سياسة أفضل الممارسات الممكنة للبريد الإلكتروني

محلل الحوادث السيبرانية: فاطمة الشهري

مقدمة

تهدف هذه الخطة إلى رفع مستوى الوعي الأمني لدى موظفي شركة STC وتوفير إطار عمل شامل لسياسة أمن البريد الإلكتروني، وذلك لحماية الشركة من التهديدات السيبرانية المتزايدة.

الهدف:

- زيادة وعي الموظفين بالمخاطر السيبرانية الشائعة.
- تعزيز فهم الموظفين لأفضل الممارسات في الأمن السيبراني.
- تشجيع الموظفين على الإبلاغ عن أي نشاط مشبوه.

الأنشطة:

- **ورش عمل تفاعلية :**تنظيم ورش عمل دورية لتغطية مواضيع مختلفة مثل:
  - تهديدات التصيد الاحتيالي
  - حماية كلمات المرور
  - التعرف على البرامج الضارة
  - حماية الأجهزة الشخصية
- **برامج تدريبية عبر الإنترنت :**توفير برامج تدريبية عبر الإنترنت يمكن للموظفين الوصول إليها في أي وقت.
- **حملات توعية :**إطلاق حملات توعية دورية عبر البريد الإلكتروني، لوحات الإعلانات، والشاشات الداخلية.
- **سيناريوهات هجوم محاكاة :**إجراء تدريبات محاكاة لهجمات سيبرانية لتقييم استجابة الموظفين.

التقييم:

- **استبيانات :**إجراء استبيانات دورية لقياس مدى فعالية برامج التوعية.
- **تتبع الحوادث :**تتبع الحوادث الأمنية لتحديد نقاط الضعف وتحسين برامج التوعية.

سياسة أمن البريد الإلكتروني

الغرض:

حماية أصول الشركة من خلال ضمان استخدام آمن ومسؤول للبريد الإلكتروني.

الهدف:

- منع الوصول غير المصرح به إلى البريد الإلكتروني.
- حماية البيانات الحساسة من التسرب.
- الحد من انتشار البرامج الضارة.
- ضمان الامتثال للوائح التنظيمية.

نطاق السياسة:

تنطبق هذه السياسة على جميع موظفي الشركة الذين يستخدمون نظام البريد الإلكتروني الخاص بالشركة.

مسؤولية الموظفين:

- الحفاظ على سرية كلمات المرور.
- عدم فتح مرفقات من مصادر غير موثوقة.
- عدم النقر على الروابط المشبوهة في رسائل البريد الإلكتروني.
- الإبلاغ عن أي نشاط مشبوه إلى فريق أمن المعلومات.
- عدم استخدام البريد الإلكتروني لأغراض شخصية غير ذات صلة بالعمل.

مسؤولية موظفي أمن المعلومات:

- تنفيذ وتطبيق سياسة أمن البريد الإلكتروني.
- توفير التدريب اللازم للموظفين.
- مراقبة أنظمة البريد الإلكتروني بحثًا عن أي تهديدات.
- الاستجابة للحوادث الأمنية.

نص السياسة:

١. **استخدام البريد الإلكتروني :**يجب استخدام البريد الإلكتروني لأغراض العمل فقط.
٢. **كلمات المرور :**يجب على الموظفين اختيار كلمات مرور قوية وفريدة لكل حساب، وتغييرها بانتظام.
٣. **المرفقات :**يجب توخي الحذر الشديد عند فتح المرفقات، خاصة تلك التي تأتي من مصادر غير معروفة.
٤. **الروابط :**يجب التحقق من صحة أي رابط قبل النقر عليه.
٥. **المعلومات الحساسة :**يجب تجنب إرسال المعلومات الحساسة عبر البريد الإلكتروني غير المشفر.
٦. **البرامج الضارة :**يجب على الموظفين تجنب تنزيل وتثبيت أي برامج أو ملحقات غير مصرح بها.
٧. **الإبلاغ عن الحوادث :**يجب على الموظفين الإبلاغ عن أي نشاط مشبوه إلى فريق أمن المعلومات على الفور.

الخلاصة:

تعتبر التوعية السيبرانية وسياسة أمن البريد الإلكتروني جزءًا أساسيًا من حماية أصول الشركة .من خلال تنفيذ هذه الخطة والسياسة، يمكن لشركة STC تقليل المخاطر السيبرانية وتحسين أمن المعلومات.

الخطة التوعوية

الاسم: فاطمة الشهري	البريد الإلكتروني: rfyfa19@gmail.com
التاريخ: 31/07/2024	المدة الزمنية للحملة: شهر
الهدف العام: رفع مستوى الوعي الأمني لدى موظفي شركة STC وتوفير إطار عمل شامل لسياسة أمن البريد الإلكتروني، وذلك لحماية الشركة من التهديدات السيبرانية المتزايدة.	
تاريخ نهاية الحملة: 25/09/2024	تاريخ بداية الحملة: 01/09/2024

#	نوع التوعوية	الفئة المستهدفة	المحتوى التوعوي	تاريخ البداية	تاريخ النهاية	الهدف
١	ورش عمل تفاعلية	جميع الموظفين	تهديدات التصيد الاحتيالي - حماية كلمات المرور – الاستجابة للحوادث الأمنية – حماية الأجهزة الشخصية	01/09/2024	04/09/2024	نشر التوعية للحوادث السيبرانية
٢	برامج تدريبية عبر الإنترنت	جميع الموظفين	حماية الأجهزة والشبكات - حماية البيانات - الهندسة الاجتماعية والتصيد الاحتيالي – امن البريد الإلكتروني	08/09/2024	11/09/2024	نشر التوعية للحوادث السيبرانية
٣	سيناريوهات محاكاة هجوم	جميع الموظفين	هجمات التصيد الاحتيالي- هجمات الهندسة الاجتماعية - هجمات البرامج الضارة – هجمات الفدية	15/09/2024	18/09/2024	نشر التوعية للحوادث السيبرانية
٤	حملات رسائل إرشادية	جميع الموظفين	الاستخدام الآمن للبريد الإلكتروني – البرامج الضارة- الهندسة الاجتماعية والتصيد الاحتيالي – أمن الأجهزة المحمولة	22/09/2024	25/09/2024	نشر التوعية للحوادث السيبرانية

ورش العمل التفاعلية 01/09/2024 – 04/09/2024

يهدف محتوى هذه الورش إلى تزويد الموظفين بالمعرفة والمهارات اللازمة لحماية أنفسهم والشركة من التهديدات السيبرانية الشائعة.

اليوم الأول: تهديدات التصيد الاحتيالي 01/09/2024

- **ما هو التصيد الاحتيالي؟** تعريف التصيد الاحتيالي وأمثلة حقيقية على هجمات التصيد التي تستهدف الشركات.
- **كيف يعمل التصيد الاحتيالي؟** شرح آليات عمل هجمات التصيد، من إنشاء رسائل البريد الإلكتروني الوهمية إلى استهداف المستخدمين.
- **كيفية التعرف على رسائل التصيد:** تدريب الموظفين على التعرف على العلامات التحذيرية لرسائل التصيد، مثل الأخطاء الإملائية، الروابط المشبوهة، ومطالبات تقديم معلومات شخصية حساسة.
- **كيفية التصرف عند تلقي رسالة تصيد: تقديم** إرشادات واضحة حول كيفية التعامل مع رسائل التصيد، مثل عدم النقر على الروابط أو فتح المرفقات، والإبلاغ عن الرسالة.

اليوم الثاني: حماية كلمات المرور 02/09/2024

- **أهمية كلمات المرور القوية:** شرح أهمية استخدام كلمات مرور قوية وفريدة لكل حساب.
- **ممارسات جيدة لإدارة كلمات المرور:** تقديم نصائح حول كيفية إنشاء كلمات مرور قوية، وتجنب استخدام كلمات المرور الشائعة، واستخدام أداة إدارة كلمات المرور.
- **الهجمات التي تستهدف كلمات المرور:** شرح أنواع الهجمات التي تستهدف كلمات المرور، مثل هجمات القوة الغاشمة وهجمات الرش.

اليوم الثالث: الاستجابة للحوادث الأمنية 03/09/2024

- **الإبلاغ عن الحوادث الأمنية:** شرح أهمية الإبلاغ الفوري عن أي نشاط مشبوه.
- **إجراءات الاستجابة للحوادث:** شرح الإجراءات التي يجب اتخاذها عند حدوث حادثة أمنية، مثل قطع الاتصال بالإنترنت، تغيير كلمات المرور، والاتصال بفريق أمن المعلومات.

اليوم الرابع: حماية الأجهزة الشخصية 04/09/2024

- **أهمية حماية الأجهزة الشخصية:** شرح أهمية حماية الأجهزة الشخصية، مثل الهواتف المحمولة وأجهزة الكمبيوتر المحمولة، من الهجمات السيبرانية.

- **أفضل الممارسات لحماية الأجهزة الشخصية:** تقديم نصائح حول كيفية حماية الأجهزة الشخصية، مثل استخدام كلمات مرور قوية، وتجنب الاتصال بشبكات واي فاي عامة غير آمنة، وتجنب تثبيت تطبيقات من مصادر غير موثوقة.

برامج تدريبية عبر الإنترنت 11/09/2024 – 08/09/2024

يهدف محتوى هذه البرامج إلى تزويد الموظفين بمعرفة ومهارات شاملة في مجال الأمن السيبراني، وذلك من خلال منصة تعليمية مرنة يمكن الوصول إليها في أي وقت ومكان.

اليوم الأول: حماية الأجهزة والشبكات 08/09/2024

- **أمن الأجهزة:** كيفية حماية أجهزة الكمبيوتر، الهواتف المحمولة، والأجهزة اللوحية من التهديدات.
- **أمن الشبكات:** فهم أساسيات أمن الشبكات، مثل جدران الحماية، ونظم الكشف عن الاختراقات.
- **أمن الواي فاي:** نصائح لحماية الشبكات اللاسلكية المنزلية والعملية.

اليوم الثاني: حماية البيانات 09/09/2024

- **أنواع البيانات الحساسة:** التعرف على أنواع البيانات الحساسة التي تحتاج إلى حماية إضافية، مثل البيانات الشخصية والمالية.
- **طرق حماية البيانات:** شرح طرق حماية البيانات المختلفة، مثل التشفير، والوصول المحدود، والنسخ الاحتياطي.
- **اللوائح المتعلقة بحماية البيانات:** التعريف باللوائح والقوانين المتعلقة بحماية البيانات.

اليوم الثالث: الهندسة الاجتماعي والتصيد الاحتيالي 10/09/2024

ما هي الهندسة الاجتماعية؟ تعريف الهندسة الاجتماعية وأمثلة على أساليبها المختلفة.
كيف تتعرف على هجمات التصيد الاحتيالي؟ تدريب الموظفين على التعرف على العلامات التحذيرية لرسائل التصيد.
كيفية التصرف عند التعرض لهجوم هندسة اجتماعية: تقديم نصائح حول كيفية التصرف عند التعرض لمحاولة احتيال.

اليوم الرابع: أمن البريد الإلكتروني 11/09/2024

أمن البريد الإلكتروني: أهمية حماية البريد الإلكتروني من التهديدات.
أفضل الممارسات في استخدام البريد الإلكتروني: نصائح حول كيفية استخدام البريد الإلكتروني بأمان، مثل عدم فتح مرفقات من مصادر غير موثوقة وتجنب النقر على الروابط المشبوهة.
حماية ضد رسائل البريد الإلكتروني الضارة: شرح طرق حماية البريد الإلكتروني من الفيروسات والبرامج الضارة.

سيناريوهات محاكاة هجوم 18/09/2024 – 15/09/2024

تهدف سيناريوهات محاكاة الهجوم إلى رفع مستوى الوعي الأمني لدى الموظفين وتدريبهم على التعامل مع الحوادث الأمنية بشكل فعال .يمكن تصميم هذه السيناريوهات لتغطية مجموعة واسعة من التهديدات الشائعة، مثل:

- **هجمات التصيد الاحتيالي :**محاكاة رسائل بريد إلكتروني وهمية تحتوي على روابط أو مرفقات ضارة.
- **هجمات الهندسة الاجتماعية :**محاكاة مكالمات هاتفية أو رسائل نصية من أشخاص يدعون أنهم من الشركة أو من مصادر موثوقة.
- **هجمات البرامج الضارة :**محاكاة تنزيل برامج ضارة عن طريق النقر على روابط أو فتح مرفقات.
- **هجمات الفدية :**محاكاة تشفير الملفات المهمة للمستخدم.
- **هجمات الوصول غير المصرح به :**محاكاة محاولات الوصول غير المصرح به إلى الأنظمة أو البيانات.

أهداف سيناريوهات المحاكاة:

- **تقييم مستوى الوعي الأمني :**قياس مدى فهم الموظفين للمخاطر الأمنية وكيفية التعامل معها.
- **تحسين مهارات اتخاذ القرار :**تدريب الموظفين على اتخاذ القرارات الصحيحة في مواجهة تهديدات حقيقية.
- **اختبار خطط الاستجابة للحوادث :**تقييم فعالية خطط الاستجابة للحوادث الأمنية.
- **تعزيز ثقافة الأمن :**تشجيع الموظفين على الإبلاغ عن أي نشاط مشبوه.

مكونات سيناريوهات المحاكاة:

- **السيناريو :**وصف مفصل للحادثة الأمنية، بما في ذلك الشخصيات المعنية، والوقت والمكان، والهدف من الهجوم.
- **دور المشاركين :**تحديد دور كل مشارك في السيناريو، سواء كان ضحية أو شاهد أو مستجيب.
- **الأدوات والموارد :**توفير الأدوات والموارد اللازمة للمشاركين، مثل رسائل البريد الإلكتروني الوهمية، والمواقع الإلكترونية المزيفة.
- **تقييم الأداء :**تقييم أداء المشاركين بناءً على قراراتهم وإجراءاتهم.
- **التغذية الراجعة :**تقديم تغذية راجعة للمشاركين حول أدائهم واقتراحات لتحسينه.

محتوى توعوي يجب تضمينه في السيناريوهات:

- **أهمية الإبلاغ عن الحوادث :**تشجيع الموظفين على الإبلاغ عن أي نشاط مشبوه فوراً.
- **أفضل الممارسات الأمنية :**تذكير الموظفين بأهمية اتباع أفضل الممارسات الأمنية، مثل استخدام كلمات مرور قوية وتجنب فتح مرفقات البريد الإلكتروني المشبوهة.
- **خطوات الاستجابة للحوادث :**شرح الإجراءات التي يجب اتخاذها عند حدوث حادثة أمنية، مثل قطع الاتصال بالإنترنت، وتغيير كلمات المرور، والإبلاغ عن الحادثة لفريق أمن المعلومات.
- **التكاليف المترتبة على الهجمات السيبرانية :**شرح التكاليف المادية والمالية التي يمكن أن تترتب على الهجمات السيبرانية.

أمثلة على سيناريوهات محاكاة:

- **سيناريو تصيد احتيالي :**تلقي الموظف رسالة بريد إلكتروني مزيفة تطلب منه تحديث كلمة سره.
- **سيناريو فقدان الجهاز :**فقدان أحد الموظفين لجهازه المحمول الذي يحتوي على بيانات حساسة.
- **سيناريو هجوم فدية :**تشفير جميع الملفات على جهاز كمبيوتر تابع للموظف.

من خلال تنفيذ سيناريوهات محاكاة الهجوم بشكل منتظم، يمكن للشركات تقوية دفاعاتها السيبرانية وتحسين قدرتها على التعامل مع التهديدات المتزايدة.

حملات رسائل ارشادية 22/09/2024 – 25/09/2024

تهدف الحملات الرسائل الإرشادية إلى نشر الوعي الأمني بين الموظفين وتزويدهم بالمعلومات اللازمة لحماية أنفسهم والشركة من التهديدات السيبرانية .

اليوم الأول: التصيد الاحتيالي 22/09/2024

- كيفية التعرف على رسائل التصيد الاحتيالية.
- عدم النقر على الروابط المشبوهة أو فتح المرفقات غير المعروفة.
- الإبلاغ عن رسائل التصيد الاحتيالية.

اليوم الثاني: البرامج الضارة 23/09/2024

- أنواع البرامج الضارة الشائعة (فيروسات، ديدان، فدية).
- كيفية حماية الأجهزة من البرامج الضارة.
- تجنب تنزيل وتثبيت البرامج من مصادر غير موثوقة.

اليوم الثالث: الاستجابة للحوادث الأمنية 24/09/2024

- الإبلاغ عن أي نشاط مشبوه فوراً.
- اتباع إجراءات الاستجابة للحوادث.

اليوم الرابع: أمن الأجهزة المحمولة 25/09/2024

- حماية الهواتف الذكية والأجهزة اللوحية من التهديدات.
- تثبيت تطبيقات أمنية على الأجهزة المحمولة.
- عمل نسخ احتياطي للبيانات.