مواجهة هجمات تصيد البيانات

جمال مراد قيس

2025-10-26

في عصر يتّسع فيه نطاق الاتصال الرقمي يوماً بعد يوم، أصبحت البيانات تمثّل المورد الأكثر قيمة في العالم المعاصر، وهو ما جعلها هدفاً رئيسياً للهجمات الإلكترونية. ومن أخطر هذه التهديدات ما يُعرف بـ"تصيّد البيانات" أو Phishing، وهي ممارسات احتيالية تهدف إلى خداع المستخدمين للكشف عن معلوماتهم الحساسة مثل كلمات المرور أو تفاصيل بطاقاتهم البنكية. ورغم أن هذه الهجمات بدأت بأساليب بدائية قبل عقدين، فإنها اليوم أكثر تطوراً وتعقيداً بفضل الذكاء الاصطناعي والتعلم الآلي وقدرة المهاجمين على تقليد المؤسسات الرسمية بإتقان مذهل.

أصبح التصيّد الرقمي يعتمد على ما يُسمّى بـ"الهندسة الاجتماعية"، حيث يتم استغلال سلوك الإنسان نفسه كنقطة ضعف في النظام الأمني. إذ يتلقّى المستخدم رسالة إلكترونية أو إشعاراً يبدو من جهة موثوقة، تطلب منه تحديث بياناته أو النقر على رابط معيّن. وبمجرد استجابته، يتم تحويله إلى موقع مزيف يحاكي الموقع الأصلي لسرقة بياناته أو إدخال برامج خبيثة في جهازه. وقد تحوّل هذا النوع من الهجمات إلى منظومة كاملة تُدار باحتراف، وتتنوّع بين التصيّد العام الذي يستهدف أكبر عدد ممكن من المستخدمين، والتصيّد المتخصّص (Spear Phishing) الذي يركّز على أشخاص بعينهم في مؤسسات حيوية.

تلعب التكنولوجيا الحديثة دوراً محورياً في التصدي لهذا الخطر، لكنها ليست الحل الوحيد. فالتعامل مع التصيّد يتطلّب منظومة أمنية متكاملة تجمع بين التقنية المتقدمة والسياسات الصارمة والوعي البشري المستمر. إن أدوات الكشف الذكي، وبرامج الحماية القائمة على الذكاء الاصطناعي، وتقنيات العزل الافتراضي، والتوثيق متعدد العوامل، جميعها تمثّل خطوط دفاع مهمة. ومع ذلك، تظلّ فعالية هذه الأدوات رهينة بمدى التزام الأفراد بإجراءات الحذر، وبتعاون المؤسسات في تعزيز ثقافة الأمن السيبراني.

تشير الدراسات الحديثة إلى أن مواجهة التصيّد تتطلّب مقاربة ديناميكية تتطوّر مع تطوّر أساليب المهاجمين. فقد أكّد تقرير نُشر في مجلة MDPI حول "العامل البشري في هجمات التصيّد" أن ما يزيد على 80% من هذه الهجمات تنجح بسبب التفاعل البشري غير الواعي، وليس بسبب ضعف الأنظمة التقنية. ويؤكد الباحثون في هذا التقرير أن التركيز على بناء ثقافة أمنية رقمية داخل المؤسسات، عبر التدريب المستمر ومحاكاة الهجمات، هو السبيل الأنجع لتقليل المخاطر. فالتكنولوجيا مهما بلغت قوتها لا يمكنها وحدها مواجهة العنصر البشري إذا ظلّ غير مدرّب أو قليل الوعي، مما يجعل الاستثمار في التعليم الأمني جزءاً لا يتجزأ من أي استراتيجية وطنية للأمن السيبراني.

الإجراءات التقنية لمواجهة التصيّد

1- تطبيق أنظمة التوثيق المتعدد لضمان أن الدخول إلى الحسابات لا يتم إلا عبر خطوات تحقق إضافية. 2- اعتماد أنظمة فلترة ذكية للبريد الإلكتروني لرصد الرسائل المزيفة والروابط الخبيثة قبل وصولها إلى المستخدم. 3- استخدام التعلّم الآلي لتحليل أنماط الرسائل المشبوهة والتعرّف المبكر على محاولات الاختراق. 4- تحديث البرمجيات والأجهزة بشكل دوري لإغلاق الثغرات الأمنية التي قد يستغلها المهاجمون.

الإجراءات البشرية والتنظيمية

1- تعزيز الوعي الأمني بين الموظفين من خلال برامج تدريب منتظمة على التعرّف إلى رسائل التصيّد وأساليب الخداع الشائعة. 2- وضع سياسات مؤسسية واضحة تحكم التعامل مع البريد الإلكتروني والمرفقات والمواقع الخارجية. 3- تشجيع الإبلاغ السريع عن الرسائل المشبوهة دون خوف من العقوبة، لضمان سرعة الاستجابة داخل المؤسسة. 4- تنفيذ اختبارات اختراق دورية لمحاكاة هجمات تصيّد وتقييم جاهزية الأنظمة والموظفين في مواجهتها.

الخاتمة

تؤكد التجربة العالمية أن التصيّد ليس تهديداً تقنياً فحسب، بل ظاهرة سلوكية-اجتماعية تستغل الثقة البشرية قبل الثغرات البرمجية. لذلك فإن مواجهة هذا الخطر تتطلب وعياً رقمياً شاملاً، يبدأ من المستخدم الفردي ويمتد إلى المؤسسات والحكومات. فكل ضغطة زرّ غير محسوبة قد تكون مدخلاً لتسريب معلومات تمس الأمن الاقتصادي أو الخصوصية الشخصية.

ولا يمكن تحقيق الحماية الكاملة إلا بتكامل ثلاثي: التقنية، والسياسة، والثقافة الأمنية. وعندما يدرك الإنسان أن أمنه الرقمي هو مسؤوليته

الشخصية، يمكن القول إننا قطعنا الخطوة الأولى نحو فضاء سيبراني أكثر أمناً واستقراراً.

المصادر

Mitigation Strategies Against Phishing Attacks: A Systematic Review
How to Protect Against Understanding and Preventing Phishing Attacks
Phishing and the Human Factor: Insights from Evolving Phishing Attacks
a Bibliometric Analysis — MDPI

تواصل مع الكاتب: mohamedmouradgamal@gmail.com

https://arsco.org/articles/article-detail-47306/