

การสร้างตระหนักรู้ด้านความมั่นคงทางไซเบอร์  
(Cybersecurity Awareness)

คุณพลกร สากองกรณ์  
ผู้จัดการส่วนบริการลูกค้า  
สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน)  
Digital Government Development Agency (Public Organization)

DGA TDGA

Cybersecurity  
คืออะไร?

## Cybersecurity คือ ?

Cybersecurity หรือ ความมั่นคงปลอดภัยไซเบอร์ คือ การนำเครื่องมือทางด้านเทคโนโลยี และกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกันและรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ระบบ หรือโปรแกรมที่อาจเกิดความเสียหายจากการที่ผู้เข้าถึงจากบุคคลที่สามโดยไม่ได้รับอนุญาต

ในปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลายมากยิ่งขึ้น และสร้างความเสียหายให้กับองค์กรเพิ่มมากขึ้นเรื่อยๆ

## กฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

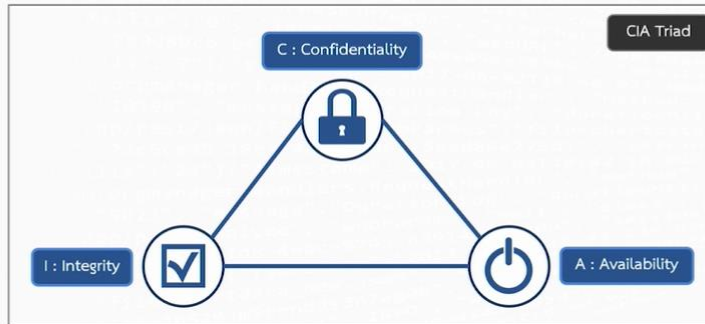
### ตัวอย่างกฎหมายและมาตรฐานที่เกี่ยวข้องกับความปลอดภัยทางไซเบอร์

- 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

**Confidentiality** หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุด ข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น

- ข้อมูลส่วนเงินเดือนของพนักงานในบริษัท จัดเป็น **ความลับสูงสุด** ผู้ที่สามารถเข้าถึงได้ คือ **ผู้จัดการส่วนทรัพยากรบุคคลเท่านั้น**

### CIA Triad (2)

**Integrity** หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร

### CIA Triad (3)

**Availability** หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล ตัวอย่างเช่น

- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์



รูปแบบภัยคุกคามของ Cybersecurity

ENISA Threat Landscape  
15 Top Threats in 2020

Source : <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape-2020-top-15-threats>

- Malware
- Web-based attacks
- Phishing
- Web application attacks
- Spam
- DDoS
- Data breach
- Insider threat
- Botnets
- Ransomware
- Cryptojacking

Source : <https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape-2020-top-15-threats>

ประเภท : ภัยคุกคามทางไซเบอร์, ภัยคุกคามทางเทคโนโลยีสารสนเทศ, ภัยคุกคามทางเศรษฐกิจ, ภัยคุกคามทางสังคม, ภัยคุกคามทางสุขภาพ

- ภัยคุกคามทางไซเบอร์
- ภัยคุกคามทางเทคโนโลยีสารสนเทศ

## รูปแบบภัยคุกคามของ Cybersecurity

### Malware

**Malware** คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแจ้งข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่างๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง

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

### Web-based attacks

**Web-based attacks** คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปเป้าหมายปลายทางที่เป็น เว็บไซต์ที่ทำการวาง Malware ไว้เพื่อให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

#### เพิ่มเติม

เว็บไซต์ส่วนใหญ่ที่โดน Hack เพื่อแก้ไข Code ส่วนมากจะเป็นเว็บไซต์ประเภท CMS (Content Management System)

ประเภทของภัยคุกคาม Hack ที่พบได้บ่อย เช่น การโจมตีระบบความปลอดภัยของเว็บไซต์ (OWASP Top 10 Security Vulnerabilities)

## รูปแบบภัยคุกคามของ Cybersecurity

### Phishing

**Phishing** คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่างๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่างๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือ ข้อมูลสำคัญอื่นๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

### Web application attacks

**Web application attacks** คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่างๆ เช่น

- Code ของเว็บไซต์ เช่น CMS
- Web Server หรือ Database Server

วิธีการโจมตีที่นิยมใช้

- Cross-Site Scripting
- SQL Injection
- Path Traversal

สามารถศึกษาวิธีการป้องกันเพิ่มเติมได้จากมาตรฐาน OWASP Top Ten

## รูปแบบภัยคุกคามของ Cybersecurity

### Spam

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

### DDoS

DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกันจุดประสงค์ที่ ทำให้เว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม



## รูปแบบภัยคุกคามของ Cybersecurity

### Data breach

Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์, ข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่างๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชัน หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้นๆ

#### ผลกระทบ

- ข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปเผยแพร่
- ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล
- สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

### Insider threat

Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจเกิดจากความตั้งใจ หรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

#### วิธีการป้องกัน

นำหลักการ Zero Trust มาใช้งานภายในองค์กร



### รูปแบบภัยคุกคามของ Cybersecurity

#### Botnets

**Botnets** หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัว อยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่างๆ เพื่อรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้

ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

#### Ransomware

**Ransomware** คือ Malware ประเภทหนึ่งที่ถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อกไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อกไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อกไฟล์เพื่อให้ไฟล์ที่อยู่ในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

**วิธีการป้องกัน**

- สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล
- ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
- ก่อนเปิดไฟล์ต่างๆ ที่ได้รับมา ควรความตระหนักก่อนที่จะทำการเปิด



### รูปแบบภัยคุกคามของ Cybersecurity

#### Cryptojacking

Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่างๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวลผลเพื่อสร้างรายได้กลับไปให้ Hacker

Source : <https://www.dga.or.th/document-sharing/info/sguqahj036181/>  
 gdnvca : <https://www.dga.or.th/document-sharing/info/sguqahj036181/>





ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

วันทำงาน



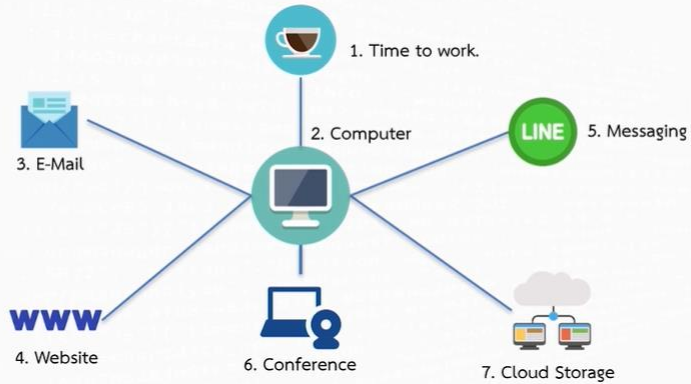
วันพักผ่อน





## ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

### วันทำงาน



Website

WWW

Conference

Conference

Cloud Storage

Cloud Storage

### Computer

#### สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ควรมีการแยก User ใช้งานกันของแต่ละบุคคล
2. ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
3. ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
4. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
5. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
6. **ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ**
7. มีการใช้ Password ที่ดี และ **ไม่ควรบอก Password แก่ผู้อื่น**



1. หน่วยงาน/ผู้ใช้งาน/ผู้ใช้/ระบบ/ความปลอดภัย

2. หน่วยงาน/ผู้ใช้งาน/ผู้ใช้/ระบบ/ความปลอดภัย



## Website

### สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่างๆ
2. ไม่ควรทำการบันทึก Password ต่างๆ บน Browser
3. เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น
4. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome, Mozilla Firefox เป็นต้น
5. ควรมีการ Update Version ของ Browser อย่างสม่ำเสมอ
6. ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web Browsing
7. ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

## Messaging

### สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ไม่ควรบันทึก Password ไว้ที่โปรแกรม
2. กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่างๆ ไว้บนเครื่อง
3. มีความระมัดระวังก่อนเปิด Link หรือ ไฟล์ต่างๆ ที่ได้รับมา
4. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

### เพิ่มเติม

ไม่ควรแชร์ข้อมูลหรือข่าวสารต่างๆ โดยไม่ทราบที่มาของข้อมูล



## Fake News

Fake News หรือ ข่าวปลอมเป็นภัยคุกคามใกล้ตัวประเภทหนึ่งที่มีความน่ากลัวอย่างมาก เนื่องจากข่าวปลอมที่นำมาเผยแพร่นี้ดูมีความน่าเชื่อถือ ซึ่งทำให้ผู้ที่รับข่าวสารหลงเชื่อ สามารถสร้างกระแส ปลุกปั่นได้อย่างมีประสิทธิภาพ ส่วนใหญ่ใช้วิธีการเผยแพร่ผ่านทางช่องทางออนไลน์ เช่น LINE, Facebook ทำให้มีการกระจายข่าวได้อย่างรวดเร็วมากยิ่งขึ้น

### วิธีการสังเกตข่าวปลอม

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



ที่: <https://www.antifakenewscenter.com>

## Conference

### สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ใช้สถานที่ที่เหมาะสมกับการ Conference
2. ในการประชุม Conference ควรมีผู้ที่เกี่ยวข้อง
3. แอร์เอกสารต่างๆ อย่างระมัดระวัง
4. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน
5. มีการ Update Version ของโปรแกรม 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. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ
6. มีการตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น



## ความตระหนักรู้ด้าน Cybersecurity ในชีวิตประจำวัน

### วันพักผ่อน



1. Computer



3. Internet Connection



2. Mobile



4. IoT Devices



## Computer

### สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ควรมีการแยก User ใช้งานกันของแต่ละบุคคล
2. ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์
3. ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
4. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
5. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ
6. **ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ**
7. มีการใช้ Password ที่ดี และ **ไม่ควรบอก Password แก่ผู้อื่น**



## Free WIFI

### สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. ไม่ควรใช้งาน WIFI ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน
2. หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ

Welcome to



FREE WIFI

## Mobile

### สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. เปิดการใช้งาน PIN / Password, Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์
2. ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา
3. กำหนด Application permission ให้เหมาะสม
4. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ
5. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ



## Internet Connection

### สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

1. เปลี่ยน Default Password ของ Router ที่มาจากโรงงาน
2. เปลี่ยน SSID และรหัสผ่านของ WIFI ที่กำหนดมาจากผู้ให้บริการ
3. กำหนดผู้ที่สามารถเข้าใช้งาน Internet เท่าที่จำเป็น



## IoT Devices

IoT Devices คือ อุปกรณ์อิเล็กทรอนิกส์ที่มีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตเพื่อใช้ในการทำงานร่วมกับระบบต่างๆ หรือแอปพลิเคชันต่างๆ ได้ เช่น หลอดไฟ, พัดลม, เครื่องกรองอากาศ ซึ่งเมื่อสามารถต่อกับเครือข่ายได้ก็จำเป็นที่จะต้องมีความปลอดภัยทางด้านเครือข่าย เปรียบได้กับเป็นคอมพิวเตอร์ขนาดจิ๋ว

สรุป : การสร้างความตระหนักรู้ด้านความมั่นคงทางไซเบอร์

