หน่วยการเรียนรู้ที่ 3 : การรับมือภัยคุกคามและการรักษาความปลอดภัยในโลกออนไลน์

ผู้สอน

อาจารย์วิศรุต ขวัญคุ้ม

หลักสูตรวิทยาการคอมพิวเตอร์ คณะวิทยาศาสตร์และเทคโนโลยี

ห้องพัก IT201 อาคารศูนย์ภาษา

วัตถุประสงค์

- สามารถอธิบายถึงทักษะในการรับมือกับการคุกคามทางโลกออนไลน์ และทักษะการรักษาความปลอดภัยของตนเองในโลกออนไลน์ได้
- มีความรู้ความเข้าใจเกี่ยวกับการรังแกกันผ่านโลกไซเบอร์
- มีความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัย
- สามารถป้องกันตนเองจากสถานการณ์การรังแกกันผ่านโลกไซเบอร์ได้
- สามารถป้องกันและรักษาความปลอดภัยของตนเองได้

การรับมือภัยคุกคามในโลกออนไลน์

- ความหมาย
- รูปแบบ
- ตัวอย่าง
- ผลกระทบ
- แนวทางการรับมือ

ภัยคุกคามในโลกออนไลน์ ?!?

ความหมาย

การรับมือภัยคุกคามในโลกออนไลน์ (Cyberbullying management) หรือ ความปลอดภัยทางดิจิตอล (Digital Safety)

- การรับมือกับปัญหาการกลั่นแกล้งบนโลกไซเบอร์ได้อย่างชาญฉลาด
- ทักษะในการบริหารจัดการความเสี่ยงในโลกออนไลน์
    - การไม่ไปรังแกและสามารถจัดการกับการถูกรังแกบนโลกไซเบอร์ (Cyberbullying) ได้อย่างตลอดรอดฝั่ง รวมไปถึงการเกี้ยวพาราสี การเหยียดผิว-เหยียดชนชั้น รวมไปถึงเนื้อหาต่างๆ ที่สุ่มเสี่ยงเช่น เนื้อหาที่มีความรุนแรง โป๊เปลือย ลามกหยาบคายด้วย

Cyberbullying คืออะไร ?

Cyberbullying คือ การรังแกของเด็กและเยาวชนในยุคไฮเทค เป็นกรณีพิพาทระหว่างเด็กกับเด็กด้วยกัน โดยที่ใช้เครื่องมือสื่อสารอย่างโทรศัพท์มือถือ แท็บเล็ต คอมพิวเตอร์ เชื่อมต่อเครือข่ายสังคมออนไลน์ ไม่ว่าจะเป็นเฟซบุ๊ก ทวิตเตอร์ อินสตาแกรม แชท หรือเว็บไซต์ต่าง ๆ เป็นเครื่องมือหลักในการรังแกและกลั่นแกล้งกัน โดยการกลั่นแกล้งนี้สามารถทำได้ 24 ชั่วโมง ต่างจากสมัยก่อนที่เด็ก ๆ จะรังแกกันได้ในโรงเรียนหรือแบบซึ่ง ๆ หน้าเท่านั้น

ผลลัพธ์ของการโจมตี

รูปแบบภัยคุกคาม

1. การโจมตี ขู่ทำร้าย หรือใช้ถ้อยคำหยาบคาย
2. การคุกคามทางเพศแบบออนไลน์
3. การแอบอ้างตัวตนของผู้อื่น
4. การแบล็กเมล์กัน
5. การหลอกลวง
6. การสร้างกลุ่มในโซเชียลเพื่อโจมตีโดยเฉพาะ

1. การโจมตี ขู่ทำร้าย หรือใช้ถ้อยคำหยาบคาย

การโพสต์ด่าทอ พูดจาส่อเสียด ให้ร้าย หรือขู่ทำร้าย ผ่านช่องทางการสนทนา หรือโพสต์ อย่างโจ่งแจ้งที่หน้าโซเชียลมีเดียของผู้ถูกกระทำ เช่น แชทเฟซบุ๊กหรือไลน์มาว่าจะดักทำร้าย เมื่อเจอหน้ากันที่โรงเรียนหรือที่ไหนก็ตาม เป็นต้น

2. การคุกคามทางเพศแบบออนไลน์

โดยการพูดจาคุกคามทางเพศผ่านโซเชียลมีเดีย การบังคับให้แสดงกิจกรรมทางเพศผ่านกล้อง การส่งภาพหรือวิดีโอโป๊เปลือยมาให้โดยที่ผู้รับไม่ได้ต้องการ การแฉหรือตัดต่อภาพโป๊เปลือยไปโพสต์ในโซเชียลเพื่อให้ได้รับความอับอาย เป็นต้น

3. การแอบอ้างตัวตนของผู้อื่น

โดยเฉพาะกรณีเปิดเผยรหัสผ่านของโซเชียลให้ผู้อื่นรู้ ยกตัวอย่างเช่น ให้เพื่อนสมัครเฟซบุ๊กหรือไลน์ให้ เคสนี้ก็อาจโดนรังแกด้วยการถูกสวมรอยใช้เฟซบุ๊กของตัวเองโพสต์ข้อความหยาบคาย ให้ร้ายบุคคลอื่น โพสต์รูปโป๊ คลิปวิดีโอลามก หรือสร้างความเสียหายในรูปแบบต่าง ๆ

4. การแบล็กเมล์กัน

โดยนำความลับหรือภาพลับของเพื่อนมาเปิดเผยผ่านเครือข่ายสังคมออนไลน์ มีการแชร์ต่อกันไปอย่างกว้างขวาง หรือการใส่ร้ายป้ายสี เช่น ตัดต่อรูปภาพน่าเกลียด ๆ หรือการแอบถ่ายภาพหลุดที่น่าขำมาโพสต์ประจาน และแสดงความคิดเห็นอย่างสนุกสนานเกินเลย

5. การหลอกลวง

มีทั้งการหลอกลวงให้หลงเชื่อ ล่อลวงให้ออกมานัดเจอเพื่อทำมิดีมิร้าย หรือการหลอกลวงให้ผู้เสียหายโอนเงินไปให้ด้วยวิธีการต่าง ๆ

6. การสร้างกลุ่มในโซเชียลเพื่อโจมตีโดยเฉพาะ

อย่างที่เราเห็นคนตั้งเพจแอนตี้ โจมตีบุคคลหนึ่งขึ้นมา มีการจับผิดทุกอิริยาบถ แล้วนำมาถกประเด็นให้เกิดความเสียหายต่อคนที่ตัวเองไม่ชอบ หรืออาจมีการโน้มน้าวให้คนอื่นรู้สึกรังเกียจ และกีดกันให้ออกจากกลุ่ม จากสังคมที่อยู่


REAKFAST

ผลกระทบจาก Cyberbullying มีอะไรบ้าง

- ผลกระทบจาก Cyberbullying ที่มีต่อเด็ก ๆ อาจมีตั้งแต่สร้างความรำคาญ ความเดือดเนื้อร้อนใจ บางคนรู้สึกเบื่อชีวิต ไม่อยากไปโรงเรียน ไม่อยากพบเจอใคร โดยมีเรื่องที่ถูกรังแกตามมาหลอกหลอนเป็นระยะ หรือบางรายอาจมีความเครียดอย่างหนัก ทำให้กินไม่ได้ นอนไม่หลับ และอาจร้ายแรงถึงขั้นไม่อยากมีชีวิตอยู่ เป็นผลให้รู้สึกอยากฆ่าตัวตาย
- ส่วนคนที่เป็นฝ่ายรังแก อาจมีความรู้สึกไม่สบายใจหรือเกิดความรู้สึกผิดกัดกินใจในภายหลังได้เช่นกัน แต่อย่างไรก็ดี ผลกระทบจาก Cyberbullying ไม่ว่าจะต่อผู้รังแกหรือผู้ถูกรังแกนั้นจะมากหรือน้อย ก็ขึ้นอยู่กับบุคลิกของแต่ละบุคคล รวมไปถึงทักษะการรับมือของแต่ละคนด้วย

สถิติที่น่าสนใจของ cyberbully

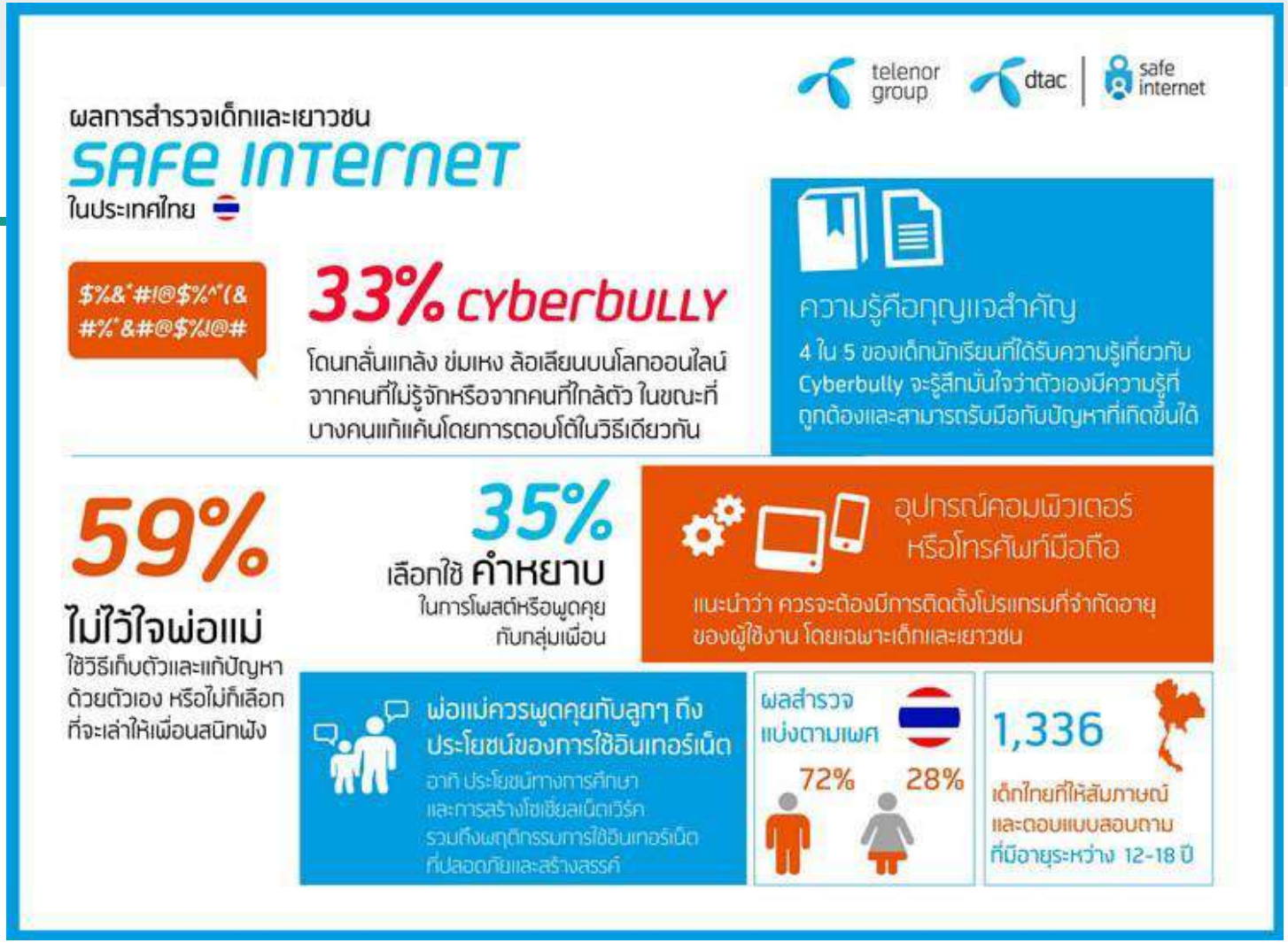
75% คือ อัตราการเข้าถึงอินเทอร์เน็ต
ของกลุ่มที่ใช้งานอินเทอร์เน็ตมากที่สุดคือ เด็กและเยาวชน อายุ 5-28 ปี
และใช้อินเทอร์เน็ตมากที่สุดถึง เกือบ 8 ชม.ต่อวัน

เด็กและเยาวชนไทย เจอภัยคุกคาม ล่อลวง
และการกลั่นแกล้งโรงเรียนและบนโลกอินเทอร์เน็ต
และเป็นอันดับต้นๆของเอเชีย **80%**

28%
ของเด็กไทย มองว่า
Cyberbullying
เป็นเรื่องปกติ

39%
ของเด็กไทย มองว่า
Cyberbullying
เป็นเรื่องสนุก

และกว่า
59%
ของเด็กไทย บอกว่า
“เคยเป็นส่วนหนึ่งในCyberbullying”


telenor group
dtac
safe internet
ผลการสำรวจเด็กและเยาวชน
SAFE INTERNET
ในประเทศไทย
$%&*#!@$%^*(&
#%*&#@$%!@#
33% CYBERBULLY
โดนกลั่นแกล้ง ข่มเหง ล้อเลียนบนโลกออนไลน์
จากคนที่ไม่รู้จักหรือจากคนที่ใกล้ตัว ในขณะที่
บางคนแก้แค้นโดยการตอบโต้ในวิธีเดียวกัน
ความรู้คือกุญแจสำคัญ
4 ใน 5 ของเด็กนักเรียนที่ได้รับความรู้เกี่ยวกับ
Cyberbully จะรู้สึกมั่นใจว่าตัวเองมีความรู้ที่
ถูกต้องและสามารถรับมือกับปัญหาที่เกิดขึ้นได้
59%
ไม่ไว้ใจพ่อแม่
ใช้วิธีเก็บตัวและแก้ปัญหา
ด้วยตัวเอง หรือไม่ก็เลือก
ที่จะเล่าให้เพื่อนสนิทฟัง
35%
เลือกใช้ คำหยาบ
ในการโพสต์หรือพูดคุย
กับกลุ่มเพื่อน
อุปกรณ์คอมพิวเตอร์
หรือโทรศัพท์มือถือ
แนะนำว่า ควรจะต้องมีการติดตั้งโปรแกรมที่จำกัดอายุ
ของผู้ใช้งาน โดยเฉพาะเด็กและเยาวชน
พ่อแม่ควรพูดคุยกับลูกๆ ถึง
ประโยชน์ของการใช้อินเทอร์เน็ต
อาทิ ประโยชน์ทางการศึกษา
และการสร้างโซเชี่ยลเน็ตเวิร์ค
รวมถึงพฤติกรรมการใช้อินเทอร์เน็ต
ที่ปลอดภัยและสร้างสรรค์
ผลสำรวจ
แบ่งตามเพศ
72%
28%
1,336
เด็กไทยที่ให้สัมภาษณ์
และตอบแบบสอบถาม
ที่มีอายุระหว่าง 12-18 ปี

สถิติเด็กไทย

1 ใน 3 ของเด็กไทยมีประสบการณ์
กลั่นแกล้งและถูกกลั่นแกล้งบนโลกออนไลน์

34.6 %
เคยแกล้งผู้อื่น

37.8 %
เคยถูกกลั่นแกล้ง

39 %
เข้าไปร่วมวง
ในเหตุการณ์กลั่นแกล้ง

สื่อสังคมออนไลน์ที่ใช้

96.59%	Facebook	29.44%	e-mail	14.42%	เกมออนไลน์
88.14%	Line	29.10%	Twitter	6.06%	Bee Talk
69.28%	YouTube	17.92%	Google+	4.52%	Whatapp
57.59%	Instagram	15.87%	Pantip	3.07%	Skype

การพบเห็นพฤติกรรม Cyberbullying

29.18%	การโพสต์ด่าทอ พูดจาส่อเสียด ให้ร้าย ดูถูก หรือข่มขู่ทำร้าย
17.04%	การแอบอ้าง การสวมรอย
14.30%	การหลอกลวง ล้อโกง ต้มตุ๋น
13.67%	การสร้างกลุ่มโซเชียลเพื่อโจมตีโดยเฉพาะ
11.39%	การแบล็กเมล์กัน
11.06%	การคุกคามทางเพศแบบออนไลน์
3.37%	ไม่เคยพบเห็นพฤติกรรม Cyberbullying

(ที่มาสถาบันแห่งชาติเพื่อการพัฒนาเด็กและครอบครัว มหาวิทยาลัยมหิดล)

สถิติ

- 75% คือ อัตราการเข้าถึงอินเทอร์เน็ต ของกลุ่มที่ใช้งานอินเทอร์เน็ตมากที่สุด คือ เด็กและเยาวชน อายุ 5-28 ปี และใช้อินเทอร์เน็ตมากที่สุดถึง เกือบ 8 ชม.ต่อวัน (ที่มา ผลสำรวจจากสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์)
- 80% ของเด็กและเยาวชนไทย เจอภัยคุกคาม ล่อลวงและการกลั่นแกล้งโรงเรียนและบนโลกอินเทอร์เน็ต และเป็นอันดับต้นๆของเอเชีย (ที่มา www.nobullying.com)
- 28% ของเด็กไทย มองว่า Cyberbullying เป็นเรื่องปกติ
- 39% ของเด็กไทย มองว่า Cyberbullying เป็นเรื่องสนุก
- กว่า 59% ของเด็กไทยบอกว่า “เคยเป็นส่วนหนึ่งใน Cyberbullying

วิธีรับมือกับ Cyberbullying

- อย่าเก็บเรื่องไว้คนเดียวเพราะจะเป็นการกดดันตัวเอง
- บันทึกหลักฐานไว้ฟ้อง (อ่านรายละเอียดเพิ่มเติมที่หัวข้อกฎหมายข้างล่าง)
- ถ้าโดนคุกคามถึงขั้นร้ายแรงก็อาจจะต้องเปลี่ยนเบอร์โทรศัพท์ อีเมล์ ที่อยู่
- เมื่อโดนกล่าวด่าแบบไม่มีเหตุผล ก็ไม่ควรไปสนใจ เพราะไม่มีเหตุผลที่เราจะต้องไปทะเลาะกับเขา ถึงแม้จะคุยกันไปก็ไม่รู้เรื่องกันอยู่ดีเพราะเขาไม่มีเหตุผล
- ห้ามส่งรูป หรือข้อมูลสำคัญ ลงบนอินเตอร์เนต ถึงแม้ว่าจะส่งแบบส่วนตัวก็ตาม ต้องคิดไว้เสมอว่ารูปพวกนี้มีโอกาสที่จะถูกเผยแพร่ได้


ไง
ไอ้อ้วน
เรียกมันแบบนี้
เดี๋ยวมันเสียใจหรอก
มันไม่อะไรหรอก
เล่นกันปกติ
เพื่อนกัน 55
ใช่ 555
555
555
ทำไมเราต้องเก็บความรู้สึก
เพื่อให้เพื่อนๆสบายใจวะ T_T


Bowie Hiyee
1 ชม.
คนที่ชอบเหยียดรูปลักษณ์คนอื่น แย่มากๆ
คิดว่าตัวเองสูงส่ง แต่จิตใจต่ำมาก
Bowie Hiyee เดี๋ยวนี้มีคนเอาอุรังอุตัง
มาปล่อยในเมืองด้วยเหรอ
ถูกใจ
#ข่าวลือน่าจัง บราๆๆๆ
มึงคนเดียวกัน
รึเปล่าวะ?


Bowie Hiyee
7 ชม.
เห็นกูแรงๆแบบนี้ ไม่ใช่ว่าได้กูง่ายๆนะ
fb.com/CostrostTH
Bowie Hiyee อยากโดนพี่เมฆเยบ้างจัง
เยดุมากๆ
ถูกใจ

อ้างอิง

- https://thumbsup.in.th/2016/10/how-digital-intelligence-important-for-all-children/
- https://mgronline.com/columnist/detail/9590000063569
- https://health.kapook.com/view150050.html
- http://www.js100.com/th/site/post_share/view/25700

การรักษาความปลอดภัยของตนเองในโลกออนไลน์

- ความหมาย
- องค์ประกอบของความมั่นคงปลอดภัย
- ภัยคุกคาม และช่องโหว่
- แนวทางการรักษาความมั่นคงปลอดภัยในไซเบอร์

ความหมาย

- Cybersecurity management มีความรู้ความเข้าใจและสามารถดูแลด้านความปลอดภัยของข้อมูลบนโลกไซเบอร์ได้ เช่น การสร้างพาสเวิร์ดที่เจาะได้ยาก หรือการรับมือกับภัยคุกคามบนโลกดิจิทัล
- ความปลอดภัยในโลกดิจิตอล (Digital security) ซึ่งหมายความถึง การมีความสามารถในการตรวจสอบเบื้องต้นว่าตนเองมีภัยคุกคามในโลกไซเบอร์หรือไม่ เช่น การแฮกบัญชีผู้ใช้อีเมล์ เฟซบุ๊ก เครื่องมือสื่อสารติดไวรัสคอมพิวเตอร์ มัลแวร์ ถูกขโมยรหัสผ่าน แฮกบัญชีธนาคาร ฯลฯ และครอบคลุมไปถึงการป้องกัน การหลีกเลี่ยง และจัดการอย่างถูกวิธีเมื่อเจอภัยคุกคามหรือถูกละเมิดความปลอดภัยด้วย

องค์ประกอบความมั่นคงปลอดภัยของสารสนเทศ

1. ความลับ (Confidentiality)
2. ความถูกต้อง ความสมบูรณ์ (Integrity)
3. ความพร้อมใช้ (Availability)

1. Confidentiality (ความลับ)

- เป็นการรับประกันว่า ผู้มีสิทธิ์และได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลได้
- สารสนเทศที่ถูกเข้าถึงโดยบุคคลที่ไม่มีสิทธิ์หรือไม่ได้รับอนุญาต จะถือเป็นสารสนเทศที่เป็นความลับถูกเปิดเผย ซึ่งองค์กรต้องมีมาตรการป้องกัน เช่น
  - การจัดประเภทของสารสนเทศ
  - การรักษาความปลอดภัยให้กับแหล่งข้อมูล
  - การกำหนดนโยบายความมั่นคงปลอดภัยและนำไปใช้งาน
  - การให้การศึกษาแก่ทีมงานความมั่นคงปลอดภัยและนำไปใช้

2. Integrity (ความถูกต้อง ความสมบูรณ์)

- ความครบถ้วนถูกต้อง และไม่มีสิ่งปลอมปน ดังนั้นสารสนเทศที่มีความสมบูรณ์จึงเป็นสารสนเทศที่นำไปใช้ประโยชน์ได้อย่างถูกต้องและครบถ้วน เช่น ถูกทำให้เสียหาย ไฟล์หาย เนื่องจา virus, worm หรือ Hacker ทำการปลอมปน สร้างความเสียหายให้กับข้อมูลองค์การได้ ยอดเงินในบัญชีธนาคารหรือแก้ไขราคาในการสั่งซื้อ

3. Availability (ความพร้อมใช้)

- สารสนเทศจะถูกเข้าใช้หรือเรียกใช้งานได้อย่างราบรื่น โดยผู้ใช้ระบบอื่นที่ได้รับอนุญาตเท่านั้น หากเป็นผู้ใช้ระบบที่ไม่ได้รับอนุญาต การเข้าถึงก็จะล้มเหลวถูกขัดขวาง เช่น การป้องกันเนื้อหางาน วิจัยในห้องสมุด เนื้อหางานวิจัยพร้อมที่ใช้ต่อผู้ใช้ที่ได้รับอนุญาต คือสมาชิกของห้องสมุดนั่นเอง ดังนั้น จึงต้องมีการระบุตัวตน (Identification) ว่าเป็นสมาชิกห้องสมุดและพิสูจน์ได้ว่าได้รับอนุญาตจริง (Authorization)


1 เงินดิจิทัล เป็นเป้าโจมตี
2 AI และ Machine Learning จะถูกใช้เป็นเครื่องมือโจมตี
3 การโจมตี Supply Chain กลายเป็นกระแสหลัก
4 มัลแวร์ไร้ไฟล์และที่เป็นลักษณะไฟล์ขนาดเล็กจะพุ่งสูงขึ้น
5 องค์กรจะยังคงวุ่นวายกับ Security ของ Software-as-a-Service (SaaS)
CYBERSECURITY PREDICTIONS 2018
6 องค์กรจะยังคงต่อสู้กับ Security ของ Infrastructure-as-a-Service (IaaS)
7 โทรจันการเงินจะยังคงสร้างความเสียหายมากกว่ามัลแวร์เรียกค่าไถ่
8 อุปกรณ์เครื่องใช้ IoT ราคาแพงภายในบ้านจะถูกเรียกค่าไถ่
9 อุปกรณ์ IoTจะถูกยึดครองและใช้เป็นฐานในการโจมตี DDoS
10 อุปกรณ์ IoT จะเปิดช่องทางเชื่อมต่ออย่างกาวรกับเน็ตเวิร์กภายในบ้าน
ที่มา: Symantec
https://www.symantec.com/blogs/feature-stories/2018-cyber-security-predictions
ETDA

Symantec คาดการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ในปี 2561

1. เงินดิจิทัลเป็นเป้าโจมตี แม้บล็อกเชนจะมีการนำไปใช้ในด้านอื่น ๆ นอกเหนือจากเรื่องเงินดิจิทัล แต่เรื่องเงินที่แลกเปลี่ยนบนบล็อกเชนและกระเป๋าเงินอิเล็กทรอนิกส์คือเป้าหมายของอาชญากรไซเบอร์ เหยื่อจะโดนหลอกให้ติดตั้งโปรแกรมขุดเหรียญในคอมพิวเตอร์และอุปกรณ์โมบาย และลักลอบนำพลังในการประมวลผลบนเครื่องที่ติดตั้งโปรแกรมไปใช้ในการก่ออาชญากรรมไซเบอร์ที่มีความรุนแรงขึ้น
2. จะถูกใช้เป็นเครื่องมือโจมตี โดยปกติแล้วเทคโนโลยี AI และ ML จะใช้ในการป้องกันและตAI และ Machine Learning รวจจับภัยคุกคาม แต่สถานการณ์นี้จะเปลี่ยนไปในปี 2561 เพราะกลุ่มอาชญากรไซเบอร์จะนำ AI และ ML มาประยุกต์ใช้ในการโจมตี และเป็นปีแรกที่เราจะเห็น AI ต่อสู้กับ AI ในบริบทของความมั่นคงปลอดภัยไซเบอร์ โดยอาชญากรไซเบอร์จะใช้ AI ในการโจมตีและลอบแฝงเข้าไปในเครือข่ายของเหยื่อหลังจากสามารถเจาะเข้าสู่ระบบ ซึ่งโดยปกติจะต้องใช้เวลาและคนจำนวนมาก

Symantec คาดการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ในปี 2561

3. การโจมตี Supply Chain กลายเป็นกระแสหลัก การโจมตี Supply Chain ไม่ใช่เรื่องใหม่ และเป็นการโจมตีที่ได้ผลเสมอ เพราะโจมตีผ่านคู่ค้าหรือพาร์ตเนอร์องค์กร ปัจจุบันมีข้อมูลสำคัญและกระบวนการมากมายบน Supply Chain อาชญากรไซเบอร์อาจเจาะข้อมูลผ่านคู่ค้าเพราะง่ายกว่าการเจาะเข้าระบบบริษัทใหญ่โดยตรง
4. มัลแวร์ไร้ไฟล์และที่เป็นลักษณะไฟล์ขนาดเล็กจะพุ่งสูงขึ้น ในระยะเวลา 2 ปีที่ผ่านมามีจำนวนมัลแวร์ไร้ไฟล์และมัลแวร์ที่เป็นลักษณะไฟล์ขนาดเล็กเพิ่มขึ้นอย่างต่อเนื่อง โซลูชันที่สามารถที่จะระบุการโจมตียังมีจำกัดและไม่สามารถตรวจจับมัลแวร์ไร้ไฟล์ได้ในทันที ซึ่งจะกลายภัยคุกคามและพุ่งสูงขึ้นในปี 2561 นี้

Symantec คาดการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ในปี 2561

5. องค์กรจะยังคงวุ่นวายกับ Security ของ Software-as-a-Service (SaaS) เป็นปัญหาที่องค์กรต้องเจอต่อไปในปี 2018 เพราะส่วนใหญ่อาศัยเครื่องมือดิจิทัลเพิ่มความคล่องตัวให้ธุรกิจในการทำ Digital Transformation และเคลื่อนย้ายข้อมูลไปไว้บนคลาวด์ ก่อให้เกิดความท้าทายด้านความมั่นคงปลอดภัย เช่น การควบคุมการเข้าถึงข้อมูล การควบคุมข้อมูล การติดตามพฤติกรรมของผู้ใช้ และการเข้ารหัสข้อมูลระหว่างแอปพลิเคชัน SaaS นอกจากนี้ยังมีกฎหมายคุ้มครองข้อมูลส่วนบุคคลฉบับใหม่ที่จะส่งผลทั่วโลก และมีผลกระทบที่สำคัญในแง่ของบทลงโทษและที่สำคัญกว่าคือความเสียหายต่อชื่อเสียงขององค์กร
6. องค์กรจะยังคงต่อสู้กับ Security ของ Infrastructure-as-a-Service (IaaS) แม้ IaaS จะเปลี่ยนวิถีระบบการทำงานเดิมอย่างสิ้นเชิง โดยเพิ่มความคล่องตัว ความสามารถในการสร้างสรรค์นวัตกรรม และความมั่นคงปลอดภัย แต่ความผิดพลาดเพียงเล็กน้อยอาจส่งผลให้เกิดการรั่วไหลของข้อมูลจำนวนมหาศาล และทำให้ทั้งระบบหยุดทำงานได้ และเนื่องจากการควบคุมแบบเดิมไม่ได้เหมาะกับสิ่งแวดล้อมที่อยู่บนระบบคลาวด์ การเพิกเฉยต่อการควบคุมแบบใหม่จะนำไปสู่การโจมตีมากขึ้นในปี 2561 ซึ่งจะทำให้องค์กรต้องดิ้นรนเปลี่ยนโปรแกรมด้านความมั่นคงปลอดภัยเพื่อให้ IaaS ทำงานได้อย่างมีประสิทธิภาพ

Symantec คาดการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ในปี 2561

7. เงินดิจิทัลเป็นเป้าโจมตี แม้บล็อกเชนจะมีการนำไปใช้ในด้านอื่น ๆ นอกเหนือจากเรื่องเงินดิจิทัล แต่เรื่องเงินที่โทรจันการเงินจะยังคงสร้างความเสียหายมากกว่ามัลแวร์เรียกค่าไถ่ โดยเปลี่ยนจากโจมตีบนคอมพิวเตอร์มาโจมตีผ่านมือถือที่มีประสิทธิภาพในการป้องกันภัยน้อยกว่า ซึ่งคาดว่าจะทำให้คนร้ายแสวงหากำไรได้มากขึ้นและสร้างความเสียหายได้มากกว่ามัลแวร์เรียกค่าไถ่ (Ransomware)
8. อุปกรณ์เครื่องใช้ IoT ราคาแพงภายในบ้านจะถูกเรียกค่าไถ่ แฮกเกอร์กำลังขยายการโจมตีด้วยมัลแวร์เรียกค่าไถ่ไปสู่ IoT ที่เชื่อมต่อกับอุปกรณ์เครื่องใช้ราคาแพงภายในบ้านซึ่งเพิ่มขึ้นจำนวนมาก ไม่ว่าจะเป็นสมาร์ตทีวี ของเล่นอัจฉริยะ หรืออุปกรณ์อัจฉริยะต่าง ๆ ซึ่งผู้ใช้ไม่ได้ตระหนักในเรื่องนี้

Symantec คาดการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ในปี 2561

9. อุปกรณ์ IoT จะถูกยึดครองและใช้เป็นฐานในการโจมตี DDoS โดยใช้ประโยชน์จากการตั้งค่าความมั่นคงปลอดภัยที่ไม่เข้มงวดและขาดการจัดการที่เหมาะสมของอุปกรณ์ IoT ภายในบ้าน โดยสามารถใช้การโจมตีเข้าควบคุมอุปกรณ์ด้วยการป้อนเสียง ภาพ หรือข้อมูลปลอมอื่น ๆ เพื่อสั่งให้อุปกรณ์เหล่านั้นทำตามคำสั่งของอาชญากรโจมตีลักษณะ DDoS ส่งผลให้ระบบที่เป็นเป้าหมายให้บริการช้าลง หรือหยุดให้บริการ
10. อุปกรณ์ IoT จะเปิดช่องทางเชื่อมต่ออย่างถาวรกับเน็ตเวิร์กภายในบ้าน จากการไม่ตระหนักถึงผลกระทบด้านความมั่นคงปลอดภัยไซเบอร์ของอุปกรณ์ IoT ภายในบ้าน ละทิ้งการตั้งค่ามาตรฐาน และไม่อัปเดตซอฟต์แวร์สม่ำเสมอเหมือนการใช้คอมพิวเตอร์ การเปิดช่องทางอย่างถาวรคือ ไม่ว่าจะแก้ไขโดยการล้างเครื่องหรือปกป้องคอมพิวเตอร์เท่าไร ผู้โจมตีก็ยังสามารถเข้าถึงเน็ตเวิร์กและระบบต่าง ๆ ผ่านช่องทางลับที่ถูกสร้างไว้

แนวทาง
การรักษาความมั่นคงปลอดภัยไซเบอร์

สำหรับบุคคลทั่วไป

1

หลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม
ไม่คลิกไฟล์แนบที่ไม่มั่นใจ

2

ไม่ใช้รหัสผ่านชุดเดียวกัน
กับทุกระบบ

3

พิจารณาข้อมูลก่อนการแชร์ต่อ
ไม่ส่งต่อข้อมูลที่ไม่ได้รับการยืนยัน
จากผู้เกี่ยวข้อง

สำหรับหน่วยงาน

1 ตรวจสอบ
และยืนยันสิทธิ์การเข้าระบบ

2 เพิ่มมาตรการป้องกันเว็บไซต์สำคัญ
โดยสามารถขอรับบริการได้ที่
ThaiCERT/ETDA

3 หลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม
ระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่าน
ช่องทาง Social Media

4 หากพบพิรุธว่าระบบถูกโจมตี
ให้ตรวจสอบข้อมูลการเข้าถึงระบบย้อนหลัง
เพื่อตรวจหาความผิดปกติในการเข้าถึงข้อมูล

5 ตั้งค่าระบบงานที่สำคัญ
ให้บันทึกเหตุการณ์ (Log)
การเข้าใช้งานระบบไม่ต่ำกว่า 90 วัน

6 ให้หน่วยงานส่งรายชื่อผู้ติดต่อ
(Contact Point)
กรณีเกิดเหตุภัยคุกคามไซเบอร์มายัง
ThaiCERT

แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับบุคคลทั่วไป

1. ระมัดระวังในการใช้อินเทอร์เน็ต โดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม ไม่คลิกไฟล์แนบจากผู้อื่นกรณีที่ไม่ได้ตกลงกันก่อนที่จะส่งให้ และโปรดระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่านโปรแกรม Internet Messaging หรือช่องทาง Social Media ทั้งนี้เพื่อหลีกเลี่ยงการติดมัลแวร์ เนื่องจากหลายครั้งพบว่ามัลแวร์มักจะถูกส่งมากับไฟล์แนบหรือจากเว็บไซต์ที่ไม่เหมาะสม
2. ไม่ใช้รหัสผ่านชุดเดียวกันกับทุกระบบ
3. ติดตามข้อมูลข่าวสารเกี่ยวกับความมั่นคงปลอดภัย และพิจารณาข้อมูลก่อนการแชร์ต่อ ตลอดจนไม่ส่งต่อข้อมูลที่ไม่ได้รับการยืนยันจากผู้เกี่ยวข้อง

แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงาน

1. ตรวจสอบและยืนยันสิทธิการเข้าระบบที่สำคัญของบัญชีผู้ใช้ให้สอดคล้องกับความจำเป็นเข้าถึงระบบและข้อมูล
2. เพิ่มมาตรการป้องกันเว็บไซต์สำคัญด้วยระบบการป้องกันการโจมตี เช่น Web Application Firewall หรือ DDoS Protection โดยสามารถขอรับบริการได้ที่ ThaiCERT/สพธอ.
3. แจ้งเจ้าหน้าที่ของหน่วยงานให้เพิ่มความระมัดระวังในการใช้อินเทอร์เน็ต โดยหลีกเลี่ยงการเข้าเว็บไซต์ที่ไม่เหมาะสม ไม่คลิกไฟล์แนบจากผู้อื่นกรณีที่ไม่ได้ตกลงกันก่อนที่จะส่งให้ และโปรดระมัดระวังความเสี่ยงจากการเปิดไฟล์ผ่านโปรแกรม Internet Messaging หรือช่องทาง Social Media ทั้งนี้เพื่อหลีกเลี่ยงการติดมัลแวร์ เนื่องจากหลายครั้งพบว่ามัลแวร์มักจะถูกส่งมากับไฟล์แนบหรือจากเว็บไซต์ที่ไม่เหมาะสม

แนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงาน

4. หากพบพิรุธว่าระบบถูกโจมตี เช่น ไม่สามารถเข้าใช้งานระบบ/เว็บไซต์ได้ หรือมีความล่าช้ากว่าปกติ ควรตรวจสอบข้อมูลการเข้าถึงระบบที่สำคัญ เช่น ข้อมูล Log ย้อนหลัง 30 วัน เพื่อตรวจหาความผิดปกติในการเข้าถึงข้อมูล
5. ตั้งค่าระบบงานที่สำคัญให้บันทึกเหตุการณ์ (Log) การเข้าใช้งานระบบไม่ต่ำกว่า 90 วัน หรือตามที่กฎหมายกำหนด
6. หากเป็นไปได้ ให้หน่วยงานส่งรายชื่อผู้ติดต่อ (Contact Point) กรณีเกิดเหตุภัยคุกคามไซเบอร์มายัง ThaiCERT

กรณีศึกษา

ข่าวกรณีศึกษา


แฉแหลก! บอยสกล หนุ่มลวงโลก
ปลอมตัวเรียน ม.ดัง - โกงเงิน


เพื่อนเก่าแฉ #บอยสกล
โกง 7แสนเผ่นจุฬา!


Wayar
@thewayar_
บอยสกล!!
แหกตาเรียนจุฬาฯ

ที่มา : https://youtu.be/hXgugK42xcw

อ้างอิง

https://thumbsup.in.th/2016/10/how-digital-intelligence-important-for-all-children/

https://mgronline.com/columnist/detail/9590000063569

http://jjsao.blogspot.com/2015/05/blog-post.html

https://www.etda.or.th/content/cybersecurity-predictions-2018-by-symantec.html

การบ้าน

1. ให้นักศึกษาหาข่าว สถานการณ์ เกี่ยวกับการถูกรังแกบนโลกไซเบอร์ โดยอธิบายถึงลักษณะการถูกรังแก
2. จากข้อ 1 ถ้าหากเหตุการณ์ดังกล่าวเกิดขึ้นกับเรา เราจะมีวิธีแก้ปัญหาอย่างไร เพื่อทำให้เหตุการณ์ดีขึ้น
3. จากข้อ 1 ถ้าหากเหตุการณ์ดังกล่าวไม่ได้เกิดขึ้นกับเรา จะมีวิธีป้องกันอย่างไร
4. ความเสี่ยงจากการใช้อินเตอร์เน็ตมีอะไรบ้าง (ยกตัวอย่างมา 5 ข้อ)
5. จะใช้สมาร์ตโฟนอย่างไรให้ปลอดภัยจากภัยความมั่งคงทางไซเบอร์ (ยกตัวอย่างมา 5 ข้อ)
6. ให้พิจารณาจากภาพกิจกรรมในเฟสบุคด้านล่าง นักศึกษาคิดว่ากิจกรรมที่เกิดขึ้นมีผลดีหรือผลเสียอย่างไรบ้าง

ตลาดนัดหมอดู
Follow · 1 hr ·

รหัสเอทีเอ็ม บ่งบอกนิสัยบ่งบอกให้ท่านรู้ว่าท่านจะรวยถาวร หรือว่ารวยแบบล้มละลาย เงินไหลเข้าไหลออก ปรึกษา รับออกแบบรหัสเอทีเอ็มสวยๆ

19 60 Comments

Like Comment Share

View 30 more comments

092215คะ
Like · Reply · 4m

419041
Like · Reply · 3m

0410
Like · Reply · 3m

703703 คะ
Like · Reply · 2m

192021
Like · Reply · 2m

230643

Write a comment...