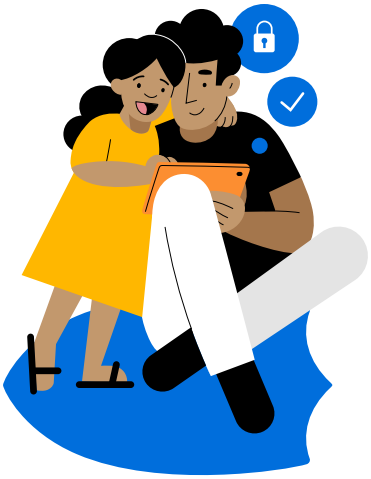


การสร้างระบบนิเวศที่น่าเชื่อถือสำหรับแอปนับล้านๆ

บทบาทสำคัญของระบบป้องกัน
ใน App Store

มิถุนายน 2021

2007

"เราพยายามทำสองสิ่งที่ต่างกันแบบสุดขั้วไปพร้อมๆ กัน นั่นคือการจัดทำแพลตฟอร์มอันล้ำสมัยและเปิดกว้างสำหรับนักพัฒนา ซึ่งในขณะเดียวกันยังปกป้องผู้ใช้ iPhone จากไวรัส มัลแวร์ การโจมตีด้านความเป็นส่วนตัว และอื่นๆ ด้วย ซึ่งไม่ใช่งานง่ายเลย"

Steve Jobs, ปี 2007[1]

2016

"ใช้พื้นที่ซื้อขายแอปพลิเคชันอย่างเป็นทางการเท่านั้น ผู้ใช้ไม่ควร [ดาวน์โหลดแอปพลิเคชัน] จากแหล่งอื่น ทั้งนี้ก็เพื่อลดความเสี่ยงจากการติดตั้งแอปพลิเคชันอันตรายนั่นเอง และผู้ใช้ก็ไม่ควรติดตั้งแอปพลิเคชันด้วยวิธีไซด์โหลด ถ้าไม่ได้มาจากแหล่งที่มีการรับรองและน่าเชื่อถือ"

หน่วยงานด้านความปลอดภัยไซเบอร์แห่งสหภาพยุโรป (ENISA), ปี 2016[2]

2017

"เราพบว่าแนวทางปฏิบัติที่ดีที่สุดที่จะช่วยลดความรุนแรงของภัยคุกคามจากแอปที่สุ่มเสี่ยงนั้นมีความเกี่ยวข้องโดยตรงกับแอปที่เป็นอันตรายและรุกล้ำความเป็นส่วนตัว นอกจากนี้ สิ่งที่ผู้ใช้ควรหลีกเลี่ยง (และองค์กรควรห้ามไม่ให้กระทำบนอุปกรณ์ของตน) คือการติดตั้งแอปด้วยวิธีไซด์โหลด และการใช้แอปสโตร์ต่างๆ ที่ไม่ได้รับอนุญาต"

รายงานจากกระทรวงความมั่นคงแห่งมาตุภูมิของสหรัฐอเมริกา, ปี 2017[3]

วันนี้โทรศัพท์ของเราไม่ใช่แค่โทรศัพท์ หากแต่เป็นสิ่งที่จัดเก็บข้อมูลบางส่วนที่สำคัญที่สุดของเรา ทั้งชีวิตส่วนตัวและการทำงาน เราพกโทรศัพท์ติดตัวไปทุกที่ และเราใช้โทรศัพท์เพื่อโทรติดต่อและส่งข้อความถึงคนที่เรารัก ถ่ายและเก็บรูปของลูกๆ ดูเส้นทางเมื่อเราหลงทาง นับจำนวนก้าว และโอนเงินให้เพื่อน เรียกว่าโทรศัพท์อยู่กับเราทั้งในยามสุขและในยามฉุกเฉิน

เราออกแบบ iPhone โดยคำนึงถึงเรื่องนี้เป็นสำคัญ และเรายังสร้าง App Store เพื่อให้นักพัฒนาทั่วโลกมีที่สำหรับสร้างแอปอันล้ำสมัยที่สามารถเข้าถึงชุมชนผู้ใช้งานกว่าหนึ่งพันล้านคนทั่วโลกที่กำลังเพิ่มจำนวนและเติบโตขึ้นเรื่อยๆ โดยในตอนนี้มีแอปเกือบ 2 ล้านแอปให้ผู้ใช้ดาวน์โหลดใน App Store และยังมีเพิ่มเรื่อยๆ อีกหลายพันแอปทุกสัปดาห์ ซึ่งเมื่อดูจากขนาดที่ใหญ่โตมโหฬารของแพลตฟอร์ม App Store แล้ว การทำให้ iPhone มีความปลอดภัยในทุกส่วนจึงเป็นเรื่องที่เราให้ความสำคัญสูงสุดมาตั้งแต่แรกเริ่ม และนักวิจัยด้านความปลอดภัยต่างก็เห็นตรงกันว่า iPhone เป็นอุปกรณ์พกพาที่ปลอดภัยที่สุด ซึ่งช่วยให้ผู้ใช้ของเราสามารถเชื่อใจและเก็บข้อมูลสำคัญที่สุดไว้ในอุปกรณ์ของตนเองได้ นอกจากนี้ เรายังใส่ระบบป้องกันเพื่อความปลอดภัยระดับชั้นแนวหน้าของอุตสาหกรรมรวมเป็นส่วนหนึ่งในอุปกรณ์ พร้อมกับสร้าง App Store ซึ่งเป็นที่ที่น่าเชื่อถือที่ผู้ใช้จะได้ค้นพบและดาวน์โหลดแอปได้อย่างปลอดภัย โดยใน App Store นั้น แอปต่างๆ จะมาจากนักพัฒนาที่มีตัวตนอยู่จริงและได้ตกลงที่จะปฏิบัติตามแนวทางของเรา นอกจากนี้แอปยังได้รับการแจกจ่ายไปถึงผู้ใช้อย่างปลอดภัยโดยไม่มีการแทรกแซงจากบุคคลหรือบริษัทอื่นอีกด้วย ขณะเดียวกันเราก็มีการตรวจสอบทุกแอปและการอัปเดตแอปแต่ละครั้งเพื่อประเมินว่าแอปนั้นผ่านมาตรฐานระดับสูงของเราหรือไม่ เรียกได้ว่ากระบวนการนี้ออกแบบมาเพื่อปกป้องผู้ใช้โดยการป้องกันไม่ให้มัลแวร์ อาชญากรไซเบอร์ และมิจฉาชีพเล็ดลอดเข้ามาใน App Store ได้ และยังมีการปรับปรุงกระบวนการนี้อย่างต่อเนื่องด้วย ส่วนแอปที่สร้างมาสำหรับเด็กก็จะต้องปฏิบัติตามแนวทางที่เคร่งครัดด้านการเก็บข้อมูลและความปลอดภัย ซึ่งออกแบบมาเพื่อดูแลความปลอดภัยของเด็กๆ อีกทั้งจะต้องผสานรวมเป็นหนึ่งเดียวกับคุณสมบัติการควบคุมโดยผู้ปกครองใน iOS

เมื่อเป็นเรื่องความเป็นส่วนตัวแล้ว เราไม่เพียงแค่เชื่อว่านี่คือเรื่องสำคัญ แต่เราเชื่อว่านี่คือสิทธิมนุษยชนขั้นพื้นฐาน และเราใช้หลักการนี้เป็นแนวทางในการกำหนดมาตรฐานระดับสูงด้านความเป็นส่วนตัว ซึ่งรวมเป็นส่วนหนึ่งอยู่ในผลิตภัณฑ์ของเรา นั่นคือเราจะเก็บเฉพาะข้อมูลส่วนตัวที่จำเป็นจริงๆ ต่อการส่งมอบผลิตภัณฑ์หรือบริการเท่านั้น และให้ผู้ใช้เป็นผู้ควบคุมโดยการขออนุญาตจากผู้ใช้ก่อนที่แอปจะเข้าถึงข้อมูลสำคัญ รวมถึงมีการบ่งบอกอย่างชัดเจนเมื่อแอปเข้าใช้คุณสมบัติที่ละเอียดอ่อนบางอย่าง เช่น ไมโครโฟน กล้อง และตำแหน่งที่ตั้งของผู้ใช้ อีกส่วนที่แสดงให้เห็นถึงความมุ่งมั่นที่เรามีต่อความเป็นส่วนตัวของผู้ใช้มาอย่างต่อเนื่อง ก็คือสองคุณสมบัติใหม่ล่าสุดด้านความเป็นส่วนตัวอย่างป้ายแสดงแนวทางปฏิบัติด้านความเป็นส่วนตัวใน App Store และ "ความโปร่งใสในการติดตามของแอป" ซึ่งช่วยให้ผู้ใช้สามารถควบคุมความเป็นส่วนตัวอย่างที่ไม่เคยทำได้มาก่อน เพราะยิ่งมีความโปร่งใสและข้อมูลเพิ่มมากขึ้นก็ยิ่งทำให้ผู้ใช้นำข้อมูลนั้นมาช่วยตัดสินใจได้อย่างเหมาะสม และระบบป้องกันทั้งหมดนี้ล้วนมีส่วนช่วยให้ผู้ใช้ดาวน์โหลดแอปไหนก็ได้ใน App Store ได้อย่างอุ่นใจ ส่วนนักพัฒนาเองก็ได้ประโยชน์จากความอุ่นใจนี้ตรงที่สามารถเข้าถึงกลุ่มผู้ใช้ในวงกว้างที่ดาวน์โหลดแอปของพวกเขาด้วยความมั่นใจ

รู้หรือไม่

Apple ตรวจสอบแอปและการอัปเดตทั้งหมดใน App Store เพื่อสกัดกั้นแอปที่อาจเป็นอันตรายต่อผู้ใช้ ไม่ว่าจะเป็นแอปที่มีเนื้อหาไม่เหมาะสม รุกล้ำความเป็นส่วนตัวของผู้ใช้ หรือจงใจใส่มัลแวร์ ซึ่งเป็นซอฟต์แวร์ที่ใช้เพื่อจุดประสงค์ที่ไม่ดีหรือเป็นอันตราย

จากการศึกษาพบว่าอุปกรณ์ที่ใช้ Android ถูกโจมตีจากซอฟต์แวร์อันตรายมากกว่า iPhone ถึง 15 เท่า ซึ่งเหตุผลสำคัญก็คือแอป Android นั้น "สามารถดาวน์โหลดจากที่ไหนก็ได้" ในขณะที่ผู้ใช้ iPhone ทั่วไปสามารถดาวน์โหลดแอปได้จากที่เดียว นั่นคือ App Store[4]

แนวทางด้านความปลอดภัยและความเป็นส่วนตัวนี้ได้ผลอย่างยอดเยี่ยมมาโดยตลอด จนทุกวันนี้การที่ใครสักคนจะพบมัลแวร์บน iPhone นั้นเป็นเรื่องที่ยากมาก[5] แม้จะมีบางคนเสนอว่าเราควรสร้างช่องทางให้นักพัฒนาสามารถแจกจ่ายแอปของตนนอก App Store ได้ เช่น ผ่านทางเว็บไซต์หรือแอปสโตร์ของบริษัทอื่น ซึ่งเป็นกระบวนการที่เรียกว่า "การไซด์โหลด" แต่การอนุญาตให้มีการไซด์โหลดจะส่งผลให้แพลตฟอร์ม iOS มีความปลอดภัยลดน้อยลง และทำให้ผู้ใช้ต้องเผชิญความเสี่ยงด้านความปลอดภัยที่ร้ายแรง ซึ่งไม่ใช่แค่ในแอปสโตร์ของบริษัทอื่นเท่านั้น แต่ยังรวมถึงใน App Store ของเราด้วย นั่นเป็นเพราะฐานผู้ใช้ iPhone มีขนาดใหญ่ และผู้ใช้ต่างก็จัดเก็บข้อมูลสำคัญไว้ในโทรศัพท์ ทั้งรูปภาพ ข้อมูลตำแหน่งที่ตั้ง ข้อมูลด้านสุขภาพและการเงิน ดังนั้นหากอนุญาตให้มีการไซด์โหลดก็จะเป็นการเปิดช่องให้เกิดการลงทุนครั้งใหม่เพื่อมุ่งโจมตีแพลตฟอร์มนี้ และผู้ไม่หวังดีก็จะฉกฉวยโอกาสนี้โดยการหันมาทุ่มทรัพยากรมากยิ่งกว่าเดิมเพื่อพัฒนาวิธีโจมตีที่สลับซับซ้อนโดยมีผู้ใช้ iOS เป็นกลุ่มเป้าหมาย และผลลัพธ์ที่ได้ก็คือมีช่องโหว่และการโจมตีที่ถูกนำมาใช้เป็นอาวุธเพิ่มมากขึ้นเรื่อยๆ หรือที่มักเรียกกันว่า "โมเดลการคุกคาม" จนต้องมีการคิดหาวิธีป้องกันสำหรับผู้ใช้ทุกคน และความเสี่ยงจากการถูกโจมตีโดยมัลแวร์ที่เพิ่มขึ้นนี้เองก็ทำให้ผู้ใช้มีความเสี่ยงสูงขึ้น แม้แต่กับผู้ที่ดาวน์โหลดเฉพาะแอปจาก App Store ยิ่งไปกว่านั้น แม้แต่ผู้ใช้ที่เลือกดาวน์โหลดเฉพาะแอปจาก App Store ก็อาจถูกบังคับให้ดาวน์โหลดแอปที่ต้องใช้สำหรับการทำงานหรือการเรียนจากสโตร์ของบริษัทอื่นในกรณีที่ไม่มีแอปนั้นบน App Store หรือผู้ใช้อาจถูกหลอกให้ดาวน์โหลดแอปจากแอปสโตร์ของบริษัทอื่นที่ปลอมเป็น App Store ก็ได้

จากการศึกษาพบว่าแอปสโตร์ของบริษัทอื่นสำหรับอุปกรณ์ Android ซึ่งเป็นที่ที่แอปไม่ต้องผ่านการตรวจสอบนั้น มีความเสี่ยงและแนวโน้มสูงกว่ามากที่จะมีมัลแวร์ เมื่อเทียบกับแอปสโตร์อย่างเป็นทางการ[6] ด้วยเหตุนี้เอง ผู้เชี่ยวชาญด้านความปลอดภัยจึงแนะนำให้ผู้ใช้งานทั่วไปอย่าใช้แอปสโตร์ของบริษัทอื่นเพราะไม่ปลอดภัย[3,7] นอกจากนี้การอนุญาตให้ไซด์โหลดยังเป็นการเปิดประตูสู่โลกที่ผู้ใช้อาจไม่มีทางเลือกอื่นใดนอกจากยอมรับความเสี่ยงเหล่านี้ เพราะบางแอปอาจไม่มีให้ดาวน์โหลดใน App Store อีกต่อไป และมิจฉาชีพก็อาจหลอกล่อให้ผู้ใช้คิดว่ากำลังดาวน์โหลดแอปจาก App Store อย่างปลอดภัยทั้งๆ ที่ในความเป็นจริงแล้วไม่ใช่เลย และการไซด์โหลดยังทำให้ผู้ใช้ตกเป็นเป้าของมิจฉาชีพที่แสวงหาผลประโยชน์จากแอปโดยหลอกลวงผู้ใช้ โจมตีคุณสมบัติด้านความปลอดภัยของ iPhone และละเมิดความเป็นส่วนตัวของผู้ใช้อีกด้วย ทั้งยังทำให้ผู้ใช้ไว้ใจคุณสมบัติต่างๆ ได้ยากขึ้น อย่างการ "ขออนุญาตซื้อ" ซึ่งเป็นคุณสมบัติการควบคุมโดยผู้ปกครองที่ช่วยให้ผู้ปกครองควบคุมการดาวน์โหลดแอปและการซื้อภายในแอปของเด็กๆ ได้ รวมถึง "เวลาหน้าจอ" ซึ่งเป็นคุณสมบัติสำหรับจัดการกับเวลาที่ตนเองและเด็กๆ ใช้งานอุปกรณ์ ซึ่งมิจฉาชีพจะฉวยโอกาสนี้หลอกล่อและสร้างความสับสนให้กับเด็กและผู้ปกครองโดยการปกปิดจุดประสงค์ที่แท้จริงของแอป ทำให้ทั้งสองคุณสมบัติทำงานได้ไม่เต็มประสิทธิภาพ

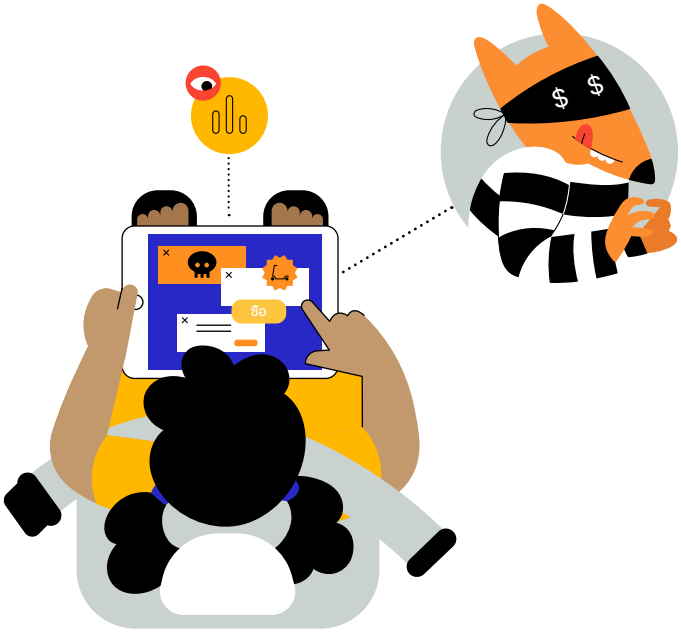
ในที่สุดแล้ว ผู้ใช้ก็ต้องมาคอยระวังอยู่ตลอดเวลาว่าจะถูกหลอกเมื่อไหร่ โดยไม่รู้เลยว่าจะเชื่อใจใครหรืออะไรได้บ้าง จนส่งผลให้ผู้ใช้หลายๆ คนดาวน์โหลดแอปน้อยลงและจำนวนนักพัฒนาที่ผู้ใช้เลือกดาวน์โหลดแอปก็น้อยลงด้วย ส่วนนักพัฒนาเองก็มีความสุ่มเสี่ยงมากขึ้นเช่นกัน เพราะอาจหลงกลผู้ไม่หวังดีที่มาเสนอเครื่องมือสำหรับนักพัฒนาที่มีมัลแวร์แอบแฝงอยู่และรอวันแพร่กระจาย มิหนำซ้ำนักพัฒนายังอาจตกเป็นเหยื่อของการละเมิดลิขสิทธิ์มากขึ้นด้วย ทำให้นักพัฒนาไม่ได้รับค่าตอบแทนจากผลงานของตัวเองอย่างที่ควรได้

การโจมตีที่เกิดขึ้นจริงกับแพลตฟอร์มที่อนุญาตให้มีการไซด์โหลด

มีการค้นพบว่าแอป Android ที่มีกลุ่มเป้าหมายเป็นเด็กนั้นเก็บข้อมูลในลักษณะที่ละเมิดความเป็นส่วนตัวของเด็ก และแอปลักษณะนี้ยังคงเพิ่มจำนวนมากขึ้นและพุ่งเป้าไปที่กลุ่มผู้ใช้ Android ในแอปสโตร์ของบริษัทอื่น แม้ว่าจะถูกถอดออกจาก Google Play Store แล้วก็ตาม[8]

ผู้ไม่หวังดีวางโฆษณาที่ไม่เหมาะสมหรือลามกอนาจารไว้ในแอปที่มีกลุ่มเป้าหมายเป็นเด็ก[9]

มาดูกันว่าประสบการณ์การใช้งาน iPhone ในชีวิตประจำวันของครอบครัวหนึ่งจะแตกต่างไปอย่างไรหากมีการไซด์โหลด โดยเราจะติดตามชีวิตของ John กับ Emma ลูกสาววัย 7 ขวบ ที่ต้องผจญกับโลกใบนี้ในแบบที่ไม่แน่ไม่นอนยิ่งขึ้น



เกมที่ติดตั้งด้วยวิธีไซด์โหลดหลบหลีกการควบคุมโดยผู้ปกครอง

Emma ถาม John ว่าเธอจะสามารถเล่นเกมที่ได้ยินมาจากเพื่อนๆ ที่โรงเรียนได้มั้ย John จึงหาเกมที่ว่าใน App Store แต่พบว่านักพัฒนาเปิดให้ดาวน์โหลดเกมนี้ผ่านทางแอปสโตร์ของบริษัทอื่นเท่านั้น ซึ่งเป็นเรื่องที่ John ไม่ค่อยสบายใจ แต่เขาก็ดาวน์โหลดมาเพราะเห็นว่า Emma อยากลองเล่นเกมนี้จริงๆ และแอปสโตร์ของบริษัทอื่นนั้นก็ยืนยันว่าแอปนี้เหมาะกับเด็ก ต่อมาขณะอยู่ระหว่างทางไปสวนสาธารณะ ในช่วงที่ Emma กำลังนั่งเล่นเกมอยู่เบาะหลังของรถนั่นเอง แอปก็กระหน่ำส่งลิงก์ซึ่งเชื่อมโยงไปยังเว็บไซต์ภายนอกและโฆษณาที่เจาะจงเป้าหมายให้กับเธอมากมาย ซึ่งก่อนหน้านั้น John ก็เพิ่งใส่ข้อมูลบัตรเครดิตเพื่อซื้อแพ็คเริ่มต้นตอนที่ดาวน์โหลดเกมไปด้วยโดยที่ไม่รู้ว่าการ "ขออนุญาตซื้อ" ซึ่งเป็นคุณสมบัติการควบคุมโดยผู้ปกครองนั้นไม่สามารถใช้กับแอปที่ติดตั้งด้วยวิธีไซด์โหลดแบบนี้ได้ ดังนั้นในขณะที่ Emma เล่นเกมอยู่ เธอจึงได้ซื้อรอบเกมและไอเท็มพิเศษมากมายหลายอย่างโดยไม่รู้ตัวเลยว่าคุณพ่อยังไม่ทันได้อนุมัติการซื้อด้วยซ้ำ ยิ่งไปกว่านั้นแอปนี้ยังฝังตัวติดตามของบริษัทอื่น ซึ่งเก็บรวบรวม วิเคราะห์ และขายข้อมูลของ Emma ให้กับนายหน้าหาข้อมูล ถึงแม้ว่าแอปนั้นจะมีกลุ่มเป้าหมายเป็นเด็กก็ตาม

การโจมตีที่เกิดขึ้นจริงกับแพลตฟอร์มที่อนุญาตให้มีการไซด์โหลด

มีแอปบน Android ที่ติดตั้งด้วยวิธีไซด์โหลดก่อเหตุโจมตีด้วยแรนซั่มแวร์ชนิด "ล็อคเกอร์" ซึ่งเมื่อติดตั้งแล้ว แอปอันตรายเหล่านี้จะล็อคโทรศัพท์ของผู้ใช้จนไม่สามารถใช้งานได้ หรือใช้รูปภาพเป็นตัวประกันเพื่อเรียกค่าไถ่[10,11]

ผู้ใช้ Android เคยถูกหลอกให้ใช้วิธีที่ไม่ปลอดภัยในการดาวน์โหลดแอปอย่าง Netflix และ Candy Crush เวอร์ชั่นปลอม โดยเมื่อแอปปลอมเหล่านี้ได้รับอนุญาตให้เข้าถึงข้อมูลหรือโดยการอาศัยช่องโหว่ของแพลตฟอร์ม ก็จะสามารถสอดส่องผู้ใช้ Android ผ่านทางไมโครโฟน, ถ่ายภาพหน้าจอของอุปกรณ์, ดูตำแหน่งที่ตั้ง ข้อความ และรายชื่อ, ขโมยข้อมูลประจำตัวสำหรับการล็อกอิน และการเปลี่ยนแปลงสิ่งต่างๆ ในโทรศัพท์ของผู้ใช้ได้[12,13,14] และยังมีการใช้แอปอื่นๆ เพื่อขโมยข้อมูลประจำตัวสำหรับการทำธุรกรรมทางธนาคาร และยึดบัญชีธนาคารของผู้ใช้อีกด้วย[15,16,17,18]

ในการหลอกลวงด้วยแรนซั่มแวร์ที่เกิดขึ้นเมื่อไม่นานนี้ มีการใช้แอป Android ที่มีฉากหน้าเป็นแอปติดตามการสัมผัสเชื้อ COVID-19 ซึ่งหากติดตั้ง แอปนี้จะเข้ารหัสข้อมูลส่วนตัวทั้งหมด แล้วฝากที่อยู่อีเมลไว้ให้ผู้ใช้ติดต่อกลับหากต้องการกู้ข้อมูลคืนมา[19]

มีการตรวจพบแอปหนึ่งในแอปสโตร์ Android ของบริษัทอื่นที่หลอกล่อผู้ใช้โดยแอบอ้างว่าเป็นการอัปเดตระบบ ซึ่งเมื่อติดตั้งแล้ว แอปนั้นจะแสดงการแจ้งเตือนว่า "กำลังค้นหารายการอัปเดต" แต่ในขณะเดียวกันกลับพยายามเข้าถึงและขโมยข้อมูลส่วนตัวของผู้ใช้ เช่น ข้อความ รายชื่อ และรูปภาพ[20,21]

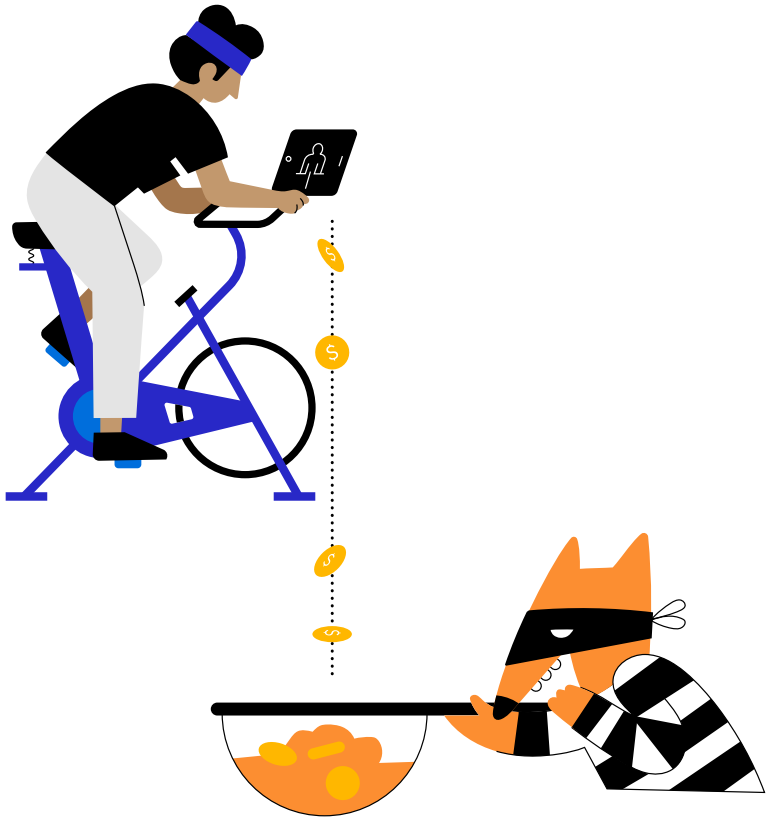
ขณะอยู่ที่สวนสาธารณะ แอปฟิลเตอร์ซึ่งเป็นของลอกเลียนแบบที่ John ติดตั้งด้วยวิธีไซด์โหลดขู่ว่าจะลบรูปภาพทั้งหมดถ้าเขาไม่ยอมจ่ายเงิน

ขณะที่ John และ Emma อยู่ในสวนสาธารณะ John เห็นโฆษณาแอปฟิลเตอร์สำหรับเซลฟี่จากนักพัฒนาแอปชื่อดังที่ดูแล้วน่าจะสนุกดีถ้าใช้กับ Emma ซึ่งโฆษณานั้นก็พาเขาไปยังเพจสำหรับดาวน์โหลดแอปที่ดูเหมือนเพจของนักพัฒนาแอปรายนั้นใน App Store ซึ่งทำให้ John คิดว่าทุกอย่างปลอดภัยดี โดยที่เขาไม่รู้ตัวเลยว่าจริงๆ แล้วกำลังดาวน์โหลดแอปเวอร์ชั่นลอกเลียนแบบจากแอปสโตร์ของบริษัทอื่น และเพราะ John คิดว่าแอปฟิลเตอร์นั้นมาจากนักพัฒนาชื่อดังที่น่าเชื่อถือ เขาจึงอนุญาตให้แอปเข้าถึงรูปภาพ แต่พอแอปเริ่มทำงาน John ก็รู้ตัวเลยว่าเขาพลาดท่าแล้ว เพราะแอปขู่ว่าจะลบรูปภาพทั้งหมดในเครื่องถ้าเขาไม่ยอมใส่ข้อมูลบัตรเครดิตแล้วจ่ายค่าไถ่ ซึ่งโดยปกติแล้วระบบป้องกันบนอุปกรณ์ของ iPhone จะให้ John เป็นผู้ควบคุมว่าต้องการอนุญาตให้แอปใดเข้าถึงรูปภาพได้ แต่ในกรณีนี้ แอปที่ติดตั้งด้วยวิธีไซด์โหลดหลอกล่อให้เขาอนุญาตให้แอปเข้าถึงรูปภาพโดยการสวมรอยเป็นแอปฟิลเตอร์สำหรับเซลฟี่

การโจมตีที่เกิดขึ้นจริงกับแพลตฟอร์มที่อนุญาตให้มีการไซด์โหลด

จากการศึกษาพบว่าแอปเถื่อนที่เผยแพร่ทางแอปสโตร์ของบริษัทอื่นทำให้นักพัฒนาสูญเสียรายได้หลายพันล้านต่อปี[22]

แอปเถื่อนและแอปผิดกฎหมายเป็นสิ่งที่แพร่หลายบน Android ซึ่งแอปลักษณะนี้มีตั้งแต่แอปเกมที่สามารถโกงเกมได้ (เช่น Pokémon Go เวอร์ชั่นเถื่อนที่สามารถจำลองตำแหน่งให้ผู้เล่นอยู่ที่ไหนก็ได้) หรือแอปที่ถูกดัดแปลงแก้ไขเพื่อลักลอบเข้าถึงคอนเทนต์หรือคุณสมบัติพรีเมี่ยม รวมถึงแอปการพนันผิดกฎหมายและแอปที่มีคอนเทนต์สำหรับผู้ใหญ่[23,24,25]

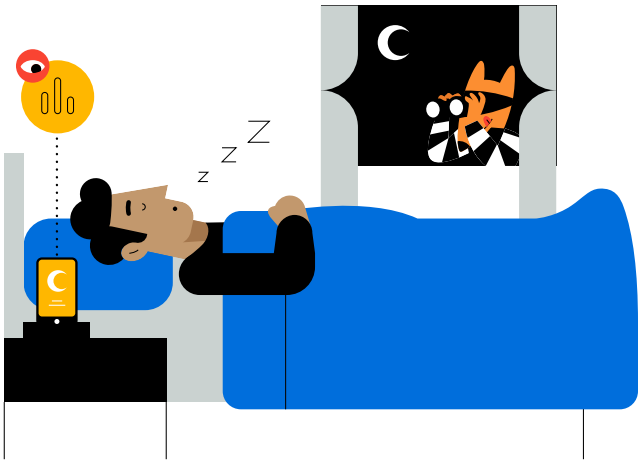


John เผลอดาวน์โหลดแอปเถื่อนจากแอปสโตร์ของบริษัทอื่นโดยไม่รู้ตัว

เพื่อนของ John ชอบแอปฟิตเนสที่เธอใช้อยู่มาก เธอจึงส่งรหัสอ้างอิงมาเพื่อให้ John ได้ลองใช้ดูบ้าง แต่รหัสอ้างอิงนั้นกลับใช้ได้เฉพาะในกรณีที่เขาดาวน์โหลดแอปผ่านแอปสโตร์ของบริษัทอื่นที่ไม่ได้ผ่าน App Store เท่านั้น เขาจึงดาวน์โหลดแอป แล้วสมัครสมาชิกรายเดือน แต่เรื่องที่ทั้งคู่ไม่รู้เลยก็คือ จริงๆ แล้วแอปนี้เป็นแอปเถื่อน นั่นหมายความว่าเงินที่เขาจ่ายทุกเดือนนั้นไปไม่ถึงมือของนักพัฒนาผู้ออกแบบและสร้างแอปนี้ แต่เข้ากระเป๋าของมิจฉาชีพที่ขโมยแอปนี้มาแทน ในขณะที่ John เองก็เชื่อว่าเขากำลังทำสิ่งที่ถูกต้อง นั่นคือการสนับสนุนนักพัฒนาแอปฟิตเนสที่ยอดเยี่ยมแอปนี้ แต่กลับกลายเป็นว่าเขากำลังทำให้มิจฉาชีพหาเงินเข้ากระเป๋าได้มากขึ้น พร้อมกับสนับสนุนกลวิธีฉ้อโกงที่ทำให้นักพัฒนาขาดรายได้โดยไม่รู้ตัว

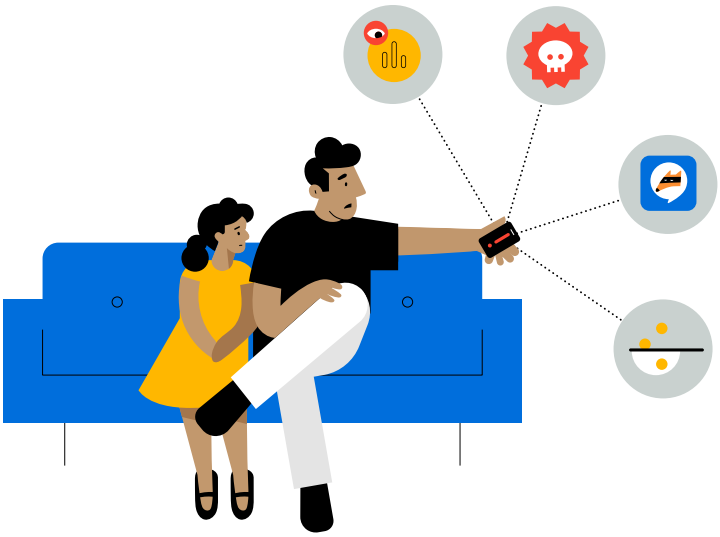
ดูเพิ่มเติมเกี่ยวกับการปกป้องความเป็นส่วนตัวของ Apple

หากต้องการข้อมูลเพิ่มเติมว่าคุณสมบัติ "ความโปร่งใสในการติดตามของแอป" และป้ายแสดงแนวทางปฏิบัติด้านความเป็นส่วนตัวใน App Store ช่วยเพิ่มความโปร่งใสและทำให้คุณควบคุมวิธีเก็บและใช้ข้อมูลของแอปได้อย่างไร โปรดอ่าน **"ในหนึ่งวันเกิดอะไรขึ้นกับข้อมูลของคุณบ้าง"** และไปที่ **apple.com/th/privacy/control**



แอปที่ติดตั้งด้วยวิธีไซด์โหลดละเมิดความเป็นส่วนตัวของ John

John ได้ยินมาว่ามีแอปใหม่สำหรับติดตามการนอนหลับที่เขาอยากลองใช้ แต่แอปนี้ไม่มีให้ดาวน์โหลดใน App Store เขาจึงดาวน์โหลดจากแอปสโตร์ของบริษัทอื่น ลงทะเบียนด้วยที่อยู่อีเมลส่วนตัว แล้วเริ่มใช้แอปนั้นเพื่อติดตามคุณภาพการนอนหลับของตัวเอง และแอปนี้ยังอ้างว่าจะเก็บข้อมูลสุขภาพและการใช้งานของผู้ใช้เป็นส่วนตัวทั้งหมดโดยไม่มีการเชื่อมโยงกับข้อมูลภายนอกหรือแชร์กับบริษัทอื่นอีกด้วย แต่ปรากฏว่าคำกล่าวอ้างนี้ไม่เป็นความจริงแต่อย่างใด เพราะแอปนี้ติดตั้งด้วยวิธีไซด์โหลด นักพัฒนาแอปจึงสามารถทำอะไรก็ได้อย่างอิสระ ซึ่งผลปรากฏว่าแอปนี้ได้ติดตาม John โดยใช้ที่อยู่อีเมลของเขาโดยไม่ขออนุญาต ซึ่งวิธีนี้ทำให้นักพัฒนาสามารถเชื่อมโยงข้อมูลของ John กับข้อมูลที่เก็บโดยแอปอื่น แล้วขายข้อมูลสุขภาพของเขาให้นายหน้าหาข้อมูล ทั้งหมดนี้โดยไม่ได้รับอนุญาตจากผู้ใช้ และยังไม่ต้องกังวลด้วยว่าจะมีอะไรมาหยุดการกระทำนี้ได้



ผู้คนมากกว่า 1 พันล้านคนใช้ iPhone ทุกวัน ทั้งสำหรับการทำธุรกรรมทางธนาคาร เพื่อจัดการกับข้อมูลสุขภาพ และถ่ายภาพครอบครัว และฐานผู้ใช้ที่ใหญ่ขนาดนี้ก็มักตกเป็นเป้าหมายการทำเงินที่ล่อตาล่อใจเหล่าอาชญากรไซเบอร์และมิจฉาชีพ ดังนั้นหากอนุญาตให้มีการไซด์โหลดก็จะยิ่งเป็นการเปิดช่องให้เกิดการลงทุนครั้งใหม่เพื่อมุ่งโจมตี iPhone ในระดับที่ใหญ่ยิ่งกว่าการโจมตีแพลตฟอร์มอื่นๆ อย่าง Mac ซึ่งบรรดามิจฉาชีพก็จะรู้สึกตื่นตัวอยากพัฒนาเครื่องมือและทักษะความชำนาญในการโจมตีระบบความปลอดภัยของอุปกรณ์ iPhone และถึงแม้ว่า App Store จะออกแบบมาเพื่อตรวจจับและสกัดกั้นการโจมตีที่มีอยู่ในปัจจุบัน แต่ถ้าโมเดลการคุกคามเปลี่ยนแปลงไป ก็อาจสามารถหลบหลีกระบบป้องกันเหล่านี้ได้ จากนั้นมิจฉาชีพก็จะใช้เครื่องมือและทักษะความชำนาญที่พัฒนาขึ้นใหม่นี้เพื่อมุ่งโจมตีสโตร์ของบริษัทอื่นรวมถึง App Store ซึ่งเป็นการเพิ่มความเสี่ยงให้กับผู้ใช้ทุกคน แม้แต่กับผู้ใช้ที่ดาวน์โหลดเฉพาะแอปจาก App Store เพราะเมื่อมีช่องทางการเผยแพร่เพิ่มมากขึ้นจากการที่สามารถติดตั้งแอปด้วยวิธีไซด์โหลดได้ ผู้ไม่หวังดีจึงมีโอกาสในการเจาะช่องโหว่ในระบบเพิ่มมากขึ้นด้วย และยิ่งเป็นการจูงใจให้ผู้โจมตีหันมาพัฒนาและกระจายมัลแวร์มากขึ้น

นั่นหมายความว่าผู้ใช้อย่าง John ซึ่งเริ่มไม่เห็นความสำคัญของระบบความปลอดภัยและการป้องกันใน iPhone และ App Store แล้ว ก็คงต้องคอยระแวดระวังกลวิธีของอาชญากรไซเบอร์และมิจฉาชีพที่เปลี่ยนไปอยู่ตลอดเวลา โดยไม่รู้ว่าจะเชื่อใจใครหรืออะไรได้บ้าง ซึ่งในบางกรณี John อาจไม่มีทางเลือกอื่นเลยนอกจากยอมรับความเสี่ยงในการติดตั้งแอปที่ไม่มีใน App Store ด้วยวิธีการไซด์โหลดจากสโตร์ของบริษัทอื่น หรือเขาอาจถูกหลอกให้ทำเช่นนั้นก็ได้ และในกรณีที่ร้ายแรงที่สุดก็คือ แอปที่ติดตั้งด้วยวิธีไซด์โหลดอาจแอบอ้างว่าเป็นอย่างอื่น เช่น อ้างว่าเป็นการอัปเดตซอฟต์แวร์ของ Apple หรือปลอมแปลงหน้าดาวน์โหลดของตัวเองให้ดูเหมือน App Store แล้วพยายามเจาะระบบป้องกันบนอุปกรณ์ของ iPhone เพื่อเข้าถึงข้อมูลที่ป้องกันไว้ อย่างข้อความ รูปภาพ และตำแหน่งที่ตั้ง จากนั้นเมื่อ John เริ่มเจอกับความเสี่ยงและการหลอกลวงแบบนี้มากเข้า เขาก็คงระวังตัวมากขึ้นเมื่อจะดาวน์โหลดแอป จนในที่สุดเขาก็คงดาวน์โหลดแอปน้อยลง และใช้เพียงแอปจากนักพัฒนาที่น่าเชื่อถือเพียงไม่กี่ราย ส่งผลให้นักพัฒนารายย่อยหน้าใหม่เข้าถึงกลุ่มผู้ใช้ด้วยแอปใหม่ๆ ที่ล้ำสมัยได้ยากขึ้นตามไปด้วย และสิ่งที่ขาดหายไปก็คงเป็นความอุ่นใจที่มาพร้อมกับการได้รู้ว่าแอปบน iPhone เป็นตัวเลือกที่ปลอดภัยที่สุดสำหรับทั้งตัวเขาเองและลูกสาวนั่นเอง

รู้หรือไม่

ผู้ใช้ที่กังวลเกี่ยวกับความปลอดภัยและความเป็นส่วนตัวมีแนวโน้มมากขึ้นที่จะดาวน์โหลดแอปน้อยลงและลบแอปออกจากอุปกรณ์[26,27,28] และระบบนิเวศที่ไม่ค่อยปลอดภัยจนทำให้ผู้ใช้รู้สึกไม่สบายใจที่จะดาวน์โหลดแอป อาจส่งผลให้ผู้ใช้มีแนวโน้มที่จะทดลองใช้แอปใหม่ๆ อันล้ำสมัยน้อยลงตามไปด้วย หรือไม่อยากเสี่ยงกับแอปที่มาจากนักพัฒนาหน้าใหม่ที่ยังไม่ค่อยเป็นที่รู้จัก ซึ่งอาจทำให้การเติบโตของระบบเศรษฐกิจของแอปชะลอตัว และส่งผลเสียต่อทั้งผู้ใช้และนักพัฒนา

ความปลอดภัยหลายชั้นและการตรวจสอบแอปของ Apple ช่วยปกป้อง John, Emma และอุปกรณ์ของพวกเขา

เราใช้แนวทางที่หลากหลายและการป้องกันแบบหลายชั้นเพื่อปกป้องผู้ใช้ iOS จากแอปอันตราย พร้อมมอบการรักษาความปลอดภัยที่ดีที่สุดในโลกให้กับแพลตฟอร์มของเรา ซึ่ง iOS ต้องเผชิญกับความท้าทายด้านความปลอดภัยที่ไม่เหมือนใคร เนื่องจากผู้ใช้มักจะดาวน์โหลดแอปใหม่ลงบนอุปกรณ์ของตนอย่างสม่ำเสมอ และอุปกรณ์ iOS ยังต้องมีความปลอดภัยมากพอที่เด็กๆ จะสามารถใช้งานด้วยตนเองได้โดยไม่ต้องมีผู้ปกครองคอยดูแล นั่นหมายความว่าเราต้องยกระดับแนวทางการรักษาความปลอดภัยบน iPhone ไปอีกขั้นเมื่อเทียบกับบน Mac เนื่องจากจำนวนผู้ใช้ รวมถึงพฤติกรรม และความคาดหวังของผู้ใช้มีความแตกต่างกันออกไป

- **สำหรับ Mac นั้น เราใช้ซอฟต์แวร์อัตโนมัติในการสแกนแอปเพื่อหามัลแวร์ที่รู้จักและป้องกันไม่ให้แอปดังกล่าวเข้าสู่ App Store ซึ่งอาจนำไปสู่การเข้าถึงข้อมูลผู้ใช้หรือสร้างอันตรายให้แก่ผู้ใช้ได้**
- **นอกจากนี้ นักพัฒนาแอปยังต้องส่งคำอธิบายเกี่ยวกับแอปและคุณสมบัติต่างๆ ของแอปมาให้เราด้วย** ซึ่งข้อมูลนี้จะได้รับการตรวจสอบความถูกต้องโดยทีมผู้เชี่ยวชาญในระหว่างกระบวนการตรวจสอบแอป และจะแสดงต่อผู้ใช้เพื่อเป็นข้อมูลประกอบการตัดสินใจในการดาวน์โหลดแอป กระบวนการนี้มีผลอย่างยิ่งในการป้องกันการกระจายมัลแวร์ผ่านกลวิธีหลอกล่อที่พบบ่อยที่สุด อย่างการบิดเบือนมัลแวร์ให้ดูเหมือนแอปยอดนิยม หรือการอ้างว่าแอปมาพร้อมคุณสมบัติที่ดึงดูดใจซึ่งไม่ได้ให้มาจริงๆ
- นอกจากจะต้องตรวจสอบว่าคุณสมบัติของแอปทำงานตามที่อธิบายไว้หรือไม่ และหน้า App Store ของแอปนั้นถูกต้องหรือไม่แล้ว **ผู้เชี่ยวชาญเหล่านี้ยังต้องตรวจสอบด้วยตนเองว่าแอปนั้นๆ มีการขออนุญาตเข้าถึงข้อมูลสำคัญของผู้ใช้โดยไม่จำเป็นหรือไม่ รวมถึงประเมินว่าแอปที่ทำขึ้นมาสำหรับเด็กเป็นไปตามข้อกำหนดด้านการรวบรวมข้อมูลและความปลอดภัยที่เข้มงวดหรือไม่**
- **ในกรณีที่แอปเข้าสู่ App Store เรียบร้อยแล้ว แต่ถูกตรวจพบในภายหลังว่ามีการละเมิดหลักเกณฑ์ของเรา เราจะทำงานร่วมกับนักพัฒนาเพื่อรีบแก้ปัญหาอย่างรวดเร็ว** ส่วนในกรณีที่เกิดเหตุร้ายแรง เช่น หากพบว่าแอปเกี่ยวข้องกับการฉ้อโกงและกิจกรรมที่เป็นอันตราย แอปนั้นจะถูกลบออกจาก App Store ทันที และผู้ใช้ที่ดาวน์โหลดแอปไปแล้วจะได้รับการแจ้งเตือนถึงพฤติกรรมที่เป็นอันตรายของแอปด้วย
- **หากผู้ใช้พบปัญหาเกี่ยวกับแอปที่ดาวน์โหลดจาก App Store ผู้ใช้สามารถขอความช่วยเหลือจาก Apple Care และทำเรื่องขอคืนเงินได้**

เป้าหมายของการตรวจสอบแอปคือการตรวจสอบให้แน่ใจว่าแอปที่อยู่บน App Store นั้นมีความน่าเชื่อถือ และข้อมูลของแอปบนหน้า App Store ต้องบอกวิธีการทำงานและข้อมูลที่แอปจะเข้าถึงไว้อย่างถูกต้อง ซึ่งเราได้พัฒนากระบวนการนี้อย่างต่อเนื่องด้วยการอัปเดตและปรับปรุงเครื่องมือรวมถึงขั้นตอนการทำงานอย่างสม่ำเสมอ

เมื่อผู้ใช้ดาวน์โหลดแอปผ่าน App Store เรียบร้อยแล้ว พวกเขาจะสามารถควบคุมวิธีการทำงานของแอปและข้อมูลที่แอปเข้าถึงได้ ผ่านทางคุณสมบัติ เช่น "ความโปร่งใสในการติดตามของแอป" และการอนุญาตต่างๆ ขณะเดียวกันก็ยังมีคุณสมบัติเพิ่มเติม เช่น คุณสมบัติ "ขออนุญาตซื้อ" ที่ช่วยให้ผู้ปกครองควบคุมการซื้อของบุตรหลานได้ หรือคุณสมบัติ "เวลาหน้าจอ" ที่ใช้ควบคุมเวลาใช้งานสำหรับแอปบางหมวดหมู่ รวมทั้งข้อมูลที่พวกเขาแชร์ นอกจากนี้ ผู้ใช้ยังสามารถจัดการการชำระเงินที่เกี่ยวข้องกับแอปทั้งหมดได้จากศูนย์กลางในที่เดียว รวมทั้งสามารถดูและยกเลิกการสมัครสมาชิกแบบจ่ายเงินผ่าน "การชำระเงินภายในแอป" ได้อย่างง่ายดายอีกด้วย ซึ่งการควบคุมเหล่านี้ไม่สามารถใช้งานได้อย่างเต็มที่กับแอปที่ติดตั้งด้วยการไซด์โหลด

นอกเหนือจากการป้องกันโดยการตรวจสอบแอปแล้ว เรายังได้ออกแบบฮาร์ดแวร์และซอฟต์แวร์ของอุปกรณ์ให้เป็นด่านสุดท้ายในการปกป้องผู้ใช้ในกรณีที่มีการดาวน์โหลดแอปที่เป็นอันตรายลงบนอุปกรณ์ เช่น แอปจาก App Store ที่ดาวน์โหลดลงบน iPhone จะถูกทำ "แซนด์บ็อกซ์" ซึ่งหมายความว่าแอปนั้นจะไม่สามารถเข้าถึงไฟล์ที่จัดเก็บโดยแอปอื่นหรือเปลี่ยนแปลงสิ่งต่างๆ บนอุปกรณ์ได้ เว้นแต่จะได้รับอนุญาตจากผู้ใช้อย่างถูกต้อง

การป้องกันที่ดีที่สุดจะต้องอาศัยการผสมผสานทุกชั้นของความปลอดภัย ตั้งแต่การตรวจสอบแอปอย่างเข้มงวดเพื่อช่วยป้องกันการติดตั้งแอปอันตราย และการปกป้องแพลตฟอร์มอย่างแข็งแกร่งเพื่อจำกัดความเสียหายที่อาจเกิดขึ้นจากแอปอันตรายเหล่านั้น ระบบรักษาความปลอดภัยที่ออกแบบมาสำหรับ iOS เป็นเครื่องป้องกันที่ทรงพลังสำหรับผู้ใช้และยอดเยี่ยมที่สุดในบรรดาอุปกรณ์ทั้งหมด แต่ระบบป้องกันเหล่านั้นไม่ได้ออกแบบมาเพื่อป้องกันสิ่งที่ผู้ใช้อาจถูกหลอกให้ทำ การตรวจสอบแอปจึงให้ความสำคัญกับนโยบายของ App Store ที่ออกแบบมาเพื่อปกป้องผู้ใช้จากแอปที่อาจพยายามทำอันตรายหรือหลอกล่อให้ผู้ใช้อนุญาตให้มีการเข้าถึงข้อมูลที่สำคัญ และหากเกิดกรณีที่ร้ายแรงที่สุด เมื่อแอปอันตรายพยายามหลบหลีกการป้องกันบนอุปกรณ์ การตรวจสอบแอปก็จะช่วยทำให้แอปเหล่านั้นเข้าถึงอุปกรณ์ของผู้ใช้ได้ยากขึ้นตั้งแต่แรก

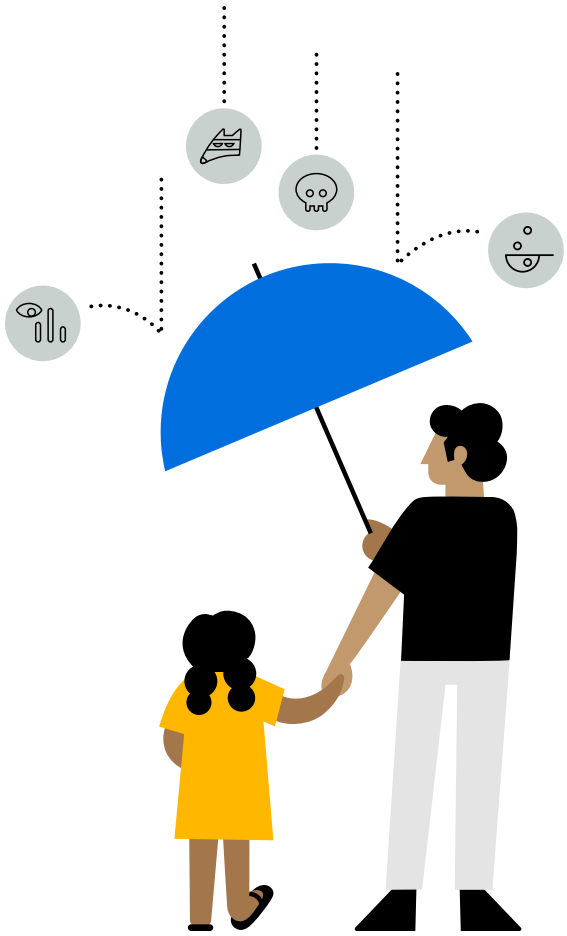
ทั้งหมดนี้ทำให้ผู้เชี่ยวชาญด้านความปลอดภัยเห็นตรงกันว่า iPhone เป็นอุปกรณ์พกพาที่ปลอดภัยที่สุด เรียกได้ว่า การรักษาความปลอดภัยแบบหลายชั้นของ Apple ช่วยปกป้องผู้ใช้จากซอฟต์แวร์อันตรายในระดับที่ไม่มีใครเทียบได้ ผู้ใช้จึงใช้งานอุปกรณ์ Apple ได้อย่างสบายใจ

การตรวจสอบแอป

ในกระบวนการตรวจสอบแอป เราจะดูจนมั่นใจและยืนยันได้ว่าแอปมาจากแหล่งที่เชื่อถือได้และไม่มีส่วนที่เป็นอันตราย นอกจากนี้เรายังตรวจสอบด้วยว่าแอปจะไม่มีการพยายามหลอกล่อให้คุณซื้อโดยไม่ตั้งใจ หรือหลอกให้คุณมอบสิทธิ์การเข้าถึงข้อมูลส่วนบุคคลให้ รวมถึงตรวจสอบนักพัฒนาและผู้ใช้โดยละเอียดแล้วคัดผู้ที่ประพฤติตัวไม่เหมาะสมออกไป และแม้ว่ากระบวนการตรวจสอบแอปจะไม่สามารถป้องกันการเผยแพร่แอปคุณภาพต่ำได้ทั้งหมด แต่เรายังคงสร้างสรรค์และพยายามปรับปรุงเทคโนโลยี แนวทางปฏิบัติ และกระบวนการตรวจสอบอย่างต่อเนื่อง

ผลลัพธ์จากระบบป้องกันของแอปของ Apple ในปี 2020

- **แอปและการอัปเดตใหม่ 100,000 รายการได้รับการตรวจสอบโดยเฉลี่ยทุกสัปดาห์** โดยทีมงานผู้เชี่ยวชาญกว่า 500 คนซึ่งทำหน้าที่ตรวจสอบแอปในภาษาต่างๆ
- **แอปใหม่ที่มีปัญหาเกือบหนึ่งล้านแอปและรายการอัปเดตจำนวนพอๆ กัน ได้ถูกปฏิเสธหรือลบ:**
  - มีรายการที่เป็นสแปม การลอกเลียนแบบ หรือทำให้ผู้ใช้เข้าใจผิด กว่า 150,000 รายการ
  - มีรายการที่ละเมิดแนวทางด้านความเป็นส่วนตัวกว่า 215,000 รายการ
  - มีรายการที่ปกปิดคุณสมบัติหรือไม่ได้ระบุคุณสมบัติไว้เป็นลายลักษณ์อักษร กว่า 48,000 รายการ
  - มีการฉ้อโกง ซึ่งส่วนใหญ่จะเป็นการใช้วิธี "ล่อลวงให้ติดกับแล้วเปลี่ยนเงื่อนไขในตอนท้าย หรือ Bait and Switch" เพื่อกระทำความผิดทางอาญาหรือการกระทำที่ต้องห้ามอื่นๆ ประมาณ 95,000 รายการ
- **Apple หยุดยั้งการทำธุรกรรมที่อาจเป็นการฉ้อโกงรวมมูลค่ากว่า 1.5 พันล้านดอลลาร์**
- **Apple ถอดถอนทีมนักพัฒนา 470,000 ทีมออกจากโปรแกรมนักพัฒนาของ Apple ด้วยเหตุผลเรื่องการฉ้อโกง** นอกจากนี้ยังปฏิเสธความพยายามในการลงทะเบียนนักพัฒนาซอฟต์แวร์เกือบ 205,000 ครั้ง เนื่องจากข้อกังวลเรื่องการฉ้อโกง
- **Apple ปิดใช้งานบัญชีของลูกค้า 244 ล้านบัญชี เนื่องด้วยเหตุผลเรื่องการฉ้อโกงและการกระทำที่ไม่เหมาะสม ซึ่งรวมถึงการเขียนรีวิวปลอม** นอกจากนี้ยังปฏิเสธความพยายามในการสร้างบัญชี 424 ล้านครั้ง เนื่องจากมีรูปแบบที่เป็นการฉ้อโกงและการใช้งานในทางที่ผิด



การตรวจสอบแอปช่วยให้ John ดาวน์โหลดแอปได้อย่างสบายใจ

คุณสมบัติด้านความปลอดภัยและความเป็นส่วนตัวของ App Store ช่วยให้ John สบายใจได้เมื่อเขาดาวน์โหลดแอปสำหรับตัวเองและลูกสาว เพราะเขารู้ว่า Apple ตรวจสอบแอปบน App Store แบบ 100% เพื่อหามัลแวร์ที่รู้จัก ซึ่งนั่นทำให้มีโอกาสน้อยมากที่ผู้ใช้จะพบซอฟต์แวร์อันตรายบน iPhone เมื่อเทียบกับอุปกรณ์อื่นๆ

คำถามที่พบบ่อย

ดูเพิ่มเติมเกี่ยวกับการปกป้องความเป็นส่วนตัวของ Apple

หากต้องการข้อมูลเพิ่มเติมว่า Apple ปกป้องความปลอดภัยและความเป็นส่วนตัวของคุณอย่างไรบน App Store โปรดไปที่ **apple.com/th/app-store**

หากต้องการข้อมูลเพิ่มเติมว่า Apple ปกป้องข้อมูลบอกตำแหน่งของคุณอย่างไร ก็สามารถอ่านได้ใน **รายงานอย่างเป็นทางการเกี่ยวกับบริการหาตำแหน่งที่ตั้ง**

หากต้องการข้อมูลเพิ่มเติมเกี่ยวกับการควบคุมโดยผู้ปกครองบน iOS โปรดไปที่ **apple.com/th/families**

การไซด์โหลดคืออะไร

"การไซด์โหลด" คือกระบวนการดาวน์โหลดและติดตั้งแอปลงบนอุปกรณ์เคลื่อนที่โดยที่แอปนั้นมาจากแหล่งอื่น เช่น เว็บไซต์หรือแอปสโตร์ของบริษัทอื่น ซึ่งไม่ใช่ App Store อย่างเป็นทางการของ Apple โดยเราได้ออกแบบ iPhone มาเพื่อไม่ให้ผู้ใช้ทั่วไปสามารถติดตั้งแอปด้วยวิธีไซด์โหลดได้มาตั้งแต่แรก เพื่อปกป้องความปลอดภัยและความเป็นส่วนตัวของผู้ใช้

โมเดลการคุกคามคืออะไร

โมเดลการคุกคามคือการสร้างแบบจำลองชุดการโจมตีและช่องโหว่ที่ผู้ใช้จะต้องได้รับการปกป้อง โดยอุปกรณ์ ผู้ใช้ และสภาพแวดล้อมแต่ละประเภทก็จะมีโมเดลการคุกคามที่แตกต่างกันออกไป และเป็นสิ่งที่เราต้องคำนึงถึงในการรักษาความปลอดภัย ซึ่ง App Store ถือเป็นองค์ประกอบที่สำคัญในการป้องกันภัยจากโมเดลการคุกคามสำหรับ iPhone และเป็นที่ที่น่าเชื่อถือที่ผู้ใช้สามารถเข้าไปดาวน์โหลดแอปที่ได้รับการตรวจสอบโดย Apple ได้อย่างปลอดภัย ซึ่งแอปทั้งหมดนั้นเป็นแอปจากนักพัฒนาที่เป็นที่รู้จักและเป็นไปตามแนวทางของ Apple

การอนุญาตให้ติดตั้งแอปบน iPhone ด้วยวิธีไซด์โหลดจากเว็บไซต์และแอปสโตร์ของบริษัทอื่นจะสร้างภัยคุกคามต่อผู้ใช้ที่ดาวน์โหลดแอปจาก App Store เพียงอย่างเดียวด้วยหรือไม่

แน่นอน การไซด์โหลดบน iPhone เป็นการเพิ่มช่องทางในการเผยแพร่แอป เปลี่ยนโมเดลการคุกคาม และเพิ่มความเสี่ยงต่อการถูกโจมตีในหลากหลายรูปแบบยิ่งขึ้น สิ่งนี้จึงทำให้ผู้ใช้ทุกคนตกอยู่ในความเสี่ยงอย่างแน่นอน แม้กระทั่งผู้ที่พยายามป้องกันตนเองด้วยการดาวน์โหลดแอปผ่านทาง App Store เพียงอย่างเดียวด้วย เพราะการอนุญาตให้มีการไซด์โหลดจะเป็นการเปิดช่องให้เกิดการลงทุนครั้งใหม่เพื่อมุ่งโจมตี iPhone และทำให้ผู้ไม่หวังดีเกิดแรงจูงใจในการพัฒนาเครื่องมือและทักษะฝีมือในการโจมตีระบบความปลอดภัยของอุปกรณ์ iPhone ในระดับที่ไม่เคยเกิดขึ้นมาก่อน และเมื่อมีทักษะฝีมือในการโจมตีที่ซับซ้อนมากขึ้นแล้ว ผู้ไม่หวังดีจะเริ่มกำหนดเป้าหมายไปที่สโตร์ของบริษัทอื่นรวมถึง App Store ด้วย ซึ่งนั่นจะทำให้ผู้ใช้ทั้งหมดมีความเสี่ยงมากขึ้น ยิ่งไปกว่านั้น แม้แต่ผู้ใช้ที่เลือกดาวน์โหลดเฉพาะแอปจาก App Store ก็อาจถูกบังคับให้ดาวน์โหลดแอปที่ต้องใช้สำหรับการทำงานหรือการเรียนจากสโตร์ของบริษัทอื่นในกรณีที่ไม่มีแอปนั้นบน App Store หรือผู้ใช้อาจถูกหลอกให้ดาวน์โหลดแอปจากแอปสโตร์ของบริษัทอื่นที่ปลอมเป็น App Store ก็ได้

การตรวจสอบแอปของ Apple มีขั้นตอนอะไรบ้าง

เราใช้ทั้งเทคโนโลยีที่ซับซ้อนและความเชี่ยวชาญของคนจริงๆ ในการตรวจสอบแอปและการอัปเดตทั้งหมดอย่างถี่ถ้วนเพื่อประเมินว่าแอปและการอัปเดตเหล่านั้นเป็นไปตามแนวทางด้านความเป็นส่วนตัวและความปลอดภัยที่เคร่งครัดของ App Store หรือไม่ โดยเราจะอาศัยความเชี่ยวชาญของคนจริงๆ เป็นหลัก ในกรณีที่การตรวจสอบแบบอัตโนมัติไม่สามารถตรวจจับปัญหาแบบเฉพาะเจาะจงได้ดีพอ เช่น การละเมิดความเป็นส่วนตัวหรือแอปสำหรับเด็กที่ไม่เป็นไปตามแนวทางอันเคร่งครัดของเรา แนวทางต่างๆ ของเรามีการเปลี่ยนแปลงอยู่ตลอดเวลาเพื่อให้สามารถรับมือกับภัยคุกคามและความท้าทายใหม่ๆ ได้ โดยเป้าหมายของเราก็คือการปกป้องผู้ใช้และมอบประสบการณ์ที่ดีที่สุดให้แก่ผู้ใช้บน App Store ซึ่งในตอนนี้แอปและการอัปเดตใหม่ 100,000 รายการได้รับการตรวจสอบโดยเฉลี่ยทุกสัปดาห์โดยทีมงานผู้เชี่ยวชาญกว่า 500 คนทั่วโลก

มีการตรวจสอบอะไรบ้าง

แอปและการอัปเดตทั้งหมดที่ถูกส่งมายัง App Store จะต้องเข้าสู่กระบวนการตรวจสอบแอป

ผู้ปกครองสามารถควบคุมอุปกรณ์ Apple ได้อย่างไรบ้าง

เราออกแบบคุณสมบัติต่างๆ ที่ช่วยให้ผู้ปกครองสามารถควบคุมการใช้งานอุปกรณ์ของเด็กๆ ได้ ไม่ว่าจะเป็นคุณสมบัติ "เวลาหน้าจอ" ที่ช่วยให้ผู้ปกครองเข้าใจเกี่ยวกับเวลาที่เด็กๆ ใช้ไปกับแอป การเยี่ยมชมเว็บไซต์ต่างๆ และการใช้งานอุปกรณ์ได้ดียิ่งขึ้น ซึ่งคุณสมบัติ "เวลาหน้าจอ" ยังให้ผู้ปกครองกำหนดระยะเวลาที่เด็กๆ จะใช้กับแอปและเว็บไซต์ในบางหมวดหมู่สำหรับแต่ละวันได้อีกด้วย นอกจากนั้นยังมีคุณสมบัติ "ขออนุญาตซื้อ" ที่ช่วยให้ผู้ปกครองอนุมัติหรือปฏิเสธการซื้อและการดาวน์โหลดแอปของเด็กๆ จากอุปกรณ์ของตัวเองได้เลย โดยการ "ขออนุญาตซื้อ" จะหมดอายุภายใน 15 นาทีเพื่อป้องกันการซื้อที่ตามมาหลังจากนั้น

คุณสมบัติ "ความโปร่งใสในการติดตามของแอป" และป้ายแสดงแนวทางปฏิบัติด้านความเป็นส่วนตัวบน App Store คืออะไร

คุณสมบัติเหล่านี้ช่วยให้ผู้ใช้ควบคุมข้อมูลและความเป็นส่วนตัวของตัวเองได้ดียิ่งขึ้น โดยคุณสมบัติ "ความโปร่งใสในการติดตามของแอป" จะกำหนดให้แอปต้องขออนุญาตผู้ใช้ก่อนที่จะติดตามข้อมูลของผู้ใช้ข้ามไปยังแอปหรือเว็บไซต์ของบริษัทอื่น และเมื่อมีป้ายแสดงแนวทางปฏิบัติด้านความเป็นส่วนตัวบน App Store เราก็ได้กำหนดให้แอปทุกแอปบน App Store ต้องแสดงข้อมูลสรุปแนวทางปฏิบัติด้านความเป็นส่วนตัวของนักพัฒนาให้ผู้ใช้เห็นในแบบที่เข้าใจง่าย โดยจะต้องให้ข้อมูลหลักๆ ว่าแอปใช้ข้อมูลของพวกเขาอย่างไรบ้าง

แหล่งที่มา

1. Jobs, Steve, "Third Party Applications on the iPhone," 17 ตุลาคม 2007, เผยแพร่ทาง tidbits.com/2007/10/17/steve-jobss-iphone-sdk-letter/

2. ENISA, "Vulnerabilities - Separating Reality from Hype," *European Union Agency for Cybersecurity*, 24 สิงหาคม 2016

3. Griffin, Robert Jr., "Study on Mobile Device Security," *U.S. Department of Homeland Security*, เมษายน 2017

4. Nokia, "Threat Intelligence Report 2020," *Nokia*, 2020

5. Johnson, Dave, "Can iPhones get viruses? Here's what you need to know," *Business Insider*, 4 มีนาคม 2019

6. Symantec, "Internet Security Threat Report, Volume 23," เมษายน 2018

7. Golovin, Igor, "Malware in Minecraft mods: story continues," *Kaspersky*, 9 มิถุนายน 2021

8. Lunden, Ingrid, "Google removes 3 Android apps for children, with 20M+ downloads between them, over data collection violations," *Tech Crunch*, 23 ตุลาคม 2020

9. Henry, Josh, "Malicious Apps: For Play or Prey?" *United States Cybersecurity Magazine*, 2021

10. Schwartz, Jaime-Heather, "How to protect your Android phone from ransomware – plus a guide to removing it," *Avira*, 13 สิงหาคม 2020

11. Seals, Tara, "Emerging Ransomware Targets Photos, Videos on Android Devices," *ThreatPost*, 24 มิถุนายน 2020

12. Owaida, Amer, "Beware Android trojan posing as Clubhouse app," *WeLiveSecurity by ESET*, 18 มีนาคม 2021

13. Desai, Shivang, "SpyNote RAT posing as Netflix app," *Zscaler*, 23 มกราคม 2017

14. Peterson, Andrea, "Beware: New Android malware is 'nearly impossible' to remove," *The Washington Post*, 6 พฤศจิกายน 2015

15. Palmer, Danny, "This Android trojan malware is using fake apps to infect smartphones, steal bank details," *ZDNet*, 1 มิถุนายน 2021

16. O'Donnell, Lindsey, "Banking.BR Android Trojan Emerges in Credential-Stealing Attacks," *ThreatPost*, 21 เมษายน 2020

17. Stefanko, Lukas, "Android Trojan steals money from PayPal accounts even with 2FA on," *WeLiveSecurity* by ESET, 11 ธันวาคม 2018

18. Cybereason Nocturnus Team, "FakeSpy Masquerades as Postal Service Apps Around the World," *Cybereason*, 1 กรกฎาคม 2020

19. Stefanko, Lukas, "New ransomware posing as COVID-19 tracing app targets Canada; ESET offers decryptor," *WeLiveSecurity by ESET*, 24 มิถุนายน 2020

20. Yaswant, Aazim, "New Advanced Android Malware Posing as 'System Update'," *Zimperium*, 26 มีนาคม 2021

21. Aamir, Humza, "Beware of this newly discovered Android spyware that pretends to be a system update," *TechSpot*, 29 มีนาคม 2021

22. Koetsier, John, "The Mobile Economy Has A $17.5B Leak: App Piracy," *Forbes*, 2 กุมภาพันธ์ 2018

23. Koetsier, John, "App Developers Losing $3-4 Billion Annually Thanks To 14 Billion Pirated Apps," *Forbes*, 24 กรกฎาคม 2017

24. Maxwell, Andy, "Cheat Maker Agrees to Pay Pokémon Go Creator $5m to Settle Copyright Infringement Lawsuit," *TorrentFreak*, 8 มกราคม 2021

25. Campaign for a Commercial-Free Childhood, "Apps which Google rates as safe for kids violate their privacy and expose them to other harms," 12 ธันวาคม 2019

26. J.P. Morgan, "2020 E-commerce Payments Trends Report: Japan," *J.P. Morgan*, 2020

27. Deloitte, "Trust: Is there an app for that? Deloitte Australian Privacy Index 2019," 2019

28. Gikas, Mike, "How to Protect Your Privacy on Your Smartphone," *Consumer Reports*, 1 กุมภาพันธ์ 2017