الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

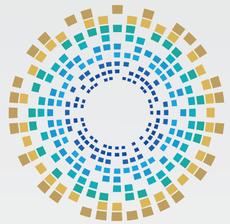
مبادئ عامة في السلامة الرقمية

الشريحة المستهدفة

القطاع المالي والمصرفي

كُتيّب المُدَرّب

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

مبادئ عامة في السلامة الرقمية

الشريحة المستهدفة

القطاع المالي والمصرفي

كُتَيّب المُدَرّب

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

الفهرس	رقم الصفحـة

تمهيد

السَّلامة الرقميَّة ركيزة أساسيَّة لضمان أمْن المعلومات، وحماية الأفراد والمجتمعات من التهديدات السيبرانية المتزايدة باستمرار.

تم تصميم هذا الكُتَيِّب بهدف توعية العاملين في القطاع المالي والمصرفي بالمخاطر السيبرانية المتزايدة، وأفضل الممارسات للحماية منها؛ حيث يهدف هذا الكُتَيِّب إلى تقديم حلول وقائية وإرشادات فعَّالة لرَفْع مستوى الوعي وتعزيز السلامة الرقمية، بما في ذلك التَّصيُّد الاحتيالي، وحماية الأجهزة والبيانات، وتأمين التعاملات المالية.

وتُعدّ هذه الجهود جزءًا من المبادرة الوطنية للسلامة الرقمية التي تُنظّمها الوكالة الوطنية للأمن السيبراني، لبناء بيئة رقمية آمِنَة لجميع فئات المجتمع.

المبادرة الوطنيّة للسلامة الرقميّة

Digital Safety National Initiative

تعريف المبادرة

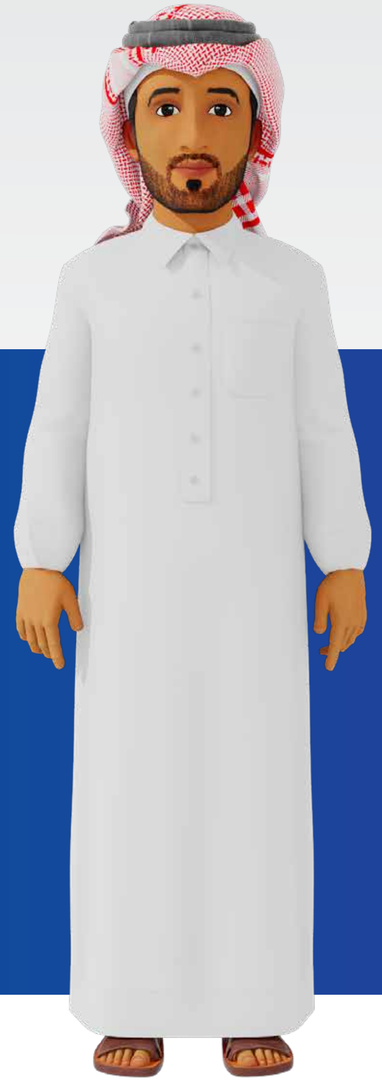
مجموعة من فعاليات التوعية في مجال السلامة الرقمية والأمن السيبراني؛ تستهدف المجتمع المحلي على اختلاف الشرائح العُمرية والاجتماعية والقطاعات المهنية.

تعمل المبادرة على نشر الوعي بالسلامة الرقمية والاستخدام الآمِن لشبكة الإنترنت والتطبيقات التكنولوجية المختلفة، وتوضيح المخاطر المحتمَلة؛ وذلك بهدف بناء مجتمع آمِن سيبرانيًّا ومتمكّن تكنولوجيًّا.

الشرائح المستهدَفة

تستهدف المبادرة مختلف شرائح المجتمع، مع تركيزها في السنة الأولى على الشرائح التالية:

- كبار القَدْر
- المرأة والأسرة
- ذوو الاحتياجات الخاصة
- طلبة الجامعات
- العمالة الوافدة
- مؤسسات المجتمع المدني
- القطاع المالي والمصرفي



أدوات التوعية

تعتمد المبادرة على أدوات توعية متنوّعة ومتكاملة، تشمل ما يلي:

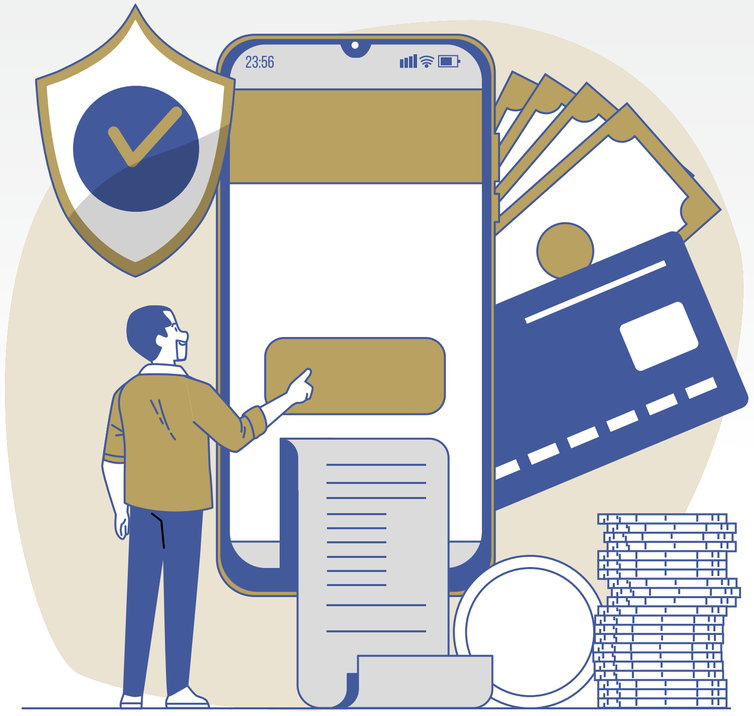
- دليل السلامة الرقمية
- كتيبات توعية
- ألعاب سيبرانية
- فيديوهات توعية
- ألعاب تعليمية مبتكَرة
- ورش توعية

المحور الأول

التهديدات السيبرانية في القطاع المالي

المعاملات المالية

تُعدّ عمليات التحويل والدفعات المالية من أكثر المعاملات حساسية، ما يَجْعلها هدفًا مباشرًا للهجمات السيبرانية.



01

لجنة التجارة الفيدرالية: بلغت خسائر الاحتيال في التحويلات البنكية في الولايات المتحدة أكثر من 12.5 مليار دولار عام 2024

02

كثير من الهجمات تعتمد على انتحال الهوية أو اعتراض رسائل التحويل عن طريق هجمات التنصت الوسيط (Man-in the-Middle)

03

تقوم بعض الهجمات بتعديل نظام التحويل من داخل البريد الرسمي للموظفين

04

نقاط الضعف في واجهات الـAPI المالية قد تؤدّي إلى وصولٍ غير مصرّح به

الاحتيال عبر القنوات المصرفية

تطوّرت الهجمات على القنوات المصرفية الإلكترونية مع انتشار الخدمات الرقمية.

نسبة كبيرة من محاولات الاحتيال تتمّ عبر تطبيقات مُزيَّفة أو مواقع شبيهة بالخدمات الرسمية.

- إنشاء مواقع بنكية مُزَيَّفة لخداع المستخدمين
- تطوير تطبيقات جوَّال مُزيَّفة مشابهة لتطبيقات البنوك
- اعتراض بيانات الجلسات عبر الشبكات غير الآمِنَة
- استغلال ضَعْف حماية كلمات المرور أو المُصادَقة الثنائية

الاجتماعات عن بُعْد

يزداد الاعتماد على الاجتماعات الافتراضية، ويزداد معه معدل التهديدات الجديدة المتعلّقة بسرية القرارات المالية وحماية المستندات.

1. اختراق الجلسات الافتراضية يُتيح للمهاجم الاطلاع على البيانات الحسّاسة
2. ضَعْف حماية المستندات المشتركة يؤدي لتسريب بيانات مالية
3. تسجيل بعض الجلسات دون عِلْم المشاركين يُشكِّل تهديدًا مزدوجًا.
4. يمكن أن تَستهدف الدعوات المُزيَّفة للاجتماعات عن بُعْد المستخدمين لسرقة بيانات الدخول أو أيّ معلومات أخرى مُهمَّة

العمل عن بُعْد

العمل عن بُعْد هو نَمَط من العمل يُتيح للموظفين أداء مهامهم من مواقع خارج المكاتب التقليدية، باستخدام التكنولوجيا للاتصال والتعاون مع زملائهم والمدراء.

ممارسات خاطئة في العمل عن بُعْد

- طباعة المستندات المتعلّقة بالعمل في المنزل دون أخذ احتياطات الأمان.
- الدخول إلى مواقع العمل من خلال شبكات Wi-Fi عامة.
- عدم تأمين سطح المكتب ضد هجمات التجسُّس.
- استخدام البريد الإلكتروني الشخصي لمراسَلات العمل.
- استخدام مواقع التخزين السحابي الشخصية لتخزين بيانات العمل.

الأجهزة والأنظمة التشغيلية

تُعدّ الأجهزة الداخلية ونقاط البيع والصرافات الآلية من أكثر الأنظمة استهدافًا نتيجة الضعف البنيوي أو عدم تحديث الأنظمة بشكلٍ دوري.

استغلال ثغرات أنظمة التشغيل يُتيح التحكُّم الكامل بالجهاز

برمجيات تسجيل لوحة المفاتيح (Key loggers) تُستخدَم لسرقة بيانات الدخول

ضعف صيانة الأجهزة قد يسمح بزرع أجهزة تجسُّس داخلية

استخدام منافذ USB المفتوحة قد يُؤدّي إلى زَرْع برمجيات خبيثة دون اكتشافها

مخاطر الشبكات العامة

الاتصال بالشبكات العامة يُعدّ من أخطر الممارسات للعاملين في القطاع المالي للأسباب التالية:

- اعتراض كلمات المرور في أثناء الاتصال
- ضَعْف تشفير الاتصال في بعض الشبكات المفتوحة
- إنشاء شبكات اتصال وهمية (Fake Wi-Fi)
- استغلال الولوج الخارجي للوصول إلى الأنظمة المالية الداخلية
- إعادة توجيه المُستخدِم إلى مواقع مالية مُزيَّفة

احذر!

تجنَّب الاعتماد على الشبكات العامة في إجراء المعاملات المصرفية أو الدخول إلى الحسابات المهمة، فقد تكون عُرضةً للاختراق.

التصيد الاحتيالي

التصيد الاحتيالي يُعَدُّ من أخطر التهديدات السيبرانية التي تُواجه القطاع المالي والمصرفي.

يستخدم المهاجمون رسائل بريد إلكتروني أو مواقع إلكترونية مُزيَّفة لاستدراج الموظفين والعملاء للكشف عن معلومات حسَّاسة، مثل: كلمات المرور، أو بيانات الحسابات البنكية.

مخاطر التصيد الاحتيالي

1

سرقة البيانات المصرفية: عبر الحصول على معلومات حسَّاسة، مثل بيانات تسجيل الدخول وأرقام البطاقات البنكية

2

اختراق الحسابات المالية: استخدام البيانات المسروقة للوصول إلى الحسابات البنكية وسرقة الأموال أو تحويلها

3

الابتزاز المالي: استغلال البيانات المسروقة لابتزاز المؤسسات أو الأفراد مقابل مبالغ مالية

4

إرسال برمجيات خبيثة: تتسبَّب في إصابة الأنظمة المالية ببرمجيات ضارَّة عند التفاعل مع الروابط المُزيَّفة، ممَّا يُعطِّل العمليات أو يُؤدِّي إلى سرق البيانات

5

انتحال هُويَّة العملاء أو الموظفين: استخدام المعلومات المسروقة لإجراء معاملات مالية أو تنفيذ أنشطة احتيالية باسم الضحية

برمجيات الفدية Ransomware

هي نوع من البرمجيات الخبيثة التي تقوم بتشفير بيانات المستخدِم أو قفل جهازه؛ مما يمنع الوصول إلى الملفات أو النظام.

يطلب المهاجمون فدية (عادةً ما تكون مبلغًا ماليًّا) مقابل فكّ تشفير البيانات أو إعادة الوصول إلى الجهاز.

كيف تعمل برمجيات الفدية؟

- التسلّل إلى النظام: يتم التسلّل عادة عبر
  - مرفقات البريد الإلكتروني
  - مواقع الإنترنت المشبوهة
  - الإعلانات المنبثقة
  - الثغرات الأمنية في النظام

- تشفير الملفات

بمجرد دخول البرمجيات الخبيثة إلى النظام، يبدأ تشفير الملفات المهمة، مثل المستندات والصور وملفات قواعد البيانات

- طلب الفدية

بعد تشفير الملفات، تظهر رسالة على شاشة الضحية تطلب فدية مالية مقابل مفتاح فكّ التشفير.

مخاطر برمجيات الفدية Ransomware

1. **تشفير الملفات:** تقوم برمجيات الفدية بتشفير الملفات؛ مما يجعل الوصول إلى البيانات مستحيلاً دون دفع الفدية.

2. **سرقة البيانات:** لا يكتفي المهاجمون بتشفير البيانات، بل يسرقونها أيضاً.

3. **تعطيل الأعمال:** يمكن أن تُؤدّي هجمات برمجيات الفدية إلى توقُّف كامل للعمليات المالية

4. **بطء الاستعادة:** قد تستغرق عملية استعادة النظام والبيانات بعد الهجوم وقتاً طويلاً.

حقائق ومعلومات

أصبحت برمجيات الفدية أحد أكبر التهديدات السيبرانية للشركات والحكومات على حدٍّ سواء؛ حيث تتسبَّب في خسائر مالية ضخمة.

نقاط البيع (POS)

تشهد أنظمة نقاط البيع ارتفاعًا مستمرًّا في مستوى الاستهداف؛ نظرًا لاعتمادها على الاتصالات اللحظيّة، ومعالجتها المباشرة لبيانات البطاقات المصرفية.

تُعدّ هذه الأنظمة إحدى أكثر الأنظمة التقنية حساسيةً في مؤسسات التجزئة والقطاع المصرفي.

- تعتمد الهجمات على برمجيات تُزْرَع داخل الجهاز لالتقاط بيانات البطاقات المصرفية (RAM Scraping)
- تُعدّ الثغرات في أنظمة التشغيل وقلة تحديث الأجهزة أحد الأسباب الرئيسة لنجاح الاختراق
- يمكن للمهاجمين استغلال الاتصال بين جهاز POS والخوادم المصرفية لاعتراض بيانات الدَّفْع
- ضَعْف إجراءات التدقيق على مُزوّدي الخدمة الخارجيين يرفع قابلية الإصابة بالبرمجيات الخبيثة

أجهزة الصرّاف الآلي (ATM)

تُعدّ أجهزة الصرّاف الآلي من الأهداف الأساسية للجرائم الإلكترونية؛ نظرًا لاحتوائها على بيانات عملاء حساسة، وقُدرتها المباشرة على صَرْف الأموال.

1. الرابطة الأوروبية للمعاملات الآمِنَة: سجَّلت الهجمات على أجهزة الـATM في أوروبا خسائر بقيمة 71 مليون يورو عام 2024

2. استغلال الثغرات غير المُحدَّثة في نظام التشغيل يسمح بالتحكُّم الكامل بالآلة

3. زَرْع أجهزة تجسُّس داخلية (Skimmers) لالتقاط بيانات البطاقات ورموز PIN

4. يُؤدّي ضَعْف حماية الشبكات المتصلة بالـATM إلى قيام المهاجمين بإرسال أوامر عن بُعْد للجهاز.

هجوم (RAM Scraping)

يُعدّ RAM Scraping من أخطر الأساليب التي تَستهدف أنظمة الدفع في المؤسسات المالية؛ حيث يعمل المهاجمون على التقاط بيانات البطاقات قبل أن تُشفَّر، وبذلك يحصلون على المعلومات الحسّاسة مباشرةً من ذاكرة الجهاز.

1. يستهدف هذا النوع من الهجمات أنظمة نقاط البيع (POS) والأنظمة المؤتمتة المرتبطة بمعالجة المدفوعات

2. يعمل المهاجم على زَرْع برمجية خَفِيَّة تُراقب الذاكرة وتلتقط بيانات البطاقات في أثناء المعالجة اللحظية

3. غالبًا لا يُكتشف الهجوم إلا بعد تسريب أعداد كبيرة من بيانات العملاء

4. تُعدّ الأنظمة القديمة ذات الذاكرة غير المحمية أكثر عُرْضَة لهذا النوع من الهجمات

هجمات حقن قواعد البيانات (SQL Injection)

تُشكّل هجمات SQL Injection تهديدًا مباشرًا للمؤسسات المالية؛ لأنها تَستهدف قواعد البيانات التي تحتوي على معلومات العملاء والمعاملات المالية والبيانات السرّية.

1. يقوم المهاجم بحَقْن أوامر خبيثة في قواعد البيانات عبر نقاط ضَعْف في واجهات الويب أو التطبيقات المالية

2. يمكن للهجوم أن يؤدي إلى قراءة أو تعديل أو حذف بيانات حساسة دون أيّ صلاحية

3. بعض الهجمات تُتِيح للمهاجم الوصول إلى لوحة التحكُّم الإدارية الكاملة للنظام

4. تظهر هذه الهجمات غالبًا في الأنظمة التي لا تَعتمد فَحْص إدخال البيانات (Input Validation)

5. قد تؤدي إلى توقُّف الأنظمة المالية، أو تسريب معلومات قد تُستخدَم في عمليات احتيال لاحقة

هجمات تغيير وجهة التحويلات (Transaction Redirection Attacks)

تستهدف هذه الهجمات الأنظمة المصرفية المتخصصة بالتحويلات المالية؛ حيث يقوم المهاجم بتغيير مسار التحويل إلى حسابات يسيطر عليها دون عِلْم المؤسسة أو الموظف الذي نَفَّذ العملية.

- يتم اعتراض بيانات التحويل عبر اختراق بريد الموظف أو استغلال ضَعْف في نظام إدارة التحويلات
- يقوم المهاجم بتعديل رقم الحساب المستفيد لحظة تنفيذ العملية دون إحداث تغييرات واضحة تُظهر الاشتباه
- تعتمد الهجمات عادةً على برامج خفية تُراقب نشاط التحويلات داخل الأجهزة المصرفية
- غالبًا ما تُكتَشَف هذه الهجمات بعد فوات الأوان؛ خاصةً في التحويلات اللحظية
- تُعدّ أنظمة الـAPI المفتوحة والربط مع جهات خارجية، من أهم نقاط الدخول لهذه الهجمات

السؤال التفاعلي الأول

أيّ من السيناريوهات التالية يُمثِّل أخطر تَهْديد للمعاملات المالية عبر القنوات المصرفية الرقمية؟

أ. مُوظّف يَستخدم البريد الشخصي للوصول إلى واجهة نظام داخلي مُؤسَّسي لتحديث بيانات العملاء.

ب. مشاركة ملفات تعريفية للعملاء مع مزوّد خدمة داخلي مُرخَّص ومؤمَّن بالشبكات المشفرة.

ج. موظف يشارك المستندات المالية على خادم داخلي آمِن باستخدام المصادقة متعددة العوامل.

السؤال التفاعلي الثاني

في سياق هجوم RAM Scraping على أنظمة الدفع، أيّ الإجراءات التالية تُعدّ الأكثر فعالية للحَدّ من الخطر على بيانات البطاقات؟

- **أ.** مشاركة بيانات العملاء مع مُزوّد خدمة خارجي غير موثوق، وعدم تقييد الوصول عبر الشبكة
- **ب.** استخدام شبكة Wi-Fi عامة للوصول إلى أجهزة POS في أثناء المُعالَجة اللحظية للمدفوعات
- **ج.** تجاهُل مراقبة الذاكرة الداخلية لأجهزة نقاط البيع، واعتماد نُسَخ احتياطية غير مُشفَّرة للبيانات
- **د.** تحديث أجهزة نقاط البيع وأنظمة تشغيلها بشكلٍ دوري، وتفعيل حلول تشفير متقدمة End-to-End Encryption

المحور الثاني

آليات الوقاية والسلامة الرقمية

الوقاية من مخاطر العمل عن بُعْد

1. استخدام برامج الحماية: التأكُّد من تثبيت برامج مضادة للفيروسات، وبرامج الحماية، على جهاز الحاسوب وتحديثها بانتظام
2. استخدام شبكة اتصال آمِنَة: تحمي هذه الخدمة أجهزة العمل من العديد من التهديدات السيبرانية
3. تحديث البرامج والتطبيقات وبرامج الحماية يُزيل الثغرات الأمنية الموجودة في النُّسخ القديمة
4. استخدام البريد الإلكتروني الخاص بالعمل
5. التواصل مع فريق تكنولوجيا المعلومات؛ للاستفسار عن أيّ تساؤلات أو اشتباه بوجود خرق أمني

أمن البيانات في نظام العمل عن بُعْد

1. تبادل البيانات من خلال البريد الإلكتروني المخصّص للعمل، وعدم استخدام البريد الشخصي
2. تخزين البيانات على موقع التخزين السحابي المخصّص للعمل، وعدم استخدام التخزين السحابي الشخصي
3. استخدام شبكة إنترنت آمِنة، واستخدام شبكة افتراضية خاصة (VPN) عند الدخول من شبكة Wi-Fi عامة
4. استخدام المصادقة الثنائية لتأمين كلمات المرور

حقائق ومعلومات

يمكن أن تستغرق الهجمات السيبرانية الموجّهة شهورًا أو حتى سنوات قبل اكتشافها؛ مما يعرّض الأنظمة لمخاطر مستمرة.

الحماية بواسطة VPN

1. توفّر VPN الحماية عند استخدام الشبكات العامة
2. تؤمّن اتصال المستخدِم عند استخدام شبكات Wi-Fi العامة
3. تمنع المتسلّلين من اعتراض البيانات الخاصة بالمستخدِم
4. توفّر تشفيراً قوياً للبيانات الحساسة
5. توفّر أماناً من هجمات القراصنة على الشبكات العامة

حقائق ومعلومات

التحسين المستمر لتقنيات الأمان السيبراني ضرورة حتمية للتكيف مع التهديدات الجديدة والمتطوّرة في العالم الرقمي.

الوقاية من برمجيات الفدية Ransomware

- الاحتفاظ بنُسَخ احتياطية منتظمة من الملفات المهمَّة على أجهزة تخزين خارجية أو على السحابة
- الحرص على تحديث نظام التشغيل والبرامج بانتظام؛ لسدّ الثغرات الأمنية
- تثبيت برامج مكافحة الفيروسات وتفعيل جدران الحماية؛ لحماية النظام
- عدم فتح مرفقات البريد الإلكتروني المشبوهة
- تحميل البرامج من مواقع إلكترونية موثوقة

الأمن السحابي

هـو مجموعـة مـن السياسـات والتقنيـات المُصمَّمـة بإحـكام لحماية البيانـات والتطبيقـات والبنيـة التحتيـة التـي تعمـل فـي بيئـات السـحابة. ويهـدف الأمـن السـحابي إلـى تأميـن المعلومـات مـن التهديـدات الداخليـة والخارجيـة.

مكوّنات الأمن السحابي

1 تأمين البيانات
يشمل تقنيات تشفير البيانات وحمايتها في أثناء التخزين والنقل.

2 التحكّم في الوصول
إدارة مَن يُمكنه الوصول إلى البيانات والتطبيقات السحابية، وعادةً ما يتم استخدام المصادقة متعددة العوامل (MFA).

3 المراقبة والتسجيل
تتبّع الأنشطة والمراقبة في الوقت الحقيقي؛ للكشف عن الأنشطة غير المعتادة أو المحتمَلة.

4 استجابة الحوادث
تطوير إستراتيجيات وخطط للتعامل مع حوادث الأمان، مثل خروقات البيانات.

حماية أنظمة نقاط البيع (POS)

تتطلّب حماية أنظمة نقاط البيع مستوى عاليًا من الصرامة الأمنية؛ نظرًا لكونها نقطة تماس مباشرة مع بيانات البطاقات المصرفيّة. إن تحسين بنيتها التقنية وتطبيق ضوابط رقابية دقيقة يَحُدّان بشكلٍ كبير من احتمالات الاختراق.

- تطبيق تحديثات دورية لنظام التشغيل والبرمجيات لتقليل الاستغلال المباشر للثغرات الأمنية
- فَصْل شبكة نقاط البيع عن باقي شبكات المؤسسة لضمان تقليل نطاق التهديد (Network Segmentation)
- استخدام حلول تشفير متقدّمة لضمان حماية بيانات البطاقات في أثناء المعالجة وقبل انتقالها للخوادم
- إجراء تدقيق منتظم على مزوّدي الخدمة؛ لضمان عدم تسريب أيّ برمجيات خبيثة عبرهم
- اعتماد أنظمة مُراقَبة آنيَّة (Real-Time Monitoring) لاكتشاف السلوك الخاطئ في أجهزة POS

حماية أجهزة الصرّاف الآلي (ATM)

الحماية الفعّالة لـATM تعتمد على الجمع بين أمْن الأجهزة المادية وأمن البرمجيات؛ نظرًا لطبيعة الهجمات التي تستهدف كلًّا من المكوّنات التقنية والهيكل المادي للآلة في الوقت نفسه.

- تحديث أنظمة تشغيل الـATM بانتظام، وإغلاق الثغرات التي تُستخدَم في هجمات التحكم عن بُعْد
- تثبيت حلول أمنيّة متقدّمة مثل Endpoint Protection داخل الجهاز لمنع تشغيل أيّ برمجيات غير معروفة
- تركيب حسّاسات داخلية لكشف محاولات فتح الجهاز أو زرع أجهزة Skimmers في القارئ.
- مراقبة شبكة الاتصال الخاصة بالـATM عبر أنظمة IDS/IPS لاكتشاف أوامر مشبوهة قبل تنفيذها
- اعتماد كاميرات عالية الدقة وأنظمة إنذار محيطي للحدّ من الهجمات المادية الداعمة للهجمات السيبرانية

الوقاية من هجمات (RAM Scraping)

تتطلّب حماية أنظمة المدفوعات من هجمات RAM Scraping تطبيق ضوابط تقنية دقيقة تضمن منع وصول البرمجيات الخبيثة إلى الذاكرة المؤقتة في أثناء معالجة بيانات البطاقات.

1. استخدام أجهزة نقاط بيع معتمدة تعتمد تقنيات End-to-End Encryption لحماية البيانات قبل دخولها الذاكرة
2. تطبيق حلول Application Whitelisting لمنع تشغيل أيّ برمجية غير مُصرَّح بها على أجهزة POS
3. تفعيل التحديثات الأمنية لأنظمة POS بشكلٍ دوري لسدّ الثغرات التي تَستغلها البرمجيات الخبيثة
4. مُراقَبة الذاكرة باستخدام أدوات Behavioral Analysis للكشف عن أيّ نَشاط مشبوه داخل الجهاز
5. فَصْل شبكة نقاط البيع عن الشبكات الأخرى، وتقييد الوصول عبر بروتوكولات اتصال محمية

الوقاية من هجمات حقن قواعد البيانات (SQL Injection)

تعتمد الحماية من هجمات SQL Injection على تعزيز أمن التطبيقات وقواعد البيانات من خلال تطوير بِنْيَة آمِنَة تمنع إدراج الأوامر الخبيثة وإعدامها.

01

تطبيق مبدأ فَحْص إدخال البيانات (Input Validation) بشكل صارم لمنع التلاعب بأوامر طلب البيانات "Queries"

02

استخدام الاستعلامات المُعمّمة Parameterized Queries بدلًا من الاستعلامات "Queries" النصية التقليدية

03

تفعيل جدران حماية تطبيقات الويب Web Application Fire-wall (WAF) للكشف عن الأنماط الهجومية

04

تقييد صلاحيات قواعد البيانات عبر مبدأ الحد الأدنى من الامتيازات Least Privilege

05

إجراء اختبارات اختراق دورية للكشف عن الثغرات قبل استغلالها من جهات مهاجمة

الوقاية من هجمات تغيير وجهة التحويلات (Transaction Redirection Attacks)

تتطلب حماية أنظمة التحويلات المالية تعزيز الرقابة والتوثيق مُتعدّد الطبقات لمنع أيّ تعديل غير مُصرَّح به على بيانات المستفيدين في أثناء تنفيذ العمليات.

- اعتماد التحقُّق الثنائي أو المتعدد للعاملين على العمليات المالية الحساسة Multi-Factor Authentication
- تفعيل أنظمة كشف التغييرات غير الطبيعية في عمليات التحويل Anomaly Detection ضمن الأنظمة المصرفية
- استخدام قنوات اتصال مُشفَّرة بالكامل لحماية بيانات التحويل في أثناء نقلها بين الأنظمة
- مراقبة البريد الإلكتروني للموظفين عبر أدوات فَحْص التهديدات لمنع اعتراض تعليمات التحويل
- حَصْر صلاحيات تعديل بيانات المستفيدين على عدد محدود من الموظفين، وتوثيق كلّ عملية بشكلٍ إلزامي

السؤال التفاعلي الثالث

أيٌّ من الإجراءات التالية يُعدّ الأكثر فاعلية لتقليل خطر برمجيات الفدية في بيئة العمل المالي؟

- **أ.** تحديث برامج مكافحة الفيروسات فقط دون تحديث نظام التشغيل أو البرامج الأخرى
- **ب.** الاحتفاظ بنُسخ احتياطية منتظمة، وتحديث نظام التشغيل والبرامج، وتثبيت برامج الحماية مع تفعيل جدار الحماية
- **ج.** فتح جميع مرفقات البريد الإلكتروني لتسريع العمل، والتأكد من سلامتها بعد التحميل
- **د.** تحميل جميع البرامج من أيّ مصدر مُتاح لتوفير الوقت دون الاهتمام بالموثوقية

السؤال التفاعلي الرابع

أيٌّ من الممارسات التالية تُعدّ الأكثر أمانًا لحماية البيانات في أثناء العمل عن بُعْد في القطاع المالي؟

- **أ.** استخدام البريد الإلكتروني الشخصي لتبادل المستندات، والاعتماد على شبكات Wi-Fi عامة
- **ب.** تخزين البيانات على السحابة الشخصية، وعدم استخدام المصادقة الثنائية لتأمين كلمات المرور
- **ج.** استخدام البريد الإلكتروني الخاص بالعمل، شبكة اتصال آمنة أو VPN، وتفعيل المصادقة الثنائية لتأمين الدخول إلى الأنظمة
- **د.** طباعة جميع المستندات المالية في المنزل، ومشاركتها عبر البريد الإلكتروني الشخصي لضمان سهولة الوصول

إجابات الأسئلة التفاعلية

01

إجابة السؤال التفاعلي الأول

أ. موظف يستخدم البريد الشخصي للوصول إلى واجهة نظام داخلي مؤسسي لتحديث بيانات العملاء

02

إجابة السؤال التفاعلي الثاني

د. تحديث أجهزة نقاط البيع وأنظمة تشغيلها بشكل دوري، وتفعيل حلول تشفير متقدمة End-to-End Encryption

03

إجابة السؤال التفاعلي الثالث

ب. الاحتفاظ بنُسخ احتياطية منتظمة، وتحديث نظام التشغيل والبرامج، وتثبيت برامج الحماية مع تفعيل جدار الحماية

04

إجابة السؤال التفاعلي الرابع

ج. استخدام البريد الإلكتروني الخاص بالعمل، شبكة اتصال آمنة أو VPN، وتفعيل المصادقة الثنائية لتأمين الدخول إلى الأنظمة.

المراجع

1. ASEE Cybersecurity. Cybersecurity statistics: 100+ cybersecurity stats to know in 2025. february 2025. on site: https://cybersecurity.asee.io/blog/cybersecurity-statistics/
2. Cate, Mia. Data Privacy Risks and Vulnerabilities in API-Driven Financial Ecosystems. May 2025, on site: https://www.researchgate.net/publication/392070830_Data_Privacy_Risks_and_Vulnerabilities_in_API-Driven_Financial_Ecosystems
3. Cybersecurity and Infrastructure Security Agency (CISA). Malware, phishing, and ransomware., on site: https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware
4. Department of the Treasury. National Money Laundering Risk Assessment. 2024. On site: https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf
5. Donohue, Brian. Kaspersky. RAM Scrapers and Other Point-of-Sale Malware. January 2014. On site: https://www.kaspersky.com/blog/ram-scrapers-and-other-point-of-sale-malware/3600/
6. Ernest, Nonum et al. Social Engineering: Understanding Human Factors in Cyber Security. International Journal of Convergent and Informatics Science Research, May 2025, on site: https://harvardpublications.com/hijcisr/article/view/326

7. European Association for Secure Transactions. European Terminal Fraud attacks double. April 2025. On site: https://www.association-secure-transactions.eu/wp-content/uploads/European-Terminal-Fraud-attacks-double-for-release-to-the-media-on-14-April-2025.pdf

8. Federal Trade Commission. New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024. March 2025. On site: https://www.ftc.gov/news-events/explore-data

9. IBM. Cost of a Data Breach Report 2025, on site: https://www.ibm.com/reports/data-breach

10. IBM. What is malware?, on site: https://www.ibm.com/think/topics/malware

11. Kaspersky. Ransomware WannaCry: All you need to know, on site: https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

12. Kosinski, Matthew. IBM. What is phishing?, on site: https://www.ibm.com/think/topics/phishing

13. Kosinski, Matthew. IBM. What is ransomware?, on site: https://www.ibm.com/think/topics/ransomware

14. Xiang, Xiaobo et all. Ghost in the Binder: Binder Transaction Redirection Attacks in Android System Services. November 2021. On site: https://dl.acm.org/doi/pdf/10.1145/3460120.3484801

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

للتواصل مع الأكاديمية الوطنية للأمن السيبراني

16555 - 40466379 - 51045944

www.ncsa.gov.qa academy@ncsa.gov.qa