การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ Cybersecurity Awareness

Cybersecurity คืออะไร

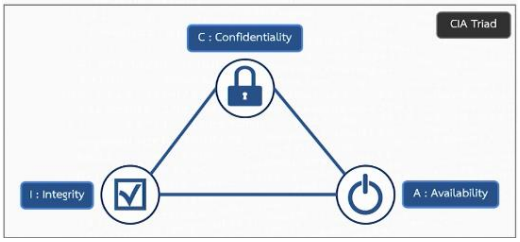
Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยีและกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบหรือโปรแกรมที่อาจจะเกิดความเสียหายจากการที่ถูกเข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต ในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อยๆ

กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

- พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ. ศ. 2562
- พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ. ศ. 2560
- พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล
- มาตรฐานด้านความปลอดภัย ISO 27001 (ระบบบริหารจัดการความปลอดภัยของข้อมูล)

ความรู้พื้นฐานของ Cybersecurity

พื้นฐานของหลักการปฏิบัติเพื่อความมั่นคงปลอดภัยทางไซเบอร์ CIA Triad หรือ CIA Model ซึ่งประกอบด้วยตัวซี(C) ตัวไอ(I) และตัวเอ(A)



C:Confidentiality หรือ การรักษาความลับของข้อมูล คือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น

- ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็น ความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น
- เบอร์โทรของพนักงานในบริษัท จัดเป็น ข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ พนักงานบริษัททุกคน

I: Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบบสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น

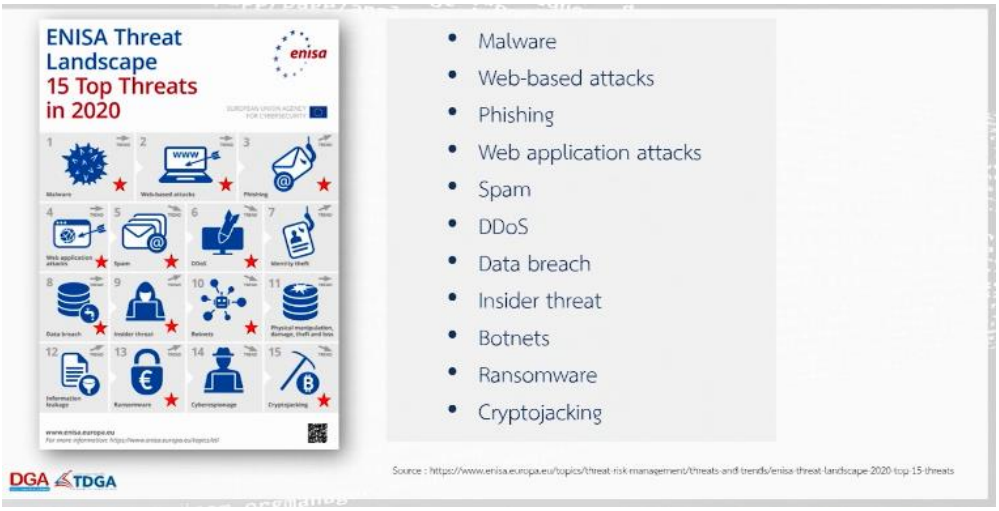
- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

A:Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ตัวอย่างเช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

สรุปคือ CIA Model สามารถนำมาปรับใช้ให้เข้ากับส่วนของข้อมูลที่อยู่บนระบบคอมพิวเตอร์ได้

รูปแบบภัยคุกคามของ Cybersecurity



ในภาพคือตัวอย่างจาก ENISA คือ องค์กรของฝั่งยุโรปที่ดูแลเรื่องภัยคุกคามทางไซเบอร์ สรุป 15 ภัยคุกคามที่เกิดขึ้นในปี 2020

Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่างๆได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง

- ไวรัส (Virus)
- เวิร์ม (Worms)
- โทรจัน (Trojans)

Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ Code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

เพิ่มเติม : เว็บไซต์ส่วนใหญ่ที่โดน Hack เพื่อแก้ไข Code ส่วนมากจะเป็นเว็บไซต์ประเภท CMS (Content Management System)

Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่างๆเช่น E-Mail,SMS,เว็บไซต์ หรือ ช่องทาง Social โดยใช้วิธีหลอกล่อเหยื่อด้วยวิธีการต่างๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือ ข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

Web application attack คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆเช่น

- Code ของเว็บไซต์ เช่น CMS
- Web Server หรือ Database Server

วิธีการโจมตีที่นิยมใช้

- Cross-Site Scripting
- SQL injection
- Path Traversal

สามารถศึกษาวิธีการป้องกันเพิ่มเติมได้จากมาตรฐาน OWASP Top Ten

Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่างๆ ผ่านช่องทางต่างๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับเพื่อสร้างความรำคาญหรือก่อกวน

DDos (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการ หรือ ระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกัน จุดประสงค์ที่ทำเพื่อให้เว็บไซต์, ระบบการให้บริการ ระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

Data Breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์, ข้อมูลของแอปพลิเคชั่น หรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการ แอปพลิเคชั่น หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ

ผลกระทบ

- ข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปเผยแพร่
- ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล
- สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

Inside threat คือ ภัยที่เกิดจากภายในบุคลากรภายในองค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น

ซึ่ง Inside threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

วิธีการป้องกัน

นำหลักการ Zero Trust มาใช้ภายในองค์กร Zero Trust เป็นคอนเซปต์การจัดการซิเคียวริตี้สมัยใหม่ ที่หลายองค์กรได้นำมาปรับใช้ ตั้งแต่การตรวจสอบผู้เข้าระบบทุกครั้ง การให้สิทธิ์ที่น้อยที่สุดหรือเท่าที่จำเป็นกับผู้ใช้งาน

Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

วิธีการป้องกัน

-สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล

-ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ

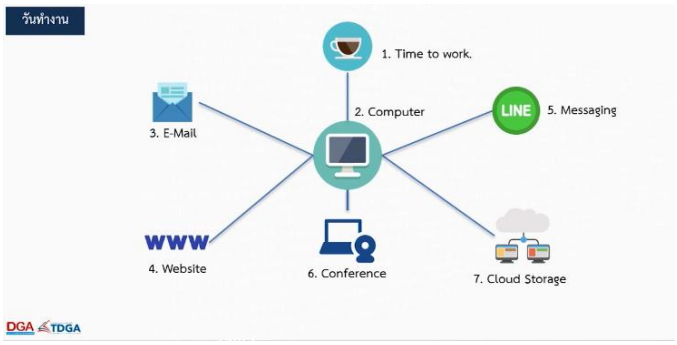
-ก่อนเปิดไฟล์ต่างๆ ที่ได้รับมา ควรมีความตระหนักก่อนที่จะทำการเปิด

Cryptocurrency คือเหรียญดิจิตอล ซึ่งเหรียญดิจิตอลจะมีการประมวลผลตลอดเวลาซึ่งในการประมวลผลจำเป็นที่จะต้องใช้ในส่วนของ CPU หรือ GPU หรือการ์ดจอบนเครื่องคอมพิวเตอร์ทำการประมวลผล และหลังจากประมวลผลเสร็จแล้วเรียบร้อยก็จะส่งกลับไปที่ส่วนกองส่วนกลางของเหรียญนั้นๆ เพื่อที่จะได้รับค่าตอบแทนในการประมวลผล

เครื่องที่ติด Cryptojacking จะเห็นว่าบางที CPU หรือ GPU เราขึ้นไปถึง 100 เปอร์เซ็นต์โดยที่เรายังไม่ได้ใช้งานอะไรเลยให้ลองเช็คดูอาจจะเกิดจาก Cryptojacking

ความตระหนักรู้ด้าน Cyber security ในชีวิตประจำวัน

- วันทำงาน
- วันพักผ่อน



วันทำงาน

1. Time to work
2. Computer
3. E-mail
4. Website
5. Messaging
6. Conference
7. Clould Storage

Computer

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ควรมีการแยก user ใช้งานกันของแต่ละบุคคล
2. ควร logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
3. ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
4. มีการอัพเดท Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
5. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
6. ไม่ควรจด password และติด password ไว้ที่หน้าจอ
7. มีการใช้ password ที่ดีและไม่ควรบอก password แก่ผู้อื่น

Password

การใช้ Password ที่ดี คือ

1. มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ

2. มีความยาวของ Password อย่างน้อย 8 ตัวอักษร

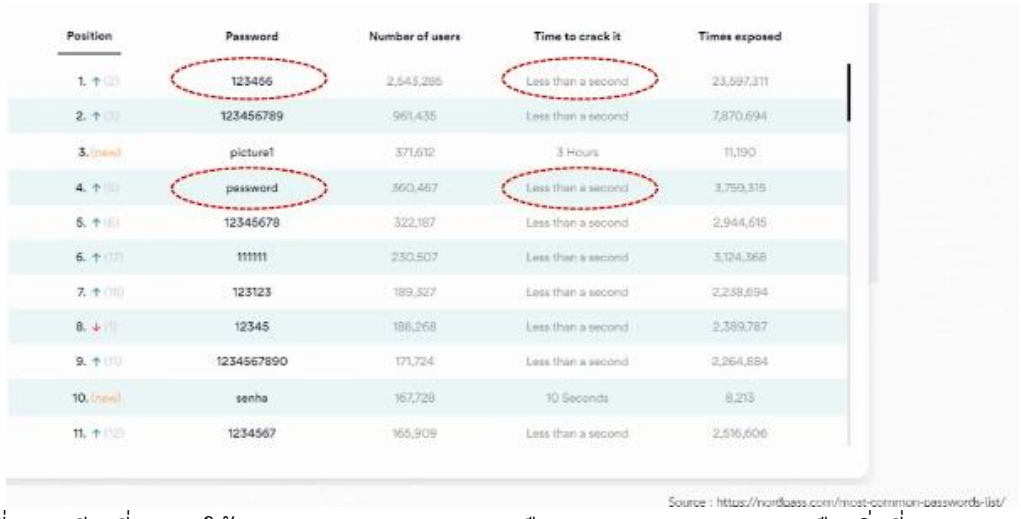
3. ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดาได้ง่าย เช่น password,123456,วันเกิด,หมายเลขโทรศัพท์

4. มีการเปลี่ยน Password อย่างสม่ำเสมอ

5. ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้

6. ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ

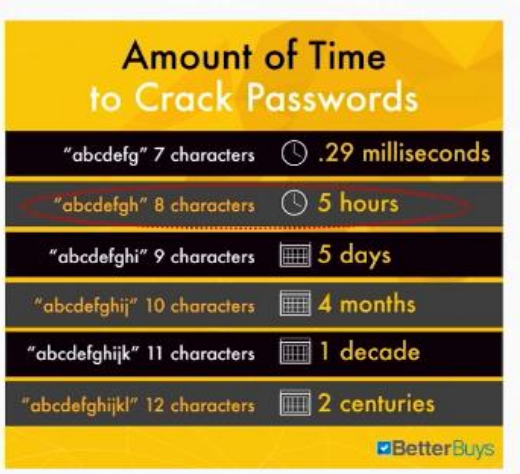
7. ไม่ควรบอก Password แก่ผู้อื่น



Position	Password	Number of users	Time to crack it	Times exposed
1. ↑ (2)	123456	2,643,286	Less than a second	23,697,311
2. ↑ (3)	123456789	961,435	Less than a second	7,870,694
3. (new)	picture1	371,612	3 Hours	11,190
4. ↑ (5)	password	360,467	Less than a second	3,759,315
5. ↑ (6)	12345678	322,187	Less than a second	2,944,615
6. ↑ (17)	111111	230,507	Less than a second	3,124,368
7. ↑ (18)	123123	189,327	Less than a second	2,238,694
8. ↓ (1)	12345	188,268	Less than a second	2,389,787
9. ↑ (10)	1234567890	171,724	Less than a second	2,264,884
10. (new)	senha	167,728	10 Seconds	8,213
11. ↑ (12)	1234567	165,909	Less than a second	2,516,606

Source : https://nordpass.com/most-common-passwords-list/

เหตุผลที่ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือ สิ่งที่สามารถคาดเดาได้ง่าย เช่น password,123456,วันเกิด,หมายเลขโทรศัพท์



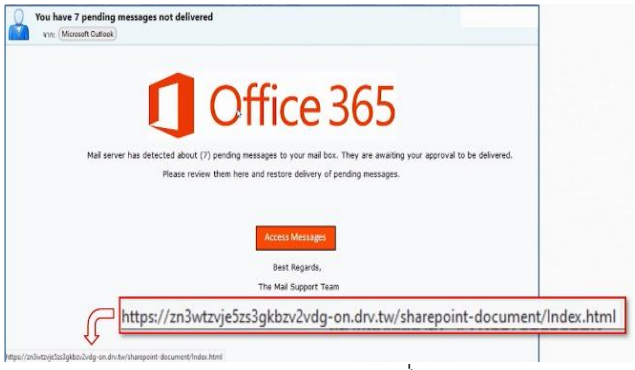
เหตุผลที่ต้องมีความยาวของ Password อย่างน้อย 8 ตัวอักษร

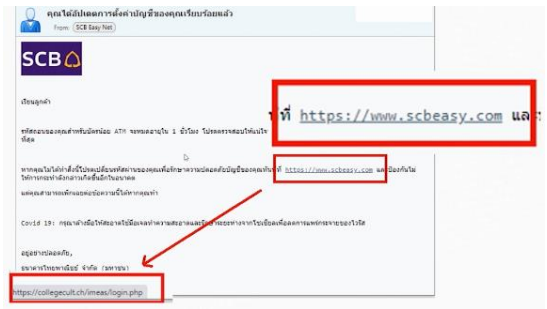
E-mail

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

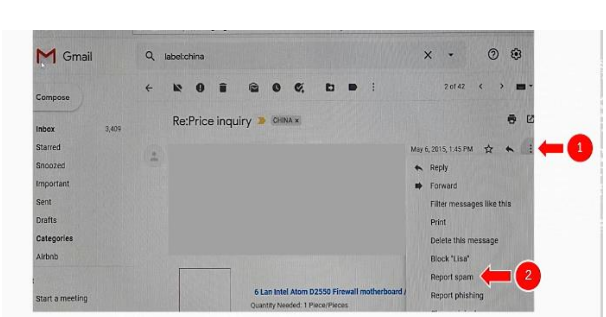
1. ไม่เปิด E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน
2. ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน
3. ไม่คลิกลิงก์ใน E-mail โดยไม่มีการตรวจเช็ค
4. เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่างๆ ควรมีการเช็คผ่านทางช่องทางอื่นๆ เพิ่มเติม

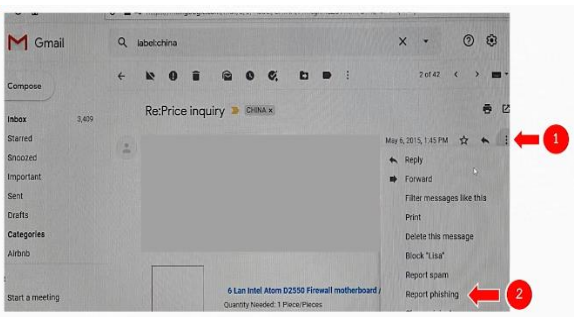
เหตุผลที่ไม่เปิด E-mail ที่น่าสงสัยหรือผู้ส่งไม่ชัดเจน





เหตุผลที่ไม่คลิกลิงก์ใน E-mail โดยไม่มีการตรวจเช็ค





Gmail-Report Spam Mail /Gmail-Report Phishing Mail

Website

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง social ต่างๆ

2. ไม่ควรทำการบันทึก Password ต่างๆบน Browser

3. เว็บไซต์สำหรับการทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น

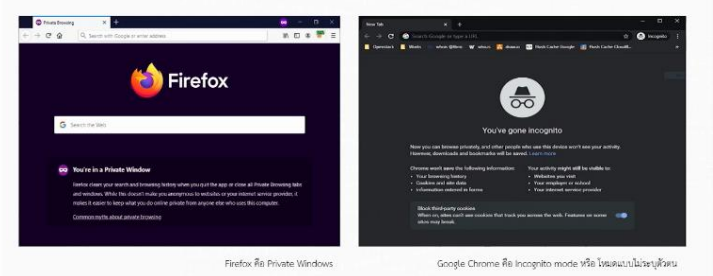
4. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งานเช่น google chrome mozilla firefox เป็นต้น

5. ควรมีการอัพเดทเวอร์ชั่นของ Browser อย่างสม่ำเสมอ

6. ในกรณีที่เครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน browser ในโหมด safe web browsing

7. ควรติดตั้ง anti-malware และ update อย่างสม่ำเสมอ

เว็บไซต์สำหรับการทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น



ในกรณีที่เครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน browser ในโหมด safe web browsing

ตัวอย่าง Facebook ที่ผ่านการยืนยันความถูกต้อง

Messaging

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ไม่ควรบันทึก password ไว้ที่โปรแกรม
2. กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัวไม่ ควรบันทึกไฟล์ต่างๆ ไว้บนเครื่อง
3. มีความตระหนักก่อนเปิดลิงค์หรือไฟล์ต่างๆที่ได้รับมา
4. มีการอัพเดทเวอร์ชั่นของโปรแกรมอย่างสม่ำเสมอ

เพิ่มเติม : ไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆโดยไม่ทราบที่มาของข้อมูล

Fake News

Fake News หรือ ข่าวปลอมเป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวปลอมที่นำมาเผยแพร่นั้นดูมีความน่าเชื่อถือจึงทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแส ปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ทางช่องทางออนไลน์ เช่น LINE,Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น

วิธีการสังเกตข่าวปลอม

1. มีการพาดหัวข่าว หรือข้อความที่เกินจริง เพื่อสร้างความน่าสนใจ
2. ระบุที่มาของข่าวไม่ได้
3. มักจะไม่ระบุวันที่ และเวลาที่เกิดเหตุการณ์
4. สำนวนการเขียนออกแนวการโฆษณา

ที่มา http://www.antifakenewcenter.com

Line Official Account

ชนิดของบัญชี Line Official Account

Conference

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

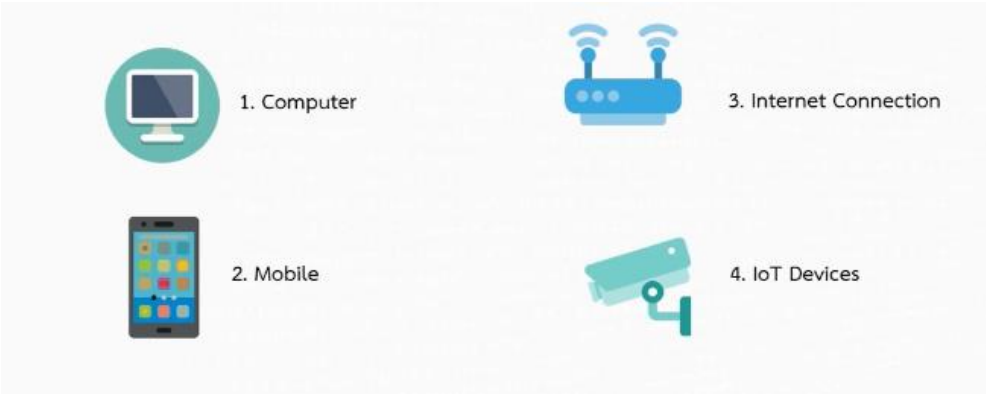
1. ใช้สถานที่เหมาะสมกับการ Conference
2. ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง
3. แชร์เอกสารต่างๆ อย่างระมัดระวัง
4. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน
5. มีการอัพเดทเวอร์ชั่นของโปรแกรม Conference อย่างสม่ำเสมอ

เพิ่มเติม : ควรมีการขออนุญาตผู้เข้าร่วมประชุม Conference ก่อนที่จะบันทึกภาพและเสียงในการประชุม

Cloud Storage

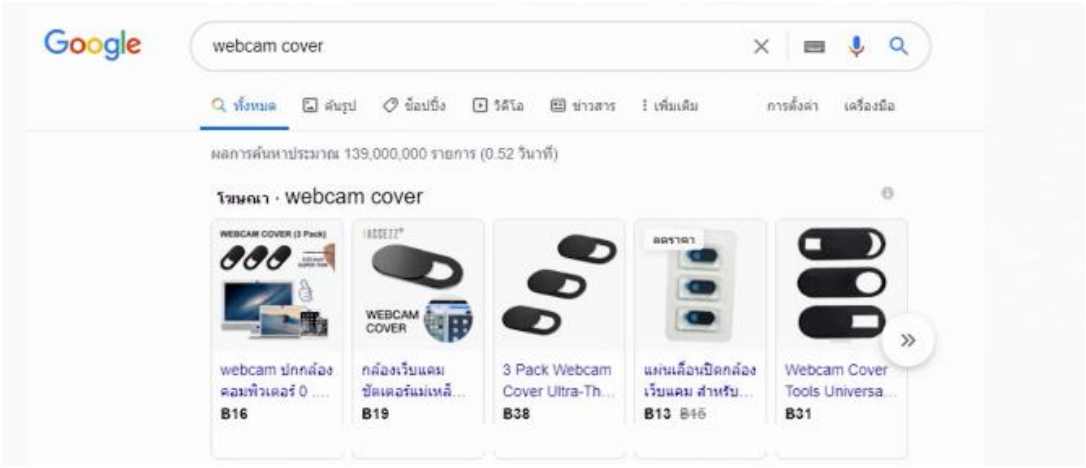
สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. แยก User ในการใช้งานของแต่ละบุคคล
2. ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น
3. ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น
4. ควรติดตั้ง anti-malware และ update อย่างสม่ำเสมอ
5. มีการอัพเดทเวอร์ชั่นของโปรแกรมอย่างสม่ำเสมอ
6. มีการตั้ง Password ที่ดีและไม่บอก Password แก่ผู้อื่น



วันพักผ่อน

1. Computer
2. Mobile
3. Internet Connection
4. IoT Devices



-Webcam Cover

Computer

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ควรมีการแยก User ใช้งานกันของแต่ละบุคคล
2. ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
3. ควรติดตั้ง anti-malware และมีการอัพเดตอย่างสม่ำเสมอ
4. มีการอัพเดท Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
5. มีการอัพเดทเวอร์ชั่นของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
6. ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ
7. มีการใช้ Password ที่ดีและไม่ควรบอก Password แก่ผู้อื่น

Free WIFI

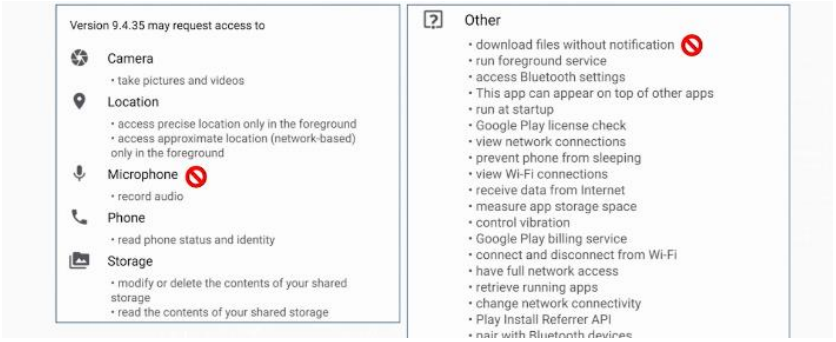
สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ไม่ควรใช้งาน WiFi ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน
2. หลีกเลี่ยงการใช้งาน WiFi ที่ไม่รู้ที่มาในการให้บริการ

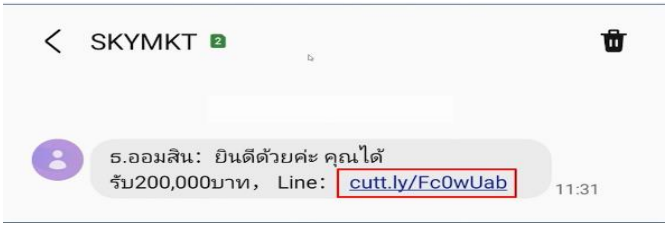
Mobile

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. เปิดการใช้งาน PIN/Password,Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์
2. ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา
3. กำหนด Application permission ให้เหมาะสม
4. มีการอัพเดท Patch ระบบปฏิบัติการ (OS) อย่างเหมาะสม
5. มีการอัพเดทเวอร์ชั่นของโปรแกรมบนเครื่องอย่างสม่ำเสมอ



กำหนด Application permission ให้เหมาะสม



SMS หลอกลวง

Internet Connection

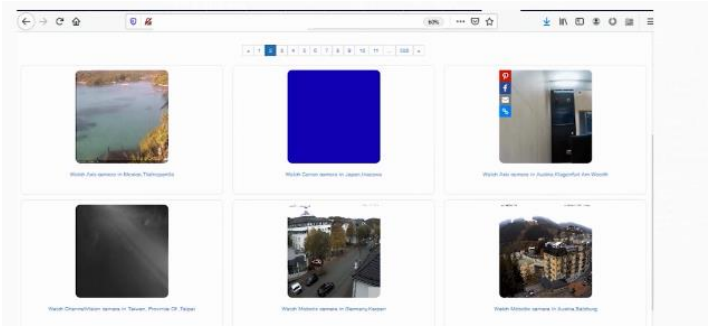
สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. เปลี่ยน Default Password ของ Router ที่มาจากโรงงาน
2. เปลี่ยน SSID และรหัสผ่านของ WiFi ที่กำหนดมาจากผู้ให้บริการ
3. กำหนดผู้ที่สามารถเข้าใช้งานอินเทอร์เน็ตเท่าที่จำเป็น

IoT Devices คือ อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตเพื่อใช้ในการทำงานร่วมกับระบบต่างๆ หรือ Application ต่างๆ ได้ เช่น หลอดไฟ,พัดลม,เครื่องกรองอากาศ ซึ่งเมื่อสามารถต่อกับเครือข่ายได้ก็จำเป็นที่จะต้องมีความปลอดภัยทางด้านเครือข่าย เปรียบได้กับเป็นคอมพิวเตอร์ขนาดจิ๋ว

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. เปลี่ยน Default Password ที่มาจากโรงงาน
2. ควรมีการอัพเดทเฟิร์มแวร์ให้เป็นเวอร์ชั่นล่าสุด
3. ใช้ application ที่ใช้ในการคอนโทรลกับอุปกรณ์ต่างๆให้เป็นเวอร์ชั่นล่าสุด



กล้องวงจรปิดที่ดูผ่านอินเตอร์เน็ตควรมีการเปลี่ยน password ที่ไม่ใช่ default password จากโรงงาน

ตัวอย่าง IoT Devices เช่น เตาแม่เหล็กไฟฟ้ารุ่นใหม่ต้องต่อกับสมาร์ทโฟนเพื่อทำการคอนโทรล

สรุปเรื่องการสร้างความตระหนักรู้ความมั่นคงทางไซเบอร์ในส่วนของความปลอดภัยกับความสะดวกสบาย ตัวอย่างในรูปจะให้เห็นว่าสิ่งที่เราต้องทำคือเราต้องพยายามถ่วงน้ำหนักให้เท่ากันในส่วนของเรื่องความปลอดภัยทางด้านไซเบอร์ซีเคียวริตี้และความสะดวกสบาย หลักสูตรนี้น่าจะสร้างความตระหนักรู้ความมั่นคงทางไซเบอร์ให้ทุกท่านได้เห็นภาพมากยิ่งขึ้นและในหลายๆส่วนอยากจะให้ทุกท่านนำไปปฏิบัติตามเพื่อความปลอดภัยในชีวิตประจำวัน

การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์ Cybersecurity Awareness

รายละเอียดบทเรียน

คำอธิบายบทเรียน

เรียนรู้เกี่ยวกับภัยคุกคามไซเบอร์ที่เกิดขึ้นในการทำงานและมีความรู้เกี่ยวกับวิธีการป้องกันภัยคุกคามไซเบอร์ให้ปลอดภัยจากภัยคุกคามไซเบอร์รูปแบบต่าง ๆ และสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวัน

วัตถุประสงค์

1. เพื่อให้ผู้เรียนมีความตระหนักรู้ถึงภัยคุกคามไซเบอร์ที่เกิดขึ้นในปัจจุบัน
2. เพื่อให้ผู้เรียนมีความรู้เกี่ยวกับภัยคุกคามประเภทต่างๆและแนวทางป้องกันแก้ไข
3. เพื่อให้ผู้เรียนสามารถนำความรู้ไปประยุกต์ใช้ในการทำงานและชีวิตประจำวันได้

หัวข้อในบทเรียน

- แนะนำบทเรียน
- Cybersecurity คืออะไร
- ความรู้พื้นฐานของ Cybersecurity
- รูปแบบภัยคุกคามของ Cybersecurity
- ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

ระยะเวลา

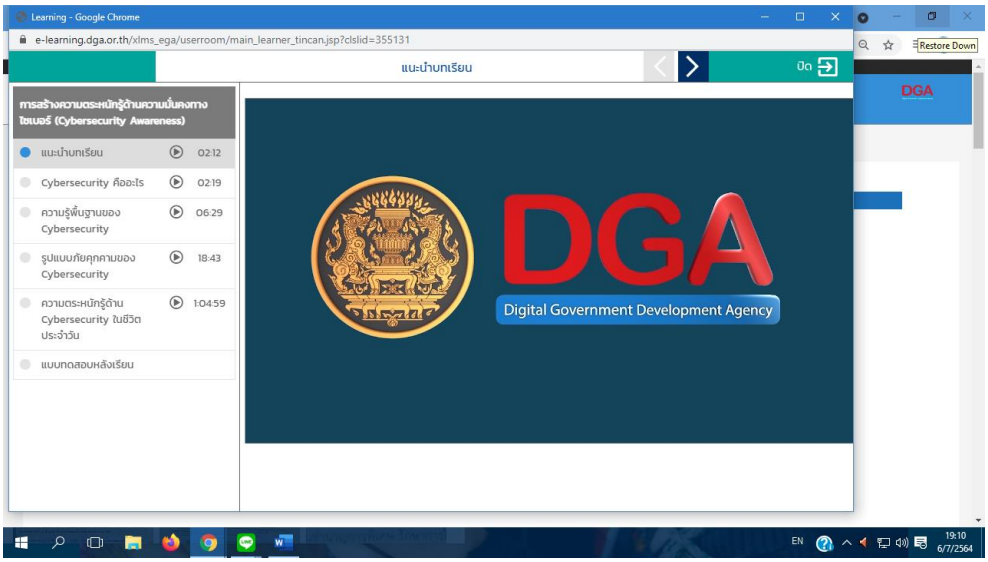
1 : 30 ชม.

ผู้สอน

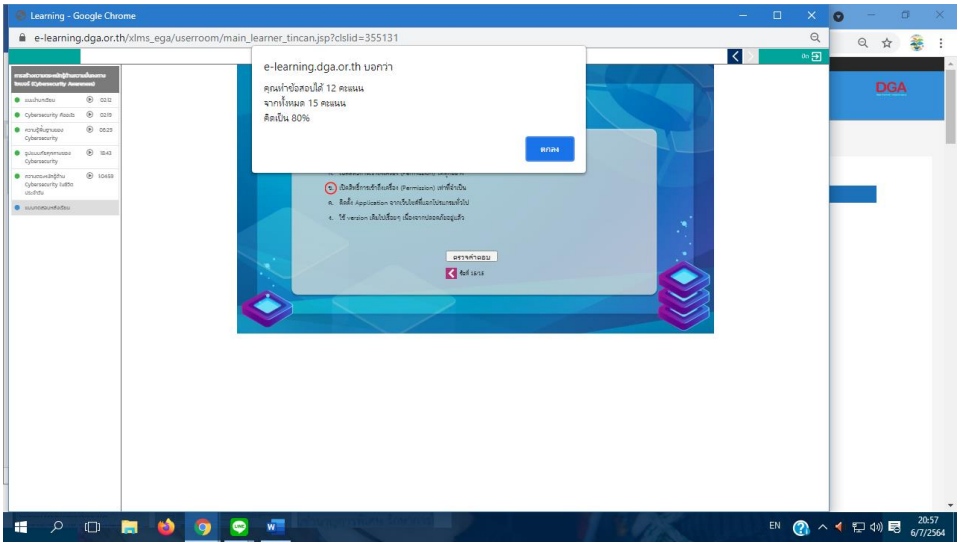
คุณพลากร ลาภอลงกรณ์

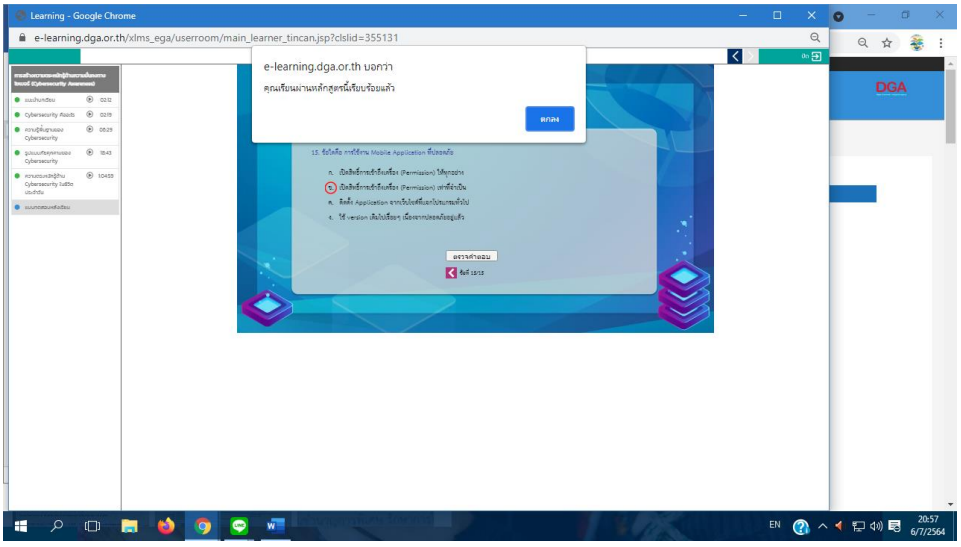
ผู้จัดการส่วนบริการลูกค้า ฝ่ายปฏิบัติการ

สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)




Learning - Google Chrome
e-learning.dga.or.th/xlms_ega/userroom/main_learner_tincan.jsp?clslid=355131
DGA
การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์
(Cybersecurity Awareness)
DGA
TDGA


Learning - Google Chrome
e-learning.dga.or.th/xlms_ega/userroom/main_learner_tincan.jsp?clslid=355131
e-learning.dga.or.th บอกว่า
คุณทำข้อสอบได้ 12 คะแนน
จากทั้งหมด 15 คะแนน
คิดเป็น 80%
ตกลง


Learning - Google Chrome
e-learning.dga.or.th/xlms_ega/userroom/main_learner_tincan.jsp?clslid=355131
e-learning.dga.or.th บอกว่า
คุณเรียนผ่านหลักสูตรนี้เรียบร้อยแล้ว
ตกลง

DGA TDGA

ประกาศนียบัตร

ให้ไว้เพื่อแสดงว่า

นางสาวอัญชลี บุญมีประภา

ได้ผ่านการอบรมด้วยระบบการเรียนออนไลน์ในบทเรียน
การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์
Cybersecurity Awareness

รวมระยะเวลาทั้งสิ้น 1 : 30 ชั่วโมง

โดยสถาบันพัฒนาบุคลากรภาครัฐด้านดิจิทัล
ภายใต้การดำเนินงานของสำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)
ให้ไว้ ณ วันที่ 6 กรกฎาคม 2564

(นางไอรดา เหลืองวิไล)

กรณีมีข้อสงสัยเพิ่มเติมหรือติดปัญหา

สอบถามได้ที่

contact@dga.or.th

DGA TDGA