ภัยบนอินเทอร์เน็ต

อ. ธีรารัตน์ รัตนวิสุทธิ์อมร*

Abstract

Personal data is the important key to identify yourself. The advantage of this data is using for doing business or contract. From the rapid changing of technology, internet usage is applied to use for communicating, trading, or even gaming that it makes a risk to client who use an online service on internet which hacker can get their personal data by many ways to breaking through. In this article is going to talk about only phishing, pharming, and gold farmer to hack the personal data.

บทคัดย่อ

ข้อมูลส่วนบุคคลมีความสำคัญเพราะใช้ในการบ่งบอกตัวตนของเจ้าของข้อมูลเพื่อใช้ประโยชน์ในการทำธุรกรรมและนิติกรรมต่าง ๆ ตามกฎหมาย ปัจจุบันเทคโนโลยีมีการเปลี่ยนแปลงไปอย่างรวดเร็ว เกิดระบบอินเทอร์เน็ตเพื่อใช้ในการติดต่อสื่อสาร การค้าขาย หรือแม้กระทั่งการเล่นเกม รูปแบบการให้บริการต่าง ๆ บนอินเทอร์เน็ตมีการพัฒนาขึ้นมาเพื่อรองรับความต้องการของผู้บริโภคมากยิ่งขึ้น จึงเป็นสาเหตุที่ทำให้ข้อมูลส่วนบุคคลของผู้ใช้บริการมีความเสี่ยงที่จะเข้าไปอยู่ในมือของเหล่ามิจฉาชีพได้ง่ายมากยิ่งขึ้นด้วยวิธีการที่หลากหลาย ซึ่งในบทความนี้จะกล่าวถึงเพียงวิธีการขโมยข้อมูลส่วนบุคคลแบบ Phishing Pharming และ Gold farmer เท่านั้น

คำสำคัญ

ความปลอดภัยในระบบคอมพิวเตอร์ แฮกเกอร์ อาชญากรรมทางคอมพิวเตอร์

บทนำ

โลกอินเทอร์เน็ตเป็นโลกของเครือข่ายขนาดใหญ่ที่สามารถติดต่อเชื่อมโยงกันไปได้ทั่วโลก มีการใช้งานได้อย่างไม่จำกัดขอบเขตสามารถติดต่อสื่อสารกันได้ทั่วโลก ด้วยความก้าวหน้าของเทคโนโลยีอินเทอร์เน็ตที่ได้ถูกพัฒนาขึ้นมารองรับความต้องการของผู้ใช้ให้ได้รับความสะดวกสบายมากยิ่งขึ้นนี่เอง ทำให้ผู้ประกอบการจำเป็นต้องหายุทธวิธีในการพัฒนาองค์กรของตนเองให้มีความทันสมัยและสอดคล้องกับความต้องการของผู้ใช้บริการมากยิ่งขึ้น ไม่ว่าจะเป็นการค้นหาข้อมูล การค้าขาย การบันเทิง ฯลฯ ซึ่งสิ่งต่าง ๆ เหล่านี้สามารถใช้บริการผ่านระบบอินเทอร์เน็ตได้แล้วในปัจจุบัน เช่น การจองตั๋วเครื่องบิน การซื้อของผ่านระบบ e-commerce การใช้บริการระบบอีเมล์ (e-mail) การศึกษาทางไกล การแลกเปลี่ยนข่าวสาร การแสดงความคิดเห็น และอื่น ๆ อีกมากมาย จากความสะดวกสบายที่เป็นผลต่อเนื่องมาจากการพัฒนาเทคโนโลยีนี่เองที่เป็นสาเหตุให้เกิดช่องโหว่แก่เหล่ามิจฉาชีพได้นำไปใช้เป็นเครื่องมือในการหาผลประโยชน์ต่าง ๆ และที่พบมากที่สุด คือ การใช้อินเทอร์เน็ตเป็นเครื่องมือในการโจรกรรมข้อมูลส่วนบุคคลจากเว็บไซต์หรือเซิร์ฟเวอร์ต่าง ๆ ที่ให้บริการแก่สมาชิกในการติดต่อสื่อสารและการซื้อขาย เพื่อนำข้อมูลส่วนบุคคลเหล่านั้นไปใช้ในการหาผลประโยชน์ให้แก่ตนเอง ซึ่งเหล่ามิจฉาชีพที่ทำการโจรกรรมข้อมูลต่าง ๆ บนโลกแห่งอินเทอร์เน็ตนั้น เรามักจะเรียกพวกเขาเหล่านี้ว่า "แฮกเกอร์" (Hacker) แต่แท้ที่จริงแล้วนอกจากคำว่าแฮกเกอร์นั้น ยังมีคำว่า "แคร็กเกอร์" (Cracker) ที่กระทำการเช่นเดียวกันกับเหล่าแฮกเกอร์อีกด้วย

---

* อาจารย์ประจำภาควิชาเทคโนโลยีสารสนเทศ คณะวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยฟาร์อีสเทอร์น

ข้อมูลส่วนบุคคล

ข้อมูลส่วนบุคคล (Personal Data) หมายถึง ข้อมูลหรือสิ่งใดๆ ก็ตามที่เป็นเครื่องบ่งชี้ให้เห็นและเข้าใจถึงเรื่องราวหรือลักษณะเฉพาะตัวของบุคคลหนึ่งบุคคลใด เช่น ประวัติการศึกษา ฐานะการเงิน ประวัติสุขภาพ ประวัติการทำงาน ประวัติอาชญากรรม ฯลฯ ซึ่งมีชื่อหรือสิ่งบอกลักษณะที่ทำให้รู้ตัวบุคคลผู้นั้นได้ (นคร เสรีรักษ์, ม.ป.ป.) นอกจากนี้ยังรวมไปถึงข้อมูลในส่วนของ Username และ Password ที่ใช้ login เพื่อใช้งานในระบบต่าง ๆ อีกด้วย ความสำคัญของข้อมูลส่วนบุคคลเหล่านี้ก็คือการระบุถึงตัวตนของผู้ที่เป็นเจ้าของข้อมูลนั้น ๆ เพื่อใช้ในการทำธุรกรรมหรือนิติกรรมต่าง ๆ ได้ตามกฎหมาย เช่น หากคุณซื้อสินค้าผ่านทางระบบอินเทอร์เน็ต ข้อมูลส่วนบุคคลของคุณก็จะถูกนำไปใช้ในการกรอกคำสั่งซื้อสินค้าเพื่อระบุตัวตนของคุณ รวมไปถึงการเรียกเก็บเงิน ซึ่งก็หมายความว่า หากข้อมูลส่วนบุคคลเหล่านี้ตกไปอยู่ในมือของเหล่ามิจฉาชีพ พวกเขาก็สามารถทำธุรกรรมหรือนิติกรรมได้อย่างถูกต้องตามกฎหมายโดยที่คุณไม่รู้ตัว

Hacker และ Cracker ผู้ก่อการร้ายบนโลกอินเทอร์เน็ต

แฮกเกอร์ (Hacker) นั้นมีความหมาย 2 แบบ โดยส่วนใหญ่เมื่อพูดถึงแฮกเกอร์ก็จะเข้าใจว่าหมายถึงบุคคลที่พยายามจะเจาะเข้าระบบโดยไม่ได้รับอนุญาต หรืออาจเรียกได้อีกชื่อหนึ่งคือ ผู้โจมตี ส่วนความหมายที่สองซึ่งเป็นความหมายดั้งเดิมของคำว่า แฮกเกอร์นั้นหมายถึงบุคคลผู้ใช้ความรู้ความเชี่ยวชาญเกี่ยวกับคอมพิวเตอร์แต่ไม่ได้มีจุดมุ่งหมายเพื่อทำลายหรือมีความหมายในด้านลบ ดังนั้น ในความหมายที่สองนี้จะหมายถึงผู้ที่ใช้ความรู้ในทางบวก เช่น การสำรวจเครือข่ายเพื่อค้นหาเครื่องแปลกปลอม เป็นต้น อย่างไรก็ตาม การเจาะเข้าระบบคอมพิวเตอร์คนอื่นนั้นเป็นสิ่งที่ผิดกฎหมาย แต่แฮกเกอร์จะมองว่าเป็นเรื่องที่ถูกจริยธรรม ถ้าไม่มีการขโมยข้อมูลล้วงความลับหรือทำลายระบบ ซึ่งนี่ก็คือ จรรยาบรรณของแฮกเกอร์ (Hacker code of ethics) นั่นเอง

แรงจูงใจของแฮกเกอร์นั้นก็เพื่อการพัฒนา หรือปรับปรุงระบบเพื่อให้มีความปลอดภัยมากขึ้น ซึ่งเป็นความรับผิดชอบของพวกเขาที่ต้องค้นหาช่องโหว่หรือจุดอ่อนของระบบและแก้ไขหรือปิดช่องโหว่นั้นก่อนเหตุการณ์ที่ไม่พึงประสงค์จะเกิดขึ้น ความจริงก็ คือ โดยส่วนใหญ่ช่องโหว่หรือปัญหาของซอฟต์แวร์หรือระบบนั้นจะถูกค้นพบก่อนโดยแฮกเกอร์ไม่ใช่นักพัฒนาซอฟต์แวร์หรือฮาร์ดแวร์ แฮกเกอร์ที่มีจรรยาบรรณก็จะประกาศว่าพบช่องโหว่หรือติดต่อเจ้าของซอฟต์แวร์เพื่อให้แก้ไขปัญหาดังกล่าว

แฮกเกอร์นั้นจะพยายามทำให้เกิดความเสียหายต่อระบบน้อยที่สุดและเขาเชื่อว่าสิ่งที่เขาพยายามจะทำนั้นก็เพื่อบริการสังคมโดยรวม แต่ถ้ามีผลเสียกับระบบก็จะไม่ถือว่าเป็นเรื่องอาชญากรรม และแทนที่จะโทษตัวเองก็จะกล่าวหาเจ้าของระบบว่าไม่มีความระมัดระวังหรือป้องกันที่ดี

แคร็กเกอร์ (Cracker) คือ บุคคลที่พยายามจะทำลายระบบและมีแรงจูงใจที่จะทำเช่นนั้น แคร็กเกอร์จะเหมือนกับแฮกเกอร์ตรงที่ต่างก็มีความรู้และความชำนาญสูงเกี่ยวกับระบบคอมพิวเตอร์และเครือข่าย สามารถใช้ประโยชน์จากช่องโหว่หรือจุดอ่อนที่ค้นพบได้ดี แต่จะแตกต่างตรงที่แฮกเกอร์จะพยายามค้นหาช่องโหว่หรือจุดอ่อนของระบบเท่านั้น ในขณะที่แคร็กเกอร์นั้นจะใช้ประโยชน์จากมันเพื่อทำลายระบบ หรือปฏิเสธการให้บริการกับผู้ใช้งานที่ได้รับอนุญาต หรือทำให้เกิดปัญหาต่าง ๆ ขึ้นกับระบบคอมพิวเตอร์หรือเครือข่าย (จตุพร แพงจันทร์, 2550, น.72-73)

Phishing, Pharming และ Gold farmer ภัยร้ายของข้อมูลส่วนบุคคล

จากการสำรวจเพื่อจัดอันดับภัยที่เกิดจากอินเทอร์เน็ตของ SANS Institute ในปี 2551 นั้นพบว่า ภัยที่เกิดจากการถูกขโมยข้อมูลส่วนบุคคล จากการแอบเอาชื่อผู้ใช้และรหัสผ่านในการเข้าใช้งานระบบออนไลน์ผ่านทางอินเทอร์เน็ต (Username/Password and Identity Theft) เป็นภัยอันดับ 1 ใน 10 ที่เกิดขึ้นอย่างรุนแรงในโลกปัจจุบัน (Top Ten Cyber Security Menaces for 2008, n.d.) การโจมตีเพื่อให้ได้ข้อมูลส่วนบุคคลของผู้ที่ตก

เป็นเหยื่อมีอยู่มากมายหลายรูปแบบ ซึ่งวิธีที่เหล่าแฮกเกอร์นิยมใช้กันมากที่สุดในขณะนี้คือการโจมตีแบบฟิชชิ่ง (Phishing Attack) หรือการตกปลา โดยจะเปรียบเสมือนว่าเหล่าแฮกเกอร์คือคนตกปลา ซึ่งเราจะเรียกบุคคลพวกนี้ว่าฟิชเชอร์(Phisher) และคนที่ถูกโจมตีจะเป็นเหยื่อให้กับเหล่าแฮกเกอร์ได้เอาสิ่งที่พวกเขาต้องการไปใช้ได้อย่างสบายใจ หลักการของการโจมตีแบบฟิชชิ่ง คือ การปลอมแปลงอีเมล์แอดเดรส (e-mail Address) โดยอ้างจากสถาบันหรือเว็บไซต์ที่เชื่อถือได้ส่งไปให้เหยื่อ เพื่อทำการหลอกลวงให้เหยื่อเปิดเผยข้อมูลส่วนบุคคลหรือข้อมูลทางด้านการเงิน เช่น หมายเลขบัตรเครดิต หมายเลขบัตรประจำตัวประชาชน ให้แก่เหล่าแฮกเกอร์ ซึ่งในปัจจุบันกระบวนการฟิชชิ่งนิยมทำผ่าน 3 ช่องทางดังนี้

1. ทางอีเมล์ (email based phishing)

เหล่าฟิชเชอร์จะสุ่มส่งอีเมล์ไปให้กับเหยื่อโดยพยายามลวงให้เหยื่อเข้าใจผิดว่าอีเมล์นี้ส่งมาจากองค์กรหรือสถาบันที่เหยื่อติดต่ออยู่ เนื้อความในอีเมล์จะโน้มน้าวให้เหยื่อคลิกลิงค์ไปยังเว็บไซต์ปลอมที่ถูกสร้างเลียนแบบเว็บไซต์สถาบันการเงินหรือองค์กรต่าง ๆ ที่น่าเชื่อถือ เพื่ออัพเดทข้อมูลส่วนตัวของตนเองหรือเพื่อทำธุรกรรมอื่นๆ เช่น paypal.com ก็ใช้เป็น paypa1.com (ใช้เลขหนึ่งแทนตัวแอล) หรือ www.citibank.com ก็ใช้เป็น www.citibenk.com (เปลี่ยนตัว a เป็นตัว e) หรือเพิ่มเติมบางอย่างเข้าไปใน URL เดิม เช่น www.yourbank.com/ จะถูกเปลี่ยนเป็น www.yourbank.com:login&mode=secure/ เป็นต้น ซึ่งเหล่าฟิชเชอร์จะไม่สามารถคัดลอกทุกอย่างของเว็บไซต์จริงๆ มาได้ แต่จะเลียนแบบให้ใกล้เคียงกับเว็บไซต์จริงให้มากที่สุด และทันทีที่เหยื่อกรอกข้อมูลผู้ใช้ และรหัสผ่านของตนลงไป ฟิชเชอร์จะบันทึกข้อมูลเหล่านั้นและนำมาใช้เข้าบัญชีจริงของลูกค้าเพื่อทำธุรกรรมในเว็บไซต์จริง

2. ทางโทรศัพท์ (phishing by phone)

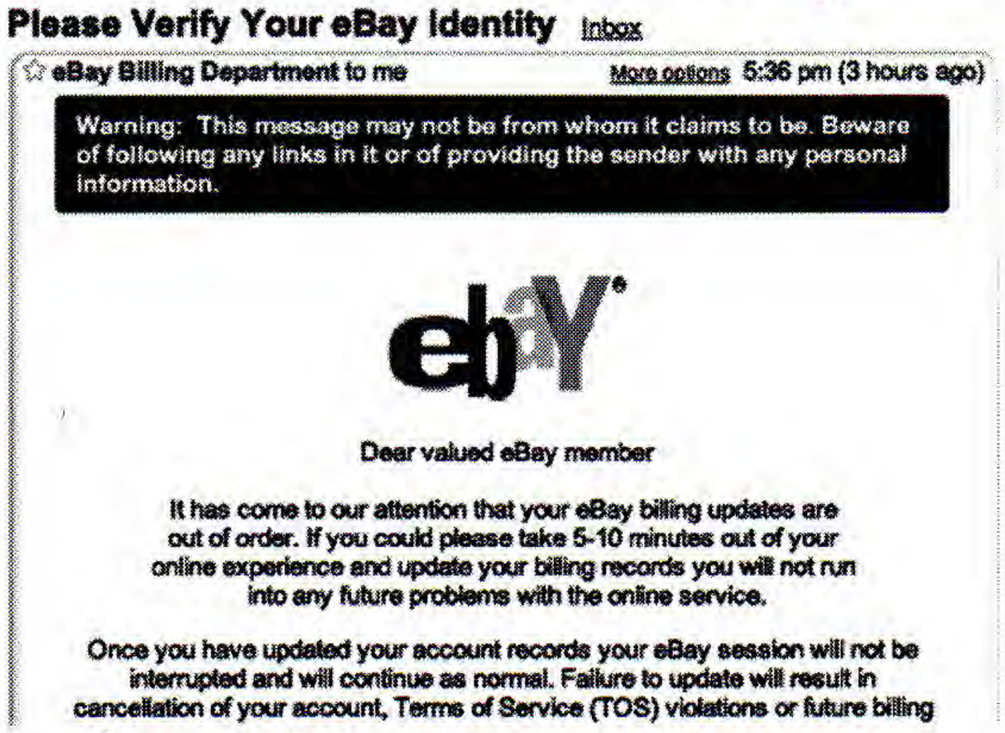
เหยื่ออาจได้รับโทรศัพท์จากบุคคลซึ่งแสดงตนว่ามาจากสถาบันการเงินหรือองค์กรที่เชื่อถือแล้วอ้างว่าองค์กรมีปัญหาทางระบบหรือปัญหาบางอย่างซึ่งต้องการให้ลูกค้าแจ้งข้อมูลส่วนตัวเพื่อยืนยันตัวบุคคลหรืออัพเดทข้อมูลส่วนตัว เช่น เลขบัญชี เลขบัตรประชาชน รหัสผ่าน เป็นต้น หลังจากที่เหยื่อให้ข้อมูลของตนเองแก่เหล่าฟิชเชอร์แล้ว ฟิชเชอร์จะทำการบันทึกและนำข้อมูลเหล่านั้นมาใช้เข้าบัญชีจริงของเหยื่อเพื่อทำธุรกรรมต่อไป

3. ทางไวรัสโทรจัน (Trojan horse)

ในปัจจุบันนอกจากการใช้โทรศัพท์หรือการหลอกลวงจากเว็บไซต์ต่าง ๆ แล้วฟิชเชอร์สามารถจู่โจมเครื่องคอมพิวเตอร์ลูกค้าหรือพนักงานด้วยไวรัสโทรจัน ซึ่งไวรัสชนิดนี้จะเข้าก่อกวนระบบการทำงานของคอมพิวเตอร์และโปรแกรมการอ่านเอกสารทางอินเตอร์เน็ต ไวรัสโทรจันสามารถจับข้อมูลการพิมพ์ของคีย์บอร์ดเมื่อลูกค้าเยี่ยมชมเว็บไซต์ทางการเงิน ดังนั้น ฟิชเชอร์จึงสามารถรวบรวมรหัสชื่อผู้ใช้ และรหัสผ่านของลูกค้าและสามารถทำธุรกรรมจากบัญชีของลูกค้าซึ่งจะใช้เทคนิคการส่งอีเมล์แฝงโปรแกรมโทรจัน อเล็กซ์ ชิปป์ (Alex Shipp) นักพัฒนาเทคโนโลยีแอนตี้ไวรัสอาวุโสของบริษัท MessageLabs ซึ่งกำลังศึกษาเรื่องการรักษาความปลอดภัยในอีเมล์ กล่าวว่าจุดเด่นของฟิชชิ่งแบบใหม่นี้ คือการไม่ต้องรอให้ผู้ใช้คลิกเว็บไซต์แอดเดรสที่แนบมากับอีเมล์ให้ยุ่งยาก แต่โปรแกรมโทรจันนี้จะเปิดหน้าเว็บไซต์หลอกลวงให้โดยอัตโนมัติ

เมื่อเปิดอีเมลครั้งแรก โปรแกรมโทรจันจะแอบเขียนชื่อแอดเดรสปลอมทับรายชื่อเว็บไซต์แอดเดรสแท้ของธนาคารใด ๆ ก็ตามที่เก็บอยู่ในเครื่อง เมื่อผู้ใช้ต้องการเปิดเว็บไซต์ของธนาคารเพื่อใช้งานตามปกติ หน้าเว็บไซต์ของธนาคารที่ปรากฏก็จะกลายเป็นเว็บไซต์ปลอมโดยอัตโนมัติ อเล็กซ์ ชิปป์ กล่าวอีกว่า "มันสามารถทำอันตรายได้มากกว่าการจู่โจมแบบฟิชชิ่งเดิมๆ เพราะเทคนิคใหม่ที่เพิ่งค้นพบว่ามีการใช้โทรจันเข้ามาช่วย" การแพร่กระจายของกลการแฮกข้อมูลเหล่านี้ มักจะเริ่มขึ้นในเมืองหนึ่งๆก่อน จากนั้นจึงค่อย ๆ ขยายและลุกลาม แต่เมื่อเดือนที่แล้ว ตำรวจของประเทศบราซิล ออกแถลงการณ์ว่าได้มีการจับกุมผู้มีส่วนเกี่ยวข้องกับการโจรกรรมโดยอาศัยข้อมูลที่ได้จากการฟิชชิ่งจำนวนประมาณ 53 คน ซึ่งมีวงเงินค่าเสียหายประมาณ 16 ล้านปอนด์ (เตือนภัยเทคนิคฟิชชิ่งใหม่โทรจันเสริมทัพร้ายกว่าเดิม, ม.ป.ป.)

นอกจากนี้ยังมีการใช้อีเมล์หลอกลวงโดยใช้หลักจิตวิทยาในการหลอกล่อให้เหยื่อหลงเชื่อในข้อความที่ส่งผ่านทางเว็บไซต์หรืออีเมล์ ซึ่งเราเรียกการโจมตีแบบนี้ว่า Social Engineering โดยทำให้เหยื่อไว้วางใจและมีน้ำหนักในความน่าเชื่อถือมากยิ่งขึ้น ดังเช่นในกรณีของ ebay ดังปรากฏในภาพที่ 1



Please Verify Your eBay Identity Inbox

☆ eBay Billing Department to me More options 5:36 pm (3 hours ago)

Warning: This message may not be from whom it claims to be. Beware of following any links in it or of providing the sender with any personal information.

ebay

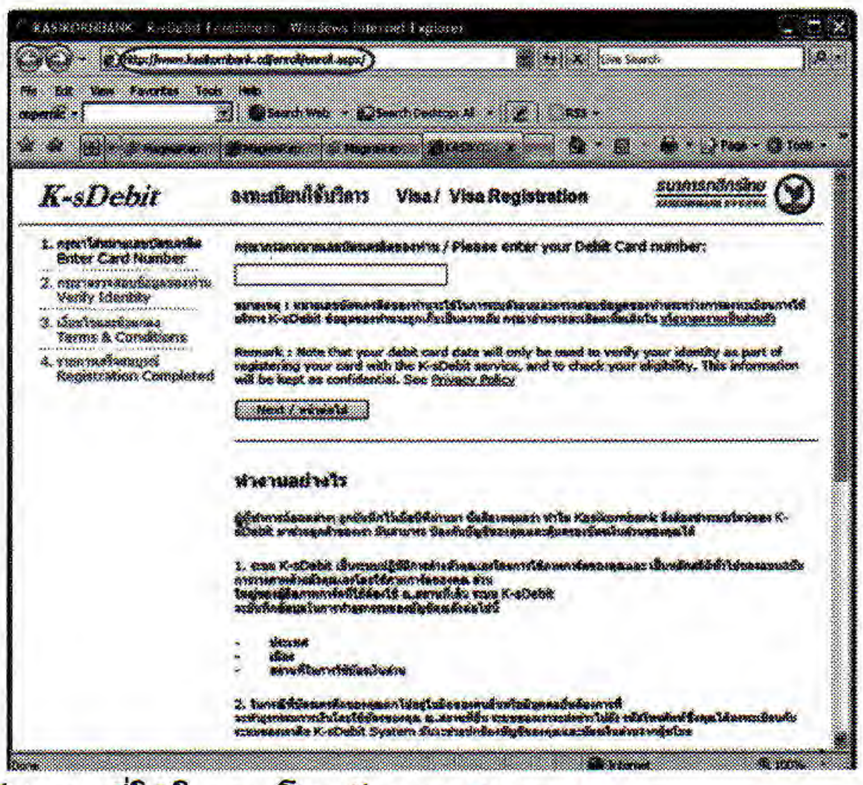
Dear valued eBay member

It has come to our attention that your eBay billing updates are out of order. If you could please take 5-10 minutes out of your online experience and update your billing records you will not run into any future problems with the online service.

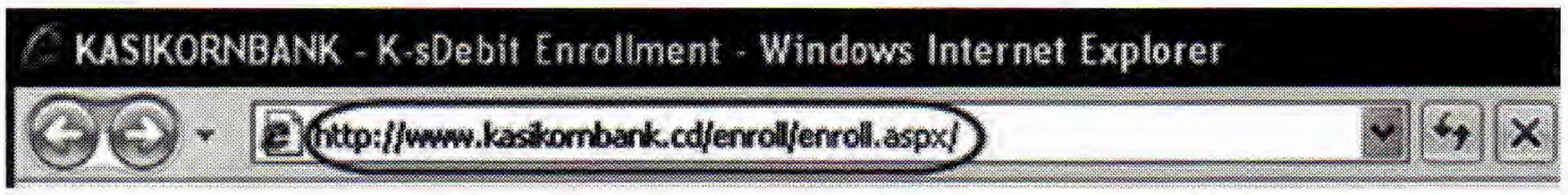
Once you have updated your account records your eBay session will not be interrupted and will continue as normal. Failure to update will result in cancellation of your account, Terms of Service (TOS) violations or future billing

ภาพที่ 1: อีเมล์ที่ใช้ในการ phishing
ที่มา: http://www.thaicert.org/paper/basic/phishing.php

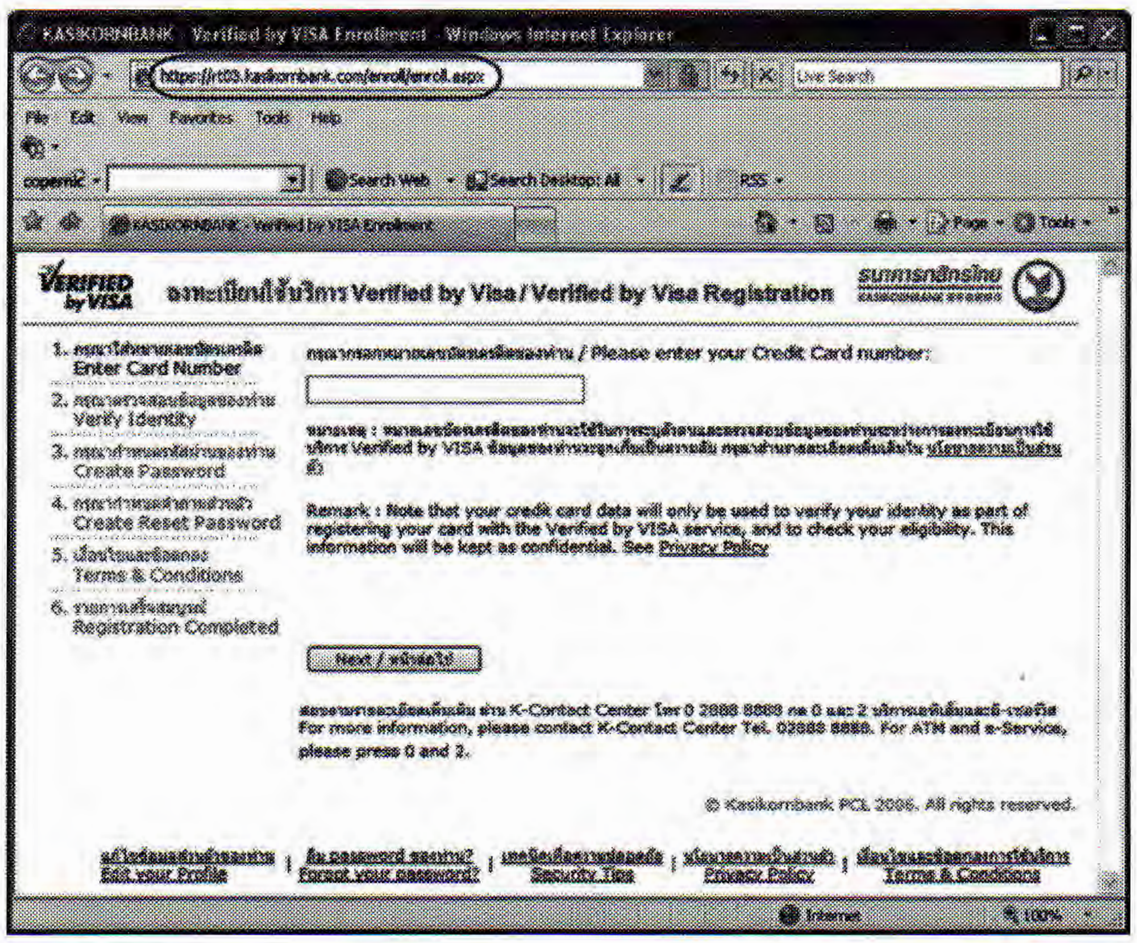
จากภาพที่ 1 เป็นตัวอย่างอีเมล์ ที่ดูคล้ายจะถูกส่งมาจากเว็บไซต์ ebay โดยแจ้งให้คุณไปอัพเดตข้อมูลของตัวเอง เพื่อป้องกันไม่ให้เกิดปัญหาตามมาในอนาคตหากจะใช้บริการออนไลน์นี้ และหลังจากที่คุณได้กรอกข้อมูลของคุณลงไปแล้วก็สามารถใช้บริการได้ตามปกติ และในอีเมล์ นี้ ได้เน้นย้ำว่า หากไม่ปรับปรุงข้อมูลของคุณจะส่งผลถึงการยกเลิกบัญชีของคุณไปด้วย ซึ่งอาจจะทำให้ผู้ที่ใช้บริการในเว็บไซต์นี้อยู่เกิดความตื่นตระหนกและรีบไปกรอกข้อมูลส่วนบุคคลของตัวเองให้กับเหล่าแฮกเกอร์ได้เอาไปใช้ได้ตามใจชอบ นอกจากนี้ในปัจจุบันยังมีเว็บไซต์ปลอมระบาดเกิดขึ้นอีก ไม่ว่าจะเป็นเว็บไซต์ของ Hi5 เว็บไซต์ของธนาคารต่าง ๆ และที่หนีไม่พ้นก็คือพวก Mail hosting ดัง ๆ อย่างเช่น hotmail หรือ yahoo ซึ่งวิธีในการปลอมเว็บไซต์หลอกให้ผู้ใช้เข้าใจว่าเป็นเว็บไซต์ที่ให้บริการจริง ๆ เราเรียกว่า การโจมตีแบบฟาร์มมิ่ง (Pharming Attack) ซึ่งจะต่างจากการโจมตีแบบฟิชชิ่ง โดยที่การโจมตีแบบฟาร์มมิ่งจะโจมตีระบบ Domain Name System (DNS) หรือ โจมตีที่ไฟล์ Host ของเครื่องลูก โดยวิธีการ Re-direct หรือการย้ายชื่อของเว็บไซต์ให้ชี้ไปยัง IP ปลอมที่สร้างขึ้นมาที่ไม่ใช่ IP จริง ๆ ของเว็บไซต์ ซึ่งเหยื่อแทบจะแยกไม่ออกเลยว่าอันไหนคือเว็บไซต์จริงและอันไหนคือเว็บไซต์ปลอม เมื่อผู้ใช้ทำการกรอกข้อมูลเช่น Username หรือ Password ลงไปก็จะทำให้เหล่าแฮ็กเกอร์สามารถเข้าไปจัดการกับระบบได้ ดังเช่น กรณีของธนาคารกสิกรไทยในภาพที่ 2 -5



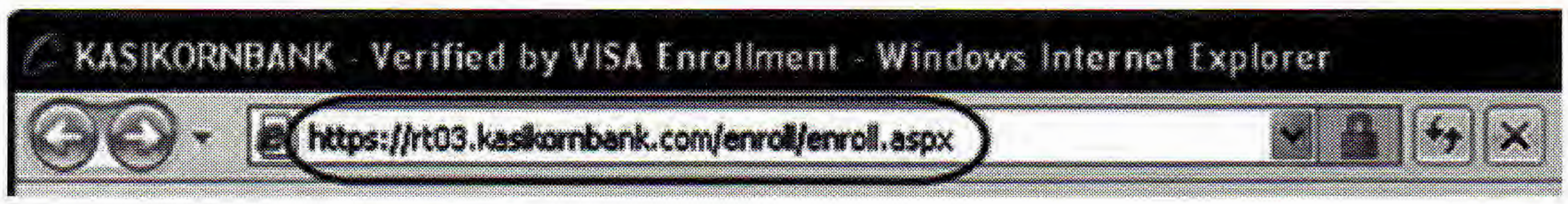
ภาพที่ 2: เว็บไซต์ปลอมที่ใช้ในการโจมตีแบบ Pharming
ที่มา : http://www.magmareport.com/content/585?PHPSESSID=cb9804ca8647cca



ภาพที่ 3 : URL ของ web phishing
ที่มา : http://www.magmareport.com/content/585?PHPSESSID=cb9804ca8647cca



ภาพที่ 4 : เว็บไซต์จริงของธนาคาร
ที่มา : http://www.magmareport.com/content/585?PHPSESSID=cb9804ca8647cca



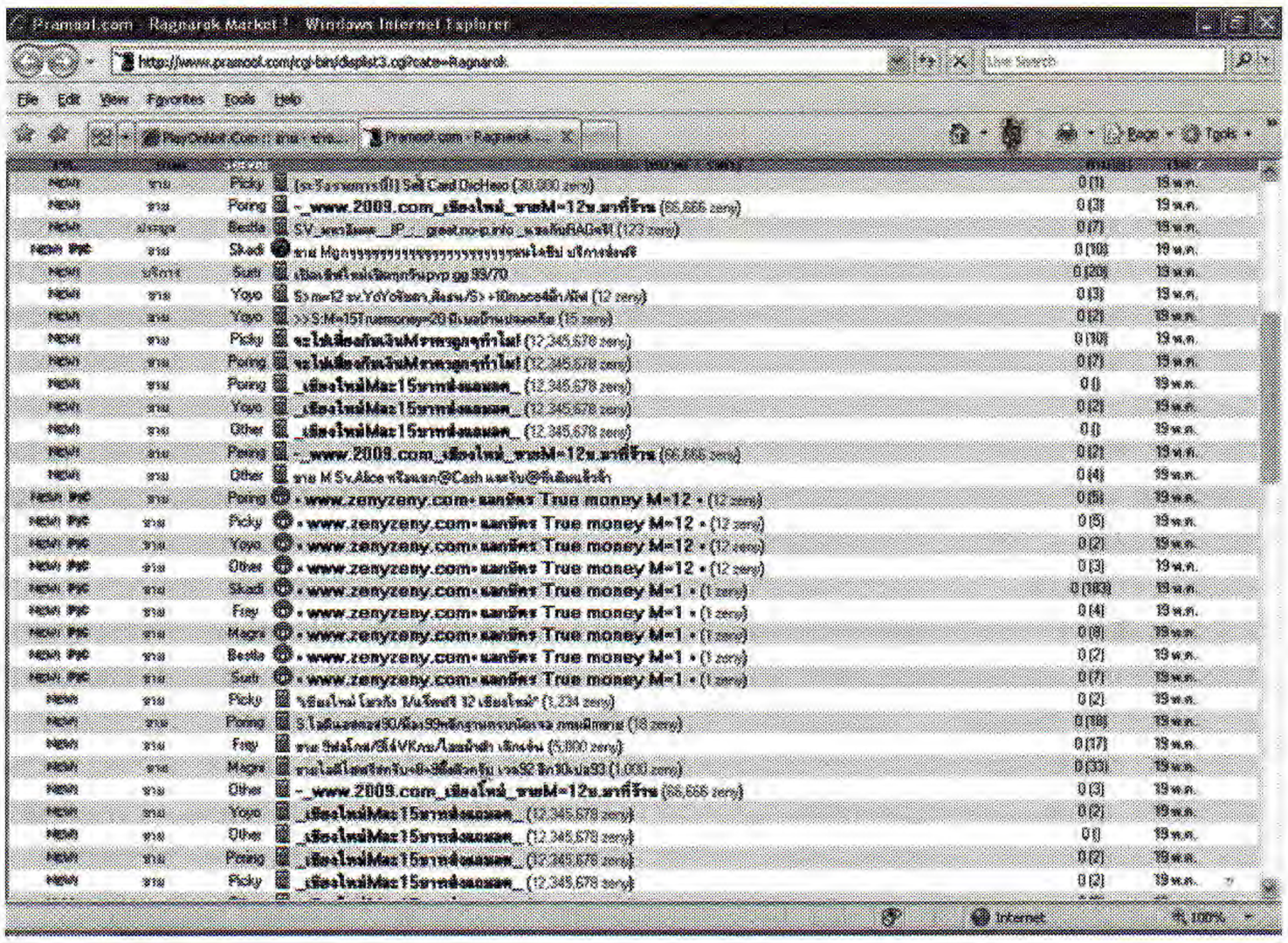
ภาพที่ 5 : URL เว็บไซต์ของจริง
ที่มา : http://www.magmareport.com/content/585?PHPSESSID=cb9804ca8647cca

หากสังเกตหน้าจอเว็บไซต์ในภาพที่ 2 และภาพที่ 3 จะพบข้อแตกต่างกันตรงที่เว็บไซต์ที่แท้จริงของทางธนาคารทางด้านซ้ายมือที่จะมีโลโก้ Verified by Visa อยู่ แต่ในเว็บไซต์ฟาร์มมิ่งจะเป็น K-sDebit

นอกจากการโจมตีแบบฟิชชิ่งและการโจมตีแบบฟาร์มมิ่งแล้ว ปัจจุบันการขโมยข้อมูลส่วนบุคคลเพื่อเอาไปใช้ประโยชน์ ได้ลุกลามไปถึงเกมออนไลน์ ไม่ว่าจะเป็นเกมแนวการต่อสู้ (Battle) เช่น สเปเชียลฟอต เกมแนวกีฬา (Sport) เช่น ปังย่าและอื่น ๆ ในโลกแห่งเกมเหล่านี้เราถือได้ว่าเป็นโลกเสมือน (Virtual World) ที่สามารถมีชีวิตและการซื้อ-ขายของ มีการสะสมเงินจากกิจกรรมต่าง ๆ เหมือนกับการใช้ชีวิตจริง (Real World) ซึ่งในเกมออนไลน์เหล่านี้ได้มีการผสมผสานระหว่างจุดเด่นของการเล่นเกมกับการสนทนาออนไลน์ (Chat) เข้าไว้ด้วยกันทำให้ผู้เล่นสามารถคุยไปพร้อมกับการเล่นเกมไปด้วย ดังในภาพที่ 6

ภาพที่ 6 : การสนทนาออนไลน์ระหว่างการเล่นเกม
ที่มา : http://tirkx.online-station.net/news/view.php?id=5572

จากเทคโนโลยีเหล่านี้ทำให้เหล่าแฮกเกอร์เห็นช่องทางในการหาผลประโยชน์จากการเล่นเกมเหล่านี้ โดยการเข้าไปเอาสิ่งของจากผู้เล่นเกมหรือตัวละครในเกมเอาไปประกาศขายในโลกแห่งความเป็นจริงและเหล่าแฮกเกอร์ที่ทำแบบนี้ จะเรียกตัวเองว่า นักขุดทอง (Gold Farmer) สินค้าที่ถูกนำมาเสนอขายตามช่องทางสนทนาออนไลน์มักจะเป็นพวกอาวุธที่หาได้ยากจากเกมหรือเครื่องแต่งกายที่จะมีเฉพาะในตัวละครที่มีความสามารถระดับสูงๆ เพื่อแลกกับเงินสดในโลกแห่งความเป็นจริง เช่น การซื้อตัวละครระดับสูงๆ เพื่อนำไปเล่นต่อ หรือแม้กระทั่งการใช้เงินในเกมแลกเปลี่ยนกับบัตรเติมเวลาแอร์ไทม์ของเกมนั้นๆ ทำให้ผู้เล่นจำนวนมากที่ใช้การแลกบัตรเติมเวลาที่มีทรัพย์สินในเกมจำนวนมากๆ สามารถเล่นเกมได้เรื่อยๆ โดยไม่ต้องซื้อบัตรเติมเวลา ดังเช่นในภาพที่ 7



ภาพที่ 7 : ภาพตัวอย่างการประกาศขาย item ต่าง ๆ บนเว็บไซต์
ที่มา : http://www.pramool.com/cgi-bin/displist3.cgi?cate=Ragnarok

ปัจจุบันกระแสนิยมเล่นเกมออนไลน์ที่นำเข้าจากประเทศเกาหลีหรือญี่ปุ่น กำลังอยู่ในช่วงร้อนแรง ทำให้ค่ายเกมใหญ่ ๆ แข่งขันกันนำเข้าเกมใหม่ ๆ เพื่อตอบสนองความต้องการของลูกค้า เมื่อมีเกมออนไลน์มากขึ้น ธุรกิจการค้าสินค้าจากเกมออนไลน์ก็จึงมีมากขึ้นตามไปด้วยและสิ่งเหล่านี้เองที่เป็นสิ่งยั่วยุทำให้เหล่าแฮกเกอร์หันมาหาผลประโยชน์จากช่องทางนี้กันเพิ่มขึ้น

วิธีการโจมตีแบบอื่น ๆ

ข้อมูลเหล่านี้เป็นเพียงแค่ส่วนหนึ่งของการโจมตีเพื่อหาผลประโยชน์จากเหยื่อเท่านั้น ซึ่งในความเป็นจริงยังมีการโจมตีแบบอื่น ๆ อีก เช่น

- การโจมตีโดยใช้ระบบโทรศัพท์ หรือที่เราเรียกว่า Vishing (Voice SPAM Attack) ที่เราได้ยินข่าวกันหนาหูในช่วงก่อนหน้านี้ การใช้เทคโนโลยี VoIP เข้ามาใช้เป็นช่องทางในการหาผลประโยชน์โดยการโทรศัพท์มาหลอกอ้าง เช่น บอกว่าโทรมาจากสถาบันที่เกี่ยวข้องกับการเงินต่างๆ ให้เหยื่อหลงเชื่อแล้วหลอกถามข้อมูลส่วนบุคคลของเหยื่อไป หรือไม่ก็ให้เหยื่อโอนเงินเข้าบัญชีของผู้แอบอ้าง
- Spyware/ Keylogger Attack เป็นการโจมตีโดยการดักข้อมูลจากคีย์บอร์ด หรือ Keylogger ซึ่งจัดได้ว่าเป็นโปรแกรมประเภท Spyware ประเภทหนึ่ง ทำได้โดยการติดตั้งโปรแกรมเหล่านี้ลงในเครื่องที่ถูกเปิดหน้าจอทิ้งไว้ และหลังจากนั้นไม่ว่าคนที่เข้ามาใช้งานในเครื่องนั้นจะพิมพ์อะไรลงไป ข้อมูลก็จะถูกส่งกลับไปยังเหล่าแฮกเกอร์อย่างง่ายดาย
- HOAX/SCAM (จดหมายหลอกลวง) ถือเป็นพวก SPAM อย่างหนึ่งที่ใช้การโจมตีผ่าน e-mail โดยการหลอกว่าผู้ที่ได้รับ e-mail ฉบับนี้ถูกรางวัลอย่างใดอย่างหนึ่ง แต่ต้องเสียค่าธรรมเนียม หรือเสียภาษี จะต้องโอนเงินเหล่านั้นเสียก่อนจึงจะได้รับเงินรางวัลทั้งหมด ทำให้เหยื่อเกิดความโลภแล้วส่งเงินไปให้แก่พวกมิจฉาชีพ

บทสรุป

อินเทอร์เน็ตทำให้เกิดความรวดเร็วและเอื้ออำนวยความสะดวกสบายให้แก่ผู้ใช้บริการอย่างมากมาย แต่หากผู้ใช้บริการและผู้ให้บริการขาดความระมัดระวังในการป้องกันและรักษาความลับ ก็จะกลายเป็นเหยื่อให้แก่เหล่ามิจฉาชีพได้ด้วยความรู้เท่าไม่ถึงการณ์ ดังนั้นทั้งผู้ให้บริการและผู้ใช้บริการควรจะทำการศึกษาถึงวิธีการป้องกันในด้านความปลอดภัยในการใช้อินเทอร์เน็ตให้เพียงพอ เพื่อป้องกันการตกเป็นเหยื่อของเหล่ามิจฉาชีพ การติดตามข้อมูลข่าวสารใหม่ ๆ การติดตั้งโปรแกรมดักจับพวก Spyware หรือ พิชชิ่งเพื่อกรองเว็บไซต์ที่อาจทำให้เกิดความเสี่ยงจากการโจมตีแบบต่าง ๆ และการให้ความใส่ใจในด้านการรักษาความปลอดภัยของข้อมูลส่วนบุคคลโดยการพิจารณาความปลอดภัยของเว็บไซต์ก่อนกรอกข้อมูลส่วนบุคคลต่าง ๆ ของตนเองลงไป

เอกสารอ้างอิง

โกเมน พิบูลย์โรจน์. (2547). **เทคนิคการโจมตีแบบ "Phishing".** ค้นเมื่อวันที่ 5 พฤษภาคม 2551, จาก http://www.thaicert.org/paper/basic/phishing.php

'กฎ5ข้อ' ป้องกันถูกโกงออนไลน์. (ม.ป.ป.). สืบค้นเมื่อ 12 สิงหาคม 2551, จาก http://www.adslcool.com/internet/viewrecord.php?id=80

จตุชัย แพงจันทร์ (2550). **Master in Security.** นนทบุรี : ไอดีซีฯ.

เตือนภัยเทคนิคฟิชชิ่งใหม่ โทรจันเสริมทัพร้ายกว่าเดิม . (ม.ป.ป.). สืบค้นเมื่อ 12 สิงหาคม 2551, จาก http://expert2you.com/view__news.php?art__id=2156

ธุรกิจเงินเกมออนไลน์บูม!. (ม.ป.ป.). สืบค้นเมื่อ 10 พฤษภาคม 2551, จาก http://www.bloggang.com/viewblog.php?id=sleepsheep&date=16-06-2007&group=6&gblog=2

นคร เสรีรักษ์. (ม.ป.ป.) .**ข้อมูลส่วนบุคคลสำคัญไฉน**. สืบค้นเมื่อวันที่ 5 พฤษภาคม 2551, จาก http://www.fpps.or.th/news.php?detail=n1156791089.news

ระวัง Phishing เว็บไซต์ธนาคารกสิกรไทยปลอม โปรดตรวจสอบให้ดีก่อนใช้บริการ. (ม.ป.ป.). สืบค้นเมื่อวันที่ 5 พฤษภาคม 2551, จาก http://www.magmareport.com/content/585?PHPSESSID=cb9804ca8647cca

10 อันดับภัยอินเทอร์เน็ตล่าสุดประจำปี พ.ศ. 2551. (ม.ป.ป.). สืบค้นเมื่อวันที่ 5 พฤษภาคม 2551, จาก http://www.idin9.com/main/content/view/180/60/lang,th

ING Life Limited. (n.d.). **Anti-Phishing Awareness.** Retrieved August 12, 2008, from http://www.inglife.co.th/pages/thi/news/news__display.asp?newsID=868&ReloadFlag=yes

Top Ten Cyber Security Menaces for 2008. (n.d.) Retrieved May 5, 2008, from http://www.sans.org/2008menaces/?utm__sousrce=web-sans&utm__medium=text-ad&utm__content=textlink__2008menaces__homepage&utm__campaign=Top__10____Cyber__Security__Menaces__-__2008&ref=22218