الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

ورشـــــة

السلامة الرقمية في العمل الدبلوماسي

الشريحة المُستهدَفة
الدبلوماسيون

المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

تمهيد

السَّلامة الرقميَّة لم تَعُد خيارًا، بل أصبحت ركيزة أساسيَّة لضمان أمْن المعلومات، وحماية الأفراد والمجتمعات من التهديدات السيبرانية المتزايدة تعقيدًا وشراسةً.

تم تصميم هذا الكُتَيِّب ليكون مرشدًا عمليًّا للدبلوماسيين، الذين يقفون في الخطوط الأمامية للدفاع عن مصالح دولهم، ليس فقط في العالم المادي، بل وفي الفضاء السيبراني الذي أصبح ساحة رئيسية للعلاقات الدولية.

يهدف هذا الكتيب لرفع وعي الدبلوماسيين بمبادئ السلامة الرقمية، وتعزيز قُدراتهم على حماية المعلومات والأجهزة في بيئة عملٍ تتزايد فيها التهديدات السيبرانية، وتتطوّر أدواتها باستمرار.

يُسلِّط الكُتَيِّب الضوء على أبرز المخاطر الرقمية التي قد تُواجه البعثات الدبلوماسية من هجمات التصيد الموجَّهة بدقة إلى برمجيات التجسُّس المتقدمة، مع توضيح أساليب الوقاية منها بلغة واضحة ومباشرة.

كما يتضمَّن أفضل الممارسات والإجراءات الوقائية لحماية الأجهزة والحسابات الرسمية، وضمان سلامة الاتصالات التفاوضية، والاستجابة الفعَّالة والمنظَّمة للحوادث السيبرانية، إضافةً إلى ذلك، يُقدِّم إرشادات حول كشف حملات التضليل والأخبار المُضلّلة والتعامل معها بوَعْي واتزان دبلوماسي.

ولأن التهديدات لا تتوقَّف عن التطوُّر؛ يتطرَّق هذا الكُتَيّب أيضًا إلى التحدّيات السيبرانية الناشئة، مثل: أمن سلسلة التوريد الرقمية، ومخاطر إنترنت الأشياء في المقارّ الدبلوماسية، والتأثير المزدوج للذكاء الاصطناعي؛ لضمان استعداد الدبلوماسي للمستقبل الرقمي.

يأتي هذا الكُتَيِّب ضمن الجهود الوطنية لتعزيز الثقافة السيبرانية في العمل الدبلوماسي، وبالتعاون مع الوكالة الوطنية للأمن السيبراني، لبناء بيئة رقمية آمِنة تُواكب التحوّل الرقمي، وتَصُون المصالح الوطنية في الفضاء الإلكتروني.

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 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 في السنة الأولى على الشرائح التالية:

ذوو الاحتياجات الخاصة

المرأة والأسرة

كبار القَدْر

القطاع المالي
والمصرفي

مؤسسات
المجتمع المدني

العمالة الوافدة

طلبة الجامعات

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

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 توعوية 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

01 إعداد وتنفيذ الإستراتيجية الوطنية للأمن السيبراني

02 رَصْد التهديدات السيبرانية، والاستجابة للحوادث عبر فِرَق متخصّصة

03 وضع السياسات والمعايير الفنية والتنظيمية لحماية البنية التحتية الرقمية

04 تنسيق الجهود الوطنية بين الجهات الحكومية والخاصة في مجال الأمن السيبراني

05 رَفْع الوعي المجتمعي حول الأمن السيبراني من خلال حملات وبرامج تدريبية

06 تمثيل الدولة دوليًّا في المحافل والاتفاقيات المتعلّقة بالأمن السيبراني

07 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

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

تتولَّى الوكالة جانب التوعية والتوجيه التقني؛ من خلال إطلاق المبادرات، إعداد السياسات والمعايير، تنفيذ برامج التوعية، تقديم الدعم الفني، ورصد ومتابعة التهديدات الرقمية.

وزارة الداخليـــــــــة
Ministry of Interior
State of Qatar • دولـــة قطـــر

تتولَّى الوزارة حماية الجانب الأمني؛ من خلال رَصْد الجرائم الإلكترونية، والتحقيق فيها، وضبط مرتكبيها، وجَمْع الأدلة الرقمية وفق الأُطُر القانونية، وإحالة المتّهمين للمحكمة المختصة للفصل في القضايا، وتطبيق العقوبات.

سؤال تفاعلي

أيٌّ مِن الأهداف التالية لا يندرج ضمن مهام الوكالة الوطنية للأمن السيبراني، بل يقع ضمن مهام وزارة الداخلية؟

- **أ.** تعزيز الأمن السيبراني عبر تطوير السياسات والإجراءات الوقائية
- **ب.** رَفْع مستوى الوعي من خلال برامج تدريبية وحملات توعية
- **ج.** التحقيق في الجرائم الإلكترونية وضبط مرتكبيها
- **د.** بناء القدرات الوطنية وتدريب الكوادر على أحدث تقنيات الأمن السيبراني

المحور الثاني

الأمن السيبراني والعمل الدبلوماسي

الأمن السيبراني والعمل الدبلوماسي

01 مجموعة من الممارسات والتقنيات والإجراءات التي تهدف إلى حماية الأنظمة والشبكات والبرامج والبيانات من الهجمات الرقمية

02 في السياق الدبلوماسي، يتجاوز هذا المفهوم مجرد حماية الحواسيب؛ حيث إنه امتداد للأمن القومي في الفضاء الرقمي

03 كل معلومة يتمّ تبادلها، وكلّ جهاز يتم استخدامه، يُمثّل أصلًا وطنيًّا يجب حمايته

04 الهجمات السيبرانية على البعثات الدبلوماسية لا تهدف فقط لسرقة البيانات، بل للتأثير على مواقف الدول

أهداف الأمن السيبراني

السرية (Confidentiality)

حماية المراسلات السرية، وتقارير تقييم المواقف، ومسودات الاتفاقيات

01

السلامة (Integrity)

الحفاظ على دقّة واكتمال البيانات الدبلوماسية، ومَنْع تعديلها أو العبث بها

02

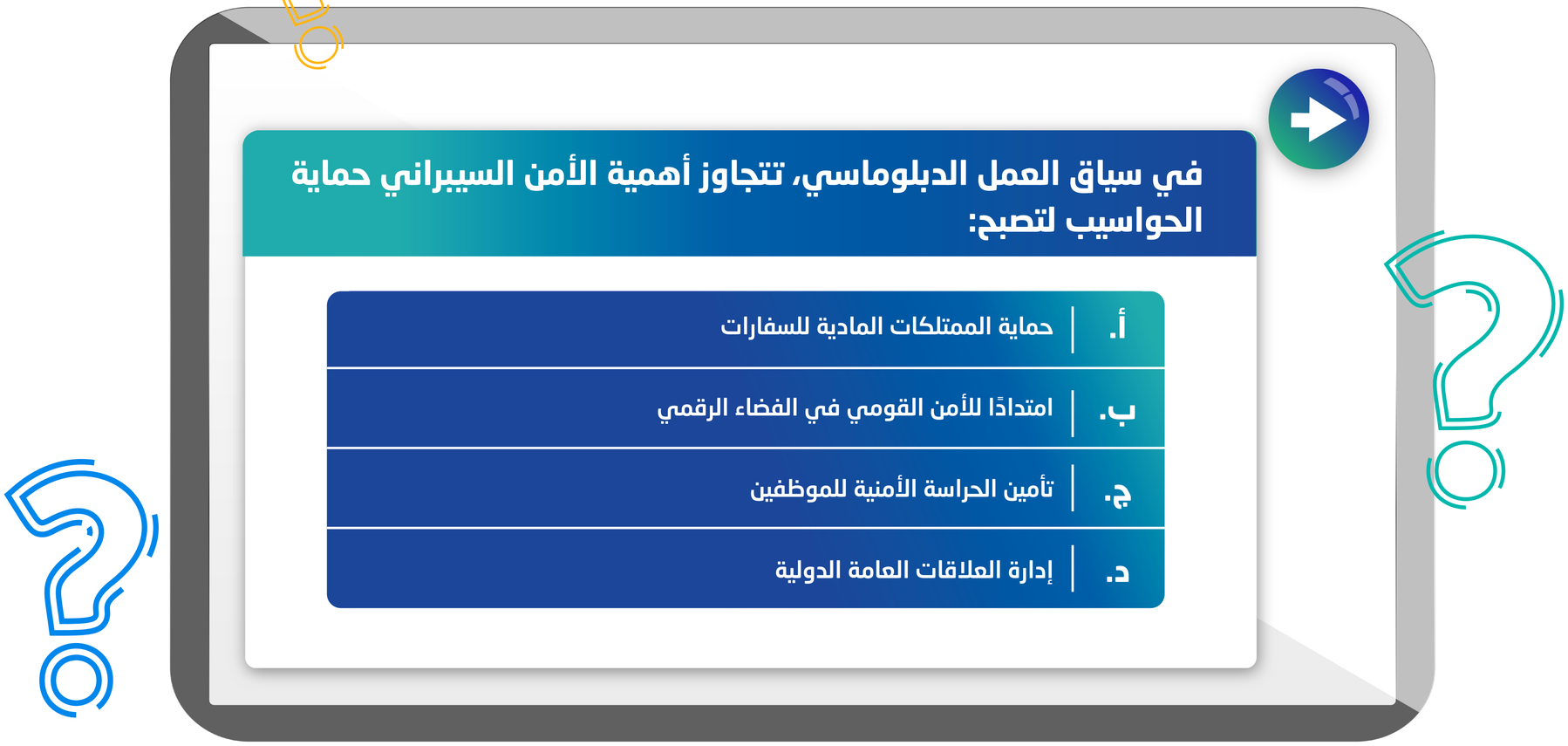
التوافر (Availability)

ضمان أن تظلّ الأنظمة والبيانات الدبلوماسية متاحة، ويمكن الوصول إليها عند الحاجة

03

هجوم حجب الخدمة (DDoS) الذي قد يستهدف المواقع الإلكترونية للسفارات قبل حدث دولي مُهِمّ هو مثال على استهداف "التوافر"؛ لإحداث ضرر سياسي وتشغيلي.

سؤال اختيار من متعدد



في سياق العمل الدبلوماسي، تتجاوز أهمية الأمن السيبراني حماية الحواسيب لتصبح:

أ. حماية الممتلكات المادية للسفارات

ب. امتدادًا للأمن القومي في الفضاء الرقمي

ج. تأمين الحراسة الأمنية للموظفين

د. إدارة العلاقات العامة الدولية

الإجابة الصحيحة: ب. امتدادًا للأمن القومي في الفضاء الرقمي

المحور الثالث

أمن الأجهزة والهواتف

الأجهزة الذكية في العمل الدبلوماسي

الهاتف أو الجهاز الذكي أداة أساسية للعمل الدبلوماسي تحمل بريدك الإلكتروني، جهات اتصالك، تطبيقات المراسلة، وربما نُسَخًا من مستندات حسّاسة. لذلك، هو هدف ثمين للمهاجمين.

الهجمات على الأجهزة الدبلوماسية

الهواتف الذكية أصبحت المكتب المحمول للدبلوماسي، وقد تكون بوّابة رئيسية للهجمات

تُستخدَم تطبيقات تجسُّس متطوّرة مثل Pegasus & Predator في اختراق هواتف مسؤولين ودبلوماسيين

مؤشرات اختراق الأجهزة

1 **استنزاف البطارية بشكلٍ سريع وغير معتاد**

البرمجيات الخبيثة التي تُسجّل الصوت أو تنقل البيانات، تعمل باستمرار في الخلفية

2 **ارتفاع حرارة الجهاز حتى عند الاستخدام البسيط**

المُعالِج يعمل بجُهْد إضافي لمعالجة الأوامر الخبيثة

3 **استهلاك بيانات الإنترنت بشكلٍ غير مُبرَّر**

برمجيات التجسُّس تُرسل البيانات المُجمَّعة (رسائل، صور، مواقع) إلى خوادم المهاجم

4 **تلقّي رسائل مشبوهة أو ظهور نوافذ منبثقة غريبة**

قد تكون هذه محاولات لخداعك لتثبيت المزيد من البرمجيات الضارَّة

5 **تغييرات غريبة في إعدادات الجهاز**

مثل تفعيل البلوتوث أو الـ GPS دون تدخُّل منك، مما قد يُستخدَم لتتبُّع موقعك

كيف يتم تتبُّع حركة الدبلوماسي؟

عبر تطبيقات عادية

مثل: الخرائط، الطقس، أو بعض الألعاب تجمع بيانات الموقع في الخلفية

بعض البرمجيات الخبيثة

تجمع بيانات الموقع كلّ بضع ثوانٍ، وتُرسلها لخوادم خارجية، ما يَسمح ببناء خريطة تحرُّكات الدبلوماسي

جهاز رسمي أم شخصي؟

الجهاز الرسمي

مُعدّ وَفْق معايير أمنية، مُرَاقَب، ومُزوَّد بتطبيقات حكومية مُشفَّرة

الجهاز الشخصي

أقل ضبطًا أمنيًّا، ملـيء بتطبيقـات غيـر موثوقـة، ولا يخضـع للفحص الدوري

لماذا يُعدّ الفصل بين الأجهزة ضروريًّا؟

لأن أيّ اختراق للجهاز الشخصي قد يُستغَلّ للوصول للهوية الرقمية للدبلوماسي أو مراسلاته الرسمية

خطوات عملية لتأمين الهاتف

تحديث نظام التشغيل والتطبيقات بانتظام

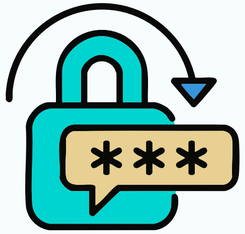
التحديثات خطّ الدفاع الأول لسدّ الثغرات الأمنية

تجنُّب شبكات Wi-Fi العامة

هذه الشبكات غالبًا ما تكون غير مشفَّرة، ممّا يسمح للمهاجمين على نفس الشبكة بالتنصّت على اتصالك

تفعيل المصادقة الثنائية (2FA)

بدلًا من الرسائل النصية (SMS) إن أمكن؛ فالرسائل يمكن اعتراضها



استخدام كلمات مرور قوية

مع تفعيل القفل التلقائي بعد فترة قصيرة من عدم الاستخدام

أدوات السلامة الرقمية للدبلوماسيين

لكي يضمن الدبلوماسي سلامته الرقمية، هناك أدوات يجب أن تكون جزءًا من تجهيزاته اليومية

01

استخدام VPN رسمي

لتأمين اتصال الإنترنت، وحماية البيانات في أثناء التصفُّح

02

بريد دبلوماسي آمن

لضمان الحفاظ على سرية الرسائل الإلكترونية

03

جهاز عمل منفصل

منعًا لانتقال أيّ تهديد من الأجهزة الشخصية إلى بيانات العمل الحساسة

04

قنوات اتصال مشفّرة

مثل المكالمات أو الرسائل المشفّرة لتأمين التواصل مع الأطراف الرسمية

أساليب الحماية المتقدّمة

1 تحديث نظام التشغيل والبرامج فور صدورها

الهجمات تستغل ثغرات أمنية يتم إصلاحها بسرعة من خلال التحديثات

2 إعادة تشغيل الجهاز يوميًّا

بعض برمجيات التجسُّس المُتقدّمة لا تكون دائمة (Non-persistent) وتتم إزالتها عند إعادة التشغيل، مما يجبر المهاجم على إعادة إصابة الجهاز

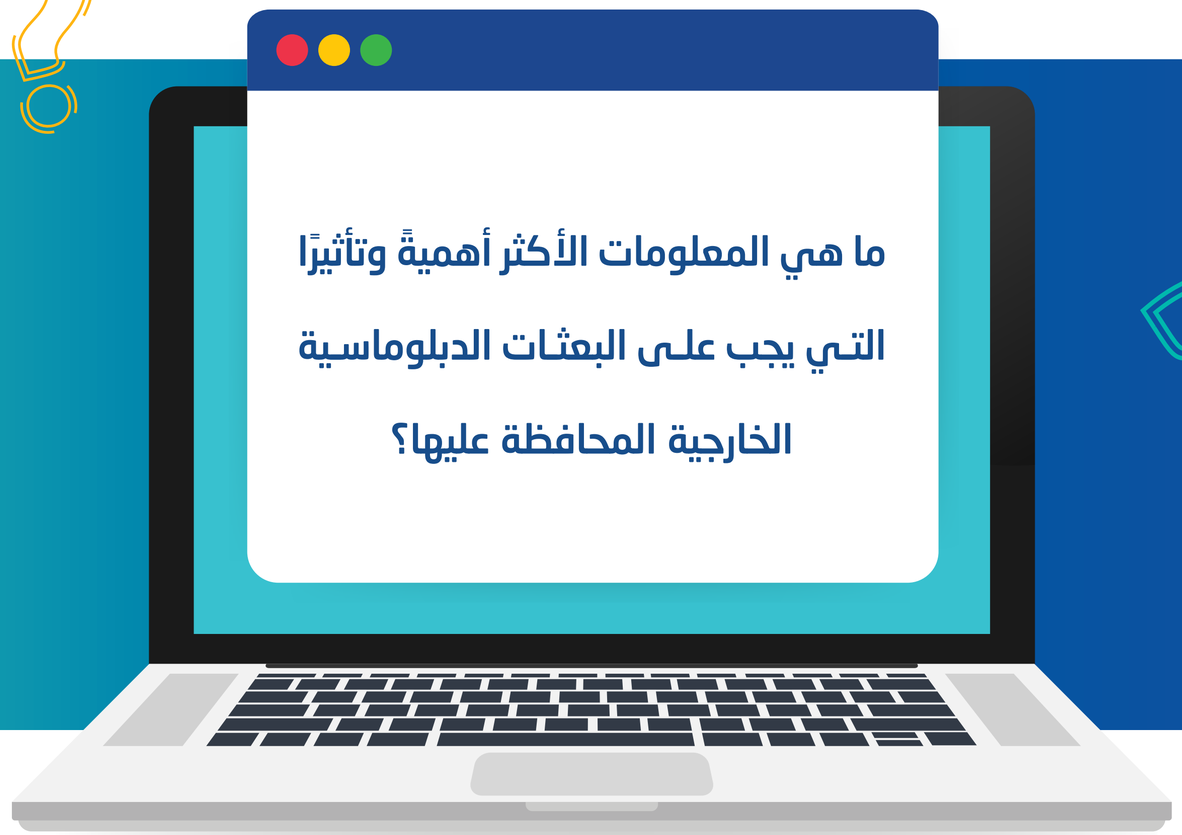
3 استخدام هواتف دبلوماسية مخصَّصة للعمل الرسمي فقط

هذا يُقلِّل من معدلات الهجوم الإلكتروني

4 تفعيل "وضع الإغلاق" (Lockdown Mode) في أجهزة أيفون

يُقيِّد هذا الوضع الميزات التي تستغلها برمجيات التجسُّس، مثل معاينة الروابط في الرسائل، وأنواع معينة من المرفقات

سؤال تفاعلي



ما هي المعلومات الأكثر أهميةً وتأثيرًا
التـي يجب علـى البعثـات الدبلوماسـية
الخارجية المحافظة عليها؟

المحور الرابع

التهديدات السيبرانية للدبلوماسيين

التهديدات السيبرانية للدبلوماسيين

يواجه الدبلوماسيون اليوم مجموعة من التهديدات الرقمية المتطورة، تَستهدفهم باعتبارهم مصادر معلومات حساسة وواجهات تُمثِّل دولهم.

من أبرزها

01 التصيد الموجّه (Spear Phishing)

رسائل مُصمَّمة بعناية لاستهداف شخصيات محددة داخل البعثات، وتحتوي على روابط أو مرفقات خبيثة

02 برمجيات التجسُّس على الأجهزة

تُستخدَم لاعتراض الاتصالات والتجسُّس على المراسلات والملفات الشخصية

03 انتحال الهويات عبر البريد الرسمي

انتحال عناوين بريد حكومية أو دبلوماسية؛ لتضليل الأطراف واستدراجهم

04 تسريب الوثائق الحساسة عبر الإنترنت

عبر اختراق خوادم أو حسابات شخصية تَفتقر لتأمين كافٍ

آليات الوقاية

01 التصيد الموجّه (Spear Phishing)

01 تدريب الموظفين على كشف الرسائل الاحتيالية

02 عدم فتح الروابط أو المرفقات مجهولة المصدر

03 استخدام فلاتر بريدية وأنظمة كشف التصيد

02 برمجيات التجسّس على الأجهزة

01 تحديث الأنظمة والتطبيقات باستمرار

02 استخدام برامج حماية موثوقة

03 فَصْل الأجهزة الرسمية عن الشخصية

آليات الوقاية

انتحال الهويات عبر البريد الرسمي

03

01 تفعيل المصادقة الثنائية

02 التحقُّق من عناوين المرسلين قبل الرد

03 تطبيق بروتوكولات البريد الآمِن

تسريب الوثائق الحساسة عبر الإنترنت

04

01 تشفير الملفات الحساسة قبل الإرسال

02 تحديد صلاحيات الوصول داخل الفريق

03 حِفْظ النُّسَخ الاحتياطية في بيئات آمِنَة ومراقَبة

البرمجيات الخبيثة (Malware)

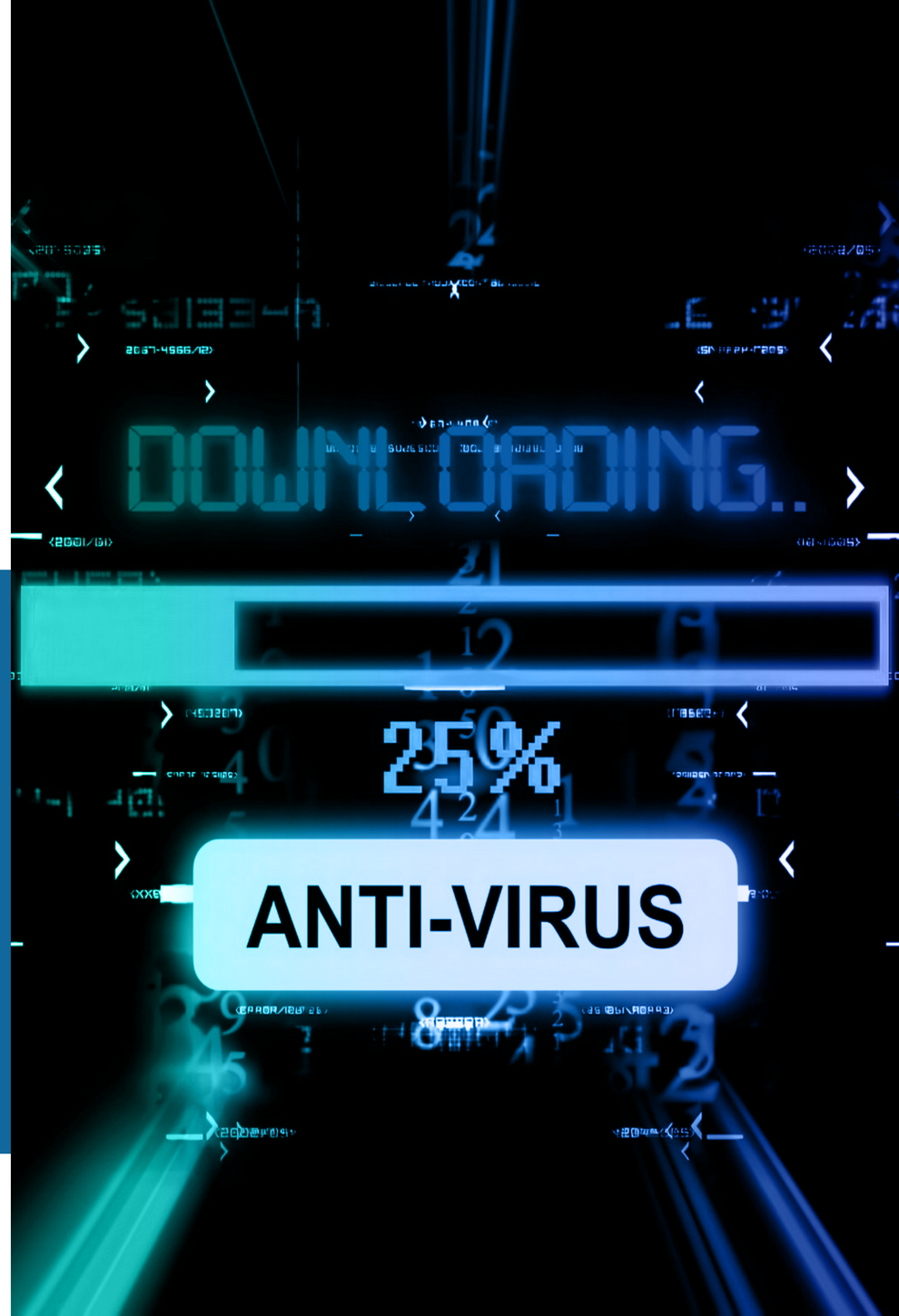
يقوم المهاجمون بإرسال البرمجيات الخبيثة إلى الأجهزة بهدف إلحاق الضرر، أو سرقة البيانات، أو التحكُّم في المحتويات.

السمات الرئيسية

- تنتقل عبر المرفقات أو الروابط المشبوهة
- قد تُخْفِي نفسها داخل برامج أو تطبيقات ظاهرها سليم
- تتنوّع بين فيروسات، ديدان، برمجيات فدية، أو برمجيات تجسُّس
- تؤدي إلى فقدان السيطرة على الأجهزة أو البيانات
- تُستخدَم أحيانًا للتجسُّس على عمل الصحفيين

طرق الوقاية

- تثبيت برامج مكافحة الفيروسات، وتحديثها بانتظام
- تجنُّب تحميل البرامج من مواقع غير موثوقة
- عدم الضغط على الروابط أو المرفقات مجهولة المصدر
- تشغيل جدار الحماية لصدّ الهجمات
- إجراء فَحْص دوري للجهاز؛ للتأكُّد من خلوّه من البرمجيات الضارَّة



الفيروسات

الفيروس هو برمجيَّة ضارَّة تَدخل إلى الجهاز وتُغيِّر طريقة عمله، أو تُتْلِف البيانات الموجودة عليه.

السمات الرئيسية

- يُرفَق غالبًا مع ملفات تبدو طبيعية؛ مثل الصور أو المستندات
- بعض الفيروسات تتسبَّب في حذف الملفات أو تعطيل النظام بالكامل
- يبدأ الفيروس بالانتشار عند فَتْح الملف أو تشغيله
- ينتقل من جهاز إلى آخر عبر الإنترنت أو وسائط مثل USB

طـــــرق الوقـــاية

- فحـص وسـائط التخزيـن (USB) قبـل تشـغيلها
- اسـتخدام برامـج مكافحـة الفيروسـات المُحدَّثـة باسـتمرار
- تحديـث أنظمـة التشـغيل والبرامـج لإغلاق الثـغرات الأمنيـة
- عدم فَتْح الملفات مجهولة المصدر

أحصنة طروادة (Trojans)

هي نوع من الفيروسات التي تُصيب الحواسيب وأجهزة الهواتف المحمولة، ويكون على شكل ملف يُرفِق نفسه مع أحد البرامج الموجودة على الإنترنت.

السمات الرئيسية

- تُقدَّم كأداة لتحرير الفيديو أو إدارة البريد
- تفتح بابًا خلفيًّا يُتيح للمهاجم التحكُّم بالجهاز
- قد تُستخدَم لسرقة كلمات مرور الحسابات

طرق الوقاية

- تحميل البرامج من المواقع الرسمية فقط
- مراقبة نشاط الجهاز والبرامج المثبّتة بانتظام
- استخدام برامج كشف التسلل ومكافحة الفيروسات
- عدم تثبيت أيّ برنامج غير معروف أو مشكوك فيه

برمجيات الفدية (Ransomware)

هي أحد أخطر أنواع الهجمات؛ حيث يتم تشفير الملفات ثم يُطلَب دَفْع مبلغ مالي لفَكّ التشفير.

السمات الرئيسية

- تُرسَل عادة عبر رسائل بريد إلكتروني تحتوي على مرفقات مزيَّفة
- المهاجم يطلب فدية غالبًا بعُمْلة رقمية مثل البيتكوين
- بعد الإصابة، تُغْلق الملفات أو النظام بالكامل
- حتى عند الدفع، لا يُوجَد ضمان لاسترجاع الملفات

طـــــرق الوقـــاية

- استخدام برامج أمنية متخصّصة في منع هجمات الفدية
- النّســـخ الاحتـــياطي المنتظِـــم للملفات المهمة Offline Backup
- تحديث النظام والتطبيقات باستمرار لسدّ الثغرات
- تجنُّب فتح المرفقات من مصادر مجهولة

حملات التضليل الدبلوماسي

أصبحت حملات التضليل الرقمي أحد أسلحة الحرب الهجينة الحديثة؛ حيث تُستخدم المعلومات المضللة للتأثير على سمعة الدول وسفرائها.

السمات الرئيسية

- تقوم جهات مُعادية بإنشاء مواقع أو حسابات مُزيَّفة تنشر روايات كاذبة عن نشاطات السفارات
- قد تُستخدَم صور قديمة أو مجتزأة لخلق انطباعات خاطئة عن المواقف الدبلوماسية
- الرد المتسرع أو غير المنسَّق قد يُضخِّم الضرر بدلًا من احتوائه

طرق الوقاية

01 التحقّق الدقيق من مصدر المعلومة قبل الرد

02 التنسيق مع الجهات الإعلامية المختصة في الدولة الأم قبل إصدار أيّ بيان

03 مراقبة الفضاء الرقمي بانتظام لرصد حملات التضليل في مراحلها الأولى

نصائح الحماية السيبرانية

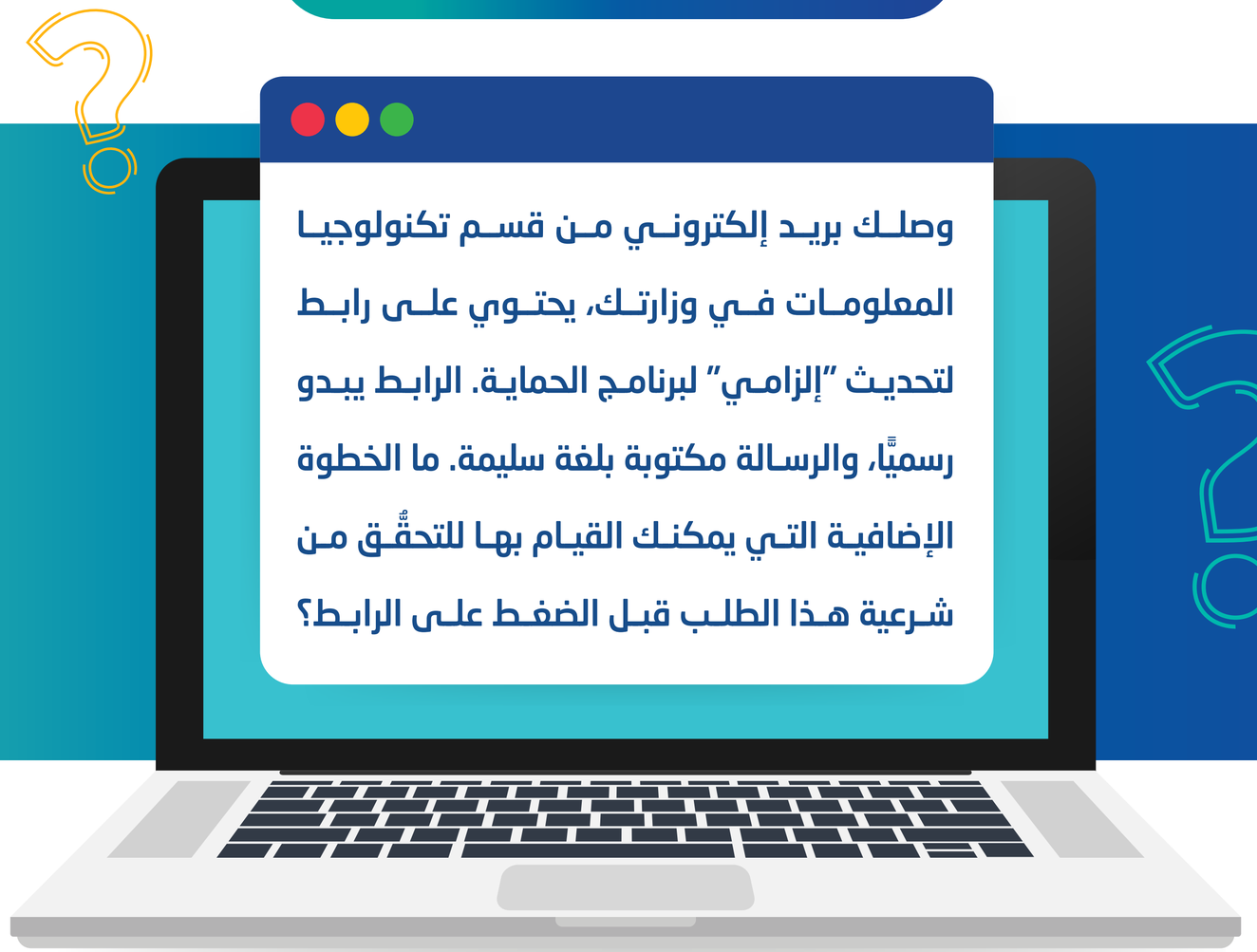
01 عدم فتح الروابط أو المرفقات مجهولة المصدر

02 تجنُّب استخدام شبكات (Wi-Fi) العامة للقيام بالأعمال الرسمية

03 عدم مشاركة كلمات المرور أو رموز الدخول حتى مع الزملاء

04 الامتناع عن استخدام الأجهزة الشخصية في نَقْل أو تخزين الملفات الرسمية

سؤال تفاعلي



وصلك بريد إلكتروني من قسم تكنولوجيا المعلومات في وزارتك، يحتوي على رابط لتحديث "إلزامي" لبرنامج الحماية. الرابط يبدو رسميًّا، والرسالة مكتوبة بلغة سليمة. ما الخطوة الإضافية التي يمكنك القيام بها للتحقُّق من شرعية هذا الطلب قبل الضغط على الرابط؟

المحور الخامس

حماية المستندات والبيانات الدبلوماسية

المستندات الدبلوماسية

تُعدّ الركيزة الأساسية للدبلوماسيين، وأيّ تسريب لها قد يَضُرّ بالدولة ويُؤثّر على سُمعتها وعلاقاتها الخارجية.

تصنيف المستندات الدبلوماسية

01

شديدة السرية (Top Secret)

معلومات حساسة قد تُؤثّر على الأمن القومي أو العلاقات الدولية إذا سُرِّبت

02

حسّاسة (Confidential)

بيانات مهمة، لكنّ تسريبها لا يُهدِّد الأمن القومي بشكلٍ مباشر

03

عامة (Public)

معلومات يمكن نَشْرها للجمهور العام دون أيّ خطر

أخطاء شائعة عند تخزين المستندات

- حفظ جميع المستندات على جهاز واحد غير مُشفّر
- استخدام أقراص USB شخصية أو غير مُراقَبة
- إرسال الملفات عبر البريد الشخصي أو تطبيقات غير رسمية
- عدم عمل نُسَخ احتياطية مُشفّرة للملفات المهمة

أنواع تخزين المستندات

01

التخزين المحلي

يتسم بالتحكُّم الكامل بالملفات، وسرعة الوصول إليها. وفقدان الجهاز قد يُؤدّي لفقدان البيانات، وهذا التخزين يتّصف بصعوبة مشاركة الملفات بأمان.

02

التخزين السحابي الخارجي

يتّسم بسهولة الوصول والمشاركة، خطر تسرُّب البيانات، الاعتماد على طرف ثالث

03

التخزين السحابي الحكومي الرسمي

يوفّر درجة أمان أعلى، متوافق مع سياسات الدولة، محدودية الوصول خارج الشبكة الحكومية، لكنه قد يكون أبطأ

حماية المستندات الدبلوماسية

تشفير الملفات الحساسة

باستخدام معايير حكومية قوية، مثل (AES-256)

استخدام حلول إدارة الحقوق الرقمية (DRM)

لمنع الطباعة أو المشاركة أو النَّسْخ غير المصرَّح به

تحديد صلاحيات الوصول (Access Control)

على أساس مبدأ "الحاجة للمعرفة" (Need-to-Know)، وليس الثقة الشخصية

تتبُّع كلّ عملية فتح أو تعديل عبر سجِلّ تدقيق (Audit Log) لمعرفة مَن وصل إلى المستند، ومتى، ولماذا؟

تخزين النُّسَخ الاحتياطية في بيئات مُغلَقة وآمِنَة (Intranet) أو سحابة حكومية مؤمنة.

حماية وحدات التخزين الخارجية

الأقراص الصلبة ووحدات USB أدوات أساسية لنقل الملفات؛ لكنّها مُعرَّضة للاختراق أو الضياع أو الحقن ببرمجيات خبيثة

ممارسات التخزين الآمنة

تشفير الأقراص الصلبة ووحدات التخزين

باستخدام أدوات مثل BitLocker أو FileVault لحماية البيانات في حال فقدانها

عدم توصيل أيّ وحدة تخزين

مجهولة المصدر بجهازك

استخدام وحدات تخزين مزودة بحماية ضد الكتابة (Write Protected)

عند استخدامها على أجهزة غير موثوقة

فحص أي وحدة تخزين ببرنامج مكافحة فيروسات

قبل فتح أي ملف منها.

نموذج إدارة المستندات الدبلوماسية (DMS)

نظام إدارة المستندات يساعد على

- تصنيف الملفات تلقائيًّا بحسب درجة السرية
- تتبُّع مَن فتَح أيّ مستند أو عدَّل فيه
- إنشاء نُسَخ احتياطية مُشفَّرة بشكلٍ دوريّ

سؤال اختيار من متعدد

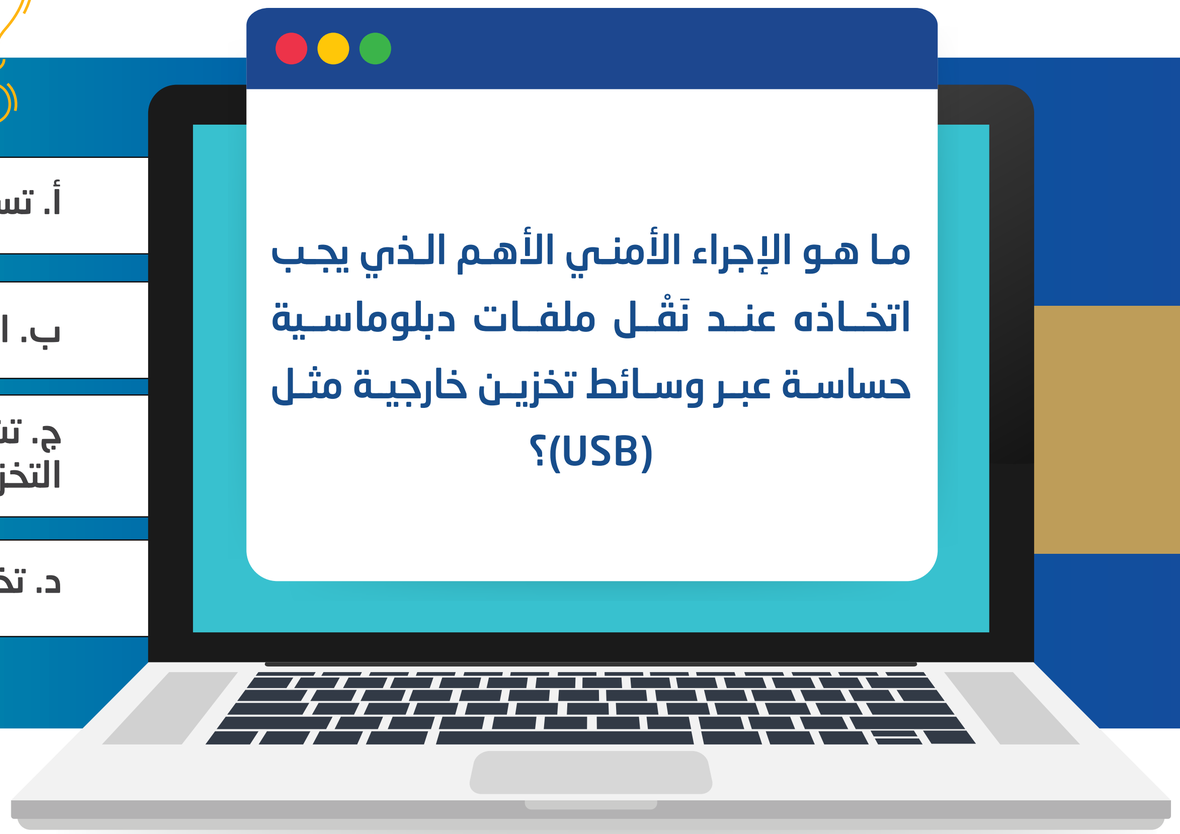
ما هو الإجراء الأمني الأهم الذي يجب اتخاذه عند نَقْل ملفات دبلوماسية حساسة عبر وسائط تخزين خارجية مثل (USB)؟

أ. تسمية الملفات بأسماء غير واضحة

ب. استخدام وسائط تخزين جديدة في كل مرة

ج. تشفير الملفات قبل نَقْلها، وفحص وسيط التخزين ببرنامج مكافحة الفيروسات

د. تخزينها في مكان آمِن في المنزل



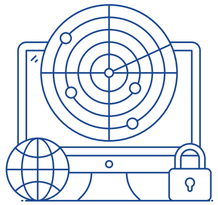
الإجابة الصحيحة: ج. تشفير الملفات قبل نقلها وفحص وسيط التخزين ببرنامج مكافحة الفيروسات

المحور السادس

البريد الإلكتروني الدبلوماسي

كيف يتم اختراق البريد الإلكتروني لدبلوماسي؟

يُستهدف الدبلوماسي غالبًا عبر رسائل تبدو رسمية، لكنّها تحمل روابط خبيثة أو ملفات ملوّثة



الهجمات تكون مُوجَّهة بدقة؛ لأنها تَستهدف الوصول إلى مراسلات حسَّاسة أو حسابات حكومية

من علامات الرسائل المُزيَّفة

روابط مختصرة أو غريبة

أخطاء لغوية، أو صياغة غير مألوفة

طلب عاجل دون مُبرّر

طلب تغيير كلمة مرور أو تحديث بيانات مفاجئ

آليات الوقاية

- التحقُّق من هوية المرسل عبر قناة رسمية
- تمرير الرابط أو الرسالة للخبير التقني في البعثة قبل فتحها
- عدم الضغط على الروابط من الهاتف خصوصًا في أثناء السفر
- التبليغ عن أيّ رسالة مشبوهة فورًا

سيناريو تدريبي

في أثناء وجودك في دولة مضيفة، تصلك رسالة على بريدك الدبلوماسي بعنوان:

"تنبيه عاجل: سيتم إيقاف حسابكم خلال ساعات؛ ما لم يتم تحديث البيانات".

الرسالة تبدو شبه رسمية؛ شعار صحيح، توقيع معروف، وصياغة قريبة من اللغة الرسمية.

لكن عند تمرير المؤشر على الرابط يظهر أنه ليس من نطاق حكومي، وفي النص خطأ لغوي صغير مع لهجة استعجال غير مألوفة.

والسؤال: كيف تتصرّف؟

1. **لا تفتح الرابط**
2. **تُرسل لقسم الـ IT لقطة شاشة فقط**
3. **تتواصل مع الوزارة عبر القناة الرسمية المشفّرة للتأكد**

سؤال تفاعلي

تلقيت رسالة بريد إلكتروني من "قسم تكنولوجيا المعلومات" في الوزارة تطلب منك الضغط على رابط "إلزامي" لتحديث نظام الحماية. الرابط يبدو رسميًّا، لكنّ الرسالة تحتوي على خطأ إملائي بسيط.

ما الإجراء الأفضل الذي يجب عليك اتخاذه قبل الضغط على الرابط؟

المحور السابع

السلامة الرقمية في أثناء السفر الدبلوماسي

السلامة الرقمية في أثناء السفر

العمل الدبلوماسي قد يَضعك في بيئات قد تكون مُعادية سيبرانيًّا

المطارات، الفنادق، وحتى شبكات الاتصالات المحلية قد تكون تحت المُراقَبة

أخطر 5 بيئات رقمية في أثناء السفر

المطارات

شبكات Wi-Fi العامة، أجهزة فَحْص غير موثوقة، وازدحام رقمي يُسهّل التعقُّب

الفنادق

شبكات Wi-Fi المشتركة، أجهزة الحاسوب العامة في اللوبي

المقاهي

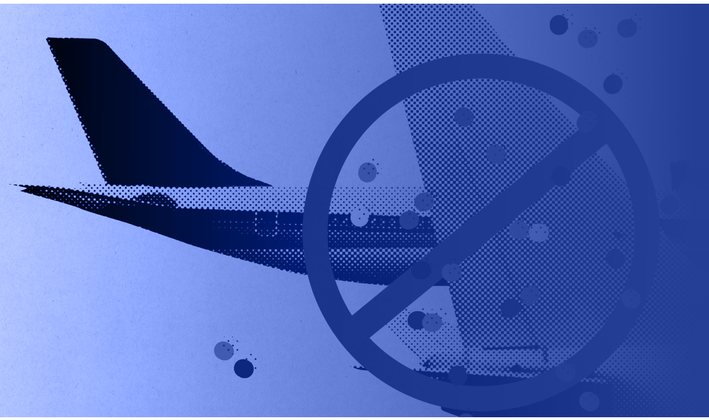
شبكات Wi-Fi غير مُؤمَّنة، وسهولة مراقبة حركة البيانات

المؤتمرات والفعاليات

شبكات ضيوف مفتوحة، وأجهزة تسجيل مجهولة

شبكات الدولة المضيفة

قد تكون مُراقَبة أو خاضعة لقوانين تسمح بالاطلاع على البيانات



أخطاء شائعة في أثناء السفر

1. التصوير السريع للوثائق، أو تصوير شاشة الهاتف أو الحاسوب في المطارات أو الفنادق

2. استخدام أجهزة USB شخصية لشَحْن أو نقل الملفات

3. الاتصال بشبكات Wi-Fi عامة أو غير موثوقة

إجراءات وقائية قبل السفر

استخدام أجهزة بديلة (Burner Devices)

هواتف وحواسيب محمولة آمِنَة لا تحتوي إلا على الحد الأدنى من المعلومات المهمة، مع تجنُّب تسجيل الدخول إلى حساباتك الشخصية من هذه الأجهزة

إعداد نُسَخ احتياطية مشفَّرة للبيانات

وتخزينها في مكان آمِن في بلدك، وليس معك

إبلاغ قسم أمن المعلومات بوِجْهتك

لتتم مراقبة حساباتك بحثًا عن أيّ نشاط دخول مشبوه

National Cyber Security Agency

خطة سفر آمِنَة للدبلوماسيين

01 جهاز سفر منفصل

استخدام جهاز مُخصَّص للسفر يحتوي فقط على الملفات الضرورية

02 عدم استخدام USB خارجي

لتفادي نقل البرمجيات الخبيثة أو سرقة البيانات

03 تعطيل Wi-Fi التلقائي

منع الاتصال التلقائي بأيّ شبكة غير موثوقة

04 عدم شحن الأجهزة في USB علني (Juice Jacking)

استخدام شواحن رسمية أو مأخذ كهرباء مباشر لتجنُّب سرقة البيانات عبر منافذ USB

إدارة البيانات بعد العودة من السفر

- عدم توصيل أجهزة السفر بالشبكة الداخلية مباشرة؛ يجب أن يتم فَحْصها مِن قِبَل الفريق التقني أولًا
- حذف البيانات بالكامل (Wipe) من الأجهزة المستعمَلة في أثناء السفر
- تغيير جميع كلمات المرور التي استخدمتها خلال السفر

سؤال تفاعلي

في أثناء انتظارك في صالة مطار دولي، كانت بطارية هاتفك الرسمي على وشك النفاد. وجدت منفذ شحن USB عامًّا متاحًا بجانب مقعدك. هل تستخدمه لشحن هاتفك؟ وما هو البديل الأكثر أمانًا في هذا الموقف؟

المحور الثامن

الدبلوماسية السيبرانية

الدبلوماسية السيبرانية

الأمـن السيبرانـي فـي العمـل الدبلوماسـي يهـدف إلـى إدارة العلاقـات الدوليـة فـي الفضاء السيبرانـي، وتعزيـز التعـاون بيـن الـدول فـي مجـالات الأمـن السيبرانـي، والحوكمة الرقميـة، وحمايـة البيانـات.

أهمية الدبلوماسية السيبرانية

- تمثيل مصالح الدولة في القضايا الرقمية الدولية
- تعزيز التعاون في مكافحة الجرائم السيبرانية
- دعم المفاوضات المتعلّقة بالفضاء السيبراني وحماية البيانات
- الإسهام في بناء صورة رقمية إيجابية للدولة في المحافل الدولية
- حماية البعثات الدبلوماسية من الهجمات السيبرانية الموجَّهة

أهداف الدبلوماسية السيبرانية

01	تعزيز التعاون الدولي في مواجهة التهديدات السيبرانية العابرة للحدود
02	دَعْم التشريعات والمعايير الدولية لحماية البيانات والخصوصية
03	تعزيز الثقة الرقمية بين الدول والمؤسسات
04	الدفاع عن المصالح الوطنية السيبرانية في المحافل الدولية
05	بناء شراكات تقنية وإستراتيجية في مجالات الذكاء الاصطناعي والأمن السيبراني

السلامة الرقمية في العمل الدبلوماسي

المخاطر الرقمية في بيئة العمل الدبلوماسي

- استهداف البريد الإلكتروني الدبلوماسي
- حملات تضليل وتشويه السُّمعة عبر الإنترنت
- مراقبة الهواتف والأجهزة المحمولة
- تسريب وثائق المفاوضات أو البيانات السرية

أفضل الممارسات العملية

- استخدام أجهزة وشبكات آمِنَة تابعة للبعثة فقط
- تفعيل المصادقة الثنائية لجميع الحسابات
- الامتناع عن استخدام التطبيقات العامة في التواصل الرسمي
- عدم مناقشة القضايا الحساسة على المنصات الاجتماعية
- فَحْص دوري للأجهزة بواسطة مختصين في الأمن السيبراني


ماذا يعني مصطلح "الدفاع السيبراني النشط" (Active Cyber Defense)؟
سؤال تفاعلي

المحور التاسع

إدارة الحادث السيبراني الدبلوماسي

الحادث السيبراني

هو أيّ نشاط رقمي غير مألوف يُعرِّض سرّية أو سلامة أو توافر المعلومات للخطر داخل الأنظمة الدبلوماسية أو البعثات الخارجية.

يشمل ذلك

- اختراق البريد الإلكتروني الرسمي وسرقة المراسلات
- تعطيل مواقع السفارات أو بوابات التأشيرات الإلكترونية
- تسريب وثائق أو بيانات سرية
- استخدام برمجيات تجسُّس لاستهداف هواتف أو حواسيب الدبلوماسيين

إدارة الحوادث السيبرانية

01 الإدارة الفعّالة للحوادث تمنع تسريب المعلومات الحساسة أو استغلالها مِن قِبَل أطراف معادية

02 تُظهر الاستجابة السريعة والمنظَّمة صورة إيجابية عن كفاءة البعثة واحترافيتها أمام الدول المضيفة والمنظمات الدولية

03 الشفافية المقنَّنة في التعامل مع الحوادث جزء من الدبلوماسية الحديثة؛ إذ تمنع انتشار الشائعات وتَحُدّ من الضرر الإعلامي

مراحل إدارة الحادث السيبراني

01 التحضير ووضع السياسات

إعداد خطط استجابة واضحة، وتدريب الموظفين، وتحديد نقاط الاتصال المعتمدة في كلّ بعثة

02 الاكتشاف والتحليل

استخدام أنظمة مراقبة لاكتشاف الأنشطة المشبوهة، وتحليل نوع التهديد، ومصدره المحتمل

03 الاحتواء

عَزل الأنظمة المصابة لمنع انتشار الهجوم إلى بقية الشبكة الدبلوماسية

04 الاستئصال

إزالة البرمجيات الخبيثة، واستعادة السيطرة الكاملة على الأنظمة المتضررة

05 التعافي

استعادة الخدمات الحيوية، وتشغيل الأنظمة بعد التأكُّد من سلامتها الرقمية

06 المراجعة واستخلاص الدروس

تحليل جذور المشكلة، وتحديث السياسات الأمنية لتفادي الحوادث المستقبلية

أخطاء يجب تجنُّبها في أثناء إدارة الحادث

1

حذف الأدلة الرقمية
قبل تحليل الحادث

2

محاولة إصلاح الأجهزة المُختَرَقة دون
إشراف تقني من خبير

3

عدم الإبلاغ المُبكّر عن الحادث للجهات
المعنية

دور الدبلوماسي في أثناء الحادث

01

الإبلاغ الفوري عن أيّ سلوك غير طبيعي عبر القنوات الرسمية؛ مثل: رسائل غريبة، أو بطء مفاجئ في الأنظمة

02

عدم حذف الملفات أو الرسائل المشبوهة؛ لأنها قد تُشكّل دليلًا رَقميًّا مهمًّا في التحقيق

03

عدم التعامل مع الملفات أو الرسائل المشبوهة، وتركها للمختصين

04

استخدام القنوات الرسمية للتبليغ (مكتب أمن المعلومات في الوزارة أو السفارة)

05

الامتناع عن التحدُّث للإعلام أو الأطراف الخارجية بشأن الحادث قبل صدور تعليمات رسمية

06

المشاركة في إجراءات الطوارئ عند الحاجة؛ مثل: فَصْل الأجهزة، أو تغيير كلمات المرور

عناصر أمنية يجب توافرها في البعثات الدبلوماسية

خطـة اسـتجابة واضحـة للحـوادث السيبرانيـة

سِجِلّ لحوادث سيبرانية سابقة

مسـؤول اتصـال مباشـر مـع الوحـدة السيبرانيـة الوطنيـة التابعـة للدولـة

حفظ الأدلة الرقمية

حفظ الأدلة عنصر أساسي في أيّ تحقيق سيبراني دبلوماسي.

الخطوات الأساسية

- توثيق وقت الحادث، ومكانه، وطبيعته بدقة
- عدم استخدام الأنظمة المصابة حتى يتم تحليلها مِن قِبَل الخبراء
- الاحتفاظ بنُسَخ من السجلات (Logs) وبيانات الشبكة قبل إجراء أيّ تعديل
- التعاون مع فريق التحليل الجنائي الرقمي المحلي أو الدولي لتحديد مصدر الهجوم

آليات للوقاية من تكرار الحوادث السيبرانية

01 تحديث الأنظمة والبرامج باستمرار لتجنُّب الثغرات

02 تطبيق مبدأ "أقل صلاحية": بحيث لا يمتلك أيّ موظف أكثر مما يحتاج من صلاحيات

03 إجراء اختبارات اختراق داخلية كلّ ثلاثة أشهر لتقييم جاهزية الأنظمة

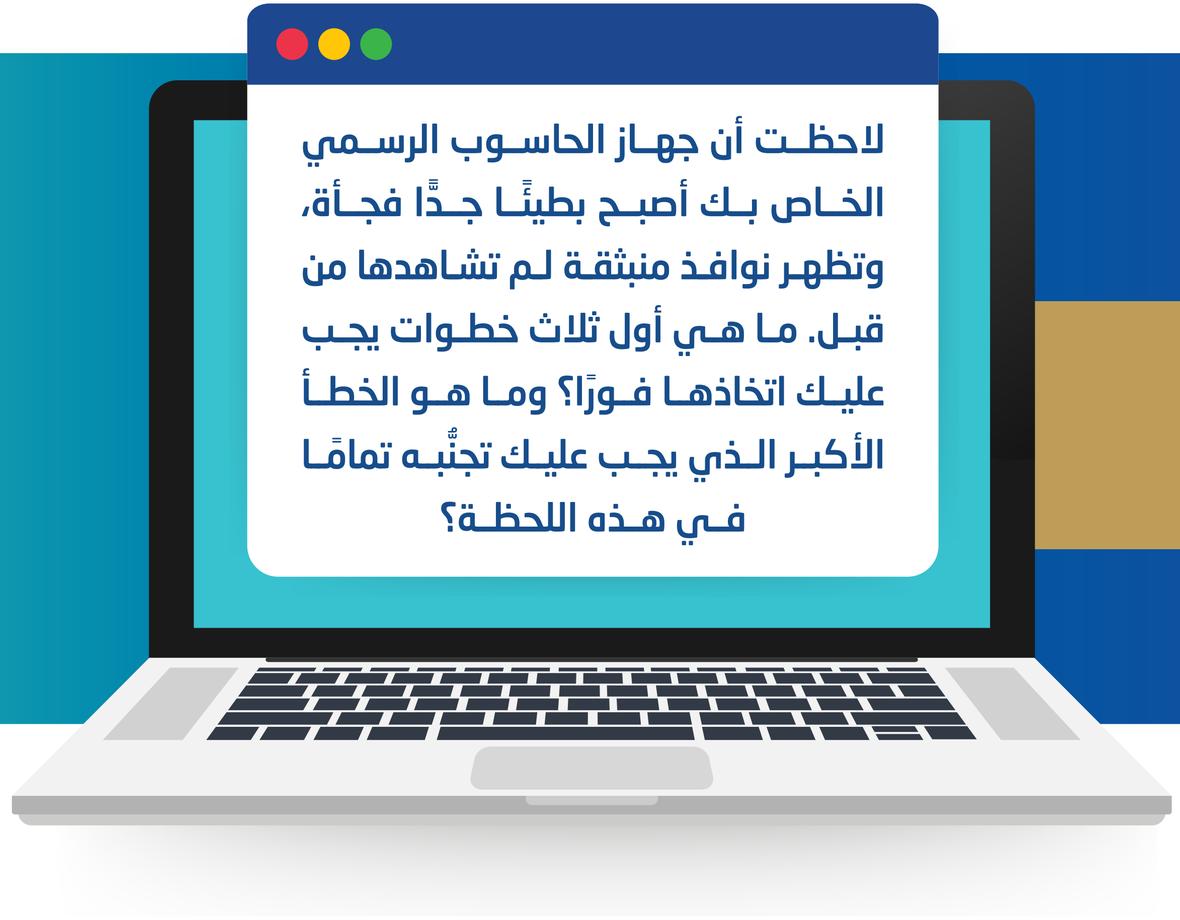
04 تنظيم تدريبات محاكاة للحوادث داخل البعثات والسفارات

05 تبادل الخبرات بين السفارات في مجال الأمن الرقمي

ميثاق السلامة الرقمية للدبلوماسي

الالتزام بالحفاظ على سرية المعلومات، استخدام القنوات الرسمية، التحقق قبل الضغط على أي رابط، والإبلاغ الفوري عن أي حادث سيبراني.

سؤال تفاعلي



لاحظت أن جهاز الحاسوب الرسمي الخاص بك أصبح بطيئًا جدًّا فجأة، وتظهر نوافذ منبثقة لم تشاهدها من قبل. ما هي أول ثلاث خطوات يجب عليك اتخاذها فورًا؟ وما هو الخطأ الأكبر الذي يجب عليك تجنُّبه تمامًا في هذه اللحظة؟

المحور العاشر

التفاوض في الفضاء السيبراني

التفاوض الدبلوماسي الرقمي

في ظل التحوُّل الرقمي، أصبحت المفاوضات بين الدول والمنظمات تُدار عبر منصات افتراضية، واجتماعات عبر الفيديو، وتبادل مستندات عبر البريد الإلكتروني المشفَّر.

هذا التحوُّل، رغم ما يُقدِّمه من سرعة ومرونة، يجعل السرية هدفًا أصعب من أيّ وقت مضى.

أهمـية المحـافـظة على الســـرية

التهديدات لم تَعُد تأتي من أطراف التفاوض فقط، بل من جهات استخباراتية أو مجموعات مخترقين

ضعف تأمين قناة واحدة قد يُتيح تسريب اتفاقيات أو تعطيل جلسات حساسة

مخاطر التفاوض الإلكتروني

التحوُّل إلى المفاوضات الرقمية يُرافقه مزيج من التهديدات التقنية والاستخباراتية، ومن أبرزها:

01

التنصت على الاجتماعات الافتراضية

يمكن للمهاجمين اعتراض الصوت أو الفيديو في حال استخدام منصات غير مُؤمَّنَة

02

تزوير الهويات في الاتصالات الرقمية

مثل انتحال شخصية مسؤول أو مستشار لإرسال توجيهات مُضلّلة

03

اختراق البريد الدبلوماسي وسرقة وثائق المفاوضات

الهدف عادة هو الحصول على بيانات داخلية سرية

04

استخدام الروابط والمرفقات الخبيثة

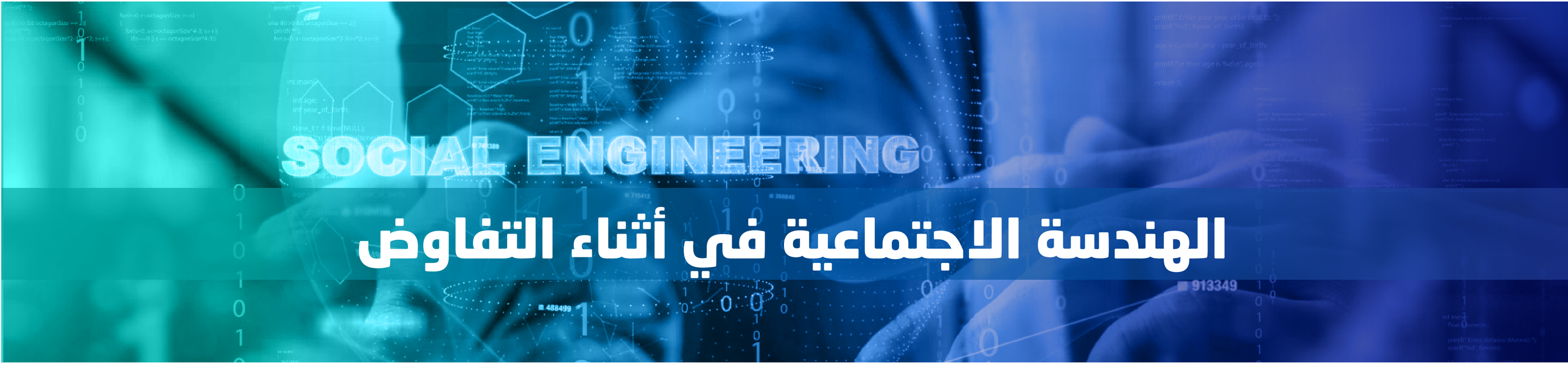
خلال مراحل التفاوض؛ لجمع معلومات عن مواقف الطرف الآخر

حماية قنوات الاتصال

الحماية تبدأ من اختيار القناة الآمِنَة، وتنتهي بالالتزام بالبروتوكولات الدبلوماسية الرقمية.

من وسائل حماية قنــوات الاتصال

- استخدام أنظمة تشفير شامل (End-to-End Encryption) لجميع الرسائل والمكالمات
- تجنُّب استخدام تطبيقات عامة أو مجانية لا تخضع لرقابة الوزارة أو السفارة
- إنشاء قنوات اتصال مُؤقَّتة وخاصة لكل جولة تفاوضية، يتم إغلاقها بعد انتهاء المفاوضات
- تحديد صلاحيات الدخول للأعضاء الأساسيين فقط
- مراقبة الدخول غير المعتاد إلى القنوات أو مستندات التفاوض



الهندسة الاجتماعية في أثناء التفاوض

الهندسة الاجتماعية هي أقوى سلاح استخباراتي رقمي؛ حيث يسعى المهاجم إلى خداع الأفراد بدلًا من الأنظمة.

في بيئة التفاوض، قد يحاول المهاجم

- انتحال صفة دبلوماسي أو خبير تقني لطلب مستندات حساسة
- إرسال رابط باسم "مستند تفاوض جديد"، يحمل برمجية تجسُّس
- جَمْع معلومات عن مواقف الطرف الآخر من خلال محادثات جانبية

طرق الحماية

- التحقُّق المزدوج من هوية كلّ طرف في المحادثات الرقمية
- عدم إرسال ملفات تفاوضية دون تشفير رسمي أو توقيع إلكتروني مُعتمَد
- الحذر من المرفقات غير المتوقَّعة أو الروابط المجهولة

التزييف العميق في المجال الدبلوماسي

تقنية Deep fake أصبحت خطرًا حقيقيًّا في العلاقات الدولية.

حيث يمكن من خلالها

- إنشاء فيديو مُزيّف لمسؤول يقول تصريحات لم يُدْلِ بها
- تحريف صوت أو صورة لإرباك مفاوضات حساسة أو إفساد علاقات ثنائية
- نشر مقاطع مُزيَّفة قبيل اجتماعات دولية للتأثير في الرأي العام أو وفود المفاوضين

طرق الحماية

- التحقُّق من مصدر أيّ محتوى قبل التفاعل معه أو نشره
- استخدام أدوات كشف التزييف العميق (Deep fake Detection Tools)
- اعتماد سياسات إعلامية واضحة للتعامل مع التسريبات الرقمية

حماية الهوية الرقمية للدبلوماسي

يتم تحليل بَصْمتك الرقمية (منشوراتك على وسائل التواصل الاجتماعي، اهتماماتك، علاقاتك)؛ لاستخدامها في أغراض غير مشروعة.

أيّ معلومة شخصية تشاركها عبر الإنترنت يمكن أن تُستخدَم في هجوم تصيُّد مُوجَّه شديد الإقناع.

المخاطر: يمكن استخدام معلوماتك الشخصية لانتحال هويتك وخداع زملائك، أو لابتزازك

قواعد الأثر الرقمي المنضبط

1. نشر رقمي محدود وهادف
2. عدم كشف تفاصيل السفر أو الاجتماعات عبر المنصات الاجتماعية
3. مُراجعة إعدادات الخصوصية باستمرار
4. عدم التفاعل مع حسابات مجهولة

المراجع

1. CISA – Cybersecurity & Infrastructure Security Agency. Incident Response Playbook (Federal)., on site: https://www.cisa.gov/incident-response-playbook.
2. Cybersecurity Best Practices, CISA, on site: https://www.cisa.gov/topics/cybersecurity-best-practices.
3. Cyberattacks, IBM, on site: https://www.ibm.com/think/topics/cyber-attack#498277090.
4. . Diplomacy in Cyberspace, American Foreign Service Association, on site: https://afsa.org/diplomacy-cyberspace?utm_source=chatgpt.com.
5. Digital Rights Management (DRM), FORTINET, on site: https://www.fortinet.com/resources/cyberglossary/digital-rights-management-drm.
6. ENISA – European Union Agency for Cybersecurity. Cybersecurity for Public Sector & Government Entities., on site: https://www.enisa.europa.eu/topics/csirt-cert-services.
7. How to Protect the Data that is Stored on Your Devices, CISA, on site: https://www.cisa.gov/resources-tools/training/how-protect-data-stored-your-devices.
8. INTERPOL. Social Engineering & Spear Phishing Threats., on site: https://www.interpol.int/Crimes/Cybercrime
9. Kaspersky Securelist. Red October – malware campaign targeting government missions and research organizations to extract sensitive information., on site: https://securelist.com/red-october-diplomatic-cyber-attacks-investigation/36740/?utm_source=chatgpt.com.
10. Ministry of Foreign Affairs – Czech Republic. APT31 (China) targeting the Czech Ministry of Foreign Affairs., on site: https://mzv.gov.cz/jnp/en/issues_and_press/press_releases/statement_by_the_government_of_the_czech.mobi?utm_source=chatgpt.com.
11. Multifactor Authentication, CISA, on site: https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication.
12. NATO CCDCOE – Cooperative Cyber Defence Centre of Excellence. Threats to Government and Diplomatic Communications., on site: https://ccdcoe.org/library/
13. NCSC – UK National Cyber Security Centre. Cyber Security Guidance for Diplomatic Missions., on site: https://www.ncsc.gov.uk/guidance.

المراجع

14. Reuters. Russian FSB targeting embassies in Moscow – cyberattacks on foreign embassies to intercept communications and spy on diplomatic missions., on site: https://www.reuters.com/business/aerospace-defense/russias-fsb-targets-foreign-embassies-moscow-cyber-espionage-campaign-microsoft-2025-07-31/?utm_source=chatgpt.com
15. Reuters. Operation Newscaster (Iran) – Iranian hackers used fake accounts and a fake news website to target diplomats., on site: https://www.reuters.com/article/us-iran-hackers/iranian-hackers-use-fake-facebook-accounts-to-spy-on-u-s-others-idUSKBN0E90A220140529?utm_source=chatgpt.com.
16. . Spoofing and Phishing, FBI, on site: https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/spoofing-and-phishing.
17. US Department of State – Bureau of Diplomatic Security. Cybersecurity Guidelines., on site: https://www.state.gov/bureau-of-diplomatic-security.
18. Viruses vs. Ransomware & Malware: Types and Explanation, CISCO, on site: https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-virus-vs-ransomware-malware.html.
19. What is 'Juice Jacking' and Tips to Avoid It, Federal Communications Commission, on site: https://www.fcc.gov/juice-jacking-tips-to-avoid-it.
20. . What is incident response? IBM, on site: https://www.ibm.com/think/topics/incident-response.
21. What is spear phishing? IBM, on site: https://www.ibm.com/think/topics/spear-phishing

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