2 แกะเปลือกสายที่เชื่อมระหว่างตู้เอทีเอ็มกับธนาคารแล้วเชื่อมต่อสายทองแดงเข้าไปเพื่อดักรับหรือเปลี่ยนแปลงข้อมูลที่รับส่ง (**Wire tapping**)


MasterCard
Maestro
Cirrus


Insert Here
VISA
VISA
Cirrus
PLUS

3 ใช้อุปกรณ์บางอย่างไปปิดทับช่องที่เงินออก

เมื่อผู้ใช้กดถอนเงินแล้วจะไม่ได้รับเงินที่กด หลังจากเดินออกจากตู้ คนร้ายกลับมานำเงินออก (Slot tampering)


1
2
3
STOP
4
5
6
CORR.
7
8
9
OK
0

4 ใช้เทปกาวติดไว้ในช่องใส่บัตร เมื่อผู้ใช้บริการสอดบัตรเข้าไปในเครื่อง จะติดอยู่ข้างใน คนร้ายแกล้งทำเป็นว่าเดินมาเสนอให้ความช่วยเหลือ โดยลองกดรหัสบัตรเพื่อให้เครื่องคายบัตร แต่กดอย่างไรเครื่องก็ไม่ยอมคาย พอหลังจากที่เหยื่อเดินออกจากตู้แล้วคนร้ายจะนำบัตรเอทีเอ็มออกมาแล้วกดเงินเอง (**Lebanese Loop)**

How the scam works

1 Thief puts thin plastic or metal sleeve into the cash machine slot. Customer is left unaware as it is difficult to see from the outside.

2 When next customer tries to withdraw money, card is caught in sleeve. The machine continues to ask for PIN number as it cannot read the card.

3 As customer tries to key in PIN number again, thief either 'shoulder surfs' to see number or stands nearby with micro-camera.

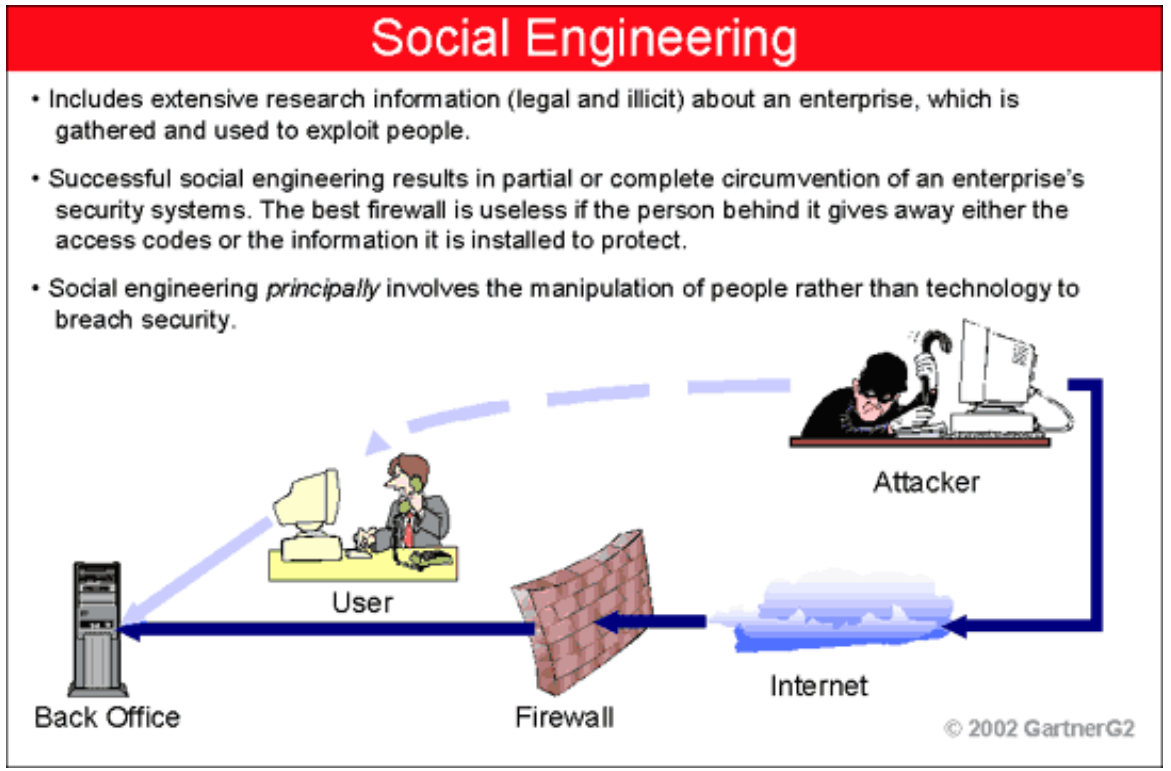
4 Customer leaves thinking the machine has 'swallowed' card and thief moves in to remove sleeve with card inside. Card is either reused or skimmed for data and cloned.

5 สร้างตู้เอทีเอ็มปลอม มาวางไว้ข้างๆ ตู้เอทีเอ็มของจริง


自动柜员机 ATM
中国银行
BANK OF CHINA
自动柜员机 ATM

6 Case call center – Social Engineering Attack

GSM
Voip



Wetalk IOS

WePhone Android

องค์กรอาชญากรรมข้ามชาติ

แก๊งคอลเซ็นเตอร์

สำนักงานป้องกันและปราบปรามการฟอกเงิน
Anti-Money Laundering Office (AMLO)

สายด่วน ปปง.

1710

แจ้งร้องเรียน ร้องทุกข์
เบาะแสการฟอกเงิน

ระวัง! จะเสียเงินฟรี

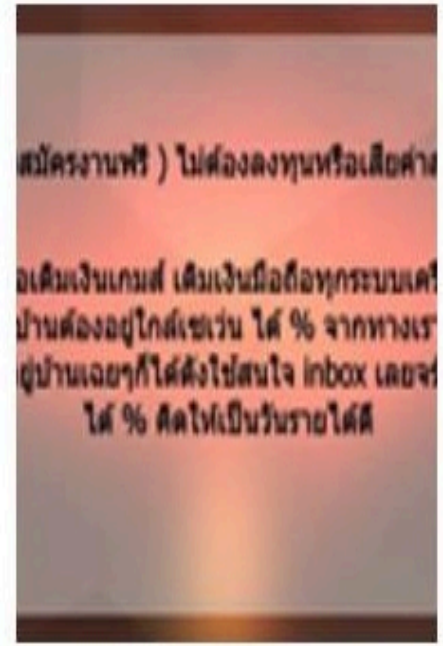
อย่าหลงเชื่อคนร้ายโทรศัพท์หลอกให้โอนเงิน
ผ่านตู้เอทีเอ็ม หรือตู้รับฝากเงินสด

โทร. Hotline : 1710

[redacted]orn ▶️ หางานกรุงเทพ งานอิสระ

21 hours ago ·

รับสมัครเติมเงินออนไลน์ #ไม่เสียค่าสมัครจ้า สนใจติดต่อขออายุ 18 ปีขึ้นไป #รับ2คนจ้ะ รายได้ #300บขึ้นไปต่อวัน



2

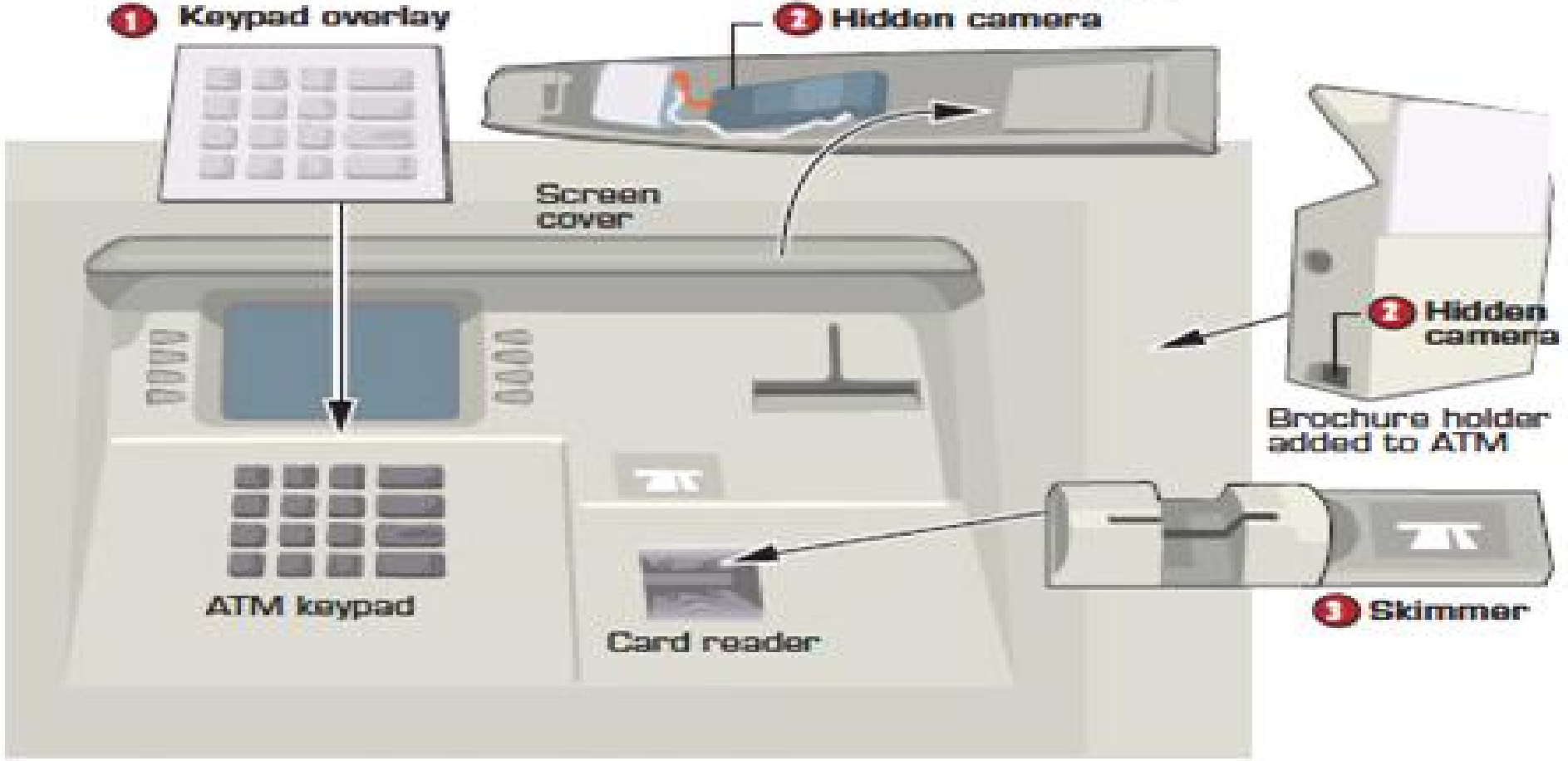
1 Comment

7 Skimmer

card 'skim' scheme

ATM cardholders have been warned for years about the dangers of card skimmers. The technology is now so compact that many consumers might not notice it. Here are some elements of a typical skim operation.

1. Keypad overlays capture PIN numbers on a memory chip.
2. Hidden cameras can also copy customers' PIN numbers.
3. Skimmers are placed over the card reader to copy the card's magnetic stripe. These are often legal credit card readers.

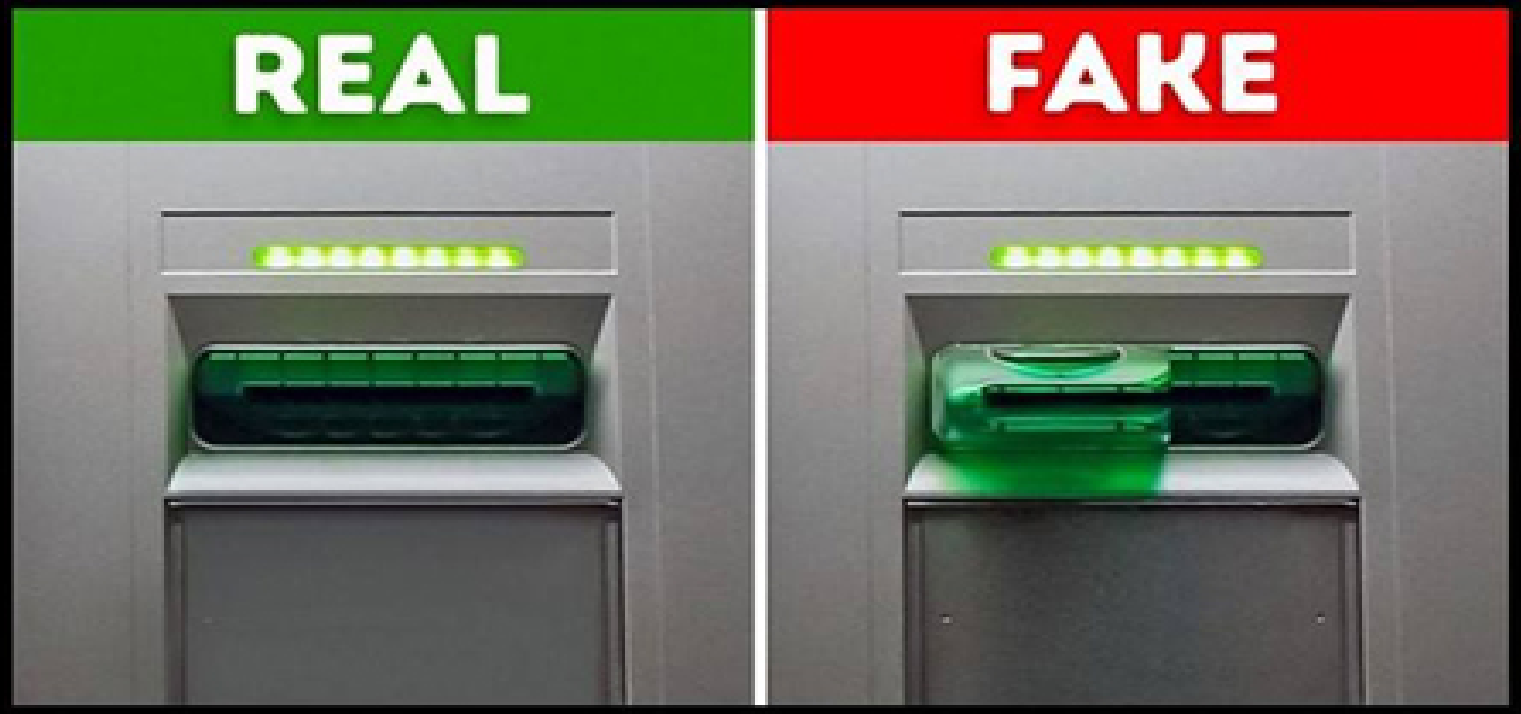


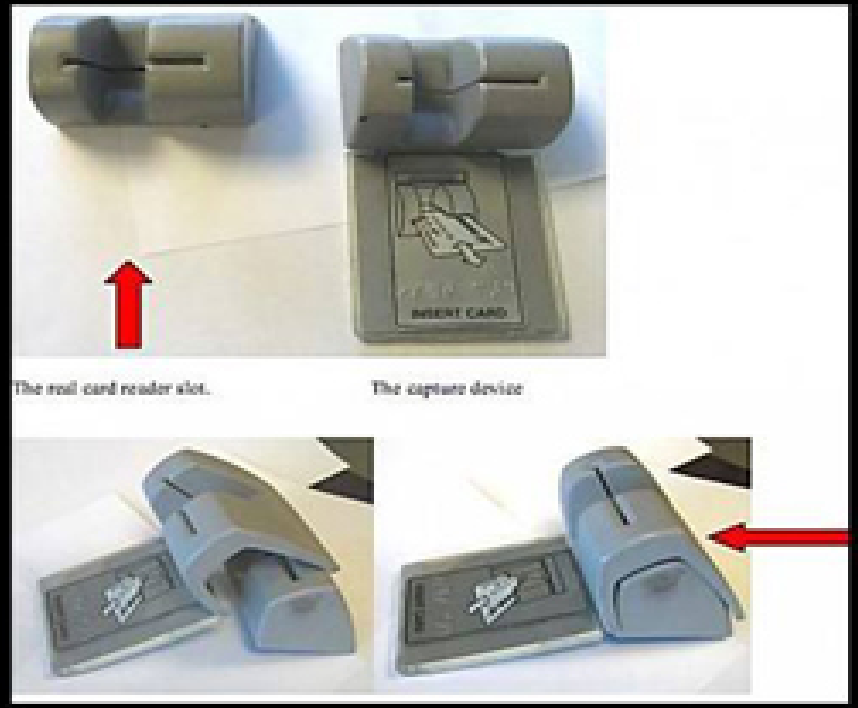
Sources: about.com, networkworld.com, ATM Parts & Services

BALTIMORE SUN GRAPHIC: LAMONT W. HARVEY


Looking For
An Envelope?


Receipt


REAL
FAKE


INSERT CARD
The real card reader slot.
The capture device

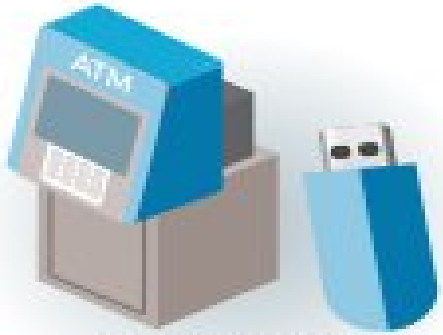
8.Malware
“ATM Jackpotting”


JACKPOT
BAR BAR BAR
7 7 7

Insight this case

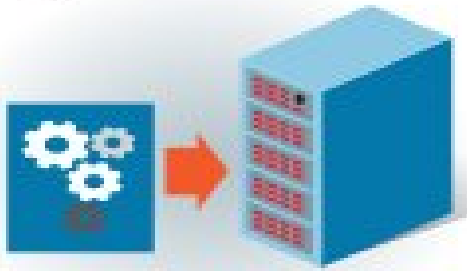
1. ATM Physical
2. One Key All Machine
3. Default Password
4. Vulnerability

ภัยมัลแวร์แฮกตู้เอทีเอ็ม



เสียบยูเอสบี
หรือบัตรเอทีเอ็มเข้าตู้
เพื่อปล่อยมัลแวร์

ถ่ายโอนไฟล์
เข้าระบบธนาคาร



ถ่ายโอนไฟล์
เข้าเซิร์ฟเวอร์

รีโมทแฮก
จากอินเทอร์เน็ต

เมื่อมัลแวร์ถูกติดตั้ง แฮกเกอร์รีโมท
สั่งให้เครื่องจ่ายเงินสดออกมา
โดยกำหนดวัน/เวลาที่แน่นอน

เป้าหมายอยู่ที่เครื่องเอทีเอ็มซึ่งใช้
ระบบปฏิบัติการวินโดว์ส ซีอี วินโดว์ส เอ็กซ์พี
หรือวินโดว์ส 7 ที่ไมโครซอฟท์ประกาศ
ยุติการให้บริการไปแล้ว

วิธีป้องกันภัยคุกคาม

กราฟฟิก กรุงเทพธุรกิจ

- ธนาคารต้องสแกนไวรัสตามตารางพื้นฐาน ที่ใช้เทคโนโลยี Whitelisting
- กำหนดนโยบายจัดการอุปกรณ์ที่ดี เข้ารหัสดิสก์อยู่เสมอ
- ปกป้อง BIOS ของตู้เอทีเอ็มด้วยรหัสผ่าน
- อนุญาตการบูตเครื่องฮาร์ดดิสก์เท่านั้น
- แยกเน็ตเวิร์คของตู้เอทีเอ็ม ออกจากเน็ตเวิร์คภายในอื่นๆ ของธนาคาร
- จัดแคมเปญทดสอบยูสเซอร์ว่าสนองต่ออีเมลประเภทแฝงไวรัส แฝงลิงค์ที่นำไปสู่การเป็นเหยื่อของแรนซัมแวร์หรือไม่
- ล็อกเอาท์ออกจากระบบทุกครั้งที่ไม่ใช้งาน

1.4 Payment Gateway Fraud

แนวโน้มธนาคารมุ่งเป็น **Partner** กับ **Platform** ที่สร้างงาน เช่น **Lazada , Grab** หรือ **Fastwork** เป็นต้น

เพราะธนาคารต้องการแลกเปลี่ยนข้อมูล เช่น ความถี่การจ้างงาน จำนวนเงินที่จ้าง เพื่อพิจารณา อนุมัติ **Pesonal Loan** กรณีผู้กู้ทำงานฟรีแลนซ์ เป็นต้น

Payment Gateway Fraud

1 เจ้าของบัตรเครดิต นำบัตรตนเองไปรูด

2 เจ้าของบัตร ถูกขโมยบัตรไปรูด

3 เจ้าของบัตร ถ่ายเลขบัตร ไปซื้อของ แล้วไม่ได้ของ

4 เจ้าของบัตร ถูกแอบถ่ายบัตร ไปซื้อของ

How to credit card work?

Credit Card Machine

Payment - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites Media Address Links

PAYMENT GATEWAY

ธนาคารกสิกรไทย KASIKORNBANK

Payment Detail

VISA KBANK e-Web Card VERIFIED by VISA MasterCard SecureCode

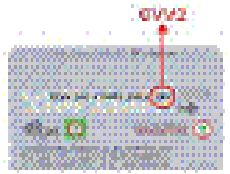
K-Payment Gateway is the highly secure payment processor for your seller, **MERCHANT TEST**. Please verify the purchase information and enter your credit card details below.

Pay To:	MERCHANT TEST
Invoice No:	000000002101
Payment For:	Test Payment
Amount:	1.00 Baht

Payment Gateway

Credit Card Number:

Security Code (CVV2): Last 3 digits on the back ofhe card



Expiry Date (mm/yyyy): MM YYYY

Card Type : Please Select One

Country of Issuing Bank : Please Select One

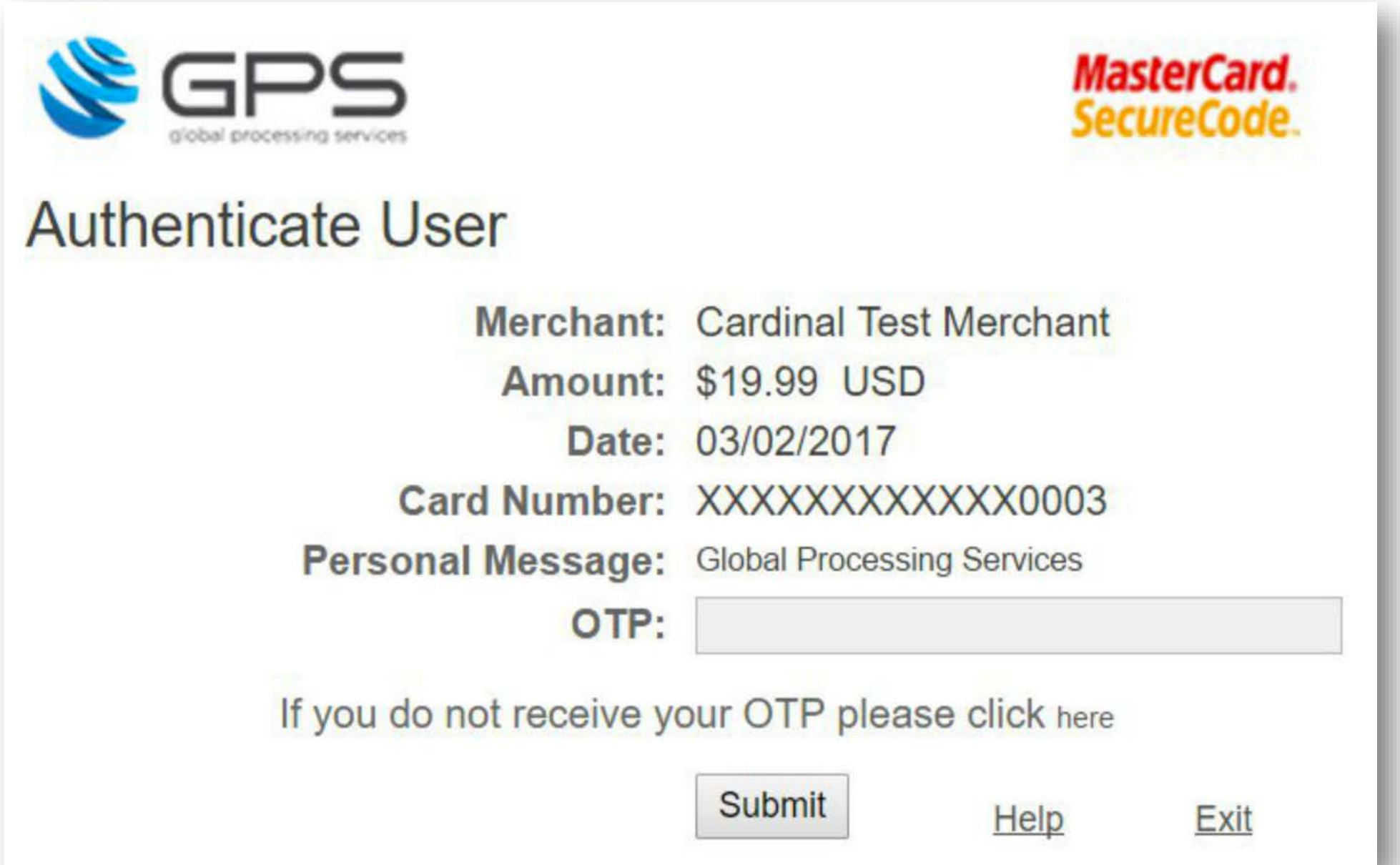
Issuing Bank :

Not in List (Please Specific):

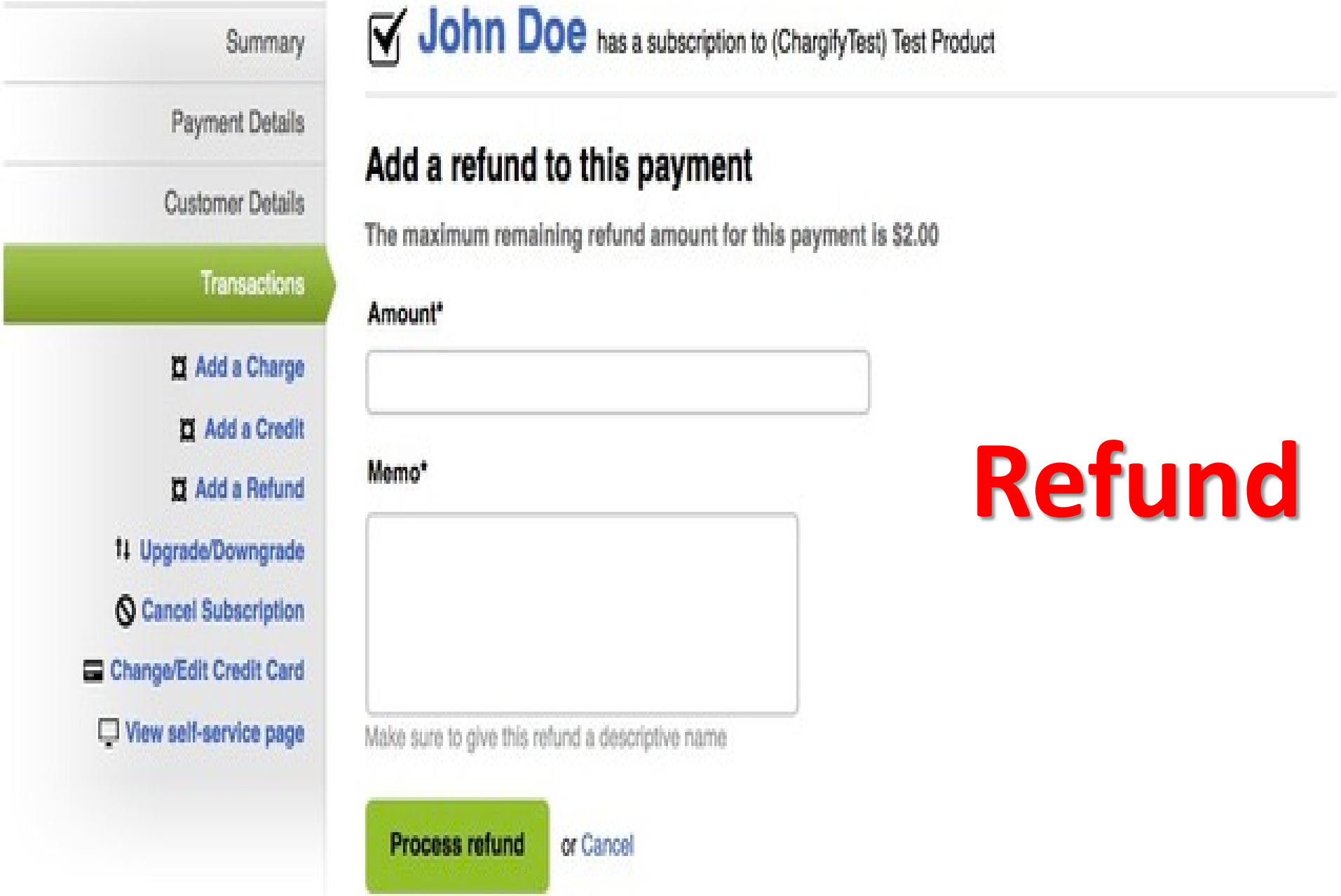
PAY NOW

Done Internet

3D Secure


GPS
global processing services
MasterCard.
SecureCode.
Authenticate User
Merchant: Cardinal Test Merchant
Amount: $19.99 USD
Date: 03/02/2017
Card Number: XXXXXXXXXXXX0003
Personal Message: Global Processing Services
OTP:
If you do not receive your OTP please click here
Submit
Help
Exit

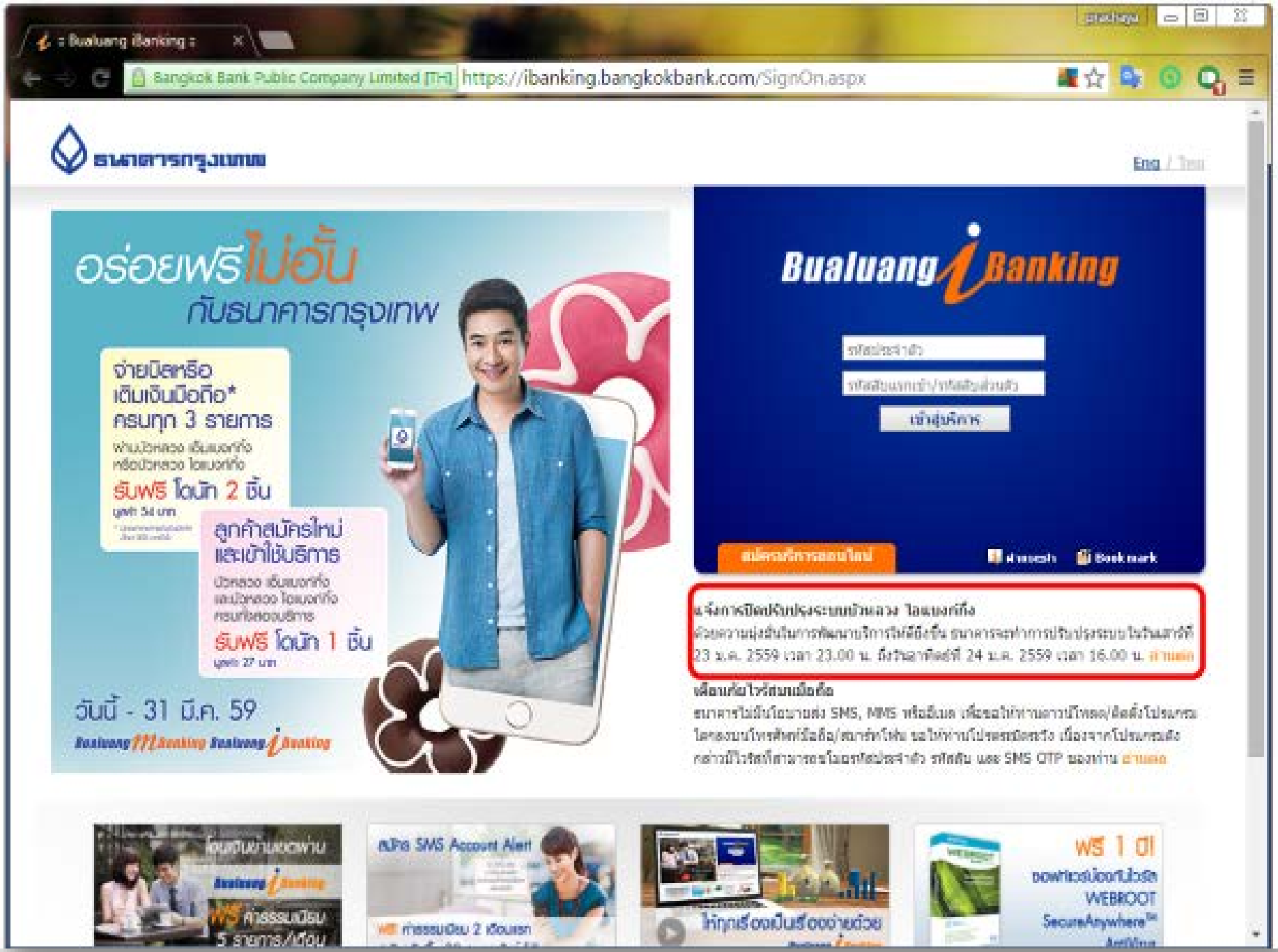
3D Secured and credit card payment

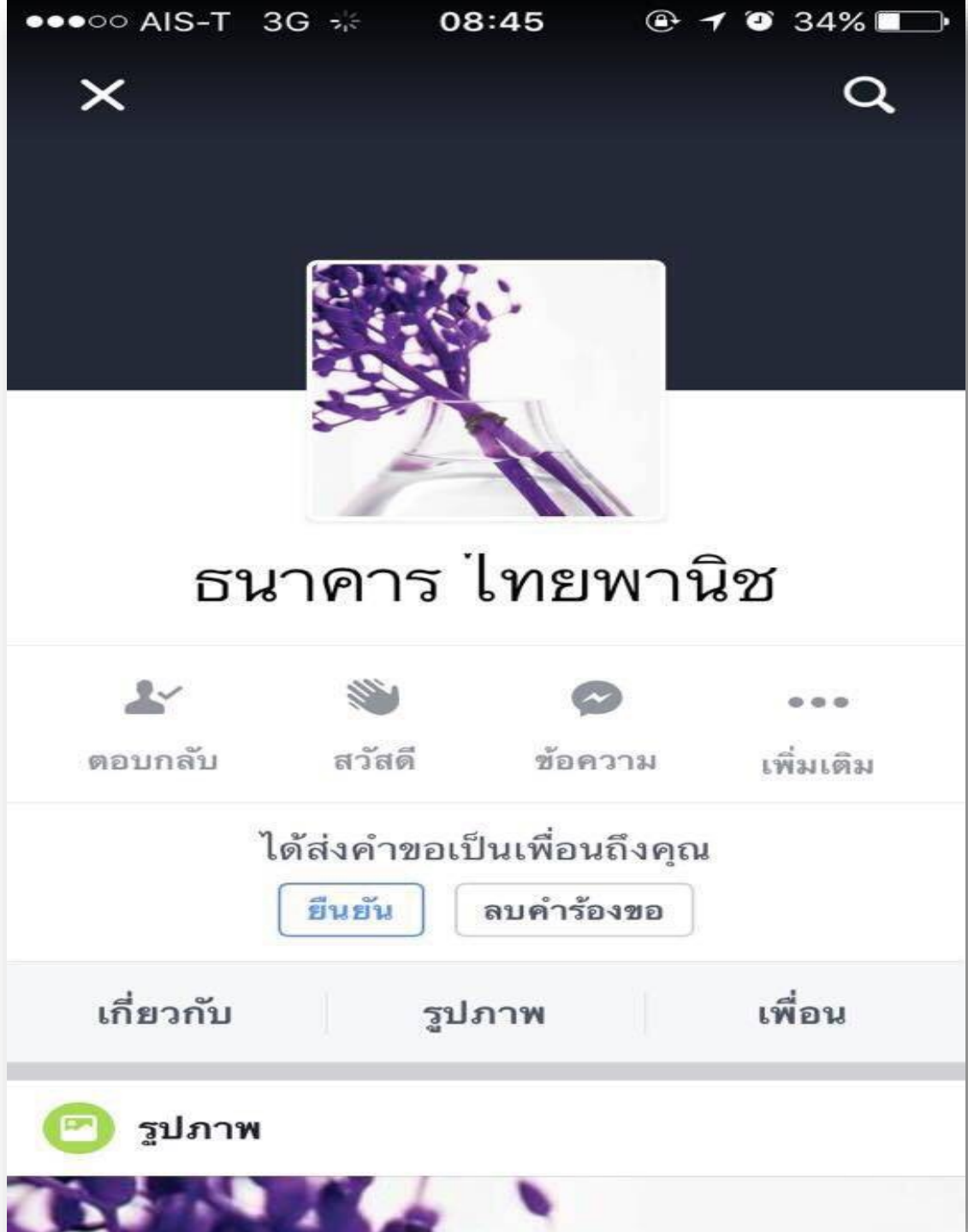

Summary
Payment Details
Customer Details
Transactions
Add a Charge
Add a Credit
Add a Refund
Upgrade/Downgrade
Cancel Subscription
Change/Edit Credit Card
View self-service page
John Doe has a subscription to (ChargifyTest) Test Product
Add a refund to this payment
The maximum remaining refund amount for this payment is $2.00
Amount*
Memo*
Make sure to give this refund a descriptive name
Process refund
or Cancel
Refund

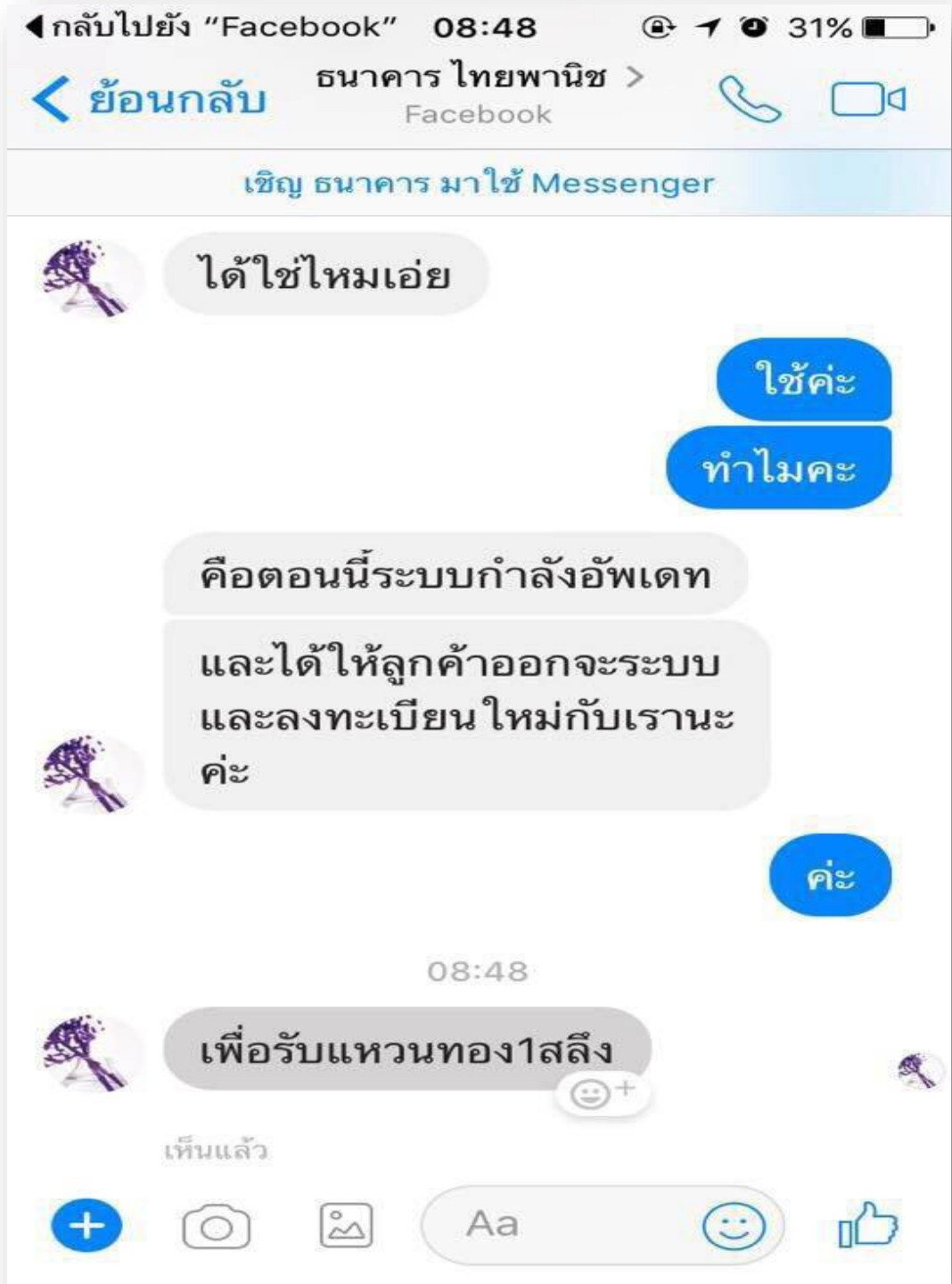
How to refund?

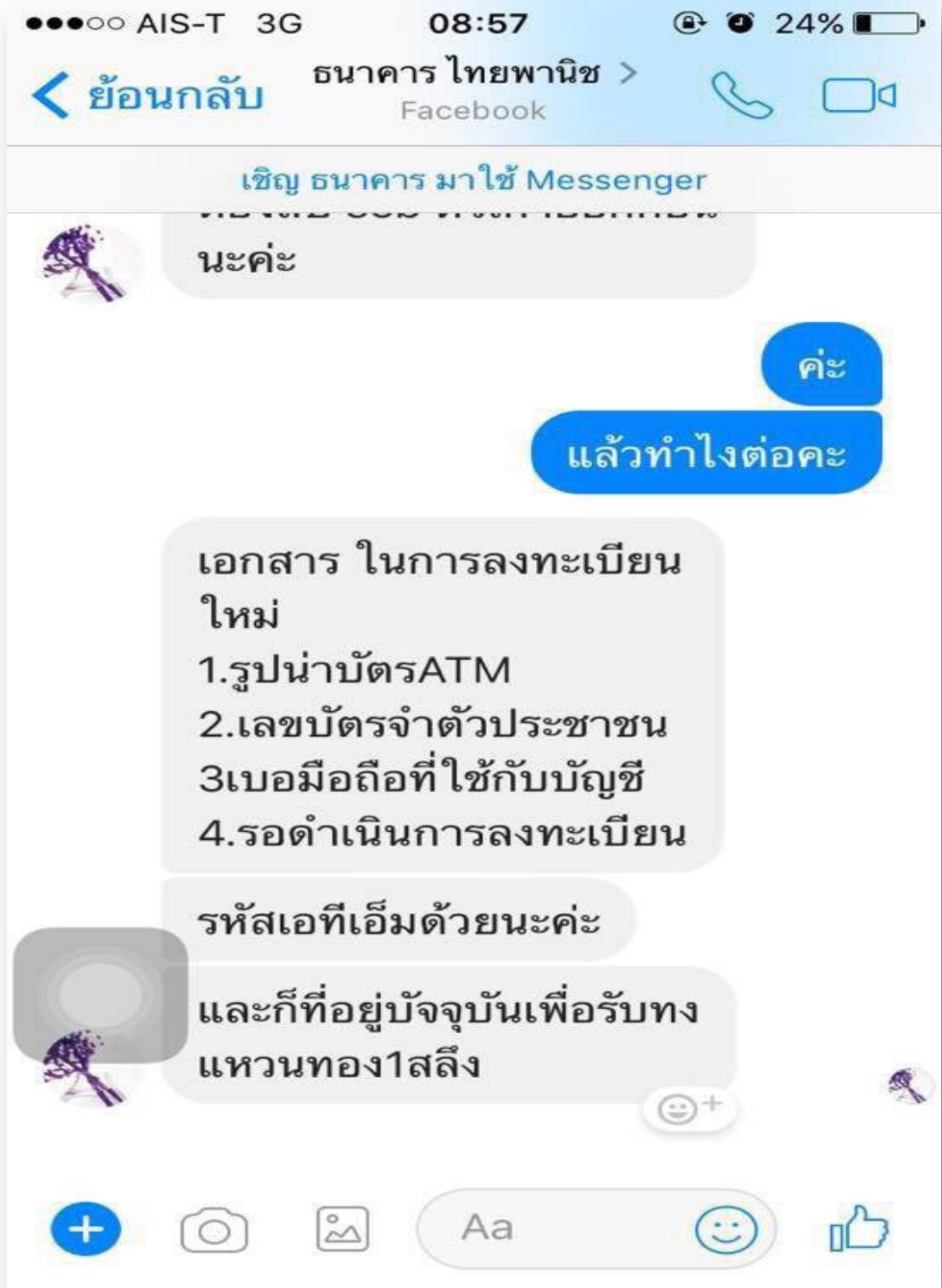
Online Transaction

1.5 Internet Banking Fraud (7 Cases)


: Bualuang iBanking :
Bangkok Bank Public Company Limited [TH]
https://ibanking.bangkokbank.com/SignOn.aspx
ธนาคารกรุงเทพ
อร่อยฟรีไม่อั้น
กับธนาคารกรุงเทพ
จ่ายบิลหรือ
เติมเงินมือถือ*
ครบทุก 3 รายการ
รับฟรี โดนัท 2 ชิ้น
ลูกค้าสมัครใหม่
และเข้าใช้บริการ
รับฟรี โดนัท 1 ชิ้น
วันนี้ - 31 มี.ค. 59
Bualuang iBanking
เข้าสู่ระบบ
สมัครบริการออนไลน์
Book mark
ฟรี 1 ปี
WEBROOT
SecureAnywhere


AIS-T 3G 08:45 34%
ธนาคาร ไทยพานิช
ตอบกลับ
สวัสดี
ข้อความ
เพิ่มเติม
ได้ส่งคำขอเป็นเพื่อนถึงคุณ
ยืนยัน
ลบคำร้องขอ
เกี่ยวกับ
รูปภาพ
เพื่อน
รูปภาพ

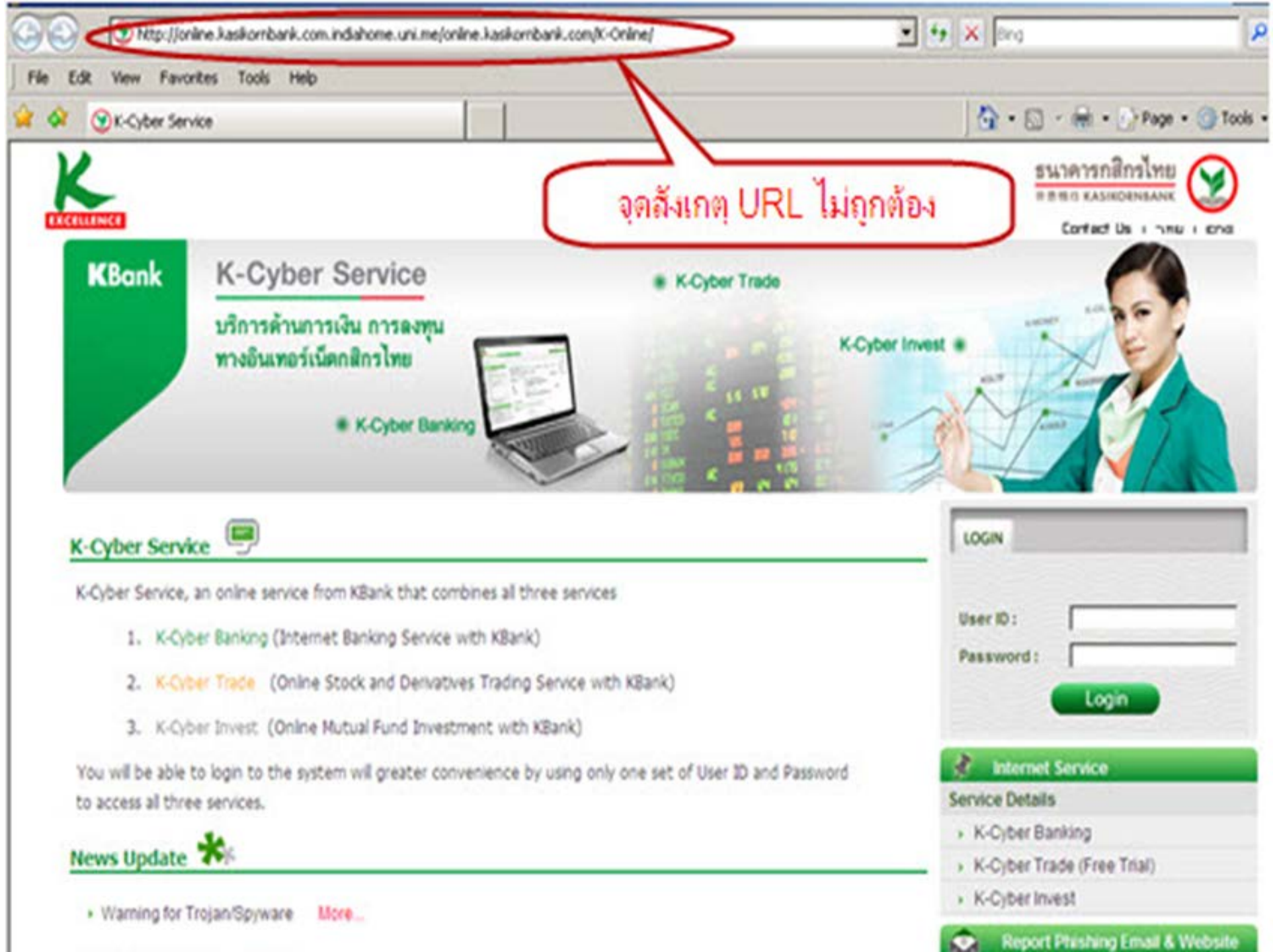

กลับไปยัง "Facebook" 08:48 31%
ย้อนกลับ
ธนาคาร ไทยพานิช >
Facebook
เชิญ ธนาคาร มาใช้ Messenger
ได้ใช่ไหมเอ่ย
ใช้ค่ะ
ทำไมคะ
คือตอนนี้ระบบกำลังอัพเดท
และได้ให้ลูกค้าออกจะระบบ
และลงทะเบียนใหม่กับเรานะ
ค่ะ
ค่ะ
08:48
เพื่อรับแหวนทอง1สลึง
เห็นแล้ว
Aa


AIS-T 3G
08:57
24%
ย้อนกลับ
ธนาคาร ไทยพานิช >
Facebook
เชิญ ธนาคาร มาใช้ Messenger
นะค่ะ
ค่ะ
แล้วทำไงต่อคะ
เอกสาร ในการลงทะเบียน
ใหม่
1.รูปน่าบัตรATM
2.เลขบัตรจำตัวประชาชน
3เบอมือถือที่ใช้กับบัญชี
4.รอดำเนินการลงทะเบียน
รหัสเอทีเอ็มด้วยนะค่ะ
และก็ที่อยู่บัจจุบันเพื่อรับทง
แหวนทอง1สลึง
Aa

1) Phishing

----- Forwarded Message -----
From: Kasikorn Bank <alert@kasikorn.com>
To: [redacted]com
Sent: Saturday, September 15, 2012 7:23 PM
Subject: New Message From Kasikorn Bank

Dear Esteemed Customer,
At Kasikorn Bank Thailand, We take security Seriously. You are recieving This Email as you are a customer with Kasikorn Bank.
Your Account has been flagged for security issues, you must now login and validate your account for your own protection. กรุณาอย่าคลิกลิ้งค์ใดๆ ที่อยู่ในอิเมลล์หลอกลวงนี้
Click here to login and validate your Account
This Email is subject to security From Kasikorn Bank,Please view our privacy poliy statement.
Regards,
Technical Service /Internet security,
Kasikorn Bank,
Thailand


http://online.kasikornbank.com.indiahome.uni.me/online.kasikornbank.com/K-Online/
File Edit View Favorites Tools Help
K-Cyber Service
Page Tools
จุดสังเกต URL ไม่ถูกต้อง
ธนาคารกสิกรไทย
KASIKORNBANK
Contact Us
KBank
K-Cyber Service
บริการด้านการเงิน การลงทุน
ทางอินเทอร์เน็ตกสิกรไทย
K-Cyber Trade
K-Cyber Banking
K-Cyber Invest
K-Cyber Service
K-Cyber Service, an online service from KBank that combines all three services
1. K-Cyber Banking (Internet Banking Service with KBank)
2. K-Cyber Trade (Online Stock and Derivatives Trading Service with KBank)
3. K-Cyber Invest (Online Mutual Fund Investment with KBank)
You will be able to login to the system will greater convenience by using only one set of User ID and Password to access all three services.
News Update
Warning for Trojan/Spyware More...
LOGIN
User ID :
Password :
Login
Internet Service
Service Details
K-Cyber Banking
K-Cyber Trade (Free Trial)
K-Cyber Invest
Report Phishing Email & Website

"AVG AntiVirus Mobile PRO" สำหรับลูกค้า Kasikorn Bank

Kasikorn Bank ให้ลูกค้าใช้ "AVG AntiVirus Mobile PRO" โดยไม่เสียค่าใช้จ่ายเพื่อป้องกันในระหว่างทำธุรกรรมการเงิน

ระบุหมายเลขโทรศัพท์มือถือเพื่อรับ URL ในการดาวน์โหลด (ต้องเป็นหมายเลขที่จดทะเบียนใน Kasikorn Bank)

+66 (0)

ถัดไป

แนะนำผลิตภัณฑ์และสิทธิพิเศษ

บริการทุกระดับประทับใจ

เข้าสู่ระบบ

รหัสผู้ใช้งาน :

รหัสผ่าน :

เข้าสู่ระบบ

บริการทางอินเทอร์เน็ต

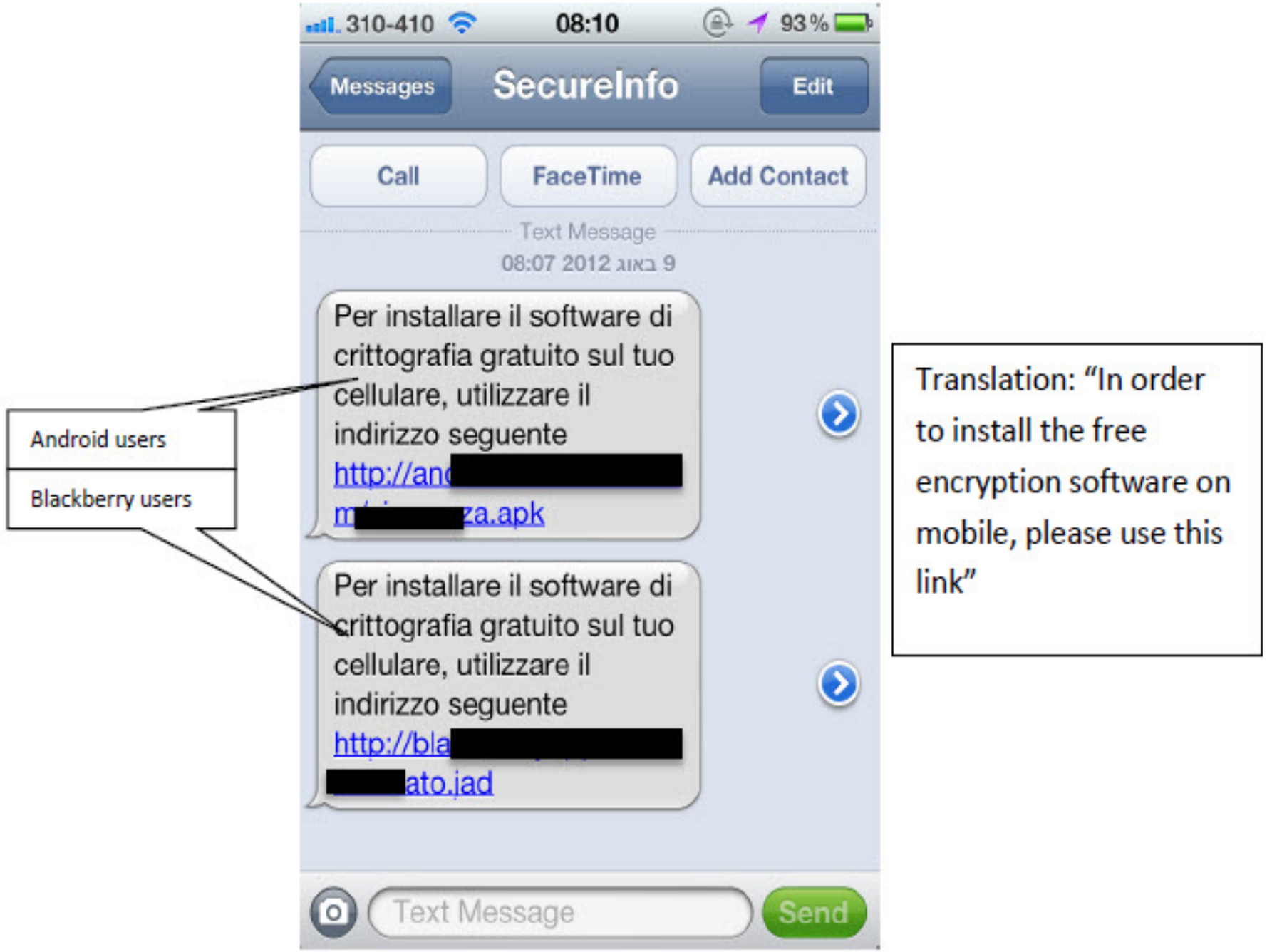
รายละเอียดบริการ

- K-Cyber Banking
- K-Cyber Trade (ทดลองใช้ 15 วัน)
- K-Cyber Invest

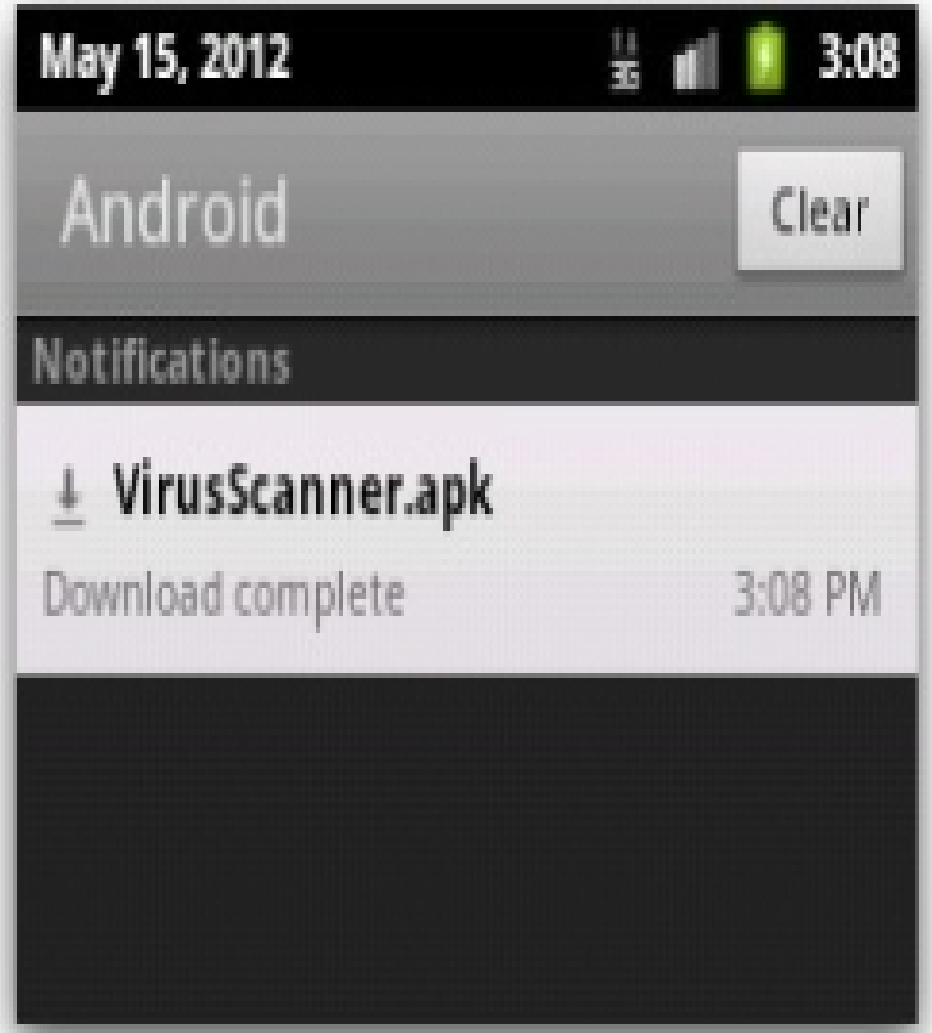
Report Phishing Email & Website

ท่านสามารถแจ้งอีเมล์หรือเว็บไซต์ที่น่าสงสัย
ที่มีการแอบอ้างชื่อธนาคารกสิกรไทย โปรดส่ง
เมลมาที่
report.phishing@kasikornbank.com

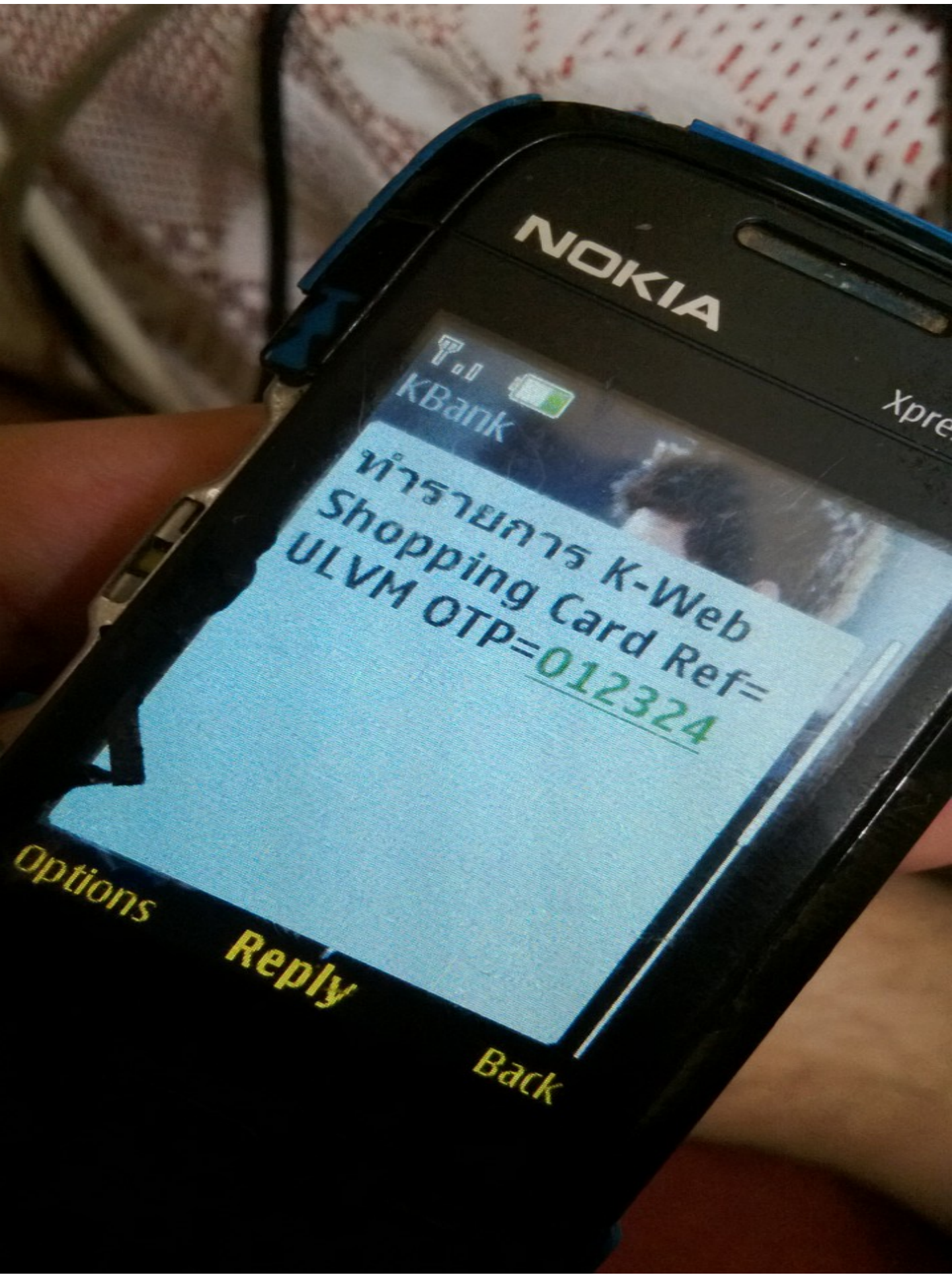
Security Tips
คำแนะนำเรื่องความปลอดภัย

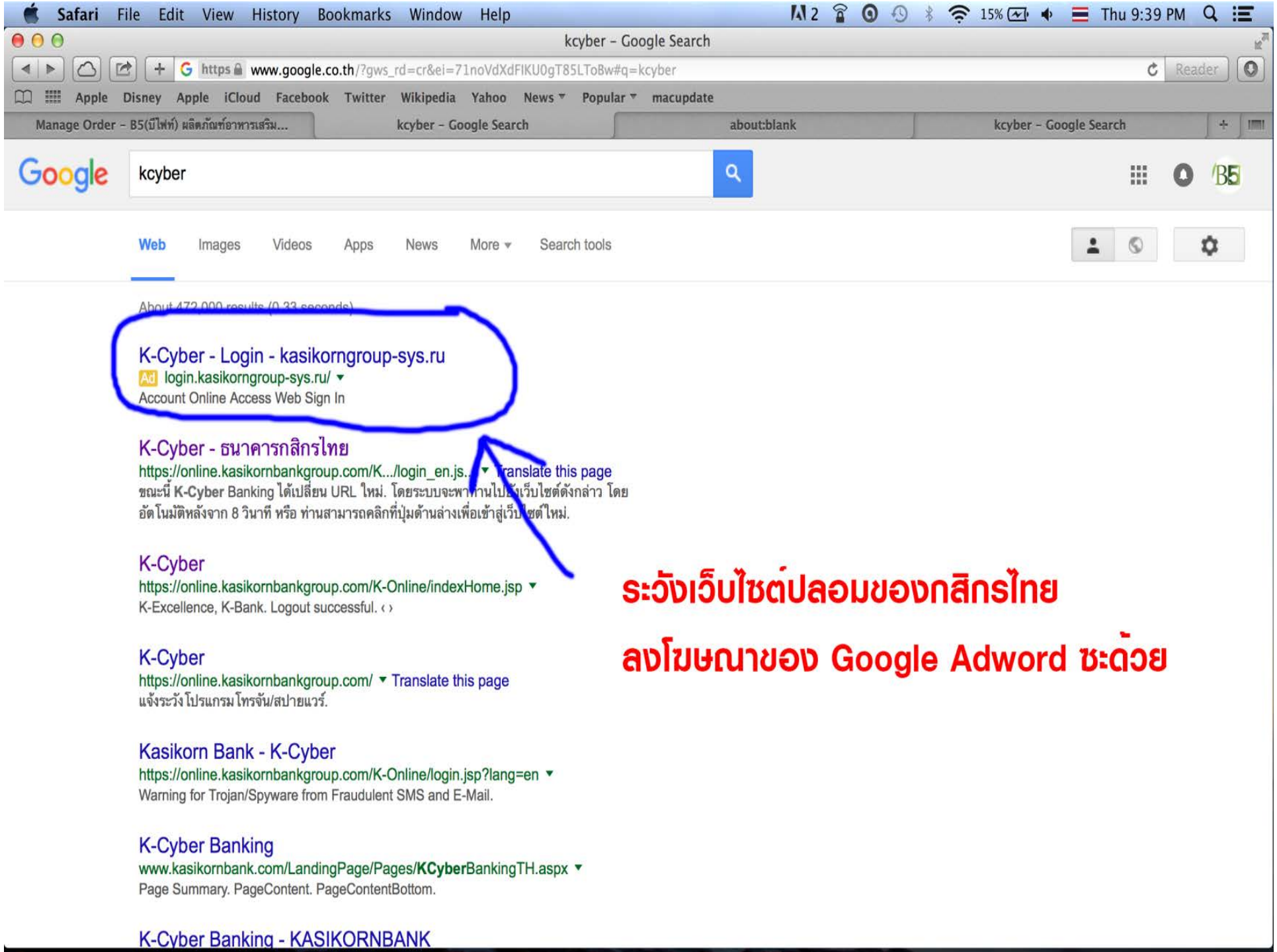


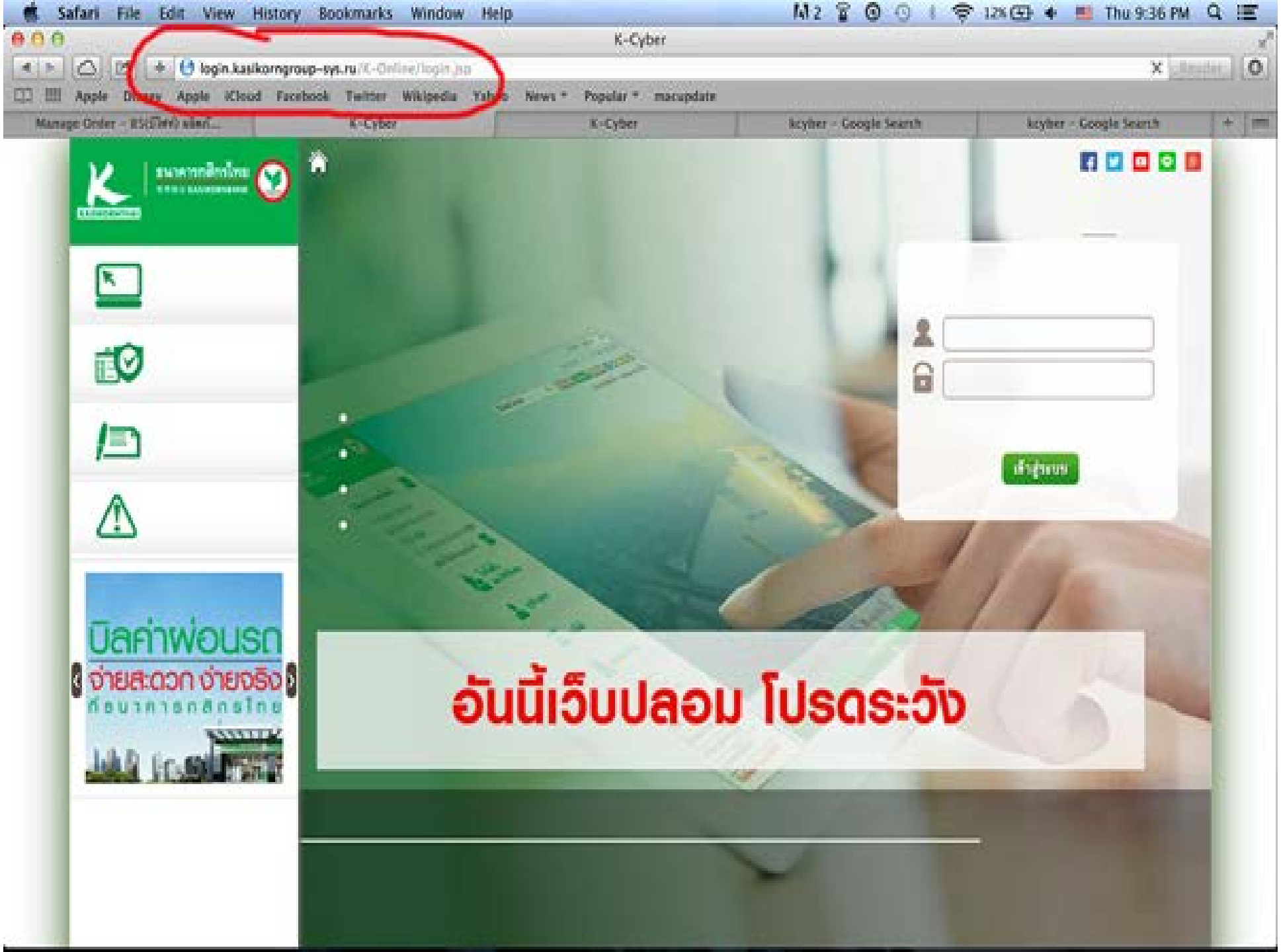
Translation: "In order to install the free encryption software on mobile, please use this link"

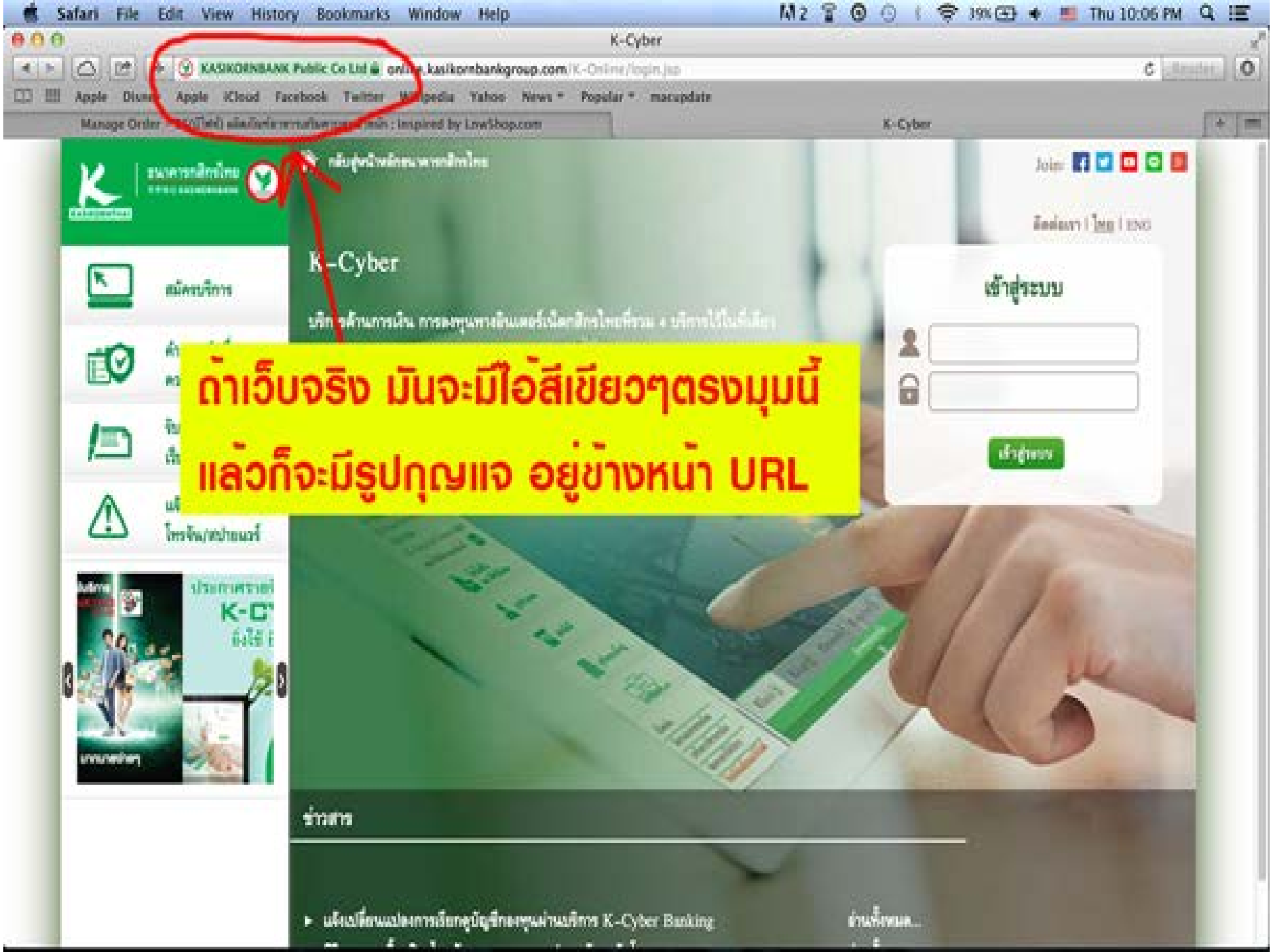

May 15, 2012
3:08
Android
Clear
Notifications
VirusScanner.apk
Download complete
3:08 PM


3:11
Antivirus
Browser
Calculator
Calendar
Camera
Clock
Contacts
Dev Tools
Downloads
Email
Gallery
Messaging

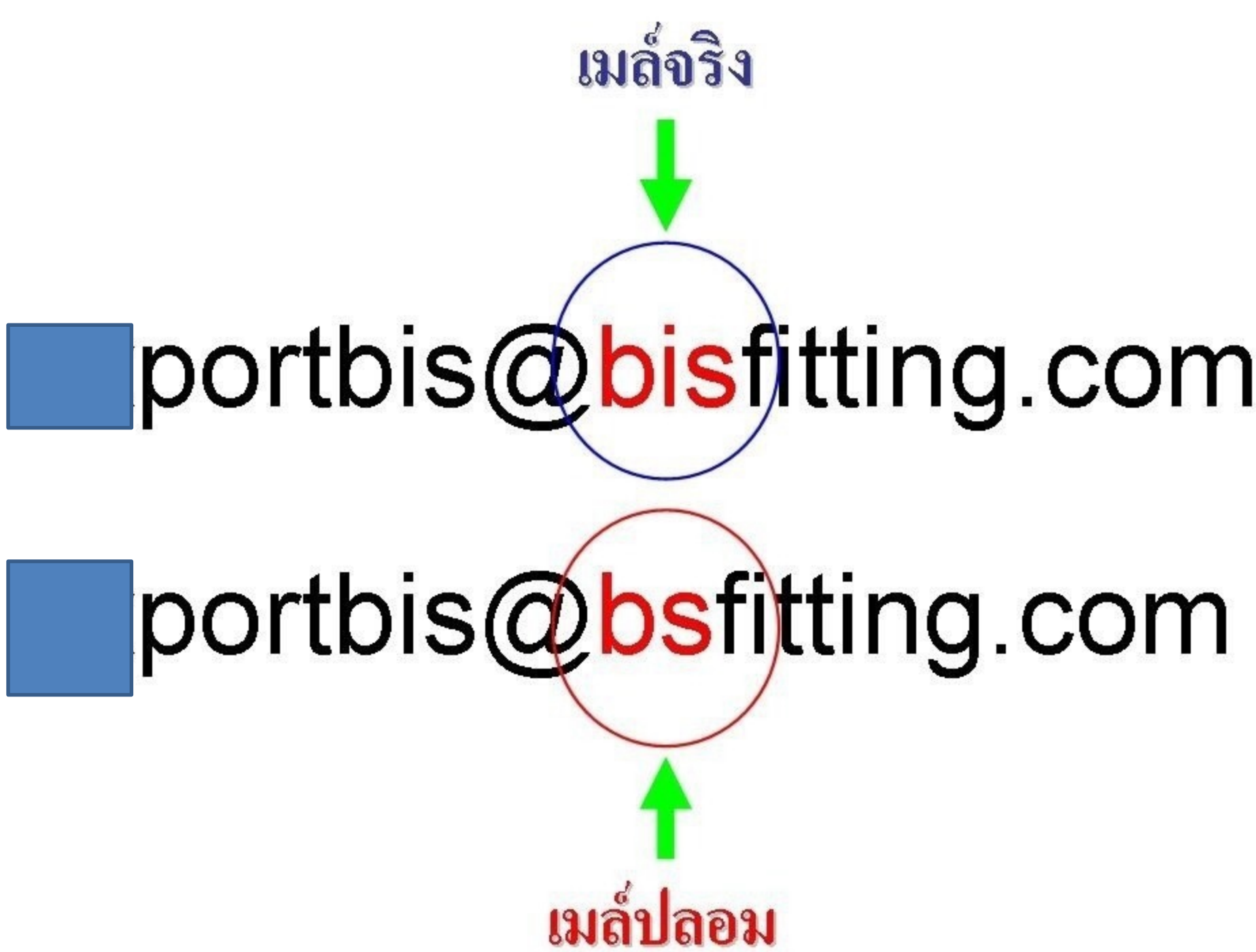

NOKIA
KBank
ทำรายการ K-Web
Shopping Card Ref=
ULVM OTP=012324
Options
Reply
Back


Safari File Edit View History Bookmarks Window Help
Thu 9:39 PM
kcyber - Google Search
https www.google.co.th/?gws_rd=cr&ei=71noVdXdFIKU0gT85LToBw#q=kcyber
Reader
Apple Disney Apple iCloud Facebook Twitter Wikipedia Yahoo News Popular macupdate
Manage Order - B5(บีไฟท์) ผลิตภัณฑ์อาหารเสริม...
kcyber - Google Search
about:blank
kcyber - Google Search
Google
kcyber
Web Images Videos Apps News More Search tools
About 472,000 results (0.33 seconds)
K-Cyber - Login - kasikorngroup-sys.ru
Ad login.kasikorngroup-sys.ru/
Account Online Access Web Sign In
K-Cyber - ธนาคารกสิกรไทย
https://online.kasikornbankgroup.com/K.../login_en.js... Translate this page
ขณะนี้ K-Cyber Banking ได้เปลี่ยน URL ใหม่. โดยระบบจะพาท่านไปยังเว็บไซต์ดังกล่าว โดย
อัตโนมัติหลังจาก 8 วินาที หรือ ท่านสามารถคลิกที่ปุ่มด้านล่างเพื่อเข้าสู่เว็บไซต์ใหม่.
K-Cyber
https://online.kasikornbankgroup.com/K-Online/indexHome.jsp
K-Excellence, K-Bank. Logout successful.
K-Cyber
https://online.kasikornbankgroup.com/ Translate this page
แจ้งระวังโปรแกรมโทรจัน/สปายแวร์.
Kasikorn Bank - K-Cyber
https://online.kasikornbankgroup.com/K-Online/login.jsp?lang=en
Warning for Trojan/Spyware from Fraudulent SMS and E-Mail.
K-Cyber Banking
www.kasikornbank.com/LandingPage/Pages/KCyberBankingTH.aspx
Page Summary. PageContent. PageContentBottom.
K-Cyber Banking - KASIKORNBANK
ระวังเว็บไซต์ปลอมของกสิกรไทย
ลงโฆษณาของ Google Adword ซะด้วย


Safari File Edit View History Bookmarks Window Help
Thu 9:36 PM
K-Cyber
login.kasikorngroup-syt.ru/K-Online/login.jsp
Apple iCloud Facebook Twitter Wikipedia News Popular macupdate
K-Cyber
K-Cyber
kcyber - Google Search
kcyber - Google Search
ธนาคารกสิกรไทย
เข้าสู่ระบบ
บิลค่าพ่อนรถ
จ่ายสะดวก จ่ายจริง
ที่ธนาคารกสิกรไทย
อันนี้เว็บปลอม โปรดระวัง

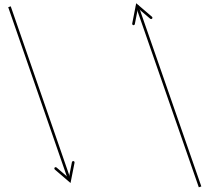

ถ้าเว็บจริง มันจะมีไอ้สีเขียวๆตรงมุมนี้
แล้วก็จะมีรูปกุญแจ อยู่ข้างหน้า URL
K-Cyber
เข้าสู่ระบบ
ข่าวสาร

2) Email Scam


เมล์จริง
portbis@bisfitting.com
portbis@bsfitting.com
เมล์ปลอม

a0t@hotmail.com

เปลี่ยนเลขบัญชี



aot@hotmail.com → **abc@hotmail.com**

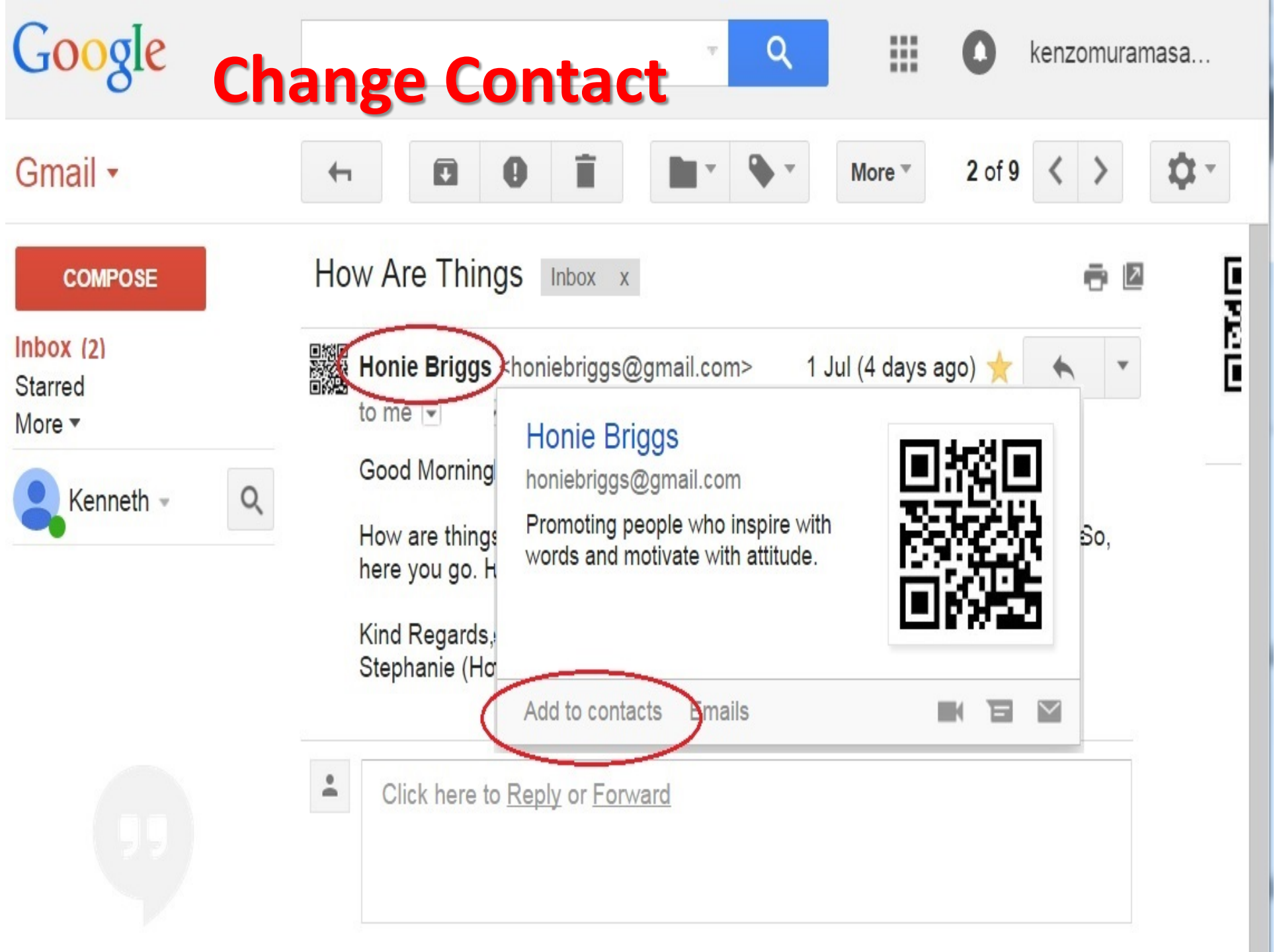
คนขาย **คนซื้อ**

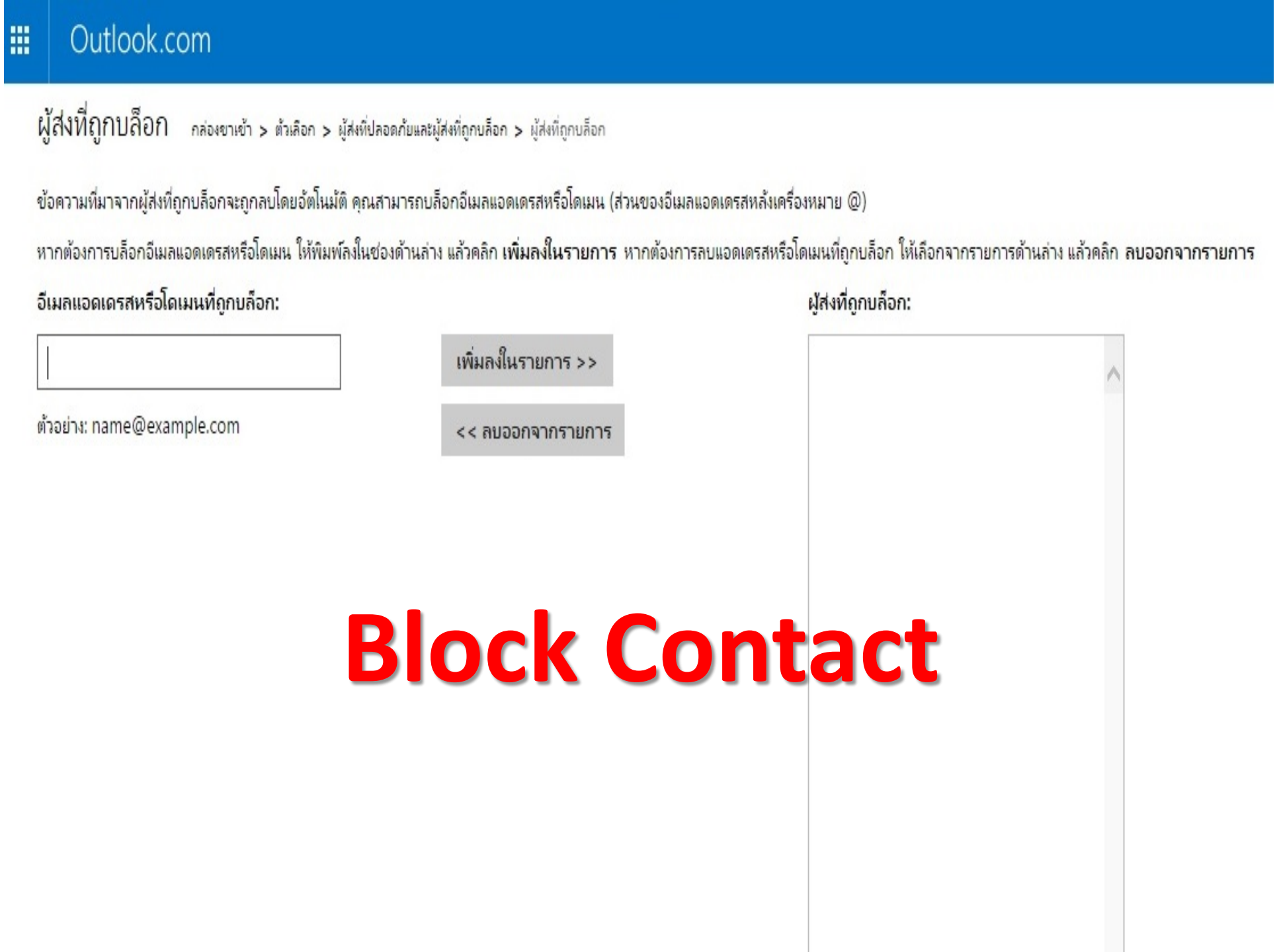
ส่งเลขบัญชี **โอนเงิน**

Change Contact ฝั่งส่ง

Block Contact ฝั่งรับ

Change Contact





Block Contact


Email Scam
JailBreak
in London

Email Scam Prevent

Gmail Security

2-step verification

Take action now!

2)Malware


WORMS
ROOTKITS
SPYWARE
TROJANS
CRIMEWARE
MALWARE
VIRUSES
ADWARE

Gustuff Malware Targets Banking and Crypto apps

bestoffer

kilobyte

Group: Members
Posts: 34
Join Date: 08-04-2017
Пользователь №: 81 752
Activities: вирусология

Reputation: no
(0%)

5.04.2018, 11:52

Android Bot Gustuff The

bot works with 4.xx on 8.xx version

I. Functionality:

1.Sms

All incoming sms aredefaulted to the **admin panel.**

Deletion on versions above 4.4.x + works through the change of the standard application, via query

2.Squakes / ussd

3.Html injections, with a restart in 1 click

Work on all versions of androyd!

4.Socks5 5.

Download photo from phone.

a) Total-unloading of all the photos in a reduced size

b) Separate-unloading the desired photo as the original

6.SMS spam

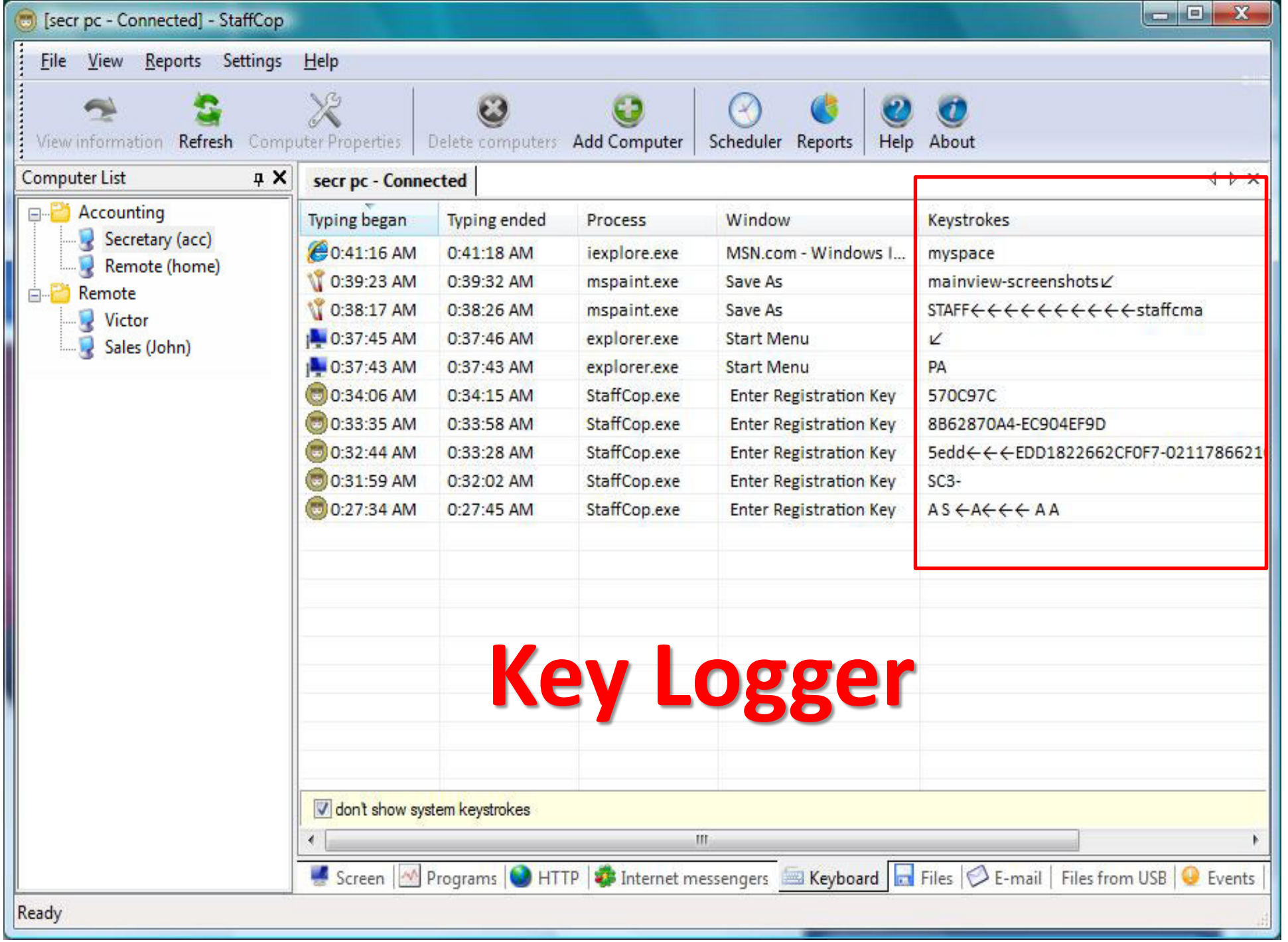
a) Spam on the contact book

b) Spam on the database of numbers collected from the contact books of the bots

7.Push notifications with the icons of the banks

8 .Diagi with the icons of banks

9. Transferring links from the browser of the Holder


[secr pc - Connected] - StaffCop
File View Reports Settings Help
View information Refresh Computer Properties Delete computers Add Computer Scheduler Reports Help About
Computer List
Accounting
Secretary (acc)
Remote (home)
Remote
Victor
Sales (John)
secr pc - Connected
Typing began | Typing ended | Process | Window | Keystrokes
0:41:16 AM | 0:41:18 AM | iexplore.exe | MSN.com - Windows I... | myspace
0:39:23 AM | 0:39:32 AM | mspaint.exe | Save As | mainview-screenshots↙
0:38:17 AM | 0:38:26 AM | mspaint.exe | Save As | STAFF←←←←←←←←←staffcma
0:37:45 AM | 0:37:46 AM | explorer.exe | Start Menu | ↙
0:37:43 AM | 0:37:43 AM | explorer.exe | Start Menu | PA
0:34:06 AM | 0:34:15 AM | StaffCop.exe | Enter Registration Key | 570C97C
0:33:35 AM | 0:33:58 AM | StaffCop.exe | Enter Registration Key | 8B62870A4-EC904EF9D
0:32:44 AM | 0:33:28 AM | StaffCop.exe | Enter Registration Key | 5edd←←←EDD1822662CF0F7-0211786621
0:31:59 AM | 0:32:02 AM | StaffCop.exe | Enter Registration Key | SC3-
0:27:34 AM | 0:27:45 AM | StaffCop.exe | Enter Registration Key | A S ←A←←← A A
Key Logger
don't show system keystrokes
Screen Programs HTTP Internet messengers Keyboard Files E-mail Files from USB Events
Ready