

# ปัญหาที่เกิดจาก คอมพิวเตอร์ และมาตรการควบคุม

# เนื้อหาในบทเรียน

1. การปกป้องข้อมูลเมื่อใช้อินเทอร์เน็ต
2. ความรู้เบื้องต้นเกี่ยวกับไวรัสคอมพิวเตอร์
3. ความรู้เบื้องต้นเกี่ยวกับ Phishing
4. ความรู้เบื้องต้นเกี่ยวกับ Firewall
5. ความรู้เบื้องต้นเกี่ยวกับ Proxy, Cookies
6. มาตรการควบคุมด้านจริยธรรม
7. กลศาสตร์ (Ergonomics)

# ทำไมต้องสนใจเรื่องความปลอดภัยจากการถูกโจมตี

เมื่อใช้งานอินเทอร์เน็ต? เพราะมีเครื่องที่ต่ออยู่กับอินเทอร์เน็ตและมีผู้ใช้งานอินเทอร์เน็ตจำนวนมาก

- จะเห็นได้ว่าเป็นใครก็ได้ที่เข้าใช้งานบนเครือข่ายอินเทอร์เน็ต
- เครือข่ายอินเทอร์เน็ตมีทรัพยากรสมบัติทางด้านข้อมูลจำนวนมาก
- หากมีระบบที่ใช้ป้องกันไม่พอเพียงรวมทั้งผู้ใช้ยังมีความรู้ไม่พอในการป้องกันตัวเอง ระบบของเราอาจจะโดนโจมตีได้

# ตัวอย่างการถูกโจมตีบนอินเทอร์เน็ต

เช่น

- Denial of Service
- Scan
- Malicious Code

# Denial of Service

คือ การโจมตีเครื่องหรือเครือข่ายเพื่อ  
iiiiทำให้เครื่องมีภาระงานหนักจนไม่สามารถ  
iiiiให้บริการได้หรือทำงานได้ช้าลง

# Scan

คือ วิธีการเข้าสู่ระบบโดยใช้เครื่องมือ  
อัตโนมัติหรือเป็นโปรแกรมที่เขียนขึ้นเพื่อ  
scan เข้าสู่ระบบหรือหาช่องจากการติดตั้งหรือ  
การกำหนดระบบผิดพลาด

# Malicious Code

คือ การหลอกส่งโปรแกรมให้ โดยจริงๆ แล้ว อาจเป็นไวรัส  
เวอร์ม และม้าโทรจัน และถ้าเรียกโปรแกรมนั้น โปรแกรมที่แอบ  
ซ่อนไว้ก็จะทำงานตามที่กำหนด เช่น  
ทำลายข้อมูลในฮาร์ดดิสก์ หรือเป็นจุดที่คอยส่งไวรัสเพื่อแพร่ไป  
ยังที่อื่นต่อไป เป็นต้น

# การป้องกันตนเองจากการโจมตี เมื่อใช้งานอินเทอร์เน็ตภายในองค์กร



# ไวรัสคอมพิวเตอร์

# ไวรัสคอมพิวเตอร์

หมายถึง โปรแกรมคอมพิวเตอร์หรือชุดคำสั่ง  
ที่มนุษย์เขียนขึ้นมามีวัตถุประสงค์เพื่อ  
รบกวนการทำงานหรือทำลายข้อมูล รวมถึง  
เพิ่มข้อมูลในระบบคอมพิวเตอร์

# ตัวอย่างลักษณะของไวรัส(1)

- นำขยะหรือข้อมูลอื่น ๆ ไปซ้อนทับข้อมูลเดิม  
บางส่วนที่ถูกต้องอยู่แล้วในแฟ้มข้อมูลหนึ่ง ๆ ทำให้  
แฟ้มข้อมูลเดิมผิดเพี้ยนไปจากเดิม
- ควบคุมการทำงานของระบบปฏิบัติการคอมพิวเตอร์  
แทนระบบเดิม โดยกำหนดให้ ระบบปฏิบัติหยุด  
การทำงานบางหน้าที่ ซึ่งก่อให้เกิดความเสียหายแก่  
ระบบคอมพิวเตอร์

# ตัวอย่างลักษณะของไวรัส(2)

- เพิ่มเติมบางคำสั่งลงในโปรแกรมระบบปฏิบัติการ
- ทำให้แสดงผลเป็นข้อความอันเป็นเท็จทางจอภาพ เพื่อเตือนให้ผู้ใช้ทำอะไรบางอย่าง ซึ่งอาจก่อให้เกิดความเสียหายแก่ระบบได้
- เปลี่ยนข้อมูลในโปรแกรมหรือเพิ่มข้อมูลหนึ่ง ๆ ซึ่งเจ้าของไม่รู้สีกว่าเพิ่มข้อมูลของตนเองติดไวรัส เมื่อมีการใช้หรือสำเนาแฟ้มดังกล่าวไปยังที่อื่น ๆ ก็จะส่งผลให้ติดไวรัสตามไปด้วย

# ชนิดของไวรัสคอมพิวเตอร์

ไวรัสคอมพิวเตอร์แบ่งออกเป็นสองชนิดใหญ่ ๆ  
ได้แก่

1. Application viruses
2. System viruses

# Application viruses

- จะมีผลหรือมีการแพร่กระจายไปยังโปรแกรมประยุกต์ต่าง ๆ เช่น โปรแกรมประมวลคำ หรือโปรแกรมตารางคำนวณ เป็นต้น
- การตรวจสอบการติดเชื้อไวรัสชนิดนี้ทำได้โดยดูจากขนาดของแฟ้มว่ามีขนาดเปลี่ยนไปจากเดิมมากน้อยแค่ไหน เช่น ถ้าแฟ้มมีขนาดโตขึ้น นั่นหมายถึงแฟ้มดังกล่าวอาจได้รับการติดเชื้อจาก

# System viruses

- ไวรัสนี้จะติดหรือแพร่กระจายในโปรแกรม  
จำพวกระบบปฏิบัติการหรือโปรแกรมระบบ  
อื่นๆ
- โดยไวรัสนี้มักจะแพร่เชื้อในขณะที่เปิด  
เครื่องคอมพิวเตอร์

โดยทั่วไปเราอาจแบ่งแยกไวรัสเป็นชนิดต่าง ๆ

$\eta$     $\frac{1}{\eta}$     $D$     $-$     $\eta$     $\frac{1}{\eta}$     $D$     $-$     $\eta$     $|$     $D^{\frac{1}{2}}$

# เวิร์ม (Worm)

- หมายถึงโปรแกรมซึ่งเป็นอิสระจากโปรแกรมอื่นๆ โดยจะแพร่กระจายผ่านเครือข่ายไปยังคอมพิวเตอร์และอุปกรณ์ที่อยู่บนเครือข่าย
- การแพร่กระจายจะคล้ายกับตัวหนอนและแพร่พันธุ์ด้วยการคัดลอกตนเองออกและส่งต่อผ่านเครือข่ายออกไป
- ตัวอย่างเช่น เวิร์มที่แนบมากับแฟ้มในอีเมล เมื่อผู้รับเปิดแฟ้มดังกล่าวเวิร์มจะเริ่มทำงานทันทีโดยจะ



# โลจิกบอมบ์ (Logic bombs)

## หรือ ม้าโทรจัน (Trojan Horses)(1)

หมายถึงโปรแกรมซึ่งถูกออกแบบมาให้มีการทำงานในลักษณะถูกตั้งเวลาเหมือนระเบิดเวลา เช่น ม้าโทรจัน ซึ่งถูกออกแบบมาให้แฝงตัวเองเข้าไปในระบบและจะทำงานโดยการดักจับเอารหัสผ่านเข้าสู่ระบบต่าง ๆ และส่งกลับไปยังเจ้าของหรือผู้ส่ง เพื่อบุคคลดังกล่าวสามารถเข้าใช้หรือโจมตีระบบในภายหลัง

# โลจิกบอมบ์ (Logic bombs)

## หรือ ม้าโทรจัน (Trojan Horses)(2)

- โปรแกรมม้าโทรจันสามารถแฝงมาในได้ในหลายรูปแบบ เช่น game , e-mail
- ม้าโทรจัน ต่างจากไวรัสและหนอน คือมันไม่สามารถทำสำเนาตัวเองและแพร่กระจายตัวเองได้ แต่มันสามารถที่จะอาศัยตัวกลาง
- เมื่อเรียกใช้งานไฟล์เหล่านี้ โปรแกรมม้าโทรจันก็จะทำงานและจะเปิดช่องทางต่างๆให้ผู้บุกรุกเข้าโจมตีระบบได้

# ข่าวไวรัสหลอกลวง (Hoax)

- เป็นข่าวที่ต้องการให้ผู้ใช้อินเทอร์เน็ตเข้าใจผิด
- มักถูกส่งมาใน E-mail หรือส่งข้อความต่อกันไปผ่านทางโปรแกรมรับส่งข้อความ หรือห้องสนทนาต่างๆ ซึ่งสามารถสร้างความวุ่นวายได้
- หัวเรื่องของ E-mail จะน่าสนใจ อาจอ้างบริษัทหรือองค์กรขนาดใหญ่เพื่อสร้างความเชื่อมั่น
- การป้องกันและแก้ไขคือไม่ควรส่งต่อ E-mail ที่ได้รับไปให้คนอื่นๆ หรือควรตรวจสอบจากแหล่งข้อมูลที่ถูกต้องก่อนทำการส่งต่อไป

# แนวทางหรือมาตรการ ในการป้องกันการเข้าถึงข้อมูล

# แนวทางหรือมาตรการในการป้องกันการเข้าถึงข้อมูล

1. การกำหนดแนวปฏิบัติหรือระเบียบปฏิบัติและนโยบายต่างๆ ไปในองค์กร อาทิเช่น เปลี่ยนรหัสผ่านบ่อยๆ , กำหนดสิทธิเข้าใช้ , สำรองข้อมูล , มีการเก็บ Log files เป็นต้น
2. การป้องกันโดยซอฟต์แวร์
3. ใช้เทคนิควิธีช่วยป้องกันการเข้าถึงข้อมูล เช่น
  - ลายมือชื่ออิเล็กทรอนิกส์ (Digital signatures)
  - การเข้ารหัสและถอดรหัส (Encryption)

# Phishing

# Phishing คืออะไร

- คือการหลอกลวงทางอินเทอร์เน็ตอย่างหนึ่ง โดยใช้วิธีการปลอมแปลงอีเมลติดต่อไปยังผู้ใช้อินเทอร์เน็ต โดยหลอกให้ผู้ใช้เข้าใจว่าเป็นจดหมายจากองค์กร หรือบริษัท ห้างร้านที่ผู้ใช้ทำการติดต่อ หรือเป็นสมาชิกอยู่
- เนื้อหาจดหมายอาจเป็นข้อความหลอกให้ผู้ใช้กรอกข้อมูลส่วนตัวซึ่งเป็นความลับ และมีความสำคัญ

# ตัวอย่างการหลอกลวงด้วยวิธี Phishing

## ■ กรณีตัวอย่างการหลอกลวงลูกค้า Citibank


ผู้หลอกลวงปลอมแปลงอีเมล ส่งไปยังลูกค้าของ Citibank โดยมีการเชื่อมโยง link ไปยังเว็บไซต์ปลอม ที่มีลักษณะที่คล้ายคลึงเว็บไซต์ของธนาคารมาก มีการแจ้งกับลูกค้าธนาคารในการเปลี่ยนแปลงฐานข้อมูลและมีการให้ลูกค้าธนาคารกรอกข้อมูลใหม่ ทั้งนี้ข้อมูลต่างๆที่ลูกค้ากรอกใหม่ เช่น รหัสบัตรเครดิต ข้อมูลส่วนบุคคล บัญชีผู้ใช้ (Username) รหัสผ่าน (Password)

สามารถดูข้อมูลการหลอกลวงเพิ่มเติมได้ที่

<http://www.thaicert.nectec.or.th/paper/basic/phishing.php>



# ตัวอย่าง Web ปลอมที่ให้ผู้ใช้กรอกข้อมูลส่วนตัว

[Products & Services](#) [Planning & Tools](#) [Investing & Markets](#) [Help Desk](#)

[Sign on](#) • [Open account](#) • [Contact us](#) • [Search](#) • [Privacy](#) • [Citi.com](#)

myCiti

Update your ATM/Debit Card on your Citibank account :

Use this secure form to update your ATM/Debit Card information on your Citibank account. The transmitted ATM/Debit Card information is protected by the industry standard encrypted SSL connection.

ATM/Debit Card (CEN):

Expiration Date: Month  Year

Pin Number:

Email Address:

Your User ID:

Your Password:

Submit

Welcome to the place where you can do it all!

To get started using My Citi, just sign on with your User ID and Password. Then you can take advantage of:

[Award Winning Services](#)  
The #1 Online Bank!

[Free Online Bill Payment](#)  
The easiest way to pay virtually anyone, anytime!

[Your Home Page](#)  
The one place to manage your Citi accounts

learn more  
Take a tour


get started  
Register for free

[Sign on](#) with an ATM/Debit Card number and PIN.

1 Citibank was ranked the #1 overall online bank by Gomez™, the Internet Quality Measurement firm, in its Internet Banker Scorecard™ for Q4 2003. Gomez, the Gomez logo and Gomez Internet Banker Scorecard are trademarks of Gomez, Inc.



[about us](#) | [careers](#) | [locations](#) | [site map](#)

My Citi gives you access to accounts and services provided by Citibank and its affiliates.  
Citibank, N.A., Citibank, F.S.B., Citibank (West), FSB. Member FDIC.

  
[Citi.com](#)

Member of Citigroup

[Citigroup Privacy Promise](#)  
[Terms & Conditions](#)  
Copyright © 2003 Citicorp



28

# วิธีป้องกันและรับมือกับ Phishing

- ระวังอีเมลที่มีลักษณะในการขอให้ท่านกรอกข้อมูลส่วนตัวใดๆ หรือ ยืนยันข้อมูลส่วนตัวใดๆ โดยส่วนใหญ่เนื้อหาในจดหมายจะระบุว่า เป็นจดหมายเร่งด่วน หากพบอีเมลลักษณะดังกล่าว ให้ลบอีเมลดังกล่าวทันที และอาจใช้การ โทรศัพท์ติดต่อกับทางองค์กร บริษัทห้างร้านด้วยตนเองอีกทีหากมีข้อสงสัย
- หากต้องการกระทำธุรกรรมใดๆ ควรไปที่ website โดยตรงโดยการพิมพ์ URL ใหม่
- ไม่ควรคลิกที่ hyperlink ใดๆ หรือรันไฟล์ใดๆ ที่มากับอีเมล หรือ โปรแกรมสนทนาต่างๆ จากบุคคลที่ไม่รู้จัก

# วิธีป้องกันและรับมือกับ Phishing (ต่อ)

- ควรติดตั้งโปรแกรมตรวจสอบไวรัส และ Firewall เพื่อป้องกันการรับอีเมลที่ไม่พึงประสงค์ หรือการสื่อสารจากผู้ที่ไม่ได้รับอนุญาต
- ควรติดตั้งโปรแกรมปรับปรุงช่องโหว่ (Patch) ของซอฟต์แวร์ต่างๆ ที่เราใช้งานอยู่ ตลอดเวลา
- ในการกรอกข้อมูลส่วนตัวที่สำคัญใดๆ ที่เว็บไซต์หนึ่งๆ ควรตรวจสอบให้แน่ใจว่าเป็นเว็บไซต์ที่ถูกต้องและปลอดภัย ซึ่งเว็บไซต์ที่ปลอดภัยจะใช้โปรโตคอล https:// แทน http://
- ควรตรวจสอบข้อมูลบัญชีธนาคาร บัตรเครดิตต่างๆ ที่มีการใช้งานผ่านอินเทอร์เน็ต เป็นประจำ

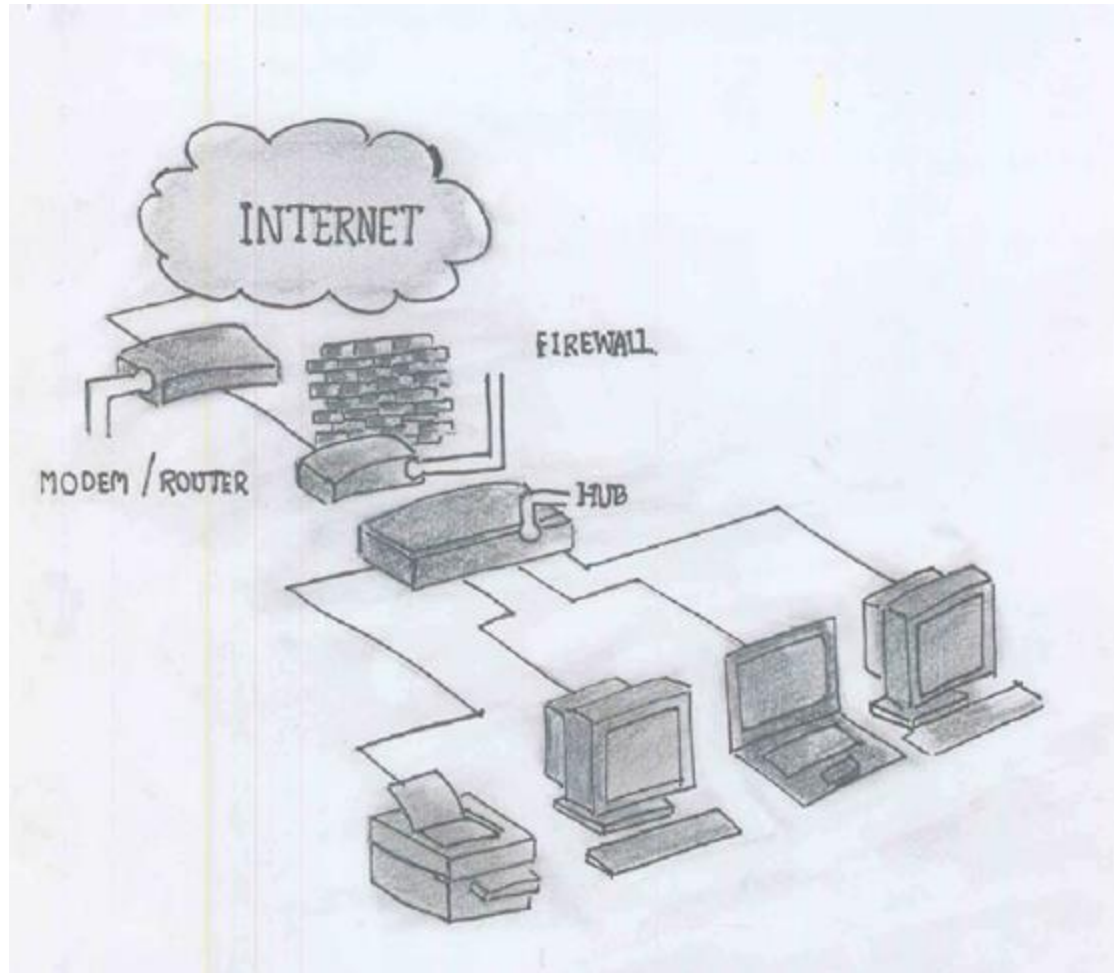
# **ข้อควรรู้ทางเทคนิค เกี่ยวกับมาตรการในการเข้าถึง ข้อมูล**

# Firewall(1)

ความหมายของ ไฟร์วอลล์ ( Firewall )

ไฟร์วอลล์ คือ รูปแบบของโปรแกรมหรืออุปกรณ์ที่ถูกจัดตั้งอยู่บนเครือข่ายเพื่อทำหน้าที่เป็นเครื่องมือรักษาความปลอดภัยให้กับเครือข่ายภายใน (Intranet) โดยป้องกันผู้บุกรุก (Intrusion) ที่มาจากเครือข่ายภายนอก (Internet) หรือเป็นการกำหนดนโยบายการควบคุมการเข้าถึงระหว่างเครือข่ายสองเครือข่าย โดยสามารถกระทำได้โดยวิธีแตกต่างกันไป แล้วแต่ระบบ

# การทำงานของ Firewall



# ลักษณะของ Firewall

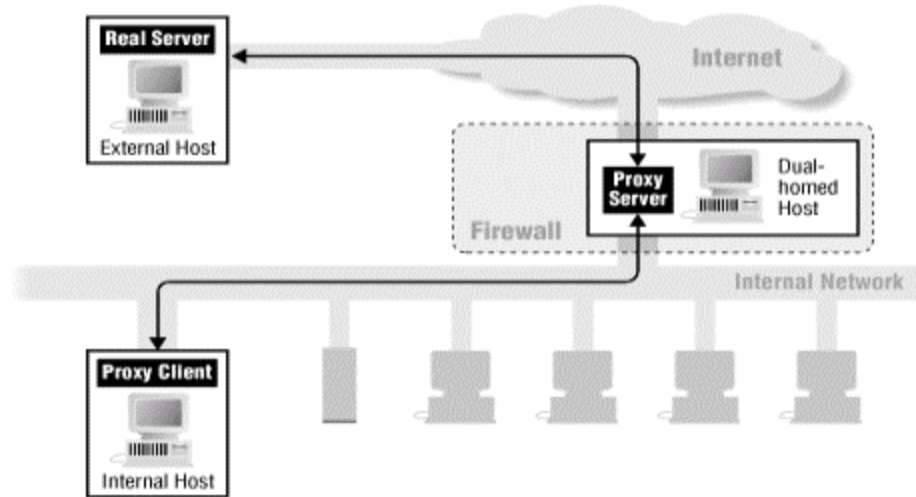
- ไม่อนุญาตการ Login สำหรับผู้ใช้ที่ไม่มีสิทธิ์ในการเข้าใช้งานในเครือข่าย
- แต่ผู้ใช้ที่มีสิทธิ์ใช้งานจะมีสิทธิ์ใช้งานทั้งภายในและติดต่อภายนอกเครือข่ายได้ โดยจำกัดข้อมูลจากภายนอกเครือข่ายไม่ให้เข้ามาในเครือข่าย
- ไม่สามารถป้องกันการโจมตีจากภายในเครือข่ายกันเอง
- ไม่สามารถป้องกันการบุกรุกที่สามารถมากับโปรแกรมประยุกต์ต่าง ๆ ไวรัส และอันตรายในรูปแบบวิธีใหม่ๆ ได้

# Proxy คืออะไร

- เป็นโปรแกรมที่ทำงานอยู่บนไฟร์วอลล์ที่ตั้งอยู่ระหว่างเน็ตเวิร์ก 2 เน็ตเวิร์ก
- ทำหน้าที่เพิ่มความปลอดภัยของระบบเน็ตเวิร์กโดยการควบคุมการเชื่อมต่อระหว่างเน็ตเวิร์กภายในและภายนอก



# หลักการทำงานของ Proxy



# หลักการทำงานของ Proxy (ต่อ)

- เมื่อผู้ใช้คอมพิวเตอร์ในระบบภายใน (Intranet) ทำการติดต่อไปยังระบบภายนอก (Internet) เช่น ไปยังเว็บหนึ่งๆ คอมพิวเตอร์นั้นจะติดต่อไปยัง proxy server ก่อนและ proxy server จะทำหน้าที่ติดต่อเว็บนั้นให้
- เมื่อเว็บได้รับการร้องขอก็จะทำการส่งข้อมูลมายัง proxy server ก่อนและ proxy server จะทำการส่งข้อมูลเหล่านั้นให้กับเครื่องคอมพิวเตอร์ในระบบ Intranet ที่มีการร้องขอเว็บนั้นต่อไป

# ประโยชน์ของ Proxy

- Proxy server สามารถถูกใช้เพื่อเก็บข้อมูลเหตุการณ์การใช้งานระหว่างเน็ตเวิร์กภายในและรับส่งข้อมูลระหว่างอินเทอร์เน็ต เช่น URL วันเวลาที่ใช้งาน จำนวนไบต์ที่ดาวน์โหลด เป็นต้น
- สามารถกำหนดเงื่อนไขให้กับ Proxy server ในการรักษาความปลอดภัยของระบบภายในได้ เช่น การกำหนดให้ระบบภายในดาวน์โหลดไฟล์จากอินเทอร์เน็ตได้ แต่ไม่อนุญาตให้ระบบภายในดาวน์โหลดไฟล์จากระบบภายในได้
- Proxy server สามารถช่วยเพิ่มความเร็วได้ โดยการสร้างแคชข้อมูลเว็บที่เคยถูกร้องขอ

# ข้อควรรู้ทางเทคนิค ในการป้องกัน การละเมิดสิทธิส่วนบุคคล

# Cookie

# Cookie คืออะไร

- Cookie คือแฟ้มข้อมูลชนิด text ที่เว็บเซิร์ฟเวอร์ทำการจัดเก็บไว้ที่ฮาร์ดดิสก์ของผู้ที่ไปเรียกใช้งานเว็บเซิร์ฟเวอร์นั้น
- ข้อมูลที่อยู่ในไฟล์ Cookie นี้จะเป็นข้อมูลที่เรากรอกที่เว็บไซต์ใดๆ หรือมีการทำธุรกรรม ต่างๆ ที่เว็บไซต์นั้น แล้วเว็บไซต์นั้นได้มีการจัดเก็บข้อมูลเช่น ชื่อ นามสกุล ที่อยู่ อีเมล ชื่อผู้ใช้ รหัสผ่าน ของเราเอาไว้ที่ไฟล์นี้

# Cookie คืออะไร (ต่อ)

- แต่ละเว็บไซต์ก็มีการจัดเก็บข้อมูลที่แตกต่างกันไป
- ข้อมูลใน Cookie นี้ก็จะเป็นประโยชน์สำหรับเว็บไซต์ เมื่อเราเข้าไปใช้งานเว็บไซต์ในครั้งถัดๆ ไป ก็สามารถดูข้อมูลจาก Cookie นี้เพื่อให้ทราบว่าผู้ที่เข้าใช้是谁 และมีข้อมูลส่วนตัวอะไรบ้าง

# ข้อมูล Cookie ถูกเคลื่อนย้าย อย่างไร

- เมื่อเราพิมพ์ URL ของเว็บไซต์หนึ่ง ไปยังโปรแกรมเว็บเบราว์เซอร์ เพื่อร้องขอให้เว็บไซต์นั้นแสดงเว็บเพจ บนเว็บเบราว์เซอร์ที่เราใช้งานอยู่
- โปรแกรมเว็บเบราว์เซอร์จะทำการตรวจสอบที่ฮาร์ดดิสก์ว่ามีไฟล์ Cookie ที่ เว็บไซต์นั้นเคยเก็บไว้หรือไม่ ถ้าพบไฟล์ Cookie ที่เว็บไซต์นั้นสร้างไว้ โปรแกรมเว็บเบราว์เซอร์จะทำการส่งข้อมูลที่อยู่ในไฟล์ Cookie นั้น ไปยังเว็บไซต์นั้นด้วย



# ข้อมูล Cookie ถูกเคลื่อนย้าย อย่างไร (ต่อ)

- ถ้าหากไม่มีไฟล์ Cookie ส่งไปให้กับเว็บไซต์ เว็บไซต์นั้นก็จะทราบว่าผู้ใช้เพิ่งเคยเข้ามาใช้งานเว็บไซต์เป็นครั้งแรก เว็บไซต์ก็จะสร้างแฟ้มข้อมูลชนิด text ซึ่งก็คือ Cookie นั้นเอง ซึ่งมีข้อมูลหมายเลขที่ถูกกำหนดขึ้นมาโดยเว็บไซต์และอาจมีข้อมูลอื่นๆ แล้วส่งมาเก็บไว้ที่ฮาร์ดดิสก์ของผู้ใช้
- ในการเข้าใช้งานเว็บไซต์ครั้งต่อไป เว็บไซต์ก็สามารถที่จะทำการเพิ่มเติมข้อมูลเปลี่ยนแปลงแก้ไขข้อมูลในไฟล์

# เว็บไซต์ใช้ Cookie เพื่ออะไร

- เพื่อให้ทราบจำนวนผู้ที่เข้ามาใช้งานเว็บไซต์
- สำหรับเว็บไซต์ E-commerce ต่างๆ สามารถใช้ cookie เก็บข้อมูลสินค้าที่ลูกค้าได้เลือกใส่ตะกร้าไว้แต่ยังไม่ชำระเงินได้

# ข้อควรระวังที่เกี่ยวกับ Cookie

- ข้อมูล Cookie อาจถูกลักลอบขโมยข้อมูลส่วนตัวจากบุคคลอื่นได้ในระหว่างการถ่ายโอนไฟล์ไปมาระหว่างเครื่องผู้ใช้และเว็บไซต์ ซึ่งผู้ใช้ควรระมัดระวังในการให้ข้อมูลต่างๆ แก่เว็บไซต์
- หากเราไม่มั่นใจในเว็บไซต์ใดๆ ที่ไป เราสามารถที่จะไม่อนุญาตให้มีการสร้างไฟล์ Cookie เก็บไว้ที่ฮาร์ดดิสก์ของเราก็ได้ ซึ่งเว็บเบราว์เซอร์จะแสดงข้อความถามความสมัครใจของเรว่าจะอนุญาตหรือไม่

# มาตรการควบคุมการใช้ อินเทอร์เน็ต

# ภัยคุกคามอันเกิดจากการใช้อินเทอร์เน็ต

- ปัจจุบันภัยคุกคามอันเกิดจากการใช้งานอินเทอร์เน็ตมีมากมาย
- เช่นภัยจากเรื่องเว็บลามกอนาจาร
- ปัจจุบันมีความพยายามที่จะแก้ไข  
ปราบปรามการเผยแพร่อย่างต่อเนื่อง

# มาตรการควบคุมการใช้ อินเทอร์เน็ต

“ผู้ใดประสงค์แจกจ่ายแสดง อดทำ ผลิตภัณฑ์  
ประชาชนหรือทำให้เผยแพร่ซึ่งเอกสาร ภาพ  
ระบายสี สิ่งพิมพ์ แถบบันทึกเสียง บันทึกภาพ  
หรือเกี่ยวเนื่องกับสิ่งพิมพ์ดังกล่าว มีโทษจำคุก  
ปรับ หรือทั้งจำทั้งปรับ”

ตัวอย่างซอฟต์แวร์ได้แก่ House Keeper เป็น  
โปรแกรมสำหรับแก้ปัญหา “ภาพลามกอนาจาร  
เนื้อหาสาระที่ไม่เหมาะสม ควรใช้วิธีไม่เหมาะสม

# คำแนะนำเบื้องต้นในการใช้อินเทอร์เน็ต

- ควรตั้งเครื่องคอมพิวเตอร์ไว้ในที่โล่งที่ผู้ปกครองสามารถมองเห็นหน้าจอระหว่างที่เด็กii ใช้งานได้
- ผู้ปกครองเองก็ควรเรียนรู้เพื่อใช้อินเทอร์เน็ตให้เหมาะสมด้วย
- มีจิตสำนึกรับผิดชอบและการเอาใจใส่ต่อ

# กิลศาสตร

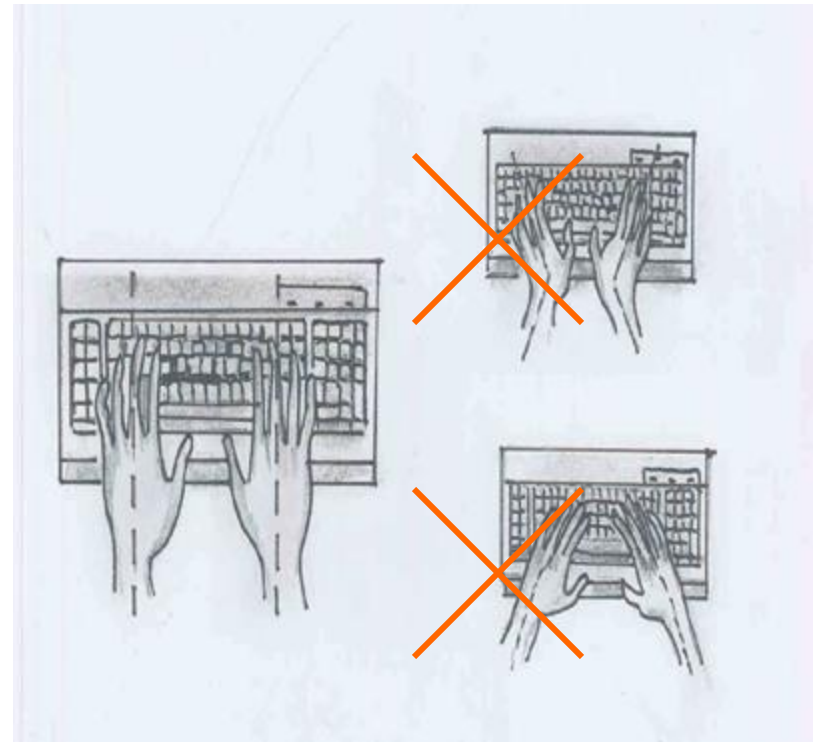
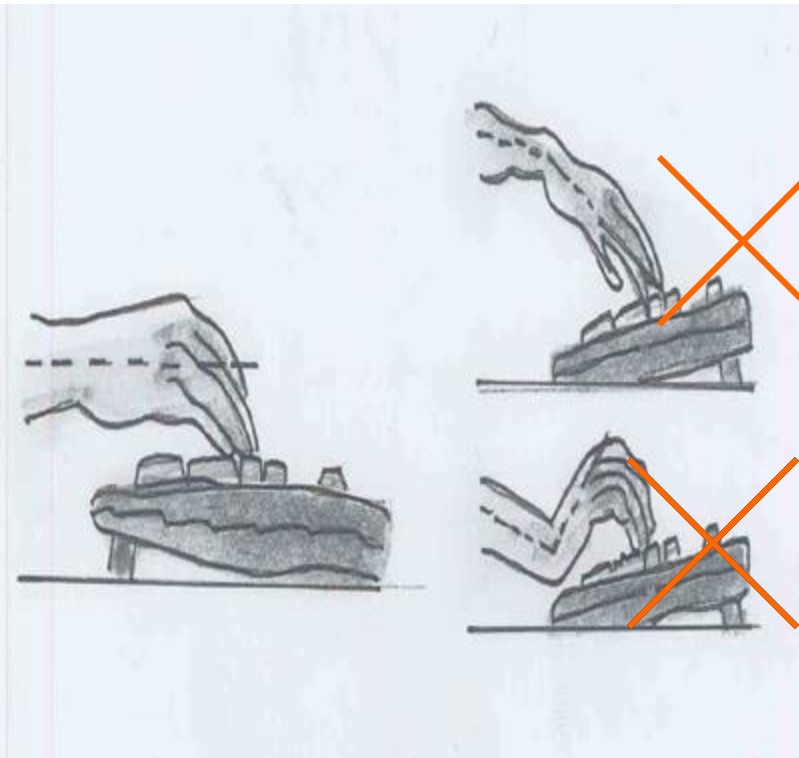
## (Ergonomics)



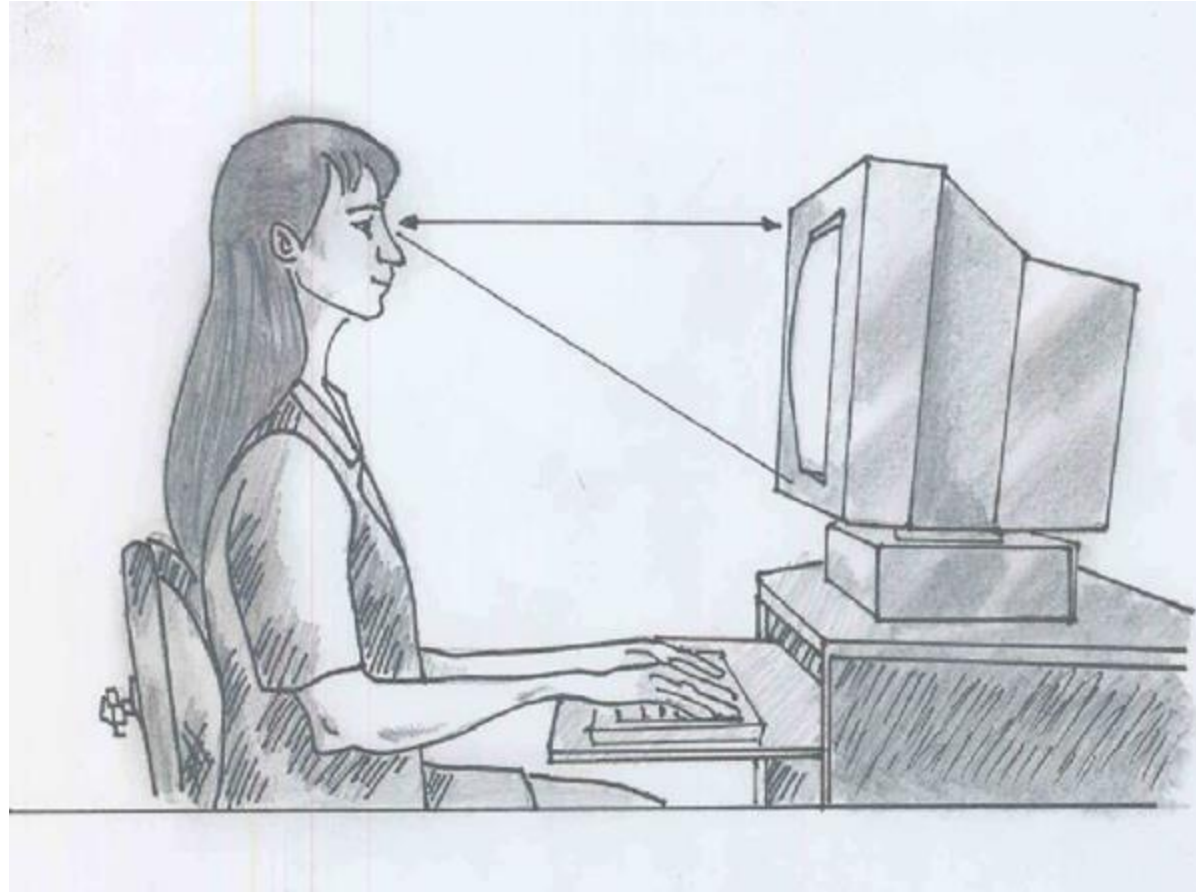
# กลศาสตร์ (Ergonomics)

- คือการศึกษาการใช้งานเครื่องมือเครื่องกลต่าง ๆ  
เกิดขึ้นมาพร้อม ๆ อุปกรณ์ไฮเทคสมัยใหม่ต่าง ๆ  
ทั้งนี้เพื่อลดปัญหาจากการใช้วัตถุเหล่านั้น
- เช่นการติดตั้งและวิธีการใช้งานของคีย์บอร์ด  
จอมอนิเตอร์ เมาส์ แก้ว การปรับระดับแสง เป็นต้น

# รูปแสดงการใช้งานคีย์บอร์ด (3)



# รูปแสดงการใช้งาน จอคอมพิวเตอร์



# คำแนะนำการใช้งานเมาส์ (1)

- อย่าเกร็งข้อมือเพื่อจับเมาส์จะทำให้เกิดอาการบาดเจ็บที่โพรงกระดูกข้อมือได้
- หากต้องทำงานตลอดวัน การรองข้อมือและกดทับบนโต๊ะจะทำให้เส้นเอ็นหรือเส้นประสาทที่ข้อมือเกิดอาการปวดได้
- ในระยะยาวอาจจะเกิดการอักเสบ นำไปสู่การปวด ชา และปวดรุนแรงที่นิ้วมือได้

# รูปแสดงการใช้งานเก้าอี้



# คำแนะนำการใช้งานเกี่ยวกับแสง

- ควรใช้คอมพิวเตอร์ทำงานสีขาวที่มีความสว่างเพียงพอต่อการมองเห็น
- ตำแหน่งของแสงไฟควรจะสามารถปรับขึ้นลงได้
- การใช้ผ้า màn จะช่วยควบคุมแสงจากภายนอก
- หลอดไฟที่ใช้ก็ควรให้แสงสว่างในโทน

[illegible]

Thank  
you.

A stylized smiley face is integrated into the word 'Thank'. The face is drawn with thick black lines, featuring a wide, curved mouth and two small, upward-curving lines for eyes. Two bright red circles are positioned on either side of the face, serving as cheeks. The entire graphic is rendered in a hand-drawn, informal style.