JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

كتيّب الدورة

دورة متقدمة في ثقافة الوعي بالأمن السيبراني للمديرين

info@jupiterprime.uk

jupiterprime.uk

مسجّلة في المملكة المتحدة والمملكة العربية السعودية

دورة متقدمة في ثقافة الوعي بالأمن السيبراني للمديرين

ثقافة الوعي بالأمن السيبراني للمديرين دورة تدريبية متقدمة مدتها أسبوعين لمديري الأقسام وشركاء الموارد البشرية ورؤساء الإدارات الذين يشكلون طريقة تعامل الموظفين مع البريد وكلمات المرور والملفات الحساسة، وتنتهي بمخطط حملة توعية للفريق جاهز للإطلاق. فمعظم الاختراقات ما زالت تبدأ بموظف ينقر رابطا أو يشارك ملفا أو يعيد استخدام كلمة مرور، لذا باتت العادات اليومية تحدد حجم الانكشاف. وتقدم جوبيتر برايم للتدريب هذه الدورة للمديرين المسؤولين عن ذلك السلوك.

لماذا تهم ثقافة الوعي بالأمن السيبراني الآن

تلتقي في هذا الموضوع ثلاثة ضغوط: رسائل التصيد وانتحال الشخصية التي باتت تقلد كبار التنفيذيين والموردين بإتقان، والعمل الهجين الذي ينقل الملفات الحساسة إلى شبكات منزلية وأجهزة شخصية، ومجالس إدارة ومدققون يطلبون دليلا على تحسن سلوك الموظفين لا سجلا بعدد العروض التي شوهدت. المنشأة ذات الثقافة الأمنية الراسخة تتلقى بلاغات الرسائل المريبة خلال دقائق، أما غيرها فتكتشف الاحتيال بعد أسابيع. وتستند الدورة إلى متطلبات الوعي والكفاءة في المعيار الدولي ISO/IEC 27001:2022 لأنظمة إدارة أمن المعلومات.

المستفيدون من ثقافة الوعي بالأمن السيبراني

- مديرو الأقسام الذين يحددون التوقعات اليومية لتعامل فرقهم مع البريد والملفات والأجهزة
- شركاء الموارد البشرية الذين يدمجون السلوك الأمني في التهيئة والتقييم وسياسة الانضباط
- رؤساء الإدارات الذين يعتمدون طلبات الصلاحيات ومشاركة المعلومات مع الأطراف الخارجية
- مسؤولو الاتصال الداخلي الذين يصوغون نبرة الرسائل الأمنية وتوقيتها
- منسقو التوعية الذين يجدولون المحاكاة ويرفعون اتجاهات السلوك إلى القيادة

تجني الطبقة الإدارية الفائدة الكبرى حين توفد مديرين من عدة إدارات معا، لأن توحيد التوقعات بين الوظائف يمنع وصول رسائل أمنية متضاربة إلى الموظفين.

قدرات ثقافة الوعي بالأمن السيبراني

يغادر المشاركون قادرين على تحويل التوقعات الأمنية إلى عادات يحافظ عليها الموظفون فعلا، وعلى إثبات هذا التحول بالأرقام.

- تقييم الثقافة الأمنية القائمة عبر الاستبيانات وبلاغات الحوادث ونتائج المحاكاة — أولويات ميزانية التوعية
- تصميم محاكاة تصيد تطابق الطعوم الحقيقية التي تصل كل إدارة — مالكو الحملات والموارد البشرية
- تحديد قواعد كلمات المرور والتحقق المتعدد والصلاحيات التي يمكن للموظفين اتباعها — تقنية المعلومات ومديرو الأقسام
- تطبيق قواعد تصنيف المعلومات وتداولها على المهام اليومية — مالكو المعلومات ومسؤولو الامتثال
- بناء مقاييس سلوكية تتتبع معدلات الإبلاغ والنقرات المتكررة — الرعاة التنفيذيون
- إيصال الرسائل الأمنية عبر المديرين بدلا من البريد الجماعي — ثقة الموظفين وتفاعلهم

مصطلحات ثقافة الوعي بالأمن السيبراني الأساسية

- الهندسة الاجتماعية — التلاعب بالأشخاص لكشف معلومات أو القيام بتصرف غير آمن، غالبا بانتحال صفة زميل أو مورد أو جهة موثوقة.
- محاكاة التصيد — رسالة هجوم وهمية مضبوطة ترسل إلى الموظفين لقياس من ينقر ومن يبلغ وأين يلزم التوجيه.
- اختراق البريد الإلكتروني للأعمال — احتيال ينتحل فيه المهاجم صفة تنفيذي أو مورد لتحويل الدفعات أو الحصول على ملفات حساسة.
- التحقق متعدد العوامل — طريقة دخول تتطلب إثباتين أو أكثر للهوية مثل كلمة المرور وإشعار على الهاتف.
- معدل الإبلاغ — نسبة الرسائل المريبة الحقيقية أو المحاكاة التي يبلغ عنها الموظفون لفريق الأمن بدلا من تجاهلها.
- الثقافة العادلة — نهج يعامل الأخطاء غير المقصودة فرصا للتعلم مع محاسبة السلوك المتعمد أو المتهور.

ثقافة الوعي بالأمن السيبراني يوما بيوم

اليوم 1: الجانب البشري من المخاطر السيبرانية

- العامل البشري في أنماط الاختراق — مواضع انكشاف المنشأة بسبب سلوك الموظفين
- نماذج نضج الثقافة الأمنية — نقطة البداية لكل إدارة
- متطلبات الوعي في ISO/IEC 27001:2022 — الأدلة التي سيطلبها المدققون
- خريطة مساءلة المديرين — من يملك كل عادة أمنية
- استبيان تشخيص الثقافة — الاتجاهات الأساسية والنقاط العمياء

اليوم 2: أساليب التصيد والهندسة الاجتماعية

- تشريح طعم التصيد — إشارات يلتقطها الموظف في ثوان
- الاحتيال عبر المكالمات والرسائل النصية — خطوات التحقق قبل التصرف
- سيناريوهات اختراق البريد الإلكتروني للأعمال — ضوابط اعتماد الدفعات
- حالات الذريعة والتسلل خلف الموظفين — ضوابط الاستقبال والدخول المادي
- مخاطر الانتحال بالتزييف العميق — قواعد معاودة الاتصال للطلبات العليا

اليوم 3: كلمات المرور والهوية ونظافة الصلاحيات

- سياسة عبارات المرور ومديري كلمات المرور — سهولة الاستخدام مقابل القوة
- تعميم التحقق متعدد العوامل — نقاط المقاومة والاستثناءات
- مراجعات صلاحيات المنضمين والمنتقلين والمغادرين — واجبات اعتماد المدير
- إلغاء الحسابات المشتركة — المساءلة عن كل عملية دخول
- طلبات الصلاحيات المميزة — معايير الاعتماد لرؤساء الإدارات

اليوم 4: تداول المعلومات الحساسة يوميا

- تصنيفات المعلومات — خيارات الموظف عند حفظ الملفات
- المشاركة الآمنة للملفات وتشفير البريد — قواعد التعاون الخارجي
- عادات المكتب النظيف وقفل الشاشة — الانكشاف في المكتب والمنزل
- الوسائط القابلة للإزالة والتخزين السحابي الشخصي — مسارات التسرب الواجب إغلاقها
- إتلاف السجلات والاحتفاظ بها — خيارات إتلاف الورق والأجهزة

اليوم 5: العمل الهجين وأمن الأجهزة

- إرشادات الشبكة المنزلية وشبكات الاتصال العامة — شروط الوصول عن بعد
- اتفاقيات استخدام الأجهزة الشخصية — مقايضات الخصوصية والتحكم
- عادات التحديث وتصحيح البرمجيات — مسؤوليات الموظف على جهازه
- إجراء الإبلاغ عن الأجهزة المفقودة — سرعة قرار المسح عن بعد
- إعدادات منصات التعاون — حدود وصول الضيوف ومشاركة الروابط

اليوم 6: العلوم السلوكية لبناء العادات الأمنية

- أساليب التحفيز والخيارات الافتراضية — جعل الخيار الآمن هو الأسهل
- حلقات العادة والتذكيرات — توقيت التنبيهات الأمنية
- شبكات سفراء الأمن — تأثير الأقران داخل الإدارات
- الثقافة العادلة والإبلاغ دون خوف — مواءمة سياسة الانضباط
- أنظمة التلعيب والتقدير — التحفيز دون إرهاق

اليوم 7: تصميم محاكاة التصيد

- أخلاقيات المحاكاة وقواعد الموافقة — الثقة بين الموظفين وفريق الأمن
- تدرج صعوبة القوالب — مقارنة عادلة بين الإدارات
- التعلم المصغر في صفحة الهبوط — التوجيه لحظة النقر
- مسار دعم المتكررين في النقر — التوجيه مقابل التصعيد
- تبني زر الإبلاغ — تحويل الموظفين إلى أجهزة إنذار مبكر

اليوم 8: قياس السلوك الأمني

- إطار المقاييس السلوكية — مؤشرات النقر والإبلاغ وزمن الاستجابة
- لوحة التوعية للتنفيذيين — اتجاهات تستحق انتباه مجلس الإدارة
- وسم السبب الجذري للحوادث — ربط الخطأ البشري بالتوجيه
- الاستبيانات النبضية ومجموعات التركيز — تحول الاتجاهات بمرور الوقت
- مقارنة حالات من المصارف والرعاية الصحية — أنماط الثقافة القطاعية

اليوم 9: إيصال الأمن عبر المديرين

- صياغة الرسائل لجماهير مختلفة — موظفو الميدان والمكاتب والقيادة
- نصوص إحاطة الفريق — لحظات أمنية من خمس دقائق في الاجتماعات
- وحدة الأمن في برنامج التهيئة — توقعات الأسبوع الأول للمنضمين الجدد
- سرد قصص الحوادث — دروس تشارك دون لوم
- تخطيط تقويم الحملات — موضوعات موزعة على العام

اليوم 10: ممارسة مخطط حملة توعية الفريق

- تطبيق تشخيص الثقافة على إدارة حقيقية — السلوكيات ذات الأولوية
- صياغة خطة المحاكاة — القوالب والتوقيت وخطوات التوجيه
- اختيار المقاييس ونموذج اللوحة — صيغة التقرير للراعي
- مراجعة الأقران لرسائل الحملة — فحص الوضوح والنبرة
- استكمال مخطط حملة توعية الفريق — المسؤولون والمراحل والمقاييس

تطبيق ثقافة الوعي بالأمن السيبراني بعد الدورة

- تنفيذ محاكاة تصيد مرجعية لإدارة واحدة باستخدام القوالب المتدرجة ومسار التوجيه الذي جرى التدرب عليه
- تخصيص لحظة أمنية في كل اجتماع أسبوعي للفريق مدة شهر وتتبع معدلات الإبلاغ على لوحة المقاييس السلوكية

أسئلة حول ثقافة الوعي بالأمن السيبراني

ما ثقافة الوعي بالأمن السيبراني ولماذا تهم الآن؟

ثقافة الوعي بالأمن السيبراني هي مجموعة العادات المشتركة التي تدفع الموظفين إلى رصد التهديدات والإبلاغ عنها وتجنبها دون تذكير مستمر. وتهم الآن لأن التصيد والانتحال يستهدفان الأشخاص أولا، والعمل الهجين يوسع مواضع وقوع الأخطاء.

من يستفيد أكثر من دورة ثقافة الوعي بالأمن السيبراني للمديرين؟

يستفيد أكثر مديرو الأقسام وشركاء الموارد البشرية ورؤساء الإدارات ومنسقو التوعية. وتزداد فائدتك إن كنت تعتمد الصلاحيات أو تضع روتين الفريق أو تتابع سلوك الموظفين، لأن إشاراتك اليومية تشكل السلوك الأمني أكثر من التعلم الإلكتروني السنوي.

كيف تختلف دورة ثقافة الوعي بالأمن السيبراني عن دورة التوعية الأساسية للموظفين؟

تعد الدورة المديرين لقيادة تغيير السلوك بدلا من تعليم الموظفين رصد التهديدات فحسب. فأنت تصمم المحاكاة والمقاييس والرسائل للآخرين، وتربط التوجيه وسياسات الموارد البشرية والتقارير في جهد متواصل واحد.

ماذا تعود به من دورة ثقافة الوعي بالأمن السيبراني؟

تعود بمخطط حملة لفريقك. ويحدد السلوكيات ذات الأولوية وجدول المحاكاة وخطوات التوجيه وموضوعات التواصل والمقاييس التي سيطلع عليها الراعي، لتبدأ الأنشطة الأولى خلال أسابيع.

ثقافة الوعي بالأمن السيبراني: الطريق إلى الأمام

يوجه مخطط حملة توعية الفريق أولا اختيار السلوك المستهدف في الربع الافتتاحي وطريقة تدرج المحاكاة الأولى. ويديره مديرو الأقسام، وتواعم الموارد البشرية سياساتها معه، ويقرأ الرعاة التنفيذيون لوحته. وبعد الدورة الأولى من الحملة يستحق مسار دعم المتكررين في النقر مراجعة جديدة، إذ تكشف النتائج المبكرة هل يغير الدعم أم التصعيد السلوك أسرع.