

ภัยกลลวงทางไซเบอร์จะระบอบาดช่วงฤดูกาลกีฬาโอลิม

มปีค

โดยคาร์ลิน เดอ ปงเตर्फ์ นักวิเคราะห์แอนตี้ไวรัส ทีมฟอร์ตการ์ด แห่งฟอร์ติเน็ต



ในช่วงครึ่งปีหลังของปีค.ศ. 2012 นี้ มีกิจกรรมระดับโลกมากมาย อาทิ การแข่งขันกีฬาโอลิมปิกเกมส์ และการแข่งขันฟุตบอล UEFA European Football Championship ตลอดจนการแข่งขันเลือกตั้งประธานาธิบดีแห่งสหรัฐอเมริกา จึงทำให้มีการใช้งานอินเทอร์เน็ตพุ่งขึ้นสูงมากแน่นอน และมักจะมีภัยคุกคามแพร่กระจายมากขึ้นตามตัว โดยภัยประเภทแปลกปลอมกลลวง (Scams) อยู่ในอันดับต้นๆ



ในปัจจุบันมี Scams แพร่กระจายนับพันๆ ชนิด มีเป้าหมายลวงข้อมูลด้านบัตรเครดิต โดยภัยประเภทแปลกปลอมกลลวงที่มาเป็นอันดับแรกคือ พวกกลลลือเตอเรียปลอม (Fake Lotteries) ที่มักจะมาในรูปแบบอีเมลที่แจ้งว่าท่าน (อาจจะ) ได้สิทธิ์รับรางวัลใหญ่ราคาสูง แต่ท่านต้องจ่ายค่าภาษี และแน่นอนไม่ว่าท่านจะจ่ายหรือไม่จ่ายภาษี ท่านจะไม่ได้รางวัลนั้นอย่างแน่นอน

ภัยแพร่กระจายหนักที่รองลงมาคือพวกหลอกให้ซื้อ (Purchase fraud) ที่เชิญชวนว่าท่านมีสิทธิ์ซื้อตัวของท่านใหญ่ๆ ได้ในราคาพิเศษ เมื่อท่านเข้าเว็บพวก eBay และ Craigslist ท่านอาจพบหน้าโฆษณาที่อยู่ข้าง ซึ่งดูราคาจูงใจมากเพราะช่วงนี้มีกิจกรรมกีฬามาก ท่านอาจตกเป็นเหยื่อได้ ขอให้ระวัง

ภัยประเภทที่ 3 ได้แก่ โปรแกรมแอนตี้ไวรัสปลอม (Rogue AV) ในช่วงที่มีกิจกรรมมากมายนี้ จะมีการใช้อินเทอร์เน็ตเพื่อติดตามข่าวสาร อาทิ คะแนน ผลการเลือกตั้ง และข่าวด่วนอื่นๆ อาจเกิดเว็บไซต์ปลอม (ที่อาจเกิดจากเว็บที่ถูกต้องโดนแฮค) โดนอาจมีหน้าต่างป๊อปอัพขึ้นมาบนหน้าจอแจ้งว่า เครื่องคอมพิวเตอร์ของท่านติดไวรัส (ทั้งๆ ที่มีโปรแกรมแอนตี้ไวรัสอยู่แล้ว) ด้วยความรู้เท่าไม่ถึงการณ์ คนทั่วไปมักจะคลิกที่ป๊อปอัพนั้น ดูเหมือนเป็นการลงโปรแกรมแอนตี้ไวรัส (ปลอม) แต่จริงๆ แล้วจะเป็นการแพร่โทรจันลงไปเครื่องแล้วจะเก็บข้อมูลต่างๆ เช่น รหัสผ่านและเลขบัญชีธนาคาร

ดังที่กล่าวข้างต้น ในช่วงกีฬาโอลิมปิกเกมส์ การแข่งขันฟุตบอล UEFA European Football Championship และการแข่งขันเลือกตั้งประธานาธิบดีแห่งสหรัฐอเมริกา อาจมีภัยเพิ่มขึ้นเท่าตัว อย่างไรก็ตาม ภัยประเภทอื่นที่พบเห็นในปัจจุบัน ได้แก่

ภาพวิดีโอปลอม (Video Hoaxes and Social Networks)

ในกรณีนี้ ท่านอาจจะได้รับข้อความจากเพื่อนในเฟสบุ๊คชวนให้ไปดูวิดีโอหายากหรือลับเฉพาะของดารา โดยท่านต้องคลิกและวางลิงค์ที่ให้มาที่เบราว์เซอร์ จึงเป็นการติดตั้งมัลแวร์ลงในเครื่องโดยไม่รู้ตัว ทางป้องกันคือท่านไม่ควรคลิกเปิดดูหรือตอบอีเมลนั้น และท่านอาจจะไปดูข้อมูลจริงๆ ที่เว็บไซต์ที่เป็นทางการของเรื่องนั้นแทน

การปลอมแปลงอีเมลหรือเว็บ และการขโมยข้อมูล (Phishing & Identity Theft)

การปลอมแปลงอีเมลและเว็บไซต์รูปแบบหนึ่งโดยส่วนใหญ่จะมีวัตถุประสงค์ที่จะต้อง การขโมยข้อมูลข่าวสารต่างๆ ท่านอาจได้รับอีเมลปลอมจากธนาคาร แจ้งว่าบัญชีของท่านโดยบล็อก ท่านไม่ควรตอบอีเมลนั้น และจำไว้ว่าธนาคารไม่เคยถามเลขบัญชีของท่านทางอีเมล

ภัยขอค่าธรรมเนียมก่อน (Advance Fee “Nigerian” Fraud)

ภัยนี้เกิดมานานแล้ว กลลวงนั้นง่ายมาก โดยจะแจ้งว่าท่านได้รับรางวัลเงินสดก้อนโตแต่ท่านต้องจ่ายค่าธรรมเนียมก่อน และเมื่อท่านให้ข้อมูลไป แน่แน่นอนว่าท่านจะตกเป็นเหยื่อและได้รับความเสียหายมากมายภายหลัง

ภัยรักลวงโลก (Sweetheart Swindles)

อาชญากรมักจะทำปลอมแปลงเป็นนักธุรกิจที่มีฐานะ ทำงานอยู่ต่างประเทศ หรือปลอมเป็นสตรีที่มีเสน่ห์ จะทำตัวใกล้ชิดสนิทสนมกับเหยื่อให้ตายใจ และเมื่อถึงเวลาหนึ่งก็จะออกมายขอเงินทองและทรัพย์สิน

ทีมวิจัยฟอร์ติการ์ดแห่งฟอร์ติเน็ตขอเสนอเกร็ดเล็กๆ น้อยๆ ป้องกันมิให้ท่านตกเป็นเหยื่อได้

- เมื่อมีการขอข้อมูลด้านการเงินของท่าน ขอให้ท่านไตร่ตรองให้รอบคอบหลายๆ ครั้งก่อนจะทำตาม
- ระวังลิงค์ที่เชื่อมโยงไปสู่แอปพลิเคชันหรือเว็บไซต์ภายนอก โดยเฉพาะอย่างยิ่งที่ฝังมากับอีเมลหรือข้อความที่สนทนาเรื่องเกี่ยวกับดาราและกิจกรรมใหญ่ต่างๆ
- ยูอาร์แอลที่ถูกย่อให้สั้นลงอาจเป็นการใช้งานที่มีประสิทธิภาพ และเมื่อท่านคลิกไปแล้ว ท่านอาจโดนเชื่อมไปยังเว็บไซต์ปลอมได้
- เมื่อท่านต้องกู้รหัสผ่านของบริการด้านเว็บใดๆ ที่มีขั้นตอนต้องกรอกข้อมูล อาทิ โรงเรียนเดิม ชื่อของมารดา และอื่นๆ ขอให้ระวังในการเปิดเผยข้อมูลเหล่านั้นเป็นอย่างยิ่ง ซึ่งอาจโดนแอบรวบรวมและสรุปหาบัญชีของท่าน หรือนำไปแอบอ้างในธุรกรรมปลอม เช่น การกู้เงินโดยใช้ข้อมูลของท่าน
- อย่าส่งเงินให้ใคร อย่างนัดพบเป็นการส่วนตัว
- ตรวจสอบรายงานบัญชีการเงินของท่านทุกสัปดาห์ ทุกเดือน เมื่อพบปัญหาเร็วจะสามารถแก้ไขปัญหาได้เร็ว
- จงเชื่อว่า “ในโลกนี้ ไม่มีใครดี ใครหล่อ (สวย) เกินจริงเสียขนาดนั้น”
- และ คิดว่า “ท่านไม่เคยซื้อล็อตเตอรี่ แล้วจะถูกรางวัลได้อย่างไร”