



دورة دفاع الموظفين ضد التصيد والسلامة السيبرانية



دورة دفاع الموظفين ضد التصيد والسلامة السيبرانية

المرجع: 157727_758 التاريخ: 5 - 9 أبريل 2027 المكان: برلين الرسوم: Euro 5700

نظرة عامة

دورة دفاع الموظفين ضد التصيد والسلامة السيبرانية دورة تأسيسية لمدة 5 أيام للموظفين وقادة الفرق وفرق خدمة العملاء والإدارة والعاملين عن بعد والمديرين، ويعود المشاركون منها بخطة عمل السلامة السيبرانية للقوى العاملة. يمارس المشاركون اكتشاف التصيد وأمن البريد الإلكتروني وحماية بيانات الاعتماد والعمل الآمن عن بعد والإبلاغ عن الحوادث وتعزيز السلوك داخل الفرق. تحول الدورة الوعي السيبراني إلى قرارات وقائية قابلة للتكرار. تطور أجائل للتدريب ممارسة دفاع الموظفين ضد التصيد والسلامة السيبرانية.

الفئة المستهدفة

- وظائف الأعمال المسؤولة عن البريد الإلكتروني والملفات المشتركة ورسائل التعاون
- الوظائف المواجهة للعملاء والمسؤولة عن حماية المحادثات والحسابات والمعلومات المقدمة
- الوظائف الإدارية المسؤولة عن المستندات والمواعيد والمدفوعات وطلبات الوصول
- وظائف قيادة الفرق المسؤولة عن تعزيز السلوك الرقمي الآمن ومسارات الإبلاغ
- وظائف العمل عن بعد والعمل الهجين المسؤولة عن الاتصال بأنظمة الأعمال خارج بيئة العمل المدارة

تفترض الدورة أن المشاركين يستخدمون أجهزة العمل أو حساباته أو بريده أو خدمات التعاون يوميا، وتستبعد هندسة الأمن وإدارة الأنظمة واختبار الاختراق والتحقيق في الحوادث.

الإدارات والقطاعات المستهدفة

تدعم الدورة الإدارات والقطاعات التي تعتمد على الأشخاص في حماية الحسابات والاتصالات والمعلومات المشتركة.

- العمليات والإدارة والمالية والموارد البشرية
- المبيعات وخدمة العملاء والمشترقات والدعم التنفيذي
- الخدمات المالية والرعاية الصحية
- التجزئة والضيافة والنقل
- التعليم والخدمات العامة والمنصات الرقمية



أهداف التعلم

بنهاية هذه الدورة، سيتمكن المشاركون من:

- تطبيق أسلوب فحص الرسائل على البريد والنصوص وطلبات التعاون
- تحليل مؤشرات التصيد وضغط الهندسة الاجتماعية ومحاولات انتحال الهوية
- استخدام ممارسات حماية بيانات الاعتماد والمصادقة متعددة العوامل والتحديث والأجهزة
- تقييم الروابط والمرفقات ورموز الاستجابة السريعة وطلبات المعلومات قبل التصرف
- تطبيق خطوات الإبلاغ عن الحوادث واحتواء الحساب
- بناء خطة عمل السلامة السيبرانية للقوى العاملة

جدول الدورة

اليوم 1: اكتشاف المخاطر السيبرانية البشرية

- خريطة سلوك وقرار التوعية بالأمن السيبراني
- قائمة مؤشرات التأثير والضغط في الهندسة الاجتماعية
- مصفوفة قنوات التصيد ومسارات الهجوم
- لوحة سيناريو انكشاف معلومات الأعمال
- أسلوب التوقف والتحقق والإبلاغ

اليوم 2: فحص الرسائل والطلبات

- قائمة التحقق من مرسل البريد والنطاق
- إجراء فحص الروابط والمرفقات ورموز الاستجابة السريعة
- دليل مؤشرات صفحات سرقة بيانات الاعتماد
- اختبار انتحال صفة التنفيذي والمورد والزميل
- ورقة تصنيف الرسائل المشبوهة



اليوم 3: حماية الحسابات والأجهزة

- ممارسة كلمات المرور القوية ومدير كلمات المرور
- دليل التحقق من طلبات المصادقة متعددة العوامل
- قائمة تحديث البرمجيات وحماية الأجهزة
- مراجعة صلاحيات البيانات المشتركة وأدوات التعاون
- قواعد التعامل مع الأجهزة المحمولة والوسائط القابلة للإزالة

اليوم 4: العمل والإبلاغ بأمان

- فحص سلامة الاتصال عن بعد والشبكات العامة
- بروتوكول التحقق من الصوت والفيديو والرسائل
- خريطة مسار الإبلاغ عن حادث تصيد
- بطاقة الاستجابة الأولى لاختراق الحساب
- خطة تعزيز السلوك والتغذية الراجعة للتعلم داخل الفريق

اليوم 5: ممارسة قرارات السلامة السيبرانية

- تمرين: فحص بريد ورابط مشبوهين
- تمرين: تحدي انتحال الهوية وطلب الدفع
- تمرين: تأمين حساب وجلسة عمل عن بعد
- تمرين: الإبلاغ عن حادث تصيد وتعزيز الدرس
- المشروع الختامي: خطة عمل السلامة السيبرانية للقوى العاملة

التمارين التطبيقية

تستخدم الدورة أنشطة مقترحة من الرعاية الصحية والخدمات المالية والتجزئة والضيافة والتعليم.

- نشاط مقترح: مقارنة الرسائل السليمة والمخادعة وفق المرسل والسياق والاستعجال والرابط والمرفق وطبيعة الطلب.
- نشاط مقترح: الاستجابة لسيناريو انتحال مورد من دون كشف بيانات الاعتماد أو الدفع أو الملفات المشتركة.
- نشاط مقترح: تطبيق فحوص حماية الحساب والعمل عن بعد على يوم عمل واقعي.
- نشاط مقترح: إعداد مسار إبلاغ وإجراء لتعزيز سلوك الفريق بعد حادث تصيد.



الأسئلة الشائعة

لمن تناسب دورة دفاع الموظفين ضد التصيد، وماذا تفترض؟

تناسب الموظفين وقادة الفرق وفرق خدمة العملاء والإدارة والعاملين عن بعد والمديرين، وتفترض استخدام حسابات العمل وأجهزته ووسائله أو خدمات التعاون.

كيف يختلف دفاع الموظفين ضد التصيد عن التدريب التقني في الأمن السيبراني؟

يطور دفاع الموظفين ضد التصيد سلوك الاكتشاف والتحقق والحماية والإبلاغ في العمل اليومي، بينما يركز التدريب التقني على تهيئة تقنيات الأمن أو مراقبتها أو اختبارها أو التحقيق فيها.

ما مؤشرات التحذير التي تدعم اكتشاف التصيد؟

تشمل مؤشرات اكتشاف التصيد اختلاف بيانات المرسل والسياق غير المعتاد والضغط والسرية والروابط أو المرفقات غير المتوقعة وطلبات بيانات الاعتماد أو تغيير الدفع أو تجاوز مسار التحقق.

كيف يبلغ الموظفون عن التصيد المشتبه به؟

يوقف الموظفون التفاعل ويحفظون الرسالة ويستخدمون مسار الإبلاغ المعتمد ويقدمون السياق اللازم ويتبعون إرشادات احتواء الحساب ويتجنبون إعادة إرسال المحتوى الضار عبر القنوات العادية.

كيف تعزز الفرق السلامة السيبرانية بعد التدريب؟

تعزز الفرق السلامة السيبرانية بمناقشات قصيرة للسيناريوهات ومسارات إبلاغ ظاهرة وسلوك إداري قدوة وتغذية راجعة سريعة وتذكير متكرر ومراجعة القرارات من دون لوم من أبلغ عن المخاوف.

الخاتمة

يعود المشاركون بخطة عمل السلامة السيبرانية للقوى العاملة التي تربط فحص الرسائل وحماية الحساب والعمل الآمن عن بعد والإبلاغ عن الحوادث وتعزيز سلوك الفريق. تحول الخطة الوعي العام إلى قرارات واضحة قابلة للتكرار في العمل اليومي. وتدعم التحقق المنتظم والإبلاغ الأسرع والتعامل الآمن مع المعلومات والتعلم العملي من الأحداث المشبوهة.