مبادئ عامة في السلامة الرقمية

السلامة الرقمية في العمل الدبلوماسي

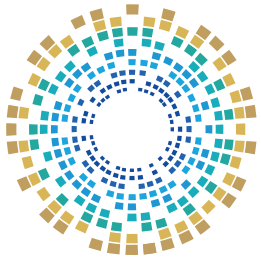
الشريحة المستهدفة
الدبلوماسيون

كُتَيّب المُدرّب

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

مبـــادئ عامـــة فـي السلامـــة الرقميـة
السلامة الرقمية في العمل الدبلوماسي

الشريحة المستهدفة

الدبلوماسيون

كُتَيّب المُدَرّب

حقوق الملكية الفكرية

المادة مملوكة للوكالة الوطنية للأمن السيبراني في دولة قطر، وكافَّة حقوق الملكية الفكرية التي تشمل حقّ المؤلِّف وحقوق التأليف والنشر والطباعة، كلها مكفولة للوكالة الوطنية للأمن السيبراني في دولة قطر. وعليه، فجميع الحقوق محفوظة للوكالة، ولا يجوز إعادة نشر أي جزء من هذا الكُتَيّب، أو الاقتباس منه، أو نسخ أي جزء منه، أو نقله كلياً أو جزئياً في أي شكلٍ وبأي وسيلة، سواء بطرق إلكترونية أو آلية، بما في ذلك التصوير الفوتوغرافي، أو التسجيل، أو استخدام أي نظام من نُظم تخزين المعلومات واسترجاعها سواء من الأنظمة الحالية أو المبتكَرة في المستقبل؛ إلا بعد الرجوع إلى الوكالة، والحصول على إذنٍ خطّي منها.

ومَن يُخالِف ذلك يُعرّض نفسه للمُساءَلة القانونية.

عزيزي المشارك

في ظلّ التطوّر التكنولوجي المتسارع، ودخول الإنترنت إلى مختلف مجالات الحياة؛ أصبحت التهديدات السيبرانية تُواجه مختلف شرائح المجتمع. ومن هنا، أصبح تعزيز الوعي بمفاهيم السلامة الرقمية ضرورة إستراتيجية؛ إذ تُشكِّل الدرع الأساسي لحماية المجتمع من هذه التهديدات.

وفي سياق جهود المبادرة الوطنية للسلامة الرقمية لتعزيز مؤشرات السلامة الرقمية على مستوى المجتمع، يُقدّم هذا الكُتَيِّب الصادر عن الوكالة الوطنية للأمن السيبراني مجموعة من النصائح والإرشادات العملية للدبلوماسيين التي تساعد على تعزيز الحماية الرقمية، سواء على الصعيد الشخصي أو المهني.

الفهرس	رقم الصفحة

مقـدمـة

في عصرٍ تتسارع فيه وتيرة التحوّل الرقمي، لم تَعُد السلامة الرقمية خيارًا تكميليًّا، بل أصبحت ركيزة أساسية لضمان أمن الدول ومؤسساتها وموظفيها، خصوصًا في بيئة العمل الدبلوماسي التي تعتمد على تداول المعلومات الحساسة، والتواصل عبر القنوات الإلكترونية، وإدارة الملفات التفاوضية في فضاءٍ مفتوحٍ يَعُجّ بالتحديات السيبرانية.

يهدف هذا الكُتَيِّب إلى رَفْع الوعي بالسلامة الرقمية لدى الدبلوماسيين والعاملين في البعثات الخارجية، وتعزيز قدرتهم على حماية بياناتهم وأجهزتهم ومراسلاتهم من التهديدات السيبرانية المحتملة. كما يسعى إلى تمكينهم من التعامل الذكي والآمِن مع التقنيات الحديثة التي أصبحت جزءًا من الممارسة اليومية في العمل الدبلوماسي.

الفصل الأول

حماية البيانات والأجهزة

تُعَدّ حماية البيانات والمعلومات في بيئة العمل الدبلوماسي مسؤولية وطنية بالدرجة الأولى؛ إذ تعتمد البعثات الخارجية والسفارات على التكنولوجيا في التواصل وإدارة الملفات الحساسة. ومن هنا تأتي أهمية الوعي بالسلامة الرقمية كركيزة لضمان أمن المراسلات وصَوْن أسرار الدولة في الفضاء السيبراني.

أولًا: مفهوم الأمن السيبراني وأهدافه

يُمثِّل الأمن السيبراني الإطار الذي يهدف إلى حماية الأنظمة والشبكات والمعلومات من التهديدات السيبرانية؛ سواء كانت هجمات أو محاولات اختراق، أو محاولة تسريب للبيانات.

أهمية الأمن السيبراني

تأمين قنوات الاتصال الرسمية، مثل البريد الإلكتروني والمنصات الافتراضية

ضمان سرّية المعلومات وسلامة البيانات

حماية الأنظمة والشبكات من محاولات المراقبة أو الاختراق

أهداف الأمن السيبراني

01 حمايـــة المعلومـــات الحساسة من التسريب أو الوصول غير المصرّح بـــه

02 ضمان استمرارية العمل دون انقطاع أو تعطيل

03 رفـــــع كفـــاءة الدبلوماسييـــن في التعامـل مع المخاطر السيبرانية

04 تعزيـز الثقـة الدوليـة بالدبلوماسية الرقمية

هل تعلم؟

هـل تعلـم أن الدبلوماسـية السـيبرانية (Cyber Diplomacy) هـي مجـال ناشـئ مُهِـمّ يهـدف إلـى وَضْـع قواعـد مقبولـة للسـلوك الدولـي فـي الفضـاء السـيبراني[1]؟

1. Diplomacy in Cyberspace, American Foreign Service Association, on site: https://afsa.org/diplomacy-cyberspace?utm_source=chatgpt.com.

ثانيًا: حماية الأجهزة

تُعَدّ الأجهزة الرقمية -ولا سيما الهواتف الذكية- أداة أساسية في عمل الدبلوماسي؛ إذ تُستخدَم في التواصل، وتبادل المراسلات الرسمية، وإدارة الملفات اليومية. لكن في الوقت نفسه، تُشكِّل هذه الأجهزة مدخلًا رئيسيًّا للتهديدات السيبرانية إذا لم تُؤمَّن بالشكل الصحيح.

لحماية الأجهزة والهواتف الذكية، يُوصَى باتباع الممارسات الوقائية التالية[2]:

1

تحديث نظام التشغيل والتطبيقات بشكلٍ دوريّ؛ لضمان سدّ الثغرات الأمنية التي قد يستغلها المخترقون.

2

تفعيل المصادقة الثنائية لجميع الحسابات والبريد الإلكتروني، مما يمنع الوصول غير المصرّح به حتى في حال تسريب كلمات المرور.

3

استخدام كلمات مرور قوية وفريدة، تجمع بين الحروف الكبيرة والصغيرة والأرقام والرموز، وتغييرها بشكل منتظم.

4

تثبيت برامج الحماية الموثوقة، مثل تطبيقات مكافحة الفيروسات وفحص الأمان، مع التأكُّد من تحديثها باستمرار.

2. Cybersecurity Best Practices, CISA, on site: https://www.cisa.gov/topics/cybersecurity-best-practices.

5

تجنُّب تثبيت التطبيقات من مصادر غير رسمية أو الضغط على الروابط المجهولة التي قد تحتوي على برمجيات تجسُّس.

6

إيقاف تشغيل الكاميرا أو الميكروفون عند عدم الحاجة؛ لأن بعض البرمجيات الخبيثة قادرة على تفعيلها عن بُعْد دون عِلْم المستخدِم.

7

تشفير البيانات والملفات الحساسة داخل الجهاز، واستخدام خاصية القَفْل التلقائي في حال تَرْك الهاتف أو الحاسوب دون استخدام.

8

تجنَّب الاتصال بشبكات Wi-Fi العامة أو المفتوحة، خصوصًا في المطارات والفنادق والمقاهي؛ لأنها تُمثِّل بيئة مثالية لاعتراض البيانات.

ثالثًا: السلامة الرقمية في أثناء السفر

يُشكِّل السفر أحد أكثر المواقف التي تتعرَّض فيها الأجهزة والبيانات للمخاطر الرقمية، خصوصًا عند المشاركة في المؤتمرات أو الاجتماعات الدولية، أو استخدام شبكات أجنبية قد تكون غير آمِنَة.

وينبغي للدبلوماسي اتباع مجموعة من الإجراءات الوقائية قبل وفي أثناء وبعد السفر؛ لضمان الحفاظ على سلامة البيانات والأجهزة، وتشمل:

قبل السفر

- إجراء فَحْص شامل للأجهزة للتأكُّد من خلوّها من البرمجيات الخبيثة أو التطبيقات غير المصرّح بها
- إعادة ضبط المصنع المُؤقَّت للأجهزة المحمولة، والاكتفاء بالبيانات الضرورية فقط
- أَخْذ نُسْخة احتياطية مُشفَّرة للملفات الحساسة
- تفعيل المصادقة الثنائية على جميع الحسابات الرسمية قبل السفر

في أثناء السفر

- تجنَّب استخدام شبكات الإنترنت العامة أو المجانية
- عدم توصيل الأجهزة الشخصية إلى منافذ USB عامة
- عدم تحميل أو تثبيت أيّ تطبيقات جديدة أو فتح روابط مجهولة المصدر في أثناء السفر

بعد السفر

- مَحْو البيانات المؤقَّتة من الأجهزة المستخدَمة في أثناء السفر
- تغيير كلمات المرور لجميع الحسابات المستخدَمة خلال الرحلة
- مراجعة البريد الإلكتروني الرسمي؛ للتأكد من عدم وجود أيّ نشاط غير مألوف

احذر!

احذر استخدام الشبكات العامة المفتوحة (Public Wi-Fi) أو المنافذ المفتوحة (USB) في الأماكن العامة؛ فقد يؤدي ذلك لاختراق جهازك[3]!

3. What is ‹Juice Jacking› and Tips to Avoid It, Federal Communications Commission, on site: https://www.fcc.gov/juice-jacking-tips-to-avoid-it

رابعًا: تأمين البيانات والمستندات

يُشكِّل تأمين البيانات والمستندات إحدى أهم ركائز السلامة الرقمية، ويتطلّب اتباع مجموعة من الممارسات التي تضمن حفظ المعلومات بطريقة آمِنَة وسِرِّية، سواء في أثناء تخزينها أو في أثناء تبادلها إلكترونيًّا.

أبرز هذه الممارسات

1. استخدام تقنيات التشفير القوي (AES-256) لحماية الملفات الحساسة؛ بحيث لا يمكن فَتْحها أو قراءتها إلا باستخدام مفاتيح تشفير معتمدة من الجهة الرسمية[4].

2. تخزين المستندات المهمة داخل بيئات داخلية مُغلَقة (Intranet) بدلًا من الخدمات السحابية العامة؛ لتقليل احتمالية الاختراق أو التسريب.

3. تطبيق مبدأ صلاحيات الوصول المحدودة؛ بحيث يتم تحديد الأشخاص المُصَرَّح لهم بفتح الملفات أو تعديلها وفقًا لمستواهم الوظيفي ودورهم في البعثة.

4. تفعيل خاصية إدارة الحقوق الرقمية (Digital Rights Management) لمنع الطباعة أو النَّسْخ أو المشاركة غير المصرّح بها للملفات الرسمية[5].

4. 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

5. Digital Rights Management (DRM), FORTINET, on site: https://www.fortinet.com/resources/cyberglossary/digital-rights-management-drm

5 الاحتفاظ بنُسَخ احتياطية مُشفَّرة للبيانات المهمة، وتخزينها في مواقع منفصلة؛ لضمان استعادتها في حال فُقْدان النُّسَخ الأصلية أو تَلفها.

6 استخدام وحدات تخزين خارجية (USB)، أو أقراص صلبة مُشفَّرة بكلمة مرور قوية، وعدم تركها في الأماكن العامة أو أجهزة غير مأمونة.

7 تتبُّع عمليات الوصول والتعديل على الملفات الحساسة، عبر سِجِلّات التدقيق (Audit Logs) التي تُسجِّل كل إجراء يتم على المستندات.

هل تعلم؟

هل تعلم أن هجمات التصيد الاحتيالي والهندسة الاجتماعية هي أكثر الطرق شيوعًا التي يَستخدمها القراصنة لسرقة بيانات الاعتماد من خلال خداع المستخدمين لمشاركة معلومات حساسة أو تحميل برمجيات خبيثة[6]؟

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

الفصل الثاني

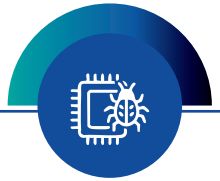
إدارة الحوادث السيبرانية

لا تخلو بيئة العمل الدبلوماسي من المخاطر السيبرانية؛ فكل رسالة إلكترونية أو نظام إداري أو قناة تواصل قد تكون مدخلًا محتملًا لحادث سيبراني. لذا، فإنّ فَهْم طبيعة هذه الحوادث وآليات التعامل معها يُعَدّ عنصرًا أساسيًّا لضمان استمرارية العمل والحماية من أيّ تهديد رقمي مفاجئ.

أولًا: الحوادث السيبرانية

يُعرَّف الحادث السيبراني بأنه أيّ حادث غير مُتوقَّع يُؤثِّر سلبًا على سرّية أو سلامة أو توافر الأنظمة والمعلومات داخل بيئة العمل الرقمي. وقد يكون هذا الحادث ناتجًا عن خطأ بشري، أو خلل تقني، أو هجوم متعمَّد يهدف إلى التجسس أو التخريب أو الابتزاز.

وتشمل هذه الحوادث



التصيّد الموجّه (Spear Phishing)، الذي يستهدف موظفين محددين

هجمات البرمجيات الخبيثة (Malware) وبرمجيات الفدية

اختراق البريد الإلكتروني الدبلوماسي، وسرقة أو تسريب المراسلات الرسمية

الهجمات على أنظمة الاتصالات أو المواقع الإلكترونية الرسمية

التلاعب بالمحتوى الإعلامي أو البيانات الرسمية، مثل نَشْر بيانات مزيفة

ثانيًا: الاستجابة للحوادث

هي عمليات وتقنيات للكشف عن التهديدات السيبرانية أو الخروقات الأمنية أو الهجمات السيبرانية، والاستجابة لها. تُمكِّن خطة الاستجابة الرسمية للحوادث فِرَق الأمن السيبراني من الحدّ من الأضرار أو مَنْعها[7].

7. What is incident response? IBM, on site: https://www.ibm.com/think/topics/incident-response

أهمية الاستجابة للحوادث

1. **تقليل الخسائر؛** من خلال العزل السريع للأنظمة المصابة قبل انتشار الهجوم
2. **حماية السُّمعة،** عبر السيطرة على الموقف ومَنْع تسريب أو نشر المعلومات الحساسة
3. **توفير أدلة رقمية دقيقة؛** تُستخدَم لاحقًا لتحديد مَصْدر الهجوم، وتقييم مستوى التهديد
4. **ضمان استمرارية العمل؛** من خلال خطط الطوارئ التي تُمكِّن الفريق من مواصلة المهام دون تعطيل
5. **تحسين منظومة الأمن السيبراني؛** من خلال مراجعة الإجراءات المتَّبَعة، واستخلاص الدروس بعد كل حادث

هل تعلم؟

هل تعلم أن استخدام الذكاء الاصطناعي في الأمن السيبراني يمكن أن يساعد على كشف الهجمات المعقَّدة مثل هجمات التصيد الاحتيالي والهجمات المُوجَّهة قبل أن تتسبّب في أضرار كبيرة[8]؟

8. Cyberattacks, IBM, on site: https://www.ibm.com/think/topics/cyber-attack#498277090

ثالثًا: دور الدبلوماسي ومسؤولياته

عند وقوع حادث سيبراني، يصبح كلّ دبلوماسي جزءًا أساسيًّا من منظومة الاستجابة. إنّ تصرُّف الموظف في اللحظات الأولى قد يُحدِّد مدى انتشار الضرر أو نجاح الفريق التقني في السيطرة على الموقف.

المسؤوليات في أثناء الحادث

1. الإبلاغ الفوري عن أيّ نشاط غير مألوف في البريد الإلكتروني أو الأجهزة أو الشبكة الداخلية، وعدم محاولة إصلاح المشكلة بشكلٍ شخصي.

2. تجنُّب التعامل مع الملفات أو الروابط المشبوهة، حتى لو كانت تبدو مُرسَلَة من جهة رسمية أو زميل في العمل.

3. عدم حَذْف أو تعديل الأدلة الرقمية، مثل الرسائل أو السجلات أو الملفات المصابة؛ لأنها تُعدّ عناصر مُهِمَّة في التحقيق والتحليل اللاحق.

4. التعاون الكامل مع فريق الأمن السيبراني، عبر تقديم المعلومات اللازمة، ومشاركة الملاحظات أو الأوقات التي لُوحِظ فيها الخلل.

5. الالتزام بالتعليمات الصادرة عن الفريق الفني، كفصل الجهاز من الشبكة، أو إعادة تعيين كلمات المرور فورًا عند الطلب.

6. الحفاظ على سرّية الحادث، وعدم تداوله عبر وسائل التواصل أو الحديث عنه خارج الإطار الرسمي، لتجنُّب نَشْر الشائعات أو استغلال الموقف إعلاميًّا.

الفصل الثالث

التهديـــدات السيبرانيـــة وأساليـب الوقايـة

تتزايد التهديدات السيبرانية يوميًّا، لتصبح أكثر ذكاءً واستهدافًا، خاصةً ضد القطاعات الحساسة مثل العمل الدبلوماسي. فالهجمات اليوم لم تَعُد عشوائية، بل باتت تُصمَّم بعناية لجمع معلومات دقيقة، أو للتأثير في مواقف سياسية واقتصادية.

أولًا: أنواع التهديدات الرقمية

يُعدّ الدبلوماسي أحد أبرز الأهداف التي تَستهدفها الهجمات السيبرانية حول العالم؛ نظرًا لحساسية المعلومات التي يتعامل معها، وطبيعة القرارات التي تُبْنَى عليها.

أنواع التهديدات السيبرانية

التصيّد الموجَّه (Spear Phishing)

يُعدّ أكثر الأساليب شيوعًا ضد الدبلوماسيين؛ حيث تُرسَل رسائل بريد إلكتروني تبدو رسمية ومُقنِعة تحتوي على روابط أو مرفقات خبيثة. بمجرد فَتْحها، يتمكَّن المهاجم من الوصول إلى بيانات الاعتماد أو أنظمة العمل[9].

انتحال الهوية (Identity Spoofing)

يعتمد على تقليد البريد الإلكتروني أو الحسابات الرسمية للدبلوماسيين؛ لخداع الآخرين، أو إرسال رسائل مُزيَّفة بأسمائهم؛ ما قد يُؤدّي إلى تسريب معلومات أو خَلْق أزمات في التواصل الرسمي[10].

التزييف العميق

هو استخدام محتوى مزوّر، أو بيانات مُحرَّفة؛ للنَّيْل من سُمْعة البعثات الدبلوماسية، أو بثّ الفِتَن السياسية بين الدول.

هل تعلم؟

هل تعلم أن المصادقة متعددة العوامل (MFA) تُقلِّل فُرَص اختراق الحسابات بشكل كبير[11]؟

9. What is spear phishing? IBM, on site: https://www.ibm.com/think/topics/spear-phishing.

10. 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.

11. Multifactor Authentication, CISA, on site: https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication.

للوقاية من التهديدات السيبرانية

1. تفعيل المصادقة المتعددة (MFA) لجميع الحسابات الرسمية والبريد الإلكتروني؛ لضمان الحماية حتى في حال تسريب كلمات المرور.
2. التحقُّق من هوية المرسِل والمحتوى قبل التفاعل، عبر فَحْص الروابط والمرفقات والتواصل مع الجهة المرسِلة عبر قناة بديلة للتأكُّد من مصداقيتها.
3. استخدام التوقيعات والشهادات الرقمية في المراسلات الرسمية للتمييز بين البريد الحقيقي والمزوّر ومنع انتحال الهوية.
4. التدريب المستمر للدبلوماسيين والموظفين على أساليب التصيّد، والتزييف العميق، والهندسة الاجتماعية؛ لاكتساب القدرة على كشفها مبكرًا.
5. الاعتماد على أدوات وتقنيات كشف التزييف العميق، وتحليل المحتوى الرقمي المشبوه قبل تداوله أو الرد عليه رسميًّا.
6. تطبيق سياسات أمنية مؤسسية واضحة، تشمل تحديث الأنظمة بانتظام، وتشفير البيانات الحساسة، والإبلاغ الفوري عن أيّ نشاط مشبوه لتفعيل الاستجابة السريعة.

احذر!

البيانات الحساسة غير المشفَّرة أو غير المحمية جيدًا؛ يمكن استغلالها أو سرقتها!

ثانيًا: البرمجيات الخبيثة

تُعدّ البرمجيات الخبيثة (Malware) إحدى أخطر الأدوات التي يستخدمها المهاجمون لاختراق الأنظمة أو التجسس على المستخدمين. وهي برامج تُصمَّم خصوصًا لإلحاق الضرر بالأجهزة، أو سرقة البيانات، أو السيطرة على الأنظمة عن بُعْد.

أنواع البرمجيات الخبيثة[12]

الفيروسات (Viruses)

تنتقل من ملف إلى آخر، وتصيب النظام تدريجيًّا، مُسبِّبةً تلفًا في البيانات، أو بطئًا في الأداء. غالبًا ما تنتشر عبر المرفقات أو وحدات التخزين الخارجية.

برمجيات الفدية (Ransomware)

تقوم بتشفير الملفات المهمة في الجهاز، ثم تطلب من الضحية دَفْع فدية مالية مقابل فكّ التشفير.

أحصنة طروادة (Trojans)

تبدو وكأنها برامج مفيدة أو ملفات مشروعة، لكنّها في الواقع تَمْنح المهاجمين وصولًا خفيًّا إلى الجهاز المستهدَف.

برمجيات التجسس (Spyware)

تعمل في الخلفية دون عِلْم المستخدِم، وتقوم بجمع البيانات والمراسلات والصُّوَر وتسجيل ضغطات لوحة المفاتيح.

12. 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

للوقاية من البرمجيات الخبيثة

تثبيت برامج الحماية الموثوقة، وتحديثها باستمرار

استخدام الشبكات الآمِنَة فقط، وتجنُّب الاتصال بشبكات عامة أو مفتوحة

عدم فتح أيّ ملفات أو روابط مجهولة المصدر

إجراء فَحْص دَوْري للأجهزة للكشف عن أيّ نشاط غير مألوف أو ملفات مشبوهة