الأمن السيبراني للمؤسسات الأصغر حجمًا

# قائمة التدقيق الخاصة بمدير أمن البيانات: حماية عملائك

## تقديم المشورة للعملاء والموظفين بشأن حماية البيانات على المستوى الفردي

☐ **زود الموظفين والعملاء بالمبادئ التوجيهية الشخصية التالية الواجب اتباعها لحماية بياناتهم بشكل أفضل:**

- استخدم كلمات مرور قوية على جميع الأجهزة الشخصية والمهنية، وفكر في استخدام مدير كلمة المرور.
- حافظ على تحديث أنظمة التشغيل والبرامج والتطبيقات الأخرى على جميع أجهزة الكمبيوتر والأجهزة المحمولة.
- قم بتثبيت برامج مكافحة الفيروسات ومكافحة البرامج الضارة ومكافحة برامج الفدية التي تمنع البرامج الضارة وتكتشفها وتزيلها.
- استخدم برنامج جدار حماية لمنع الوصول غير المصرح به إلى جهاز الكمبيوتر.
- استخدم منتجات الأمان فقط من الشركات ذات السمعة الطيبة. اقرأ المراجعات من الكمبيوتر ومنشورات المستهلكين وانظر في استشارة الشركة المصنعة لجهاز الكمبيوتر أو نظام التشغيل.
- كن حذرًا عند التعامل مع المعلومات الحساسة. لا ترسل كلمات مرور الحساب المصرفي أو بيانات الحساب المالي الحساسة الأخرى عبر البريد الإلكتروني غير المشفر.
- تعامل بذكاء عندما يتعلق الأمر بمكان اتصالك بالإنترنت وكيفية قيامك بذلك لأغراض الخدمات المصرفية أو الاتصالات الأخرى التي تتضمن معلومات شخصية حساسة.
- لا تفتح مرفقات البريد الإلكتروني على الفور أو تنقر على روابط في رسائل بريد إلكتروني غير مرغوب فيها أو مشبوهة. توقف. فكر. انقر.
- كن حذرًا إذا اتصل بك شخص ما على نحو غير متوقع عبر الإنترنت أو عبر الهاتف وطلب معلوماتك الشخصية. حتى عند الاتصال بالعناوين المعروفة، حاول الحد من مشاركة المعلومات الشخصية عبر البريد الإلكتروني.
- تذكر أنه لن تقوم أي مؤسسة مالية بإرسال بريد إلكتروني لك أو الاتصال بك وطلب معلومات سرية لديها بالفعل.
- افترض أن طلب الحصول على معلومات من بنك لم تقم مطلقًا بفتح حساب فيه هو عملية احتيال.
- تحقق من صحة رسالة بريد إلكتروني مشبوهة أو مربع منبثق قبل تقديم المعلومات الشخصية. انتبه جيدًا إلى عنوان البريد الإلكتروني.

## إدارة الحسابات

☐ **اطلب من العملاء استخدام معرفات مستخدمين وكلمات مرور قوية لتسجيل الدخول إلى خدماتك. أبلغهم بعدم استخدام كلمة المرور نفسها التي يستخدمونها للحسابات الأخرى.**

☐ **استخدم التحقق الفوري والتحقق في الوقت الفعلي والتحقق من الإيداع التجريبي والتحقق من الهوية و/أو أسئلة المصادقة للتحقق من صحة العملاء الحقيقيين وتقليل فرصة الاحتيال.**

☐ **اعرض أو اطلب، بشكل مثالي، مصادقة ثنائية للعملاء لاستخدامها عند تسجيل الدخول إلى خدماتك.**

☐ **تحقق بانتظام من حسابات المستخدم لاكتشاف علامات الاحتيال.**

## حماية البيانات

- ☐ **فكّر في بيانات العملاء التي يجب على مؤسستك جمعها لتقديم خدماتها، وكن حذرًا من جمع أي بيانات خاصة بالعملاء تتجاوز ذلك.**
- ☐ **ضع سياسات الاحتفاظ بالبيانات ووزعها. تخلص من بيانات العملاء عندما لم تعود هناك حاجة إليها.**
- ☐ **قم بتشفير بيانات العملاء عند نقلها وعندما تكون غير نشطة.**
- ☐ **ضع سياسات أمان البيانات لتوضيح طرق نقل البيانات المعتمدة مقابل المقيدة وتحديد ما هو مقبول لجميع الموظفين عند التعامل مع بيانات العميل. تأكد من توثيق هذه السياسات وإبلاغها وإنفاذها على جميع الموظفين، وأنه تتم مراجعتها وتحديثها بشكل دوري.**

## تأمين تطبيقات الويب العامة

- ☐ **قم بتنفيذ HTTPS على تطبيق (تطبيقات) الويب العام الخاص بمؤسستك وقم بإعادة توجيه جميع حركات مرور HTTP إلى HTTPS.**
- ☐ **استخدم سياسة أمان المحتوى على الموقع الإلكتروني (المواقع الإلكترونية).**
- ☐ **قم بتمكين تحديد المفتاح العام على الموقع الإلكتروني (المواقع الإلكترونية).**
- ☐ **تأكد من عدم استخدام تطبيق (تطبيقات) الويب العام أبدًا لملفات تعريف الارتباط بهدف تخزين معلومات العميل الحساسة أو البالغة الأهمية (مثل، كلمات المرور) وأن لديها تواريخ انتهاء صلاحية تحفظية لملفات تعريف الارتباط (عاجلاً وليس آجلاً).**
- ☐ **فكر في تشفير المعلومات المخزنة في ملفات تعريف الارتباط التي تستخدمها.**
- ☐ **فكر في تعيين خدمة اختبار الاختراق لتقييم أمن تطبيق (تطبيقات) الويب العام مرة واحدة على الأقل في العام.**

## تدريب الموظفين

- ☐ **علّم موظفيك المساءلة والإستراتيجيات للحد من الخطأ البشري الذي قد يكشف بيانات العملاء. وهذا يعني تقديم المشورة للقيام بما يلي:**
  - اقتصار وصولهم إلى بيانات العملاء ونقلها على ما هو ضروري فقط لأداء وظائفهم،
  - الحفاظ على ممارسات أمنية قوية على جميع الأجهزة والحسابات التي تتعامل مع بيانات العملاء باستخدام كلمات مرور قوية، وتمكين المصادقة الثنائية، وتحديث البرنامج، وعدم النقر فوق الروابط المشبوهة، و
  - والإبلاغ عن أي حوادث أو تهديدات أمنية داخلية أو خارجية محتملة، أو سوء إدارة للبيانات إلى موظفي المؤسسة الفنيين و/أو إدارتها العليا.
- ☐ **تأكد من فهم موظفيك للوثائق وتوقيعها للالتزام بسياسات حماية البيانات وسياسات الأمن الخاصة بالمؤسسة.**

## إخطار العملاء

☐ **افهم البيئة التنظيمية لمؤسستك عندما يتعلق الأمر بمعالجة انتهاكات بيانات العملاء لضمان استعدادك للامتثال عند وقوع الحوادث.**

☐ **عندما تصبح مؤسستك على علم بحادث الوصول غير المصرح به إلى معلومات العملاء الحساسة، قم بإجراء تحقيق لتُحدد على الفور احتمالية إساءة استخدام المعلومات أو حدوث ذلك بالفعل. اتبع أفضل ممارسات الإخطار وأخطر العميل (العملاء) المعني في أقرب وقت ممكن، وذلك عن طريق تقديم:**

- وصف عام للحادث والمعلومات التي تم اختراقها؛
- رقم هاتف لتقديم مزيد من المعلومات والمساعدة؛
- تذكير "بالبقاء يقظًا" على مدار الـ 12 إلى 24 شهرًا القادمة؛
- توصية بالإبلاغ عن حالات سرقة الهوية المشتبه بها فورًا؛
- وصف عام للخطوات التي تتخذها المؤسسة المالية لحماية تعرض المعلومات لمزيد من الوصول أو الاستخدام غير المصرح به؛
- معلومات الاتصال الخاصة بوكالات الإبلاغ عن الائتمانات؛ و
- وأي معلومات أخرى مطلوبة بموجب اللوائح التي يجب على مؤسستك الامتثال لها.