CONCEPT

التوعية بالأمن السيبراني لجميع الموظفين: التصيد الاحتيالي وكلمات المرور والعمل الآمن

التوعية بالأمن السيبراني لجميع الموظفين: التصيد الاحتيالي وكلمات المرور والعمل الآمن

العمق التقني: ممارس · **أسلوب التطبيق:** محاكاة

مقدمة

تبدأ معظم الهجمات السيبرانية الناجحة بموظف عادي يفتح رسالة بريد مقنعة، أو يتجاوب مع مكالمة محكمة، أو يعيد استخدام كلمة مرور ضعيفة. وتخفض الضوابط التقنية المخاطر، لكنها لا تستطيع إيقاف شخص لم يتعلم التعرف على علامات التحذير أو لا يعرف كيف يبلغ عنها. تبني هذه الدورة من كور كونسبت، المتاحة بمواد باللغتين العربية والإنجليزية، العادات الأمنية اليومية التي يحتاجها كل موظف، من كشف التصيد الاحتيالي إلى التعامل الآمن مع المعلومات. ويتدرب المشاركون في محاكاة واقعية، ويخرجون بخطة السلامة السيبرانية الشخصية وخطة الفريق.

أهداف الدورة

- التعرف على محاولات التصيد الاحتيالي والهندسة الاجتماعية وانتحال الشخصية عبر البريد الإلكتروني والهاتف والرسائل والتواصل المباشر
- حماية حسابات العمل بعبارات مرور قوية والتحقق متعدد العوامل ومفاتيح المرور Passkeys
- التعامل مع المعلومات حسب تصنيفها عند حفظها ومشاركتها وطباعتها والتخلص منها
- العمل بأمان على الأجهزة المحمولة والاتصالات عن بعد وأدوات الذكاء الاصطناعي التوليدي
- الإبلاغ عن الحوادث المشتبه بها فورا عبر القناة الصحيحة وبالتفاصيل المطلوبة
- تطبيق خطة السلامة السيبرانية الشخصية وخطة الفريق في العمل اليومي

الفئة المستهدفة

- الموظفون الإداريون والمكتبيون الذين يتعاملون يوميا مع البريد الإلكتروني والمستندات والاعتمادات
- موظفو خدمة الجمهور الذين يتلقون المكالمات والرسائل والطلبات من العملاء
- موظفو المالية والمشتريات والموارد البشرية الذين يعالجون المدفوعات والفواتير والبيانات الشخصية
- العاملون في الميدان وعن بعد الذين يستخدمون الحواسيب المحمولة والهواتف خارج المكتب
- الموظفون الفنيون والتشغيليون الذين يستخدمون أنظمة العمل دون دور أمني
- الموظفون الجدد في مرحلة التهيئة على ممارسات الأمن في بيئة العمل

محاور الدورة

اليوم الأول: لماذا يعد الأمن السيبراني مسؤولية الجميع

- السرية والسلامة والتوافر مثلث CIA في العمل اليومي
- أنواع الهجمات الشائعة: التصيد الاحتيالي والبرمجيات الضارة وبرامج الفدية والهندسة الاجتماعية
- العامل البشري في سلاسل الهجوم وتقارير حوادث الاختراق
- متطلبات التوعية في إطار NIST CSF 2.0 والضابط 6.3 في ISO/IEC 27001:2022
- قائمة التقييم الذاتي للنظافة السيبرانية الشخصية

اليوم الثاني: قواعد الأمن ومعايير الممارسات الجيدة

- أساسيات سياسة الاستخدام المقبول وسياسة أمن المعلومات وفق ISO/IEC 27002
- ممارسات عبارات المرور وفق NIST SP 800-63B-4 وبرامج إدارة كلمات المرور
- أساليب التحقق متعدد العوامل ومفاتيح المرور Passkeys
- علامات تصنيف المعلومات وقواعد المكتب النظيف
- إجراءات الضابط 14 في CIS Controls v8.1 الخاصة بتوعية القوى العاملة

اليوم الثالث: العمل اليومي الآمن

- كشف رسائل التصيد الاحتيالي بمؤشرات NIST Phish Scale
- التصفح الآمن وتنزيل الملفات واستخدام وسائط التخزين المنفصلة
- العمل الآمن عن بعد وشبكات Wi-Fi العامة واستخدام VPN
- أمن الأجهزة المحمولة وإعدادات أذونات التطبيقات
- فحص الإفراط في المشاركة على وسائل التواصل الاجتماعي وإعدادات الخصوصية

اليوم الرابع: التهديدات المتقدمة والإبلاغ عن الحوادث

- مؤشرات اختراق البريد الإلكتروني للأعمال والاحتيال بالفواتير
- التصيد الصوتي والتصيد بالرسائل النصية ومكالمات الانتحال بالتزييف العميق
- الاستخدام الآمن لأدوات الذكاء الاصطناعي التوليدي مع بيانات العمل
- الأمن المادي: التسلل خلف الموظفين ومرافقة الزوار وسرقة الأجهزة
- خطوات التعرف على الحوادث والإبلاغ عنها وفق ISO/IEC 27035-1

اليوم الخامس: المحاكاة والتخطيط الشخصي للعمل

- تمرين حملة تصيد احتيالي محاكاة واستخلاص الدروس
- محاكاة مكالمة هاتفية بأسلوب الهندسة الاجتماعية
- تمرين الإبلاغ عن حادث مشتبه به
- إعداد مسودة خطة السلامة السيبرانية الشخصية وخطة الفريق
- بناء قائمة التحقق الأمنية للفريق ومراجعتها مع الزملاء

المهارات المكتسبة

- كشف التصيد الاحتيالي
- مقاومة الهندسة الاجتماعية
- تأمين الحسابات
- التعامل السليم مع المعلومات
- العمل الآمن عن بعد
- الإبلاغ عن الحوادث
- الاستخدام الآمن لأدوات الذكاء الاصطناعي
- السلوك الواعي بالأمن

لماذا تحضر هذه الدورة

- تعود إلى عملك بخطة السلامة السيبرانية الشخصية وخطة الفريق لتطبيقها من اليوم الأول
- تتدرب على كشف رسائل التصيد والمكالمات الاحتيالية الواقعية في بيئة آمنة قبل أن تواجهها فعليا
- تحمي حسابات أسرتك وأجهزتها بالعادات نفسها التي تحمي مؤسستك
- تتعلم بالعربية أو الإنجليزية مع زملاء من قطاعات وأدوار مختلفة

الخاتمة

كل موظف جزء من منظومة الدفاع في مؤسسته، سواء ذكر الأمن في مسماه الوظيفي أم لا. تنتقل هذه الدورة من أسباب استهداف المهاجمين للأشخاص، مرورا بالقواعد ومعايير الممارسات الجيدة التي تحمي الحسابات والمعلومات، وصولا إلى العمل اليومي الآمن والتهديدات الأحدث مثل الاحتيال بالفواتير ومكالمات التزييف العميق والاستخدام غير الحذر لأدوات الذكاء الاصطناعي. ويضع اليوم الأخير المشاركين في محاكاة واقعية، ويحول الدروس إلى خطة سلامة سيبرانية شخصية وخطة للفريق تحافظ على العادات الجيدة بعد الدورة.