี้ เราจะเห็นจากที่เขากรณีล่าสุดที่เกิดความตื่นตระหนกว่า สายชาร์จดูดข้อมูล ซึ่งไม่ใช่เป็นเพราะมิจฉาชีพฉวยโอกาสทำรายการ ตอนที่เหยื่อกำลังชาร์จแบตเตอรี่อยู่ เพื่อไม่ให้เหยื่อรู้ตัว... **ดังนั้น เพื่อป้องกันการถูกโจรกรรมข้อมูลลักษณะดังกล่าวซึ่งมุ่งโจมตีจากการโมบายแบงกิ้ง โดยแนะนำให้ดาวน์โหลดแอปด้วยการพิมพ์ชื่อบนระบบปฏิบัติการโดยไม่คลิกลิงก์ ไม่เผยแพร่ข้อมูลมากเกินไปในสื่อสาธารณะ ไม่เชื่อมต่อไวไฟสาธารณะ** ขณะทำธุรกรรมไม่ให้ข้อมูลส่วนตัวกับคนแปลกหน้า และมีสติรอบคอบขณะทำธุรกรรม อย่างไรก็ตาม หากผู้บริการได้ดำเนินการใดๆ ที่มีความเสี่ยงไปแล้ว แนะนำให้เปลี่ยนไปใช้ระบบ Air Plane Mode หรือถอดซิมเพื่อปิดระบบการเชื่อมต่อ และเปลี่ยนพาสเวิร์ดในการเข้าสู่ระบบธนาคาร หรือติดต่อธนาคารที่ท่านใช้งาน

ลุ้นจับม้าทั้งฟาร์ม

นายกิตติกล่าวอีกว่า ในช่วงที่ผ่านมา หน่วยงานที่เกี่ยวข้อง เช่น ธนาคารแห่งประเทศไทย (ธปท.) สำนักงานกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคม (สกทช.) สมาคมธนาคารไทย ธนาคารพาณิชย์ และนอนแบงก์ หน่วยงานบังคับใช้กฎหมาย ผู้ให้บริการเครือข่าย ผู้ให้บริการโซเชียลมีเดีย ไม่นิ่งนอนใจ พยายามที่จะร่วมกันเพื่อยกระดับการป้องกัน โดยล่าสุด **กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมได้เสนอ พ.ร.ก.มาตรการป้องกัน และปราบปรามอาชญากรรมทางเทคโนโลยีที่ผ่านการพิจารณาจากคณะรัฐมนตรี โดยเน้นในการแก้ไขปัญหาซิมผี และบัญชีม้า โดยให้มีบทลงโทษที่สูงขึ้น และมอบอำนาจให้ธนาคารสามารถระงับบัญชีก่อนที่แจ้งความต่อเจ้าหน้าที่ตำรวจ**

โดยขณะนี้อยู่ระหว่างพิจารณาจากกฤษฎีกา คาดว่าจะสามารถบังคับใช้ได้ในเดือนกุมภาพันธ์นี้ ขณะที่ธนาคารพาณิชย์จะต้องมีการยกระดับการป้องกันเช่นกัน โดยอยู่ระหว่างการสร้างฐานข้อมูลกลางเพื่อแลกเปลี่ยนข้อมูลเกี่ยวกับบัญชีม้าเพื่อลดจำนวนบัญชีและการสูญเสีย

"พ.ร.ก.นี้จะช่วยให้เราสามารถระงับบัญชีได้รวดเร็วขึ้น โดยไม่ต้องรอแจ้งความ และในส่วนของการแชร์ข้อมูลของบัญชีม้าระหว่างธนาคารนั้น จะช่วยเพิ่มประสิทธิภาพในการลด-เพิ่มจำนวนบัญชีม้า เพราะบัญชีม้าแต่ละบัญชีมีต้นทุนต้องว่าจ้างเปิด การโอนผ่านบัญชีม้าก็จะต้องใช้โอนต่อๆ กันหลายๆ บัญชีจึงจะสาวถึงตัวผู้กระทำความผิดได้ยาก หากเราสามารถมีข้อมูลเชื่อมกันได้ หรือแชร์ข้อมูลของแต่ละสถาบันการเงินได้ว่ามีชื่อนี้อยู่ในธนาคารไหนบ้าง เราก็จะจับม้าได้ครั้งละหลายบัญชี หรือจับได้ทั้งฟาร์ม ก็จะทำให้ช่วยลดจำนวนได้ และผู้กระทำความผิดก็จะใช้วิธีการนี้ลดลง เพราะเสียต้นทุนครั้งละมากๆ เมื่อถูกจับได้" .

ผู้จัดการรายวัน 360°
Poo Jadkarn Daily 360 Degree
Circulation: 850,000
Ad Rate: 1,500

Section: iBusiness/iBusiness
วันที่: จันทร์ 13 กุมภาพันธ์ 2566
ปีที่: 15 **ฉบับที่:** 3887 **หน้า:** 1(ล่างซ้าย), 2
Col.Inch: 233.78 **Ad Value:** 350,670 **PRValue (x3):** 1,052,010 **คลิป:** สี่สี
หัวข้อข่าว: TB-CERT เปิดกลโกงภัยไซเบอร์

แบงก์กรุงเทพแนะ 8 พฤติกรรมต้องทำ ลดเสี่ยง!

นายกิตติ โฆษะวิสุทธิ์ ผู้จัดการบริหารความมั่นคงปลอดภัยด้านสารสนเทศ และความปลอดภัยไซเบอร์ ธนาคารกรุงเทพ จำกัด (มหาชน) (BBL) กล่าวว่า ธนาคารมีความห่วงใยผู้ใช้งาน เนื่องจากรูปแบบภัยไซเบอร์มีความหลากหลายและซับซ้อนมากขึ้น จนทำให้ผู้ใช้งานตกเป็นเหยื่อโดยไม่รู้ตัว และมิจฉาชีพมักปรับเปลี่ยนรูปแบบโจรกรรมอยู่ตลอดเวลา จึงติดตามให้เท่าทันได้ยาก เพื่อป้องกันการถูกโจรกรรมข้อมูลลักษณะดังกล่าว ผู้ใช้งานควรตรวจสอบด้วยตัวเองอย่างสม่ำเสมอ ว่าสมาร์ทโฟนของตนเองมีการอนุญาตให้แอปพลิเคชันที่ไม่รู้จัก ขอสิทธิ์ใช้งาน Accessibility Service หรือไม่ หรือให้อนุญาตการเข้าถึงมากเกินกว่าความจำเป็นหรือไม่ ซึ่งหากพบว่ามีความเสี่ยงลักษณะดังกล่าว ให้รีบปิดหรือยกเลิกสิทธิ์การใช้งาน Accessibility service ของแอปพลิเคชันดังกล่าวทันที

ทั้งนี้ ได้แนะ 8 พฤติกรรมปลอดภัย เพื่อไม่ให้ตนเองตกอยู่ในความเสี่ยงจากการถูกโจรกรรมข้อมูลหรือดูดเงินออกจากบัญชี ดังนี้

1. **อุปกรณ์ปลอดภัย** ห้ามใช้โทรศัพท์มือถือที่ไม่ปลอดภัยมาทำธุรกรรมทางการเงิน อาทิ เครื่องที่ถูกปลดล็อก (root/jailbreak) หรือใช้เครื่องที่มีระบบปฏิบัติการล้าสมัย และตั้งล็อกหน้าจอ

2. **ตัวตนปลอดภัย** ไม่เปิดเผยข้อมูลส่วนตัวในสื่อสาธารณะเกินความจำเป็น

3. **รหัสปลอดภัย** ตั้งค่ารหัส (Password) ที่ไม่ง่ายเกินไป ไม่ซ้ำกับรหัสการใช้ทั่วไป และไม่บอกผู้อื่น

4. **สื่อสารปลอดภัย** ไม่ให้ข้อมูลส่วนตัวกับคนแปลกหน้าและไม่แสดงตัวก่อน หากถูกถามให้ตรวจสอบคู่สนทนาให้แน่ชัด

5. **เชื่อมต่อปลอดภัย** ไม่ทำธุรกรรมทางการเงินผ่านสัญญาณ Wi-Fi สาธารณะ หรือฟรี

6. **ดาวน์โหลดหรือติดตั้งโปรแกรมจากแหล่งที่ได้รับรองโดยผู้พัฒนาระบบปฏิบัติการ (Official Store)** เช่น Play Store หรือ App Store เท่านั้น โดยไม่คลิกจากลิงก์ และตรวจเช็กการอนุญาต หรือ Permission ของแอปพลิเคชัน และสังเกต การขออนุญาตเข้าใช้งานอุปกรณ์หรือข้อมูลที่ไม่สัมพันธ์สอดคล้องวัตถุประสงค์การใช้งานและกับประเภทการทำงานของแอปพลิเคชัน

7. **มีสติรอบคอบก่อนการทำธุรกรรมทุกครั้ง** อ่านข้อความที่ขึ้นเตือนบนเครื่องโทรศัพท์มือถือให้ถี่ถ้วน ไม่คลิกลิงก์จาก SMS, Chat หรืออีเมลที่ถูกส่งมาจากแหล่งที่ไม่รู้จักหรือไม่น่าเชื่อถือ

8. **ศึกษา และติดตามข่าวสารการใช้งานเทคโนโลยีเป็น**

ผู้จัดการรายวัน 360°

Poo Jadkarn Daily 360 Degree
Circulation: 850,000
Ad Rate: 1,500

Section: iBusiness/iBusiness
วันที่: จันทร์ 13 กุมภาพันธ์ 2566
ปีที่: 15 **ฉบับที่:** 3887 **หน้า:** 1(ล่างซ้าย), 2
Col.Inch: 233.78 **Ad Value:** 350,670 **PRValue (x3):** 1,052,010 **คลิป:** สี่สี
หัวข้อข่าว: TB-CERT เปิดกลโกงภัยไซเบอร์

ประจำสม่ำเสมอ โดยหมั่นตรวจเช็กการตั้งค่า ไม่ให้ติดตั้งแอปพลิเคชันที่ไม่รู้จัก (Install unknown apps) และใช้งาน Anti-virus software

ปัจจุบันแม้ว่าแนวโน้มการถูกมิจฉาชีพล่อลวงยังคงสูงขึ้นต่อเนื่อง แต่เมื่อเรามาถึงจุดนี้ที่มีผู้คนใช้ช่องทางดิจิทัลมาถึงระดับนี้แล้ว คงไม่สามารถกลับไปใช้ระบบเดิมได้ เราต้องอยู่กับมันให้ได้ ในฝั่งของธนาคารเองก็มีความเป็นห่วงและดำเนินการป้องกัน-แก้ไขมาโดยตลอด ขณะเดียวกันฝั่งผู้ทุจริตเองก็พยายามที่จะหาวิธีการที่ซับซ้อนมากขึ้นเรื่อยๆ

“ดังนั้น จึงต้องใช้ความร่วมมือจากทุกหน่วยงานที่เกี่ยวข้องเพื่อให้ทันต่อเล่ห์เหลี่ยมของมิจฉาชีพ ซึ่งจะเห็นได้จากปัจจุบันมิจฉาชีพจากเดิมที่ใช้การเจาะเข้าระบบต่างๆเพื่อขโมยข้อมูล มาเปลี่ยนเป็นการล่อลวงที่ตัวบุคคลแทน ดังนั้น ลูกค้าเองก็เป็นส่วนหนึ่งที่จะต้องพยายามศึกษาข้อมูลให้ทันที่สำคัญที่ต้องพิจารณาให้มากเมื่อจะกดเข้าลิงก์ หรือให้ข้อมูลส่วนใดๆ กับผู้ที่เราไม่รู้จักดี และมีสติในการทำธุรกรรมทางการเงิน อย่ารีบร้อน ก็จะตกเป็นเหยื่อได้ง่าย” .

นายกิตติ โฆษะวิสุทธิ์

มติชน
Matichon
Circulation: 950,000
Ad Rate: 1,200

Section: First Section/เศรษฐกิจ - ต่างประเทศ
วันที่: จันทร์ 13 กุมภาพันธ์ 2566
ปีที่: 46 **ฉบับที่:** 16409 **หน้า:** 8(ซ้าย)
Col.Inch: 19.11 **Ad Value:** 22,932 **PRValue (x3):** 68,796 **คลิป:** ขาว-ดำ
คอลัมน์: คอฟฟี่เบรก: สงสัยโดนแฮก!!

คอฟฟี่เบรก

สงสัยโดนแฮก!!

สำนักงานคณะกรรมการกิจการโทรคมนาคมแห่งชาติ (กสทช.) นับวันยิ่งเงียบเหงา กลายเป็นเมืองลับแล จนกระจิบข่าวเริ่มนั่งตบยุง รอข่าวเด็ดข่าวดังจากพี่ๆ กรรมการ กสทช.

เอ๊ะ หรือเพราะมีใบสั่งจากบิ๊ก กสทช.ห้ามพูด พรายกระซิบบอกให้เงียบไว้ก่อน เพราะอยากให้ข่าวไปในทิศทางเดียวกัน แต่อีกมุมถ้าไม่มีข่าวเลย ประชาชนจะรู้ได้ยังไงว่าพวกท่านกำลังทำอะไรกันอยู่...ฮิฮิ

ศ.ดร.พิรงรอง รามสูต

ล่าสุด กระจิบมือลั่นกดเข้าไปดูเฟซบุ๊กส่วนตัวของ **ศ.ดร.พิรงรอง รามสูต** กรรมการ กสทช. ด้านกิจการโทรทัศน์ ถึงกับตึกกะใจ เพราะโพสต์เก่าๆ ที่เจ้าตัวเคยชี้แจงทั้งประเด็นการควบรวมทรู-ดีแทค และบอลโลกต่างหายวับ เกลี้ยงงงง

เก็บความอยากรู้อยากเห็นไว้ในใจ จนมีโอกาสพูดคุยกับ อาจารย์พิรงรอง อดไม่ได้ขอถามเรื่องนี้ เพราะสงสัยจริงจิ๊ง

เจ้าตัวตอบไปขำๆ *"ไม่รู้วว่า สงสัยโดนแฮก"*

โถวววว่า พี่มาร์คไม่อ่อนโยนกับอาจารย์เลย ยังไงขอให้อาจารย์กู้ข้อมูลได้ไวๆ นะคร๊าบบ เชื่อว่าเอฟซีรออ่านอีกเย้อะ (ฮาาาา)