الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبادئ عامة في السلامة الرقمية

الفئة المستهدفة
الرياضيون

كُتَيّب 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

الفئة المستهدفة

الرياضيون

كُتَيّب المُدَرّب

تمهيد

أصبح العالم الرقمي جزءًا أساسيًّا لا يتجزَّأ من الحياة المهنية للرياضيين في العصر الحديث، ولم يَعُد مقتصرًا على التواصل الاجتماعي أو الترفيه فقط، بل امتدَّ ليشمل بناء السُّمعة العامة، وإدارة العلاقات المهنية، والتفاوض على العقود، والتعاون مع الرعاة. فالمنصات الرقمية أصبحت واجهة اللاعب أمام الجماهير ووسائل الإعلام والشركات، وأي خطأ أو اختراق قد يُؤثِّر سلبًا على مسيرته الرياضية ومكانته الجماهيرية.

وقد تم تصميم هذا الكُتَيّب بهدف توعية الرياضيين بمبادئ السلامة الرقمية، وأفضل الممارسات التي تساعدهم على تفادي هذه المخاطر؛ حيث يهدف إلى تعزيز وعيهم بأبرز التهديدات السيبرانية التي قد يتعرَّضون لها على المستويَيْن الشخصي والمهني.

كما يُقدِّم الكُتَيّب أفضل الممارسات والإجراءات الوقائية للحماية من الهجمات السيبرانية، وتأمين البيانات الشخصية والأجهزة الإلكترونية، وأُسُس التعامل السريع والآمِن مع حوادث الاختراق.

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 نَشْر الوعي بالسلامة الرقمية والاستخدام الآمِن لشبكة الإنترنت والتطبيقات التكنولوجية المختلفة، وتوضيح المخاطر المحتمَلة؛ وذلك بهدف بناء مجتمع آمِن سيبرانيًّا ومُتمكِّن تكنولوجيًّا.

الشرائح المستهدَفة

تستهدف المبادرة مختلف شرائح المجتمع، مع تركيزها على الفئات التالية:

01 السنة الأولى

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

02 السنة الثانية

الدبلوماسيون

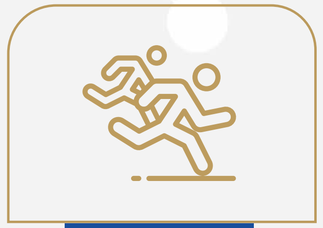
الإعلاميون

الجمهور العام

المرأة (العنف الرقمي ضد المرأة)

العاملون في المجال الصحي

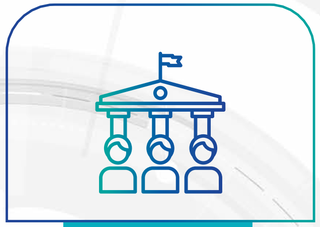
المؤسسات العقابية والنيابة والمؤسسات الإصلاحية



الرياضيون

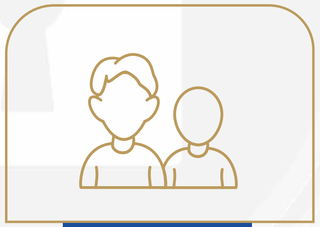
03 السنة الثالثة

العاملون في قطاع الطاقة



العاملون في وزارتي الدفاع والداخلية

الجمهور العام



اليافعون والشباب

ذوو الاحتياجات الخاصة

العاملون في قطاع التعليم

أدوات التوعية

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

دليل السلامة الرقمية

كُتَيّبات توعية مطبوعة

شرائح العرض (للمُدرّبين)

فيديوهات التوعية (أنيميشن)

فيديوهات التوعية (تمثيلية)

الألعاب السيبرانية

بوابة التوعية السيبرانية

الروبوت التفاعلي

وِرَش التوعية

01 المحور الأول

الوكالة الوطنية للأمن السيبراني وحماية المجتمع الرقمي

التأسيس والأهداف

التأسيـــس

تأسَّسـت الوكالـة الوطنيـة للأمـن السيبرانـي بمُوجـب المرسـوم الأميـري رقـم (1) لعـام 2021م، كمرجعيَّـة وطنيـة لحمايـة الفضـاء السيبرانـي؛ بهـدف تعزيـز الأمـن السيبرانـي للدولـة، وضمـان حمايـة الأصـول الرقميـة والبِنْيـة التحتيـة الحيويـة مـن التهديـدات السيبرانيـة المتزايـدة.

الأهـــداف

تعزيز الأمن السيبراني

تطويـر سياسـات مُتقدّمـة لضمـان حمايـة الأنظمـة الرقميـة، وتطبيـق إجراءات وقائيـة شـاملة للكشـف عـن التهديـدات السيبرانيـة، ومعالجتهـا

رَفْع مستوى الوعي

تنظيـم برامـج تدريبيـة وحـملات توعيـة تهـدف إلـى تثقيـف الأفراد والمؤسسـات حـول أهميـة الأمـن السيبرانـي، وكيفيـة التصـدّي للهجمـات السيبرانيـة

بناء القدرات الوطنية

تدريـب الكـوادر الوطنيـة علـى أحـدث تقنيـات الأمـن السيبرانـي، ودعـم الأبحـاث والدراسـات التـي تُـعزِّز مـن قـدرة الدولـة علـى التصـدّي للتحديـات السيبرانية

التعاون الدولي

إقامـة شراكات مـع المنظمـات الدوليـة، وتبـادل الخـبرات مـع الـدُّوَل الرائـدة فـي مجـال الأمـن السيبرانـي؛ لمكافحـة الجرائـم السيبرانيـة، وتعزيـز الحمايـة السيبرانيـة

الرؤية والاختصاصات

الرؤية الإستراتيجية

01

بلـوغ فضـاء سيبرانـي آمِـن يدعـم التنميـة الاجتمـــاعية والاقتصاديـة

02

تمكيـن اقتصـاد المعرفـة عَبْـر تعزيـز الثقـة فـي الخدمـــات الرقميـة

الاختصـــاصات

- إعـــداد وتنفيـــذ الإستراتيجية الوطنية للأمـن السيبرانـي
- رَصْـــد التهديـــدات السيبرانية والاستجابة للحـــوادث عبر فِـرَق متخصصـة
- وضـع السياســـات والمعـــايير الفنيـة والتنظيمية لحمـــاية البنيـة التحتيـة الرقمية
- تنسـيق الجهـــود الوطنيـة بيـن الجهـات الحكوميـة والخـاصة فـي مجـــال الأمـن السيبـرانـي

رَفْع الوعي المجتمعي حول الأمن السيبراني من خلال حملات وبرامج تدريبية

تمثيل الدولة دوليًّا في المحافل والاتفاقيات المتعلّقة بالأمن السيبراني

تطوير خبرات الكوادر الوطنية عبر التدريب والشهادات المهنية في المجال

التكامل في التعامل مع الجرائم الإلكترونية

تتكامل الأدوار بين الوكالة الوطنية للأمن السيبراني ووزارة الداخلية في حماية الفضاء الرقمي.

دور

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

- إطلاق المبادرات الوطنية للسلامة الرقمية
- إعداد السياسات والمعايير والإجراءات الوقائية
- تنفيذ برامج التوعية والتثقيف المجتمعي
- تقديم الدعم الفني والتقني للقطاعات المختلفة
- رَصد ومتابعة التهديدات الرقمية على المستوى الوطني

دور

وزارة الداخليـــــــة
Ministry of Interior
State of Qatar • دولـــة قطـــر

التحقيق في الجرائم الإلكترونية وضبط مرتكبيها

جَمْع الأدلة الرقمية وفق الأُطُر القانونية

حماية المجتمع من الأنشطة الإجرامية عبر الإنترنت

التنسيق مع الإنتربول والجهات الأمنية الدولية عند الحاجة

تطبيق العقوبات وفق القوانين ذات الصلة بالجرائم الإلكترونية

02 المحور الثاني

التهديدات السيبرانية الشائعة للرياضيين

المخاطر السيبرانية

جميع التهديدات التي تنشأ نتيجة استخدام الإنترنت والأجهزة الرقمية، والتي قد تؤدي إلى اختراق الحسابات، أو سرقة البيانات، أو تسريب المحتوى الخاص، أو استغلال الهوية الرقمية للرياضي دون عِلْمه.

تمسّ هذه المخاطر الرياضي بشكلٍ مباشر لأن:

- حساباته الرقمية تُمثِّل واجهته الرسمية أمام الجمهور والإعلام والرعاة
- هاتفه وبريده الإلكتروني يحتويان على مراسلات مهنية خاصة مع الأندية، والمدربين، والوكلاء
- أيّ تسريب لمحتوى خاص قد يُستخدَم للضغط النفسي أو للتشهير قبل أو في أثناء المنافسات
- بياناته الصحية والبدنية المُخزَّنة في التطبيقات الذكية معلومات حسَّاسة عُرضَة للاستهداف

لماذا يُعدّ الرياضي هدفًا سهلًا للمخترقين؟

الشهرة والاهتمام الجماهيري؛ حيث يسهل استغلال أيّ خطأ أو معلومة لتحقيق مكاسب مالية أو إعلامية

امتلاك حسابات ذات قيمة عالية من حيث عدد المتابعين والتأثير

الانشغال الدائم بالتدريب والسفر والمباريات، ممّا يُقلّل من التدقيق في الرسائل والروابط

تعدُّد الدوائر المحيطة به، مثل: الجهاز الفني، والإدارة، والزملاء، والمعجبين

الطموح المهني، خاصةً لدى اللاعبين الناشئين، والذي يُستغل عبر عروض وهمية للاحتراف أو المعسكرات الخارجية

ضَعْف الوعي الرقمي لدى بعض الرياضيين، مثل: استخدام كلمات مرور ضعيفة أو عدم تفعيل وسائل الحماية الإضافية

السؤال التفاعلي الأول

تأثير المخاطر السيبرانية

الإضرار بالسُّمعة العامة نتيجة نشر محتوى مسيء أو مجتزأ خارج سياقه

فقدان ثقة الرعاة والشركاء، مما قد يُؤدي إلى إلغاء العقود أو عدم تجديدها

توتُّر العلاقات المهنية في حال تسريب معلومات داخلية أو خطط تدريبية

التأثير النفسي السلبي على اللاعب بسبب التهديد أو الابتزاز، وهو ما ينعكس على مستوى الأداء

التعرُّض لمُساءَلَة قانونية أو إدارية نتيجة نشر معلومات حساسة دون موافقة رسمية

الخصوصية الرقمية وحماية السُّمعة

تُمثِّل الخصوصية الرقمية خطّ الدفاع الأول عن سُمعة الرياضي؛ إذ إن أيّ محتوى يُنشَر أو يُسَرَّب قد يُؤثِّر بصورة مباشرة على الجمهور، والنادي، والرعاة، ويصعب التحكُّم في نتائجه بعد انتشاره.

مفهوم الخصوصية الرقمية

قدرة الرياضي على التحكُّم في معلوماته وصوره ورسائله، وما يشاركه عبر الإنترنت، وتحديد مَن يحقّ له الاطلاع عليها، ومتى، ولماذا

لماذا تُعدّ السرية مُهِمّة في حياة الرياضي؟

الرياضي شخصية عامة، لكنّ حياته الخاصة ليست مادة مفتوحة للجميع.

الحفاظ على السرية يمنع:

- إساءة تفسير التصرُّفات الشخصية
- استغلال الخصوم لأيّ محتوى خارج سياقه
- حدوث مشكلات تنظيمية أو قانونية

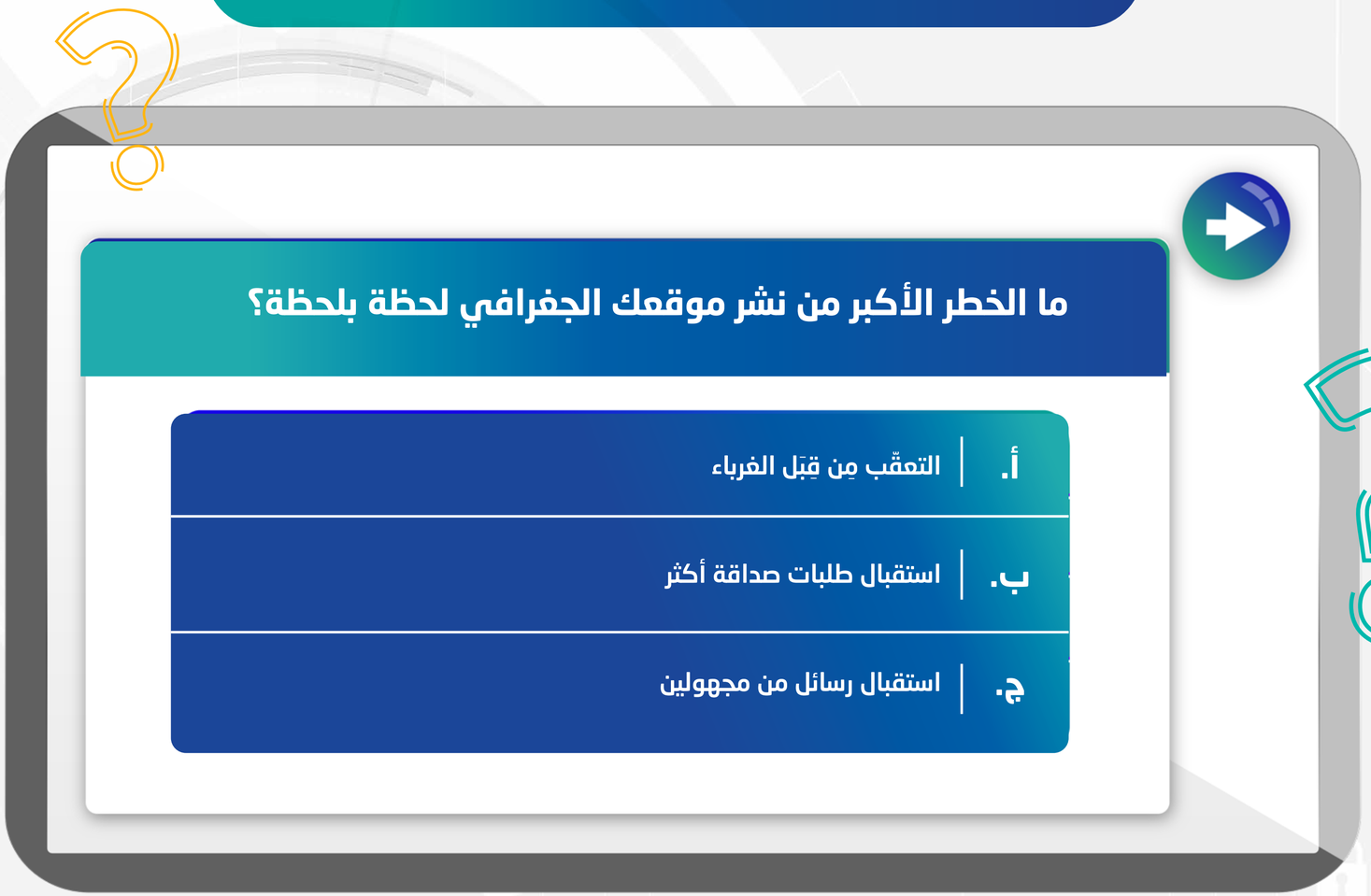
مخاطر مشاركة المعلومات الشخصية

تؤدّي مشاركة البيانات الشخصية دون وعي إلى تعرُّض المستخدِم لمخاطر متعددة.

أبــرز المخـــاطر

- انتحال الهوية الرقمية
- الاحتيال المالي والإلكتروني
- انتهاك الخصوصية الشخصية
- استغلال البيانات لأغراض تسويقية
- فقـــدان السيطرة على المعلومـــات المنشورة

السؤال التفاعلي الثاني



مخاطر كلمات المرور

يقع كثير من المستخدمين في أخطاء تُقلّل من قوة كلمات المرور، وتجعلها عُرضة للتخمين أو الخرق.

أبرز الأخطاء الشائعة

1. استخدام كلمات مرور بسيطة يسهل توقّعها أو تخمينها
2. الاعتماد على معلومات شخصية معروفة أو متاحة للآخرين
3. اختيار كلمات مرور قصيرة لا تُوفّر حماية كافية
4. إعادة استخدام كلمة المرور نفسها في أكثر من حساب
5. مشاركة كلمة المرور مع أشخاص آخرين بدافع الثقة

مخاطر وسائل التواصل الاجتماعي

توفر وسائل التواصل الاجتماعي فرصًا كبيرة للرياضي لبناء سُمعته وصورته العامة، لكنّها في الوقت نفسه تحمل مخاطر حقيقية إذا استُخْدِمَت دون وَعْي أو ضبط.

أبرز المخاطر

تتبُّع البصمة الرقمية

وهي كل ما يَنشره الرياضي أو يُنشَر عنه على الإنترنت، ويظل قابلًا للوصول أو الاسترجاع في أيّ وقت، حتى بعد الحذف

رسائل مجهولة تدّعي تمثيل شركة رعاية

كثير من المحتالين يستغلون طموح الرياضيين عبر رسائل تدّعي تمثيل شركات أو وكلاء، ويهدفون من خلالها إلى سرقة بيانات أو السيطرة على الحسابات

روابط وهمية لزيادة عدد المتابعين

هذه الروابط غالبًا ما تكون بوابة لاختراق الحساب أو سرقة كلمة المرور

السؤال التفاعلي الثالث

أيّ خطوة من التالي تساعدك أكثر في حماية حساباتك عبر المنصات الاجتماعية؟

أ. تعيين كلمة سر قوية

ب. استخدام التحقّق متعدّد العوامل

ج. رفض طلبات الصداقة

سرقة البيانات والتحليلات البدنية

البيانات الصحية والبدنية للرياضي تُعدّ معلومات حساسة، وقد يكون تسريبها مؤثرًا على قرارات المشاركة، والخطط الفنية، والحالة النفسية.

ماذا تشمل البيانات البدنية؟

معدلات اللياقة، والإصابات، وبرامج التدريب، ونتائج أجهزة التتبُّع، والخطط الخاصة بالإعداد البدني

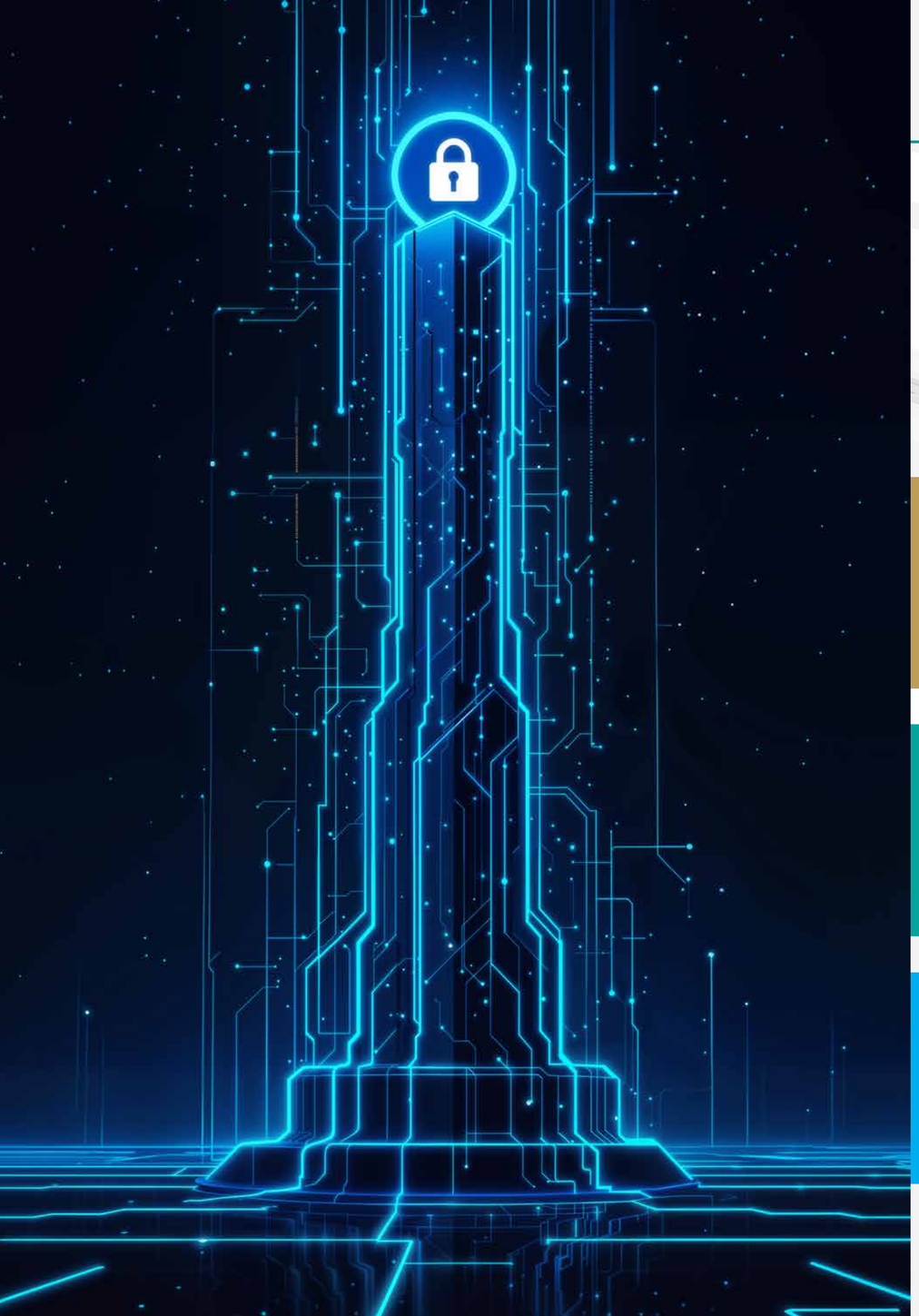
كيف يمكن اختراق أجهزة تتبُّع الأداء؟

من خلال ربطها بشبكات غير آمِنَة، أو تثبيت تطبيقات غير موثوقة، أو مشاركة البيانات دون وعي

لماذا تُعدّ هذه البيانات مُهمَّة؟

لأنها تكشف مستوى الجاهزية، ونقاط القوة والضعف، وقد تُستخدَم للضغط الإعلامي أو الفني

السؤال التفاعلي الرابع



الابتزاز الإلكتروني للرياضيين

الابـتزاز الإلكترونـي مـن أخطـر التهديـدات الرقميـة، وغالبًـا مـا يَبـدأ بخطـوة بسـيطة يُقْـدِم عليهـا الضحيـة دون وَعْـي ثـم تتصاعـد الأحـداث سريعًـا.

ما معنى الابتزاز الإلكتروني؟

تهديد بنَشْر محتوى خاص أو معلومات حسّاسة مقابل الحصول على المال أو تنفيذ طلب معين

لماذا يُستهدَف الرياضيون؟

بسبب الشهرة، والضغط النفسي، والقدرة المالية، ووجود محتوى شخصي قد يُساء استخدامه

كيف يُميِّز الرياضي الرسائل المشبوهة؟

مِن خلال نَبْرة التهديد، أو طلب السرية، أو الإلحاح، أو الادّعاء بامتلاك معلومات سرية

السؤال التفاعلي الخامس

الاحتيال الرياضي عبر الإنترنت

الاحتيال الرقمي يستغل طموح الرياضيين، خاصةً في مراحل البحث عن الاحتراف أو الشهرة.

- مواقع وَهْمية لعروض احتراف خارجية تستخدم أسماء أندية معروفة
- تسجيلات مُزيَّفة لمدربين كبار يتم فيها انتحال صفات مدربين أو وكلاء معروفين
- استغلال الطموح الرياضي للحصول على المال عبر طلب رسوم تسجيل أو معسكرات غير حقيقية

03 المحور الثالث

أساليب الوقاية والسلامة الرقمية

مبادئ السلامة الرقمية للرياضيين

التفكير قبل الضغط على أيّ رابط أو فتح أيّ رسالة مجهولة

عدم التفاعل مع الحسابات غير المُوثّقة أو المجهولة

الإبلاغ الفوري عن أيّ حادث اختراق أو محاولة للاستغلال

التعامل مع الإنترنت كجزء من الحياة المهنية، وليس وسيلة ترفيه فقط

خصائص كلمة المرور القوية

تعتمد قوة كلمة المرور على مجموعة من الخصائص التي تزيد من صعوبة خَرْقها باستخدام الأساليب التقليدية أو الآلية.

خصائص كلمة المرور القوية

- تكون بطول كافٍ يجعل تخمينها أمرًا بالغ الصعوبة
- تحتوي على مزيج من الحروف الكبيرة والصغيرة
- تتضمّن أرقامًا ورموزًا خاصة لزيادة التعقيد
- غير مرتبطة بمعلومات شخصية أو متوقّعة
- فريدة وغير مستخدَمة في حسابات أخرى

إدارة كلمات المرور

استخدام كلمة مرور قوية وفريدة لكل حساب

عدم مشاركة كلمات المرور مع أيّ شخص

تغيير كلمات المرور بشكل دوري

استخدام مدير كلمات مرور موثوق

تفعيل المصادقة الثنائية

يُقصَد بها إضافة خطوة تحقُّق ثانية، بالإضافة إلى كلمة المرور (مثل: إرسال رمز على الهاتف، بطاقة ذكية، أو تطبيق مصادقة)، قبل الولوج إلى الحسابات أو البريد الإلكتروني، بما يُقلِّل بشكل كبير من احتمال الاختراق حتى لو سُرِقَت كلمة المرور.

- تفعيل المصادقة الثنائية على جميع حسابات التواصل والبريد
- استخدام تطبيقات التحقق بدلًا من الرسائل النصية عند الإمكان
- عدم مشاركة رمز التحقّق مع أيّ جهة
- حفظ رموز الاسترداد في مكان آمِن

التعامل الآمِن مع الروابط والمرفقات

- عدم فتح الروابط المجهولة أو المختصرة
- التحقُّق من عنوان الموقع قبل إدخال أيّ بيانات
- تجاهل الرسائل العاجلة التي تضغط لاتخاذ قرار سريع
- عدم تحميل ملفات من مصادر غير موثوقة

إعدادات الخصوصية على وسائل التواصل الاجتماعي

- مراجعة إعدادات الخصوصية بشكلٍ منتظم
- إخفاء الموقع الجغرافي من القصص والمنشورات
- تقييد مَن يمكنه إرسال رسائل خاصة إلى حسابك
- عدم نَشْر محتوى من أماكن حساسة مثل: غُرَف الملابس

السؤال التفاعلي السادس

حماية الأجهزة الشخصية

- قفل الهاتف والأجهزة الذكية ببصمة أو رمز قوي
- تحديث نظام التشغيل والتطبيقات باستمرار
- تحميل التطبيقات من المتاجر الرسمية فقط
- الحذف الدوري للتطبيقات غير المستخدَمة

تحديث الأنظمة والتطبيقات

تُسهم التحديثات الدورية في مُعالجة الثغرات الأمنية، وتحسين مستوى الحماية العامة للأجهزة

تحسين استقرار وأداء الجهاز

سدّ الثغرات الأمنية المكتشفة حديثًا

رفع مستوى التوافق مع تقنيات الأمان الحديثة

تعزيز خصائص الحماية في النظام

الحماية من البرمجيات الخبيثة

تشمل البرمجيات الخبيثة برامج تُصمَّم لإلحاق الضرر بالأجهزة أو سرقة المعلومات.

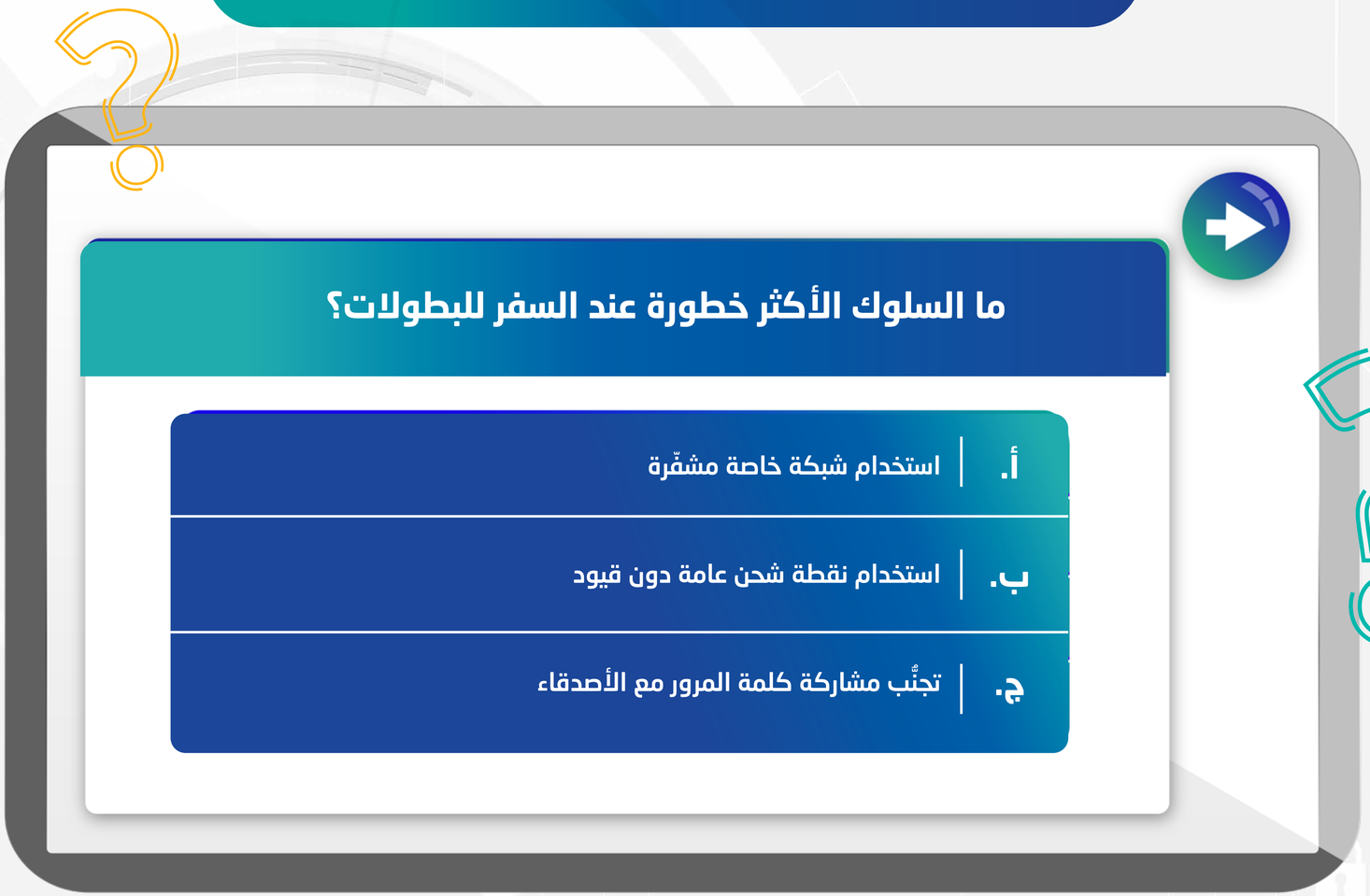
وسائل الحماية الأساسية

- تجنُّب تحميل الملفات من مصادر غير موثوقة
- عدم تثبيت البرامج المقرصنة أو المجهولة
- تحديث النظام وبرامج الحماية بانتظام
- فَحْص الملفات قبل فتحها أو تشغيلها
- الحذر من الروابط والمرفقات المشبوهة

السلامة الرقمية في أثناء السفر

- تجنُّب استخدام شبكات Wi-Fi العامة
- استخدام شبكة خاصة أو اتصال آمِن مشفّر VPN
- عدم شحن الأجهزة عبر منافذ USB عامة
- إبقاء الأجهزة الشخصية تحت المراقبة دائمًا

السؤال التفاعلي السابع



أمان الأجهزة المحمولة

تحتوي الأجهزة المحمولة على بيانات شخصية حساسة، وتتطلب حماية خاصة.

إجراءات تعزيز الأمان

- تفعيل قفل الشاشة بوسيلة آمِنة
- تحديث نظام التشغيل والتطبيقات باستمرار
- تجنّب تثبيت التطبيقات من مصادر غير موثوقة
- تفعيل ميزة تحديد الموقع والمسح عن بُعْد
- عدم ترك الجهاز دون رقابة في الأماكن العامة

الاستخدام الآمِن للأجهزة في الأندية والملاعب

الأجهزة المستخدَمة يوميًّا قد تتحوَّل إلى نقطة ضَعْف إذا أُهْمِلَت إجراءات الأمان الأساسية.

1. تجنّب توصيل USB غير معروف؛ لأنه قد يحتوي على برمجيات خبيثة
2. عدم مشاركة الإنترنت مع الغرباء؛ لأن الشبكات المشتركة تُسهِّل الاختراق
3. قفل الحاسوب في صالة التدريب لمنع الوصول غير المصرَّح به
4. فَصْل الأجهزة الشخصية عن أجهزة النادي لحماية البيانات المهنية

الاستجابة السريعة للحوادث السيبرانية

تغيير كلمات المرور فور الاشتباه بأيّ اختراق

تسجيل الخروج من كل الأجهزة المرتبطة بالحساب

توثيق رسائل التهديد أو محاولات الابتزاز

الإبلاغ الفوري لدى الجهة المختصة، وعدم التصرُّف منفردًا

إجابات الأسئلة التفاعلية

01	**إجابة السؤال التفاعلي الأول** كلمات مرور الحسابات
02	**إجابة السؤال التفاعلي الثاني** التعقّب من قِبل الغرباء
03	**إجابة السؤال التفاعلي الثالث** استخدام التحقق متعدد العوامل
04	**إجابة السؤال التفاعلي الرابع** لأنها عُرضة للاختراق
05	**إجابة السؤال التفاعلي الخامس** تجاهل التهديد وإبلاغ المسؤولين
06	**إجابة السؤال التفاعلي السادس** الاتصال بالنادي رسميًّا
07	**إجابة السؤال التفاعلي السابع** استخدام نقطة شحن عامة دون قيود

المراجع

1. Cybersecurity Considerations for Professional Athletes and Sports Organizations, on site: https://wwwenisaeuropaeu/publications/cybersecurity-in-sports
2. Digital Identity Guidelines, NIST SP 800-63-4, on site: https://nvlpubsnistgov/nistpubs/SpecialPublications/NISTSP800-63-4pdf
3. NIST SP 800-63B: Authentication and Lifecycle Management, on site: https://nvlpubsnistgov/nistpubs/SpecialPublications/NISTSP800-63Bpdf
4. Social Engineering Attacks and Mitigation Strategies, on site: https://wwwcisagov/social-engineering
5. Cyber Threats to Sports Organizations and Athletes, on site: https://wwwinterpolint/en/Crimes/Cybercrime

6. Data Privacy and Protection in Sports Technology, on site: https://wwwi-scoopeu/data-protection/sports-data-privacy/

7. Cybersecurity Best Practices for Mobile Devices, on site: https://wwwncscgovuk/guidance/mobile-device-security

8. Identity Theft and Digital Footprint Risks, on site: https://wwwidentitytheftgov/

9. Cybersecurity and Athlete Data Protection – IOC Guidelines, on site: https://olympicscom/ioc/athlete365

10. Ransomware Threats and Prevention Strategies, on site: https://wwwcisagov/ransomware

11. Artificial Intelligence and Deepfake Risks, on site: https://wwwweforumorg/publications/deepfakes-and-cybersecurity

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