كشف التصيد الاحتيالي والهندسة الاجتماعية

التصيد الاحتيالي هجوم يرسل فيه المحتال رسالة تدعي أنها من جهة نثق بها، على أمل أن ننقر على رابط أو نفتح ملفا أو نسلمه معلومات خاصة. وهو نوع من الهندسة الاجتماعية، أي استهداف عادات الناس وعواطفهم بدل اقتحام الحواسيب. وتعتمد سلمى، موظفة الحسابات الدائنة في شركة تصنيع، على خمس عادات كل يوم، لتسبق رسائل قد تصل بالبريد الإلكتروني أو الرسائل النصية أو المحادثات أو المكالمات. وهذا الفيديو مادة تعليمية مساعدة، ولذلك ينبغي دائما الرجوع إلى قواعد فريق الأمن في المؤسسة.

1. معرفة الحيلة

تنجح الهندسة الاجتماعية لأنها تستغل ردود فعل إنسانية معتادة، مثل احترام السلطة والاستعجال والانفعال القوي. ويستفيد المحتالون من معلومات منشورة على الإنترنت، ومنها وسائل التواصل الاجتماعي، فقد تذكر الرسالة أسماء ومشاريع وموردين حقيقيين وتبقى فخا. ولم يعد حسن الصياغة دليلا على الصدق، لأن الأدوات تنتج اليوم نصا سليما تماما. والعادة الأولى هي أن نسأل عن الإجراء الذي تريده الرسالة فعلا، سواء كان نقرة أو دفعة أو كلمة مرور أو ملفا يفتح.

مثال: يتلقى موظف جديد في مكتب محاماة رسالة محادثة تستخدم اسم الشريك الإداري وصورته، وتطلب بطاقات هدايا لأحد العملاء. فيسأل الموظف عن الإجراء المطلوب، فيجد أنه عملية شراء تتم عبر المحادثة. وبدل أن ينفذ الطلب، يسأل مدير المكتب، فيتوقف الطلب عند أول فحص.

في العمل: تتلقى سلمى بريدا إلكترونيا يخاطبها باسمها، ويذكر موردا حقيقيا، ويشير إلى أمر شراء فعلي. وتتذكر أن هذه التفاصيل يمكن جمعها من صفحات عامة، فلا تثبت شيئا. وتسأل عما يريده البريد فعلا، فتجد أن الجواب هو تغيير حساب مصرفي. فلا ترد على البريد، بل تتحقق من الطلب أولا.

2. التمهل

الضغط أفضل أدوات المحتال، لأن من يستعجل يتجاوز الفحوص. وتقول الرسائل المعتادة إن حسابا سيغلق، أو إن هناك دفعة متأخرة، أو إن مديرا كبيرا يحتاج إلى أمر قبل اجتماع. وتعد الإرشادات الرسمية اللغة العاجلة والانفعالية والتهديد بعواقب خطيرة من علامات التصيد الاحتيالي. والعادة الثانية هي التوقف حين نشعر بالاستعجال، واعتبار هذا الشعور نفسه إنذارا.

مثال: تقول رسالة نصية إن طردا سيعاد ما لم يدفع المتلقي رسوما صغيرة خلال ساعة واحدة. فيشعر المتلقي بالعجلة، ثم يتوقف، ويلاحظ أنه لا يوجد في الرسالة رقم طلب. ويتتبع الطرد في موقع شركة الشحن نفسها فلا يجد شيئا في انتظاره، فلا يدفع شيئا. وذلك هو معنى التمهل بالضبط.

في العمل: يبدو أن بريدا إلكترونيا صادرا عن المدير المالي لسلمى يطلب تحويلا عاجلا إلى مورد جديد قبل الظهر. وتلاحظ سلمى ذعرها هي نفسها، وتعده إشارة إلى التمهل. فتتصل بالمدير على الرقم الموجود في دليل الشركة. فيتبين أنه لا يعلم شيئا عن الطلب.

3. فحص المرسل والروابط

العادة الثالثة هي أن ننظر بدقة إلى مصدر الرسالة الحقيقي وإلى وجهتها. فاسم العرض قد يكون أي شيء، ولذلك نفحص العنوان الكامل بحثا عن حرف مبدل أو كلمة زائدة أو نطاق غير معتاد. وقد يظهر الرابط باسم ويقود إلى غيره، وإذا وضع المؤشر فوقه ظهرت وجهته الحقيقية دون نقر. ولا نثق بالروابط المختصرة لأنها تخفي وجهتها، ونحذر من المرفقات غير المتوقعة.

مثال: تدعي رسالة أنها من مصرف، وتستخدم عنوانا فيه حرفان مبدلان في اسم المصرف. والحرفان يتشابهان للنظرة الأولى، ولهذا تنجح هذه الحيلة. فيفحص العميل العنوان كاملا، ويحذف الرسالة، ويفتح تطبيق المصرف نفسه. وهذا هو معنى فحص المرسل عمليا.

حقوق الطبع والنشر محمية © - أكاديمية أساسيات (شركة أساسيات للخدمات الاستشارية)

في العمل: تتلقى سلمى رابطا إلى بوابة فواتير لدى مورد، ويبدو اسم المرسل عاديا تماما. ويظهر وضع المؤشر فوقه موقعا لا صلة له بالمورد، فلا تنقر. وتتصل بقسم الحسابات لدى المورد على الرقم الموجود في العقد. فتعلم أن بريد المورد اخترق صباح ذلك اليوم.

4. التحقق من الطلبات غير المعتادة

العادة الرابعة تتعلق بما تطلبه الرسالة. فطلبات كلمات المرور والدفعات وبطاقات الهدايا وتغيير بيانات الحساب المصرفي تحتاج إلى فحص ثان، مهما كان الاسم الظاهر على الرسالة. ونؤكد الطلب عبر قناة نعرفها سلفا، مثل الرقم الموجود في العقد، ولا نؤكده أبدا عبر بيانات الاتصال الواردة في الرسالة. والمصارف لا تطلب منا تأكيد بيانات الحساب عبر الهاتف، فالمتصل الذي يفعل ذلك علامة تحذير.

مثال: يتصل شخص يدعي أنه من المصرف، ويطلب الرمز الذي أرسل للتو في رسالة نصية، زاعما أنه سيحمي الحساب. فينهي صاحب الحساب المكالمة، ويتصل بالرقم المطبوع على بطاقة المصرف. فيؤكد المصرف أنه لم يتصل أحد، فيبقى الحساب آمنا. ولهذا نتحقق دائما من الطلب غير المعتاد.

في العمل: يخبر بريد من مورد سلمى بأن بياناته المصرفية تغيرت، ويطلب منها استخدام الحساب الجديد ابتداء من الفاتورة التالية. وتتبع سلمى قاعدة الشركة التي تقضي بتأكيد كل تغيير باتصال على الرقم الموجود في العقد. فيقول المورد إن شيئا لم يتغير، ويمنع اتصالها دفعة كانت ستذهب إلى محتال.

5. الإبلاغ السريع

إذا بدت الرسالة مشبوهة فلا نرد عليها، ولا ننقر، ولا نفتح مرفقا، ولا نتصل برقم وارد فيها. ونبلغ عنها عبر قناة المؤسسة نفسها، مثل زر الإبلاغ أو فريق الأمن، وتتيح خدمات بريد كثيرة كذلك خيار الإبلاغ عن الرسائل المزعجة. وتفيد البلاغات لأنها تبين لفريق الأمن أي الهجمات قيد الاستخدام. وإذا كان أحدهم قد نقر أو شارك معلومات، أبلغ فريق الأمن فورا وغيرت كلمات المرور المعرضة للخطر. والإبلاغ ليس سببا للوم أبدا، لأن أي شخص قد ينخدع، ومن يخاف العقاب قد يتوقف عن الإبلاغ.

مثال: تصل إلى هاتف شخصي رسالة تبدو كإشعار بالفوز بجائزة، وتعد برحلة مجانية إن نقر صاحب الهاتف على رابط. فلا يرد صاحب الهاتف ولا ينقر. ويستخدم خيار الإبلاغ عن الرسائل المزعجة ثم يحذف الرسالة، فيصل البلاغ إلى الخدمة. وذلك هو معنى الإبلاغ السريع.

في العمل: تشك سلمى في بريد يقول إن صندوق الشركة البريدي شارف على الامتلاء، ويطلب تسجيل الدخول عبر رابط. فلا تنقر، وتستخدم زر الإبلاغ بدل ذلك. ويفحص فريق الأمن الرسالة، وينبه الزملاء الذين تلقوا الرسالة نفسها. وهكذا يحمي بلاغ واحد زملاء كثيرين.

الخاتمة

خلاصة القول إن التصيد الاحتيالي والهندسة الاجتماعية يحاولان دفع الناس إلى التصرف بسرعة وبلا انتباه. وتساعد خمس عادات على مقاومتهما، هي معرفة الحيلة، والتمهل، وفحص المرسل والروابط، والتحقق من الطلبات غير المعتادة، والإبلاغ السريع. وعند الشك نتوقف ونتحقق عبر قناة نثق بها سلفا. ويبين روتين سلمى الهادئ أن كل فحص سريع، وأن التوقف للتحقق يستحق وقته. وهذا الفيديو مادة تعليمية مساعدة، ولذلك تتقدم قواعد فريق الأمن في المؤسسة على كل ما فيه.

المصادر

- CISA (وكالة الأمن السيبراني وأمن البنية التحتية الأمريكية): التعرف على التصيد الاحتيالي والإبلاغ عنه (علامات التصيد والإبلاغ عن الرسائل المزعجة والتحقق المستقل) – https://www.cisa.gov/secure-our-world/recognize-and-report-phishing
- CISA: تجنب هجمات الهندسة الاجتماعية والتصيد الاحتيالي (التعريفات ووضع المؤشر فوق الروابط والتحقق عبر جهات اتصال معروفة وما ينبغي فعله عند الاختراق) – https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks
- المركز الوطني للأمن السيبراني في المملكة المتحدة (NCSC): هجمات التصيد والاحتيال (المعلومات العامة التي يستخدمها المحتالون وفائدة الإبلاغ) – https://www.ncsc.gov.uk/collection/phishing-scams
- NCSC: اكتشاف رسائل الاحتيال والمكالمات (السلطة والإلحاح والعاطفة، والمصارف لا تطلب تأكيد بيانات الحساب هاتفيا، والاتصال بالجهة مباشرة) – https://www.ncsc.gov.uk/collection/phishing-scams/spot-scams
- NCSC: هجمات التصيد والتعامل مع الرسائل المشبوهة (ثقافة بلا لوم، والبلاغات تبين الهجمات قيد الاستخدام) – https://www.ncsc.gov.uk/guidance/phishing
- فتحت الصفحات الخمس في السادس والعشرين من أكتوبر بأداة الجلب وقرئ نصها.

حقوق الطبع والنشر محمية © - أكاديمية أساسيات (شركة أساسيات للخدمات الاستشارية)