

عنوان النشاط: لعب الأدوار – الاستجابة لتهديد رقمي

الهدف:

مساعدة المشاركين على التعرف على محاولة التصيد الإلكتروني (Phishing)، فهم مخاطرها، ومعرفة كيفية الاستجابة الصحيحة لمثل هذه التهديدات الرقمية.

المدة الزمنية:

15-20 دقيقة

المواد المطلوبة:

- نسخ مطبوعة أو عرض رقمي لسيناريو رسالة البريد الإلكتروني الاحتيالية لكل مجموعة.
- دفاتر ملاحظات وأقلام (اختياري) لتدوين الملاحظات أثناء المناقشة.

التعليمات:

1. تشكيل المجموعات:

يتم تقسيم المشاركين إلى أزواج (2 لكل مجموعة).

2. السيناريو:

تلقى المستخدم رسالة بريد إلكتروني تبدو وكأنها من البنك الخاص به. تطلب الرسالة منه التحقق من تفاصيل حسابه من خلال النقر على رابط معين.

مثال على نص البريد الإلكتروني الاحتيالي:

الموضوع: "هام: يرجى التحقق من معلومات حسابك"

نص الرسالة:

"عزيزي العميل،

لاحظنا نشاطاً غير معتاد في حسابك البنكي. لحماية حسابك، نحتاج منك التحقق من التفاصيل الخاصة بك.

يرجى الضغط على الرابط أدناه وتسجيل الدخول إلى حسابك:

 [FakeBank.com Login Link]

شكراً لاختيارك خدماتنا.

مع تحيات،

فريق دعم العملاء"

3. توزيع الأدوار:

- ◆ المشارك الأول: يؤدي دور المستخدم الذي تلقى البريد الإلكتروني الاحتيالي.
- ◆ المشارك الثاني: يلعب دور خبير الأمن السيبراني الذي ينصح المستخدم بكيفية التعامل مع الموقف.

4. المهمة:

المشارك الأول:

- يشرح كيف كان سيتفاعل مع البريد الإلكتروني في البداية، وهل كان سيشك في كونه محاولة تصيد أم لا؟

المشارك الثاني:

- يقدم نصائح أمنية حول:
 - ✓ لماذا يُرجح أن يكون البريد الإلكتروني محاولة تصيد؟
 - ✓ ما العلامات التحذيرية التي تكشف عن الاحتيال؟ (مثل اللغة غير المعتادة، الطلبات العاجلة، الروابط المشبوهة).
 - ✓ ما هي الخطوات الصحيحة للاستجابة؟ (عدم النقر على الروابط، الاتصال بالبنك مباشرة، الإبلاغ عن الرسالة).

خطوات لعب الأدوار:

1 تحديد التهديد الرقمي:

💡 مناقشة سبب خطورة البريد الإلكتروني:

- الرابط المشبوه (يمكن للمستخدم تحريك المؤشر فوق الرابط لرؤية عنوان URL الحقيقي).
- لغة مستعجلة تهدف إلى خلق حالة من الذعر.
- عدم ذكر اسم المستخدم الحقيقي، مما يشير إلى أن البريد الإلكتروني قد يكون عامًا وليس موجّهًا خصيصًا له.

2 استراتيجية الاستجابة:

💡 المشارك الثاني يوجه المشارك الأول حول الإجراءات الصحيحة:

- ✓ عدم النقر على أي روابط أو تحميل مرفقات.
- ✓ الإبلاغ عن البريد الإلكتروني على المنصة (Gmail) ، Outlook ، إلخ (كتصيد احتيالي).
- ✓ التواصل مع البنك مباشرة عبر القنوات الرسمية للتحقق من صحة الطلب.
- ✓ حذف البريد الإلكتروني بعد الإبلاغ عنه.

النقاش الختامي:

- 📢 بعد إتمام لعب الأدوار، تقوم كل مجموعة بتقديم:
- ◆ العلامات التحذيرية التي حددها في البريد الإلكتروني.
- ◆ الخطوات التي اتبعوها لحماية هويتهم الرقمية.

🗣️نقاش جماعي حول:

- لماذا تكون رسائل التصيد الإلكتروني فعالة؟
- ما هي أمثلة أخرى لمحاولات التصيد التي صادفها المشاركون سابقاً؟

دور الميسر:

- 📌 ضمان فهم المشاركين لهدف النشاط.
- 📌 تشجيع "خبير الأمن السيبراني" على تقديم تفسيرات واضحة حول التصيد الإلكتروني وكيفية اكتشافه.
- 📌 اختتام النشاط بتعزيز أفضل ممارسات السلامة الرقمية وكيفية الاستجابة الفعالة لمحاولات التصيد الإلكتروني.
- 🎯 هدف النشاط هو مساعدة المشاركين على اتخاذ قرارات أكثر وعياً لحماية بياناتهم الرقمية.