



دورة النظافة السيبرانية والسلوك الرقمي الآمن



دورة النظافة السيبرانية والسلوك الرقمي الآمن

المرجع: 157891_761 التاريخ: 2 - 6 أغسطس 2027 المكان: كوالالمبور الرسوم: Euro 5200

نظرة عامة

دورة النظافة السيبرانية والسلوك الرقمي الآمن دورة تأسيسية لمدة 5 أيام للموظفين والمتقاعدين والمشرفين والمستخدمين غير التقنيين، ويعود المشاركون منها بخطة عمل للنظافة السيبرانية في بيئة العمل. تبني الدورة عادات متكررة لحماية الحسابات والأجهزة والاتصالات والبيانات مع اكتشاف النشاط المريب والإبلاغ عنه بسرعة. وتعتمد بطاقات القرار وقوائم التحقق ومواقف العمل بدلا من الإدارة التقنية. تطور أجايل للتدريب ممارسة النظافة السيبرانية والسلوك الرقمي الآمن.

الفئة المستهدفة

- وظائف القوى العاملة المسؤولة عن الحسابات والرسائل والملفات والأنظمة المشتركة
- وظائف الإشراف المسؤولة عن ترسيخ العادات الرقمية الآمنة
- وظائف العمل عن بعد والهجين المسؤولة عن الوصول والاتصالات الآمنة
- وظائف خدمة العملاء المسؤولة عن حماية المعلومات أثناء تقديم الخدمة
- وظائف المتقاعدين والشركاء المسؤولة عن استخدام الموارد الرقمية للجهة

تفترض الدورة أن المشاركين يستخدمون حسابات أو أجهزة أو رسائل أو بيانات في العمل، وتستبعد اختبار الاختراق والهندسة الأمنية وإدارة الأنظمة والتحضير للشهادات.

الإدارات والقطاعات المستهدفة

تدعم الدورة الإدارات والقطاعات التي تعتمد على السلوك الرقمي اليومي الآمن.

- الموارد البشرية والإدارة والمالية وخدمة العملاء
- الرعاية الصحية والتعليم
- الخدمات المالية والتأمين
- التجزئة والضيافة والخدمات اللوجستية
- الخدمات العامة والعمليات المدعومة بالتقنية



أهداف التعلم

بنهاية هذه الدورة، سيتمكن المشاركون من:

- تطبيق قائمة عادات النظافة السيبرانية في العمل اليومي
- استخدام ممارسات أقوى للحسابات والمصادقة والأجهزة
- تحليل الرسائل والطلبات بحثًا عن مؤشرات التصيد
- ترتيب أولويات التعامل الآمن مع الملفات والبيانات والاتصالات
- تقييم خيارات العمل عن بعد والتصفح قبل اتخاذ الإجراء
- بناء خطة عمل للنظافة السيبرانية في بيئة العمل

جدول الدورة

اليوم 1: بناء النظافة السيبرانية اليومية

- ورقة خريطة التعرض الرقمي الشخصي
- قائمة خط الأساس لعادات النظافة السيبرانية
- مصفوفة مسؤوليات الحسابات والأجهزة
- خريطة قرار الخطأ البشري والتهديد
- بطاقة تعهد السلوك الرقمي الآمن

اليوم 2: حماية الحسابات والأجهزة

- ممارسة عبارات المرور القوية ومدير كلمات المرور
- دليل قرار المصادقة متعددة العوامل
- قائمة عادة تحديث البرمجيات والتصحيات
- روتين قفل الجهاز وتخزينه والتخلص منه
- بطاقة إجراء فقد الجهاز واستعادة الحساب



اليوم 3: اكتشاف الهندسة الاجتماعية

- أسلوب فحص مؤشرات التصيد
- قائمة التحقق من المرسل والربط والمرفق
- خريطة محفزات الاستعجال والسلطة والعاطفة
- شجرة قرار الخداع الصوتي والرسائل والرموز
- مسار الإبلاغ عن الاتصالات المريبة

اليوم 4: التعامل الآمن مع البيانات والعمل عن بعد

- بطاقة قرار حساسية البيانات ومشاركتها
- قائمة التصفح والتنزيل الآمن
- دليل مخاطر الشبكات العامة والوصول عن بعد
- مراجعة صلاحيات الملفات السحابية والتعاون
- روتين خصوصية مساحة العمل وحماية الشاشة

اليوم 5: ممارسة السلوك الرقمي الآمن

- تمرين: تشخيص فجوات عادات الحسابات والأجهزة
- تمرين: تقييم مواقف التصيد والهندسة الاجتماعية
- تمرين: اختيار إجراءات آمنة للبيانات والعمل عن بعد
- تمرين: التدريب على الإبلاغ السريع عن الحوادث
- المشروع الختامي: خطة عمل للنظافة السيبرانية في بيئة العمل

التمارين التطبيقية

تستخدم الدورة أنشطة مقترحة من المكاتب والرعاية الصحية والتجزئة والتعليم والعمل عن بعد.

- نشاط مقترح: فحص الرسائل والروابط والمرفقات والطلبات باستخدام بطاقة قرار التصيد.
- نشاط مقترح: تدقيق عادات الحسابات والمصادقة والتحديث والنسخ الاحتياطي وقفل الأجهزة.
- نشاط مقترح: اختيار إجراءات آمنة للمشاركة والتصفح والشبكات والتعاون في مواقف العمل.
- نشاط مقترح: ممارسة الإبلاغ عن حدث مريب بالمعلومات التي يحتاجها المستجيبون.



الأسئلة الشائعة

لمن تناسب دورة النظافة السيبرانية، وماذا تفترض؟

تناسب الموظفين والمتقاعدين والمشرفين والمستخدمين غير التقنيين، وتفترض الاستخدام المعتاد لحسابات العمل أو أجهزته أو اتصالاته أو بياناته.

كيف تختلف النظافة السيبرانية عن التدريب التقني في الأمن السيبراني؟

تبني النظافة السيبرانية سلوكيات وقرارات متكررة للمستخدم، بينما يركز التدريب التقني على إعداد الأنظمة أو اختبارها أو مراقبتها أو الدفاع عنها.

ما عادات النظافة السيبرانية التي تقلل مخاطر الحسابات اليومية؟

تشمل العادات عبارات مرور منفصلة ومدير كلمات المرور والمصادقة متعددة العوامل والتحديثات السريعة ومراجعة تسجيل الدخول وقفل الجهاز والإبلاغ الفوري عن طلبات الوصول غير المتوقعة.

كيف يتعامل السلوك الرقمي الآمن مع الرسائل المريبة؟

يتوقف المستخدم قبل التنفيذ ويتحقق من المرسل والسياق عبر قناة موثوقة ويتجنب الروابط والمرفقات غير المعروفة ويحفظ التفاصيل اللازمة ويتبع مسار الإبلاغ.

ماذا تتضمن خطة عمل النظافة السيبرانية في بيئة العمل؟

تسجل الخطة العادات ذات الأولوية والإجراءات المسؤولة ومسارات الإبلاغ ونقاط المراجعة والتغييرات المطلوبة للحسابات والأجهزة والاتصالات والبيانات والتصفح والعمل عن بعد.

الخاتمة

يعود المشاركون بخطة عمل للنظافة السيبرانية في بيئة العمل تربط حماية الحسابات والعناية بالأجهزة وقرارات التصيد والتعامل مع البيانات والعمل عن بعد والإبلاغ. تحول الخطة الاحتياطات المتفرقة إلى ممارسات يومية ظاهرة. وتدعم خيارات أكثر أماناً وتصعيداً أسرع وتوقعات مشتركة ومراجعة دورية لفجوات السلوك.