السلامة الرقمية في المؤسسات المالية والمصرفية

الفئة المستهدَفة
القطاع المالي والمصرفي

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

السلامة الرقمية في المؤسسات المالية والمصرفية

الفئة المستهدَفة: القطاع المالي والمصرفي


Privacy Policy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

حقوق الملكية الفكرية

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

للتواصل مع الأكاديمية الوطنية للأمن السيبراني

00974 404 663 62
00974 404 663 79
academy@ncsa.gov.qa
www.ncsa.gov.qa/

يناير 2025م
الدوحة، قطر

◆ عزيزي المشارك

في ظلّ التطوُّر التكنولوجي المتسارع، ودخول الإنترنت إلى مختلف مجالات الحياة؛ أصبحت التهديدات السيبرانية تُواجِه مختلف شرائح المجتمع، ما يتطلَّب العمل على تعزيز الوعي بمفاهيم السلامة الرقمية؛ التي تُعدّ الدّرع الذي يحمي المجتمع من هذه التهديدات.

وفي سياق جهود «المبادرة الوطنية للسلامة الرقمية» لتعزيز مؤشرات السلامة الرقمية في المجتمع؛ تُقدِّم الوكالة الوطنية للأمن السيبراني هذا الكُتَيّب، والذي يتضمَّن مجموعةً من النصائح والإرشادات العامَّة المتعلّقة بالسلامة الرقمية.

الفهـــرس	رقم الصفحـة
مُقدّمــة	9
الفصل الأول: السلامة الرقمية في القطاع المالي والمصرفي	13
أولاً: السلامة الرقمية للخدمات المالية والمصرفية	15
ثانياً: أهمية السلامة الرقمية للخدمات المالية والمصرفية	16
ثالثاً: تحديات السلامة الرقمية في المؤسسات المالية والمصرفية	18
الفصل الثاني: إستراتيجيات تعزيز السلامة الرقمية في القطاع المالي والمصرفي	37
أولاً: الثغرات الرقمية والمعرفية في القطاع المالي والمصرفي	39
ثانياً: دَور الموظفين داخل المؤسسات المالية والمصرفية في تحقيق السلامة الرقمية	43
تمارين وتدريبات	47
المراجــع	67

مُقدّمـــة

مع دخول القطاع المالي والمصرفي عصر الرقمنة ارتفعت المخاطر السيبرانية المحيطة بعمل هذا القطاع، وقد برزت هذه المخاطر مع تفشّي جائحة كورونا (كوفيد - 19)، نتيجة الزيادة المفاجئة في الوصول عن بُعد، والتقنيات السحابية، والمعاملات غير النقدية. وعلى الرغم من فوائد التحوُّل الرقمي في القطاع المالي والمصرفي؛ إلا أن مخاطر خرق البيانات والهجمات السيبرانية تُؤرّق القائمين على مؤسسات القطاع وكذلك دُول العالم بسبب الخسائر المالية الباهظة التي يتكبّدها القطاع في حالات نجاح الهجوم السيبراني.

الأمر الذي سلَّط الضوء على أهمية تعزيز السلامة الرقمية في القطاع المالي والمصرفي حفاظاً على مستقبل هذا القطاع بالغ الأهمية. وبناءً على الأمن السيبراني تتَّخذ المؤسسات المالية والمصرفية مجموعة من التدابير لحماية أنظمتها وشبكاتها من الهجمات السيبرانية؛ حيث تستخدم البنوك والمؤسسات المالية والمصرفية أدوات وتقنيات مصمَّمة خصوصاً لاكتشاف ومَنْع الهجمات المتنوّعة مثل:

القرصنة وخرق البيانات وسرقة الهُويَّة والبرمجيات الضّارَّة والفيروسات والوصول غير المصرَّح به إلى الشبكات والبيانات الحساسة.

ويهدف استخدام المؤسسات المالية والمصرفية لتدابير الأمن السيبراني إلى حماية أصول عملائها، ومَنْع فقدان البيانات الحساسة وما يعقبه من تَعطُّل العمل وخسائر مالية وتهديدات للعملاء. ومن أجل تنفيذ هذه التدابير يتم توظيف فريق من خبراء الأمن الذين يعكفون على مراقَبة الشبكات بحثاً عن الأنشطة المشبوهة والتدخّل سريعاً لمنع وقوع الهجمات السيبرانية.

والسبب في لجوء المؤسسات المالية والمصرفية لتدابير أمنية سيبرانية هو حماية سُمعتها ومصداقيتها، فتَعَرُّض عميلٍ لخطر الهجمات الخبيثة يُقابِله تَضَرُّر سُمعة البنوك والمؤسسات المالية، إلى جانب تَعَرُّضها للغرامات المالية والعقوبات القانونية تبعاً للوائح المنظِّمة لعمل القطاع المالي والمصرفي.

إذاً يُعدّ القطاع المالي والمصرفي أكثر عُرضةً اليوم عما سبق لكثيرٍ من التهديدات مع ظهور تطبيقات الخدمات المصرفية عبر الهواتف المحمولة، وانتهاكات الطرف المجهول (الثالث)، والمخاطر الناشئة عن العملات المشفَّرة. وأمام هذه التهديدات لا يمكن الاعتماد على الإجراءات والتدابير الأمنية السيبرانية فقط، مثل عمليات التدقيق الأمني وجدران الحماية المتقدِّمة والمصادقة متعدِّدة العوامل، بل يجب أن تمتدّ هذه الإجراءات إلى عملية توعية وتثقيف للموظّفين داخل البنوك والمؤسسات المالية والمصرفية عامةً حول الممارسات الآمِنة.

ولا نقصد بالقطاع المالي والمصرفي البنوك التقليدية فقط، بل يشمل هذا القطاع: بطاقات الائتمان مثل فيزا Visa وماستر كارد MasterCard، وشركات معالَجة الدفع مثل باي بال PayPal، ومتاجر التجزئة على الإنترنت مثل أمازون Amazon وأبل Apple، وكذلك المحافظ الإلكترونية؛ حيث دَفَعَ ظهور عملة بيتكوين وغيرها من العملات المشفَّرة -التي يتم استخدامها بدلاً من الأموال التقليدية- مجرمي الإنترنت إلى استهدافها أيضاً.

إلى جانب ما سبق، على تلك المؤسسات الاستثمار في الذكاء الاصطناعي والتعلُّم الآلي لاكتشاف التهديدات السيبرانية على الفور، بما يُحقِّق الامتثال لمعايير الأمن السيبراني، لكن عليها التَّيقُّظ حيال استخدامات الذكاء الاصطناعي في مجال الأمن السيبراني، فهو يحمل جوانب إيجابية وأخرى سلبية؛ إذ يستفيد مجرمو الإنترنت من الذكاء الاصطناعي التوليدي في تنفيذ هجمات إلكترونية معقَّدة، فعلى سبيل المثال، يستغلّ هؤلاء المجرمون الذكاء الاصطناعي في صياغة رسائل بريد إلكتروني تصيدية مُقنِعة.

احذر!

يُعدّ القطاع المالي والمصرفي أكثر عُرضةً اليوم عما سبق لكثيرٍ من التهديدات مع ظهور تطبيقات الخدمات المصرفية عبر الهواتف المحمولة، وانتهاكات الطرف المجهول (الثالث)، والمخاطر الناشئة عن العملات المشفَّرة.

هل تعلم؟

من المرجَّح أن تصل تكاليف الجرائم الإلكترونية العالمية إلى 10,5 تريليون دولار أمريكي سنوياً بحلول عام 2025م.

01

الفصل الأول

السلامة الرقمية في القطاع المالي والمصرفي

- أولاً: السلامة الرقمية للخدمات المالية والمصرفية
- ثانياً: أهمية السلامة الرقمية للخدمات المالية والمصرفية
- ثالثاً: تحديات السلامة الرقمية في المؤسسات المالية والمصرفية

أولاً: السلامة الرقمية للخدمات المالية والمصرفية

يشهد مجال التكنولوجيا كثيراً من التغيّرات المستمرة التي تَفرض متطلّبات أمان معقّدة لتشغيل الأنظمة وتحقيق الأهداف المطلوبة في العمل، ولحساسية طبيعة عمل المؤسسات المالية والمصرفية وما تُقدِّمه من خدمات غاية في الأهمية؛ تتزايد الضغوط عليها من أجل توفير السلامة الرقمية لأنظمتها وشبكاتها في ظلّ تصاعُد التهديدات السيبرانية داخلياً وخارجياً.

وتأتي أهمية السلامة الرقمية للخدمات المالية والمصرفية نظراً للخطر المحيط بالبيانات الشخصية الحساسة، مثل التفاصيل المصرفية وكلمات المرور والوصول غير المصرَّح به من جهات خبيثة بواسطة الهجمات الضّارَّة كالفيروسات، وكل ما سبق يضع عبء تأمين الأنظمة والشبكات وجميع خطوات العمل على عاتق المؤسسة المالية والمصرفية؛ أولاً لحماية بيانات عملائها، وثانياً لحماية سُمعتها من التضرُّر في حال حدوث خَرْق للبيانات أو فُقدانها.

ثانياً: أهمية السلامة الرقمية للخدمات المالية والمصرفية

أصبحت الحاجة إلى اعتماد إستراتيجيات أمنية سيبرانية لحماية العمل بالمؤسسات المالية والمصرفية أمراً لا بدّ منه مع التطوّر الرقمي الحاصل الذي بات عاملاً أساسياً في المعاملات النقدية، وما رافقه من ظهور مجموعة متنوعة من التهديدات والهجمات السيبرانية المؤثرة بوضوح في العمليات المصرفية، إلى جانب الخسائر المالية المحتَمَلة للعملاء وللمؤسسات على حدٍّ سواء.

ولهذا تأتي أهمية السلامة الرقمية للخدمات المالية والمصرفية من التأثيرات السلبية للتهديدات السيبرانية المحتَمَلة، والتي تتطلّب للتغلّب عليها تبنّي المؤسسات معايير أمان قوية لمَنْع تَسرُّب البيانات وفُقدانها، ومَنْع أيّ نوع من الانتهاكات الأمنية.

وإجمالاً فإن أهمية السلامة الرقمية للمؤسسات المالية والمصرفية ترجع إلى ما يلي:

معايير الأمان غير الكفء في المؤسسات، التي تؤدي إلى تسلُّل مجرمي الإنترنت وتنفيذ هجماتهم وسرقة البيانات الحساسة بنجاح، ومع اعتماد سياسات قوية للأمن السيبراني حينها يمكن لهذه المؤسسات إحباط تلك الهجمات بكفاءة.

لا تتوقف أهمية السلامة الرقمية على المؤسسات المالية والمصرفية فقط، بل على العملاء أنفسهم الحَذر من الممارسات الاحتيالية، التي تستهدِفهم بطرق خادعة يُنفِّذها مجرمو الإنترنت لدفع الضحايا إلى الكشف عن بياناتهم المالية المهمة، مثل أرقام البطاقات الائتمانية، وهو ما يُمهِّد للوصول غير المصرَّح به إلى الحسابات المصرفية وسرقة الأموال منها[1].

يلجأ مجرمو الإنترنت إلى أساليب احتيالية مبتكَرَة، مثل تقديم عروض الهدايا المزيَّفة والقَيِّمة في الوقت نفسه، مثل أجهزة الحاسوب باهظة الثمن والهواتف الذكية، وغيرها من هدايا الهدف منها تنفيذ عملية احتيال مُغرية لعملاء البنوك للكشف عن بياناتهم الحساسة.

احذر!

يلجأ مجرمو الإنترنت إلى أساليب احتيالية مبتكَرَة، مثل تقديم عروض الهدايا المزيفة والقَيِّمة في الوقت نفسه، مثل أجهزة الحاسوب باهظة الثمن والهواتف الذكية وغيرها، لعملاء البنوك للكشف عن بياناتهم الحساسة.

1. Narayanan, Lakshmi. Benefits and Importance of Cybersecurity in Banking Sector Teceze, February 2024. On site: https://teceze.com/cybersecurity-in-banking-importance-and-threats-challenges-benefits

ثالثاً: تحديات السلامة الرقمية في المؤسسات المالية والمصرفية

ارتفعت معدلات الجرائم الإلكترونية بشكلٍ ملحوظٍ في السنوات الأخيرة؛ ما جعلها التهديد الأكبر للقطاع المالي والمصرفي بسبب تنوُّع أساليب القراصنة وتعقُّدها، الأمر الذي صعَّب عمليات الدفاع ضدّ الهجمات السيبرانية.

وفيما يلي أهم التحديات التي تواجه السلامة الرقمية في المؤسسات المالية والمصرفية:

1- تطبيقات الخدمات المصرفية عبر الهاتف المحمول

الخدمات المصرفية عبر الهاتف المحمول هي خدمات عبر الإنترنت يُقدِّمها البنك أو المؤسسة المالية للعملاء لتمكينهم من إجراء معاملاتهم النقدية من خلال الهاتف أو الجهاز اللوحي، وتُتيح الخدمة للعملاء الوصول المباشِر إلى حساباتهم المتاحة أو بياناتهم المصرفية.

ومع تزايد الاعتماد على التطبيقات لإجراء المعاملات المالية ومع الافتقار إلى التدابير الأمنية القوية، أصبحت تطبيقات الخدمات المصرفية من أكثر المخاوف إلحاحاً للمؤسسات المالية والمصرفية؛ لتعرُّضها لانتهاكات سيبرانية محتَمَلة مع اتجاه مجرمي الإنترنت إلى استهداف الأنظمة المصرفية المشتَرَكة الأقل أماناً وشبكات الطرف المجهول (الثالث) للوصول غير المصرَّح به إلى الشبكات والبيانات، لهذا لا يزال هذا النوع من الخدمات يخضع للتطوُّر لضمان استخدام آمِن للعملاء عبر الإنترنت.

وتتنوع الخدمات التي تُتيحها تطبيقات الخدمات المصرفية عبر الهاتف المحمول، مثل:

- معلومات الحساب، وتتضمَّن تاريخ الحساب ومراقَبة الودائع وبيانات البطاقات والقروض، وغير ذلك من بيانات حساسة.
- تاريخ المعاملات المالية، مثل تحويلات الأموال بين الحسابات ودَفْع الفواتير وشيكات الإيداع.
- خدمات الدعم، مثل حالات طلب الائتمان والشكاوى ومواقع ماكينات الصراف الآلي[1].
- الخدمات الاستثمارية، كأسعار الأسهم والإشعارات المتعلّقة بأسعار الأوراق المالية.

احذر!

لا تتوقف أهمية السلامة الرقمية على المؤسسات المالية والمصرفية فقط، بل على العملاء أنفسهم الحذر من الممارسات الاحتيالية التي تستهدِف دَفْعهم للكشف عن بياناتهم المالية المهمة، مثل أرقام البطاقات الائتمانية.

1. Mobile Banking: What are the Advantages and Imminent Challenges? The Salmon Factor, On site: https://thesalmonfactor.com/mobile-banking-advantages-and-imminent-challenges.

وبهذا نجد أن فوائد الخدمات المصرفية عبر الهاتف المحمول كثيرة، فهي تُسهِّل التعامل مع البنك على مدار 24 ساعة يومياً، وتُخفّض من تكلفة المعاملات والوقت المطلوب لإتمامها. ومع الزيادة الكبيرة في استخدام الهواتف والأجهزة اللوحية في المعاملات المالية، أصبح على المؤسسات المالية والمصرفية حُسْن التعامل مع التحديات المرتبطة بها، **ومن أهمها ما يلي:**

الالتزام التام بمعايير السلامة الرقمية:

بالطبع تتطلّب الخدمات المصرفية عبر الهاتف المحمول اتصالاً بالإنترنت فهذا من شأنه أن يُمثِّل تحدياً للبنوك والمؤسسات المالية عامَّة، وكذلك لمطوّري تطبيقات الهواتف المحمولة، وهذا التحدي يَتمثَّل في الجرائم الإلكترونية[1].

أمن التطبيق:

إلى جانب الأمان الذي تُقدِّمه المؤسسات المالية والمصرفية للبطاقات الائتمانية، فإن الأجهزة المستخدَمة كالهواتف والحاسوب اللوحي تحتاج أيضاً إلى اشتراطات أمنية قوية لحماية المعاملات المالية التي تتم بواسطتها عبر الإنترنت.

مصادقة الجهاز:

من الضروري أن يتم التنسيق بين المؤسسات المالية والمصرفية وبين أجهزة العملاء من خلال المصادقة قبل إجراء المعاملات المالية لمَنْع الأجهزة غير المصرَّح بها من إجراء التحويلات المالية.

1. Banking on Security: Navigating the Cyber Threat Landscape in the Digital Age, the global treasurer, April 2024, on site: https://www.theglobaltreasurer.com/2024/04/04/banking-on-security-navigating-the-cyber-threat-landscape-in-the-digital-age/

سلوك العملاء:

من التحديات التي تُواجه الخدمات المصرفية عبر الهاتف المحمول وأمن البيانات: سلوك العميل؛ إذ أظهرت الأبحاث أن أكثر من نصف المستخدِمين لتلك الخدمات يُظهرون سلوكاً محفوفاً بالمخاطر، ولا يَعُون المخاطر المرتبطة بالاحتيال، وظهر هذا مع تلقِّي المؤسسات المالية والمصرفية شكاوى كثيرة من عملائها، وبمراجعتها تبيَّن أنهم لا يُفعِّلون عامل المصادقة الثنائية خلال إجراء المعاملات المالية[1].

الوقت:

يخضع استخدام تطبيقات الخدمات المصرفية لقيود الوقت؛ حيث لا يمكن للعميل استخدامها لفترة طويلة أو إبقاؤها مفتوحة دون استخدام لفترة ما؛ لأن ذلك يزيد من فرص المعاملات الاحتيالية، مما يجعل عامل الوقت أحد التحديات التي تواجه تلك التطبيقات؛ حيث يَعتمد العملاء عليها لإنجاز العديد من المهام الضرورية، الأمر الذي يتطلَّب أن تتوافق التطبيقات مع مهام العميل وسلوكه.

1. Sarin, Arvind. Top 3 Challenges in Mobile Banking App Development. Copper Digital, on site: https://copperdigital.com/blog/problems-and-solutions-for-financial-apps/

وتُظهِر الدراسات أن **أكثر من 70% من المستخدِمين شعروا بالإحباط** تجاه أحد تطبيقات الخدمات المصرفية عبر الهاتف المحمول؛ لعدم قدرتهم على إكمال المطلوب في الوقت المناسب؛ مما دَفَعَ كثيراً منهم إلى إلغاء الاشتراك أو إلغاء تثبيت التطبيق نهائياً[1].

هل تعلم؟

كشف استطلاع للرأي عن نموّ التهديدات عبر الأجهزة المحمولة بشكلٍ مطّردٍ بنسبة 40% مع ارتفاع الخدمات المصرفية عبر الإنترنت، وكان "Faketoken" -أحد أحصنة طروادة - يقف وراء هذا الارتفاع؛ إذ يمكنه سرقة رموز الرسائل القصيرة المرسَلة إلى مستخدمي المصادقة الثنائية[2].

1. Sarin, Arvind. Top 3 Challenges in Mobile Banking App Development. Copper Digital, on site: https://copperdigital.com/blog/problems-and-solutions-for-financial-apps/
2. Alexander Eremin, The Faketoken Trojan sends out offensive texts, Kaspersky, January 2020. on site: https://www.kaspersky.com/blog/faketoken-trojan-sends-offensive-sms/32048/

◆ 2- هجمات التصيد الاحتيالي Phishing Attacks

تُعدّ هجمات التصيد الاحتيالي من التهديدات الشائعة في مجال الأمن السيبراني في الصناعة المصرفية، فالقطاع المالي هو المجال الأكثر استهدافاً من خلال هذا النوع من الهجمات السيبرانية، وقد شهد عام 2023 استهداف أكثر من 23% من هجمات التصيد الاحتيالي للمؤسسات المالية حول العالم؛ إذ يتظاهر مجرمو الإنترنت بأنهم بنوك أو مؤسسات مالية شرعية، ويُنفِّذون هجومهم من خلال إرسال نماذج مُزيَّفة أو رسائل بريد إلكتروني مضلِّلة أو رسائل بها روابط ضارة؛ من أجل الحصول على البيانات الحساسة [1].

ووسيلة مجرمي الإنترنت في تنفيذ هجمات التصيد الاحتيالي هي خَلْق شعور بالإلحاح أو الذعر؛ حيث يقومون بخداع الضحايا وإيهامهم بأن حساباتهم تواجه نشاطاً مشبوهاً، يتطلَّب التعامل معه تقديم بياناتهم فوراً؛ مما يدفع الضحايا إلى التصرُّف دون تفكير.

احذر!

وسيلة مجرمي الإنترنت في تنفيذ هجمات التصيد الاحتيالي هي خَلْق شعور بالإلحاح أو الذعر؛ حيث يقومون بخداع الضحايا وإيهامهم بأن حساباتهم تواجه نشاطاً مشبوهاً، يتطلَّب التعامل معه تقديم بياناتهم فوراً؛ مما يدفع الضحايا إلى التصرُّف دون تفكير.

1. Sasovets, Ihor. Cyber Security in Banking: How We Address Rising Challenges, Tech Magic, May 2024. on site: https://www.techmagic.co/blog/cybersecurity-in-banking/

وهناك أمثلة على هجمات التصيد الاحتيالي ضدّ المؤسسات المالية والمصرفية، نذكر منها:

◆ كاربانك Carbanak

تتعرَّض المؤسسات المالية والمصرفية لهجمات التصيد الاحتيالي بطرق عدة، فعلى سبيل المثال استهدفت مجموعة تدعى "كاربانك" Carbanak الشبكات المصرفية حول العالم، مما أدَّى إلى سرقة أكثر من مليار دولار، وذلك بعدما أصدرت المجموعة أوامر إلى أجهزة الصراف الآلي لتوزيع الأموال النقدية في أوقات معيّنة على أفراد تابعين لها[1].

وتم الكشف عن عملية السّطو الإلكتروني غير المسبوقة من خلال تحقيقات اشترك فيها الإنتربول واليوروبول والسُّلطات من مختلف دول العالم؛ حيث تم سرقة نحو مليار دولار أمريكي على مدار عامين من المؤسسات المالية في جميع أنحاء العالم، ونفَّذ الهجوم مجموعة متعددة الجنسيات من مجرمي الإنترنت من روسيا وأوكرانيا ودول أخرى من أوروبا، والصين.

1. The Great Bank Robbery: Carbanak cybergang steals $1bn from 100 financial institutions worldwide, Kaspersky, February 2015. on site: https://www.kaspersky.com/about/press-releases/2015_the-great-bank-robbery-carbanak-cybergang-steals--1bn-from-100-financial-institutions-worldwide

وقد استخدمت المجموعة الإجرامية Carbanak تقنيات متطوّرة لسرقة الأموال مباشَرة من البنوك، وتجنُّب المستخدِمين (العملاء). وعملت المجموعة منذ عام 2013 على مهاجَمة ما يصل إلى 100 بنك وأنظمة الدفع الإلكتروني ومؤسسات مالية أخرى في 30 دولة، شملت: روسيا والولايات المتحدة وألمانيا والصين وأوكرانيا وكندا وهونغ كونغ وتايوان ورومانيا وفرنسا وإسبانيا والنرويج والهند والمملكة المتحدة وبولندا وباكستان ونيبال والمغرب وأيسلندا وأيرلندا وجمهورية التشيك وسويسرا والبرازيل وبلغاريا وأستراليا. وقُدِّرت المبالغ المسروقة في كل هجوم نفَّذته المجموعة على البنوك بنحو 10 ملايين دولار، واستغرق كل هجوم ما بين شهرين إلى أربعة أشهر بدءاً من إصابة أول جهاز حاسوب تابِع للبنك أو الشركات التابِعة له، من خلال التصيد الاحتيالي وإصابته بالبرمجيات الضّارَّة للوصول غير المصرَّح به إلى الشبكات الداخلية وباقي أجهزة الحاسوب؛ لمتابَعَة مجريات العمليات المتعلّقة بالتحويلات النقدية على شاشات الموظفين بالبنك المستهدَف لتقليد نشاطهم وتحويل الأموال والصرف النقدي[1].

1. Robert E. Holtfreter & Adrian Harrington, Employees are the weakest links, part 1, Data breaches and untrained workers, fraud Magazine, May/June 2016.on site: https://www.fraud-magazine.com/article.aspx?id=4294992844

برمجية طروادة Dyreza

من الهجمات الاحتيالية التي استهدَفَت المؤسسات المالية والمصرفية ما يُعرَف ببرمجية طروادة المصرفية Dyreza، والتي تُشبِه الاتصال الآمِن بالبنوك، وقد تمّ توزيع هذه البرمجية الضّارَّة على 100 ألف جهازٍ حول العالم[1].

وقد استهدفت البرمجية الضّارَّة عملاء البنوك البريطانية، بما في ذلك باركليز Barclays وإتش إس بي سي HSBC، من خلال رسائل البريد الإلكتروني الضّارَّة التي تهدف إلى تثبيت برمجية Dyreza الضّارَّة على أجهزة الحاسوب الخاصة بهم، والتي تُوجّههم إلى مواقع ويب تحتوي على كود JavaScript غامض تمهيداً لتثبيت حصان طروادة.

وفي يومٍ واحدٍ تم إرسال 30 ألف رسالة من رسائل البريد الإلكتروني الضّارَّة من خوادم في المملكة المتحدة وفرنسا وتركيا والولايات المتحدة وروسيا؛ لسرقة بيانات تسجيل الدخول الخاصة بالخدمات المصرفية عبر الإنترنت من المستخدِمين.

1. Stuart, Dredge, Banking trojan Dyreza generating 'tens of thousands' of malicious emails a day, The Guardian, February 2015. on site: https://www.theguardian.com/technology/2015/feb/16/banking-trojan-dyreza-malicious-emails

والبرمجية الضّارَّة Dyreza يتم تثبيتها على أجهزة المستخدِمين وتكون نَشِطَةً فقط عندما يكتبون بيانات تسجيل الدخول على الموقع الخاص بالمؤسسة المصرفية أو الخدمة المالية، ليبدأ مجرمو الإنترنت بحقن كود جافا سكريبت الضّارّ؛ مما يَسمح لهم بسرقة بيانات تسجيل الدخول والتلاعب بالحسابات سراً.

وبرمجية Dyreza تم اكتشافها للمرة الأولى في عام 2014، واعتمدت في تنفيذ هجومها على رسائل البريد الإلكتروني المخادِعة التي تظهر كأنها رسائل رسمية من البنوك. والمقلق في هذه البرمجية الضّارَّة هو قدرتها على تجاوز أمان SSL المستخدَم في الخدمات المصرفية عبر الإنترنت. أما بالنسبة للحدّ من مخاطر وتهديدات هذه البرمجية الضّارَّة فهذا يقع على المستخدِم النهائي أو العميل، وليس المؤسسات المالية والمصرفية المستهدَفة فقط[1].

بالنسبة لهجمات التصيد الاحتيالي التي تُصيب المؤسسات المالية والمصرفية -كما في الأمثلة السابقة- لُوحِظ أنه تم تنفيذها عبر رسائل البريد الإلكتروني المزيَّفة التي كان يَسْهل اكتشاف زيفها في حال كان الموظّف داخل المؤسسة أو المستخدِم النهائي (العميل) على دراية بطرق الاحتيال، وهو ما يتطلّب توعية سيبرانية وتثقيفاً رقمياً لهما.

هل تعلم؟

- أكثر من 90% من جميع عمليات القرصنة الناجحة تبدأ بهجوم تصيد احتيالي، وتُشير التقديرات إلى أن عدد رسائل البريد الإلكتروني التصيدية تضاعف أربع مرّات في عام واحد فقط؛ حيث يتم إرسال نحو 15 مليار رسالة بريد إلكتروني غير مرغوب فيها يومياً، نصفها يَستهدِف مؤسسات مالية أو ينتحل شخصيتها[2].
- في عام 2016، كُشِفَ عن تنفيذ مليون هجمة طروادة مصرفية، بزيادة قدرها 30.6% عن العام 2015، وإن ما يقرب من نصف جميع هجمات التصيد الاحتيالي تضمَّنت إعادة توجيه المستخدِمين إلى موقع ويب مصرفي زائف أو صفحة تم إنشاؤها لسرقة بيانات تسجيل الدخول.

1. Chickowski, Ericka, Dyre New Banking Trojan, Dark Reading, June 2014. on site: https://www.darkreading.com/vulnerabilities-threats/a-dyre-new-banking-trojan
2. Moramarco, Stephen. Phishing attacks in the banking industry, Info Secinstitute, January 2019. on site: https://www.infosecinstitute.com/resources/phishing/phishing-banking-industry/

3- التهديدات السيبرانية المتعلّقة بالذكاء الاصطناعي Artificial Intelligence (AI)

يُمثِّل ظهور أدوات الذكاء الاصطناعي التوليدي طفرةً تكنولوجيةً هائلةً مع ما أحدثته من تأثيرات متفاوتة بين النفع والضّرر على النظام المالي.

نظرياً، يعود الذكاء الاصطناعي بالنَّفع على النظام المالي، إلا أنه عملياً يرتبط مجمل تأثيره بكيفية مُعالَجة التحديات المتعلّقة بالبيانات وتطوير النماذج ونَشْرها على مستوى المؤسسات المالية وبالنسبة للنظام المالي ككلّ.

ففي حال استُخدِمت أدوات الذكاء الاصطناعي بشكلٍ موسَّعٍ في النظام المالي؛ فإن المخاطر التشغيلية تزداد، بما في ذلك المخاطر السيبرانية.

هل تعلم؟

- منذ أواخر عام 2022، زاد الاهتمام بالذكاء الاصطناعي بشكلٍ لافتٍ، ونَمَا حجم الوظائف والابتكارات المتعلّقة به، كما ارتفعت عمليات البحث على جوجل عن المصطلحات المتعلّقة بالذكاء الاصطناعي منذ إطلاق ChatGPT.
- وفقاً لدراسة حديثة، يعتقد 64% من رؤساء الشركات أن الذكاء الاصطناعي سيزيد من إنتاجيَّتهم، بينما أَعْرَب 40% من أصحاب الأعمال عن شعورهم بالقلق بشأن الاعتماد المتزايد على التكنولوجيا[1].

1. Haan, Katherine & Rob Watts, How Businesses Are Using Artificial Intelligence In 2024, Forbes, Apr 2023. on site: https://www.forbes.com/advisor/business/software/ai-in-business/

وعلى الرغم من أن الذكاء الاصطناعي يُعزِّز بشكلٍ كبيرٍ معالَجة البيانات وتوليدها، إلا أن جودة البيانات أحد المخاوف المحيطة باستخدامه في النظام المالي والمصرفي، نتيجة التحيُّزات أو الأخطاء المتأصِّلة في البيانات التي تم تدريب نماذج الذكاء الاصطناعي عليها.

بشكلٍ عامّ، إذا كانت نماذج الذكاء الاصطناعي، بما في ذلك نماذج التعلُّم الآلي والتعلُّم العميق، تَعتمِد على بيانات متحيِّزة أو غير كاملة أو تحتوي على أخطاء؛ يُتوقَّع أن يُنتِج نموذج الذكاء الاصطناعي نتائج غير موثوقة أو متحيِّزة، ونظراً لأن نماذج الذكاء الاصطناعي الحديثة أكثر تعقيداً من النماذج التقليدية، أصبح على الموظفين فَهْم وإعادة بناء التنبؤات المقدَّمة.

وفي حال استندت المؤسسات المالية والمصرفية إلى تنبؤات الذكاء الاصطناعي الخاطئة عند اتخاذ القرارات دون التحقُّق منها، فإن هذا يتسبَّب في خسائر اقتصادية وتحرُّكات سوقية غير منظَّمة. إضافةً إلى أن تعقيد الذكاء الاصطناعي يُصعِّب مسألة تحديد السبب الجذري للأخطاء أو إيجاد تبرير لأي قرار يَعتمِد عليه، مما يُثير تساؤلاً حول مَن يتحمَّل تبعات ما يحدث من خلل وما يترتَّب عليه من عواقب مفاجِئة.

وبالنسبة للآثار المترتِّبة على الذكاء الاصطناعي حيال الاستقرار المالي، ففي حال استخدام غالبية المؤسسات المالية نفس النماذج الأساسية أو نماذج متشابهة يُقدِّمها عدد محدود من المورّدين، فمن المتوقَّع أن تعاني القرارات القائمة على الذكاء الاصطناعي من تحيُّزات وتحديات تكنولوجية مماثلة.

وبهذا يكون الاستقرار المالي مُعرَّضاً للخطر، نتيجة تركّز المورّدين والاختراق التكنولوجي المرتفع. من ناحية أخرى، إذا كانت المؤسسات التي تستخدم الذكاء الاصطناعي محدودة العدد وهناك زيادة وتنوُّع في عدد مُقدِّمي التكنولوجيا المختلفين، فإن المخاطر تحدث بشكلٍ جزئيٍّ اعتماداً على حالات استخدام المؤسسات الفردية.

أما في حال انتشار تكنولوجيا الذكاء الاصطناعي بالمؤسسات المالية وارتفاع عدد المورّدين، فإن المخاطر الناجمة عن الذكاء الاصطناعي على المستوى الجزئي تكون ملموسةً؛ مما يؤدي إلى عواقب على الاستقرار المالي[1].

ونخلص من هذا إلى أن الذكاء الاصطناعي قد يجلب فوائد ومخاطر معاً على مستوى المؤسسات المالية وعلى النظام المالي ككلّ؛ ففي الوقت الذي يعود بالنفع على المستهلِكين والشركات والاقتصاد، من حيث إمكانية زيادة كفاءة الوساطة المالية من خلال معالَجة المعلومات بشكلٍ أسرع وأكثر شموليةً بما يدعم عملية اتخاذ القرار، ويُحقِّق الاستقرار المالي، فإن التحديات التكنولوجية المرتبطة بالذكاء الاصطناعي تزيد من المخاطر المتعلّقة بالتحيُّز وسوء الاستخدام؛ مما يتسبَّب في تشويه نتائج السوق المالية، وإضعاف قوة الإطار التشغيلي؛ أي: أنه سلاح ذو حدَّين.

1. Narechania, Tejas N. and Sitaraman, Ganesh, An Antimonopoly Approach to Governing Artificial Intelligence, January 2024. on site: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=4597080

◆ 4- التهديدات المرتبطة بالعملات المشفَّرة

رغم ما تشهده أسواق العملات المشفَّرة من تطورات واستقطاب للعديد من العملاء، إلا أن البنوك التقليدية لا تزال حذرةً من التعامل بها. ووفقاً لدراسة أجرتها جمعية المتخصِّصين المعتمَدين في مكافحة غسل الأموال (ACAMS) ومعهد الخدمات المَلَكية المتحدة في المملكة المتحدة، فإن ما يقرب من 63% من المستجيبين الذين يعملون في الصناعة المصرفية رأوا أن العملات المشفَّرة تُشكِّل خطراً، وليس كما يزعم بعضهم بأنها فرصة جيدة للقطاع المالي والمصرفي[1].

هذا إضافة إلى التّقلبات التي تشهدها أسعار العملات المشفَّرة (وتحديداً البيتكوين)، وترجع أسباب ذلك إلى حجم السوق والسيولة وعدد المشاركين في السوق، مما يجعل العملة المشفَّرة ليست أداة استثمار مستقرَّة مع مرور الوقت.

كما تقلِّل العملة المشفَّرة التي تُديرها البنوك المركزية من جاذبية الأصول، لهذا لا تعتقد بعض البنوك أنها قادرة على دخول هذا المجال بنجاح، إلى جانب أن الطبيعة اللامركزية للعملة المشفَّرة يُنظَر إليها كأداة لتقويض سلطة البنوك المركزية؛ مما يجعل البعض يعتقد أن هذه البنوك لن تكون قادرةً على التَّحكُّم في المعروض النقدي.

احذر!

ما يقرب من 63% من المستجيبين الذين يعملون في الصناعة المصرفية رأوا أن العملات المشفَّرة تُشكِّل خطراً، وليس كما يزعم بعضهم بأنها فرصة جيدة للقطاع المالي والمصرفي؛ نتيجةً للتّقلبات التي تشهدها أسعارها.

1. Izenman, Kayla. this regulator wants to help banks embrace cryptocurrency, Rusi, October 2020. on site: : https://rusi.org/in-the-news/regulator-wants-help-banks-embrace-cryptocurrency.

كما أن الأصول المشفَّرة ليست مناسبة لمعظم المستثمرين الأفراد، سواء كاستثمار أو مخزن للقيمة، أو كوسيلة للدفع؛ بسبب تزايد خسائرهم المالية منها، وتشمل مخاطر حماية المستهلِك:

- المعلومات المضلِّلة.
- غياب الحقوق والحماية، مثل إجراءات الشكاوى أو آليات استرداد الحقوق.
- تعقيد المعاملات.
- الاحتيال والأنشطة الخبيثة، مثل غسل الأموال والجرائم الإلكترونية والقرصنة وبرمجيات الفدية.
- التلاعب بالسوق نتيجة الافتقار إلى شفافية الأسعار وانخفاض السيولة.

وقد يؤدي انخراط المؤسسات المالية بشكلٍ أكبر إلى تغذية نموّ الأصول المشفَّرة بشكلٍ أكبر، وبالتالي زيادة مخاطر الاستقرار المالي، ما يعني أن التعرُّض للأصول المشفَّرة على أساس رأس المال من جانب المؤسسات النظامية -خاصةً إذا كانت تلك الأصول غير مدعومة- قد يتسبَّب في تعرُّض رأس المال للخطر، وله تأثيرات محتَمَلة على ثقة المستثمرين والإقراض والأسواق المالية، إضافةً إلى مواجَهة المؤسسات المالية مخاطر تتعلَّق بالسُّمعة.

احذر!

تشمل مخاطر حماية المستهلِك جرّاء العملات المشفَّرة: المعلومات المضلِّلة، غياب الحقوق والحماية مثل: إجراءات الشكاوى أو آليات استرداد الحقوق، تعقيد المعاملات، الاحتيال والأنشطة الخبيثة مثل: غسل الأموال والجرائم الإلكترونية والتلاعب بالسوق نتيجة الافتقار إلى شفافية الأسعار وانخفاض السيولة.

ومن التحديات التي تواجه القطاع المالي والمصرفي:

شبكات الجيل الخامس 5G:

شكّل انتشار شبكات الجيل الخامس على نطاق واسعٍ، مع ما توفّره من نطاق تردُّدي متزايد وزمن انتقال أقل، تحديات أمنية جديدة تتعلّق بثغرات شبكة الجيل الخامس؛ حيث تتزايد فرص تنفيذ هجمات رفض الخدمة الموزّعة (DDoS).

القياسات الحيوية السلوكية Behavioral Biometrics:

تستخدِم القياسات الحيوية السلوكية أنماط سلوك المستخدِم، مثل نمط الكتابة وحركات الفأرة (الماوس) وإيماءات شاشة اللمس؛ للتحقُّق من هُويَّة المستخدِمين. ويمكن الاستفادة من هذه التقنية في تعزيز الأمان من خلال مراقَبة تفاعلات المستخدِم باستمرار لمَنْع الوصول غير المصرَّح به والأنشطة الاحتيالية[1].

تطوّر برمجيات الفدية Ransomwar:

يُتوقَّع أن يتسبّب تطوّر هجمات برمجيات الفدية في تنفيذ هجمات أكثر استهدافاً وتخصيصاً. ومن التقنيات المتطوّرة التي أُدْخِلت على برمجيات الفدية "الابتزاز المزدوج" Double Extortion، ويُقصَد به: التهديد بتسريب البيانات المسروقة لممارسة مزيدٍ من الضغط على الضحايا.

1. Cyber Shockwave: Exposing the Major Finance Industry Breaches of 2023 and Critical Lessons Learnt. Data Dynamic Sinc, on site: https://www.datadynamicsinc.com/blog-cyber-shockwave-exposing-the-major-finance-industry-breaches-of-2023-and-critical-lessons-learnt/

التزييف العميق Deepfakes والاحتيال على الهُويَّة Identity Fraud:

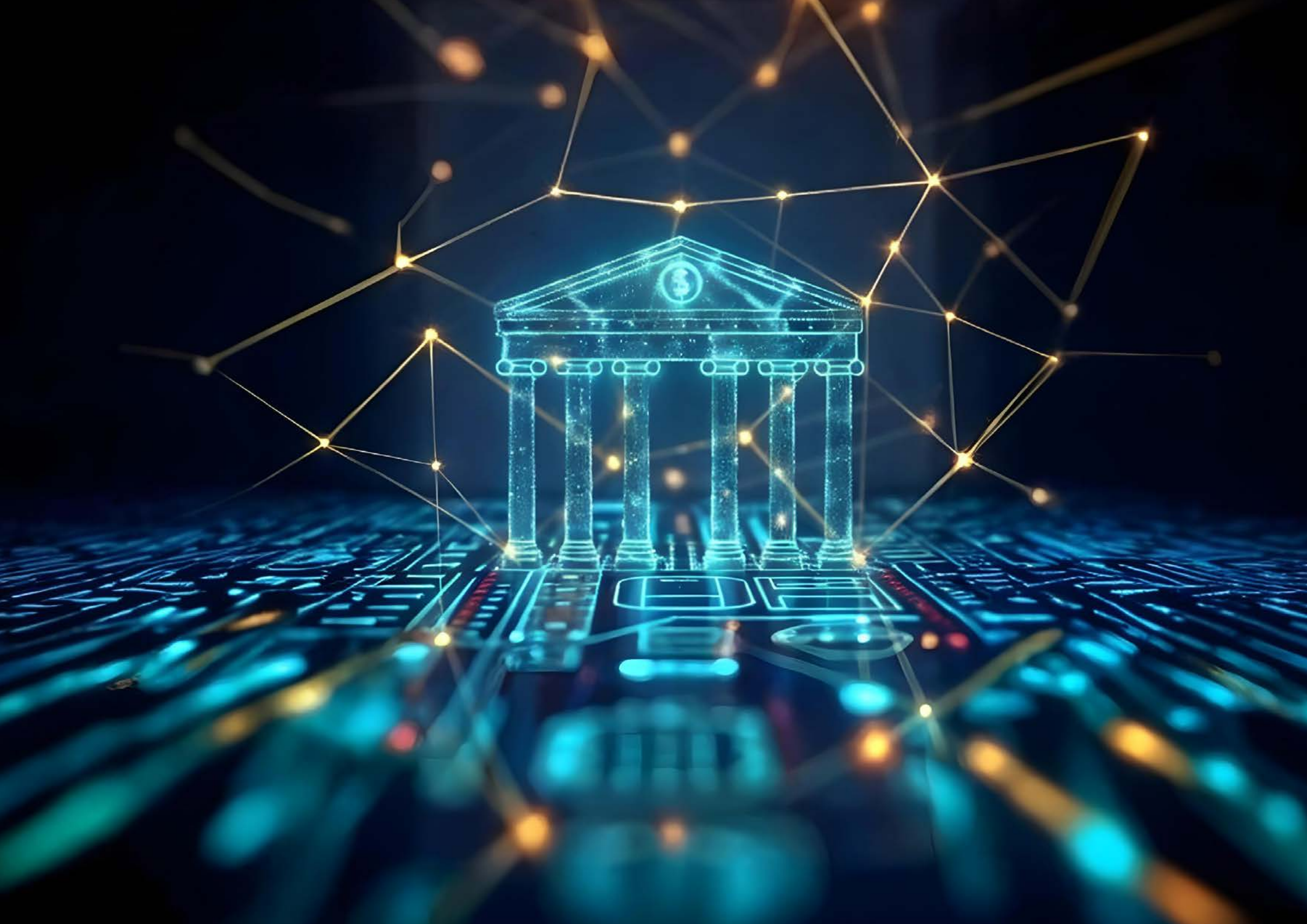
تُستخدَم تقنية التزييف العميق في إنشاء محتويات صوتية وفيديوهات واقعية مزيفة تُحاكِي الأصلية؛ بهدف الاحتيال على الهُويَّة وتنفيذ هجمات الهندسة الاجتماعية.

أمن السحابة Cloud Security:

مع الاعتماد المتزايد على تخزين البيانات على السحابة، شكَّلت مسألة تأمين بيئات السحابة أمراً مقلقاً؛ إذ قد تتسبَّب التكوينات الخاطئة وواجهات برمجة التطبيقات غير الآمِنة في تعريض الخدمات السحابية للاختراقات، ومن ثَمّ سرقة البيانات الحساسة.

احذر!

من التقنيات المتطورة التي أُدْخِلت على برمجيات الفدية: "الابتزاز المزدوج" Double Extortion، الذي يسعى إلى التهديد بتسريب البيانات المسروقة لممارسة مزيدٍ من الضغط على الضحايا.



02

الفصل الثاني

إستراتيجيات تعزيز السلامـة الرقميـة في القطاع المالـي والمصرفي

- أولاً: الثغرات الرقمية والمعرفية في القطاع المالي والمصرفي.
- ثانياً: دَور الموظّفين داخل المؤسسات المالية والمصرفية في تحقيق السلامة الرقمية.

أولاً: الثغرات الرقمية والمعرفية في القطاع المالي والمصرفي

1- الثغرات المعرفية

يُقصَد بالثغرات المعرفية النقص في الوعي السيبراني لدى العاملين في القطاع المالي والمصرفي؛ بحيث يتمكّن المجرمون من خداع هؤلاء الموظّفين واستدراجهم للوقوع ضحايا للتصيد الاحتيالي، أو دَفْعهم لتسريب معلومات مصرفية مهمة دون دراية. وبشكلٍ عامّ فإن المعلومات الشخصية والبيانات المالية التي تحتفظ بها المؤسسات المالية والمصرفية تجعلها أهدافاً واضحة؛ حيث يُحقِّق مجرمو الإنترنت مكاسب مالية ضخمة من هذا النوع من المعلومات إما عن طريق بيعها على الويب المظلم؛ وإما عن طريق تحويل الأموال من الحسابات الشخصية المخترَقة إلى حساباتهم الخاصة.

لهذا تُعدّ نقاط الضعف الداخلية في البنوك والمؤسسات المالية والمصرفية من أخطر الثغرات التي يتسلَّل منها هؤلاء المجرمون، علماً بأنّ هذه الثغرات قد تَنتُج دون قصدٍ عن الموظّفين.

2- تزايد عدد مستخدمي الخدمات المالية والمصرفية

مع نقص العاملين بمجال الأمن السيبراني وتزايد عدد مستخدمي الخدمات المالية والمصرفية، أدى ذلك إلى ظهور نقطة ضعف في القطاع المالي والمصرفي تفرض على المؤسسات التعامل مع مجموعة متنوعة من نقاط الاتصال، التي لا تملك سوى القليل من صلاحيات التحكُّم في كيفية تفاعل هؤلاء المستخدِمين؛ مما يمنح مجرمي الإنترنت مزيداً من الفرص لتنفيذ هجماتهم.

فقد تتسبَّب الأجهزة الشخصية للمستخدِمين في تسلُّل مجرمي الإنترنت واختراق الشبكات المالية، خاصةً إذا لم يُفعِّل المستخدِم ميزات الأمان، مثل المصادقة متعددة العوامل.

وأمام هذا التهديد، من المهمّ تنفيذ سياسات لحماية مستخدمي الشبكة؛ بحيث تساعد على تأمين نقاط الاتصال الداخلية، مثل المصادقة متعددة العوامل، ومراجعة حقوق الوصول. بالإضافة إلى ذلك، يمكن لميزات مثل المصادقة القائمة على المخاطر Risk-Based Authentication (RBA) تطبيق المستوى الصحيح من المصادقة اعتماداً على ظروف المستخدِم، مثل الاتصال بالشبكة محلياً أو عن بُعد[1].

1. Nair, Ajit. What is Risk-Based Authentication and why banks should implement it? Wibmo, on site: https://wibmo.co/what-is-risk-based-authentication-and-why-banks-should-implement-it/

3- فجوة التكنولوجيا

تُعدّ مواقع الويب والتطبيقات المالية والمصرفية من نقاط الضعف في بنية المؤسسات المالية والمصرفية؛ حيث كانت الأكثر عُرضةً للاختراق. وقد توصلت دراسة حديثة إلى أن 80% من المواقع التي خضعت للاختبار كانت عُرضةً لهجمات البرمجيات النصية عبر المواقع (XSS)، والتي تُمكِّن مجرمي الإنترنت من تشغيل أكواد ضارَّة على موقع ويب أو تطبيق، ومِن ثَمّ الوصول إلى ملفات تعريف الارتباط الخاصة بالمستخدِم وجميع البيانات الحساسة[1].

وتؤدّي هذه الثغرات إلى انعدام الثقة بين المستخدِم والمؤسسة، لذا، لكي تكون المؤسسات المالية والمصرفية قادرة على المنافسة والحدّ من المخاطر السيبرانية عليها تأمين مواقع الويب والتطبيقات، مثل قيام المطوّرين في مراحل بناء التطبيق باختبار التعليمات البرمجية وتقييم قدرة التطبيقات على مواجهة محاولات الخرق.

احذر!

تُعدّ مواقع الويب والتطبيقات المالية والمصرفية من نقاط الضعف في بنية المؤسسات المالية والمصرفية؛ حيث كانت الأكثر عُرضةً للاختراق، وشكَّلت هجمات البرمجيات النصية عبر المواقع (XSS) التهديد الأبرز لـ 80% من المواقع التي خضعت لإحدى الدراسات.

1. Whittaker, Zack, Bank web apps are the “most vulnerable” to getting hacked, new research says, ZD NET, April 2018. On site: https://www.zdnet.com/article/bank-sites-and-web-apps-are-most-vulnerable-to-hackers/

ويساعد تشغيل جدران حماية تطبيقات الويب، سواء أكانت برامج أم أجهزة مخصَّصة أم جدران حماية للأجهزة المعيارية، على مَنْع الوصول غير المصرَّح به إلى الأقسام الإدارية بمواقع الويب أو التطبيقات المالية والمصرفية.

هل تعلم؟

1. 95% من مشكلات الأمن السيبراني نتجت عن أخطاء بشرية.
2. يحدث هجوم إلكتروني واحد كل 39 ثانية.
3. قُدِّرت تكلفة خرق البيانات في عام 2023 على مستوى العالم بنحو 4,45 مليون دولار.
4. 15% من خروقات المؤسسات نتجت عن أجهزة مفقودة، سواء أكان جهازاً خاصاً بالمؤسسات أم جهازاً شخصياً.

احذر!

15% من خروقات المؤسسات المالية والمصرفية نتجت عن أجهزة مفقودة، سواء أكان جهازاً خاصاً بالمؤسسات أم جهازاً شخصياً للموظفين العاملين بها.

ثانياً: دَور الموظّفين داخل المؤسسات المالية والمصرفية في تحقيق السلامة الرقمية

يُمثّل الموظّف جدار الحماية البشري وخطّ الدفاع الأول ضدّ التهديدات السيبرانية التي تتعرَّض لها المؤسسات المالية والمصرفية، وكلما امتلك هذا الموظّف المهارات السيبرانية اللازمة، تمكَّنت المؤسسة من مَنْع الخروقات الأمنية المحتَمَلة، فهذه المسؤولية لا تقع على كاهل قسم تكنولوجيا المعلومات فقط، بل لكل موظّف دَور مُهم بها.

ومن أجل ذلك ينبغي توعية الموظفين بما يلي:

- تمكين الموظّف من خلال التوعية بمفاهيم السلامة الرقمية؛ حيث تُزوِّد برامج التوعية الموظّفين بالمهارات اللازمة للتعرُّف على محاولات التصيد الاحتيالي، وتكتيكات الهندسة الاجتماعية، وفَهم أهمية ممارسات كلمات المرور القوية[1].
- الإبلاغ عن الحوادث: يُعدّ تشجيع الموظّفين على ثقافة الشفافية أمراً ضرورياً لدفعهم إلى الإبلاغ عن الأنشطة المشبوهة فوراً، والاستفادة من قنوات الاتصال المفتوحة بين الموظّفين وقسم تكنولوجيا المعلومات.

1. Henning, Jon, Explaining the Crucial Role Employees Play in Cybersecurity, Coordinated Business Systems, January 2024. on site: https://2u.pw/jPXiKXee.

- مع الاتجاه للاعتماد على العمل عن بُعد على مستوى العالم ظهرت تحديات جديدة فرضت على المؤسسات تأمين بيئتها الداخلية والخارجية أيضاً، مما أوجد حاجة إلى زيادة وعي فريق العمل بأهمية تأمين بيئة العمل المحيطة به، مثل التأكُّد من أمان اتصالات Wi-Fi، وتحديث برامج مكافحة الفيروسات، واستخدام قنوات الاتصال المشفَّرة.
- فَرَض التطور المستمرّ للهجمات الإلكترونية حاجة ملحَّة إلى الالتزام بالتحديثات المنتظِمة والتواصل من قسم تكنولوجيا المعلومات، وإطلاع الموظّف على التهديدات الناشئة.
- إدراك الموظّفين أن البريد الإلكتروني للمؤسسة ليس مجرد أداة تواصل، بل بوابة لشنّ هجمات التصيد الاحتيالي واختراق البيانات، وأن خطر الهجمات الإلكترونية ليس بعيداً، بل يترقَّبون مواجهته بأنفسهم وعملائهم ومؤسستهم ككلّ.
- بمجرد معرفة الموظّف كيفية تحديد رسائل البريد الإلكتروني المشبوهة أو الاحتيالية، يمكن حينئذٍ تقليل هجمات التصيد بنسبة 60%[1].
- يُقلِّل التدريب على السلامة الرقمية من الفوضى الداخلية التي تُسبِّبها الخروقات.
- الالتزام بالسياسات والممارسات الأمنية المعتَمَدة داخل المؤسسة مثل: قواعد إنشاء كلمات المرور، وضوابط الوصول، ومشاركة البيانات.

1. The Role of Employee Training in Cybersecurity for Banks. Register Bank, on site: https://register.bank/media/cybersecurity-employee-training-banks/

التمارين تعتمد على المادة العلمية المقدَّمة في سياق هذا الكتيب، وهي مذكورة هنا بدون حل، وتم إرفاق الحل في نهاية الكُتَيِّب.

التمرين الأول

- **اختر الإجابة الصحيحة**

1. تؤدي معايير الأمان غير الكفء في المؤسسات المالية والمصرفية إلى .....

1. سرقة البيانات.
2. تسلُّل مجرمي الإنترنت.
3. اختراق العملاء.
4. جميع ما سبق.

2. يتسبّب الاستخدام المتزايد لأدوات الذكاء الاصطناعي بالنظام المالي في .....

1. ظهور سلوك القطيع.
2. التمييز بين العملاء.
3. ارتفاع وتيرة المخاطر التشغيلية.
4. جميع ما سبق.

3. تشمل مخاطر حماية المستهلِك الناتجة عن الاستثمار في العملات المشفّرة .....

1. تداول المعلومات الصحيحة المثيرة لقلق العملاء.
2. غياب الحقوق والحماية.
3. سهولة المعاملات.
4. جميع ما سبق.

4. يُعدّ ..... أحد التهديدات المترتّبة على استخدام العملات المشفّرة نتيجة استخدام تقنية سلسلة الكتل Blockchain.

1. هجمات الهندسة الاجتماعية.
2. التصيد الاحتيالي.
3. غسل الأموال.
4. جميع ما سبق.

5. يُتوقَّع أن يتسبّب تطوّر هجمات برمجيات الفدية في تنفيذ هجمات أكثر استهدافاً وتخصيصاً، ومن التقنيات المتطوّرة التي أُدخِلت عليها .....

1. الابتزاز العكسي.
2. هجمات القاموس.
3. الابتزاز المزدوج.
4. جميع ما سبق.

6. من توصيات تخفيف مخاطر سلاسل التوريد

1. خفض الاستثمار في التكنولوجيا.
2. الاستعانة بأنظمة المراقَبة والإنذار المبكّر.
3. تثبيت قاعدة المورّدين.
4. جميع ما سبق.

7. من نقاط الضعف في الأمن السيبراني بالقطاع المالي والمصرفي

1. التكوين غير الصحيح للأنظمة والخوادم.
2. الاحتفاظ بالمعلومات الشخصية والبيانات المالية.
3. الاعتماد على بائعين من جهات خارجية.
4. جميع ما سبق.

التمرين الثاني

اكتب كلمة (صحيح) بجانب العبارة الصحيحة، وكلمة (خطأ) بجانب العبارة الخاطئة، وفي حال الخطأ صحح العبارة

1. تحتاج الأجهزة المستخدَمة كالهواتف والحاسوب اللوحي إلى اشتراطات أمنية قوية لحماية المعاملات المالية التي تتم بواسطتها عبر الإنترنت. (.....)

.....

2. يساعد التنسيق بين المؤسسات المالية والمصرفية وبين أجهزة العملاء قبل إجراء المعاملات في منع الوصول غير المصرَّح به. (.....)

.....

3. يساعد الاستخدام الموسَّع لأدوات الذكاء الاصطناعي بالنظام المالي في الحدّ من المخاطر التشغيلية والسيبرانية. (.....)

.....

4. رغم تعزيز الذكاء الاصطناعي لمعالجة البيانات وتوليدها، إلا أن جودة البيانات أحد المخاوف المحيطة باستخدامه في النظام المالي والمصرفي. (.....)

.....

5. تعقيد الذكاء الاصطناعي لا ينعكس على تحديد الأسباب الجذرية للأخطاء ويساعد في التوصُّل إلى القرارات سريعاً وبصورة واضحة. (.....)

.....

6. من الخدمات المقدَّمة عبر تطبيقات الخدمات المصرفية عبر الهاتف المحمول، الخدمات الاستثمارية كأسعار الأسهم والإشعارات المتعلِّقة بأسعار الأوراق المالية. (.....)

.....

7. تُعدّ هجمات التصيد الاحتيالي من التهديدات الشائعة لقطاع الصناعة المصرفية. (.....)

.....

8. لا يُشكِّل سلوك العملاء تحدياً للخدمات المقدَّمة من المؤسسات المالية والمصرفية. (.....)

.....

9. تكسر تطبيقات الخدمات المصرفية قيود الوقت، إذ يمكن للعميل استخدامها لفترة طويلة أو إبقاؤها مفتوحة دون استخدام لفترة ما. (.....)

.....

10. تُعدّ جودة البيانات أحد المكاسب المترتِّبة على استخدام الذكاء الاصطناعي في المؤسسات المالية والمصرفية. (.....)

.....

التمرين الثالث

أكمل العبارات التالية

1. ..... هي خدمة عبر الإنترنت يُقدِّمها البنك أو المؤسسة المالية للعملاء لتمكينهم من إجراء معاملاتهم النقدية من خلال الهاتف أو الجهاز اللوحي، وتُتيح الخدمة للعملاء الوصول المباشر إلى حساباتهم المتاحة أو بياناتهم المصرفية.

2. ..... من دونها لا تستطيع المؤسسات المالية والمصرفية التعامل عند حدوث هجوم إلكتروني أو خرق أمني، فهي تُخفِّف الآثار الناتجة عنها.

3. وسيلة مجرمي الإنترنت في تنفيذ هجمات التصيد الاحتيالي هي .....؛ حيث يقومون بخداع الضحايا وإيهامهم بأن حساباتهم تواجه نشاطاً مشبوهاً.

4. من التقنيات المتطورة التي أُدْخِلت على برمجيات الفدية .....، الذي يُسَرِّب البيانات المسروقة لممارسة مزيدٍ من الضغط على الضحايا.

5. ..... هي تقنية تُستخدَم في إنشاء محتويات صوتية وفيديوهات تُحاكِي الأصلية بهدف سرقة الهُويَّة.

6. يلجأ مجرمو الإنترنت إلى أساليب احتيالية مبتكَرَة مثل ..... ، لتنفيذ عملية احتيال مُغرية لعملاء البنوك للكشف عن بياناتهم الحساسة.

7. من الضروري أن يتم التنسيق بين المؤسسات المالية والمصرفية وبين أجهزة العملاء من خلال ..... قبل إجراء المعاملات المالية لمنع الأجهزة غير المصرَّح بها من إجراء التحويلات المالية.

8. تشمل مخاطر حماية المستهلِك الناتجة عن الأصول المشفَّرة ..... ، ..... ، .....

9. أسهم انتشار شبكات الجيل الخامس 5G على نطاق واسع في تزايد فرص تنفيذ هجمات .....

10. تستخدم ..... أنماط سلوك المستخدِم، مثل نمط الكتابة وحركات الفأرة (الماوس) وإيماءات شاشة اللمس، للتحقُّق من هُويَّة المستخدِمين.

حلّ التمارين والتدريبات

السؤال

التمرين الأول: اختر الإجابة الصحيحة

الإجابة

1. جميع ما سبق.
2. جميع ما سبق.
3. غياب الحقوق والحماية.
4. غسل الأموال.
5. الابتزاز المزدوج.

6. الاستعانة بأنظمة المراقَبة والإنذار المبكّر.

7. جميع ما سبق.

السؤال

التمرين الثاني: اكتب كلمة (صحيح) بجانب العبارة الصحيحة، وكلمة (خطأ) بجانب العبارة الخاطئة، وفي حال الخطأ صحح العبارة

الإجابة

1. صحيح.
2. صحيح.
3. خطأ؛ يؤدي الاستخدام الموسَّع لأدوات الذكاء الاصطناعي إلى زيادة المخاطر التشغيلية، بما في ذلك المخاطر السيبرانية.
4. صحيح.
5. خطأ؛ تعقيد الذكاء الاصطناعي يُصعِّب مسألة تحديد السبب الجذري للأخطاء أو إيجاد تبرير لأي قرار يعتمد عليه، مما يثير تساؤلاً حول مَن يتحمَّل تبعات ما يحدث من خلل وما يترتَّب عليه من عواقب مفاجئة.

6. صحيح.

7. صحيح.

8. خطأ؛ من التحديات التي تواجه الخدمات المصرفية عبر الهاتف المحمول وأمن البيانات هو سلوك العميل، إذ أظهرت أبحاث أن أكثر من نصف المستخدمين لتلك الخدمات يُظهرون سلوكاً محفوفاً بالمخاطر ولا يعون المخاطر المرتبطة بالاحتيال.

9. خطأ، يخضع استخدام تطبيقات الخدمات المصرفية لقيود الوقت؛ حيث لا يمكن للعميل استخدامها لفترة طويلة أو إبقاؤها مفتوحة دون استخدام لفترة ما؛ لأن ذلك يزيد من فرص المعاملات الاحتيالية.

10. خطأ؛ بل تُعدّ أحد المخاوف المحيطة باستخدامه في النظام المالي والمصرفي، نتيجة التحيّزات أو الأخطاء المتأصّلة في البيانات التي تم تدريب نماذج الذكاء الاصطناعي عليها.

السؤال

التمرين الثالث: أكمل العبارات التالية

الإجابة

1. الخدمات المصرفية عبر الهاتف المحمول.
2. خطة الاستجابة للحوادث.
3. خَلْق شعور بالإلحاح والذعر.
4. الابتزاز المزدوج.
5. التزييف العميق.

6 عروض الهدايا.

7 المصادقة.

8 المعلومات المضلّلة - غياب الحقوق والحماية - الاحتيال والأنشطة الخبيثة.

9 رفض الخدمة الموزّعة (DDoS).

10 القياسات الحيوية السلوكية.

المراجع

1. Narayanan, Lakshmi. Benefits and Importance of Cybersecurity in Banking Sector Teceze, February 2024. On site: https://teceze.com/cybersecurity-in-banking-importance-and-threats-challenges-benefits
2. Mobile Banking: What are the Advantages and Imminent Challenges? The Salmon Factor, On site: https://thesalmonfactor.com/mobile-banking-advantages-and-imminent-challenges.
3. Banking on Security: Navigating the Cyber Threat Landscape in the Digital Age, the global treasurer, April 2024, on site: https://www.theglobaltreasurer.com/2024/04/04/banking-on-security-navigating-the-cyber-threat-landscape-in-the-digital-age/
4. Sarin, Arvind. Top 3 Challenges in Mobile Banking App Development. Copper Digital, on site: https://copperdigital.com/blog/problems-and-solutions-for-financial-apps/
5. Sarin, Arvind. Top 3 Challenges in Mobile Banking App Development. Copper Digital, on site: https://copperdigital.com/blog/problems-and-solutions-for-financial-apps/

6. Alexander Eremin, The Faketoken Trojan sends out offensive texts, Kaspersky, January 2020. on site: https://www.kaspersky.com/blog/faketoken-trojan-sends-offensive-sms/32048/

7. Sasovets, Ihor. Cyber Security in Banking: How We Address Rising Challenges, Tech Magic, May 2024. on site: https://www.techmagic.co/blog/cybersecurity-in-banking/

8. The Great Bank Robbery: Carbanak cybergang steals $1bn from 100 financial institutions worldwide, Kaspersky, February 2015. on site: https://www.kaspersky.com/about/press-releases/2015_the-great-bank-robbery-carbanak-cybergang-steals--1bn-from-100-financial-institutions-worldwide

9. Robert E. Holtfreter & Adrian Harrington, Employees are the weakest links, part 1, Data breaches and untrained workers, fraud Magazine, May/June 2016.on site: https://www.fraud-magazine.com/article.aspx?id=4294992844

10. Stuart, Dredge, Banking trojan Dyreza generating 'tens of thousands' of malicious emails a day, The Guardian, February 2015.onsite:https://www.theguardian.com/technology/2015/feb/16/banking-trojan-dyreza-malicious-emails

11. Chickowski, Ericka, Dyre New Banking Trojan, Dark Reading, June 2014. on site: https://www.darkreading.com/vulnerabilities-threats/a-dyre-new-banking-trojan.

12. Moramarco, Stephen. Phishing attacks in the banking industry, Info Secinstitute, January 2019. on site: https://www.infosecinstitute.com/resources/phishing/phishing-banking-industry/

13. Haan, Katherine & Rob Watts, How Businesses Are Using Artificial Intelligence In 2024, Forbes, Apr 2023. on site: https://www.forbes.com/advisor/business/software/ai-in-business/

14. Narechania, Tejas N. and Sitaraman, Ganesh, An Antimonopoly Approach to Governing Artificial Intelligence, January 2024. on site: https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=4597080

15. Izenman, Kayla. this regulator wants to help banks embrace cryptocurrency, Rusi, October 2020. on site: https://rusi.org/in-the-news/regulator-wants-help-banks-embrace-cryptocurrency.

16. Cyber Shockwave: Exposing the Major Finance Industry Breaρches of 2023 and Critical Lessons Learnt. Data Dynamic Sinc, on site: https://www.datadynamicsinc.com/blog-cyber-shockwave-exposing-the-major-finance-industry-breaches-of-2023-and-critical-lessons-learnt/

17. Nair, Ajit. What is Risk-Based Authentication and why banks should implement it? Wibmo, on site: https://wibmo.co/what-is-risk-based-authentication-and-why-banks-should-implement-it/

18. Whittaker, Zack, Bank web apps are the “most vulnerable” to getting hacked, new research says, ZD NET, April 2018. On site: https://www.zdnet.com/article/bank-sites-and-web-apps-are-most-vulnerable-to-hackers/

19. Henning, Jon, Explaining the Crucial Role Employees Play in Cybersecurity, Coordinated Business Systems, January 2024. on site: https://2u.pw/jPXiKXee.

20. The Role of Employee Training in Cybersecurity for Banks. Register Bank, on site: https://register.bank/media/cybersecurity-employee-training-banks/

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative