



مصرف سورية المركزي
CENTRAL BANK OF SYRIA

بالتعاون مع



الاتحاد الدولي للمصرفيين العرب
World Union of Arab Bankers

التكنولوجيا والأمن السيبراني في العمل المصرفي

14-13
كانون ثاني / يناير
2026

فندق داماروز - دمشق
الجمهورية العربية السورية



التكنولوجيا والأمن السيبراني في العمل المصرفي

الخلاصة:

تهدف هذه الدورة التي تمتد على يومين إلى تسليط الضوء على أهمية الأمن السيبراني في تعزيز سلامة النظام المصرفي وحمايته من الجرائم المالية وغسل الأموال. في عصر الرقمية، تزداد التهديدات السيبرانية بشكل كبير، مما يستلزم من المؤسسات المالية اتخاذ تدابير وقائية فعالة لحماية المعلومات الحساسة والعمليات المصرفية.

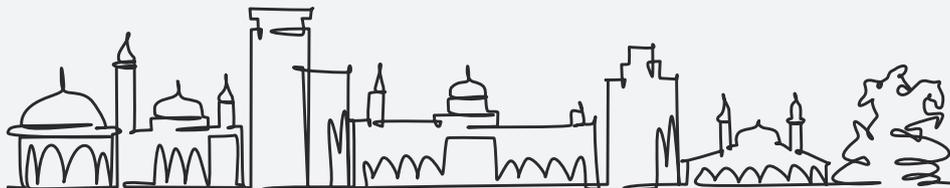
سنستعرض كيفية تأثير ضعف الأمن السيبراني على احتمال تعرض المصارف لانتهاكات مثل غسل الأموال، حيث يمكن للقرصنة استخدام الثغرات للوصول إلى بيانات العملاء وتيسير عمليات غير قانونية.

سوف نتناول استراتيجيات تعزيز الأمان، فهم التهديدات السيبرانية، وأفضل الممارسات لحماية المؤسسات من الهجمات التي يمكن أن تستغلها العصابات المالية.

ولمواجهة التحديات أعلاه، فلنبدأ بمهمتنا نحو بناء ثقافة أمان قوية، بمشاركة الجميع في مسؤولياتهم للحفاظ على استقرار وأمان القطاع المصرفي.

بناء على ما تقدم، نعدد فيما يلي الأهداف الرئيسية لهذه الدورة :

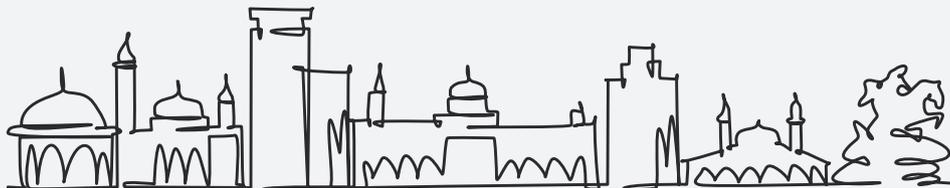
- تعزيز فهم المشاركين لأهمية الأمن السيبراني في القطاع المصرفي.
- تعريف المشاركين بأحدث الأساليب والتقنيات المستخدمة في مواجهة التهديدات السيبرانية.
- تعزيز مهارات المشاركين في وضع سياسات وإجراءات تتماشى مع معايير الأمان اللازمة.
- إعداد المشاركين ليكونوا قادرين على استجابة فعالة لحوادث الأمن السيبراني.
- توعية المشاركين بأهمية الشراكة بين التكنولوجيا والأمن لتعزيز حماية البيانات المصرفية.



التكنولوجيا والأمن السيبراني في العمل المصرفي

المواضيع:

اليوم الأول:	اليوم الثاني:
<p>١ - مقدمة</p> <p>- تعريف التكنولوجيا والأمن السيبراني</p> <p>- أهمية الأمن السيبراني في القطاع المصرفي</p> <p>٢-التحديات الحالية في الأمن السيبراني</p> <p>- أنواع التهديدات السيبرانية (الهجمات الإلكترونية، البرمجيات الخبيثة، التصيد الاحتمالي)</p> <p>- أمثلة على خروقات بيانات سابقة في البنوك</p> <p>- أثر الاختراقات على الثقة والمصادقية</p> <p>٣- الأسس التقنية للأمن السيبراني</p> <p>- مفهوم حماية المعلومات وسرية البيانات</p> <p>- آليات الأمان الأساسية (التشفير، الجدران النارية، المصادقة المتعددة العوامل)</p> <p>- تقنيات التعرف على النقاط الضعيفة (تقنيات تحليل المخاطر)</p> <p>٤- استراتيجيات مقاومة الهجمات السيبرانية</p> <p>- تطوير سياسات أمان فعالة</p> <p>- أفضل الممارسات في التعليم والتدريب للموظفين</p> <p>- أهمية تحديث الأنظمة والبرامج باستمرار</p> <p>- الإحتيال كنتيجة حتمية لمخاطر الأمن السيبراني (Fraudulent Cyber-enabled financial Crime)</p>	<p>٥ - دور التكنولوجيا الحديثة</p> <p>- استخدام الذكاء الاصطناعي في تعزيز الأمن السيبراني</p> <p>- تطبيقات التكنولوجيا المالية (FinTech) وتأثيرها على النظام المصرفي-selfies-liveness checks</p> <p>- ضرورة مراقبة الأداء الأمني وتحليل البيانات</p> <p>- استغلال الذكاء الصناعي التوليدي (GAI) في عمليات الاحتيال المصرفية وتزوير الهوية واختراق الحسابات</p> <p>٦ - حماية البيانات وخطط الاستجابة للطوارئ</p> <p>- مراجعة السياسات والقوانين المتعلقة بحماية البيانات</p> <p>- كيفية بناء خطة استجابة للحوادث الأمنية</p> <p>- أهمية التفاعل مع الجهات الحكومية ومسؤولي الأمن السيبراني</p> <p>٧ - دراسات حالة ومناقشات</p> <p>- تحليل حالات تعرض المصارف للاختراق</p> <p>- تناول المناقشات العملية حول كيفية منع حدوث ذلك مستقبلاً</p> <p>٨ - خلاصة وتوصيات</p> <p>- تلخيص النقاط الأساسية التي تم تناولها</p> <p>- إعداد خطة عمل لتعزيز ثقافة الأمن السيبراني في المصرف</p> <p>٩ - أسئلة وأجوبة</p> <p>- فتح المجال للأسئلة من المشاركين</p> <p>- مناقشة التحديات التي يواجهونها في العمل</p>



التكنولوجيا والأمن السيبراني في العمل المصرفي

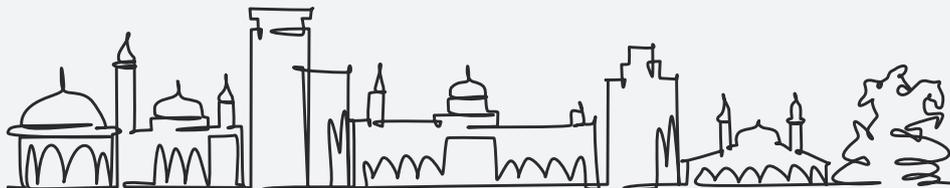
المشاركون المستهدفون:

- رؤساء ومدراء وحدات تقنية المعلومات في المصارف والمؤسسات المالية
- مدراء ومسؤولو الأمن السيبراني وأمن المعلومات
- مدراء إدارات المخاطر والامتثال ومكافحة غسل الأموال وتمويل الإرهاب
- مدراء وأعضاء دوائر التدقيق والرقابة الداخلية
- مسؤولو حماية البيانات والخصوصية والحوكمة التقنية
- مسؤولو التحول الرقمي وتطوير الأنظمة المصرفية والخدمات الإلكترونية
- المختصون في التكنولوجيا المالية (FinTech) والأنظمة المصرفية الرقمية
- مسؤولو استمرارية الأعمال وخطط الطوارئ والتعافي من الكوارث
- فرق الرصد والاستجابة للحوادث السيبرانية والتحقيقات الرقمية
- القيادات التنفيذية المعنية باتخاذ القرارات التقنية والأمنية



الجهات الرقابية والتنظيمية ذات الصلة:

- ممثلو مصرف سورية المركزي والدوائر المختصة بالرقابة والإشراف المصرفي
- الجهات الرسمية المعنية بحماية البيانات ومكافحة الجرائم الإلكترونية
- الجهات التنظيمية المشرفة على قطاع الاتصالات والتكنولوجيا الرقمية
- الجهات المعنية بتطوير السياسات والتشريعات المتعلقة بالأمن السيبراني



التكنولوجيا والأمن السيبراني في العمل المصرفي

المحاضر:



شوقي أحوش

خبير مجاز في مكافحة غسل الأموال، تمويل الإرهاب، الحوكمة، والعقوبات الدولية

خبير في مكافحة غسل الأموال وتمويل الإرهاب والعقوبات

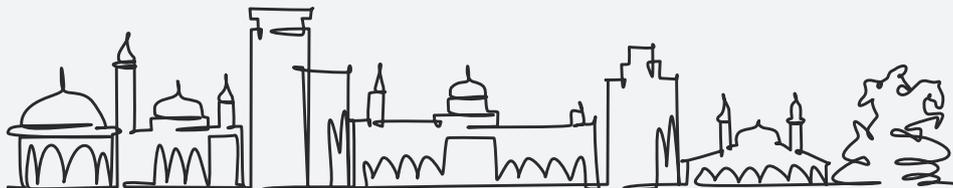
(AML/CFT & SANCTIONS) والجرائم الناشئة عن التكنولوجيا المالية

شوقي أحوش هو مدرّب مستقل ومستشار في مكافحة الجرائم المالية، يتمتع بخبرة مصرفية تتجاوز عشرين عاماً في المدفوعات العابرة للحدود، التحقيقات المالية، تمويل التجارة، انضمام العملاء (Onboarding)، أعراف عميلك (KYC)، المصارف المراسلة، والامتثال. شغل منصب مسؤول الإبلاغ عن غسل الأموال (MLRO) ورئاسة وحدة العقوبات لمدة عشر سنوات، مساهماً في تطوير الحوكمة والامتثال وفق أفضل المعايير الدولية.

قدّم برامج تدريبية لدى مؤسسات إقليمية ودولية بارزة، من بينها: أكاديمية سوق أبوظبي العالمي (ADGMA)، اتحاد المصارف العربية (UAB)، الإيسا (ESA)، ACAMS، المعهد المصرفي الروماني (RBI)، - OECD باريس، - UN Global Compact لبنان، Governance Dynamics، معهد الإمارات للدراسات المالية والمصرفية (EIF)، Pronumeris، والتحالف الإسلامي العسكري لمحاربة الإرهاب (IMCTC)، إضافة إلى جهات أخرى في مجال الجرائم المالية والعقوبات.

يشغل دور مدرّب مشارك مع أكاديمية PWC في الشرق الأوسط، وتعاقد كخبير متخصص (SME) مع شركات ال Big 4 في لندن والسعودية لتقديم استشارات متقدمة في مكافحة الجرائم المالية.

يحمل شهادتي CAMS وCGSS، وهو عضو هيئة تدريب في ACAMS ويقدم البرامج التحضيرية لامتحانات CAMS وCGSS. كما صمّم ودرب برامج في أوروبا وأفريقيا والمنطقة العربية تناولت التكنولوجيا المالية (FinTech)، التكنولوجيا التنظيمية (RegTech)، الجرائم والأمن السيبراني، العقوبات، الاحتيال، AML/CFT، تقييم المخاطر، تمويل الانتشار، غسل الأموال عبر التجارة (TBML)، مكافحة الرشوة والفساد (ABC)، وحوكمة الشركات وإطار GRC.



التكنولوجيا والأمن السيبراني في العمل المصرفي

World Union of Arab Bankers
Tel: +9611364976/8
Email: wuab@wuab.org
webmaster@wuab.org