แคสเปอร์สกี้ แลป เตือนองค์กรการศึกษาระวังภัยฟิชชิ่งออนไลน์ ลวงข้อมูลส่วนบุคคลจากเครือข่ายมหาวิทยาลัย

นักวิจัยของแคสเปอร์สกี้ แลป ตรวจพบภัยคุกคามไซเบอร์ประเภทการโจมตีแบบฟิชชิ่ง 961 ครั้งที่โจมตีมหาวิทยาลัยมากถึง 131 แห่งใน 16 ประเทศทั่วโลก ในช่วง 12 เดือนที่ผ่านมา (ตั้งแต่เดือนกันยายน 2017) เพื่อขโมยข้อมูลสำคัญของมหาวิทยาลัย นั่นคือ ข้อมูลตัวบุคคลของบุคลากรและนักศึกษา ข้อมูลไอพีแอดเดรส และโลเคชั่น โดยส่วนมาก ผู้ร้ายไซเบอร์จะสร้างเว็บเพจสำหรับใส่ล็อกอินและพาสเวิร์ดเข้าระบบดิจิทัลของมหาวิทยาลัยโดยออกแบบให้มีหน้าตาเหมือนกับเว็บจริง

จะเห็นได้ชัดว่าข้อมูลตัวบุคคลของพนักงานธนาคารและพาสเวิร์ดของลูกจ้างองค์กรอุตสาหกรรมนั้นมีความสำคัญมาก แต่ข้อมูลของนักศึกษาและพนักงานมหาวิทยาลัยนั้น ดูแล้วไม่น่าเป็นเป้าหมายของอาชญากรไซเบอร์ได้เลย แต่จริงๆ แล้ว การโจมตีสเปียร์ฟิชชิ่งอาจทำให้ผู้ร้ายเข้าถึงแหล่งข้อมูลที่มีค่า อย่างรายงานการวิจัยที่มีหัวข้อหลากหลายตั้งแต่เรื่องเศรษศาสตร์ไปจนถึงฟิสิกส์นิวเคลียร์ได้เลย นอกจากนี้ มหาวิทยาลัยมักจะร่วมมือกับองค์กรเอกชนชั้นนำ ทำให้ผู้ร้ายอาจเข้าถึงข้อมูลขององค์กรนั้นได้อีกด้วย

นักวิจัยของแคสเปอร์สกี้ แลป พบการโจมตีมหาวิทยาลัยมากถึง 131 แห่ง ส่วนมากจะเน้นที่มหาวิทยาลัยที่ใช้ภาษาอังกฤษในการสื่อสาร โดยมหาวิทยาลัยจำนวน 83 แห่งตั้งอยู่ในสหรัฐอเมริกา จำนวน 21 แห่งตั้งอยู่ในสหราชอาณาจักร และพบว่าผู้ร้ายไซเบอร์พุ่งเป้าโจมตีมหาวิทยาลัยวอชิงตันเป็นหลัก คือ โจมตีมากถึง 111 ครั้งเลยทีเดียว นอกจากนี้ องค์กรด้านการศึกษาในทวีปเอเชีย ยุโรป และแอฟริกา ก็โดนโจมตีเช่นเดียวกัน

นางสาวนาเดซด้า เดมิโดวา นักวิจัยด้านความปลอดภัย แคสเปอร์สกี้ แลป กล่าวว่า “จำนวนองค์กรที่โดนโจมตีนั้นเป็นตัวเลขที่น่ากังวลมาก อาชญากรไซเบอร์กำลังสนใจด้านการศึกษาอย่างมาก ผู้บริหารมหาวิทยาลัยจำเป็นต้องพิจารณาว่าพนักงานและนักศึกษาอาจเป็นจุดอ่อนและช่องโหว่ให้ผู้ร้ายไซเบอร์เข้าถึงระบบดิจิทัลได้ จึงควรเร่งหามาตรการเพื่อความปลอดภัยไซเบอร์”

แคสเปอร์สกี้ แลป ขอแนะนำมาตรการความปลอดภัยเพื่อป้องกันตัวเองจากการตกเป็นเหยื่อฟิชชิ่งดังนี้

• หมั่นตรวจสอบลิ้งก์และอีเมลของผู้ส่งเสมอๆ ก่อนคลิกดำเนินการใดๆ ทางที่ดี ไม่ควรคลิกลิ้งก์ แต่ควรใช้วิธีพิมพ์แอดเดรสแทน ในกรณีที่ไม่มั่นใจว่าเว็บไซต์นั้นหรือผู้ส่งนั้นเป็นตัวจริงหรือปลอดภัยหรือไม่ ห้ามกรอกข้อมูลส่วน

บุคคลเด็ดขาด หากคิดว่าได้กรอกข้อมูลลงเว็บปลอมไปแล้ว ให้รีบเปลี่ยนพาสเวิร์ดทันที

• อย่าใช้พาสเวิร์ดเดียวกันเพื่อใช้งานเว็บไซต์หรือเซอร์วิสต่างๆ เพราะถ้าหากพาสเวิร์ดถูกขโมยไปหนึ่งอัน แอคเค้าท์อื่นๆ ก็เสี่ยงเช่นเดียวกัน ควรใช้พาสเวิร์ดที่มีความแข็งแกร่ง แฮ็กยาก และหากไม่ต้องการจดจำพาสเวิร์ดที่ยากเกินไป แนะนำให้ใช้โปรแกรมจัดการพาสเวิร์ด เช่น Kaspersky Password Manager

• เพื่อป้องกันการรุกล้ำการเชื่อมต่อเน็ตเวิร์กและพาไปยังเว็บไซต์ปลอม หรือเข้าขัดขวางเว็บทราฟฟิกให้สะดุด ขอแนะนำให้ใช้การเชื่อมต่อที่ปลอดภัย มีพาสเวิร์ดป้องกัน และมีการเอ็นคริปต์ชั่นเท่านั้น โดย Kaspersky Secure Connection จะเปิดการเอ็นคริปต์ชั่นให้อัตโนมัติเมื่อพบการเชื่อมต่อที่ไม่ปลอดภัยเพียงพอ

• ควรใช้งานโซลูชั่นเพื่อความปลอดภัยไซเบอร์เสมอเมื่อใช้งานโมบายดีไวซ์ในการท่องเว็บ ซึ่งจะช่วยแจ้งเตือนหากจะหลงเข้าใช้งานเว็บฟิชชิ่ง

• องค์กรควรให้ความรู้แก่พนักงานว่า ไม่ควรให้ข้อมูลสำคัญแก่บุคคลอื่น เช่น ล็อกอิน พาสเวิร์ด และไม่ควรคลิกลิ้งก์จากผู้ส่งที่ไม่รู้จักคุ้นเคย หรือลิ้งก์ในอีเมลน่าสงสัย

• องค์กรควรติดตั้งโซลูชั่นด้านความปลอดภัยสำหรับเอ็นพอยต์ที่มีเทคโนโลยีป้องกันการฟิชชิ่ง เช่น Kaspersky Endpoint Security for Business ซึ่งจะตรวจจับและบล็อกสแปมและฟิชชิ่งได้

รายงานการค้นพบเพิ่มเติม https://securelist.com/phishing-for-knowledge/88268/