المحاضرة الثانية

مهارات التعامل مع الهاتف الذكي والموبايل بنك والتحذيرات الأمنية

Smartphone Skills, Mobile Banking and Security Warnings

المرحلة	الثانية – الدراسة الصباحية	**المادة**	الحاسوب
الإعداد	ا.م.د. حيدر حسن محمد - م.م. اثير اسماعيل فاضل	**المدة المقترحة**	ساعتان (نظري + نشاط)

أهداف المحاضرة (Learning Objectives)

بعد انتهاء المحاضرة يكون الطالب قادراً على أن:

1. يدير هاتفه الذكي (Smartphone) بكفاءة وأمان: النظام والتطبيقات والصلاحيات والنسخ الاحتياطي.
2. يعرّف الموبايل بنك (Mobile Banking) ويميّزه عن المحفظة الرقمية (Mobile Wallet).
3. يطبّق خطوات التسجيل والعمليات الأساسية والمتقدمة بأمان.
4. يتعرف على أساليب الاحتيال الشائعة (Phishing, Smishing, SIM Swap…) ويتصدى لها.
5. يتصرف صحيحاً عند فقدان الهاتف أو استلام رسالة مشبوهة.
6. يربط الموضوع بحياته الدراسية والرياضية والمهنية.

خارطة المحاضرة (Lecture Map)

المحور	العنوان	الجانب التطبيقي
1	مهارات الهاتف الذكي الأساسية (Smartphone Essentials)	قائمة ضبط إعدادات
2	الموبايل بنك: المفهوم والأنواع والمكونات	جداول ومخطط
3	مهارات الاستخدام: من التسجيل إلى الإدارة المتقدمة	خطوات عملية
4	التهديدات الأمنية وطرق الحماية (Threats & Defense)	جدول مقارنة
5	إجراءات الطوارئ: فقدان الهاتف والرسائل المشبوهة	بروتوكول خطوات
6	دراسات حالة والأثر الاقتصادي والاجتماعي والمستقبل	تحليل حالات
7	نشاط، مسرد مصطلحات، أسئلة تدريبية	تقويم ذاتي

أولاً: مهارات الهاتف الذكي الأساسية (Smartphone Essentials)

الهاتف الذكي هو اليوم محفظتك وبطاقتك الجامعية وكاميرتك وساعة تدريبك، ومن ثمّ فإن أمانه هو أمان بياناتك المصرفية والشخصية. تتركز المهارات الأساسية في الآتي:

المهارة	ما المطلوب؟	فائدتها
التحديثات (Software Updates)	تحديث نظام Android أو iOS والتطبيقات تلقائياً	سد الثغرات الأمنية (Security Patches)
المتاجر الرسمية (Official App Stores)	التحميل من Google Play أو App Store فقط	تقليل خطر البرمجيات الخبيثة (Malware)

المهارة	ما المطلوب؟	فائدتها
الصلاحيات (App Permissions)	منح كل تطبيق الصلاحيات اللازمة فقط	حماية الخصوصية (الكاميرا، الموقع، جهات الاتصال)
قفل الشاشة والبصمة (Screen Lock & Biometrics)	رمز قوي من 6 أرقام فأكثر أو بصمة/وجه	منع الوصول عند فقدان الهاتف
النسخ الاحتياطي (Backup)	نسخ الصور والمستندات سحابياً أو لجهاز آخر	استرجاع البيانات عند التلف أو السرقة
تحديد الجهاز (Find My Device)	تفعيل Find My أو Find My iPhone	تحديد الموقع والقفل والمسح عن بُعد
إدارة التخزين والبطارية	حذف الملفات المكررة ومراقبة استهلاك التطبيقات	أداء أفضل وعمر أطول للجهاز

نصيحة للرياضي (Athlete Tip)
تطبيقات اللياقة (Fitness Apps) تجمع موقعك ومسارات ركضك ونبضك. راجع إعدادات الخصوصية (Privacy Settings) فيها، وتجنّب نشر مسارات تكشف عنوان سكنك أو مواعيد تدريبك بشكل علني.

ثانياً: الموبايل بنك: المفهوم والأنواع (Mobile Banking: Concept & Types)

الموبايل بنك (Mobile Banking) هو خدمة مصرفية إلكترونية تتيح للعميل إدارة حسابه المصرفي عبر الهاتف: الاستعلام عن الرصيد، والتحويلات، ودفع الفواتير، وإدارة البطاقات، من دون زيارة الفرع.

Definition
Mobile banking is the use of a mobile device to access banking services and perform financial transactions remotely through apps, SMS or USSD.

الفرق بين الموبايل بنك والمحفظة الرقمية (Mobile Banking vs. Mobile Wallet)

وجه المقارنة	الموبايل بنك (Mobile Banking)	المحفظة الرقمية (Mobile Wallet)
الارتباط	حساب مصرفي لدى بنك مرخّص	رصيد داخل تطبيق أو مزوّد خدمة دفع
الاستخدام	كل الخدمات المصرفية: تحويل، فواتير، بطاقات	دفع وتحويل وشحن رصيد بسرعة
أمثلة	تطبيقات المصارف	Apple Pay، FastPay، ZainCash، PayPal

قنوات الخدمة المصرفية عبر الهاتف (Mobile Channels)

القناة	الوصف	ملاحظة أمنية
تطبيق الهاتف (Mobile App)	الأوسع خدمات وسهولة	حمّله من المتجر الرسمي فقط
الرسائل القصيرة (SMS Banking)	استعلام وتنبيهات بالرسائل	يمكن اعتراضها؛ لا تُرسل بيانات حساسة
USSD	رمز يُطلب بالهاتف دون إنترنت	مناسب للهواتف العادية؛ تأكد من الرمز الرسمي
الدفع بالرمز (QR Payment)	مسح رمز لإتمام الدفع	تحقق من اسم المستلم قبل التأكيد
الدفع بالتلامس (NFC / Tap to Pay)	تقريب الهاتف من جهاز الدفع	فعّل قفل الهاتف دائماً

أمثلة محلية: ينتشر في العراق استخدام بطاقات ومحافظ مثل Qi Card/Super Qi وZainCash وFastPay، إضافة إلى تطبيقات المصارف، ويُنصح الطالب بمراجعة الموقع الرسمي لجهته المصرفية والبنك المركزي لمعرفة الخدمات المتاحة وشروطها.

أهمية الموبايل بنك (Importance)

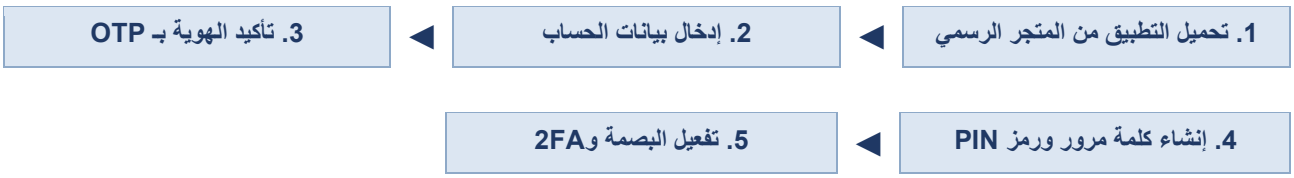
- **السرعة والراحة:** عمليات خلال ثوانٍ على مدار الساعة.
- **الشمول المالي (Financial Inclusion):** وصول من لا يملك فرعاً قريباً إلى الخدمات المالية.
- **تقليل الاعتماد على النقد:** سلامة أكبر وتتبّع أدق للمصروفات.
- **تقليل الكلفة** على المؤسسات والمستخدمين.

المكونات والمتطلبات الأساسية (Components & Requirements)



ثالثاً: مهارات الاستخدام (Usage Skills)

1) التسجيل والإعداد الأولي (Registration & Initial Setup)



OTP (One-Time Password) رمز سري مؤقت يُستخدم مرة واحدة وتنتهي صلاحيته خلال دقائق. **2FA (Two-Factor Authentication)** تحقق من خطوتين: شيء تعرفه (كلمة المرور) وشيء تملكه (الهاتف أو الرمز).

2) العمليات الأساسية (Basic Operations)

العملية	الخطوات العملية	نصيحة أمان
الاستعلام عن الرصيد (Balance Inquiry)	فتح التطبيق ← الحسابات ← عرض الرصيد	لا تفتح التطبيق في مكان مزدحم أمام الآخرين
التحويل (Fund Transfer)	اختيار المستفيد ← إدخال المبلغ ← مراجعة الاسم ← تأكيد بـ OTP/بصمة	تحقق من اسم المستفيد قبل التأكيد؛ فالتحويل الخاطئ يصعب استرجاعه
دفع الفواتير (Bill Payment)	اختيار الخدمة ← رقم الاشتراك ← مراجعة ← دفع	احفظ إشعار العملية
إدارة البطاقات (Card Management)	إيقاف/تفعيل البطاقة، تحديد حد الإنفاق	أوقف البطاقة مؤقتاً عند الشك

مثال عملي (Practical Example)
عند تحويل مبلغ لمدرب خاص مقابل اشتراك شهري: راجع اسم المستفيد المعروض في التطبيق ثم أكّد، واحتفظ بلقطة شاشة الإيصال. وإن كنت ستدفع باستمرار للجهة نفسها فاحفظها في «المستفيدين» بعد التأكد منها.

3) الإدارة المتقدمة (Advanced Account Management)

- **مراقبة الحركة المالية:** مراجعة كشف الحساب (Statement) أسبوعياً لاكتشاف أي عملية لا تعرفها.
- **التنبيهات (Alerts):** تفعيل إشعارات كل عملية بالرسائل أو التطبيق.
- **الحدود اليومية (Daily Limits):** تحديد سقف للتحويل أو الإنفاق وفق المتاح في التطبيق.
- **ميزانية شخصية (Personal Budget):** تقسيم الدخل: ضروريات، ادخار، تدريب وتجهيزات رياضية.

4) حلّ المشكلات التقنية (Troubleshooting)

المشكلة	الإجراء
نسيت كلمة المرور	استخدم خيار «استعادة كلمة المرور» داخل التطبيق الرسمي فقط وليس عبر رابط وصلك برسالة
لم يصل رمز OTP	تحقق من الإشارة والرقم المسجّل، ثم أعد الطلب مرة واحدة؛ فكثرة المحاولات قد تحجب الحساب
العملية فشلت وخُصم المبلغ	احتفظ برقم العملية وتواصل مع خدمة العملاء بالرقم الرسمي المكتوب على البطاقة أو الموقع
التطبيق لا يعمل	حدّثه، أعد تشغيل الهاتف، وإن استمر الخلل فتواصل مع الدعم

مهارة: احفظ في هاتفك رقم دعم مصرفك الرسمي مسبقاً لتستخدمه وقت الطوارئ.

رابعاً: التهديدات الأمنية وطرق الحماية (Security Threats & Defense)

يعتمد معظم المحتالين على خداع الإنسان (Social Engineering) أكثر من اختراق الأجهزة؛ لذلك فإن الوعي هو خط الدفاع الأول.

التهديد	كيف يعمل؟	مثال	الحماية
التصيّد (Phishing)	رسالة بريد أو موقع مزيف يطلب بياناتك	بريد «تحديث بياناتك أو يُغلق حسابك»	لا تضغط الروابط؛ ادخل التطبيق الرسمي مباشرة
التصيّد بالرسائل (Smishing)	الاحتيال برسائل SMS أو واتساب	رسالة «تم إيقاف بطاقتك» مع رابط	احذف الرسالة وتواصل مع البنك رسمياً
التصيّد الصوتي (Vishing)	اتصال هاتفي ينتحل صفة موظف بنك	طلب OTP «لإلغاء عملية مشبوهة»	أنهِ الاتصال؛ البنك لا يطلب رموزك
التصيّد بالرمز (Quishing)	رمز QR مزيف يوجّه لموقع خبيث	ملصق QR فوق رمز الدفع الأصلي	تحقق من الاسم والرابط قبل الدفع
تبديل الشريحة (SIM Swap)	نقل رقمك إلى شريحة بيد المحتال	توقف الشبكة فجأة دون سبب	تواصل فوراً مع شركة الاتصال، وفعّل رمز حماية للشريحة
تطبيقات خبيثة (Malware / Fake Apps)	تطبيق مقلّد أو خارج المتجر الرسمي	تطبيق «بنك» من رابط في رسالة	التحميل من المتجر الرسمي فقط
الشبكة العامة (Public Wi-Fi / MITM)	اعتراض البيانات في شبكة غير آمنة	شبكة مجانية في مقهى أو مطار	استخدم بيانات الهاتف أو VPN موثوق
التلصص (Shoulder Surfing)	مشاهدة كلمة المرور أثناء إدخالها	إدخال الرمز في مكان مزدحم	غطِّ الشاشة وفعّل البصمة

قواعد الحماية الذهبية (Golden Rules of Protection)

1. **كلمة مرور قوية:** عبارة مرور طويلة (Passphrase) من 12 حرفاً فأكثر، ومختلفة لكل حساب، مع مدير كلمات مرور (Password Manager).

2. **تفعيل MFA/2FA** لكل حساب مصرفي وبريد إلكتروني ووسائل تواصل.
3. **لا تشارك OTP أو PIN أو CVV** مع أي شخص مهما كانت صفته.
4. **حدّث الهاتف والتطبيقات** باستمرار.
5. **لا تفتح الروابط** الواردة برسائل لم تطلبها؛ اكتب عنوان الموقع بنفسك أو افتح التطبيق الرسمي.
6. **تجنّب الشبكات العامة** للعمليات المالية.
7. **راقب حسابك** وفعّل التنبيهات الفورية.
8. **اقرأ شروط الخدمة وسياسة الخصوصية** (Terms & Privacy Policy) لتعرف حقوقك.

تحذير (Warning)
لا يطلب البنك الحقيقي كلمة المرور أو رمز OTP أو رقم CVV عبر الهاتف أو الرسائل أو واتساب أبداً. أي طلب كهذا هو احتيال بنسبة شبه مؤكدة، مهما بدت الرسالة رسمية أو عاجلة.

خامساً: إجراءات الطوارئ (Emergency Procedures)

1) عند فقدان الهاتف أو سرقته (Lost or Stolen Phone)

1. الاتصال بالبنك فوراً ◄ **2. تجميد الحساب أو البطاقة** *Freeze* ◄ **3. قفل الهاتف أو مسحه عن بُعد**

4. إيقاف الشريحة من شركة الاتصال ◄ **5. تغيير كلمات المرور** ◄ **6. تقديم بلاغ رسمي**

2) عند استلام رسالة أو اتصال مشبوه (Suspicious Message / Call)

1. **توقف** ولا تتفاعل بسرعة؛ فالاستعجال سلاح المحتال.
2. **لا تضغط** الرابط ولا ترد برمز.
3. **تحقق** من المصدر عبر الموقع أو الرقم الرسمي للبنك.
4. **أبلغ** البنك وامسح الرسالة.
5. **إن كنت قد أدخلت بياناتك**: اتصل بالبنك فوراً وغيّر كلمة المرور.

سادساً: دراسات حالة وأمثلة واقعية (Case Studies)

الحالة 1: M-Pesa في كينيا – الأثر الاجتماعي (Success Story)

أُطلقت الخدمة عام 2007 عبر شركة Safaricom لتحويل الأموال بالهاتف. وأظهرت دراسة منشورة في مجلة Science (Suri & Jack, 2016) أن انتشار هذه الخدمة ارتبط بخروج نحو 2% من الأسر الكينية من الفقر، وكان أثرها أكبر لدى الأسر التي ترأسها نساء [3]. الدرس: الخدمات المالية عبر الهاتف تدعم الشمول المالي وتمكين الفئات المهمشة.

الحالة 2: Paytm والدفع الموحد UPI في الهند

ساهم تطبيق Paytm، مع نظام الدفع اللحظي UPI، في تحول ملايين المستخدمين نحو الدفع بالرمز والهاتف في الأسواق الصغيرة والكبيرة. الدرس: سهولة الاستخدام وانتشار البنية التحتية يرفعان تبنّي الدفع الرقمي.

الحالة 3: اختراق Capital One (2019) – درس في أمان المؤسسات

تعرضت مؤسسة Capital One الأمريكية عام 2019 لاختراق طال بيانات نحو 100 مليون شخص في الولايات المتحدة ونحو 6 ملايين في كندا، بسبب خطأ في إعداد جدار حماية تطبيقات الويب في بيئتها السحابية، لا بسبب خطأ من العملاء. وفرضت

الجهات الرقابية الأمريكية غرامة على المؤسسة. الدرس: حماية المستخدم ضرورية لكنها لا تكفي؛ فعلى المؤسسات اختبار أنظمتها وضبط إعداداتها ومراجعتها باستمرار [5].

الحالة 4: الدفع غير التلامسي أثناء جائحة COVID-19

دفعت الجائحة المستهلكين عالمياً نحو الدفع الإلكتروني وغير التلامسي (Contactless Payment) لتقليل الاحتكاك والزحام في الفروع [4]. الدرس: الأزمات تُسرّع التحول الرقمي وتزيد الحاجة إلى التوعية الأمنية.

الحالة 5 (سيناريو افتراضي): رسالة «منحة رياضية»

السيناريو
تصلك رسالة على واتساب تهنئك بـ«منحة رياضية دولية» وتطلب تحويل رسوم تسجيل صغيرة ثم إرسال صورة بطاقتك الجامعية ورمز تأكيد وصل إلى هاتفك.

التحليل: مغريات (منحة)، رسوم مسبقة، طلب بيانات هوية ورمز OTP، وغياب جهة رسمية مُعلنة. **الإجراء:** التحقق من الجهة عبر موقعها الرسمي، وعدم إرسال أي رمز أو وثيقة، والإبلاغ عن الرقم.

سابعاً: الأثر الاقتصادي والاجتماعي (Economic & Social Impact)

الجانب	الأثر الإيجابي (Positive)	الأثر السلبي / التحدي (Challenge)
الاقتصادي (Economic)	خفض كلف المعاملات وتسريع التجارة ودعم المشاريع الصغيرة	مخاطر الاحتيال والاختراق، وكلف الأمن السيبراني
الاجتماعي (Social)	شمول مالي للنساء والأرياف وذوي الظروف الخاصة	استغلال كبار السن وقليلي الخبرة التقنية
الفردي (Personal)	تنظيم المصروفات والادخار وسهولة الدفع	الإنفاق الاندفاعي وضعف الخصوصية

ثامناً: المستقبل والتوجهات (Future Trends)

- **الذكاء الاصطناعي في كشف الاحتيال** (AI-based Fraud Detection): تحليل سلوك المستخدم لحظياً.
- **المصادقة بدون كلمة مرور** (Passwordless / Passkeys) والمقاييس الحيوية (Biometrics).
- **المصرفية المفتوحة** (Open Banking) والتطبيقات الفائقة (Super Apps).
- **العملات الرقمية للبنوك المركزية** (CBDC) والهوية الرقمية (Digital ID).
- **تحديات الخصوصية:** قوانين مثل GDPR في الاتحاد الأوروبي وCCPA في كاليفورنيا تعكس اتجاهاً عالمياً لحماية البيانات الشخصية [6].

تاسعاً: نشاط صفّي (Class Activity)

المطلوب (مجموعات): اختاروا موقفاً من المواقف الآتية وأعدّوا إجراءً مكتوباً من 5 خطوات، ثم قدّموه للصف: (1) سرقة هاتف لاعب أثناء بطولة خارج المدينة، (2) رسالة تطلب «تحديث بيانات البطاقة»، (3) اتصال من «موظف بنك» يطلب رمز التأكيد، (4) دفع رسوم تسجيل بطولة عبر QR.

البند (Item)	إجابة المجموعة
الموقف (Scenario)	
الخطر المحتمل (Threat)	
الخطوات الخمس (Steps 5)	

البند (Item)	إجابة المجموعة
وقاية مستقبلية (Prevention)	

عاشراً: مسرد المصطلحات (Glossary)

المصطلح (Term)	المعنى
Mobile Banking	الخدمات المصرفية عبر الهاتف
Mobile Wallet	المحفظة الرقمية على الهاتف
OTP	رمز مؤقت لمرة واحدة
MFA/2FA	التحقق الثنائي / متعدد العوامل
PIN	رقم التعريف الشخصي
CVV	الرمز السري في ظهر البطاقة
Phishing	التصيّد الاحتيالي
Smishing	التصيّد عبر الرسائل
Vishing	التصيّد عبر الاتصال الصوتي
SIM Swap	تبديل الشريحة الاحتيالي
Malware	برمجية خبيثة
VPN	شبكة افتراضية خاصة
Social Engineering	الهندسة الاجتماعية: خداع الإنسان
Biometrics	المقاييس الحيوية: بصمة أو وجه
Financial Inclusion	الشمول المالي

حادي عشر: أسئلة تدريبية (Practice Questions)

أولاً: اختيار من متعدد (Multiple Choice)

1) اتصل بك شخص يدّعي أنه موظف البنك ويطلب رمز OTP، فالإجراء الصحيح:

أ) إعطاؤه الرمز لإلغاء العملية
ب) إنهاء الاتصال والاتصال بالبنك عبر الرقم الرسمي
ج) إرسال صورة البطاقة
د) الاستمرار بالحديث للتأكد

2) Smishing يعني الاحتيال عبر:

أ) البريد الورقي
ب) الرسائل النصية وتطبيقات المراسلة
ج) الاتصال الصوتي فقط
د) الشبكات العامة

3) من أفضل ممارسات كلمات المرور:

أ) استخدام الكلمة نفسها لكل الحسابات
ب) عبارة مرور طويلة مع مدير كلمات ومصادقة ثنائية
ج) كتابتها على ظهر الهاتف
د) مشاركتها مع صديق موثوق

4) عند إجراء عملية مصرفية خارج المنزل في مقهى بشبكة Wi-Fi مجانية:

أ) أستخدم الشبكة المجانية دون خوف
ب) أستخدم بيانات الهاتف أو VPN موثوقاً
ج) أفتح الروابط الواردة
د) أشارك الشبكة مع الآخرين

5) أسهمت حالة Capital One 2019 في إبراز أن:

أ) المستخدم هو سبب كل اختراق
ب) إعدادات أمان أنظمة المؤسسة مسؤولية أساسية عليها
ج) الموبايل بنك غير آمن إطلاقاً
د) التحديثات لا فائدة منها

ثانياً: صح أم خطأ (True / False)

1. يُنصح بفتح جميع الروابط الواردة في الرسائل للتحقق من الحساب. ( )
2. التحديثات الأمنية تسدّ ثغرات يستغلها المخترقون. ( )
3. قد يطلب البنك كلمة مرورك عبر رسالة SMS لتحديث الحساب. ( )
4. تفعيل التحقق الثنائي يرفع مستوى أمان الحساب. ( )

ثالثاً: أسئلة قصيرة (Short Answer)

1. اذكر ثلاثة تحذيرات أمنية تتعلق بفقدان الهاتف.
2. اذكر أثراً اقتصادياً واجتماعياً لخدمة M-Pesa في كينيا.
3. اقترح نشاطاً عملياً للتدرب على الموبايل بنك بأمان.

رابعاً: أسئلة تحليلية وتطبيقية (Analytical & Applied)

1. كيف يسهم الموبايل بنك في الاقتصاد الرقمي خلال الأزمات مثل جائحة كوفيد-19؟ استند إلى أمثلة من المحاضرة.
2. قارن بين حالة نجاح (M-Pesa أو Paytm) وحالة اختراق (Capital One) وما الدرس من كل منهما؟
3. صِف خطوة بخطوة كيف تتصرف عند سرقة هاتفك، وإذا وصلتك رسالة مشبوهة تطلب بيانات مصرفية.
4. ما رأيك في دمج الموبايل بنك مع المدن الذكية (Smart Cities) استناداً إلى التوجهات المستقبلية؟

الإجابات النموذجية (Answer Key)

القسم	الإجابة
اختيار من متعدد	1-ب ، 2-ب ، 3-ب ، 4-ب ، 5-ب
صح / خطأ	1-خطأ ، 2-صح ، 3-خطأ ، 4-صح

ملخص المحاضرة (Summary)

- الهاتف الذكي هو بوابة الخدمات المصرفية؛ تأمينه يبدأ بالتحديث وقفل الشاشة والتحميل من المتاجر الرسمية.
- الموبايل بنك يوفر السرعة والشمول المالي، لكنه يتطلب وعياً بأساليب الاحتيال وخاصة الهندسة الاجتماعية.
- القاعدة الذهبية: لا تشارك رموزك، ولا تضغط الروابط، وتحقق دائماً عبر القناة الرسمية.

المصادر والمراجع (References)

1. Verizon. Data Breach Investigations Report (DBIR). Annual report.
2. NIST. Special Publication 800-63B: Digital Identity Guidelines – Authentication and Lifecycle Management.
3. Suri T, Jack W. The long-run poverty and gender impacts of mobile money. Science. 2016;354(6317):1288–1292.
4. World Bank. The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19. Washington, DC; 2022.
5. U.S. Department of Justice and Office of the Comptroller of the Currency. Public statements on the 2019 Capital One data breach (2019–2020).
6. Regulation (EU) 2016/679 (GDPR); California Consumer Privacy Act (CCPA), 2018.
7. OWASP Foundation. OWASP Mobile Top 10 – Mobile application security risks.
8. CISA (U.S. Cybersecurity and Infrastructure Security Agency). Avoiding Social Engineering and Phishing Attacks.
9. GSMA. State of the Industry Report on Mobile Money. Annual report.

إعداد: أم.د. حيدر حسن محمد
م.م. اثير اسماعيل فاضل
مدرسي المادة