نموذج

تقييم المخاطر الرقمية

سيساعدك هذا التقييم للمخاطر الرقمية في تحديد التهديدات الأمنية الرقمية المحتملة المرتبطة بتقريرك أو مهمّتك، وتقييمها.

أثناء إعدادك التقييم، ستجد روابط بالأقسام التي تتناول الموضوع نفسه في دليلنا إلى الأمن الرقمي. وستزوّدك هذه الروابط بالمزيد من المعلومات حول كيفية تخفيف المخاطر الرقمية المختلفة وتقليل تعرّضك للتهديدات المحتملة.

راجع موارد الأمن الرقمي للحصول على المساعدة في إنجاز هذا التقييم.

نرجو منك حفظ نسخة من هذه الاستمارة على جهاز خاص بك للرجوع إليها عند الحاجة.

التاريخ

1. أوجِز مهمّتك

قبل أن تتمكّن من تحديد المخاطر الرئيسية التي تُهدّد أمنك الرقمي بشكل صحيح، من المفيد أن تُقسّم مهمّتك إلى عدّة أقسام وأن تتمعّن في عناصرها الأساسية. حاوِل تحديد جميع المكوّنات الرئيسية، أي: التقرير، والأشخاص الذين ستُجري معهم المقابلات، وترتيبات السفر فضلاً عن أي إجراءات أخرى تحتل أهميةً بالغة بالنسبة إلى خططك. وبمجرد الانتهاء من ذلك، سيكون من الأسهل عليك تحديد جميع المجالات التي سيتعيّن عليك مراعاتها عند تقييم المخاطر.

عدّد وتوسّع في أكبر قدر ممكن من التفاصيل بشأن ما يلي:

موجز عن التقرير

المقابلات الرئيسية

خطط السفر

الإقامة

الإجراءات الرئيسية

2. ما هي التهديدات الرقمية التي تترافق مع تغطية هذا التقرير؟

فكّر الآن في أبرز المخاطر والتهديدات والخصوم.

تذكَّر أنه ليس من الضروري أن تغطّي خبراً حسّاساً أو مثيراً للجدل لكي تكون عرضة للمخاطر الرقمية. وبالتالي، يجب أن يصبح إعداد تقييم المخاطر خطوةً معتادةً عند العمل على كل المهامّ أو التقارير، خاصةً وأنّ العملية قد تكشف عن تهديدات محتملة لم تكن قد فكّرت فيها قَبلاً.

فكّر في ما يلي:

1) هل ستتواصل مع أشخاص ضُعفاء أو تُجري معهم المقابلات؟

إذا أجبت بنعم:

- كيف ستقوم بتخزين بيانات الأشخاص الذين ستُجري معهم المقابلات وحمايتها؟
- كيف ستقوم بتخزين ملاحظاتك وموادّك وأين؟

راجِع القسم أدناه حول الاتصالات للاطلاع على مزيد من الأسئلة بشأن كيفية الاتصال بالأشخاص بأمان.

---

2) هل تغطّي موضوعاً حسّاساً أو مثيراً للجدل؟

إذا أجبت بنعم:

- هل ينطوي ذلك على معلومات يجب أن تظل سرّية؟
- هل تفهم وتعرف كيفية استخدام أساليب البحث الآمنة؟
- متى ستكون أكثر عرضة للخطر؟
- متى ستكون مصادرك أكثر عرضة للمراقبة المحدّدة الهدف: في مرحلة البحث أو الإنتاج، أم عند الانتهاء من التقرير، أم عند نشره؟

راجِع القسم أدناه حول إجراء الأبحاث واستخدام الإنترنت للاطلاع على مزيد من الأسئلة بشأن تعزيز الأمن عند العمل باستخدام الإنترنت.

3) ما هو موقع مهمّتك/ تقريرك؟

- ما المعروف في تلك المنطقة عن المراقبة /الرقابة الحكومية على شبكة الإنترنت والاتصالات عبر الهاتف المحمول؟
- ما هي القوانين المتعلّقة باستخدام التشفير أو الشبكات الافتراضية الخاصة أو الحقّ في حرّية التعبير على وسائل التواصل الاجتماعي؟
- ما الذي سبق ونُشر بشأن انتهاك حقوق الصحافيين أو المبلّغين عن المخالفات أو الناشطين واضطهادهم بسبب نشاطهم عبر الإنترنت؟

1) من هم الخصوم المرجّح أن يهدّدوا أمنك الرقمي؟

فكّر في خصومك بطريقتين:

(1) الخصوم المباشرون:

من هؤلاء، حكومات أو شركات أو منظمات إجرامية أو أفراد يعارضون عملك أو لا يحبّذون تسليط الضوء عليهم في وسائل الإعلام. فكّر في الجهات التي يمكن أن تواجه تبعات (من الناحية القانونية، أو المهنية، أو المتعلّقة بالسمعة إلخ.) جرّاء مهمّتك.

(2) الخصوم غير المباشرين:

من هؤلاء، المخترقون الذين يستهدفون خدمة يستخدمها آلاف الأشخاص بشكل عشوائي، بمن فيهم أنت. على سبيل المثال، قد يخترق أحدهم شبكة لاسلكية أو يمكن أن يسرق أجهزتك.

يمكن الاطّلاع على الأدلّة الإلكترونية التالية للمزيد من القراءات:

→ البرمجيات الخبيثة

→ التشفير

3. معدّاتك

عدّد كل جهاز من معدّات الاتصالات التي ستنقلها معك.

بالنسبة إلى كل جهاز، توسّع في المعلومات التالية:

- ما نوع الرسائل التي سترسلها وتستقبلها باستخدام الجهاز (مثلاً الرسائل القصيرة أو رسائل البريد الإلكتروني أو الرسائل الفورية أو المكالمات الهاتفية)؟
- هل هذا الجهاز يحتوي، أو كان يحتوي، على أي معلومات حسّاسة يمكن أن تُعرّضك للخطر أو ينبغي حمايتها؟
- هل ستكون أجهزتك معك دائماً؟
- هل ستترك الجهاز في مكان يمكن فيه لشخص ما الوصول إليه؟
- هل أضفت فحوصات أمنية (مثل كلمات المرور والتشفير وما إلى ذلك) على جهازك لمنع الآخرين من استخدامه من دون إذن؟
- هل ستستخدم أجهزة الاتصالات الخاصة بأي شخص آخر أو الإنترنت في المقاهي العامة أثناء مهمّتك؟
- ما هي الخطوات التي ستتّخذها لتقليل المخاطر التي يمكن أن تتأتّى عن استخدامك لهذا الجهاز؟

- يمكن الاطّلاع على الأدلّة الإلكترونية التالية للمزيد من القراءات:

← الحواسيب	←الهواتف المحمولة

4. موادك

فكّر في المادة/ المواد التي ستجمعها أو تُسجّلها خلال مهمّتك.

بالنسبة إلى كلّ مادة، حدّد ما يلي:

- بأي صيغة سجّلت المادة (مثلاً، فيلم، نصّ، صوت، صوَر، إلخ.)؟
- هل المحتوى مُثير للجدل؟ إذا تمكّنت أطراف مُعادية من الحصول عليه، فهل سيُعرّضك هذا الأمر أنت أو أي شخص آخر مشارك في التقرير للتهديدات؟
- أين/كيف سيتمّ تخزين هذه المادة؟ هل اتّخذت أي خطوات لحماية هذه المعلومات؟
- هل ستحتاج إلى إرسال هذه المادة؟
- ما هي الخطوات التي ستتّخذها لتقليل الخطورة الناجمة عن تسجيل/بثّ المادة والتخفيف من شدّتها؟
- كيف ستقوم بنقل هذه المادة عبر الحدود؟

يمكن الاطّلاع على الأدلة الإلكترونية التالية للمزيد من القراءات:

→ عبور الحدود وحواجز التفتيش

→الحفاظ على أمن موادك

5. الاتصالات

عدّد كلّ الأشخاص الذين ستحتاج إلى الاتصال بهم أثناء العمل على المهمّة، كالأشخاص الذين ستُجري معهم المقابلات، وزملائك من الصحافيين المستقلّين، والمصادر، والمحرّرين.

بالنسبة إلى كلّ شخص، حدّد ما يلي:

- من هو ومن يمكن أن يراقبه (صاحب العمل، الحكومة، إلخ.)؟
- كيف ستتّصل به؟ هل أجريت بحثاً عن طريقة الاتصال الأكثر أماناً؟
- هل ستحتاج إلى إرسال أي معلومات حسّاسة له أو تلقّيها منه؟
- هل ستكون أنت أو أي شخص آخر عرضة للخطر نتيجة الاتصال به؟ ما هي الخطوات التي ستتّخذها للتخفيف من احتمال تحقّق هذا الخطر وشدّته؟
- هل لديك خطة لإعداد نسخ احتياطية وحذف الرسائل؟ هل ناقشت هذه الخطة مع مصدرك؟

يمكن الاطّلاع على الأدلّة الإلكترونية التالية للمزيد من القراءات:

→ الهواتف المحمولة | → التشفير | → البريد الإلكتروني

6. البحث واستخدام الإنترنت

فكّر في المواقع والمعلومات والمحتويات الذي ستحتاج إلى الاطّلاع عليها عبر الإنترنت، وتمعّن في المخاطر التي يمكن أن تترافق مع ذلك. إذا كانت زيارة المحتوى عبر الإنترنت قد تُسبّب لك مشكلات، فصغ قائمة بها لمساعدتك على التفكير في المخاطر.

بالنسبة إلى كل خطر، حدّد ما يلي:

- هل أجريت بحثاً عن الشركة التي توفّر لك التغطية بخدمة الإنترنت وهاتفك المحمول؟ هل تربطها علاقة وثيقة بحكومة البلد الذي تعيش/تعمل فيه؟
- هل أجريت بحثاً حول القوانين لمعرفة المدة التي يحقّ خلالها لهذه الشركات الاحتفاظ ببياناتك؟
- هل هذا المحتوى محظور في البلد/المنطقة التي ستعمل فيها؟
- إذا كنت بحاجة إلى الاطّلاع على المحتوى المحظور، فكيف ستفعل ذلك؟
- ما هو احتمال أن يتعرّض نشاطك للمراقبة؟
- ما هي الخطوات التي ستتّخذها للتخفيف من هذه المخاطر؟

يمكن الاطّلاع على الأدلّة الإلكترونية التالية للمزيد من القراءات:

→ البرمجيات الخبيثة

→ تصفح الإنترنت

7. ملفّك الشخصي الرقمي

1. هل راجعت صفحتك الإلكترونية للتأكد من عدم وجود محتوى يمكن أن يُعرّضك أنت أو معارفك للخطر؟

- هل أجريت بحثاً عن اسمك عبر الإنترنت لمعرفة المعلومات المتوفّرة عنك وهل اتّخذت خطوات لإزالة البيانات التي لا تريد تركها في المجال العام؟
- هل نشرت شيئاً ينتقد خصمك أو علّقت على أمر مماثل؟
- إذا أجبت بنعم، فما الذي ستفعله للتخفيف من شدّة هذا الخطر؟

---

2. هل لديك موقع إلكتروني واحد أو أكثر؟

- هل يمكن للمعلومات المخزّنة على هذه المواقع أن تُعرّضك أنت أو معارفك للخطر؟
- إذا أجبت بنعم، فما الذي ستفعله للتخفيف من شدّة هذا الخطر؟

---

3. هل تنوي استخدام وسائل التواصل الاجتماعي أثناء عملك على المهمّة أو التقرير؟

إذا أجبت نعم:

- هل وضعت كلمات مرور طويلة وقوية لحساباتك؟
- هل حدّثت إعدادات الخصوصية التي أضفتها إلى صفحاتك على مواقع التواصل الاجتماعي؟
- هل شاركت بكثافة في أنشطة مثل التغريد، أو مشاركة محتوى، أو التعليق عليه، أو الإعجاب به، أو غير ذلك، بشكل يمكن أن يُعرّضك للخطر أثناء المهمّة؟
- هل حساباتك الشخصية على وسائل التواصل الاجتماعي منفصلة عن تلك المتعلّقة بعملك؟
- ما هي الخطوات الأخرى التي تتّخذها لتخفيف الخطر الذي تتعرّض له بسبب نشاطك على وسائل التواصل الاجتماعي وللتقليل من شدّة هذا الخطر؟
- هل فكّرت في التأثير النفسي الذي يمكن أن تُخلّفه وسائل التواصل الاجتماعي عليك أو على فريقك أو على المساهمين في تقريرك؟

يمكن الاطّلاع على الأدلة الإلكترونية التالية للمزيد من القراءات:

→ وسائل التواصل الاجتماعي

تذكّر!

يُعدّ الأمن الرقمي جانباً واحداً فقط من خطة السلامة الخاصة بالمهمّة أو المشروع، ويجب اعتباره إحدى خطوات استعداداتك للسلامة. ويمكن لموارد السلامة والأمن الصادرة عن صندوق روري بيك أن تساعدك في مجالات أخرى تتعلّق بضمان سلامتك.