

ประสาทวิทยาของ พีชชิง

GIULIANO PAIÃO

A dramatic, low-key photograph featuring a shirtless man on the left and a humanoid robot on the right. They are both looking at a single, vibrant red apple held in the robot's hand. The lighting is moody, highlighting the textures of the man's skin and the metallic surfaces of the robot. The background is dark, making the subjects and the apple stand out.

เมื่อ **ความศรัทธา** **ความโลภ**
และ **ความสุขทางใจ**
เบียดเบียนเงินมากกว่า 100 พันล้านดอลลาร์

กรณีจริงของการโจมตี
G20, NATO, ทวิตเตอร์ (X) และอื่น ๆ

เรื่องย่อ

ประสาทวิทยาศาสตร์ของฟิชซิง

อารมณ์ของมนุษย์ถูกนำมาใช้ในการโจมตีทางไซเบอร์อย่างแม่นยำได้อย่างไร

ในหนังสือเล่มนี้ จูเลียโน ปายาโอ รื้อถอนความรู้สึกปลอดภัยจอมปลอมที่สร้างขึ้นจากไฟรัวอลล์ รหัสผ่านที่รัดกุม และการยืนยันตัวตนแบบสองปัจจัย พร้อมเผยให้เห็นพื้นที่ที่เปราะบางและถูกโจมตีมากที่สุดของความมั่นคงปลอดภัยดิจิทัล นั่นคือจิตใจมนุษย์

หนังสือ "ประสาทวิทยาศาสตร์ของฟิชซิง" เจาะลึกกลไกทางอารมณ์ที่ทำให้การโจมตีทางไซเบอร์ได้ผล แม้กับผู้เชี่ยวชาญที่มีประสบการณ์และองค์กรที่มีโครงสร้างพื้นฐานแข็งแกร่ง ศรัทธา ความพึงพอใจ และความโลภไม่ใช่เพียงอารมณ์ แต่เป็นตัวกระตุ้นทางการรับรู้ที่เมื่อถูกกระตุ้นแล้ว จะลดทอนวิจารณญาณและเปิดทางให้เกิดการบุกรุก

ด้วยภาษาที่เข้าใจง่ายแต่แม่นยำทางเทคนิค ผู้เขียนนำเสนองานวิจัยทางวิทยาศาสตร์ กรณีศึกษาจริง เทคนิควิศวกรรมสังคม เครื่องมือโอเพนซอร์ส เช่น GoPhish และกลยุทธ์เชิงปฏิบัติสำหรับปกป้องสิ่งที่โปรแกรมป้องกันไวรัสตรวจจับไม่ได้ นั่นคือพฤติกรรมมนุษย์

นี่ไม่ใช่เพียงหนังสือว่าด้วยความมั่นคงปลอดภัยไซเบอร์ แต่เป็นคู่มือสงครามจิตวิทยาที่แสดงให้เห็นว่า การโจมตีครั้งใหญ่ที่สุดไม่ได้เริ่มต้นจากบรรทัดโค้ด หากเริ่มจากแนวความคิด

หากคุณทำงานเกี่ยวข้องกับผู้คน ข้อมูล หรือการตัดสินใจ
หนังสือเล่มนี้เขียนขึ้นเพื่อคุณ

สงวนลิขสิทธิ์ทุกประการ

หนังสือเล่มนี้ได้รับความคุ้มครองตามกฎหมายลิขสิทธิ์ ห้ามทำซ้ำ จัดเก็บ
ในระบบสืบค้น หรือส่งต่อส่วนหนึ่งส่วนใดของสิ่งพิมพ์นี้ ไม่ว่าในรูปแบบ
หรือด้วยวิธีการใด ทั้งทางอิเล็กทรอนิกส์ เครื่องกล การถ่ายสำเนา การ
บันทึก หรือวิธีอื่นใด โดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้เขียน
ล่วงหน้า ยกเว้นการอ้างข้อความสั้น ๆ เพื่อวัตถุประสงค์ทางวิชาการ
วารสารศาสตร์ หรือการวิจารณ์

ชื่อ แปรนต์ บุคคล และเหตุการณ์ทั้งหมดที่ใช้ในกรณีศึกษาจริงได้รับการ
ตรวจสอบตามหลักฐาน และเมื่อจำเป็นได้มีการดัดแปลงหรือทำให้ไม่
สามารถระบุตัวตนได้ เพื่อคุ้มครองบุคคลที่เกี่ยวข้อง

ผู้เขียน: จุลิอาโน ปายาโอ
© 2025 — สงวนลิขสิทธิ์ทุกประการ
พิมพ์ครั้งที่ 1 — บราซิล



บทที่ 1

หัวใจคือเอนด์พอยต์ใหม่

ตลอดหลายทศวรรษที่ผ่านมา อุตสาหกรรมความมั่นคงปลอดภัยไซเบอร์พัฒนาโดยมุ่งเน้นเทคโนโลยีแทบทั้งหมด ไม่ว่าจะเป็นไฟร์วอลล์ที่ชาญฉลาดขึ้น โปรแกรมป้องกันไวรัสที่ใช้ฮิวริสติกขั้นสูง การยืนยันตัวตนแบบหลายปัจจัย และการเข้ารหัสที่แทบถอดไม่ได้ แต่ขณะที่มาตรการทางเทคนิคก้าวหน้า พื้นที่สำคัญด้านหนึ่งยังคงเปิดรับความเสี่ยง นั่นคือ **ปัจจัยมนุษย์** และไม่ใช่ว่าเพียงพฤติกรรมทั่วไป หากคือ**อารมณ์**

การโจมตีทางไซเบอร์สมัยใหม่ไม่ได้จำกัดอยู่เพียงการใช้ประโยชน์จากช่องโหว่ของระบบปฏิบัติการหรือแอปพลิเคชันอีกต่อไป แต่พุ่งเป้าไปยังชั้นที่ลึกและเปราะบางกว่ามาก นั่นคือ**จิตใจ** วิศวกรรมสังคมได้ก้าวข้ามการเป็นกลลวงทางจิตวิทยาแบบง่าย ๆ ปัจจุบันถูกจัดโครงสร้าง ศึกษา ทำให้เป็นอัตโนมัติ และดำเนินการอย่างแม่นยำ เป้าหมายจึงไม่ใช่เพียงอุปกรณ์ แต่รวมถึงความรู้สึก อารมณ์ และสัญชาตญาณ

“โดยทั่วไป มนุษย์มักถูกชี้นำด้วยสายตามากกว่ามือ เพราะทุกคนมองเห็นได้ แต่มีเพียงไม่กี่คนที่เข้าใจสิ่งที่ตนเห็น”

นิคโคโล มาเคียเวลลี

พืชซึ่งที่ซับซ้อนไม่ได้พึ่งพาเพียงลิงก์หรือช่องโหว่ทางเทคนิค แต่ตั้งอยู่บนเสาหลักทางจิตวิทยาสามประการที่พบได้ในทุกวัฒนธรรม ทุกชนชั้น และทุกวัย ได้แก่ **ศรัทธา ความพึงพอใจ และความโลภ** ตัวกระตุ้นเหล่านี้ทรงพลังจนลดทอน วิจารณ์ญาณ ระวังการใช้เหตุผลเชิงตรรกะ และทำให้ใครก็ตาม กลายเป็นช่องทางสู่การถูกเจาะระบบ ไม่มีข้อมูลประจำตัวใด แข็งแกร่งพอเมื่อการคลิกเกิดจากความเชื่อมั่นทางอารมณ์ และ ไม่มีระบบใดปลอดภัยได้อย่างแท้จริง หากผู้ใช้ใช้ได้อิทธิพล ของคำสัญญาหลอกลวงเรื่องความรอด ความพึงพอใจชั่วขณะ หรือความร่ำรวยอย่างง่ายดาย

ณ จุดนี้เอง ช่องโหว่ซีโรเดย์ที่แท้จริงของความมั่นคงปลอดภัย สมัยใหม่จึงถือกำเนิดขึ้น ไม่ใช่ช่องโหว่ที่ผู้พัฒนาซอฟต์แวร์ยังไม่รู้จัก แต่เป็นช่องโหว่ที่ซ่อนอยู่เงียบ ๆ ในจิตใต้สำนึกของ มนุษย์ เป็นจุดอ่อนที่มองไม่เห็น ซึ่งอาจถูกใช้ประโยชน์ได้โดย ไม่ถึงขั้นบันทึกเหตุการณ์ ไม่ก่อให้เกิดการแจ้งเตือน และไม่กระตุ้น โปรแกรมป้องกันไวรัส เป็นจุดอ่อนที่เราทุกคนมีอยู่

เราต้องยอมรับว่าแคมเปญพืชซึ่งในปัจจุบันพัฒนาไปมากทั้งด้าน การเล่าเรื่อง รูปลักษณ์ และเทคนิค ผู้โจมตีไม่ได้ต้องการเพียง ให้คุณคลิกอีกต่อไป เขาต้องการให้คุณเชื่อ ต้องการให้คุณ **ปรารถนา และต้องการให้คุณรู้สึกว่าคุณขาดสิ่งนั้นไม่ได้**

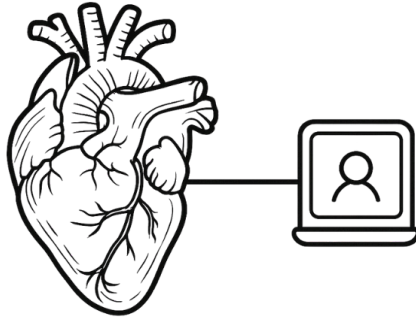
รายงานเหตุการณ์ในช่วงไม่กี่ปีที่ผ่านมาเผยให้เห็นรูปแบบ เดียวกัน นั่นคือ การเข้าถึงระบบครั้งแรกไม่ได้เกิดจากเทคนิค โจมตีระยะไกลที่ซับซ้อนเสมอไป แต่เกิดจากอีเมลที่ดูไม่มีพิษ ภัยหรือข้อความสั้น ๆ ที่ปรับให้ตรงกับผู้รับและส่งมาในเวลาที

เหมาะสม หัวเรื่องที่เขียนอย่างแนบเนียน ข้อความสั้นแต่เปี่ยมด้วยแรงกระตุ้นทางอารมณ์ ลิงก์ที่อำพรางด้วยความเร่งด่วนเพียงคลิกเดียว ทุกอย่างก็เริ่มพังทลาย

ในหนังสือเล่มนี้ เราจะสำรวจกลไกทางอารมณ์ที่อยู่เบื้องหลังการโจมตีอันซับซ้อนที่สุดในปัจจุบัน แต่ละบทจะกล่าวถึงเสาหลักหนึ่งประการ ได้แก่ **ศรัทธา ความพึงพอใจ และความโลภ** ไม่ใช่ในฐานะแนวคิดนามธรรม แต่ในฐานะพื้นผิวการโจมตีที่เกิดขึ้นจริง

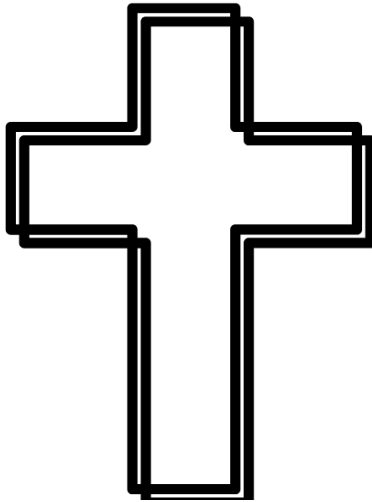
เราจะนำเสนองานวิจัยทางวิทยาศาสตร์ กรณีศึกษาจริง และการประยุกต์ใช้ในทางปฏิบัติ ที่สำคัญยิ่งกว่านั้น เราจะแสดงวิธีปกป้ององค์กรไม่เพียงด้วยเทคโนโลยี แต่ด้วยความเข้าใจพฤติกรรมและววัฒนะทางจิตวิทยา

ช่องโหว่ที่ร้ายแรงที่สุดของบริษัทอาจไม่ได้อยู่ในระบบ แต่อยู่ในการรับรู้ของผู้คน เอนด์พอยต์ไม่ได้มีเพียงคอมพิวเตอร์อีกต่อไป เอนด์พอยต์ใหม่คือหัวใจ



บทที่ 2

ศาสนา: ศรัทธาในฐานะเครื่องมือทางการรับรู้



"ผู้ก่อตั้งสาธารณรัฐใช้ศาสนาเป็นเครื่องมือที่
จำเป็นเพื่อรักษาความเชื่อฟังและความสามัคคี
ของประชาชน"

ปาฐกถาว่าด้วยทศวรรษแรกของดิตุส ลิวีส

นิคโคโล มาเคียเวลลี

นับตั้งแต่รุ่งอรุณแห่งอารยธรรม ศรัทธาเป็นหนึ่งในรากฐานของ
ประสบการณ์มนุษย์มาโดยตลอด ตั้งแต่ถ้ำยุคหินเก่า วิหารอี
ยิปต์โบราณ มหาวิหารในยุคกลาง ไปจนถึงโบสถ์สมัยใหม่ ความ
ปรารถนาที่จะเชื่อในสิ่งที่ยิ่งใหญ่กว่าตนเองอยู่คู่กับมนุษยชาติ
เสมอ **ศรัทธามอบความปลอดภัย ความหมาย และเกราะ**
ป้องกันความไม่แน่นอน และเพราะหยิ่งรักลึกเช่นนี้ จึงอาจถูก
นำมาใช้บังคับได้เช่นกัน

วิศวกรรมสังคมที่ใช้ประเด็นทางศาสนาเป็นหนึ่งในรูปแบบพิชชิง
ทางจิตวิทยาที่ได้ผลมากที่สุด ต่างจากการโจมตีแบบดั้งเดิมที่
อาศัยช่องโหว่ทางเทคนิค วิธีนี้มุ่งเป้าไปยังแก่นของความเชื่อ
ส่วนบุคคลโดยตรง เมื่อข้อความอ้างอิงศรัทธา มันจะข้าม
กระบวนการใช้เหตุผลและเข้าถึงจุดบอดทางอารมณ์ ผู้คนมักไม่
ตรวจสอบอย่างรอบคอบเมื่อเผชิญกับสิ่งที่ตนคิดว่าเป็น
ปาฏิหาริย์ การเปิดเผยจากเบื้องบน หรือการโจมตีความเชื่อของ
ตน แต่จะตอบสนองทันที

ในโลกที่แบ่งขั้วอย่างรุนแรง ซึ่งการถกเถียงเรื่องความเชื่อทาง
ศาสนาเกิดขึ้นในรัฐสภา บนโซเชียลมีเดีย และบนท้องถนน วลี
ง่ายๆ อย่าง "ดูสิว่าพวกเขาค้นพบอะไรเกี่ยวกับวันสิ้นโลก"
สามารถทำให้ผู้คนนับพันคลิกลงได้ทันที และยังข้อความ
สอดคล้องกับมุมมองโลกของแต่ละบุคคลมากเท่าไร ก็ยังมี

ประสิทธิภาพมากขึ้นเท่านั้น ความอยากรู้อยากเห็นทางจิต
วิญญาณจึงแปรเปลี่ยนไปเป็นแรงกระตุ้นทางจิต

แคมเปญพีชชิงที่ใช้เนื้อหาทางศาสนาถูกนำไปใช้ในการโจมตี
ขนาดใหญ่อย่างแพร่หลาย ตัวอย่างเช่น ในช่วงการระบาดของ
โควิด-19 มีอีเมลแอบอ้างเป็นผู้นำทางศาสนา
ตั้งแต่ศิษยาภิบาล อิหม่าม ไปจนถึงรับบี แพร่กระจายไปทั่วโลก
โดยเสนอคำแนะนำทางจิตวิญญาณ ขอให้ร่วมอธิษฐาน หรือ
แม้แต่อ้างว่าจะรักษาโรคอย่างปาฏิหาริย์ อีเมลจำนวนมากมีลิง
ก์ไปยังมัลแวร์ ซึ่งเมื่อตกเป็นเหยื่อคลิก จะติดตั้งแบ็กดอร์บน
อุปกรณ์ส่วนบุคคลและอุปกรณ์ขององค์กรโดยไม่รู้ตัว

งานศึกษาเรื่อง **“Religion and the Psychology of
Meaning”** ของ Routledge และ Shariff ซึ่งตีพิมพ์ในปี 2013
สนับสนุนตรรกะนี้ โดยชี้ว่าศรัทธาทำหน้าที่เป็นกลไกสร้าง
เสถียรภาพทั้งทางอารมณ์และการรับรู้ เมื่อถูกกระตุ้น กลไกแห่ง
ความสงสัยจะลดลง ขณะที่แนวโน้มจะลงมือทำทันทีเพิ่มขึ้น
คุณลักษณะที่มีคุณค่าต่อมนุษย์นี้จึงกลายเป็นจุดอ่อนเมื่อถูกผู้
โจมตีนำไปใช้

กรณีศึกษา

กลโกงที่โบสถ์เซนต์จอห์น

แรงจูงใจของการโจมตี

ศรัทธาและความไว้วางใจช่วยยึดโยงชุมชนทางศาสนา แต่ในเวลาเดียวกันก็ทำให้ชุมชนเหล่านี้เป็นเป้าหมายที่น่าดึงดูดสำหรับฟิชซิง มีงานวิจัยพบว่าผู้ศรัทธามีความสัมพันธ์อันอบอุ่นและให้ความเคารพต่อผู้นำทางจิตวิญญาณ จึงเปลี่ยนอำนาจทางศาสนาให้เป็นเครื่องมือของการทางอารรมณ์ได้ง่าย

ในเดือนพฤษภาคม ปี 2023 อาชญากรไซเบอร์เริ่มใช้ประโยชน์จากความไว้วางใจนี้ในการก่ออาชญากรรมทางการเงิน

ใครคือเป้าหมาย

เป้าหมายคือสมาชิกของโบสถ์เซนต์จอห์นเอพิสโกพัลในสหรัฐอเมริกา ซึ่งคุ้นเคยกับการรับข่าวสารจากโบสถ์ทางอีเมล เพียงมีชื่อใหม่ว่า “คุณเลสลี” ปรากฏบนเว็บไซต์ทางการของโบสถ์ ก็เพียงพอให้ผู้โจมตีเริ่มแผนหลอกลวง

เทคนิคที่ใช้

1. ผู้โจมตีสร้างอีเมลปลอมโดยแอบอ้างเป็นผู้นำทางศาสนาของโบสถ์ เช่น คุณเลสลีและบาทหลวงลอนนี่
2. พวกเขาใช้ที่อยู่อีเมลที่คล้ายกับที่อยู่อย่างเป็นทางการ แต่ไม่ได้เป็นของโบสถ์จริง
3. ข้อความใช้ถ้อยคำกระตุ้นอารมณ์และความเร่งด่วน เช่น:
 - “ผมต้องการความช่วยเหลืออย่างเร่งด่วน”
 - “โปรดดำเนินการโดยด่วน”
4. อีเมลขอให้เหยื่อซื้อบัตรของขวัญแล้วส่งรหัสทางอีเมล ซึ่งเป็นรูปแบบการโอนมูลค่าที่ติดตามได้ยาก
5. ในบางกรณี เหยื่อถูกส่งต่อไปยังเว็บไซต์ฟิชชิงปลอมเพื่อขโมยข้อมูลทางการเงิน

หลักฐานและรายละเอียดของการโจมตี

(no subject) 



Rev. Lonnie Lacy <revlonnie.saintjohn@gmail.com>
to me ▾

12:41 PM (2 hours ago) ☆ ↶ ⋮

Hello Amanda, are you less busy at the moment? I have a request for you to manage confidentially. I will be into a meeting in few minutes, no calls so kindly respond via email.

Blessings!
Rev. Lonnie Lacy
Rector

From: "Rev. Lonnie Lacy" <lacylonnie.saintjohn@gmail.com>

Date: Thursday, October 6, 2022 at 2:34 PM

To

Subject: Re: Emily

Thanks for the swift reply, Here's what I want you to do for me because I think you are in the best position to do this for me discreetly.

I have been counseling and encouraging some cancer patients and aimed to reward them with " Gift Cards " this week to show how much we care about them.

This should be confidential until they all have the "Gift cards" as it's a surprise.

Can you get this done? and how soon? I will be responsible for the reimbursement personally.

เหตุใดการโจมตีจึงได้ผล

การใช้**ศรัทธา**ร่วมกับอำนาจของผู้นำทางศาสนาสร้างสถานการณ์ที่ทำให้เหยื่อลดความระมัดระวัง เพราะใครเล่าจะสงสัยคำขอที่มาจาก “บาทหลวงเอง”

นอกจากนี้ ภาษาที่ใช้ยังเรียบง่าย คั่นเคย และเลียนแบบน้ำเสียงสำรวจของผู้นำทางศาสนาในโบสถ์

พลวัตทางจิตวิทยาของศรัทธาไม่ได้เรียกร้องหลักฐาน แต่เรียกร้องการยอมรับ และในช่วงเวลาแห่งการยอมรับนั่นเอง ผู้ใช้จึงคลิกลิงก์ที่เป็นอันตราย กรอกข้อมูลประจำตัว และทำให้ระบบเริ่มพังทลาย

เพื่อป้องกันการโจมตีประเภทนี้ องค์กรต้องไม่มองผู้ใช้เป็นเพียงองค์ประกอบทางเทคนิค การฝึกอบรมด้านความมั่นคงปลอดภัยต้องครอบคลุมบริบททางอารมณ์และสังคมด้วย เราจำเป็นต้องพูดถึงศาสนาด้วยความเคารพ พร้อมชี้ให้เห็นอย่างชัดเจนว่าประเด็นทางศาสนาก็อาจกลายเป็นพื้นผิวการโจมตีได้ ตัวกรองแบบปรับตัวที่ตรวจจับรูปแบบเนื้อหาทางศาสนาที่เกิดขึ้นใหม่ เครื่องมืออย่าง **VirusTotal**, **urlscan.io** และ **MXToolbox** ตลอดจนการวิเคราะห์แคมเปญด้วยคำสำคัญทางจิตวิญญาณควรเป็นส่วนหนึ่งของระบบป้องกันทางอารมณ์ ยิ่งกว่าที่เคย ศรัทธาต้องได้รับความเคารพ แต่ก็ต้องได้รับการ

ทำความเข้าใจในบริบทของภัยไซเบอร์สมัยใหม่ ในโลกที่ผู้คนอ่านข้อความด้วยอารมณ์มากกว่าเหตุผล การป้องกันที่แท้จริงเริ่มต้นจากความเข้าใจจิตใจมนุษย์

บทที่ 3

**ความพึงพอใจ: การถึงจุดสุดยอดในฐานะตัวกระตุ้นความ
หมุนหันพลันแล่น**

จิตใจมนุษย์ถูกออกแบบมาให้แสวงหารางวัล ในบรรดารางวัลตามธรรมชาติของร่างกาย ความพึงพอใจทางเพศอยู่ในลำดับต้นๆ ของลำดับชั้นแห่งความปรารถนา มันเป็นไปตามสัญชาตญาณไร้เหตุผล และมียากจะต้านทาน แรงกระตุ้นนี้ไม่ได้เป็นเพียงประสบการณ์ทางชีววิทยา แต่เป็นจุดอ่อนที่แคมเปญวิศวกรรมสังคมสามารถใช้ประโยชน์ได้ด้วยอัตราความสำเร็จสูง

ต่างจากความกลัวที่อาจทำให้เราเป็นอัมพาต ความพึงพอใจผลักดันให้เราลงมือทำ บ่อยครั้งโดยไม่ไตร่ตรอง และรูปแบบการตอบสนองอัตโนมัตินี้เองที่ทำให้ความพึงพอใจ โดยเฉพาะความพึงพอใจทางเพศ กลายเป็นเครื่องมืออันตรายพลังในการบงการระบบและตัวตนดิจิทัล

ในสภาพแวดล้อมขององค์กร ความปรารถนาที่จะมีความเป็น
ส่วนตัวและปกปิดพฤติกรรมส่วนตัวกลับสร้างสภาพแวดล้อมที่
เอื้อต่อการถูกชักจูงอย่างยิ่ง ไม่มีใครอยากยอมรับว่าตนเอง
เข้าถึงเนื้อหาสำหรับผู้ใหญ่ในระหว่างเวลาทำงาน ไม่มีใครอยาก
ให้ใครรู้ว่าตนเองได้รับข้อความลามกอนาจาร ความเจ็บและความ
อับอายนี้จึงกลายเป็นพันธมิตรของผู้โจมตี



"หากมนุษย์ควบคุมคำพูดและแรงกระตุ้นทางเพศ
ของตนได้ สงครามมากมายคงจะหลีกเลี่ยงได้"

โสกราตีส

**หลายศตวรรษผ่านไป เรายังคงเปราะบางต่อแรงกระตุ้น
เดิม และในโลกไซเบอร์ ราคาของการไม่สามารถควบคุม
แรงกระตุ้นอาจสูงมาก**

หนึ่งในกรณีที่เป็นที่รู้จักมากที่สุดเกิดขึ้นในปี 2020 เมื่อแคมเปญฟิชชิงแพร่กระจายผ่านอีเมลที่ดูเหมือนส่งมาจากเพื่อนร่วมงาน หัวเรื่องชวนสงสัยว่า “ดูสิว่ามีอะไรเกี่ยวกับคุณหลุดออกมา” เนื้อหาแนบลิงก์ไปยังเว็บไซต์ที่อ้างว่ามีภาพส่วนตัวของเหยื่อหรือคนใกล้ชิด เว็บไซต์ดังกล่าวเลียนแบบบริการแบ่งปันสื่อยอดนิยมและกำหนดให้เข้าสู่ระบบเพื่อดูภาพ ภายในเวลาไม่ถึง 48 ชั่วโมง ผู้ใช้หลายพันคนในกว่าสิบประเทศได้มอบข้อมูลประจำตัวขององค์กรให้แก่ผู้โจมตี

การโจมตีเหล่านี้ได้ผลเพราะกระทบต่อระบบลิมบิก ซึ่งเป็นบริเวณสมองที่เกี่ยวข้องกับอารมณ์และแรงจูงใจ งานศึกษา “The Neurobiology of Sexual Behavior” ของ Pfau และคณะ ซึ่งตีพิมพ์ในวารสาร **Frontiers in Neuroendocrinology** เมื่อปี 2009 ชี้ว่า การถึงจุดสุดยอดกระตุ้นวงจรสมองเดียวกับที่ถูกกระตุ้นโดยสารโอปิออยด์ เช่น มอร์ฟิน ข้อค้นพบนี้แสดงให้เห็นว่าความพึงพอใจทางเพศไม่ใช่เพียงความปรารถนา แต่เป็นปัจจัยทรงพลังที่อาจลดทอนการตัดสินใจอย่างมีเหตุผล

กรณีศึกษา

เมื่อผู้เข้าร่วมประชุม G20 คลินิกสุขภาพส่วนตัว

บรรยากาศเต็มไปด้วยความตึงเครียด นี่คือการประชุม G20 ผู้นำโลกมารวมตัวกัน แลกเปลี่ยนความลับกันหลังประตูที่ปิดสนิท การตัดสินใจที่อาจเปลี่ยนแปลงทิศทางเศรษฐกิจโลกถูกถกเถียงกันในห้องลับๆ และท่ามกลางการทูตและพิธีการต่างๆ ความปรารถนาก็ผุดขึ้นมา

ในการประชุมสุดยอดที่จัดขึ้น ณ กรุงปารีสเมื่อปี 2011 ผู้แทนและเจ้าหน้าที่รัฐบาลจากหลายประเทศ เช่น **สาธารณรัฐเช็ก บัลแกเรีย โปตุเกส ฮังการี และลัตเวีย** เริ่มได้รับอีเมลนิรนามที่มีหัวเรื่องชวนคลิกลอยๆ:

“ชมภาพส่วนตัวของคาร์ลา บรูนี”

คาร์ลา บรูนี อดีตสุภาพสตรีหมายเลขหนึ่งของฝรั่งเศสและนางแบบชื่อดัง เป็นสัญลักษณ์แห่งความงามและความสง่างาม ผู้หญิงที่ดึงดูดสายตา และในบริบทนั้น ชื่อของเธอถูกนำมาใช้เป็นเหยื่อล่อ

ลึกลับเหมือนไม่มีพิษภัย ใครจะสงสัยข้อความเช่นนี้ระหว่างการประชุมระหว่างประเทศ ท่ามกลางภารกิจและข้อมูลสำคัญมากมาย การคลิกเกิดขึ้นอย่างรวดเร็ว เป็นไปโดยอัตโนมัติและปราศจากความระแวง ซึ่งตรงกับสิ่งที่ผู้โจมตีคาดหวัง

หลักฐานของคดี



เมื่อเข้าถึงลิงก์ อุปกรณ์ของผู้เข้าร่วมประชุมถูกเจาะโดยไม่รู้ตัว โทรจันติดตั้งตัวเองอย่างเงียบ ๆ ทำให้ผู้โจมตีควบคุมเครื่องจากระยะไกลได้อย่างเต็มรูปแบบ สามารถมองเห็น รับฟัง บันทึก

และติดตามกิจกรรมต่าง ๆ ได้ ไม่มีสิ่งใดปลอดภัยอีกต่อไป
ความปรารถนาเอาชนะวิจารณ์แล้ว

การสืบสวนระบุว่าการโจมตีมีต้นทางจากจีน เป้าหมายคือการ
จารกรรมระดับสูง ทั้งข้อมูลเชิงยุทธศาสตร์ การตัดสินใจลับ และ
การสื่อสารภายใน ล้วนตกอยู่ในมือของสายลับไซเบอร์ สิ่ง
ที่ดูเหมือนเป็นเพียงอีเมลที่ไม่เหมาะสม กลับกลายเป็นหนึ่งในการ
ละเมิดความมั่นคงปลอดภัยไซเบอร์ครั้งใหญ่ที่สุดในงานระดับ
นานาชาติ

คดีนี้เปิดเผยความลับที่น่าตกใจ: ไม่ว่าเป้าหมายจะมีความ
เชี่ยวชาญ มีประสบการณ์ หรือสำคัญแค่ไหน เราทุกคนก็มี
จุดอ่อนทางอารมณ์

ที่นั่น ท่ามกลางรัฐมนตรีและนักการทูต สิ่งที่พังทลายลงไม่ใช่แค่
ความปลอดภัยของอุปกรณ์เท่านั้น ตำนานแห่งความคงกระพัน
ได้พังทลายลง ความเชื่อมั่นในความรอบคอบ และเหนือสิ่งอื่นใด
ความเชื่อที่ว่าความปรารถนาสามารถควบคุมได้ด้วยเหตุผลเพียง
แค่คลิกเดียว

นี่คือพลังที่แท้จริงของวิศวกรรมทางสังคม: มันไม่ได้ทำลาย
ระบบ แต่ทำลายผู้คน การตอบสนองทางระบบประสาทนี้บ่งชี้ว่า
เมื่อเผชิญกับคำสัญญาแห่งความสุข สมอจะลดการทำงานของ
เยื่อหุ้มสมองส่วนหน้า ซึ่งเป็นบริเวณที่รับผิดชอบการคิดอย่างมี

วิจารณ์ญาณ การประเมินความเสี่ยง และการควบคุมแรงกระตุ้น
นี่คือเหตุผลที่แม้แต่ผู้เชี่ยวชาญที่มีประสบการณ์ เมื่อเผชิญกับ
สิ่งล่อใจทางเพศ ก็ยังทำผิดพลาดด้านความปลอดภัยขั้นพื้นฐาน
การคลิกในบริบทนี้จึงเป็นเรื่องของอารมณ์มากกว่าเหตุผล

กรณีศึกษา

เมื่อความปรารถนาทำให้ทหาร NATO ตกเป็นเหยื่อ

อีกปฏิบัติการหนึ่งที่สร้างความตกตะลึงเกิดขึ้นในสภาพแวดล้อม
ทางทหาร เมื่อปี 2018 ทหารจากฐานทัพ NATO ได้รับคำเชิญ
เป็นเพื่อนจากโปรไฟล์นางแบบบนเครือข่ายสังคม จากนั้นเริ่มมี
การสนทนาส่วนตัว การส่งภาพเซ็กซี่ๆ และคำสัญญาว่าจะส่ง
วิดีโอส่วนตัว แลกกับการติดตั้ง “เวอร์ชันใหม่” ของแอปวิดีโอ
แต่ไฟล์ดังกล่าวคือมัลแวร์โทรจันที่บันทึกการกดแป้นพิมพ์
ขโมยข้อมูล และคงอยู่ในระบบโดยผู้ใช้ไม่รู้ตัว

ผลลัพธ์คือ อุปกรณ์ปลายทางหลายเครื่องถูกเจาะ และผู้โจมตี
สามารถเข้าถึงระบบภายในของฐานทัพจากระยะไกล

หลักฐานของกรณีศึกษา (เพื่อการฝึกอบรม)

WIRE

SIGN IN

SUBSCRIBE



NATO Group Catfished Soldiers to Prove a Point About Privacy

With \$60 and a few fake Facebook accounts, researchers were able to identify service members in a military exercise, track their movement, and even persuade them to disobey orders.



จากมุมมองของผู้โจมตี การหลอกลวงโดยใช้เรื่องเพศเป็นวิธีที่ทำได้ง่ายและให้ผลตอบแทนสูงมาก มันต้องการเพียงแค่สามองค์ประกอบ ได้แก่ ภาพที่ชวนให้คิดไปในทางลามก เรื่องราวที่น่าเชื่อถือ และลิงก์ที่กระชับเหยื่อจะเต็มเต็มส่วนที่เหลือนด้วยจินตนาการของตนเอง

ในฝ่ายป้องกัน เราต้องยอมรับว่าเหยื่อล่อประเภทนี้ไม่ควรถูกปฏิบัติเป็นเรื่องต้องห้าม การเพิกเฉยไม่ได้ทำให้มันมี

ประสิทธิภาพลดลง องค์กรจำเป็นต้องรวมประเด็นเรื่องความพึงพอใจและเรื่องเพศไว้ในกรอบการสร้างมาตรฐาน โดยกล่าวถึงความเสี่ยงของวิศวกรรมสังคมเชิงการมณ้อย่างจริงจัง ให้เกียรติ และชัดเจน

ในทางเทคนิค สามารถนำมาตรการควบคุมและป้องกันต่อไปนี้มาใช้:

- I. **การตรวจสอบปริมาณการเข้าชมเว็บไซต์ที่มีชื่อเสียงไม่ดี โดยเฉพาะเว็บไซต์ที่เกี่ยวข้องกับภาพลามกอนาจาร**
- II. **การบล็อกลิงก์ย่อและการนำระบบแสดงตัวอย่าง URL มาใช้**
- III. **ใช้ตัวกรองเนื้อหาอัจฉริยะร่วมกับแมชชีนเลิร์นนิ่งที่ได้รับการฝึกฝนจากรูปแบบการหลอกลวงทางเพศ**
- IV. **การจำลองฟิชซิงที่ใช้เหยื่อล่อเชิงการมณด้วยเครื่องมือ เช่น GoPhish พร้อมติดตามตัวชี้วัดและเสริมความรู้ตามความเสี่ยงที่พบ**

นอกจากนี้ สามารถใช้เครื่องมืออย่าง Cortex XSOAR, Proofpoint TAP และ Zscaler เพื่อตรวจจับแคมเปญลักษณะนี้เชิงรุก รวมถึงวิเคราะห์ความหมายของข้อความและรูปภาพที่ฝังอยู่

ท้ายที่สุด ความพึงพอใจจะยังเป็นแรงขับเคลื่อนที่ทรงพลังตราบนานเท่านานยังเป็นความปรารถนาที่เราไม่เข้าใจอย่างถ่องแท้ ความท้าทายของความมั่นคงปลอดภัยสมัยใหม่คือการพัฒนากลยุทธ์ที่ช่วยปกป้องผู้คนจากแรงกระตุ้นของตนเอง เพราะภัยคุกคามที่แท้จริงไม่ได้อยู่ในโค้ดที่เป็นอันตรายเท่านั้น แต่อยู่ในเรื่องราวที่เชื่อถือได้ว่าตนเองฟังเพื่อสร้างเหตุผลให้กับการคลิก

บทที่ 4

ความโลภ: ความปรารถนาอันไม่รู้จักพอที่จะมีมากขึ้น

หากความสุขเป็นแรงขับเคลื่อนของช่วงเวลานั้น ความโลภก็เป็นแรงขับเคลื่อนของโครงการทั้งหมด มันเป็นอารมณ์ที่เจ็บปวดกว่า ตัณหา ไม่ก่อให้เกิดข้อถกเถียงมากเท่าความศรัทธา แต่ก็อันตรายไม่น้อยไปกว่ากัน ความโลภอาจแสดงตัวออกมาในรูปแบบของความทะเยอทะยานที่ถูกต้องตามกฎหมาย ในฐานะเป้าหมาย ในฐานะความปรารถนาที่จะเติบโต อย่างไรก็ตาม เมื่อถูกบีบเบียน มันจะเปิดช่องโหว่ที่ร้ายแรงพอๆ กับจุดอ่อนที่สำคัญใดๆ และนั่นคือสิ่งที่อาชญากรไซเบอร์ใช้ประโยชน์: ความ

ปรารถนาของมนุษย์ที่จะได้มากขึ้น เงินมากขึ้น เกียรติยศมากขึ้น
ความสะดวกสบายมากขึ้น ผลตอบแทนมากขึ้น

ต่างจากสิ่งกระตุ้นทางอารมณ์อื่นๆ ความโลภเป็นสิ่งที่สังคมยอมรับและส่งเสริม มันปรากฏอยู่ในแคมเปญโฆษณา คำสัญญาเรื่องหลักสูตรมหัศจรรย์ กูรูด้านการเงิน และวาทกรรมเรื่องความสามารถที่เกินจริง ด้วยเหตุนี้เอง จึงยากที่จะมองว่ามันเป็นจุดอ่อนด้านความปลอดภัย แต่ที่จริงแล้วมันเป็นเช่นนั้น

การหลอกลวงทางสังคมที่ขับเคลื่อนด้วยความโลภได้กลายเป็นหนึ่งในปัจจัยหลักที่ก่อให้เกิดการโจมตีทางดิจิทัล โดยเฉพาะในสภาพแวดล้อมขององค์กร ผู้บริหารที่รีบร้อนเพื่อผลกำไร พนักงานที่ต้องการรายได้เสริม หรือแม้แต่ผู้ใช้ทั่วไปที่มองหาโอกาสอย่างรวดเร็ว ล้วนเป็นเป้าหมายที่เป็นไปได้

ตัวอย่างที่ชัดเจนเกิดขึ้นในบราซิลในปี 2021 ระหว่างช่วงที่การลงทุนในสกุลเงินดิจิทัลเฟื่องฟู อีเมลฉบับหนึ่งถูกส่งต่อโดยมีหัวข้อว่า "สกุลเงินใหม่สัญญาว่าจะเพิ่มขึ้น 300% ใน 15 วัน - บทวิเคราะห์พิเศษโดย Forbes" อีเมลดังกล่าวมีกราฟปลอมและลิงก์ไปยังแพลตฟอร์มการลงทุนปลอม เมื่อเหยื่อพยายามลงทะเบียน พวกเขาต้องกรอกข้อมูลส่วนตัวมากมาย ข้อมูลส่วนบุคคล และแม้แต่เอกสารประจำตัวที่สแกนแล้ว ในเวลาไม่ถึงสามสัปดาห์ มีผู้ถูกหลอกลวงมากกว่า 1,200 คน และสูญเสียเงินไปมากกว่า 12 ล้านเรียลบราซิล



**"โดยทั่วไปแล้วมนุษย์ถูกขับเคลื่อนด้วยอารมณ์
ความรู้สึกสองอย่างหลักๆ คือ ความรักและความ
กลัว แต่มีน้อยคนนักที่จะต้านทานคำสัญญาแห่ง
ผลประโยชน์ได้"**

Niccolò Machiavelli - เจ้าชาย

กรณีศึกษา

วันที่ทวีตเตอร์ถูกแฮ็ก

คำสัญญานั้นเรียบง่าย ยากจะต้านทาน และอันตรายถึงชีวิต: “ส่งบิตคอยน์จำนวนเท่าใดก็ได้ แล้วรับคืนเป็นสองเท่า” เหลือพร้อมอยู่แล้ว ความโลภคือเบ็ด และโลกก็กัดเหยื่อ

เมื่อวันที่ 15 กรกฎาคม 2020 ทวิตเตอร์ หนึ่งในแพลตฟอร์มการสื่อสารที่ใหญ่ที่สุดในโลก ตกเป็นเป้าหมายของการโจมตีทางไซเบอร์ที่อุกอาจที่สุดครั้งหนึ่งในประวัติศาสตร์ยุคใหม่ บัญชีที่ได้รับการยืนยัน ซึ่งเป็นสัญลักษณ์ของอำนาจในโลกดิจิทัล ถูกเปลี่ยนเป็นเครื่องมือฉ้อโกง อีลอน มัสก์ บาร์ค โอบามา Apple และ Uber รวมถึงบัญชีสำคัญอื่น ๆ กลายเป็นหุ่นเชิดในแผนบงการอันโหดร้าย เบื้องหลังคือคนหนุ่มสาวที่มีความรู้ทางเทคนิคและอาวุธที่มองไม่เห็น นั่นคือ วิศวกรรมสังคม

จุดเริ่มต้นของกลโกง: เมื่อความโลภเข้ามามีบทบาท

เรื่องทั้งหมดเริ่มต้นด้วยคำโกหกที่แนบเนียน แต่ไม่ใช่แค่คำโกหกธรรมดา มันคือคำสัญญาเรื่องความร่ำรวยในทันที ข้อความที่แฝงไปด้วยความเอื้อเฟื้อเผื่อแผ่ โฆษณาผ่านโปรไฟล์ที่ได้รับ ความไว้วางใจทั่วโลก: “เรากำลังตอบแทนสังคม ส่ง Bitcoin ไปที่ที่อยู่นี้ แล้วคุณจะได้รับสองเท่าในไม่ช้า”

ความโลภนั้นกระตุ้นสัญชาตญาณดั้งเดิมที่สุดของจิตใจมนุษย์โดยตรง ความปรารถนาที่จะได้กำไรง่ายๆ นั้นเหมือนไฟฟ้า มันแพร่กระจายอย่างรวดเร็วและเผาผลาญตรรกะ ในเวลาไม่ถึงสามสัปดาห์ พวกมิจนาซีพได้เงินบิตคอยน์ไปกว่า 100,000 ดอลลาร์ เพียงเพราะผู้คนเชื่อว่าพวกเขา กำลังจะได้เงินเพิ่มเป็นสองเท่า แต่สิ่งที่ไม่มีการคาดคิดก็คือ เบื้องหลังนั้น แฮกเกอร์ได้แทรกซึมเข้าไปในระบบประสาทของแพลตฟอร์มแล้ว

หลักฐานของคดี

 Resultados Fútbol AS TV

as

En unos casos en el tweet se anunciaba que cualquier cantidad enviada llegaría doblada al usuario y en otras que las empresas hackeadas **donarían 10 millones de dólares** entre los seguidores.

Un hackeo que se salta la doble verificación

Esto, más allá de la estafa que entraña, también supone un grave problema de seguridad para una de las redes sociales más usadas en todo el mundo. Algunas cuentas hackeadas contaban con un **sistema de doble verificación** y aun así se ha podido penetrar en ellas.



Barack Obama ✓
@BarackObama

I am giving back to my community due to Covid-19!

All Bitcoin sent to my address below will be sent back doubled. If you send \$1,000, I will send back \$2,000!

Captura de Tela

ผู้บังคับการคือวิศวกรสังคม

การโจมตีไม่ได้เริ่มจากโค้ดที่ซับซ้อน แต่เริ่มจากการสนทนาทางโทรศัพท์ แฮ็กเกอร์ใช้วิธีเก่าแก่แต่ได้ผล นั่นคือ วิศวกรรมสังคม พวกเขาแอบอ้างเป็นสมาชิกทีมไอทีของทวีตเตอร์ ติดต่อพนักงานตัวจริง สร้างความไว้วางใจ และค่อย ๆ ขโมยข้อมูลสำหรับเข้าถึงระบบ

วิธีการนี้เรียกว่า **สเปียร์ฟิชชิง** ซึ่งเป็นการโจมตีที่เจาะจงและปรับให้ตรงกับเป้าหมาย ทุกขั้นตอนถูกคำนวณเพื่อสลายการต่อต้านและโน้มน้าวเหยื่อ พนักงานที่ถูกหลอกจึงมอบสิ่งที่ผู้โจมตีต้องการมากที่สุด นั่นคือ การเข้าถึงเครื่องมือบริหารภายในของบริษัทโดยตรง

กฤษฎีกา

เมื่อเข้าถึงระบบได้ แฮ็กเกอร์ก็เปิดใช้แผงควบคุมภายในที่เรียกว่า “agent tool” ซึ่งสามารถรีเซ็ตรหัสผ่าน เปลี่ยนที่อยู่อีเมล และเข้าควบคุมบัญชีใด ๆ ได้อย่างสมบูรณ์

ลองนึกภาพปราสาทแห่งหนึ่ง ที่ประตูทุกบานถูกล็อกด้วยรหัสผ่านและการตรวจสอบสิทธิ์ แล้วลองนึกภาพว่ามีคนได้กุญแจหลักของปราสาทไป นั่นคือสิ่งที่เกิดขึ้น ผู้บุกรุกไม่จำเป็นต้องใช้รหัสผ่านจริงของผู้ใช้ด้วยซ้ำ ด้วยเครื่องมือภายใน พวกเขาสามารถควบคุมทุกอย่างได้ และพวกเขาก็ทำได้อย่างยิ่งใหญ่

ผลกระทบ

บัญชีประมาณ 130 บัญชีถูกเจาะ ไม่ใช่บัญชีธรรมดา แต่เป็นสัญลักษณ์แห่งอำนาจ อิทธิพล และความไว้วางใจระดับโลก เช่น อีลอน มัสก์ โจ ไบเดน บิล เกตส์ และ Apple ทุกบัญชีดูเหมือนกำลังเผยแพร่ข้อความเดียวกัน

ปฏิบัติการเกิดขึ้นอย่างรวดเร็วและแม่นยำ ภายในไม่กี่นาที ผู้คนหลายพันคนทั่วโลกเชื่อว่ากำลังมีส่วนร่วมในกิจกรรมการก่อกวนหรือการตอบแทนสังคมที่ถูกต้อง ความโกลาหลและความสงสัย

คำสัญญาว่าจะได้รับผลตอบแทนทางการเงินจากบุคคลหรือ
องค์กรที่น่าเชื่อถือดูสมจริงเกินกว่าจะตั้งคำถาม

การโต้กลับ

ทวิตเตอร์ตอบสนองอย่างรวดเร็วและสิ้นหวัง เพื่อจำกัดความ
เสียหาย บริษัทจึงบล็อกบัญชีที่ได้รับการยืนยันไม่ให้โพสต์ทวิต
เป็นการชั่วคราว เป็นครั้งแรกที่ผู้เล่นรายใหญ่เจียบงัน ความเจียบ
ที่เกิดจากความเปราะบาง

ในขณะเดียวกัน คณะทำงานเฉพาะกิจถูกจัดตั้งขึ้นเพื่อทำความเข้าใจถึงขนาดของความล้มเหลว การสอบสวนภายในเริ่มต้นขึ้น
หน่วยงานด้านความปลอดภัยทางไซเบอร์ถูกเรียกตัวเข้ามา
ความตื่นตระหนกได้เริ่มขึ้นแล้ว ไม่เพียงเพราะเงินที่ถูกขโมยไป
แต่ยังเพราะการละเมิดความไว้วางใจด้วย

การสืบสวนนำไปสู่การจับกุมบุคคลสามคน หัวหน้าแก๊งคือชาย
หนุ่มอายุเพียง 17 ปีจากรัฐฟลอริดา เด็กหนุ่มที่มีทักษะมากกว่า
วุฒิภาวะ ถูกชี้นำด้วยความปรารถนาเดียวกับเป้าหมายของเขา
นั่นคือ ผลกำไรที่ได้มาง่ายๆ การยอมรับ และอำนาจ

พวกเขาเผชิญข้อหาฉ้อโกงทางอิเล็กทรอนิกส์ การบุกรุกระบบ
และการฟอกเงิน แต่สิ่งที่คดีนี้แสดงให้เห็นนั้นนอกเหนือไป
จากการพิจารณาคดีอาญา มันแสดงให้เห็นว่าแม้แต่แพลตฟอร์ม
ที่ทรงพลังที่สุดก็ยังอ่อนแอต่อการถูกมนุษย์แทรกแซงได้

ความผิดพลาดครั้งใหญ่ที่สุดของทวิตเตอร์ไม่ใช่ความล้มเหลวทางเทคนิค แต่เป็นความผิดพลาดของมนุษย์ ความไว้วางใจ การขาดการฝึกอบรม การไม่มีระบบยืนยันตัวตนหลายปัจจัย สำหรับขั้นตอนสำคัญ ทั้งหมดนี้ทำให้เกิดช่องโหว่ที่แม้แต่ไฟร์วอลล์ที่ดีที่สุดก็ไม่สามารถป้องกันได้

การโจมตีครั้งนี้สอนให้โลกเห็นว่า ความมั่นคงปลอดภัยไซเบอร์ไม่ได้เป็นเพียงเรื่องเทคโนโลยี แต่เกี่ยวข้องกับจิตวิทยาด้วย **ความโลภ**มักเป็นจุดอ่อนที่สุดในห่วงโซ่ และเมื่อผู้ไม่ประสงค์ดีนำไปใช้ ก็อาจทำให้แม้แต่บริษัทยักษ์ใหญ่แห่งยุคดิจิทัลต้องล้มครอน

“ความไว้วางใจสร้างขึ้นทีละหยด แต่สูญเสียไปเป็นถัง”

เควิน มิตนิก

บทนี้ไม่ได้เป็นเพียงเรื่องราวของการบุกรุก แต่สะท้อนสภาพมนุษย์เมื่อต้องเผชิญคำสัญญาเรื่องเงินทองที่ได้มาง่าย ๆ และเป็นคำเตือนว่า ตราบใดที่ยังมีความโลภ ก็จะมีผู้พร้อมฉวยประโยชน์จากมัน

การโจมตีเหล่านี้ไม่ได้ผลเพียงเพราะรูปลักษณะหรือการออกแบบเว็บไซต์ที่น่าดึงดูด แต่เพราะเข้าถึงเรื่องเล่าภายในของผู้ใช้ว่า “คราวนี้ต้องได้ผลแน่” หรือ “ถ้าไม่ลองก็ไม่มีวันรู้” นี่คือการใช้ประโยชน์จากความหวังทางเศรษฐกิจ

งานศึกษา “Greed, Envy and Financial Decision-Making” ของ Rao และ George ซึ่งตีพิมพ์ใน Journal of Behavioral and Experimental Economics เมื่อปี 2016 ชี้ว่า ความโลภกระตุ้นวงจรประสาทเดียวกับความกลัวและความปีติ เป็นอารมณ์ที่ลดทอนการควบคุมตนเอง บั่นทอนการใช้เหตุผล และทำให้คนมองข้ามสัญญาณเตือนที่ชัดเจน คำสัญญาว่าจะได้ผลประโยชน์ทันทีจึงทำให้ความรอบคอบเลือนหาย

ในการจำลองที่ดำเนินการโดยบริษัทที่ปรึกษาด้านความมั่นคงปลอดภัยรายใหญ่ในสหรัฐอเมริกา ทีม Red Team ส่งอีเมลถึงประธานเจ้าหน้าที่ฝ่ายการเงิน 100 คนของบริษัทจดทะเบียน โดยใช้หัวเรื่องว่า “รายงานจาก BlackRock นำเสนอกลยุทธ์เพิ่มทุนเป็นสองเท่าภายใน 30 วัน” มีผู้คลิก 74 คน 52 คนกรอกข้อมูลส่วนตัวในหน้าเว็บปลอม และ 46 คนมอบสิทธิ์เข้าถึงบัญชีอีเมลของบริษัทอย่างเต็มรูปแบบ

สถิตินี้ไม่ได้แสดงให้เห็นเพียงแค่ปัญหาทางเทคนิค แต่เป็นปรากฏการณ์ของมนุษย์ นั่นคือ ความโลภอย่างไม่ลืมหูลืมตา และเมื่อมันปรากฏขึ้นในระดับสูงสุดขององค์กร ความเสี่ยงก็จะแพร่กระจายไปทั่วทั้งองค์กร

เพื่อลดภัยคุกคามประเภทนี้ จำเป็นอย่างยิ่งที่จะต้องดำเนินนโยบายที่นอกเหนือไปจากแคมเปญสร้างความตระหนักรู้แบบดั้งเดิม กลยุทธ์บางประการได้แก่:

- I. **การจำลองแคมเปญฟิชซึ่งโดยใช้เหยื่อล่อทางการเงิน: การสัญญาเรื่องโบนัส การลงทุน และรางวัลสำหรับผลงานที่ดี**
- II. **การวิเคราะห์พฤติกรรมโดยพิจารณาจากพฤติกรรมที่น่าสงสัยในการเกี่ยวข้องกับเอกสารการลงทุนที่ไม่ได้รับอนุญาต**
- III. **การบูรณาการเครื่องมือ เช่น dnstwist, PhishTank, OpenPhish และ urlscan.io เพื่อตรวจสอบเว็บไซต์ปลอมที่เลียนแบบหน้าเพจแพลตฟอร์มการลงทุนและธนาคาร**
- IV. **สร้างตัวกรองแบบปรับเปลี่ยนได้โดยใช้การเรียนรู้ของเครื่องจักรเพื่อตรวจจับความพยายามฉ้อโกงโดยพิจารณาจากรูปแบบทางภาษาของความโลภ**

ในมิติทางวัฒนธรรม องค์การควรทบทวนวิธีสื่อสารเรื่อง “**ระบบคุณธรรมที่ต้องมาก่อนเสมอ**” สภาพแวดล้อมที่ยกย่องรางวัลและการแข่งขันอย่างก้าวร้าวเกินไป ย่อมสร้างเงื่อนไขที่เอื้อต่อภาพลวงตาของโอกาสที่พลาดไม่ได้

ความโลภก็เหมือนความพึงพอใจ คือไม่เคยอิ่มตัว ความสำเร็จแต่ละครั้งเปิดประตูสู่ความทะเยอทะยานครั้งใหม่ ดังที่นักปรัชญาชาวเยอรมันเตือนไว้ว่า:

"เราใช้ชีวิตอยู่ในวงจรที่ไม่สิ้นสุดระหว่างความปรารถนาที่จะครอบครองและความเบื่อหน่ายหลังจากได้มาแล้ว"

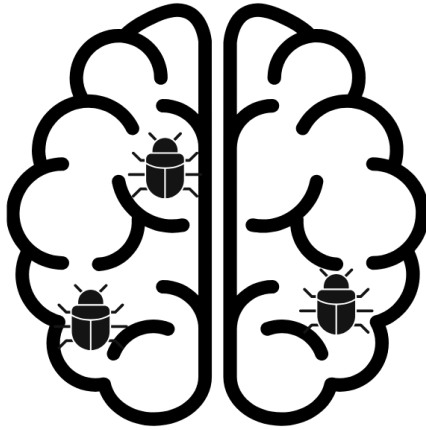
อาเธอร์ โชเพนฮาวเออร์

กลไกนี้เองที่ผู้โจมตีใช้เป็นพื้นฐานทางอารมณ์ในการบงการ

ไม่มีบริษัทใดปลอดภัย ไม่มีใครเป็นอิสระ ความแตกต่างระหว่างความปลอดภัยและการถูกรบกวน ในกรณีนี้ อยู่ที่ความสามารถในการตระหนักว่าสิ่งที่ดูดีเกินจริงมักจะไม่เป็นความจริงเสมอ และเมื่อสัญญาณในการสะสมทรัพย์สินมีน้ำหนักมากกว่าตรรกะในการประเมิน ช่องโหว่ก็ถูกใช้ประโยชน์ไปแล้วก่อนที่จะมีการคลิกละเมิดด้วยซ้ำ

บทที่ 5

ซีโรเดย์ของจิตใจมนุษย์



คำว่า “**ช่องโหว่ซีโรเดย์**” เป็นที่คุ้นเคยสำหรับผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ หมายถึงช่องโหว่ที่ผู้พัฒนาหรือผู้จำหน่ายยังไม่ทราบ จึงยังไม่มีแพตช์ และอาจถูกใช้ประโยชน์อย่างเจียบ ๆ จนสร้างความเสียหายร้ายแรง โดยทั่วไป ช่องโหว่ซีโรเดย์ที่มีมูลค่าสูงในตลาดมืดคือช่องโหว่ที่ทำให้เรียกใช้โค้ดจากระยะไกล ยกระดับสิทธิ์ หรือคงการเข้าถึงระบบโดยไม่ถูกตรวจพบ แต่มีซีโรเดย์อีกประเภทหนึ่งที่ไม่อยู่ในระบบปฏิบัติการ เบราว์เซอร์ หรือเฟรมเวิร์ก เพราะมันอยู่ในจิตใจมนุษย์

ต่างจากข้อบกพร่องทางเทคนิค ความเปราะบางทางด้านการรับรู้ ไม่สามารถแก้ไขได้ด้วยการอัปเดตซอฟต์แวร์ มันไม่ใช่บรรทัด โค้ดที่ผิดพลาด แต่เป็นภาวะทางระบบประสาท: ความอ่อนแอต่อการถูกชักจูง ช่องโหว่ที่มองไม่เห็นนี้แสดงออกมาในรูปแบบของ อคติทางความคิด แรงกระตุ้นทางอารมณ์ และรูปแบบพฤติกรรม ที่ถูกหล่อหลอมมาตลอดวิวัฒนาการของมนุษย์ และผู้โจมตีที่ เข้าใจพฤติกรรมของมนุษย์ได้ดีพอๆ กับที่เข้าใจเครือข่ายและโพรโตคอลก็สามารถใช้ประโยชน์จากช่องโหว่นี้ได้อย่างมาก

รูปแบบการใช้ประโยชน์ทางอารมณ์ที่สำคัญในหมวดนี้คือ **ศรัทธา ความพึงพอใจ และความโลภ** แต่พลังที่แท้จริงของซีโรเดย์มนุษย์เกิดจากการผสมผสานสิ่งเหล่านี้เข้ากับบริบท อีเมลทางศาสนาอาจถูกมองข้ามในวันปกติ แต่ได้ผลอย่างยิ่งในช่วงความไม่มั่นคงทางสังคม ลิงก์เชิงการมณเอาจถูกละเลยระหว่างเวลาทำงาน แต่ดึงดูดอย่างมากในยามที่อยู่ลำพัง ส่วนข้อเสนอทางการเงินอาจดูน่าสงสัยในช่วงเศรษฐกิจฝืดเคือง แต่กลับน่าเชื่อถือขึ้นท่ามกลางวิกฤต

การใช้ประโยชน์จากตัวกระตุ้นทางอารมณ์จึงเป็นการโจมตี ที่ขึ้นกับบริบทและปรับเฉพาะบุคคล ผู้โจมตีสมัยใหม่ใช้ข่าวกรองจากแหล่งข้อมูลเปิด (OSINT) เพื่อทำความเข้าใจเป้าหมายอย่างลึกซึ้งก่อนส่งเหยื่อล่อ โดยวิเคราะห์เครือข่ายสังคม ความคิดเห็นสาธารณะ รายชื่ออีเมลรั่วไหล ความชอบที่เปิดเผย และรูปแบบการมีส่วนร่วม เพื่อสร้างโปรไฟล์ทาง

จิตวิทยา การทำเช่นนี้เรียกว่า “การสร้างโปรไฟล์ทางอารมณ์” และช่วยให้ข้อความพีชชิงตรงกับความเชื่อ ความปรารถนา และ จุดอ่อนของเหยื่ออย่างแม่นยำ

ในการทดสอบหนึ่งของบริษัทความมั่นคงปลอดภัยที่เชี่ยวชาญด้านวิศวกรรมสังคม ทีมงานสร้างอีเมลพีชชิงจากการวิเคราะห์ข้อมูลพนักงานล่องหน้า โดยใช้เครื่องมือสแกนเครือข่ายสังคม ฟอรัม และข้อมูลสาธารณะ เป้าหมายรายหนึ่งเป็นพ่อของลูกสามคนและมีส่วนร่วมในกลุ่มศาสนาท้องถิ่น เขาได้รับอีเมลหัวเรื่อง “คำอธิษฐานเร่งด่วนเพื่อเด็กป่วย — โปรดร่วมแบ่งปัน” ลิงก์นำไปยังหน้าเว็บที่เหมือนเว็บไซต์ทางการขององค์กร พร้อมแบบฟอร์ม “ยืนยันการเข้าร่วม” เมื่อกรอกแบบฟอร์ม ผู้รับก็มอบข้อมูลประจำตัวให้ผู้โจมตี แคมเปญมีอัตราสำเร็จ 78% และยุติลงหลังดำเนินการเพียงเจ็ดนาที

การจำลองนี้เผยให้เห็นสิ่งที่ผู้เชี่ยวชาญหลายคนรู้กันอยู่แล้ว: จุดอ่อนที่สุดในด้านความปลอดภัยไม่ใช่เรื่องทางเทคนิค แต่เป็นเรื่องอารมณ์ และเมื่ออารมณ์ผสมกับจังหวะเวลา บริบท และความเป็นส่วนตัว แม้แต่ผู้เชี่ยวชาญที่ได้รับการฝึกฝนมาอย่างดีที่สุดก็ไม่สามารถหลีกเลี่ยงได้

นอกจากนี้ยังมีปัจจัยที่ทำให้สถานการณ์เลวร้ายลงไปอีก ระบบการศึกษาและองค์กรสอนให้ผู้ใช้ระบุนภัยคุกคามทางเทคนิค เช่น นามสกุลไฟล์ URL ที่น่าสงสัย และข้อผิดพลาดทางไวยากรณ์ แต่มีน้อยคนนักที่รู้วิธีระบุนภัยคุกคามทางอารมณ์ ไม่มีใครได้รับการฝึกฝนให้รู้จักสังเกตเมื่อตนเองกำลังถูกบงการทางจิตวิทยา

การขาดการเตรียมพร้อมนี้ทำให้พนักงานแต่ละคนกลายเป็นพาหะแฝง

การป้องกันจุดอ่อนสำคัญของจิตใจมนุษย์เริ่มต้นด้วยการตระหนักถึงความเปราะบางของตนเอง การตระหนักถึงความอ่อนแอของเราเป็นขั้นตอนแรกในการลดความเสี่ยง องค์กรจำเป็นต้องก้าวข้ามการฝึกอบรมแบบเดิมๆ และลงทุนในการให้ความรู้ด้านอารมณ์ จิตวิทยาประยุกต์ใช้กับความปลอดภัย และการสร้างวัฒนธรรมที่ส่งเสริมการคิดอย่างมีวิจารณญาณ

ตัวอย่างแนวทางปฏิบัติที่เป็นรูปธรรม ได้แก่:

- i. **การจัดทำแผนที่โพรไฟล์พฤติกรรมด้วยเครื่องมือวิเคราะห์เชิงคาดการณ์**
- ii. **การจำลองอย่างต่อเนื่องโดยใช้บริบทและสถานการณ์ที่มีแรงกระตุ้นทางอารมณ์**
- iii. **การฝึกอบรมให้รู้เท่าทันการบงการ โดยเน้นอคติทางการรับรู้**
- iv. **การบูรณาการนักจิตวิทยาและนักวิทยาศาสตร์พฤติกรรมเข้ากับทีมสร้างความตระหนักรู้**

จิตใจมนุษย์เป็นระบบซับซ้อน และเช่นเดียวกับระบบอื่น ๆ ย่อมมีข้อบกพร่อง สิ่งที่แตกต่างคือ ข้อบกพร่องเหล่านี้มองไม่เห็นด้วยเครื่องสแกน คาดการณ์ไม่ได้ด้วย SIEM และมักถูกปฏิเสธโดยตัวเหยื่อเอง นี่คือเหตุผลที่ซีโรเดย์ประเภทนี้อันตรายที่สุด

**"จิตวิญญาณของมนุษย์นั้นแข็งแกร่งกว่าสิ่งใดๆ
ยกเว้นความปรารถนา ซึ่งมันไม่เข้าใจ"**

นโปเลียน โบนาปาร์ต

บทที่ 6

**กายวิภาคของการถูกเจาะระบบทางอารมณ์
จากเหยื่อล่อสู่การถูกเจาะระบบ**

ประสิทธิผลของการโจมตีด้วยวิศวกรรมสังคมไม่ได้ขึ้นอยู่กับคุณภาพทางเทคนิคของกลลวงเพียงอย่างเดียว แต่ขึ้นอยู่กับวิธีดำเนินการตั้งแต่ต้นจนจบ เช่นเดียวกับการโจมตีดิจิทัลแบบดั้งเดิมที่ดำเนินเป็นลำดับ ตั้งแต่การสำรวจเป้าหมาย การใช้ประโยชน์ การเข้าถึง ไปจนถึงการคงอยู่ การโจมตีทางอารมณ์ก็มีโครงสร้างเชิงตรรกะเช่นกัน ความแตกต่างอยู่ที่เครื่องมือ ซึ่งแทนที่จะเป็นแพ็กเก็ตเครือข่ายหรือโค้ดที่เป็นอันตราย กลับเป็น

เรื่องเล่า ตัวกระตุ้นทางจิตวิทยา และภาษาที่ออกแบบมาอย่างพิถีพิถัน

บทนี้จะนำเสนอโครงสร้างโดยละเอียดของการโจมตีทางอารมณ์ โดยวิเคราะห์แต่ละขั้นตอนจากตัวอย่างในโลกแห่งความเป็นจริง และโครงสร้างทางเทคนิคและพฤติกรรม เป้าหมายคือการแสดงให้เห็นว่าการบิดเบือนความคิดของมนุษย์สามารถจัดระบบและทำซ้ำได้อย่างแม่นยำ คล้ายกับการพัฒนาแคมเปญมัลแวร์

การสำรวจเป้าหมาย

OSINT ทางอารมณ์

การโจมตีทุกครั้งเริ่มต้นด้วยข้อมูล ในกรณีของการโจมตีทางสังคมโดยใช้อารมณ์ ข้อมูลนี้ไม่ได้จำกัดอยู่แค่โครงสร้างพื้นฐานของเครือข่ายหรือระบบที่ใช้งานอยู่เท่านั้น แต่ยังมุ่งเน้นไปที่พฤติกรรมของเหยื่อด้วย เครือข่ายสังคม ความคิดเห็นสาธารณะ โปรไฟล์บนแพลตฟอร์มระดับมืออาชีพ พฤติกรรมการบริโภค และประวัติการมีส่วนร่วม ล้วนเป็นฐานข้อมูลที่ครบถ้วนสำหรับผู้โจมตี ด้วยข้อมูลเหล่านี้ พวกเขาสามารถอนุมานความเชื่อทางศาสนา รสนิยมทางเพศ สภาพทางการเงิน ความผูกพันทางอารมณ์ และแม้กระทั่งช่วงเวลาที่ย่อนแอที่สุด เช่น ความเศร้าโศกหรือการตกงานเมื่อเร็วๆ นี้

ในปี 2019 เกิดการโจมตีผู้บริหารฝ่ายทรัพยากรบุคคลของบริษัทข้ามชาติแห่งหนึ่ง โดยใช้ประโยชน์จากโพสต์สาธารณะที่เธอพูดถึงการเสียชีวิตของสมาชิกในครอบครัวไม่กี่วันต่อมา เธอได้รับอีเมลจากเครือข่ายให้กำลังใจทางอารมณ์ที่อ้างว่าเป็นของจริง ข้อความนั้นมีความอ่อนไหวอย่างแท้จริง และลิงก์ในอีเมลนำไปสู่หน้าลงทะเบียนปลอมที่ต้องล็อกอินด้วยที่อยู่อีเมลของบริษัท การรับรู้ทางอารมณ์นั้นถูกต้องแม่นยำ

เครื่องมือ เช่น Maltego, SpiderFoot และ FOCA รวมถึงโมดูลเก็บรวบรวมข้อมูลขั้นสูงที่เขียนด้วย Python ถูกใช้อย่างแพร่หลายในขั้นตอนนี้ เครื่องมือเหล่านี้ช่วยเชื่อมโยงข้อมูลสาธารณะ สร้างแฟ้มข้อมูล และระบุตัวกระตุ่นทางอารมณ์ที่เหมาะสมจะใช้เป็นจุดเริ่มต้น

การเตรียมเรื่องเล่า

การสร้างเหยื่อล่อ

เมื่อได้ข้อมูลเกี่ยวกับลักษณะทางอารมณ์ของเป้าหมายแล้ว ผู้โจมตีจะเริ่มวางโครงสร้างข้อความ โดยการสร้างข้อความนี้เป็นไปตามหลักการของจิตวิทยาการโน้มน้าวใจ คำต่างๆ เช่น ความขาดแคลน ความเร่งด่วน อำนาจ การตอบแทน และหลักฐานทางสังคม จะถูกนำมาใช้ในเนื้อหาเพื่อลดการคิดวิเคราะห์และกระตุ่นให้เกิดการกระทำ

ภาษาเป็นกุญแจสำคัญ อีเมลที่เขียนโดยจงใจให้มีคำผิตนั้นพบเห็นได้น้อยลงเรื่อยๆ ในปัจจุบัน อาชญากรลงทุนในการเขียนข้อความโฆษณาอย่างมืออาชีพ ข้อความสั้นๆ ที่เป็นกลาง ซึ่งสร้างผลกระทบสูงสุดโดยมีการต่อต้านน้อยที่สุด เป้าหมายคือการสร้างประสบการณ์การอ่านที่รวดเร็วและกระตุ่นอารมณ์ ซึ่งสามารถนำไปสู่การตัดสินใจโดยอัตโนมัติ

ตัวอย่าง: "ท่านได้รับการคัดเลือกจากบรรดาสมาชิกผู้ศรัทธาที่สุดในประชาคมของเรา โปรดคลิกด้านล่างเพื่อยืนยันการเข้าร่วมการประชุมพิเศษกับผู้นำทางจิตวิญญาณ" เนื้อหาในย่อหน้าเดียวนี้ สื่อถึงความศรัทธา สถานะ และความกลัวที่จะพลาดโอกาสอันพิเศษ

การดำเนินการ

การส่งเหยื่อล่อและการโต้ตอบเบื้องต้น

เมื่อสร้างเหยื่อล่อแล้ว ก็จะถูกส่งต่อไปยังอีเมล ข้อความส่วนตัวบนโซเชียลมีเดีย แอปพลิเคชันส่งข้อความ หรือแม้กระทั่งทางโทรศัพท์ เป้าหมายไม่ใช่แค่การคลิก แต่เป็นการสร้างความผูกพันทางอารมณ์ แคมเปญที่ซับซ้อนกว่านั้นมักจะมีการสนทนาเบื้องต้น ตามด้วยการกระตุ้นให้ดำเนินการ วิธีนี้พบได้ทั่วไปในกลโกงความรัก กลโกงการกุศล และการหลอกลวงทางการเงิน

หน้า Landing Page ได้รับการออกแบบด้านรูปลักษณะอย่างพิถีพิถันเช่นกัน โดยมักเลียนแบบแพลตฟอร์มจริงอย่างแนบเนียน เฟรมเวิร์ก เช่น **SET (Social-Engineer Toolkit)**, **Evilginx2** และ **Modlishka** สามารถดักจับคุกกี้ โทเค็นเซสชัน

และข้อมูลประจำตัวแบบเรียลไทม์ได้ แม้เป้าหมายจะใช้นำการยืนยันตัวตนแบบหลายปัจจัย (MFA)

การถูกเจาะระบบ

การส่งมอบข้อมูลหรือการดำเนินการ

การถูกเจาะระบบอาจเกิดได้หลายรูปแบบ เช่น การส่งมอบข้อมูลประจำตัว การติดตั้งมัลแวร์ การโอนเงิน การส่งเอกสาร หรือการเปิดให้เข้าถึงจากระยะไกล ในทุกกรณี ความสำเร็จขึ้นอยู่กับระดับการบงการทางอารมณ์ ยิ่งเหยื่อมีส่วนร่วมมาก ความไว้วางใจก็ยิ่งสูง และการยอมทำตามก็ยิ่งมากขึ้น

การโจมตีทางสังคมที่ประสบความสำเร็จไม่ได้เพียงแครวบรวมข้อมูลเท่านั้น แต่ยังปลุกฝังเรื่องราวต่างๆ ด้วย เหยื่อหลายคนแม้จะรู้ว่าตกเป็นเหยื่อแล้ว ก็ยังยากที่จะยอมรับความผิดพลาดของตนเอง เพราะเรื่องราวเหล่านั้นได้สร้างความรู้สึกร่วมทางอารมณ์อย่างมาก ความต้านทานนี้ขัดขวางการตอบสนองต่อเหตุการณ์อย่างรวดเร็ว และกระตุ้นให้การโจมตีดำเนินต่อไป

หลังการถูกเจาะระบบ

การคงอยู่ทางจิตวิทยาและทางเทคนิค

หลังจากที่ข้อมูลถูกบุกรุกในเบื้องต้นแล้ว ผู้โจมตีสามารถใช้ประโยชน์จากความผูกพันทางอารมณ์ต่อไปได้ ตัวอย่างเช่น ในกรณีการหลอกลวงความสัมพันธ์ ผู้ร้ายจะยังคงสนทนาต่อไป ขอข้อมูลเพิ่มเติม และใช้การข่มขู่ทางอารมณ์เพื่อเข้าถึงข้อมูลเพิ่มเติม ในบริบทขององค์กร การใช้บัญชีอีเมลที่ถูกบุกรุกเพื่อส่งข้อความภายในและบุกรุกสมาชิกในทีมคนอื่นๆ โดยใช้ประโยชน์จากความไว้วางใจระหว่างเพื่อนร่วมงานนั้นเป็นเรื่องปกติ

การคงอยู่ของมัลแวร์ยังเกิดขึ้นในเชิงเทคนิคด้วย มัลแวร์ขนาดเล็ก เช่น โปรแกรมขโมยข้อมูลและโปรแกรมดักจับการกดแป้นพิมพ์ ถูกนำมาใช้เพื่อรักษาการเข้าถึง ตรวจสอบพฤติกรรม และเตรียมการโจมตีใหม่ ๆ ซึ่งในปัจจุบันมีความซับซ้อนมากขึ้น

บทสรุป

การวิเคราะห์เจาะลึกการโจมตีทางอารมณ์เผยให้เห็นว่าเรากำลังเผชิญกับรูปแบบการโจมตีที่ปรับตัวได้สูงมาก มันไม่ได้อาศัยช่องโหว่ในซอฟต์แวร์ แต่กลับอาศัยช่องโหว่ในตัวบุคคล มันเจียบเจียบ ติดตามได้ยาก และมักไม่เป็นอันตรายในสายตาของระบบรักษาความปลอดภัยแบบดั้งเดิม

การทำความเข้าใจแต่ละขั้นตอนของกระบวนการนี้คือก้าวแรกในการรับมือ การป้องกันต้องไปไกลกว่ามาตรการทางเทคนิค โดยลงทุนในความฉลาดทางอารมณ์ การคิดเชิงวิพากษ์ การวิเคราะห์พฤติกรรม และเหนือสิ่งอื่นใด คือความสามารถในการยอมรับว่า **ทุกคนไม่ว่าจะมีตำแหน่งหรือภูมิหลังอย่างไร ล้วนมีจุดอ่อนภายในที่อาจถูกใช้ประโยชน์ได้**

บทที่ 7

การจำลองที่สมจริงด้วย GoPhish และแคมเปญที่ใช้ แรงกระตุ้นทางอารมณ์

ทฤษฎีมีความสำคัญ แต่ความมั่นคงปลอดภัยจะแข็งแกร่งขึ้นได้เมื่อฝึกปฏิบัติ ในบทนี้ คุณจะเรียนรู้ที่ละขั้นตอนถึงวิธีสร้างแคมเปญฟิชซิงที่ใช้แรงกระตุ้นทางอารมณ์อย่างสมจริง ด้วยเครื่องมือโอเพนซอร์สที่มีประสิทธิภาพอย่าง GoPhish เครื่องมือนี้ช่วยจำลองการโจมตีฟิชซิงในสภาพแวดล้อมที่ควบคุมได้ เก็บตัวชี้วัดอย่างแม่นยำ และเสริมความพร้อมของทีมต่อภัยคุกคามจริง

การจำลองภายในไม่ได้มีไว้แค่ "ทดสอบการคลิก" เท่านั้น แต่มีไว้เพื่อทำความเข้าใจว่าผู้คนคลิกอย่างไร ทำไม และเมื่อไหร่ และยิ่งไปกว่านั้น ยังมีไว้เพื่อปรับเปลี่ยนวัฒนธรรม กระบวนการ และเทคโนโลยีอีกด้วย

ด้านล่างนี้ คุณจะพบกับคู่มือฉบับสมบูรณ์ ตั้งแต่การติดตั้งไปจนถึงรายงานฉบับสุดท้าย โดยเน้นที่แคมเปญที่ใช้ตัวกระตุ้นทางอารมณ์ เช่น ศรีทธา ความสุข และความโลภ

บทนำสู่ GoPhish

GoPhish เป็นแพลตฟอร์มโอเพนซอร์สสำหรับจำลองฟิชชิง ใช้งานได้ฟรีและพัฒนาด้วยภาษา Go มีเว็บอินเทอร์เฟซที่เรียบง่าย ใช้งานสะดวก และทรงพลัง สำหรับสร้างแคมเปญเฉพาะจัดการผู้ใช้ และดูผลลัพธ์แบบเรียลไทม์

ข้อกำหนด:

- I. ระบบปฏิบัติการ: Windows, Linux หรือ macOS
- II. การเชื่อมต่ออินเทอร์เน็ตสำหรับส่งอีเมล
- III. บัญชี SMTP (จริงหรือสำหรับทดสอบ ขึ้นอยู่กับรูปแบบการจำลอง)
- IV. สิทธิ์ระดับผู้ดูแลระบบ (หากจำเป็นต้องเปิดพอร์ต)

ดาวน์โหลด:

- I. เยี่ยมชมเว็บไซต์อย่างเป็นทางการได้ที่:
<https://getgophish.com>
- II. คลิก “Download Latest Release”
- III. เลือกระบบปฏิบัติการที่เหมาะสม
- IV. แดกไฟล์ไปยังโฟลเดอร์ที่คุณเลือก

การติดตั้งและการเรียกใช้งาน

บน Windows:

- I. แยกไฟล์ .zip ออกมา
- II. เปิดหน้าต่าง Command Prompt ในโฟลเดอร์ที่ไฟล์ executable อยู่
- III. เรียกใช้ไฟล์ gophish.exe

บน Linux/macOS:

- I. แยกไฟล์ .tar.gz ออกมา
- II. ให้สิทธิ์ในการเรียกใช้งาน:
- III. `chmod +x gophish`
- IV. เรียกใช้คำสั่ง `./gophish`
- V. ส่วนติดต่อผู้ดูแลระบบ: <https://localhost:3333>
- VI. เซิร์ฟเวอร์หน้า Landing Page: <http://localhost:80>
(หรือที่อยู่อื่นตามการกำหนดค่า)
- VII. ชื่อผู้ใช้เริ่มต้นคือ admin ส่วนรหัสผ่านชั่วคราวจะถูกสร้างขึ้นเมื่อเปิดใช้งานครั้งแรกและแสดงในคอนโซลหรือบันทึกของ GoPhish

ควรเปลี่ยนรหัสผ่านชั่วคราวทันทีหลังเข้าสู่ระบบครั้งแรก

การกำหนดค่าเริ่มต้น SMTP (เซิร์ฟเวอร์ส่งอีเมล)

คุณสามารถใช้:

- I. เซิร์ฟเวอร์ SMTP ภายในบริษัท (เหมาะสำหรับการทดสอบภายใน)
- II. เซิร์ฟเวอร์ทดสอบ เช่น Mailtrap (สำหรับสภาพแวดล้อมที่ควบคุมได้)
- III. บริการอีเมลที่ถูกต้อง เช่น Gmail หรือ SendGrid (ใช้เฉพาะเมื่อได้รับอนุญาต)

เทมเพลตอีเมล

สร้างอีเมลด้วยภาษาที่สื่ออารมณ์:

- I. ศรัทธา: "ข้อความด่วนจากกลุ่มทางจิตวิญญาณของคุณ"
- II. ความสุข: "มีวิดีโอส่วนตัวให้ชมแล้ว - ดูเลยตอนนี้"
- III. ความโลภ: "คุณได้รับการคัดเลือกเบื้องต้นเพื่อรับโบนัส 3,000 เรียลบราซิล"

เคล็ดลับทางเทคนิค

- I. ใช้ตัวแปร เช่น {{.FirstName}} เพื่อปรับแต่งข้อความ
- II. เพิ่มลิงก์ไปยังหน้า Landing Page ที่เตรียมไว้
- III. เปิดใช้งานการติดตามการคลิกและการเก็บข้อมูลประจำตัวสำหรับทดสอบเมื่อจำเป็น โดยต้องดำเนินการเฉพาะในสภาพแวดล้อมที่ควบคุมและได้รับอนุญาตเท่านั้น

ขั้นตอนการสร้างแคมเปญที่ละขั้นตอน

- I. ล็อกอินเข้าสู่แดชบอร์ด
- II. ไปที่ Sending Profiles
 - I. ตั้งค่าอีเมลและเซิร์ฟเวอร์ SMTP ของคุณ
- II. ไปที่ Email Templates
- III. สร้างหรือแก้ไขเทมเพลตของคุณ
- IV. แทรกลิงก์ทดสอบด้วยตัวแปร {{.URL}}
- V. ไปที่ Landing Pages
- VI. สร้างหรือนำเข้าหน้า Landing Page และกำหนดค่าการเก็บข้อมูลทดสอบตามวัตถุประสงค์ของการจำลองที่ได้รับอนุญาต
- VII. เปิดใช้งานการรวบรวมข้อมูลปลอมหากคุณต้องการติดตามการส่งข้อมูล

- VIII. ไปที่ Users & Groups
- IX. นำเข้าผู้ใช้ (ชื่อ + อีเมล)
- X. สามารถอยู่ในรูปแบบ CSV ได้
- XI. ไปที่ Campaigns
- XII. ตั้งชื่อให้กับแคมเปญนี้
- XIII. เลือกกลุ่มผู้ใช้
- XIV. เลือกเทมเพลตอีเมล
- XV. เลือกโปรไฟล์ผู้ส่ง
- XVI. เริ่มแคมเปญ

การดำเนินการและการติดตามตรวจสอบ

ทันทีที่แคมเปญเริ่มต้น คุณจะเห็นผลลัพธ์แบบเรียลไทม์:

- 1) มีการส่งอีเมลไปกี่ฉบับ?
- 2) มีการเปิดไปกี่ครั้ง?
- 3) มีคนคลิกลิงก์ไปกี่ครั้ง?
- 4) มีผู้กรอกข้อมูลประจำตัวสำหรับทดสอบกี่ราย

คุณสามารถส่งออกข้อมูลแคมเปญเป็นไฟล์ CSV หรือ JSON เพื่อนำไปวิเคราะห์เพิ่มเติมได้

การนำเสนอรายงานฉบับสุดท้าย

เพื่อบันทึกและนำเสนอผลลัพธ์ของการจำลอง ให้ปฏิบัติตาม
โครงสร้างดังต่อไปนี้:

บทสรุปสำหรับผู้บริหาร

- ⇒ วัตถุประสงค์ของการจำลอง
- ⇒ ประเภทของวิศวกรรมอาณัติที่ใช้

ระเบียบวิธีวิจัย

- ⇒ เครื่องมือที่ใช้ (GoPhish)
- ⇒ แรงกระตุ้นทางอาณัติที่ทดสอบ
- ⇒ จำนวนผู้ใช้ที่ทดสอบ

ผลลัพธ์

- ⇒ อัตราการเปิดอีเมล
- ⇒ อัตราการคลิกผ่าน
- ⇒ จำนวนผู้กรอกข้อมูลประจำตัวสำหรับทดสอบ
- ⇒ เวลาตอบสนองเฉลี่ย

การวิเคราะห์

- ⇒ ตัวกระตุ้นใดมีประสิทธิภาพมากที่สุด?
- ⇒ มีความสัมพันธ์กับตำแหน่งงาน พื้นที่ หรือลักษณะงานหรือไม่?

คำแนะนำ

- ⇒ มาตรการแก้ไข
- ⇒ ความจำเป็นในการฝึกอบรมเฉพาะด้าน

⇒ การปรับแต่งการป้องกันทางเทคนิค

บทสรุป

การจำลองที่ใช้แรงกระตุ้นทางอารมณ์ไม่ใช่เพียงการทดสอบทางเทคนิค แต่เป็นการฝึกพฤติกรรม การใช้เครื่องมืออย่าง GoPhish อย่างรับผิดชอบช่วยให้องค์กรสร้างภูมิคุ้มกันที่แท้จริงต่อภัยคุกคามสมัยใหม่ ทุกการคลิกคือบทเรียน และทุกตัวชี้วัดคือโอกาสในการพัฒนา

บทที่ 8

รายการตรวจสอบการป้องกันทางอารรมณ์และทาง เทคนิค

การป้องกันการโจมตีทางไซเบอร์ที่ใช้วิศวกรรมสังคมต้องอาศัยมากกว่าไฟร์วอลล์ โปรแกรมป้องกันไวรัส และนโยบายรหัสผ่าน ดังที่บทก่อนหน้านี้แสดงให้เห็น ช่องทางการโจมตีที่อันตรายที่สุดไม่ได้เป็นเรื่องทางเทคนิค แต่เกี่ยวข้องกับมนุษย์ และเมื่อจุดเริ่มต้นคืออารรมณ์ เช่น **ศรัทธา ความพึงพอใจ หรือความโลภ** การตอบสนองต้องผสานความเข้าใจทางอารรมณ์ มาตรการทางเทคนิค และการฝึกอบรมเชิงกลยุทธ์เข้าด้วยกัน

ในบทนี้ ผู้เขียนนำเสนอรายการตรวจสอบที่แบ่งตามบริบท แต่ละรายการสามารถนำไปใช้โดยตรงในการป้องกัน การตรวจจับ หรือการตอบสนองต่อเหตุการณ์

รายการตรวจสอบการป้องกันทางอารรมณ์สำหรับพนักงาน

วัตถุประสงค์:

เสริมสร้างความตระหนักรู้และความยืดหยุ่นทางอารรมณ์ของพนักงานเมื่อเผชิญแคมเปญฟิชซิงและการบงการทางจิตวิทยา

- I. () บริษัทจัดการฝึกอบรมรายเดือนหรือรายไตรมาสโดยเน้นวิศวกรรมสังคมทางอารรมณ์
- II. () การฝึกอบรมนี้ครอบคลุมหัวข้อที่ละเอียดอ่อน เช่น ศาสนา เนื้อหาทางเพศ และสัญญาทางการเงิน โดยใช้ภาษาที่เหมาะสม
- III. () พนักงานรู้วิธีระบุสิ่งที่กระตุ้นความรู้สึกเร่งด่วน ความขาดแคลน และอำนาจ
- IV. () ทีมงานสามารถรายงานข้อความน่าสงสัยได้โดยไม่ต้องกลัวการตำหนิหรือการลงโทษ
- V. () มีช่องทางที่ชัดเจนและเข้าถึงได้ง่ายสำหรับการรายงานอีเมลฟิชซิง
- VI. () พนักงานถูกทดสอบด้วยการจำลองการโจมตีแบบฟิชซิงโดยใช้ตัวกระตุ้นทางอารรมณ์เฉพาะบุคคล
- VII. () ฝ่ายทรัพยากรบุคคลหรือผู้บริหารคำนึงถึงช่วงที่พนักงานอาจเปราะบางทางอารรมณ์ เช่น การสูญเสียบุคคลสำคัญ การเลิกจ้าง หรือความขัดแย้ง ซึ่งผู้โจมตีอาจนำไปใช้ประโยชน์

- VIII. () มีเนื้อหาภายในหรือคำแนะนำเกี่ยวกับความปลอดภัยทางอาชญากรรมสำหรับการใช้งานส่วนบุคคล
- IX. () บริษัทส่งเสริมวัฒนธรรมการรับฟังอย่างตั้งใจ เพื่อลดความโดดเดี่ยวและความอ่อนไหวต่อการชักจูงจากภายนอก
- X. () พฤติกรรมทางอาชญากรรมของพนักงานที่เกี่ยวข้องกับการสื่อสารดิจิทัลจะได้รับการประเมินเป็นระยะ

รายการตรวจสอบทางเทคนิคเพื่อลดผลกระทบจากฟิชชิง ทางอารมณ์

วัตถุประสงค์:

ทำให้โครงสร้างพื้นฐานด้านความมั่นคงปลอดภัยพร้อมตรวจจับ
สกัดกั้น และตอบสนองต่อการโจมตีที่ใช้วิศวกรรมสังคม

- I. () การกรอง DNS ที่ใช้งานอยู่จะบล็อกโดเมนที่สร้างใหม่
หรือโดเมนที่มีชื่อเสียงต่ำ
- II. () บรูณาการกับแหล่งข้อมูลและเครื่องมือ เช่น
**PhishTank, OpenPhish, VirusTotal API และ
urlscan.io**
- III. () ตรวจสอบโดเมนที่มีชื่อคล้ายกันด้วย dnstwist เพื่อ
ระบุการจดทะเบียนโดเมนแบบ typosquatting
- IV. () โปรแกรมป้องกันไวรัสและ EDR ใช้การตรวจจับเชิง
พฤติกรรมและเชื่อมต่อกับข่าวกรองภัยคุกคาม
- V. () การวิเคราะห์ปริมาณการรับส่งข้อมูลขาออกเพื่อตรวจ
จับการเชื่อมต่อกับเซิร์ฟเวอร์ที่น่าสงสัยหลังจากการคลิก
- VI. () กลไกแซนด์บ็อกซ์สำหรับการวิเคราะห์เบื้องต้นของ
ไฟล์แนบและลิงก์ที่ได้รับทางอีเมล
- VII. () รวมศูนย์บันทึกเหตุการณ์ไว้ใน SIEM และตั้งค่าการ
แจ้งเตือนสำหรับคำหรือวลีที่กระตุ้นอารมณ์ เช่น
“ปาฏิหาริย์” “ด่วน” “วิดีโอส่วนตัว” และ “ทำเร็ว”

- VIII. () กำหนดค่า SPF, DKIM และ DMARC อย่างถูกต้อง และบล็อกหรือกักกันอีเมลที่ไม่ผ่านนโยบายการยืนยันแหล่งที่มา
- IX. () การแบ่งส่วนเครือข่ายพร้อมข้อจำกัดการแพร่กระจายด้านข้างหลังจากการถูกบุกรุก
- X. () การยืนยันตัวตนแบบหลายปัจจัย (MFA) เป็นสิ่งจำเป็น รวมถึงการใช้งานอีเมลและการเข้าถึงระบบภายใน แม้กระทั่งบนอุปกรณ์เคลื่อนที่

รายการตรวจสอบด้านการบริหารเชิงกลยุทธ์และวัฒนธรรมองค์กร

วัตถุประสงค์:

ผสมผสานความมั่นคงปลอดภัยทางอารมณ์และทางเทคนิคเข้ากับภาวะผู้นำ กระบวนการ และการตัดสินใจขององค์กร

- I. () ผู้นำได้รับการฝึกฝนให้เข้าใจและระบุกลยุทธ์ทางสังคมที่มุ่งเป้าไปที่ตำแหน่งผู้บริหาร
- II. () มีนโยบายที่ชัดเจนสำหรับการสื่อสารที่ปลอดภัย รวมถึงในกรณีฉุกเฉินหรือการระดมพลภายใน

- III. () ผู้บริหารทุกคนเข้ารับการจำลองสถานการณ์การโจมตีแบบสเปียร์ฟิชชิง
- IV. () องค์กรแต่งตั้งตัวแทนหรือผู้ประสานงานด้านความมั่นคงปลอดภัยในหน่วยงานที่มีความเสี่ยงสูง
- V. () มีนโยบายตอบสนองอย่างรวดเร็วเมื่อข้อมูลของทีมหรือองค์กรรั่วไหลหรือถูกเปิดเผยต่อสาธารณะ
- VI. () แผนเผชิญสร้างความตระหนักรู้จะได้รับการปรับปรุงตามเหตุการณ์จริง (เช่น การโจมตีบริษัทต่างๆ ในภาคส่วนเดียวกันเมื่อเร็วๆ นี้)
- VII. () องค์กรลงทุนในความหลากหลายทางภาษาในการฝึกอบรม (ภาพ ข้อความ การพูด) เพื่อตอบสนองโปรไฟล์การรับรู้ที่แตกต่างกัน
- VIII. () ตัวชี้วัดด้านวุฒิภาวะทางอารมณ์และความยืดหยุ่นทางพฤติกรรมถูกนำมาใช้ในรายงานความเสี่ยงของมนุษย์
- IX. () มีการจัดสรรงบประมาณสำหรับความปลอดภัยทางอารมณ์ในแผนการสร้างความรู้ประจำปี
- X. () การสื่อสารภายในช่วยเสริมสร้างความปลอดภัยให้เป็นวัฒนธรรม ไม่ใช่เป็นการลงโทษ

การป้องกันการโจมตีทางอารมณ์ไม่ใช่หน้าที่ของทีมความมั่นคงปลอดภัยเพียงฝ่ายเดียว แต่เริ่มจากพฤติกรรมของแต่ละบุคคลขยายไปสู่วัฒนธรรมองค์กร และได้รับการเสริมด้วยกระบวนการทางเทคนิคและการศึกษา รายการตรวจสอบเหล่านี้เป็นพื้นฐาน

สำหรับสร้างสถาปัตยกรรมการป้องกันที่ไม่มองข้ามปัจจัยมนุษย์
แต่ยอมรับว่าเป็นศูนย์กลางของความมั่นคงปลอดภัย

ในส่วนถัดไป เราจะรวบรวมและอธิบายคำศัพท์สำคัญด้าน
วิศวกรรมสังคมและฟิชซิงทางอารมณ์ เพื่อให้เข้าใจวิธีโจมตีและ
มาตรการป้องกันที่กล่าวถึงในหนังสือได้ตรงกัน

บทที่ 9

อภิธานศัพท์ด้านวิศวกรรมสังคมและฟิชซิงทางอารมณ์ (พร้อมคำอธิบาย)

สำหรับผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศ การใช้คำศัพท์ทางเทคนิคอย่างถูกต้องเป็นสิ่งสำคัญ เมื่อกล่าวถึงวิศวกรรมสังคมและการใช้ประโยชน์จากอารมณ์ คำบางคำมีความหมายเฉพาะและละเอียดอ่อน จนอาจทรงพลังเทียบเท่าช่องโหว่หรือเพย์โหลด อภิธานศัพท์นี้รวบรวมคำสำคัญที่สุดในหนังสือ พร้อมคำจำกัดความ บริบทการใช้งาน และผลกระทบเชิงปฏิบัติ

1. วิศวกรรมสังคม (Social Engineering)

คำจำกัดความ: ชุดเทคนิคที่ใช้ประโยชน์จากอารมณ์ จิตวิทยา และพฤติกรรม เพื่อบังการบุคคลให้เปิดเผยข้อมูลหรืออนุญาตการเข้าถึงระบบ

คำอธิบาย: เปรียบได้กับการใช้ประโยชน์จากช่องโหว่ของระบบ แต่ “เพย์โหลด” ในกรณีนี้คือเรื่องเล่าที่ผู้โจมตีสร้างขึ้น

2. ฟิชซิง (Phishing)

คำจำกัดความ: เทคนิคที่ใช้ข้อความปลอม ซึ่งมักส่งทางอีเมล เพื่อหลอกให้เหยื่อเปิดเผยข้อมูลลับหรือดำเนินการที่เป็นอันตราย

คำอธิบาย: ฟิชซิงทางอารมณ์ใช้ตัวกระตุ้น เช่น ความกลัว ศรัทธา ความพึงพอใจ หรือความโลภ เพื่อสร้างความเร่งด่วน ความไว้วางใจ หรือความเห็นอกเห็นใจ

3. สเปียร์ฟิชซิง (Spear Phishing)

คำจำกัดความ: ฟิชซิงที่ปรับแต่งอย่างมากและมุ่งเป้าไปยังบุคคลหรือกลุ่มเฉพาะ

คำอธิบาย: เมื่อใช้ร่วมกับข้อมูลทางอารมณ์ เช่น การสูญเสีย เมื่อไม่นานมานี้หรือความคาดหวังเรื่องเลื่อนตำแหน่ง การโจมตีจะยังมีประสิทธิภาพ

4. วิชชิง หรือฟิชชิงทางเสียง (Vishing / Voice Phishing)

คำจำกัดความ: ความพยายามฉ้อโกงผ่านโทรศัพท์หรือข้อความเสียง โดยผู้โจมตีแอบอ้างเป็นบุคคลหรือองค์กรที่น่าเชื่อถือ

คำอธิบาย: พบบ่อยในกลโกงฟลายสแน็บสนุนทางเทคนิค การขโมยข้อมูล และการข่มขู่ทางอารมณ์

5. เบติง หรือการใช้เหยื่อล่อ (Baiting)

คำจำกัดความ: เทคนิควิศวกรรมสังคมที่เสนอสิ่งมีค่า ไม่ว่าจะเป็นจริงหรือสมมติ เพื่อดึงดูดเหยื่อ

คำอธิบาย: ตัวอย่างเช่น การจงใจวางแฟลชไดรฟ์ USB ให้ดูเหมือนถูกลืมไว้ หรือการสัญญาว่าจะให้เนื้อหาพิเศษ

6. ฟรีเท็กซ์ติง หรือการสร้างสถานการณ์สมมติ (Pretexting)

คำจำกัดความ: เทคนิคที่ผู้โจมตีสร้างเรื่องราว บทบาท หรือตัวตนปลอม เพื่อให้ได้ข้อมูลหรือชักจูงให้เหยื่อดำเนินการ

คำอธิบาย: เป็นพื้นฐานของการโจมตีที่อาศัยอำนาจหรือความไว้วางใจ เช่น “ผมมาจากทีมไอทีและต้องรีเซ็ตข้อมูลการเข้าถึงของคุณ”

7. เพย์โหลดทางจิตวิทยา (Psychological Payload)

คำจำกัดความ: ข้อความหรือองค์ประกอบทางอารมณ์ที่ออกแบบมาให้สร้างผลกระทบทันทีและกระตุ้นปฏิกิริยาอัตโนมัติ

คำอธิบาย: ไม่ใช่ซอฟต์แวร์ แต่เป็นวลี รูปภาพ หรือหัวเรื่อง เช่น “วิดีโอส่วนตัวของคุณถูกเผยแพร่แล้ว”

8. ตัวกระตุ้นทางอารมณ์ (Emotional Trigger)

คำจำกัดความ: สิ่งเร้าที่กระตุ้นอารมณ์เฉพาะ ลดความสามารถในการวิเคราะห์อย่างมีเหตุผล และเพิ่มความหุนหันพลันแล่น

คำอธิบาย: อารมณ์สำคัญที่กล่าวถึง ได้แก่ ความกลัว ความพึงพอใจ ความหวัง ความรู้สึกผิด ความโลภ ศรัทธา และความละอาย

9. ช่องโหว่ซีโรเดย์ของมนุษย์ (Human Zero-Day)

คำจำกัดความ: ลักษณะเปราะบางทางอารมณ์หรือการรับรู้ในพฤติกรรมของบุคคลหรือกลุ่ม ซึ่งยังไม่ได้รับการตระหนักและชดเชยด้วยมาตรการป้องกัน

คำอธิบาย: ขณะที่องค์กรค้นหาช่องโหว่ CVE ในซอฟต์แวร์ จุดเข้าถึงที่แท้จริงอาจซ่อนอยู่ในอารมณ์ที่ยังไม่ได้รับการจัดการ

10. OSINT (Open-Source Intelligence หรือข่าวกรองจากแหล่งข้อมูลเปิด)

คำจำกัดความ: การรวบรวมและวิเคราะห์ข้อมูลสาธารณะเพื่อศึกษาหรือระบุเป้าหมาย

คำอธิบาย: ใช้สร้างโปรไฟล์ทางอารมณ์อย่างละเอียดจากเครือข่ายสังคม บล็อก และปฏิสัมพันธ์สาธารณะ

11. การสร้างความตระหนักรู้ (Awareness)

คำจำกัดความ: ชุดกิจกรรมด้านการศึกษาเพื่อเพิ่มความตระหนักและความสามารถในการระบุความเสี่ยงด้านความมั่นคงปลอดภัย

คำอธิบาย: ควรก้าวจากคำเตือนว่า “อย่าคลิกลิงก์” ไปสู่การทำความเข้าใจว่า “คุณกำลังถูกบงการทางอารมณ์อย่างไร”

12. แคมเปญจำลองสถานการณ์

(การจำลองฟิชซิง)

คำจำกัดความ: การทดสอบที่ควบคุมและได้รับอนุญาต ซึ่งจำลองการโจมตีฟิชซิงเพื่อวัดการตอบสนองของผู้ใช้

คำอธิบาย: เมื่อใช้หลักวิศวกรรมทางอารมณ์ จะกลายเป็นโปรแกรมฝึกพฤติกรรมที่สมบูรณ์ยิ่งขึ้น

13. ปฏิบัติงานหุ่นหล่นเล่นทางดิจิทัล

คำจำกัดความ: พฤติกรรมอัตโนมัติและไร้เหตุผลที่เกิดขึ้นเพื่อตอบสนองต่อสิ่งเร้าทางออนไลน์

คำอธิบาย: เป้าหมายของฟิชซิงทางอารมณ์ทุกรูปแบบคือการกระตุ้นปฏิภิกิริยานี้

14. การยึดติดทางจิตวิทยา

คำจำกัดความ: สภาวะที่เหยื่อยังคงเชื่อเรื่องราวที่ได้รับ แม้จะได้รับคำเตือนแล้ว

คำอธิบาย: สิ่งนี้ตอกย้ำความสำคัญของความเห็นอกเห็นใจและการสนับสนุนทางจิตใจเมื่อตอบสนองต่อเหตุการณ์

15. วัฒนธรรมความมั่นคงปลอดภัยทางอารมณ์

คำจำกัดความ: สภาพแวดล้อมขององค์กรที่ตระหนักว่าอารมณ์เป็นส่วนหนึ่งของความเสี่ยง และลงทุนในการป้องกันเชิงพฤติกรรม

คำอธิบาย: องค์กรที่พูดถึงเพียงไฟร์วอลล์และ MFA อาจกำลังปกป้องจุดที่ไม่ใช่ช่องทางโจมตีหลัก

การใช้คำศัพท์อย่างถูกต้องเป็นอาวุธในการป้องกัน การเข้าใจไม่เพียงความหมาย แต่รวมถึงผลกระทบในโลกจริง ช่วยให้ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยเชื่อมโยงมิติทางเทคนิคและมิติมนุษย์ได้รอบคอบยิ่งขึ้น อภิธานศัพท์นี้จึงไม่ใช่เพียงแหล่งอ้างอิง แต่เป็นคำเชิญให้รักษาความตื่นตัวทางอารมณ์อย่างต่อเนื่อง

ขอพระเจ้าทรงอวยพรและคุ้มครองท่าน

ผู้เขียน: Giuliano Paião