



ธุรกรรมออนไลน์

บรรยายโดย Aj.Lattagarn Kuikaew

ธุรกิจ

ออนไลน์



“ธุรกรรมออนไลน์” คืออะไร ?





“ รุขกรรมออนไลน์ ”

การประกอบธุรกิจการพาณิชย์อิเล็กทรอนิกส์
เกี่ยวกับการให้บริการทางธุรกรรมทางการเงิน
ต่าง ๆ ผ่านอุปกรณ์หรือระบบอิเล็กทรอนิกส์
เช่น โทรศัพท์มือถือ หรืออินเทอร์เน็ต
มีการให้บริการ เช่น การฝากเงิน ถอนเงิน
โอนเงิน หรือ สอบถามยอดเงิน เป็นต้น

รูปแบบการทำธุรกรรมผ่านอินเทอร์เน็ต

① ธนาคารอินเทอร์เน็ต (Internet Banking)

สอบถามยอดเงินคงเหลือ



โอนเงิน



ชำระค่าสาธารณูปโภค



เช็ค



พิมพ์รายการเดินบัญชี



รายการใช้จ่ายผ่านบัตรเครดิตย้อนหลัง

① ธนาคารอินเทอร์เน็ต (Internet Banking)

ลักษณะบริการธนาคารอินเทอร์เน็ต

- สอบถามยอดคงเหลือในบัญชี (Account Balance Inquiry)
- สอบถามรายการเคลื่อนไหวในบัญชี (Account Statement Inquiry)
- โอนเงินระหว่างบัญชีตนเองหรือไปยังบุคคลอื่นทั้งในและต่างประเทศ (Inter-Account Funds Transfer to owner or other account)
- สอบถามสถานะเช็ค (Cheque Status Inquiry)
- สอบถามการอายัดเช็ค (Stop-Payment Cheque Inquiry)
- อายัดเช็ค (Stop-Payment of Cheque)
- การโอนเงินเพื่อชำระเป็นค้ำประกันกู้ธนาคาร



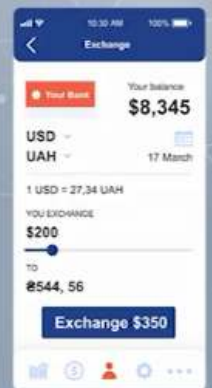
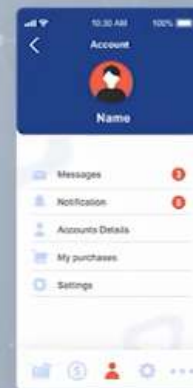
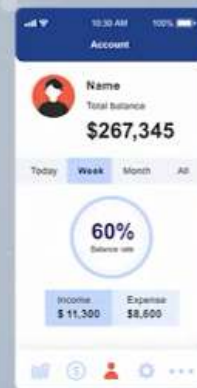
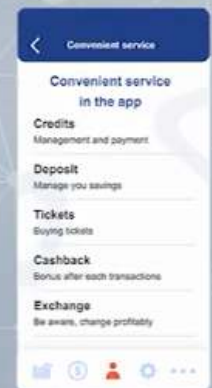
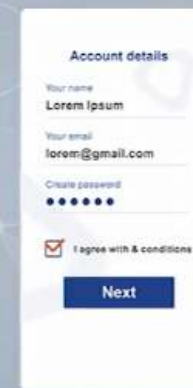
รูปแบบการทำธุรกรรมผ่านอินเทอร์เน็ต

② ชำระเงินออนไลน์ (Payment Gateway or Bill Payment)



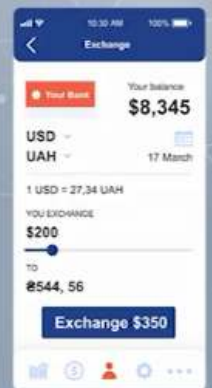
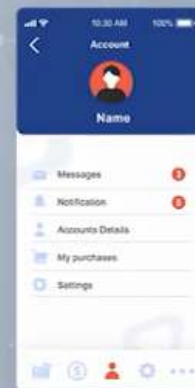
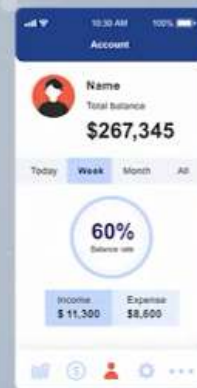
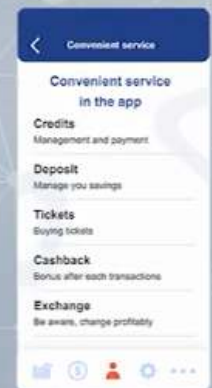
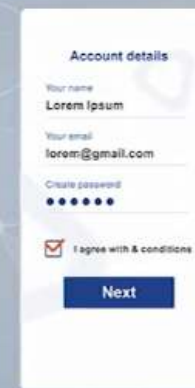
รูปแบบการทำธุรกรรมผ่านอินเทอร์เน็ต

3 Mobile Banking



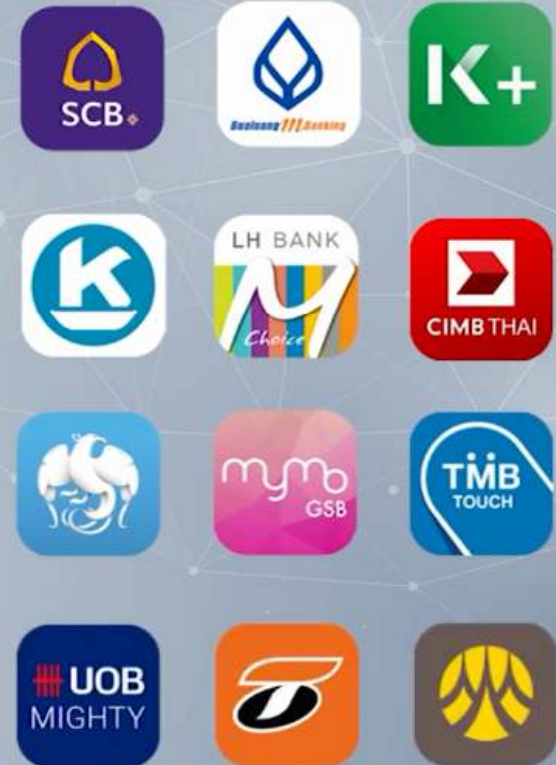
รูปแบบการทำธุรกรรมผ่านอินเทอร์เน็ต

3 Mobile Banking



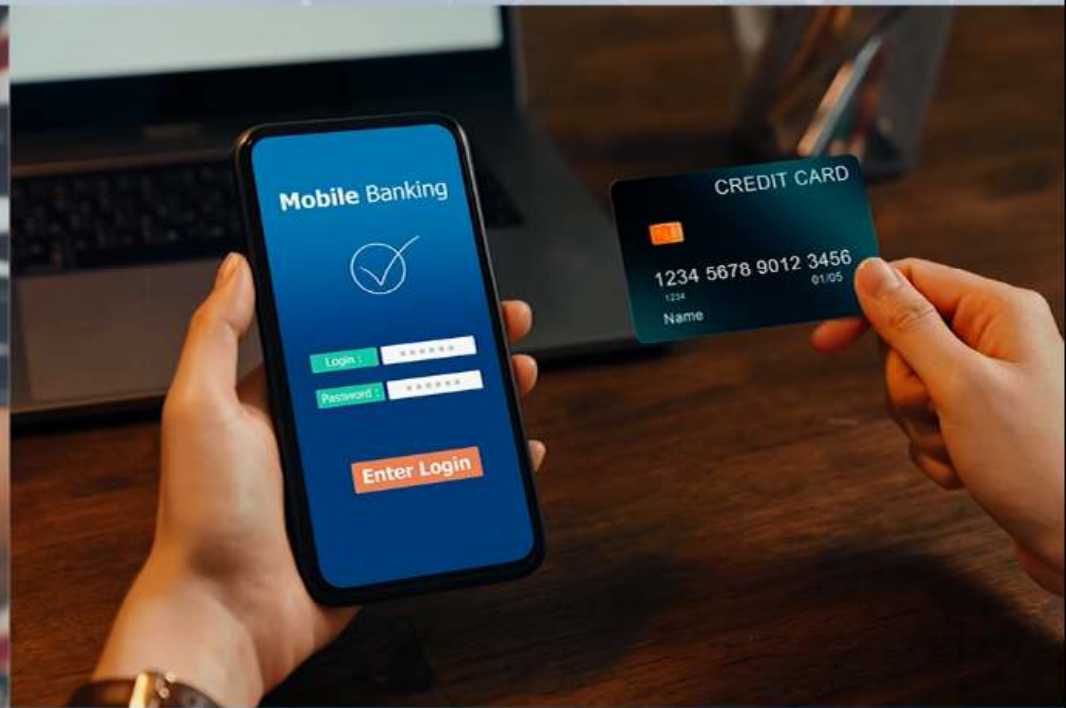
รูปแบบการทำธุรกรรมผ่านอินเทอร์เน็ต

3 Mobile Banking



ความเสี่ยงจากการทำธุรกรรมผ่านอินเทอร์เน็ต

► การถูกแอบอ้างใช้งานธนาคารออนไลน์



ความเสี่ยงจากการทำธุรกรรมผ่านอินเทอร์เน็ต

► การหลอกลวงทางอินเทอร์เน็ต (Phishing)



ความเสี่ยงจากการทำธุรกรรมผ่านอินเทอร์เน็ต

► การหลอกลวงทางอินเทอร์เน็ต (Phishing)



ความเสี่ยงจากการทำธุรกรรมผ่านอินเทอร์เน็ต

▶ โปรแกรมอันตรายต่าง ๆ



- Virus
- Worm
- Trojan Horses
- Spyware
- Key Logger

ความเสี่ยงจากการทำธุรกรรมผ่านอินเทอร์เน็ต

▶ โปรแกรมอันตรายต่าง ๆ



ความเสี่ยงจากการทำธุรกรรมผ่านอินเทอร์เน็ต

► การเข้าเว็บไซต์ธนาคารออนไลน์จากสมาร์ทโฟน หรือแท็บเล็ต



1. การไหลดใช้โปรแกรมธนาคารจากการแฮ็คโปรแกรมที่ไม่ใช่จากการอัปเดตจากธนาคารผู้ให้บริการ ซึ่งเสี่ยงที่อาจจะเป็นโปรแกรมปลอมที่เอาไว้ดักจับข้อมูลของผู้ใช้งาน
2. สมาร์ทโฟนหรือแท็บเล็ตบางรุ่นอาจมองไม่เห็น URL การเข้ารหัสของเว็บไซต์ซึ่งเสี่ยงที่เราไม่สามารถทราบได้ว่าเป็นเว็บไซต์จริงหรือปลอม
3. การใช้ระบบปฏิบัติการที่ผ่านการ Jailbreak หรือการดัดแปลงระบบปฏิบัติการของสมาร์ทโฟนซึ่งเสี่ยงต่อการถูกขโมยข้อมูลหากเชื่อมต่อเข้าสู่เว็บไซต์

แนวทางการจัดการความเสี่ยงการทารุณกรรมผ่านอินเทอร์เน็ต



ออกจากระบบ (Log out) ทุกครั้ง
หลังเลิกใช้งานระบบออนไลน์

1. ป้องกันการถูกแอบอ้างใช้งานธนาคารออนไลน์

ไม่ให้ข้อมูลส่วนตัวแก่บุคคลอื่น

เช่น หมายเลขบัตรเครดิต เลขบัญชีเงินฝาก รหัสผ่านต่าง ๆ



แนวทางการจัดการความเสี่ยงการทารุณกรรมผ่านอินเทอร์เน็ต

2. ป้องกันการหลอกลวงทางอินเทอร์เน็ต

สังเกต “อีเมลปลอม”
องค์กรหรือเจ้าหน้าที่ขององค์กรจริง
ชื่อบัญชีอีเมลมักต่อท้ายด้วยชื่อย่อ
ขององค์กรนั้น ๆ



สังเกต “สัญลักษณ์รูปกุญแจ”
ระบบธนาคารออนไลน์จะต้องมีการเข้ารหัส
ปลอดภัยที่หน้าเว็บไซต์ที่ให้ลงชื่อเข้าใช้ระบบ



สังเกต “URL”

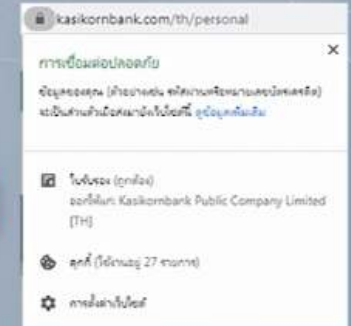


ตรวจสอบลิ้งค์เชื่อมโยงเว็บไซต์



สังเกต “ชื่อผู้ให้บริการ”

สังเกตจากตัวอักษรที่อยู่ถัดจากรูปกุญแจ
หรือโดยการคลิกที่สัญลักษณ์รูปกุญแจจะเห็นชื่อสถาบัน



แนวทางการจัดการความเสี่ยงการถูกรุกรานผ่านอินเทอร์เน็ต



การทำธุรกรรมทางการเงินผ่านสมาร์ทโฟนหรือแท็บเล็ต
ควรใช้แอปพลิเคชัน (Application) ของธนาคารโดยตรง



หลีกเลี่ยง !

การใช้งานธนาคารออนไลน์
ผ่านสมาร์ทโฟนและแท็บเล็ต
ที่ผ่านการ Jailbreak หรือ Root แล้ว

3. หลีกเลี่ยงเข้าเว็บไซต์ธนาคารออนไลน์จากสมาร์ทโฟนหรือแท็บเล็ต

หลีกเลี่ยง !

การเข้าใช้เว็บไซต์ธนาคารออนไลน์
ผ่านสมาร์ทโฟนและแท็บเล็ตบางรุ่น
ที่ไม่แสดงสัญลักษณ์รูปกุญแจ



ลือคหน้าจอการเข้าใช้สมาร์ทโฟนหรือแท็บเล็ตด้วย
รหัสผ่าน (Password) ที่ยากต่อการเดา

แนวทางการจัดการความเสี่ยงการทารุณกรรมผ่านอินเทอร์เน็ต

4. ป้องกันโปรแกรมอันตรายต่าง ๆ

- หลีกเลี่ยงการติดตั้งระบบปฏิบัติการและโปรแกรมที่ไม่มีลิขสิทธิ์
- ควรติดตั้งโปรแกรมรักษาความปลอดภัย Personal Firewall, Antivirus
- กรณีที่ใช้ระบบปฏิบัติการ Windows ควรเปิดใช้งาน Windows Firewalls และอัปเดตโปรแกรมความปลอดภัยของระบบปฏิบัติการ (Security Patch) อย่างสม่ำเสมอ
- ตรวจสอบไวรัส (Scan Virus) ทุกครั้งก่อนใช้บริการธนาคารออนไลน์
- หลีกเลี่ยงการเชื่อมต่อ หรือเข้าสู่ระบบจากอินเทอร์เน็ตสาธารณะรวมไปถึงการเชื่อมต่อกับฟรี Wifi
- ควรแยกเครื่องคอมพิวเตอร์ที่ใช้สำหรับทำธุรกรรมทางการเงินกับเครื่องคอมพิวเตอร์ที่ใช้ท่องโลกออนไลน์ หรือทำงานอื่น
- ติดตามข่าวสารกลไกของภัยทางการเงินอย่างสม่ำเสมอ

ข้อดีของการโอนเงินออนไลน์



ความสะดวก

- รวดเร็ว
- ประหยัดเวลา
- ประหยัดค่าใช้จ่ายในการเดินทาง
- สามารถโอนได้ทุกที่ทุกเวลาที่ต้องการ

ไม่ต้องพกเงินสด
จำนวนมาก
เวลาไปข้างนอก



ข้อเสียของการโอนเงินออนไลน์



ข้อจำกัดในการ
เข้าถึงอินเทอร์เน็ต



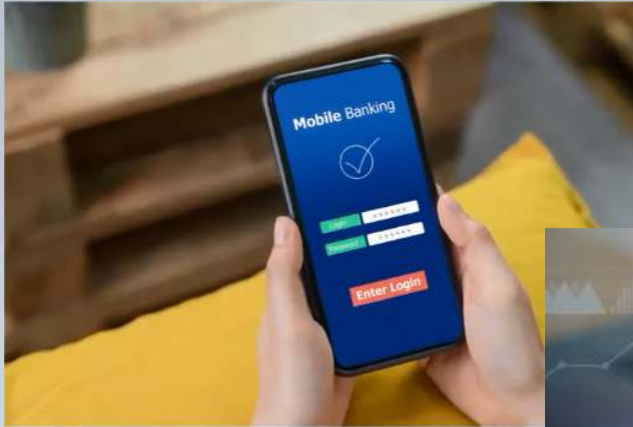
ควบคุมการใช้เงิน
ได้ยากมากขึ้น

ต้องระวัง !
เรื่องความปลอดภัย



เทคโนโลยีในการใช้งาน
อาจทำให้ผู้ใช้บริการ
บางรายสับสน





งาน

ให้นักศึกษา **สรุป**เนื้อหาจากการเรียน สัปดาห์ 12 ถึง 15
หรือทำเป็น Mind Mapping ในกระดาษ A4 1 หน้า
(ห้ามเกิน 1 หน้า A4) ต่อ 1 เนื้อหาสัปดาห์
ส่งที่ Classroom รายวิชา