الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبادئ عامة في السلامة الرقمية

الفئة المستهدَفة

المؤسسات العقابية والنيابة والمؤسسات الإصلاحية

كُتَيّب المُدَرّب

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

الفئة المستهدَفة

المؤسسات العقابية والنيابة والمؤسسات الإصلاحية

كُتَيّب المُدَرّب

تمهيد

في عصر التحوُّل الرقمي، لم تَعُد المؤسسات الإصلاحية والعقابية والنيابات العامة مجرد كيانات تقليدية، بل تحوَّلت إلى منظومات رقمية مُعقَّدة مُحاطَة بقَدْر كبير من المخاطر السيبرانية.

وقد تم تصميم هذا الكُتَيِّب بهدف توعية العاملين في هذه المؤسسات بمبادئ السلامة الرقمية، وأفضل الممارسات التي تساعدهم على تفادي هذه المخاطر؛ حيث يهدف إلى تعزيز وعيهم بأبرز التهديدات السيبرانية التي قد يتعرَّضون لها في أثناء عملهم؛ مثل: التصيّد الاحتيالي، برمجيات الفدية، الفيروسات، وسرقة الهوية الرقمية.

كما يُقدِّم الكُتَيّب أفضل الممارسات والإجراءات الوقائية لحماية الأجهزة، وتأمين الحسابات، والتعامل السريع مع مؤشرات الاختراق، وحماية المصادر البيانات وتشفيرها.

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 المستهدفة

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

المرأة والأسرة

كبار القَدْر

02 السنة الثانية

الدبلوماسيون

الإعلاميون

الرياضيون

المؤسسات العقابية والنيابة والمؤسسات الإصلاحية

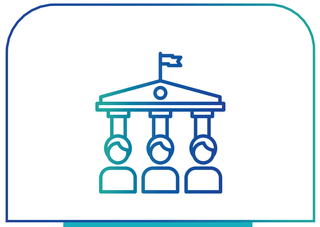
العاملون في المجال الصحي

المرأة (العنف الرقمي ضد المرأة)

الجمهور العام

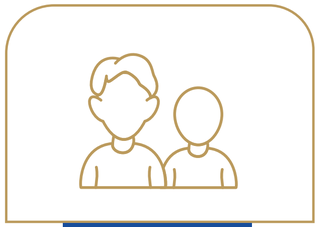
03 السنة الثالثة

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

كُتيّبات توعية مطبوعة

شرائح العرض (للمُدرّبين)

فيديوهات التوعية (أنيميشن)

فيديوهات التوعية (تمثيلية)

خَـلّك وَاعـي
وَعْيك دِرْعك

الألعاب السيبرانية

بوابة التوعية السيبرانية

الروبوت التفاعلي

وِرَش التوعية

المحور الأول

الوكالة الوطنية للأمن السيبراني وحماية المجتمع الرقمي

الوكالة الوطنية للأمن السيبراني

National Cyber Security Agency

التأسيس والأهداف

التأسيس

تأسَّست الوكالة الوطنية للأمن السيبراني بمُوجب المرسوم الأميري رقم (1) لعام 2021م، كمرجعيَّة وطنية لحماية الفضاء السيبراني؛ بهدف تعزيز الأمن السيبراني للدولة، وضمان حماية الأصول الرقمية والبِنْية التحتية الحيوية من التهديدات السيبرانية المتزايدة.

الأهداف

تعزيز الأمن السيبراني

تطوير سياسات مُتقدّمة لضمان حماية الأنظمة الرقمية، وتطبيق إجراءات وقائية شاملة للكشف عن التهديدات السيبرانية، ومعالجتها

رَفْع مستوى الوعي

تنظيم برامج تدريبية وحملات توعية تهدف إلى تثقيف الأفراد والمؤسسات حول أهمية الأمن السيبراني، وكيفية التصدّي للهجمات السيبرانية

بناء القدرات الوطنية

تدريب الكوادر الوطنية على أحدث تقنيات الأمن السيبراني، ودعم الأبحاث والدراسات التي تُعزِّز من قدرة الدولة على التصدّي للتحديات السيبرانية

التعاون الدولي

إقامة شراكات مع المنظمات الدولية، وتبادل الخبرات مع الدُّوَل الرائدة في مجال الأمن السيبراني؛ لمكافحة الجرائم السيبرانية، وتعزيز الحماية السيبرانية

الرؤية والاختصاصات

الرؤيـــــة الإستراتيجية

بلوغ فضاء سيبراني آمِن

يدعم التنمية الاجتماعية والاقتصادية

تمكين اقتصاد المعرفة

عَبْر تعزيز الثقة في الخدمات الرقمية

الاختصاصات

1. إعداد وتنفيذ الإستراتيجية الوطنية للأمن السيبراني
2. رَصْد التهديدات السيبرانية والاستجابة للحوادث عبر فِرَق متخصّصة
3. وَضْع السياسات والمعايير الفنية والتنظيمية لحماية البنية التحتية الرقمية
4. تنسيق الجهود الوطنية بين الجهات الحكومية والخاصة في مجال الأمن السيبراني
5. رَفْع الوعي المجتمعي حول الأمن السيبراني من خلال حملات وبرامج تدريبية
6. تمثيل الدولة دوليًّا في المحافل والاتفاقيات المتعلّقة بالأمن السيبراني
7. تطوير خبرات الكوادر الوطنية عبر التدريب والشهادات المهنية في المجال

حماية البيانات والقطاعات الحيوية

01 تتبنَّى الوكالة أحدث المعايير الدولية في مجال حماية البيانات؛ لضمان أمان الأنظمة الرقمية

02 تضطلع الوكالة بدور توجيهي في ضمان التزام المؤسَّسات بتطبيق القانون رقم (13) لسنة 2016 لحماية خصوصية البيانات الشخصية

03 تطوير برامج تدريبية للمؤسسات العامة والخاصة لتعزيز وَعْيها بحماية البيانات وتأهيل وتدريب العاملين فيها على تطبيق الإجراءات الوقائية اللازمة

04 إطلاق مبادرات لتعريف المُستخدِمين بحقوقهم في الوصول إلى بياناتهم وحمايتها، بما يُعزّز الشفافية والثقة المتبادلة بين المُستخدِمين والمؤسسات

05 توفير قنوات اتصال للإبلاغ عن خروقات البيانات، مع ضمان التعامل مع الشكاوى بسُرعة وفعالية لتقليل الضرر وحماية المُستخدِمين

التكامل في التعامل مع الجرائم الإلكترونية

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

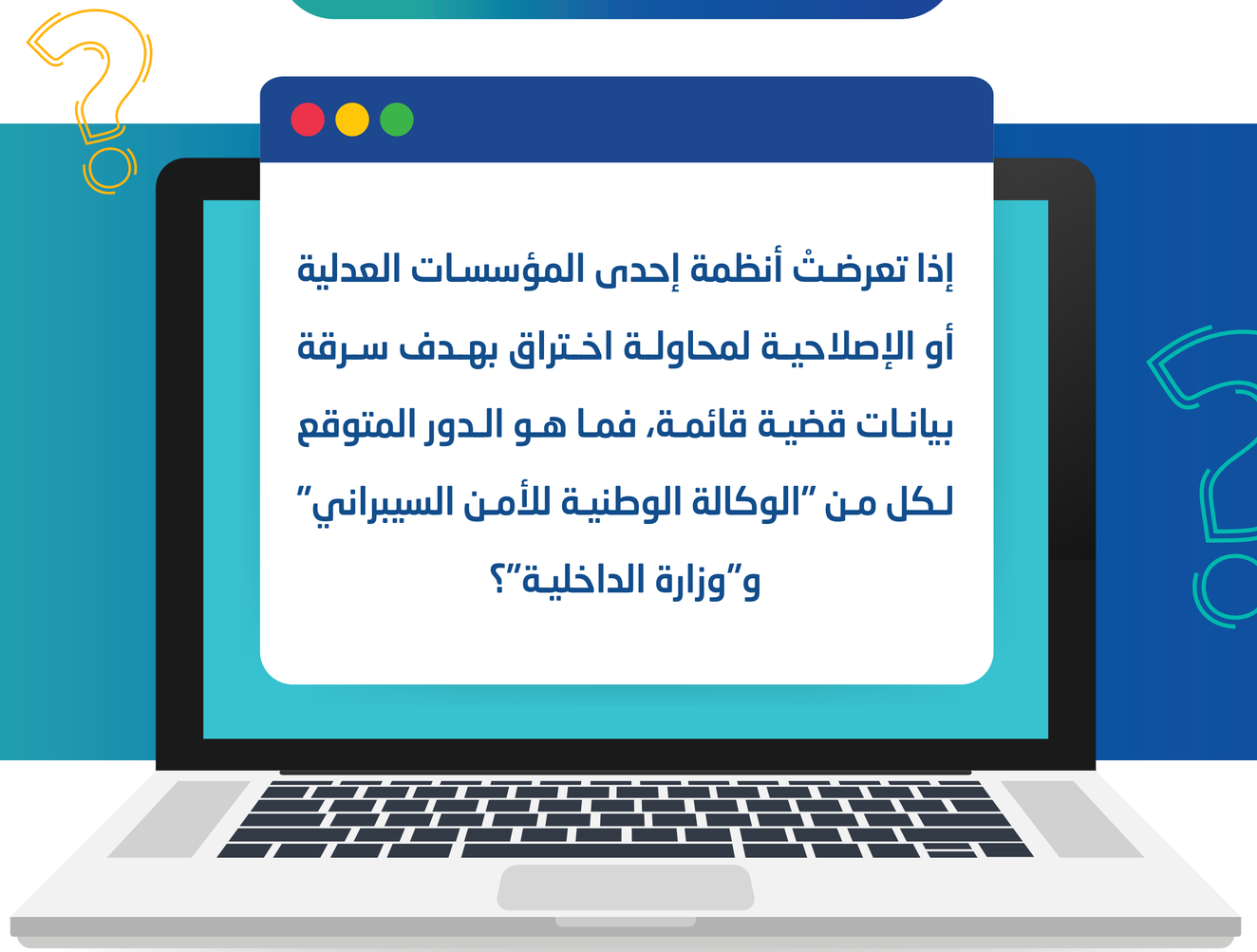
الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

- 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

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

سؤال تفاعلي



إذا تعرضتْ أنظمة إحدى المؤسسات العدلية أو الإصلاحية لمحاولة اختراق بهدف سرقة بيانات قضية قائمة، فما هو الدور المتوقع لكل من "الوكالة الوطنية للأمن السيبراني" و"وزارة الداخلية"؟

المحور الثاني

التهديدات السيبرانية الشائعة في البيئة العدلية والإصلاحية

الهندسة الاجتماعية الموجَّهة

يعتمد المهاجم في الهندسة الاجتماعية على عامِل "الاستعجال" و"السلطة"؛ فقد يتحل صفة جهة رقابية عليا أو جهة تقنية داخلية، وبمجرد الضغط على الرابط أو تحميل المرفق، يتم اختراق الشبكة الداخلية للمؤسسة.

الهدف غالبًا هو سرقة بيانات الاعتماد (اسم المستخدِم وكلمة المرور) للدخول إلى أنظمة إدارة القضايا (CMS) أو أنظمة إدارة النزلاء (IMS).

أرقام وحقائق

تشير تقارير عالمية إلى أن القطاعَيْن الحكومي والقضائي من بين أكثر القطاعات استهدافًا ببرمجيات الفدية في عام 2023.

أبرز أشكال الهجوم

البريد الإلكتروني المفخخ

رسائل تنتحل صفة وزارة العدل أو الشرطة

01

التصيد الصوتي (Vishing)

اتصال هاتفي يدّعي فيه المتصل أنه من الدعم الفني، ويطلب كلمة المرور "لحل مشكلة عاجلة"

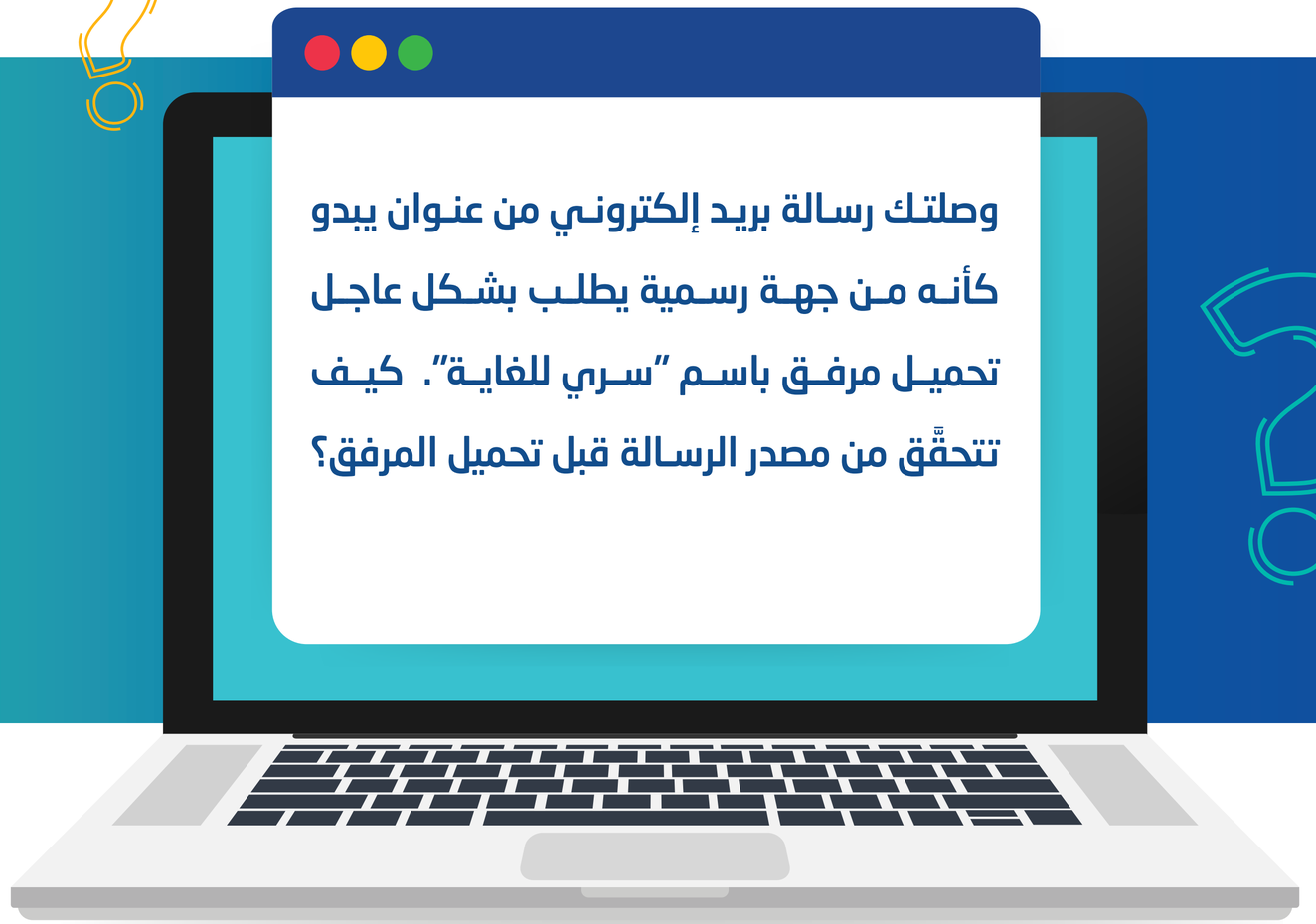
02

الاستدراج عبر وسائل التواصل

مراقبة حسابات الموظفين الشخصية لجمع معلومات تستخدم في الهجوم

03

سؤال تفاعلي



وصلتك رسالة بريد إلكتروني من عنوان يبدو كأنه من جهة رسمية يطلب بشكل عاجل تحميل مرفق باسم "سري للغاية". كيف تتحقَّق من مصدر الرسالة قبل تحميل المرفق؟

برمجيات الفدية (Ransomware)

تدخل البرمجية غالبًا عبر ثغرة غير مُحدَّثة أو مرفق بريدي خبيث. وتنتشر أُفقيًّا في الشبكة لتُشفّر الخوادم والنُّسَخ الاحتياطية المتصلة.

01 في النيابة

يـؤدي ذلـك إلـى توقُّـف التحقيقـات، تأجيـل الجلسـات، واحتمالية ضيـاع الأدلة الرقميـة؛ مما قد يؤدي لإسـقاط التُّهَم عـن مجرمين؛ لعـدم كفايـة الأدلة (بسـبب فقدانها)

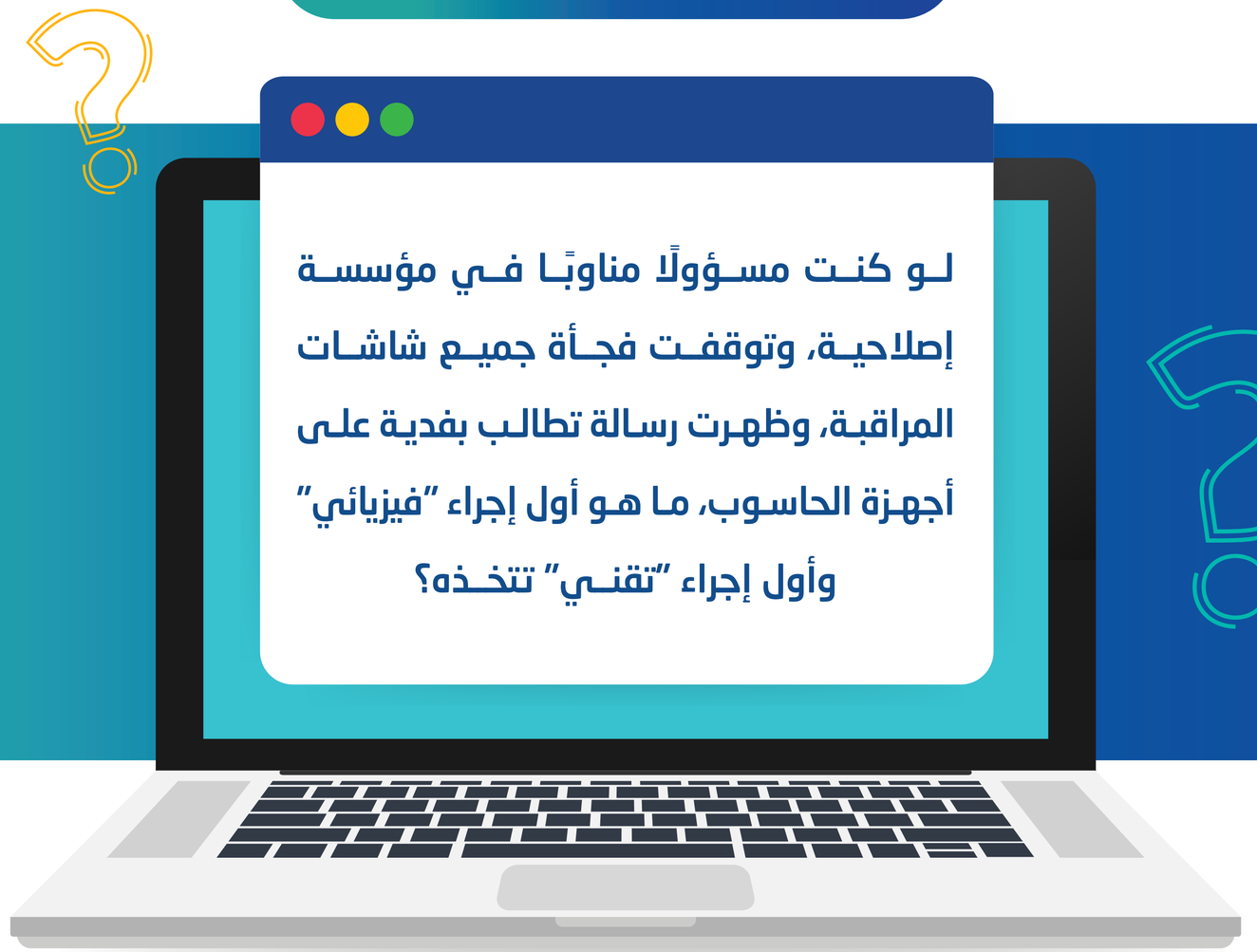
02 في المؤسسات الإصلاحية

قـد تتعطَّـل أنظمـة الزيـارات، أنظمـة المراقبـة، وحتـى أنظمـة التحكـم فـي دور الإصلاح الذكيـة بالكامـل، ممـا يسـتدعي حالـة طـوارئ أمنيـة قصـوى

إحصـــــائيات

- وفقًا لتقرير Sophos لعام 2023، تعرضت 58% من مؤسسات الحكومة المحلية (التي تشمل قطاعات القانون) لهجمات فدية
- متوسط تكلفة التعافي من هجوم فدية في القطاع الحكومي يتجاوز 1.5 مليون دولار

سؤال تفاعلي



لو كنت مسؤولًا مناوبًا في مؤسسة إصلاحية، وتوقفت فجأة جميع شاشات المراقبة، وظهرت رسالة تطالب بفدية على أجهزة الحاسوب، ما هو أول إجراء "فيزيائي" وأول إجراء "تقني" تتخذه؟

التهديدات الداخلية (Insider Threats)

المؤسسات الإصلاحية والعقابية بيئة خصبة للهجمات السيبرانية التي قد تنشأ بسبب ضعف الوعي الرقمي أو عدم الالتزام بالضوابط السيبرانية المؤسسية.

على سبيل المثال؛ قد يقوم مُوظّف باستخدام كلمة مرور ضعيفة (مثل 12345 6)، أو يشارك كلمة مروره مع زميله، مما يسهل اختراق حسابه.

نقاط الضعف الشائعة		
01	عدم وجود سجلات تدقيق وتتبُّع مَن قام بفتح أيّ ملف ومتى	
02	استخدام أجهزة التخزين الخارجية (USB) دون فحص	

اختراق أنظمة إنترنت الأشياء (IoT)

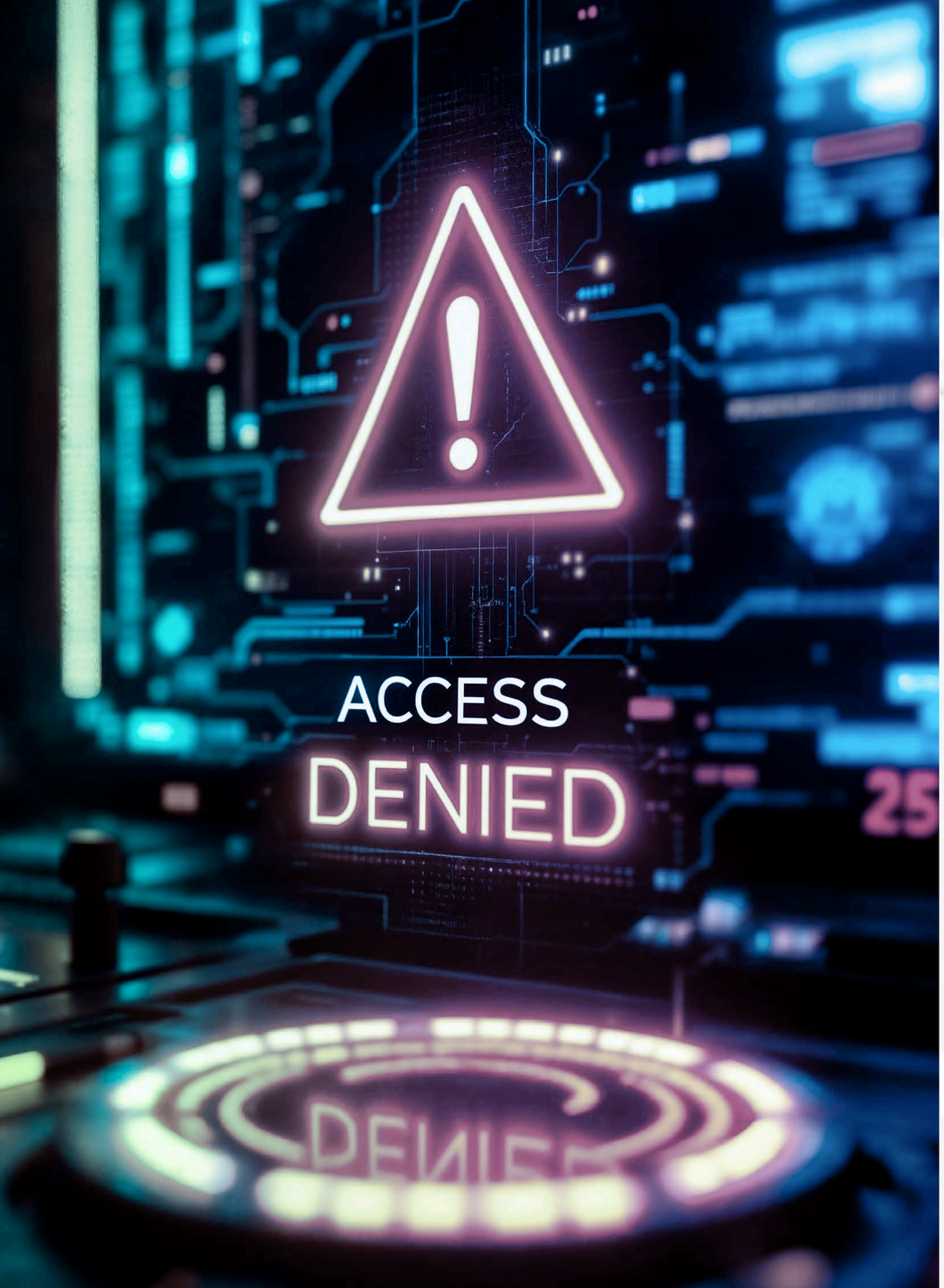
يستغل المخترقون ضَعْف برمجيات الكاميرات لاختراق الشبكة.

السيناريو المرعب

اختراق نظام الكاميرات واستبدال البث الحي بلقطات مسجلة قديمة (Looping footage)؛ لإخفاء نشاط غير قانوني أو عملية هروب

التلاعب بالأساور الإلكترونية

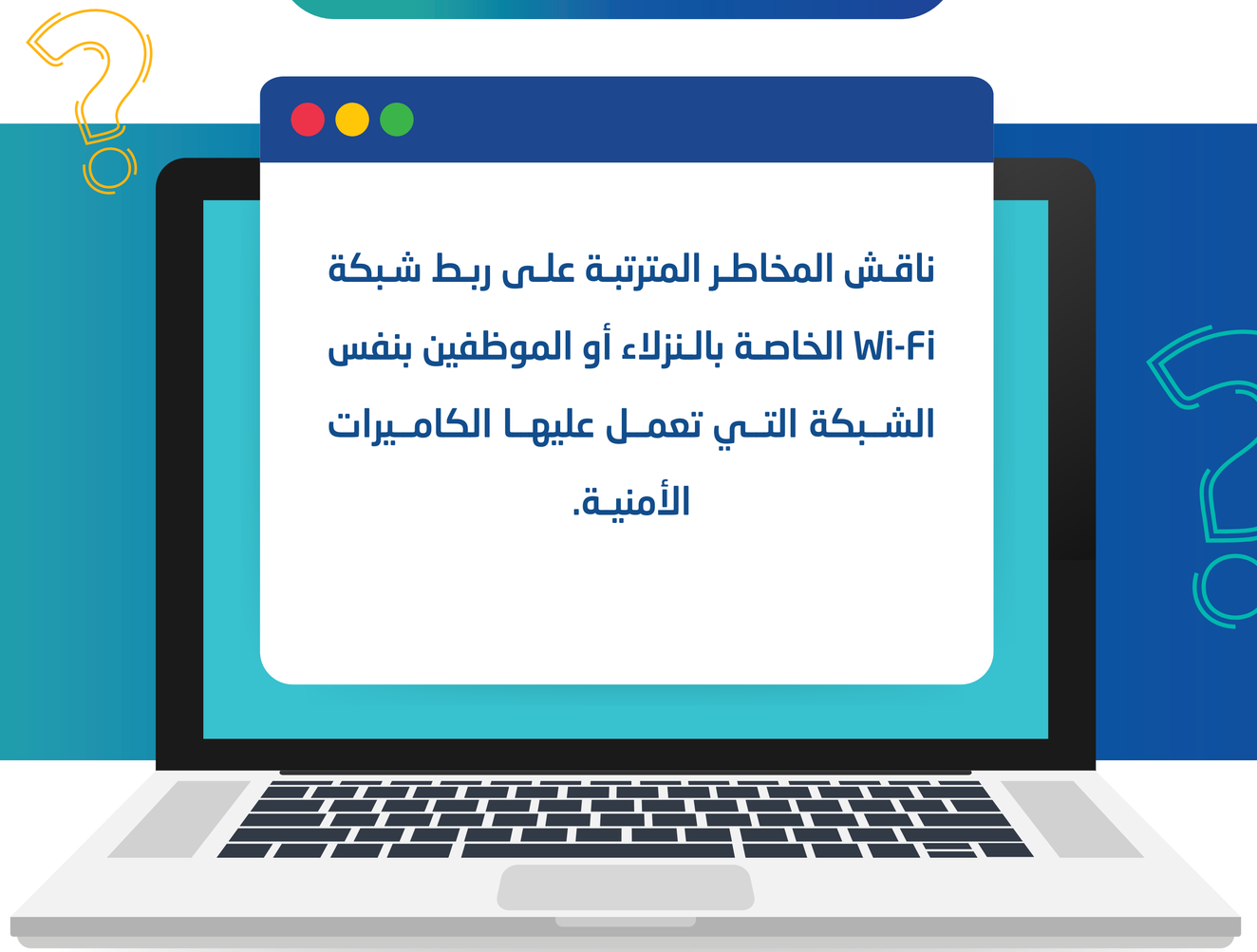
اختراق نظام تحديد المواقع (GPS) الخاص بالمُراقَبين شُرطيًّا؛ للإيحاء بأنهم في المنزل بينما هم في مكان آخر



نقاط الضعف التقنية

- عدم تغيير كلمات المرور الافتراضية للكاميرات وأجهزة الاستشعار
- رَبْط شبكة الأجهزة الأمنية بنفس الشبكة الموصولة بالإنترنت العام دون عزل
- عدم تحديث البرامج التشغيلية للأجهزة (Patching)

سؤال تفاعلي



ناقش المخاطر المترتبة على ربط شبكة Wi-Fi الخاصة بالنزلاء أو الموظفين بنفس الشبكة التي تعمل عليها الكاميرات الأمنية.

تسريب البيانات الحساسة

يحدث التسريب إما عن طريق الاختراق الخارجي لقواعد البيانات أو عن طريق الخطأ البشري (إرسال ملف بالخطأ، فقدان حاسوب غير مشفّر).

01

تأثير على القضايا

نشر تفاصيل التحقيق قد يؤدي لهروب شركاء الجريمة أو تهديد الشهود

02

الابتزاز

استخدام البيانات الطبية أو النفسية الخاصة بنزلاء أو شخصيات عامة لابتزازهم

03

المسؤولية القانونية

تعرُّض المؤسسة لدعاوى قضائية ضَخْمة لانتهاك الخصوصية

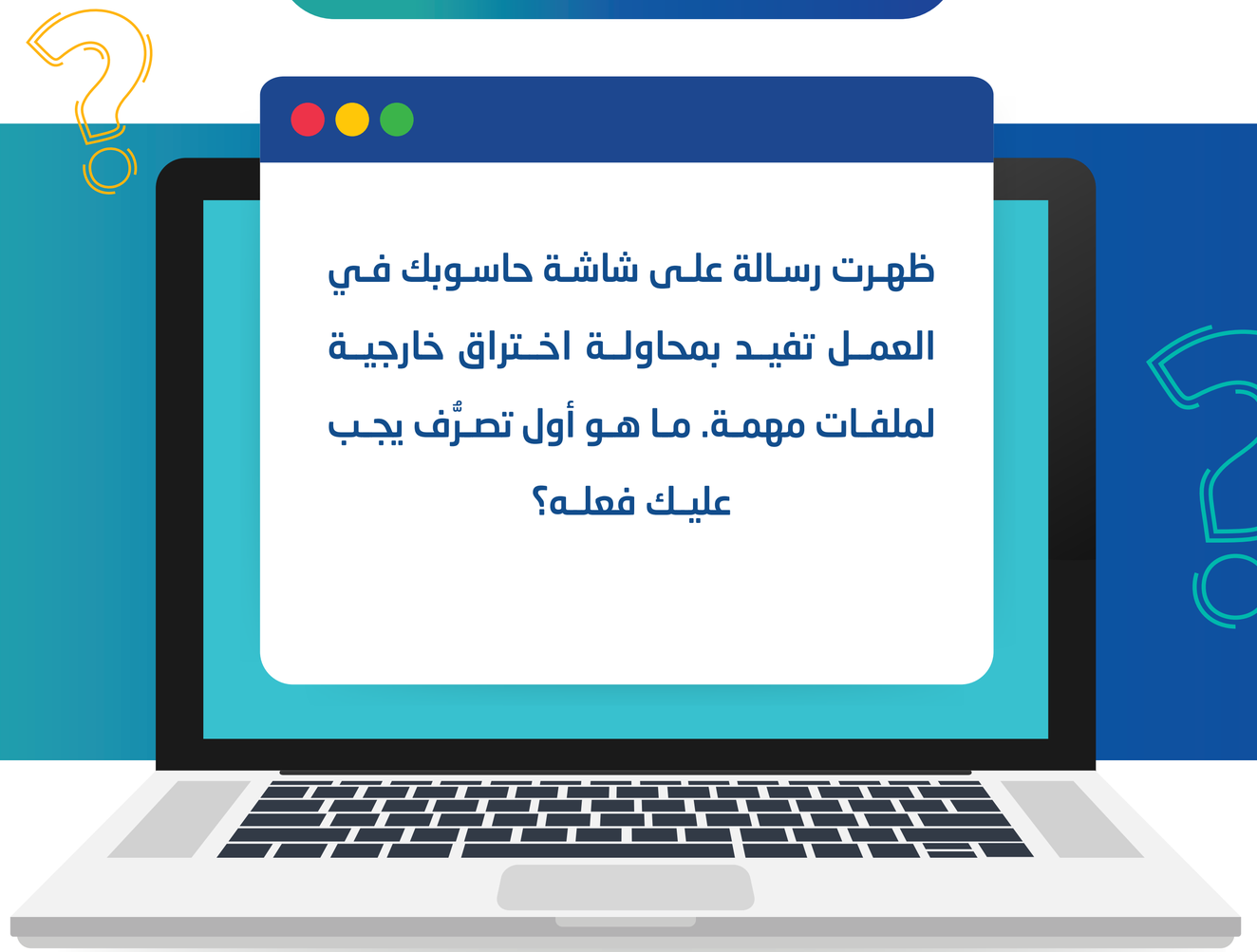
أنواع البيانات المستهدَفة

01 سجلات التحقيق (المحاضر، الأدلة)

02 بيانات الهوية البيومترية (بصمات، قزحية العين)

03 سجلات الزيارات والاتصالات الخاصة بالنزلاء

سؤال تفاعلي



ظهرت رسالة على شاشة حاسوبك في العمل تفيد بمحاولة اختراق خارجية لملفات مهمة. ما هو أول تصرُّف يجب عليك فعله؟

المحور الثالث

أساليب الوقاية والسلامة الرقمية

إدارة الهوية والوصول (IAM)

المصادقة الثنائية (MFA/2FA)

إلزامية استخدام "كلمة مرور" + "رمز يُرسَل للهاتف" أو "بصمة" للدخول للأنظمة الحساسة. هذا يمنع 99% من عمليات سرقة الحسابات

المصادقة البيومترية

استخدام بصمة اليد أو الوجه للدخول لغُرَف الخوادم أو فتح ملفات القضايا الحساسة جدًّا

المراجعة الدورية للصلاحيات

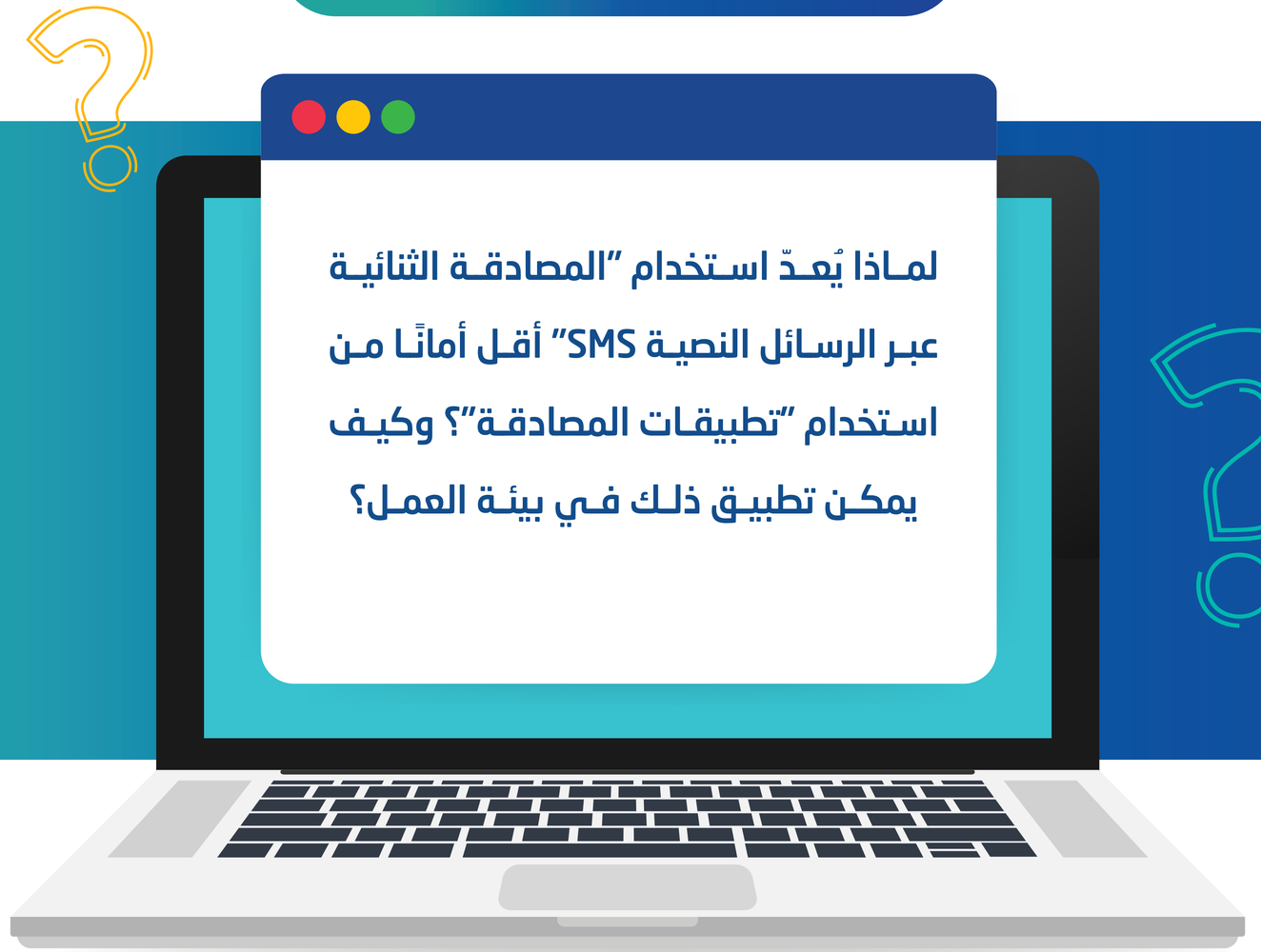
إلغاء صلاحيات الموظفين فور نقلهم أو استقالتهم لمنع "الحسابات اليتيمة" التي قد تُستغَل

أفضل الممارسات

استخدام مفاتيح أمان مادية (Security Keys) لوكلاء النيابة ومدراء الدور الإصلاحية والعقابية بدلًا من الرسائل النصية (SMS) التي يمكن اعتراضها

نظام تسجيل دخول مُوحَّد (SSO) مع رقابة صارمة

سؤال تفاعلي



لماذا يُعدّ استخدام "المصادقة الثنائية عبر الرسائل النصية SMS" أقل أمانًا من استخدام "تطبيقات المصادقة"؟ وكيف يمكن تطبيق ذلك في بيئة العمل؟

تقسيم الشبكات والعزل الرقمي (Network Segmentation)

01 شبكة منزوعة السلاح (DMZ)

وهي شبكة وسيطة محايدة تقع بين الإنترنت والشبكة الداخلية للمؤسسة، تستضيف الخدمات التي يجب أن تصل إليها جهات خارجية (مثل بوابة الخدمات الإلكترونية للنيابة)، دون منحها وصولًا مباشرًا إلى الأنظمة الحساسة داخل المؤسسة

02 عزل شبكات المعاقبين

إذا كان هناك أجهزة تعليمية للنزلاء، يجب أن تكون في شبكة منفصلة تمامًا، ولا تتصل بالإنترنت الخارجي أو الشبكة الإدارية

03 عزل الأنظمة الأمنية

شبكة الكاميرات والأبواب يجب أن تكون "شبكة مغلقة" (Intranet)، وليست متصلة بالإنترنت إلا عبر قنوات مشفرة ومؤمنة للغاية (VPN)

أهمية الإجراء

يمنع هذا الإجراء انتشار برمجيات الفدية. إذا أُصيب جهاز سكرتير في النيابة، لن تنتقل العدوى إلى خادم قاعدة البيانات الرئيسية إذا كان هناك جدار ناري وعزل شبكي بينهما.

سؤال تفاعلي

ناقِش مع زملائك أهمية الفصل بين "شبكة الـWiFi الخاصة بالنزلاء"، و"شبكة نقل البيانات الخاصة بالتحقيقات".

التشفير والنسخ الاحتياطي

01

التشفير في أثناء النقل (In-Transit)

- أي بريد إلكتروني أو ملف يُرسَل بين النيابة والشرطة أو المؤسسة الإصلاحية يجب أن يَمُرّ عبر قنوات مشفرة (VPN/SSL)

02

التشفير أثناء التخزين (At-Rest)

- تشفير الأقراص الصلبة (Hard Drives) لأجهزة الحاسوب المحمولة والخوادم. حتى لو سُرق الجهاز، لن يستطيع السارق قراءة البيانات

03

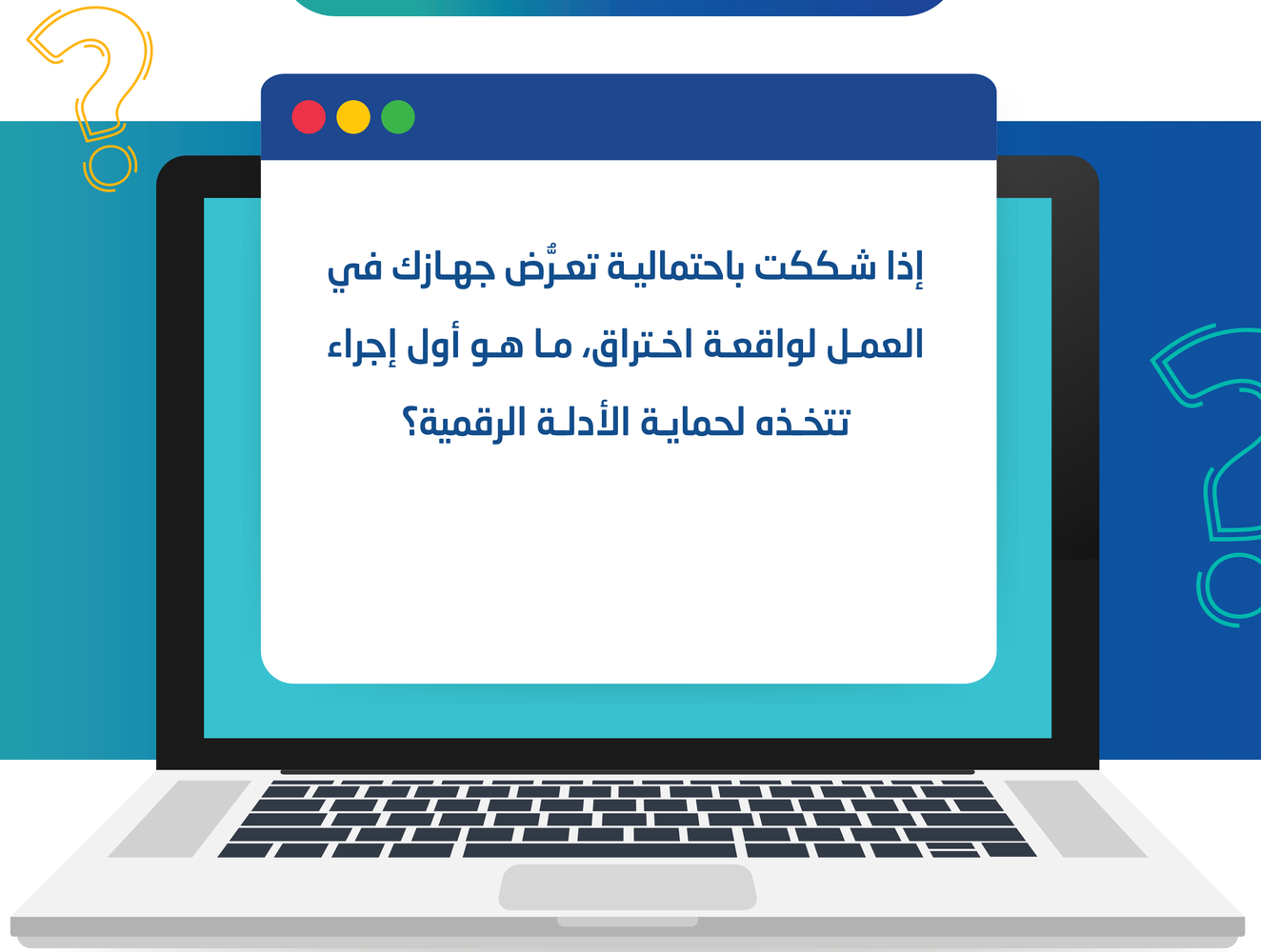
إستراتيجية النسخ الاحتياطي (3-2-1)

- إعداد 3 نسخ من البيانات
- تخزينها على وسيطين مختلفين (سحابي / محلي)
- الاحتفاظ بنسخة واحدة في مكان بعيد جغرافيًّا (Offline)؛ لحمايتها من برمجيات الفدية والكوارث الطبيعية

الأدلة الرقمية

استخدام تقنية التجزئة (Hashing) للتأكّد من أن الأدلة الرقمية (فيديوهات، مستندات)
لم يتم التلاعب بها منذ لحظة ضبطها وحتى عَرْضها في المحكمة.

سؤال تفاعلي



إذا شككت باحتمالية تعرُّض جهازك في العمل لواقعة اختراق، ما هو أول إجراء تتخذه لحماية الأدلة الرقمية؟

الاستجابة للحوادث والتحقيق الجنائي الرقمي

01 فريق الاستجابة السريعة (CSIRT)

تحديد فريق طوارئ (تقني، قانوني، إعلامي)، وتحديد أدوارهم بدقة

02 الاحتواء (Containment)

أول خطوة عند اكتشاف هجوم هي "فصل المصاب" عن الشبكة لمنع الانتشار، وليس إغلاق الجهاز؛ (لأن ذلك قد يمحو الأدلة الموجودة في الذاكرة المؤقتة RAM)

03 التحقيق الجنائي الرقمي (Digital Forensics)

الاحتفاظ بالأدلة الرقمية للهجوم لمعرفة الجاني، وتقديم دليل قانوني ضده. يتطلب ذلك عدم العبث بالأجهزة المصابة حتى وصول المختصين

بروتوكول التعامل

يحتاج كلّ موظف إلى إعداد "قائمة اتصال للطوارئ السيبرانية"؛ فالإبلاغ المبكّر يقي بنسبة كبيرة من الجرائم السيبرانية.

سؤال تفاعلي

اكتشفت أن زميلك يستخدم ذاكرة تخزين "فلاش ميموري" وجدها في موقف السيارات على جهاز متصل بشبكة العمل. فما هي الخطوات الثلاث الفورية التي تقوم بها لحماية ملفاتك؟

ثقافة الأمن السيبراني

التدريب المحاكي للواقع

01 إجراء حملات تصيُّد احتيالي وهمية (Phishing Simulation)؛ لاختبار مدى وعي الموظفين ومعرفة من يحتاج إلى تدريب إضافي

سياسة المكتب النظيف والشاشة المقفلة

02 تدريب الموظفين على عدم ترك أوراق حسَّاسة على المكاتب، وقفل شاشة الحاسوب بمجرد المغادرة ولو لدقيقة

التوعية بالمخاطر الشخصية

03 توعية الموظفين بسُبُل حماية أجهزتهم الشخصية وحساباتهم البنكية، مما ينعكس إيجابًا على سلوكهم الأمني في العمل

سؤال تفاعلي

اذكـر أهـم ثلاث أدوات تسـتخدمها وتراهـا فعّالـة لتأميـن حسـاباتك المهنيـة الحساسـة.

إدارة الثغرات والتحديثات الأمنية

1. سياسة "التحديث الفوري"

تطبيق نظام آلي لفَحْص الثغرات وتثبيت التحديثات الأمنية الحرجة خلال 48 ساعة من صدورها، خاصة للأنظمة المتصلة بالإنترنت

2. فحص الكود المصدري

بالنسبة للأنظمة التي يتم تطويرها خصيصًا للنيابة أو المؤسسات الإصلاحية والعقابية؛ يجب فحص الكود البرمجي أمنيًّا قبل إطلاقه؛ للتأكد من خلوّه من الأبواب الخلفية

معلومة

60% من الاختراقات الناجحة في القطاع العام استغلت ثغرات كان لها تحديث متاح بالفعل، ولكن لم يتم تثبيته.

أمن قنوات الاتصال والعمل عن بُعد

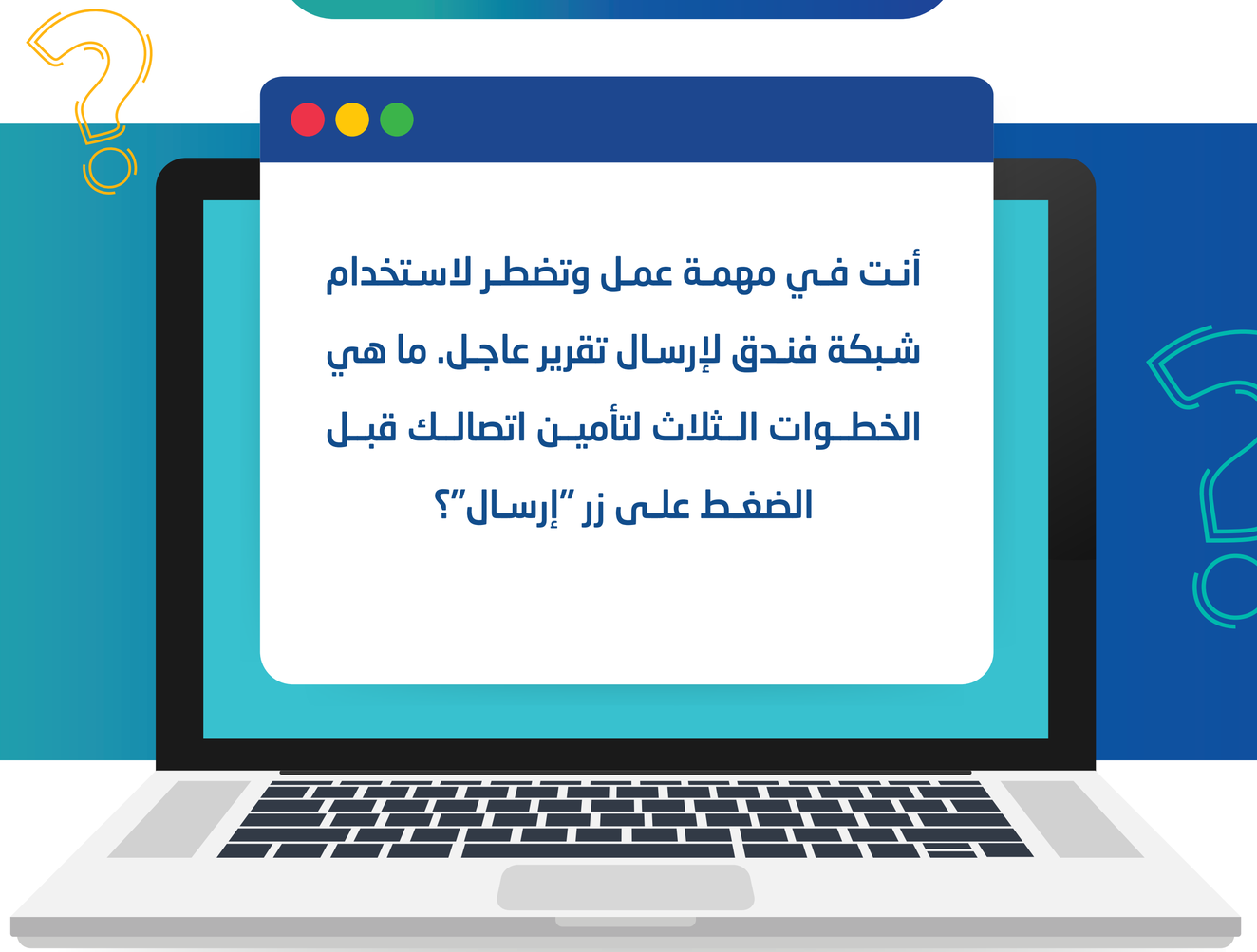
1. استخدام الشبكات الخاصة الافتراضية (VPN) ذات التشفير العالي

الاتصال بالأنظمة المركزية حصرًا عبر نفق مشفّر (VPN) معتمَد، وتجنّب استخدام شبكات Wi-Fi عامة في المقاهي أو المطارات دون حماية

2. أمن مؤتمرات الفيديو

- استخدام غرف اجتماعات محمية بكلمة مرور فريدة لكل جلسة
- تفعيل ميزة "غرفة الانتظار" للتحقُّق من هوية المنضمين قبل إدخالهم
- منع التسجيل غير المصرَّح به للجلسات

سؤال تفاعلي



أنت في مهمة عمل وتضطر لاستخدام شبكة فندق لإرسال تقرير عاجل. ما هي الخطوات الثلاث لتأمين اتصالك قبل الضغط على زر "إرسال"؟

الأمن المادي وحماية المنافذ

إغلاق منافذ البيانات (USB Blocking)

تعطيل منافذ USB في جميع أجهزة الشبكة الحساسة برمجيًّا، أو استخدام "أقفال USB بلاستيكية" (USB Port Locks)؛ لمنع إدخال أيّ وسيط تخزين غير مُصرّح به

محطات الشحن الآمنة

تجنّب شحن هواتف الموظفين عبر منافذ USB الخاصة بأجهزة الحاسوب؛ سواء كانت أجهزة العمل أو الأجهزة العامة؛ لتفادي نقل برمجيات خبيثة أو سرقة البيانات

سياسة الشاشة المقفلة

تجنّب ترك أيّ ملفات قضايا ورقية أو وسائط تخزين على المكاتب، وقفل الشاشة تلقائيًّا بعد دقيقتين من عدم النشاط

الاستجابة للحوادث والتحقيق الجنائي الرقمي

01 خطة الاستجابة للحوادث (IR Plan) عبر المراحل التالية

1. **التحضير:** تجهيز الأدوات والفِرَق
2. **الاكتشاف والتحليل:** معرفة نوع الهجوم ونطاقه
3. **الاحتواء:** عزل الأنظمة المصابة (فصل كابل الشبكة وليس إطفاء الجهاز)
4. **الاستئصال:** إزالة البرمجيات الخبيثة
5. **التعافي:** استعادة البيانات، والتأكد من نظافتها
6. **الدروس المستفادة:** كتابة تقرير لتحسين الدفاعات المستقبلية

02 الحفاظ على الأدلة

أي محاولة من غير المختصين لاستعادة الملفات قد تدمر الأدلة الجنائية الرقمية (Digital Footprints) اللازمة لإدانة المخترِق

تمرين محاكاة

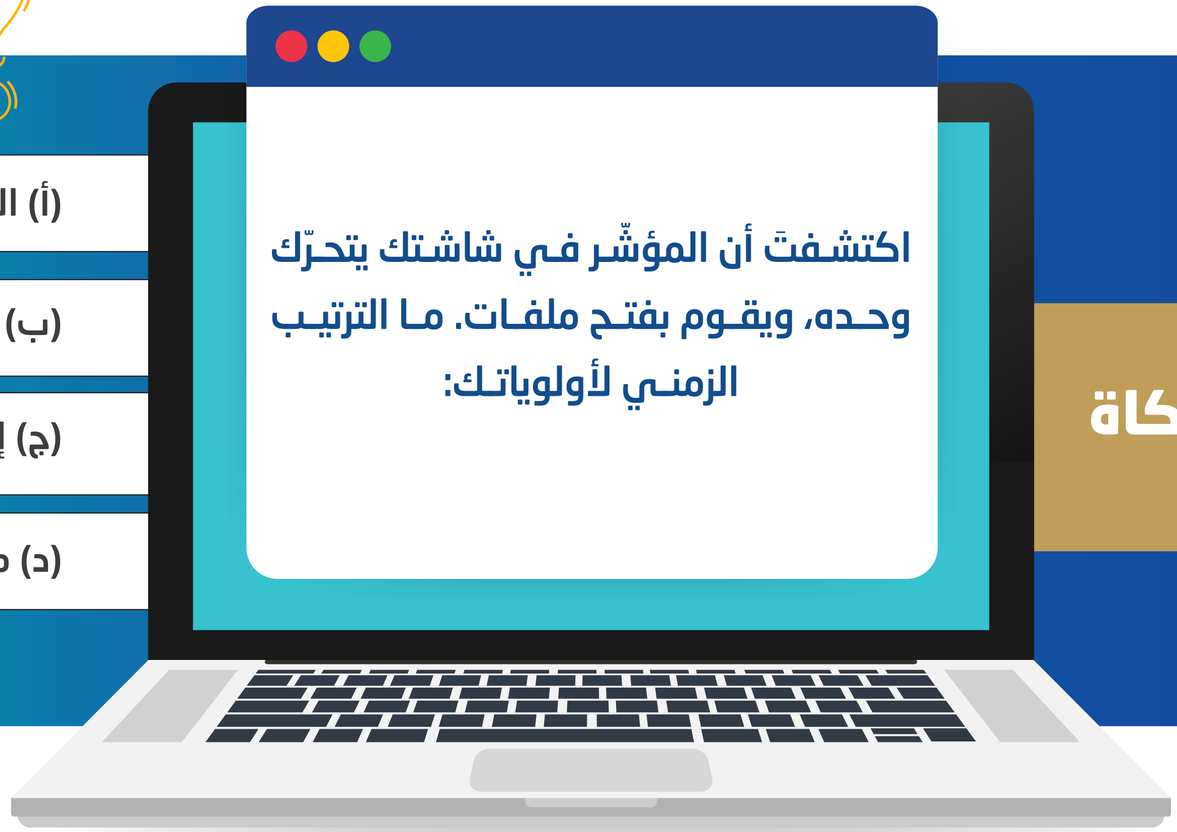
اكتشفتَ أن المؤشّر في شاشتك يتحرّك وحده، ويقوم بفتح ملفات. ما الترتيب الزمني لأولوياتك:

(أ) الاتصال بمديرك

(ب) فصل كابل الإنترنت

(ج) إيقاف تشغيل الحاسوب

(د) محاولة محاربة المخترق



المراجع

1. Casey, Eoghan. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic Press. (A bible for Digital Forensics in Prosecution). Online: https://rishikeshpansare.wordpress.com/wp-content/uploads/201602//digital-evidence-and-computer-crime-third-edition.pdf

2. Cybersecurity Challenges for Federal Attorneys and Judges. Online: https://www.fedbar.org/blog/cybersecurity-challenges-for-federal-attorneys-and-judges/

3. Jewkes, Yvonne & Reisdorf, B. (2016). Tough on Crime, Tough on Technology? The 'Smart' Prison and the Future of Corrections. Stirling University. (Specifically covers the IoT and technology risks in prisons). Online: https://www.researchgate.net/publication/304574547_A_brave_new_world_The_problems_and_opportunities_presented_by_new_media_technologies_in_prisons

المراجع

4. Veronika Hofinger and Philipp PflegerI. A reality check on the digitalisation of prisons: Assessing the opportunities and risks of providing digital technologies for prisoners. Online: https://www.researchgate.net/publication/379052768_A_reality_check_on_the_digitalisation_of_prisons_Assessing_the_opportunities_and_risks_of_providing_digital_technologies_for_prisoners

5. ENISA (European Union Agency for Cybersecurity): Threat Landscape Report. Online: https://www.enisa.europa.eu/

6. National Center for State Courts (NCSC). (2021). Cybersecurity Basics for Courts and Justice Systems. Online: https://www.ncsc.org/resources-courts/cybersecurity-basics-courts

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