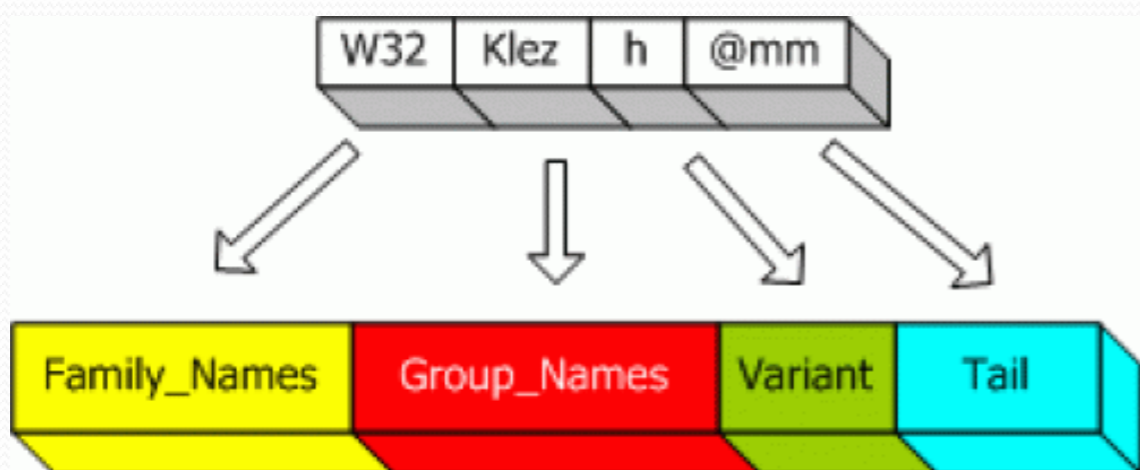


# การเตือนภัยไวรัสคอมพิวเตอร์ แก่ผู้ใช้งาน

## ความหมายของไวรัสคอมพิวเตอร์

โปรแกรมชนิดหนึ่งที่ถูกเขียนขึ้นให้สามารถจัดการกับตัวมันเอง โดยมีลักษณะเลียนแบบสิ่งมีชีวิต คือ เจริญเติบโตเองได้ ขยายและแพร่กระจายตัวเองได้ สามารถอยู่รอดได้ด้วยการอำพรางตน เหมือนกับไวรัสที่เป็นเชื้อโรค ร้ายทำลายสิ่งมีชีวิตนั่นเอง

## ส่วนประกอบต่าง ๆ ของชื่อไวรัส



**Family\_Names** ตั้งตามชนิดของปัญหาที่ไวรัส/ภาษาที่ใช้ในการพัฒนา

**Group\_Name** แทรกไว้ในโค้ดของไวรัส เปรียบเสมือนชื่อเล่น

**Variant** บอกสายพันธุ์ของไวรัสชนิดนั้น ๆ แบ่งเป็น 2 ชนิด คือ

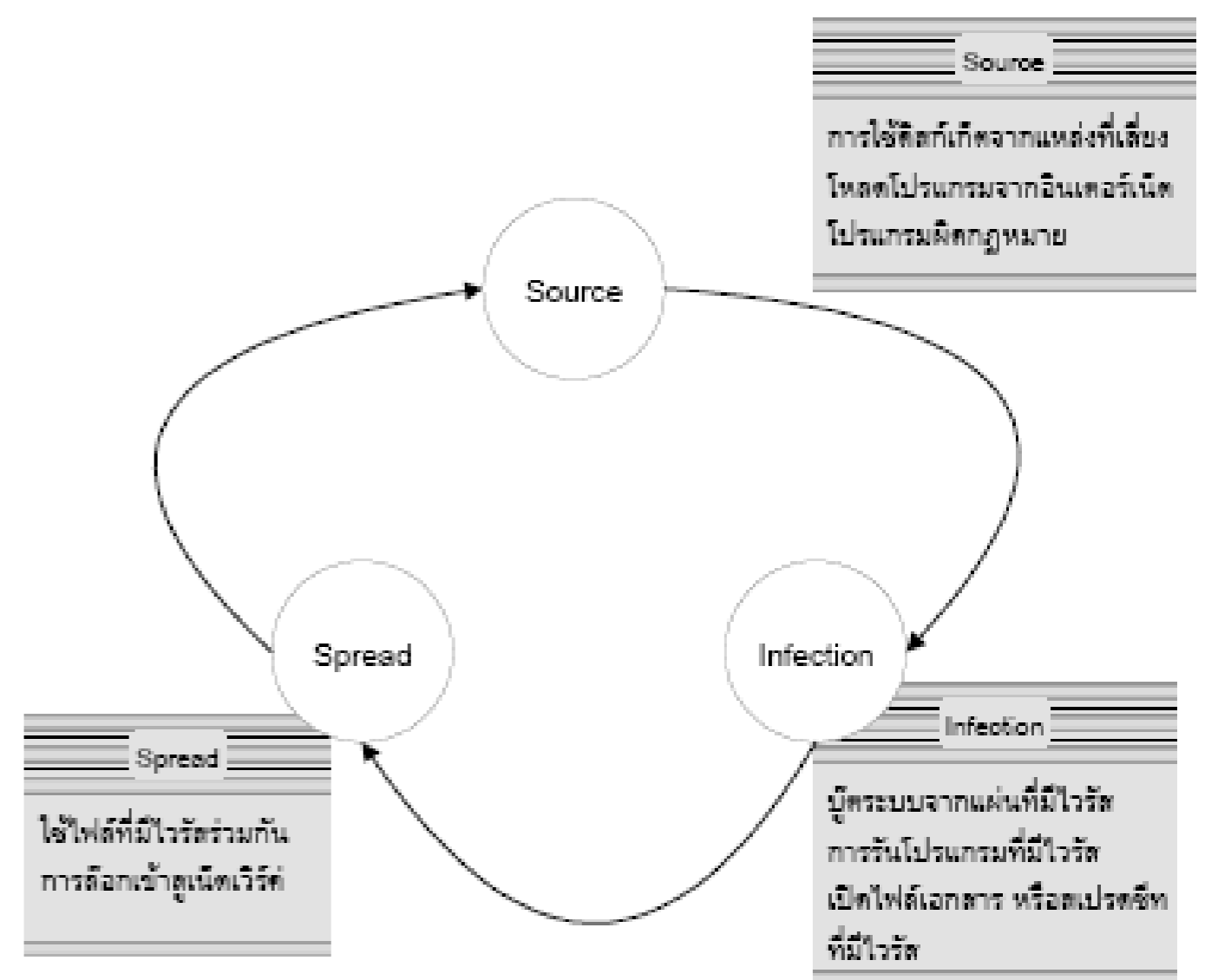
- Major\_Variants จะตามหลังส่วนชื่อของไวรัส
- Minor\_Variants ใช้บ่งบอกในกรณีที่แตกต่างกันเล็กน้อย/ขนาดไฟล์

ของไวรัส

**Tail** บอกวิธีการแพร่กระจาย

- @M / @m บอกให้รู้ว่าไวรัส/หนอนเป็น “mailer” ที่ส่งตัวเองผ่านทางอี-เมลเมื่อผู้ใช้ส่งอี-เมลเท่านั้น
- @MM / @mm บอกให้รู้ว่าไวรัส/หนอนเป็น “mass-mailer” ที่จะส่งตัวเองผ่านทุกอี-เมลแอดเดรสที่อยู่ในเมลบ็อกซ์

## วงจรชีวิตของไวรัสคอมพิวเตอร์



## เทคนิคของไวรัสคอมพิวเตอร์

**Stealth** เป็นเทคนิคที่ออกแบบให้โปรแกรมสามารถป้องกันตัวเองจากการค้นหา/กำจัดได้

**Polymorphic** อาศัยการเปลี่ยนแปลงรูปแบบของไวรัส มีการแบ่งรหัสของตัวไวรัสเป็นส่วนย่อยแทรกอยู่ระหว่างแฟ้มข้อมูล

**Multipartite** การทำงานหลากหลายรูปแบบในตัวเอง สามารถแพร่กระจายทางไฟล์ปกติในส่วนของ Boot Record ของระบบดิสก์ได้

**Companion Virus** ถูกติดตั้งขึ้นมาโดยอาศัยช่องว่างในการทำงานของระบบปฏิบัติการ และการทำงานตามเงื่อนไขที่ถูกต้องของระบบปฏิบัติการในการทำลายนระบบและแพร่กระจาย

**Malicious Program** เป็นเทคนิคที่เกิดขึ้นในช่วงหลัง ๆ จากที่มีการใช้โปรแกรมจาวา และ Active X

Family Names	ความหมาย
WM	ไวรัสที่เป็นมาโครของโปรแกรม Word
W97M	ไวรัสที่เป็นมาโครของโปรแกรม Word 97
XM	ไวรัสที่เป็นมาโครของโปรแกรม Excel
X97M	ไวรัสที่เป็นมาโครของโปรแกรม Excel 97
W95	ไวรัสที่มีผลกระทบต่อระบบปฏิบัติการวินโดวส์ 95
W32/Win32	ไวรัสที่มีผลกระทบต่อระบบปฏิบัติการวินโดวส์ 32 บิต
WNT	ไวรัสที่มีผลกระทบต่อระบบปฏิบัติการวินโดวส์ NT 32 บิต
I-Worm/Worm	หนอนอินเทอร์เน็ต
Trojan/Troj	ม้าโทรจัน
VBS	ไวรัสที่ถูกพัฒนาด้วย Visual Basic Script
AOL	ม้าโทรจัน America Online
PWSTEAL	ม้าโทรจันที่มีความสามารถในการขโมยรหัสผ่าน
Java	ไวรัสที่ถูกพัฒนาด้วยภาษาจาวา
Linux	ไวรัสที่มีผลกระทบต่อระบบปฏิบัติการลินุกซ์
Palm	ไวรัสที่มีผลกระทบต่อระบบปฏิบัติการ Palm OS
Backdoor	เปิดช่องให้ผู้บุกรุกเข้าถึงเครื่องได้
HILLW	บ่งบอกว่าไวรัสถูกคอมไพล์ด้วยภาษาระดับสูง

# ประเภทไวรัสคอมพิวเตอร์

- ❖ Boot Sector Virus
- ❖ File virus
- ❖ Macro virus
- ❖ Worm
- ❖ Trojan
- ❖ Spyware

# การตรวจหาและการกำจัดไวรัสคอมพิวเตอร์

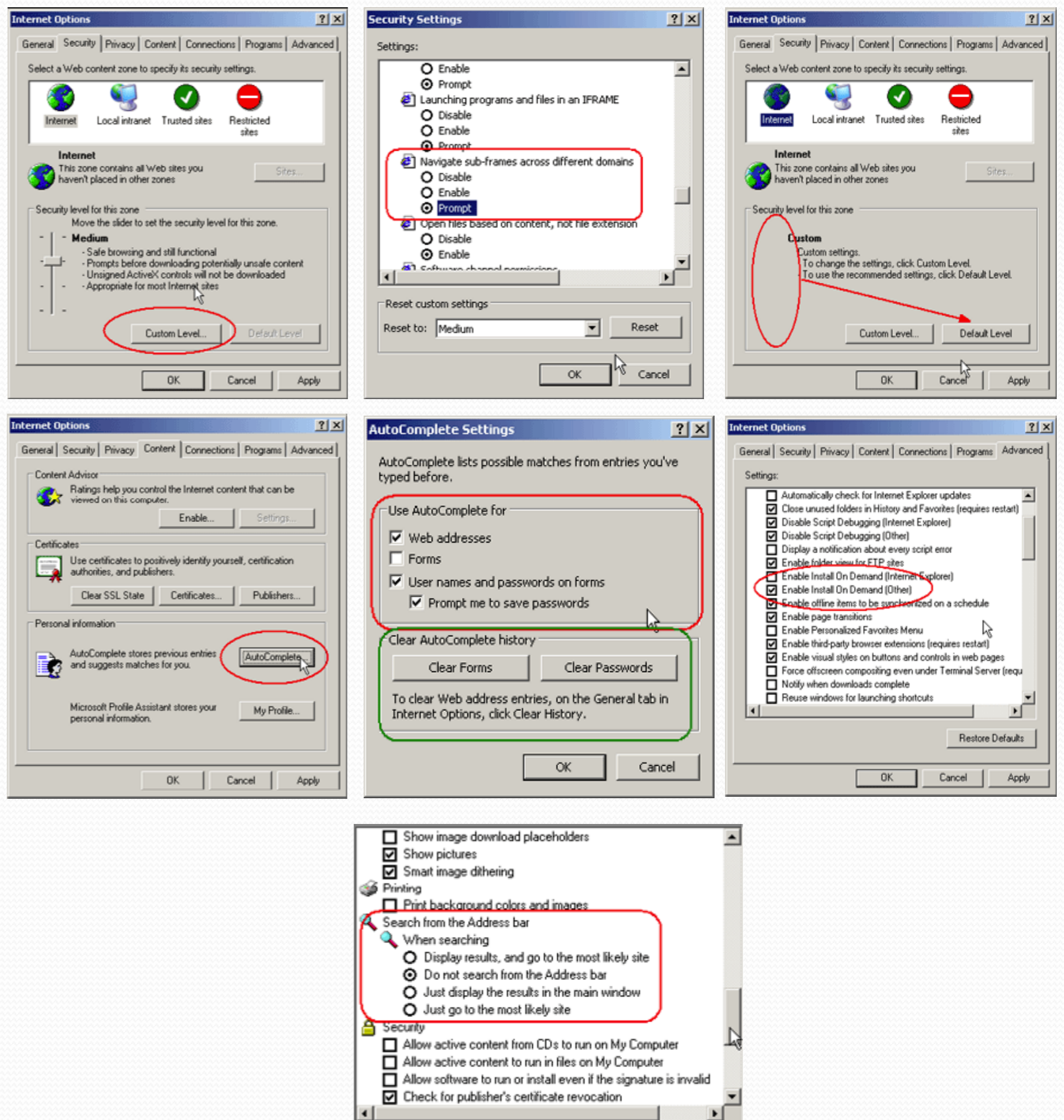
## ❖ การตรวจหาไวรัสคอมพิวเตอร์

- Scanning
- การตรวจการเปลี่ยนแปลงที่เรียกว่า Checksum
- การเฝ้าดู
- การใช้คำสั่ง netstat ตรวจสอบ

## ❖ การกำจัดไวรัสคอมพิวเตอร์

- ใช้เครื่องมือในการกำจัดไวรัส Remove Tools
- การตั้งค่าความปลอดภัยใน Internet Explorer

Tools --> Internet Options --> Security --> Custom Level



## อาการเครื่องคอมพิวเตอร์ที่ติดไวรัส

- เนื้อที่ฮาร์ดดิสก์ลดลงโดยไม่ทราบสาเหตุ ทั้งที่ไม่ได้ลงโปรแกรม/บันทึกข้อมูล
- วินโดวส์แสดงไดอะล็อกบ็อกซ์ข้อความโดยไม่ทราบสาเหตุ/โปรแกรมบางตัวทำงานโดยที่ไม่ได้สั่ง
- คอมพิวเตอร์ทำงานช้า อืดผิดปกติ ทั้งที่ไม่ได้ใช้โปรแกรมอะไร
- ไฟล์ข้อมูลมีขนาดใหญ่ขึ้นมาก ทุกครั้งที่ใช้งาน
- การเปิด/การโหลด เข้าใช้งานโปรแกรมเข้าสู่หน่วยความจำใช้เวลานานขึ้น
- เครื่องคอมพิวเตอร์เกิดอาการแฮงค์ (Hang) โดยไม่ทราบสาเหตุ

ฯลฯ

## ไวรัสคอมพิวเตอร์ในปัจจุบัน

### 1. ไวรัส Brontok

ลักษณะอาการ - Menu Folder Option จะหายไป

- จะเกิดไฟล์ .exe ชื่อเหมือน Folder ในทุก Folder ที่เปิดเข้าไปดู
- หน้าเวปขึ้นมาเขียนว่า Brontok
- ไม่สามารถเรียกใช้ Registry Editor และ Folder Option ได้

2. ไวรัสดิลิป VDO.EXE มีนามสกุลเป็น .exe ทำให้เมื่อคลิกก็จะฟังตัวไว้ใน C:WINDOWSsystem32 โดยจะรันตัวมันเองขึ้นมาเรื่อย ๆ และสร้างไฟล์ดิลิป VDO.exe

3. Svchost.exe เป็น Worm ที่สร้างชื่อเลียนแบบไฟล์ Svchost.exe ของระบบปฏิบัติการวินโดวส์ ซึ่งไฟล์ svchost.exe เป็นไฟล์ generic host process ใช้รัน กับ DLL ไฟล์เพื่อสร้าง Service ขึ้นมา

### 4. Toy.exe

ลักษณะอาการ - หน้า Desktop จะมีภาษาจีน ภาษาอังกฤษขึ้นมา  
- ไม่สามารถเข้า Local Disk ต่าง ๆ ได้ตามปกติรวมถึง Flash Drive ด้วยโดยจะดับเบิ้ลคลิกเข้า Drive ต่าง ๆ โดยตรงไม่ได้ ต้องคลิกขวาแล้ว Open / Explore เท่านั้น

## ไวรัสคอมพิวเตอร์กับ Flash drive

- ไวรัส shortcut ซ่อน folder ไว้แล้วสร้าง shortcut ชื่อเดียวกันกับ folder นั้น ๆ ขึ้นมา

การแก้ไข ----> โปรแกรม SPKAutorunKiller

1. ดับเบิ้ลคลิกที่ไฟล์ SPKAutokillerV2.4.exe --> Run --> Install เพื่อติดตั้งโปรแกรม
2. หากติดตั้งโปรแกรมแล้วเครื่องเตือนว่ามี error และไม่มีสัญลักษณ์ SPK ขึ้นที่มุมล่างขวา ให้ติดตั้งโปรแกรม DOTNET และดับเบิ้ลคลิกที่ไอคอน Spk ที่หน้าจออีกครั้ง โปรแกรมจะถูกติดตั้งไว้ในเครื่อง และลบไวรัสโดยอัตโนมัติเมื่อเสียบแฮนด์ไดรฟ์ / สื่อบันทึกข้อมูลแบบพกพา


# ระบบการเรียนรู้ทางอิเล็กทรอนิกส์

## องค์ความรู้ กรมวิชาการเกษตร

### Thai Open Source Learning Management System

หน้าหลัก รายวิชา เกี่ยวกับเรา ช่วยเหลือ ติดต่อเรา

**User Organizer**



itc1

จัดการองค์ความรู้  
กำหนดองค์ความรู้  
นำบทเรียนเข้า  
นำบทเรียนออก  
ส่งข้อความ  
ตารางนัดหมาย  
จดบันทึก  
จัดการระบบ  
แก้ไขข้อมูลส่วนตัว  
ออกจากระบบ

**User Online**

ผู้เยี่ยมชม 0 คน  
สมาชิก 1 คน



- ประเภทองค์ความรู้**
  - การส่งเสริมอาชีพเกษตรกรรายจังหวัดขยายแผนภาคใต้  
ยุทธศาสตร์ : การพัฒนาเกษตรกรและสถาบันเกษตรกร
  - การส่งเสริมและพัฒนากิจภาพเกษตรกร  
ยุทธศาสตร์ : การพัฒนาการผลิต
  - ผลงานวิจัยด้านพืชและเทคโนโลยีการเกษตร  
ยุทธศาสตร์ : การพัฒนาการผลิต
  - พันธุ์พืช และปัจจัยการผลิต  
ยุทธศาสตร์ : การพัฒนาการผลิต
  - การควบคุมกำกับดูแลตามพระราชบัญญัติการรับผิดชอบ  
พรม. 6 ฉบับ ได้แก่ พรม. กักพืช พรม. คู่มือนำพันธุ์พืช พรม. ไม้ พรม. พันธุ์พืช พรม. ความคุมยาง และ พรม. วัตถุอันตราย
- ทดสอบและพัฒนาระบบปลูกพืชทดแทนพลังงาน**  
ยุทธศาสตร์ : การพัฒนาการผลิต
- มาตรฐานและคุณภาพสินค้าเกษตร**  
ยุทธศาสตร์ : การพัฒนาการผลิต
- อำนาจการและสนับสนุน**  
สารผสม ประชาสัมพันธ์ นิติการ การคลัง การเจ้าหน้าที่ สถิติ แผนงานและวิชาการ ตรวจสอบภายใน
- เทคโนโลยีสารสนเทศ และภูมิสารสนเทศ**  
คอมพิวเตอร์ ระบบเครือข่าย ระบบสารสนเทศ ระบบสารสนเทศภูมิศาสตร์ การกำหนดตำแหน่งบนพื้นโลก การรับรู้จากระยะไกล


**Admin Message**

ระบบ e-Learning เป็นรูปแบบที่ผู้เรียนสามารถเรียนรู้ผ่านเครือข่ายคอมพิวเตอร์ด้วยตนเอง โดยสามารถเรียนรู้ได้ตามอัธยาศัยทุกที่ ทุกเวลา และยังสามารถเลือกเรียนได้ตามความสนใจและความสนใจของตนเองอีกด้วย

ผู้สอนสามารถสร้างและจัดกิจกรรมในการเรียนรู้ให้แก่ผู้เรียนเสมือนในห้องเรียนจริง

หน้าหลัก รายวิชา เกี่ยวกับเรา ช่วยเหลือ ติดต่อเรา

**User Organizer**



itc1

จัดการองค์ความรู้  
กำหนดองค์ความรู้  
นำบทเรียนเข้า  
นำบทเรียนออก  
ส่งข้อความ  
ตารางนัดหมาย  
จดบันทึก  
จัดการระบบ  
แก้ไขข้อมูลส่วนตัว  
ออกจากระบบ

**User Online**

ผู้เยี่ยมชม 0 คน  
สมาชิก 1 คน

f: การเตือนภัยไวรัสคอมพิวเตอร์แก่ผู้ใช้งาน

องค์ความรู้ สารบัญ ห้องสนทนา

**ชื่อรายการองค์ความรู้ :** f: การเตือนภัยไวรัสคอมพิวเตอร์แก่ผู้ใช้งาน

**ผู้กำหนดองค์ความรู้ :** itc1


**ระยะเวลา :** 1 วัน

**องค์ความรู้ :** การเตือนภัยไวรัสคอมพิวเตอร์แก่ผู้ใช้งาน

**วัตถุประสงค์ :** ระยะเวลาที่ผ่านมา ไวรัสคอมพิวเตอร์ได้สร้างความเสียหายแก่ระบบคอมพิวเตอร์ทั่วโลกเป็นอย่างมาก เป้าหมายการสร้างความรู้ความเสียหายที่เกิดจากไวรัสคอมพิวเตอร์ชนิดใหม่ๆ ในปัจจุบันได้ส่งผลกระทบต่อสังคมและเศรษฐกิจในทุกๆด้าน การพัฒนาการของไวรัสโดยเทคนิคแบบใหม่ แนวคิดในการเขียนโปรแกรมมีแนวโน้มที่จะสร้างความเสียหายในวงกว้างมากขึ้น การจัดการความรู้เรื่องไวรัสคอมพิวเตอร์จึงเป็นสิ่งจำเป็นและมีประโยชน์อย่างยิ่งต่อผู้ใช้คอมพิวเตอร์ในองค์กร เพื่อใช้เป็นแนวทางการป้องกันและแก้ไขปัญหาการติดไวรัสคอมพิวเตอร์

**คุณสมบัติผู้เรียนรู้ :** ข้าราชการ พนักงานกรมวิชาการเกษตร และบุคคลทั่วไป

**รายละเอียดผู้กำหนดองค์ความรู้ :**



itc1

**การมอบรางวัลยกย่องชมเชย**

**ผู้ที่นำความรู้ไปใช้ในการปฏิบัติงาน**

**นายสิทธิพงษ์ พยุหะ**

**เจ้าหน้าที่ระบบงานคอมพิวเตอร์**



