الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

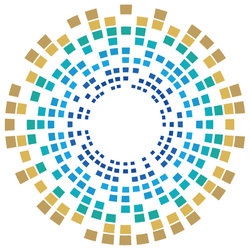
مبادئ عامة في السلامة الرقمية

الشريحة المستهدفة
طلبــة الجامعـات

كُتَـيّب المُـدَرّب

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبادئ عامة في السلامة الرقمية

الشريحة المستهدفة

طلبة الجامعات

كُتَيّب المُدَرّب

الفهرس	رقم الصفحة

الفهرس	رقم الصفحة

تمهيد

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

تم تصميم هذا الكُتَيِّب بهدف توعية كبار القَدْر بمبادئ السلامة الرقمية، وأفضل الممارسات التي تساعدهم على تفادي المخاطر السيبرانية؛ حيث يهدف هذا الكُتَيِّب إلى تعزيز وعيهم حول تهديدات سيبرانية، مثل التصيد الاحتيالي، والبرمجيَّات الضَّارَّة، وتمكينهم من حماية بياناتهم وأجهزتهم بشكلٍ فعّالٍ.

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

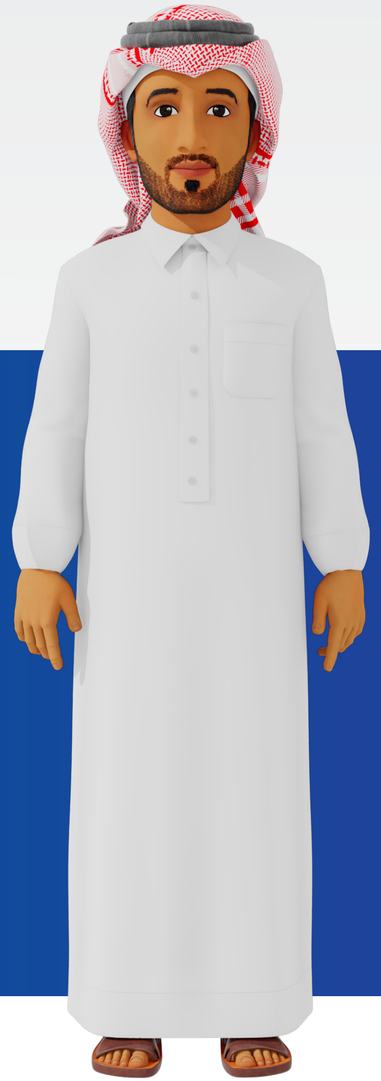
تعريف المبادرة

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

وتعمل 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 الشائعة

لماذا طلبة الجامعات؟

طلبـــة الجامعات من أكـــثر الفـئات عُرْضَـــةً للهجمات الســـيبرانيـة لعدة أســـباب، منـــها:

نقص الوعي

يعاني غالبية الطلبة من نقص الوعي السيبراني، مما يجعلهم هدفًا سهلًا للتهديدات الشائعة.

الاستخدام المكثّف للتكنولوجيا

يعتمد الطلبة بشكلٍ كبير على الأجهزة التكنولوجية والشبكات العامة (مثل شبكات المقاهي والمكتبات) للدراسة والتواصل.

البيانات القيمة

يمتلك الطلبة بيانات أكاديمية ومالية وشخصية قيّمة.

البيانات الشخصية

البيـــانات

تُشير إلى أي معلومات أو حقائق يمكن جَمْعها وتَحْليلها، وتشمل: الأرقام، النصوص، الصور، وغيرها. وتلعب البيانات دوراً مهماً في اتخاذ القرارات وتطوير التقنيات.

البيانات الشخصية

هي أي معلومات تتعلَّق بفرد معيَّن يمكن تحديد هُويَّته من خلالها. وتشمل هذه المعلومات: الاسم، العنوان، رقم الهاتف، البريد الإلكتروني، المعلومات المالية، أو حتى العناوين الإلكترونية.

من أمثلة البيانات الشخصية

01
رقم الهُويّة الوطنية

02
المعلومات الطبيّة والصحيّة

03
بيانات الحسابات المصرفية

04
الأنشطة عبر الإنترنت

05
البيانات البيومترية (مثل بصمة الإصبع والوجه)

06
سجلات الموقع الجغرافي (GPS)

06
بيانات التفاعل مع تطبيقات الذكاء الاصطناعي (AI)

سرقة الهُويَّة الرقمية

وصول شخص غير مصرَّح له إلى معلومات هُويَّة شخصٍ آخر على الإنترنت، واستخدامها بشكلٍ غير قانوني لتحقيق مكاسب شخصية أو مالية.

تشمل هذه المعلومات: بيانات الحسابات الشخصية، كلمات المرور، أو المعلومات المالية.

أمثلة على البيانات المسروقة

- أرقام بطاقات الائتمان.
- كلمات المرور.
- الأرقام القومية أو الاجتماعية.
- المعلومات البنكية.

احذر!

تجنَّب استخدام الشبكات العامة غير الآمِنة عند الوصول إلى البيانات الحساسة؛ لأنها قد تكون عُرضةً للهجمات التي تسمح للمهاجمين بالتنصت على الاتصال.

كيف تحدث سرقة الهُويَّة الرقمية؟

1

الهندسة الاجتماعية المتقدمة (Advanced Social Engineering)

استخدام تقنيات الذكاء الاصطناعي (AI) لإنشاء حسابات وهمية أو محتوى مُقنع للغاية (Deep fakes) لانتحال صفة شخصيات عامة أو موثوقة؛ بهدف الاحتيال وسرقة البيانات.

2

التصيد الاحتيالي (Phishing)

يتم خداع الضحية للكشف عن معلومات حساسة عبر رسائل أو مواقع وهميَّة تبدو شرعية

3

البرمجيات الخبيثة (Malware)

تثبيت برمجيات ضارَّة على أجهزة المستخدمين لجَمْع البيانات الشخصية دون عِلمهم

4

اختراق قواعد البيانات (Data Breaches)

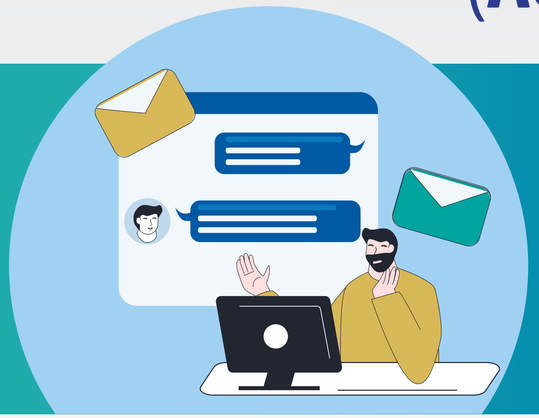
يستهدف المهاجمون الشركات أو المؤسسات لسرقة كميات كبيرة من بيانات المستخدمين المُخزَّنة على خوادمها

5

هجمات القوة الغاشمة (Brute Force Attacks)

محاولة اختراق الحسابات من خلال تجربة ملايين التركيبات من كلمات المرور المحتَمَلة

الهندسة الاجتماعية المتقدمة (Advanced Social Engineering)

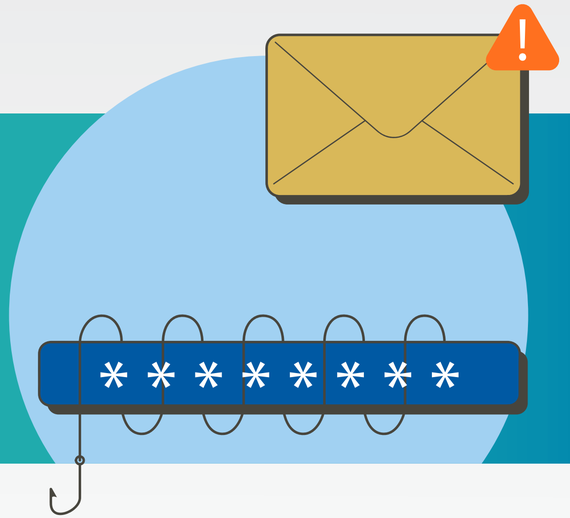


الهندسة الاجتماعية المتقدمة هي فن التلاعب بالأفراد للحصول على معلومات سرية، أو دفعهم للقيام بأفعال مُعيَّنة؛ من خلال استخدام تقنيات مُتطوّرة شديدة التعقيد.

أبرز الأساليب المُستخدَمة

1. استخدام الذكاء الاصطناعي لإنشاء رسائل أو محادثات شديدة الإقناع
2. إنشاء مقاطع Deep fake لانتحال شخصية أساتذة أو موظفين جامعيين
3. إرسال طلبات وهمية للمِنَح أو الوظائف لاستدراج الطالب وتحصيل بياناته
4. تزييف حسابات شخصية لزملاء أو حسابات رسمية تبدو وكأنها تابعة للجامعة

تهديدات البريد الإلكتروني



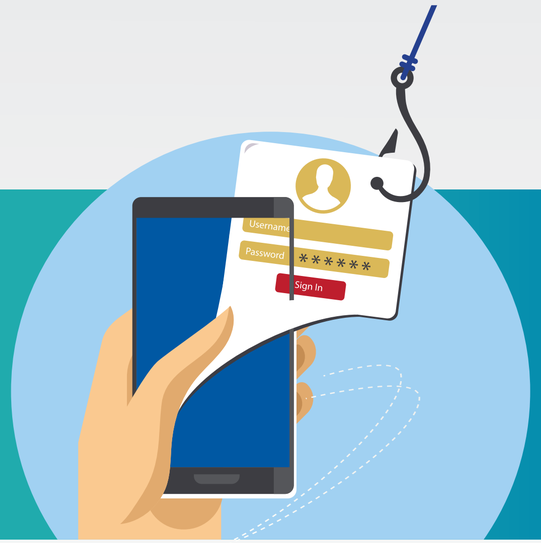
البـــريـد الإلكـترونـــي

وسيلة اتصال مهمَّة على مستوى الأفراد والشركات؛ يحتوي على معلومات وبيانات حساسة

التهـديدات الشـائعـة

1. البريد المزعج Spam
2. التصيد الاحتيالي
3. البرمجيات الخبيثة
4. الروابط الضّارّة

التصيد الاحتيالي (Phishing)



نوع من الهجمات الإلكترونية يستخدم المهاجمون فيها رسائل بريد إلكتروني أو مواقع ويب مُزيَّفة لخداع الأشخاص؛ للكشف عن معلومات حساسة، مثل كلمات المرور، أو بيانات الحسابات المصرفية.

وتتَّخـذ هـذه الهجـمات عـدة أشـكال، من أبـرزها ما يلـي

- رسائل تبدو من البريد الجامعي تطلب "تحديث كلمة المرور فورًا"
- روابط مُزيَّفة لنتائج الامتحانات أو تسجيل المواد
- إشعارات دَفْع رسوم جامعية وهمية
- صفحـات تسجـيل دخـول تشـبه Blackboard أو SIS (Student Information System) لكنها مُزيَّفة بالكامل

البرمجيات الخبيثة (Malware)

برمجيات ضارة تُزْرَع في جهاز المستخدِم بهدف سرقة البيانات أو التحكُّم بالنظام.

مـن أكـــثر الطـرق التـي تتتـشـر بـها

1. ملفات يتم تنزيلها عبر روابط مجهولة
2. برامج مقرصنة يستخدمها الطلبة مثل: أدوات التحرير أو الألعاب
3. ملحقات (Extensions) للمتصفحات تقوم بجمع بيانات الاستخدام
4. برمجيات تسجيل الضغطات Key loggers لسرقة كلمات المرور

اختراق قواعد البيانات (Data Breaches)

وصول غير مُصرَّح به إلى قواعد بيانات تحتوي على معلومات حساسة وبكميات كبيرة.

غالـبًا مـا يـؤدي هـذا النـوع مـن الهجـمات إلـى مخـاطـر مثـل:

تسريب بيانات الطلبة عند اختراق منصات جامعية.

سرقة أسماء، عناوين بريدية، سجلات أكاديمية، أو أرقام مالية.

استخدام البيانات المسروقة في حملات تصيّد تستهدف الطلبة لاحقًا.

هجمات القوة الغاشمة (Brute Force Attacks)

محاولة لاختراق الحساب عبر تجربة عدد هائل من كلمات المرور المحتمَلة.

تحدث هذه الهجمات عادةً في الحالات التالية

- يستهدف المهاجم حسابات الطلبة ذات كلمات المرور الضعيفة
- استخدام أدوات آلية لتجربة ملايين التركيبات في دقائق
- تزداد خطورة الهجوم إذا استخدم الطالب كلمة المرور نفسها في عدة منصات

الشبكات اللاسلكية (Wireless Networks)

الشَّبكات اللاسلكية هي نوع من الشبكات التي تستخدم إشارات الراديو أو الموجات الضوئية لتبادل المعلومات بين الأجهزة دون الحاجة إلى استخدام كابلات؛ تُوفِّر هذه الشبكات اتصالًا مرنًا وسريعًا.

أنــواع الشبــكات اللاســلكــية

Wi-Fi

تُستخدَم في المنازل والمكاتب لتوفير الاتصال بالإنترنت للأجهزة المختلفة.

Bluetooth

تُستخدَم لتوصيل الأجهزة القريبة، مثل الهواتف والسماعات.

الشبكات الخلوية

مثل 4G & 5G، تُستخدَم لتوفير خدمات الهاتف المحمول والبيانات.

السؤال التفاعلي الأول

أيّ ممَّا يلي يُعدّ أحد المخاطر الأساسية لاستخدام تقنيات التزييف العميق؟

أ. تقليل جودة الفيديوهات التعليمية

ب. إنشاء محتوى مزيف

ج. فقدان كلمات المرور الشخصية

د. تعطّل التطبيقات الجامعية

السؤال التفاعلي الثاني

ما الاستخدام الأكثر أمانًا لتطبيقات الذكاء الاصطناعي في إدارة البيانات؟

أ. مشاركة بيانات الطالب مع أيّ نظام دون تدقيق

ب. تحليل السلوك المشبوه لاكتشاف محاولات الاختراق

ج. رَفْع ملفات حساسة إلى أيّ منصة دون تشفير

د. تعطيل أدوات الحماية التقليدية

المحور الثاني

آليات الوقاية والسلامة الرقمية

الوقاية من خطر اختراق البيانات

الوقاية من الاختراقات تتطلب اتّباع إستراتيجيات متقدمة تضمن حماية البيانات الشخصية والأكاديمية.

01

استخدام كلمات مرور قوية وفريدة لكل حساب، وربطها بمدير كلمات مرور موثوق

02

تفعيل المصادقة الثنائية لجميع الحسابات المهمة لتعزيز طبقات الحماية

03

تحديث الأنظمة والتطبيقات بانتظام لسدّ الثغرات المكتَشفة حديثًا

04

مراقبة الحسابات والأنشطة الرقمية لاكتشاف أيّ محاولات اختراق مبكرًا

إدارة البيانات الأكاديمية

القدرة على إدارة البيانات الأكاديمية بشكلٍ منهجي وحمايتها من الضياع أو التسرب الرقمي مهارة أساسية للطالب الجامعي.

الاحتفاظ بنُسَخ احتياطية من المشاريع والملفَّات الأكاديمية على خدمات التخزين السحابي الموثوقة مثل Google Drive أو OneDrive

تطبيق قاعدة 3-2-1 للنسخ الاحتياطي: الاحتفاظ بثلاث نُسَخ من البيانات، على وسيطين مختلفين، ونسخة واحدة خارج الموقع (سحابيًّا)

حماية الملفَّات الحسَّاسة باستخدام التشفير؛ لضمان عدم وصول غير المُصرَّح لهم إليها

حَذْف الملفَّات الأكاديميَّة من الأجهزة العامَّة أو المشتركة فَوْر الانتهاء مِن استخدامها

أمان البريد الإلكتروني

اتباع إستراتيجيات متقدمة لإدارة البريد الإلكتروني يضمن حماية المعلومات من الاختراق.

1. استخدام كلمات مرور قوية ومعقّدة، تشمل حروفًا كبيرة وصغيرة وأرقامًا ورموزًا
2. تفعيل المصادقة الثنائية لتوفير طبقة أمان إضافية عند تسجيل الدخول
3. التحقُّق من مصداقية جميع الروابط قبل النقر عليها، حتى لو ظهرت ضمن رسائل من مرسلين معروفين
4. عدم مشاركة بيانات الحساب مع أيّ شخص، بما في ذلك زملاء الدراسة؛ لضمان سلامة المعلومات

أمان البريد الإلكتروني

5 مراقبة النشاطات غير المعتادة يمكن أن تساعد في اكتشاف الهجمات في مراحلها المبكّرة

6 النسخ الاحتياطي المنتظم لرسائل البريد الإلكتروني يضمن عدم فقدان البيانات المهمة في حال حدوث هجوم أو خلل في النظام

7 تحديث برامج البريد الإلكتروني وأنظمة التشغيل بانتظام لتقليل خطر استغلال الثغرات الأمنية

8 تفعيل تقنيات التشفير (End-to-End Encryption): استخدام خدمات بريد إلكتروني تدعم التشفير التام بين الطرفين

الوقاية من البريد المزعج (Spam)

البريد المزعج قد يبدو غير ضارّ لكنّه غالبًا وسيلة لنشر البرمجيات الخبيثة أو جَمْع البيانات الشخصية.

للوقاية من البريد المزعج (Spam) نُوصِي بـ:

عدم فتح الرسائل أو المرفقات من مرسلين مجهولين

تفعيل مرشّحات البريد المزعج المدمجة في خدمات البريد الجامعي؛ لتقليل تعرض الطلبة للتهديدات

الحذر من الرسائل التي تحتوي عروضًا مالية أو نتائج امتحانات مُغْرية، فقد تكون احتيالية

الإبلاغ عن الرسائل المشبوهة للإدارة التقنية بالجامعة

الوقاية من التزييف العميق (Deep fakes)

التزييف العميق أداة متطورة تستهدف الهوية الرقمية، وتستدعي وعيًا تقنيًّا وأكاديميًّا لحماية المعلومات الشخصية.

للوقـــايـــة مـــن التـــزييف العمـــيق نُـــوصِـــي بـــ:

1. التحقُّق بدقة من مصدر الصور والفيديوهات قبل الاعتماد عليها أو مشاركتها
2. استخدام أدوات متقدّمة للكشف عن التزييف العميق، والتحقُّق من أصالة المحتوى الرقمي
3. عدم مشاركة أيّ موادّ شخصية يمكن استغلالها لاحقًا في انتحال الهوية أو الهجمات الرقمية
4. نَشْر الوعي بين الزملاء حول مخاطر التزييف العميق لتعزيز بيئة أكاديمية آمِنَة

صلاحيات الوصول (Permissions)

إعدادات تُحدِّد ما الذي يمكن للتطبيقات الوصول إليه داخل جهازك أو حساباتك.

1. السماح للتطبيق بالوصول للكاميرا أو الميكروفون دون حاجة فِعْلية يُشكِّل خطرًا
2. بعض التطبيقات تطلب الوصول للصور والملفات، ثم تجمع البيانات دون عِلْمك
3. مَنْح الصلاحيات الدائمة (Always Allow) قد يؤدي إلى تتبُّع الموقع والحركة
4. مراجعة الصلاحيات في الهاتف والحاسوب بشكلٍ دوري يُقلِّل من احتمالات الاختراق

تأمين الشَّبكات اللاسلكية

- **استخدام تشفير قويّ:** معيار التشفير WPA3 أحدَث وأكثر معايير التشفير أمانًا لشبكات Wi-Fi، ويُوفّر حماية أقوى ضد هجمات القوة الغاشمة (Brute-Force Attacks) مقارنةً بـ WPA2
- **تحديث البرامج والبرامج الثابتة:** التأكُّد من تحديث أجهزة الشبكة والبرامج.
- **تعزيز إعدادات الأمان:** تعطيل بثّ اسم الشبكة SSID لجعْلها غير مرئية.
- **استخدام مصادقة قوية:** تفعيل المصادقة الثنائية عندما تكون مُتاحة.
- **تفعيل اكتشاف التهديدات والاختراقات:** استخدام أنظمة اكتشاف الاختراقات IDS أو منع الاختراق IPS للشبكات اللاسلكية.

أمن المواقع الإلكترونـــية

حـــماية المـــواقع الإلكتـــرونية تُمـــثِّل أســـاسًا للأمـــان الرقـــمي؛ إذ إن أيّ ضَعْـــف فيـــها قد يُســـتغَل للوصـــول إلـــى بيـــانات حســـاســـة.

1. التحـــقُّق مـــن شهـــادات الأمـــان الرقمـــية للمواقـــع لتعـــزيز الثـــقة فـــي مصداقـــية المصـــادر
2. تحـــديـــث المتصـــفح بانتـــظـــام لضـــمان ســـدّ الثـــغـــرات الأمـــنيـــة المكتـــشـــفة حـــديـــثًا
3. تجـــنُّب الروابـــط والمواقـــع غير الموثـــوقة التي قد تحتوي على برمجـــيات ضارَّة أو تهدف إلى الاحتيال
4. استخـــدام إضـــافات المتصفّح المُتخصّصة في كشف المواقع الخطرة والتنبـيه من المخـــاطر المحتمـــلة
5. التأكُّد من استخدام بروتوكول HTTPS المشفّر قبل إدخال أيّ بيانات حساسة؛ لضمان تشفير الاتصال بين المستخدِم والموقع

أمــن التطبيــقات

التطبيــقات الرقمــية جــزء أســاســي مــن الحــياة الأكــاديــمــية واليــومــية، ولكنّــها قــد تتحــوَّل إلــى بوابــة لاختــراق البــيانــات إذا لــم تتــمّ إدارتــها بشــكلٍ صحــيح.

1. تحميل التطبيقات فقط من المتاجر الرسمية والمعتمدة؛ لتقليل خطر البرمجيات الضارَّة
2. مراجعة الصلاحيات المطلوبة للتطبيقات، والتأكد من توافقها مع وظائف التطبيق الفعلية
3. تحديــث التطبيقــات بشــكلٍ دوري لســدّ الثــغرات الأمنيــة المكتشــفة حديثًــا
4. اســتخدام برامــج مكافحــة الفيروســات والمُراقَبــة الأمنيــة علــى الأجهــزة الشــخصية
5. حَــذْف التطبيقــات غيــر المســتخدَمة لتقليــل فُــرَص اســتغلالها مِــن قِبَــل المهاجميــن

أمـن المنصـات التعليمـية (LMS / SIS)

أنظـمة الجامـعة مثـل Blackboard، Moodle، أو نظـام المعلـومات الأكاديمـية، تحـتاج إلى استـخدام آمِن؛ لأنهـا تحتـوي على بـيانات حسـاسة.

- استخدام دخول آمِن وكلمة مرور مختلفة عن الحسابات الشخصية
- التأكُّد من تسجيل الخروج عند استخدام أجهزة الجامعة أو الأجهزة المشتركة
- تجنُّب فتح ملفات مجهولة داخل المنصة، خصوصًا المرفقات المشتركة بين الطلبة
- تحديث البيانات الأكاديمية فقط عبر الروابط الرسمية للجامعة
- تفعيل التحقُّق بخطوتين إذا وفَّرته الجامعة

أمـن السحابة (Cloud Security)

تخـــزين البـــيانات على السحـــابة يُوفّـــر مـــرونة كبيـــرة، لكـــنّه يتطلّـــب تطبـــيق إجـــراءات أمنـــية دقيـــقة؛ لضـــمان حمـــاية المعلـــومات الأكاديمـــية والشخصـــية.

01 اختيـار مُزوّد خدمـة سـحابية موثـوق وذي سـمعة جيـدة لتقليـل المخاطـر

02 تفعيل المصادقة الثنائية للوصول إلى الحسابات السحابية؛ لضمان حماية إضافية

03 تشـفير الملفـات قبـل رَفْعهـا علـى السـحابة؛ لتعزيـز مسـتوى الأمـان

04 مراقبة سجلات الدخول للحسابات السحابية؛ للكشف المبكر عن أيّ نشاط غير معتاد

05 إدارة الصلاحيات بدقة لمن يُمكنه الوصول إلى الملفات والمجلدات المشتركة

التشفير (Encryption)

أداة مُهمة لحماية البيانات؛ إذ تضمن سرية المعلومات في أثناء التخزين أو النقل، وتمنع أيّ وصول غير مُصرَّح به.

01 استخدام التشفير عند إرسال رسائل البريد الإلكتروني الحسَّاسة؛ لضمان حماية المحتوى من التنصت

02 تشفير المستندات الأكاديمية قبل مشاركتها على الإنترنت أو عبر السحابة؛ لتجنُّب تسرُّب المعلومات

03 الاعتماد على بروتوكولات تشفير قوية مثل AES-256 في الأجهزة والتطبيقات

04 استخدام الشبكات الافتراضية الخاصة (VPN) لتشفير الاتصال عند التعامل مع الشبكات العامة

05 التأكُّد من أنّ منصات التخزين السحابي تدعم التشفير الكامل للبيانات المخزنة

السؤال التفاعلي الثالث

ما المؤشر الأكثر دلالة على أن الموقع آمِن في أثناء إدخال بيانات حساسة؟

أ. وجود صور عالية الجودة في الصفحة

ب. وجود شريط بحث في أعلى الموقع

ج. وجود HTTPS وقفل في شريط العنوان

د. تحميل الصفحة بسرعة

السؤال التفاعلي الرابع

عند الاتصال بشبكة Wi-Fi عامة في الجامعة، ما أفضل إجراء لحماية البيانات؟

أ. استخدام VPN قبل تسجيل الدخول

ب. إدخال كلمات مرورك دون قلق

ج. إيقاف جدار الحماية

د. مشاركة الاتصال مع الآخرين

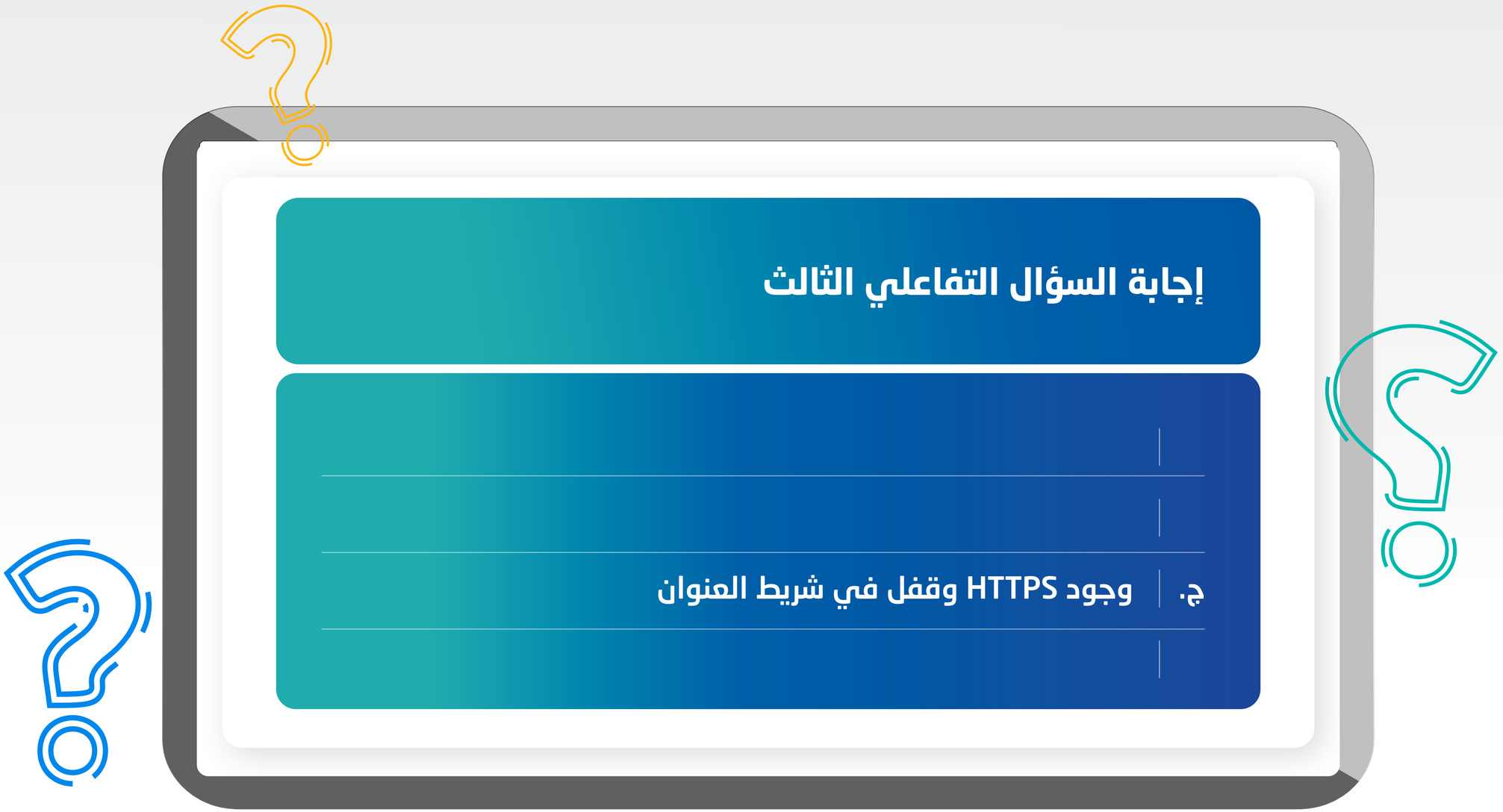
إجابات الأسئلة التفاعلية

إجابة السؤال التفاعلي الأول

ب. إنشاء محتوى مُزيَّف

إجابة السؤال التفاعلي الثاني

ب. تحليل السلوك المشبوه لاكتشاف محاولات الاختراق



إجابة السؤال التفاعلي الثالث

ج. وجود HTTPS وقفل في شريط العنوان


إجابة السؤال التفاعلي الرابع
أ. استخدام VPN قبل تسجيل الدخول

المراجع

1. Chandarman, R., & van Niekerk, B. (2017). Students› cybersecurity awareness at a private tertiary educational institution. The African Journal of Information and Communication, 20 (1), 1-15. [Online] Available at: https://www.scielo.org.za/scielo.php?pid=S2077-72132017000100007&script=sci_arttext

2. 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

3. Check Point Research. (2024). Global Cyber Attack Trends: Q2 2024. [Online] Available at: https://www.checkpoint.com/press/2024/check-point-research-q2-2024-report-reveals-30-increase-in-global-cyber-attacks/

4. 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

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

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

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

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

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

المراجع

10. Kaspersky. What is a VPN? How it works, types, and benefits of VPNs., on site:
https://www.kaspersky.com/resource-center/definitions/what-is-a-vpn
11. Microsoft Security. (2023). Credential Stuffing Attacks: What They Are and How to Prevent Them. [Online] Available at:
https://www.microsoft.com/security/blog/2023/05/10/credential-stuffing-attacks-what-they-are-and-how-to-prevent-them/
12. NIST. (2017). NIST Special Publication 800-63B: Digital Identity Guidelines. [Online] Available at:
https://pages.nist.gov/800-63-3/sp800-63b.html
13. Susnjara, Stephanie. IBM. What is cloud computing?, on site: https://www.ibm.com/think/topics/cloud-computing

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