การอบรม Cyber Awareness • 2026

# Cyber Awareness สำหรับเจ้าหน้าที่โรงพยาบาล

การสร้างความตระหนักรู้ด้านความปลอดภัยทางไซเบอร์
เพื่อปกป้องข้อมูลผู้ป่วยและความต่อเนื่องในการรักษาพยาบาล
โดยเน้นการนำไปใช้ได้จริงในชีวิตประจำวัน

ทุกคลิก ทุกไฟล์แนบ และทุกรหัสผ่าน — เกี่ยวข้องกับความปลอดภัยของผู้ป่วย

โดย นพ.กิตติภพ แจ่มโสภณ
รองผู้อำนวยการด้านสุขภาพดิจิทัล

# ทำไมโรงพยาบาลจึงตกเป็นเป้าหมายของแฮกเกอร์

## ข้อมูลผู้ป่วยมีมูลค่าสูง

HN ประวัติการรักษา ที่อยู่ และข้อมูลส่วนตัว ล้วนมีราคาสูงในตลาดมืด

## โรงพยาบาลหยุดงานไม่ได้

หากระบบล่ม ผู้ป่วยอาจได้รับผลกระทบโดยตรง ทุกนาทีที่หยุดชะงักคือความเสี่ยง

## แรงกดดันให้ยอมจ่าย

แฮกเกอร์เชื่อว่าโรงพยาบาลมีแรงกดดันสูง และมีโอกาสยอมจ่ายเพื่อให้ระบบกลับมา

**การโจมตีโรงพยาบาลไม่ใช่เรื่องไกลตัว — และไม่ใช่หน้าที่ของ IT เท่านั้น**

• ทำไมต้องสนใจ

# ผลกระทบเมื่อระบบล่ม หรือข้อมูลรั่วไหล

## ห้องยาจ่ายยาไม่ได้

ระบบค้าง ยืนยันข้อมูลผู้ป่วยไม่ได้
เกิดความล่าช้าในการจ่ายยา

## เข้าถึงประวัติผู้ป่วยไม่ได้

ทีมรักษาขาดข้อมูลสำคัญ
อาจส่งผลต่อการตัดสินใจรักษา

## กลับสู่ระบบกระดาษ

ความล่าช้าและความเสี่ยงต่อความผิดพลาด
เพิ่มขึ้นอย่างมีนัยสำคัญ

💬 ชวนคิด

**ถ้าระบบล่มเพียง 1 ชั่วโมง — งานในแผนกของคุณจะได้รับผลกระทบอะไรบ้าง?**

ภัยใกล้ตัว 1

# Phishing
# ภัยร้ายที่มาในรูปแบบการหลอกลวง


ปลอมตัวเป็น ผู้อำนวยการ, HR, ธนาคาร หรือหน่วยงานภายใน

เป้าหมาย: หลอกให้กดลิงก์, เปิดไฟล์แนบ หรือกรอกรหัสผ่าน

อาวุธหลัก: ความเร่งด่วน, ความกลัว และความไว้วางใจในชื่อที่คุ้นเคย

กว่า 80-90% ของเหตุการณ์ไซเบอร์เริ่มจากการถูกหลอกลวงผู้ใช้

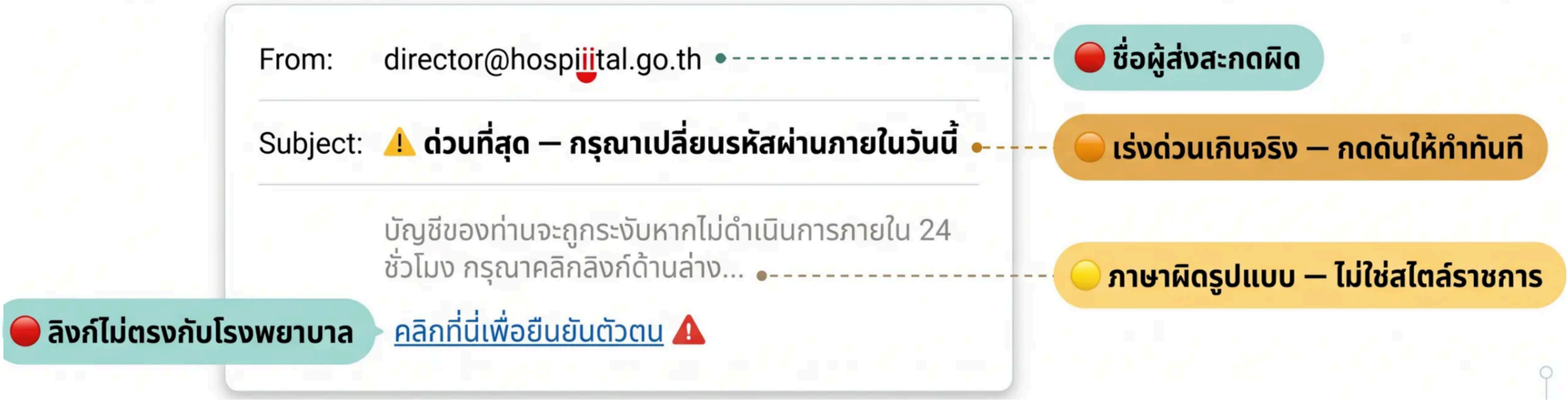
**ตัวอย่างสถานการณ์จริง:**

ข้อความต้องสงสัย

“เรียน เจ้าหน้าที่ทุกท่าน — กรุณาเปลี่ยนรหัสผ่านของท่านภายในวันนี้ มิฉะนั้นบัญชีจะถูกระงับทันที คลิกที่นี่: [hospital-secure-login.net]”

# จุดสังเกตและวิธีจับผิดอีเมลหลอกลวง

อีเมลปลอมมักซ่อนสัญญาณเตือน — ถ้ารู้จักดู ก็จะไม่ถูกหลอก




💡💡 หลักคิดง่าย ๆ: ถ้ารู้สึกว่า ‘ต้องรีบทำ’ — นั่นแหละคือสัญญาณให้ ‘หยุดก่อน’

ภัยใกล้ตัว 2

# Ransomware มัลแวร์เรียกค่าไถ่ตัวอันตราย

โปรแกรมอันตรายที่ล็อกไฟล์ข้อมูลเพื่อเรียกเงินแลกกับการปลดล็อก

## มันทำงานอย่างไร

เมื่อเครื่องติดไวรัส ไฟล์
ทั้งหมดจะถูกเข้ารหัส เปิดไม่ได้
ระบบงานหยุดชะงักทันที

## เริ่มต้นจากอะไร

มักเริ่มจากการคลิกไฟล์แนบ
ผิดปกติ หรือเสียบ Flash Drive
ที่ไม่ทราบที่มา

## ผลกระทบต่อโรงพยาบาล

ความเสียหายไม่ใช่แค่ค่าใช้จ่าย
แต่รวมถึงความล่าช้าในการรักษา
และความเสี่ยงต่อผู้ป่วย

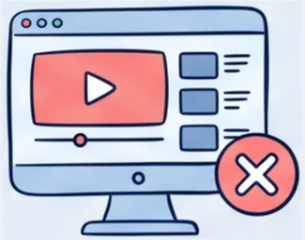
**Ransomware มักเริ่มจากพฤติกรรมเล็ก ๆ — ระวังก่อนคลิก ดีกว่าแก้ทีหลัง**

# พฤติกรรมเสี่ยงที่อาจสร้างความเสียหายต่อระบบ

ความสะดวก 1 นาที อาจกลายเป็นความเสียหายทั้งระบบ

## เสียบ Flash Drive ส่วนตัว

Flash Drive ของคนใช้หรือญาติอาจนำมัลแวร์เข้าสู่ระบบโรงพยาบาลได้โดยไม่รู้ตัว



## เข้าเว็บไซต์ที่ไม่เกี่ยวกับงาน

การดูหนัง ฟังเพลง หรือดาวน์โหลดโปรแกรมเถื่อนบนเครื่องโรงพยาบาลเพิ่มความเสี่ยงต่อการติดมัลแวร์


## จดรหัสผ่านทิ้งไว้ให้เห็น

การเขียนรหัสผ่านแปะหน้าจอหรือใต้คีย์บอร์ดทำให้ผู้อื่นสวมรอยเข้าระบบได้ง่าย

## ใช้บัญชีร่วมกันในแผนก

การใช้ Account เดียวกันทำให้ตรวจสอบย้อนหลังไม่ได้ว่าใครเป็นผู้ใช้งาน เมื่อเกิดปัญหา

💡 **ชวนคิด: คุณเคยทำพฤติกรรมเหล่านี้โดยไม่รู้ตัวบ้างไหม?**

# กฎเหล็ก 5 ข้อเพื่อความปลอดภัยไซเบอร์

แนวทางปฏิบัติที่ทุกคนในโรงพยาบาลทำได้ทันที

**1**

**ไม่แชร์บัญชี**

1 คน · 1 บัญชี · 1 รหัสผ่าน

**2**

**รหัสผ่านแข็งแรง**

หลีกเลี่ยงวันเกิด, 123456 หรือชื่อตนเอง

**3**

**ล็อกหน้าจอทุกครั้ง**

กด Win + L ก่อนลุกจากโต๊ะเสมอ

**4**

**ระวัง Flash Drive**

ห้ามเสียบอุปกรณ์ที่ไม่รู้ที่มา — แจ้ง IT ก่อน

**5**

**เอ๊ะใจก่อนคลิก**

หยุด ตรวจ ถาม แจ้ง — ก่อนเปิดทุกครั้ง

# วิธีปฏิบัติเมื่อพบสิ่งผิดปกติหรือเหตุสงสัย

4 ขั้นตอนง่าย ๆ ที่ทุกคนทำได้ทันที

## 1 หยุด

อย่าเพิ่งคลิก เปิดไฟล์
หรือกรอกรหัสผ่าน

## 2 ตรวจ

ดูผู้ส่ง ลิงก์ ไฟล์แนบ
และความสมเหตุสมผล

## 3 ถาม

โทรเช็กกับต้นทางผ่าน
ช่องทางที่รู้จัก
ไม่ใช้เบอร์ในข้อความ

## 4 แจ้ง IT

แจ้งฝ่าย IT หรือช่องทาง
รับเหตุของโรงพยาบาลทันที

**No Blame — แจ้งเร็ว ช่วยลดความเสียหาย**

ไม่ต้องกลัวการถูกตำหนิ การแจ้งเหตุคือการปกป้องโรงพยาบาลและผู้ป่วย

# บทสรุปและการสร้างความร่วมมือในองค์กร

สรุป & Q&A

**ทุกคนคือแนวป้องกัน**

ไม่ใช่หน้าที่ IT คนเดียว

**ปกป้องข้อมูลผู้ป่วย**

เหมือนทรัพย์สินสำคัญ

**ระวัง Phishing & Ransomware**

ป้องกันได้ด้วยความระมัดระวัง

**จำกฎเหล็ก 5 ข้อ**

ไม่แชร์บัญชี • ล็อกจอ • เอ๊ะไว้ก่อน

**หลังจากวันนี้ คุณจะเปลี่ยนพฤติกรรมเล็ก ๆ อะไร เพื่อช่วยให้โรงพยาบาลปลอดภัยขึ้น?**