Internews
Local voices. Global change.

Journalist Security Fellowship

دليل تيسير تمارين المحاكاة للتدريب على السلامة الرقمية

الغاية منها ومقدمة

الهدف من هذا الدليل هو أن يكون مرافقا لمجموعة مُكوَّنة من 11 سيناريو لتمارين المحاكاة تُركِّز على السلامة الرقمية، والتي يمكن استخدامها لتعزيز التدريب على الأمن الرقمي. هذا الدليل موجه ليتم استخدامه من قبل أي شخص يرغب في تصميم وتيسير تمارين المحاكاة كطريقة للتدريب على السلامة الرقمية. ستجد في هذا الدليل تعاريف موجزة لتمارين المحاكاة، ولماذا يمكن أن تكون ملحقات ذات قيمة لتدريبات السلامة الرقمية، وكيف يمكن للمرء تطويرها وتخطيطها وتيسيرها.

لقد تم تطوير السيناريوهات الأحد عشر الموجودة في هذا الدليل بالتعاون مع صحفيين في وسط وجنوب شرق أوروبا، كجزء من مشروع زمالة انترنيوز (INTERNEWS) لأمن الصحفيين (اختصارا : JSF)، وتم استخدامها في الدورات التدريبية التي أجراها زملاء JSF في المنطقة. يمكن الوصول إلى نماذج تمارين المحاكاة هذه، بما في ذلك بعض الإصدارات المُوطَّنة للغات وسط وجنوب شرق أوروبا والمترجمة إلى العربية والإسبانية، في الرابط الموجود هنا.

تم تطوير هذا الدليل خصيصا مع الوضع بعين الاعتبار السلامة الرقمية للصحفيين وغرف الأخبار، ولكنه قد يكون مفيدا أيضا في تخطيط تمارين للمحاكاة تستهدف جماهير أخرى.

ما هي تمارين المحاكاة، على أي حال؟ ولماذا تُعد ذات قيمة؟

إن تمرين المحاكاة هو أسلوب تدريب قائم على سيناريو يكون غالبا على شكل نقاش تفاعلي. توفر تمارين المحاكاة فرصة لتدريب المشاركين على تطبيق المعارف والمهارات المكتسبة حديثا من خلال الانخراط في موقف خيالي (يشار إليه بسيناريو أو مشهد محاكاة) والذي يقترب من الحياة الواقعية. يمكن لسيناريوهات المحاكاة معالجة مجموعة كبيرة من المواقف الأمنية مثل مداهمة المكتب، أو تسرب البيانات، أو حالة التشهير، أو التحقيق ذو طابع حساس. بالرغم من أن طرق التدريب التقليدية قد تركز على نقل بعض المهارات والمعارف التقنية، فإن تمرين المحاكاة يمكن أن يساعد على:

- توفير فضاء قليل المخاطر لتدريب المشاركين على التمرُّن على الاستعداد للقضايا الأمنية التي قد يواجهونها وعلى الاستجابة لها.
- الحث على النقاش النقدي لقضايا الأمن الرقمي وكيفية التعامل معها بشكل أفضل في سياقات ومواقف مختلفة. قد يكون ذلك مفيدا بالأخص لتدريب المشاركين الذين يعملون معا بانتظام للنظر في أساليبهم المشتركة أو التنظيمية عن السلامة.
- تقييم مدى جاهزية الفرد أو المنظمة للتعامل مع القضايا الأمنية التي يواجهونها.

الهدف من تمرين المحاكاة هو تحديد الفجوات الفردية والتنظيمية والمجتمعية في المعارف ونقاط القوة وحدودها. يتجاوز تمرين المحاكاة الناجح كونه مجرد أدوات وممارسات أساسية، بل يسلط الضوء أيضا على احتمال غياب بعض الإجراءات أو السياسات، أو التي قد تحتاج إلى تحسين.

تكون تمارين المحاكاة أكثر فعالية عند استخدامها كمُكمِّلات لتعزيز طرق تدريب أخرى. وذلك لأن الهدف من تمارين المحاكاة في المقام الأول ليس نقل المهارات والمعارف الجديدة ولكن لإحكام ترسيخ التعلمات وتثبيتها من خلال الممارسة والنقاش والتقييم المرتكزة على السيناريوهات.

مكونات وثائق سيناريو المحاكاة

يبلغ عدد مشاهد تمارين المحاكاة 11 مشهدًا، يرتكز كل مشهد من هذه المشاهد بشكل فضفاض على شخصية « سارة »، والتي تم توضيحها في هذا الدليل. يتضمن كل مشهد أيضا المكونات التالية:

- الهدف - الهدف المحوري لسيناريو المحاكاة.
- أهداف التعلم - الخيارات لأهداف التعلم العامة التي يتم التركيز عليها أثناء تمارين المحاكاة. سيكون من المفيد أن يختار المُنشِّطون عددا قليلا من الأهداف للتركيز عليها.
- المهارات والسلوكيات التي يجب التدرب عليها قبل أو بعد تمرين المحاكاة – الخيارات لمهارات ملموسة ومحددة والتغيرات السلوكية التي سيركز تمرين المحاكاة على تثبيتها أثناء تدريب المشاركين. سيكون من المفيد أن يختار المُنشِّطون عددا قليلا من المهارات والسلوكيات للتركيز عليها، كما يجب أن تتماشى مع أهداف وغايات التعلم التي تم تحديدها.
- السيناريو – هذا هو سيناريو المحاكاة الفعلي. ويشمل ما يلي:
- خلفية تمهيدية ومعلومات سياقية في البداية
- تقديم أجزاء إضافية من السياق خلال السيناريو
- أسئلة وتوجيهات للمناقشة والرد عليها من طرف المشاركين. يتم تمييزها بالحرف س متبوعا برقم (مثلا، س 1، س 2، س 3، الخ).
- يوجد أسفل الأسئلة والتوجيهات بعض الإجابات المحتملة. لا ينبغي إطلاع المشاركين عليها أثناء تمرين المحاكاة. تهدف هذه الإجابات إلى مساعدة المُنشِّط.
- تشمل بعض السيناريوهات عمليات إدخال (سيتم الإشارة إليها بإسم « إدخال »). الإدخال عبارة عن جزء من المعلومات الجديدة أو جزءا من تطور جديد، يقوم المُنشِّط بإدراجه في سيناريو المحاكاة في أوقات محددة، وذلك لمواصلة التقدم في السيناريو أو لإضافة التعقيدات. قد يغير الإدخال سرد أحداث تمرين المحاكاة وقد يتطلب اتخاذ إجراءات أو الحصول على استجابات من المشاركين.
- الملحقات - تتضمن بعض السيناريوهات مرفقات أيضا (مثلا، السيناريو 3: المضايقة والتشهير)، في كثير من الأحيان تُستخدم هذه المرفقات كإدخال أثناء السيناريو.

تطوير سيناريو محاكاة

Once escenarios TTX fueron desarrollados bajo el proyecto JSF (enlazado aquí). Cualquiera puede لقد تم تطوير أحد عشر سيناريو محاكاة في إطار مشروع زمالة أمن الصحفيين JSF (الرابط هنا). يمكن لأي شخص تعديل هذه السيناريوهات، بحيث تتناسب بشكل أفضل مع الاحتياجات التدريبية لمجتمعهم. يمكن للمرء أيضا إنشاء سيناريو خاص به من الصفر. إذا كنت تفكر في مراجعة أحد هذه السيناريوهات أو إنشاء سيناريو خاص بك، ضع بعين الاعتبار ما يلي.

يجب تحديد أهداف التعلم في بداية مرحلة التصميم، و أن تُكمِّل بعضها البعض، وأن تتبع ترتيبا منطقيا من حيث التعلم، وأن يتم تحديد أولويتها على أساس الأهمية، وأن ترتبط في النهاية بالهدف العام لتمرين المحاكاة. من أجل تبسيط عملية التدريب وتسهيل قياس النجاح، قم بربط أهداف التعلم بمهارات أو سلوكيات ملموسة يجب التركيز عليها من طرف المشاركين أثناء تمرين المحاكاة. من الأفضل أن تقوم بتحديد هذه الأهداف

التعلمية والمهارات الملموسة بناءً على احتياجات المشاركين وبناءً على مستوى مهاراتهم. ربما تكون لديك فكرة عنها إذا كنت تعمل مع مجتمع تعرفه. وكبديل لذلك، ربما قد تحتاج إلى إجراء تقييم أولي للاحتياجات (ربما من خلال مقابلات مع مخبرين رئيسيين أو باستخدام استطلاع أولي) لجمع هذه المعلومات إذا كنت أقل دراية بالمشاركين.

يجب أن يكون السيناريو أقرب إلى الحياة الواقعية قدر الإمكان، ولكن بشكل عام لا ينبغي أن تُذكَر الأسماء الحقيقية للأشخاص أو المنظمات. حاول التركيز على المواقف والتحديات والتجارب الحقيقية. في حالات نادرة، قد يكون من الملائم استخدام مواقع حقيقية، ولكن يجب عليك مراعاة المخاطر الأمنية والقيود المحتملة أثناء القيام بذلك. مثلا، عند إدراج مواقع حقيقية قد يقضي الأشخاص وقتا أطول لتذكُّرها والبحث في تفاصيلها بدل التركيز أكثر على السيناريو.

لا ينبغي للسيناريو أن يصل لدرجة تعقيد تجعله يطغى على عملية التعلم ويؤدي بذلك إلى تشتيت الانتباه عنه. يمكن أن تساعد الاختيارات المتعددة المشاركين على فهم التأثير الذي ستُحدِثه قراراتهم، ولكن يجب التذكر أن إضافة التعقيدات والاختيارات المتعددة ستزيد من صعوبة بناء تمرين المحاكاة وسيجعل التمرين أطول بكثير.

يمكنك أيضا استخدام الوقت كعنصر تصميم خلال السيناريو الخاص بك وذلك عن طريق تعيين أوقات للأحداث التي تقع خلال تمرين المحاكاة، أو عبر طرح أسئلة محددة زمنيا، أو استخدام أحداث ماضية أو لمحات مستقبلية. على أي حال، يجب أن تكون واضحا بشأن استخدام الوقت في بداية السيناريو وأن تحافظ على الوضوح طوال عرض المشهد.

يمكنك التفكير في إدراج عناصر تقنية في تمرين المحاكاة حسب مستوى مهارات المُنشِّط والمشاركين. قد يعني هذا استخدام المشاركين لأداة محددة أو برنامج أو عملية معينة للتقدم في السيناريو. إذا قمت بإدراج عنصر تقني، يجب منح وقت إضافي لإكمال هذه المهام، واحتفظ دائما بخطة احتياطية في حالة حدوث مشاكل تقنية أو اجعل المكون التقني اختياريا لمراعاة مستويات المهارات المختلفة.

يمكنك أيضا استخدام الإدخالات خلال تمرين المحاكاة الخاص بك. قد تكون عمليات الإدخال كبيرة أو صغيرة وقد تعتمد على المشاركين أو قد تكون مستقلة عنهم. عموما، يتم استخدام الإدخالات في سيناريوهات أطول حسب الوقت المطلوب. يتم القيام بالإدخال من قبل المُنشِّط، كما أن التوقيت هو العامل الأهم. لدمج إدخال ما في مشهد بنجاح، فاستخدام موارد المُنشِّط مطلوبة قبل وأثناء تيسير تمرين المحاكاة. يجب أن يتوافق استخدامك لعمليات الإدخال مع احتياجات تحقيق أهداف التعلم المحددة سابقا.

التخطيط لتمرين المحاكاة

قبل البدء في التخطيط لتمرين المحاكاة، توقف لحظة للتفكير في جمهورك المستهدف وكيف سيؤثر ذلك على أهداف التعلم. هل تحاول التواصل مع الصحفيين أو مديري غرف الأخبار أو أفراد الأمن؟ سيتعامل كل واحد منهم مع معلومات مختلفة تماما عن الآخر وسيكون مسؤولا عن قرارات مختلفة. كبديل لذلك، تتعامل بعض تمارين المحاكاة بشكل مدروس مع قاعدة جماهيرية أوسع — مثلا، غرفة أخبار بكاملها —- وذلك لفهم أفضل لكيفية تواصل الأشخاص فيما بينهم واتخاذهم للقرارات. ربما قد تعمل مع مشاركين يمتلكون مستويات متباينة من المهارات والمعارف والخبرات المتعلقة بالأمن الرقمي. امنح لنفسك بعض الوقت لتعديل تمرين المحاكاة بحيث يلبي الاحتياجات الخاصة للمشاركين على أفضل وجه.

بمجرد تحديد جمهورك المستهدف، خطط لأهدافك التعليمية وخذ بعين الإعتبار المهارات أو السلوكيات المحددة التي ستُدَرِّب عليها. كمدرب، يُعد اختيار مهارات محددة قبل التدريب أساسيا لمساعدتك على التركيز في تحديد أهداف تعلمية ملموسة للمشاركين، وسيساعدك في وضع معايير لقياس فعالية التدريب. راجع قائمة نماذج المهارات ضمن القسم الفرعي في كل مستند تمرين محاكاة تحت عنوان « المهارات والسلوكيات التي يجب التدرب عليها قبل أو بعد تمرين المحاكاة ». قد يكون من المغري تغطية أكبر عدد ممكن من أهداف التعلم ضمن تمرين محاكاة واحد، ولكن سيكون إجراء التدريب أكثر فعالية عندما يكون محدودا ويغطي أهدافا تعليمية محددة. تذكر أن جمهورك لديه وقت واهتمام محدودان.

حاول معرفة مقدار الوقت اللازم لأجل تمرين المحاكاة. بالرغم من أن بعض الوكالات الحكومية أو الشركات تقوم أحيانا بتمارين محاكاة تمتد لعدة أيام، إلا أن جمهورك قد لا يكون لديهم متسع من الوقت. يجب أن تضع بعين الاعتبار ساعات العمل وأوقات رعاية أولادهم وباقي

الالتزامات لحياة للمشاركين. في العادة، يستغرق إكمال تمرين محاكاة يحتوي من 4 إلى 6 أسئلة أو إدخالات حوالي ساعة إلى ساعة ونصف. يعتمد ذلك أيضا بشكل كبير على عدد أفراد مجموعتك. عادة ما تستغرق المجموعات الأكبر وقتا أطول لإكمال تمرين المحاكاة. كما ستحتاج أيضا إلى إضافة وقت زائد من أجل استخلاص المعلومات، ومراجعة أهداف التعلم، والمهارات أو مراجعة السلوكيات الملموسة التي ترغب في أن يكتسبها المشاركون بعد المشهد. قد يحتاج المشاركون إلى مزيد من التدريب أو المتابعة حتى يتمكنوا من اكتساب هذه المهارات أو السلوكيات بنجاح.

ضع في اعتبارك الفضاء المتوفر لديك لهذا النشاط. إذا تم إجراؤه حضوريا، فهذا مثالي لتيسير تمرين المحاكاة في فضاء يسمح بالتعاون. يُستحسَن أن تكون غرفةً تحتوي على طاولات وكراسي مريحة بدلا من قاعة محاضرات، وذلك لأنها أكثر ملاءمة لتمارين المحاكاة. قد تحتاج أيضا إلى التأكد من وجود شبكة Wi-Fi عالية الجودة أو وسائل تكنولوجية أخرى، مثل جهاز العرض. كما ينبغي أيضا إعطاء أولوية لإمكانية الوصول إلى فضاء التعلم ما أمكن (مثلا، إمكانية الحصول على الكراسي المتحركة، والحمامات الشاملة للجنسين، وخيارات نقل مريحة، وما إلى ذلك).

يجب أن تقرر ما إذا كان سيكون هناك عدة أدوار للتنشيط وما هي تلك الأدوار. قد يكون من المنطقي أن يتولى مُنشِّط واحد إدارة تمرين المحاكاة، بينما يساعد الآخرون في غرف مجموعات فرعية محددة أو في مهام فرعية. قد يرغب المُنشِّطون أيضا في التدرُّب على بعض العناصر مسبقًا.

حدد الموارد التي ستحتاجها لأجل تمرين المحاكاة. قد ترغب في إنشاء مجموعة من الشرائح أو النشرات أو أي نوع آخر من مواد التقديم لعرض سياق المشهد أو الأسئلة أو التوجيهات أو الإدخالات. من المهم أيضا الوضع بعين الاعتبار المواد التي قد يحتاجها المشاركون لتدوين الملاحظات.

تنشيط تمرين محاكاة

يختلف تنشيط تمرين المحاكاة عن إدارة تدريب تقليدي على الأمن الرقمي وعن حصص تحسين المهارات. في التدريب التقليدي على السلامة الرقمية، يميل المدربون إلى التحدث كثيرا ويُتوقَّع منهم مشاركة معارفهم مع المشاركين. إلا أنه في تدريب تمرين المحاكاة، معظم الحديث والعمل يحدث بين المشاركين أنفسهم، حيث يناقشون السيناريو ويتخذون القرارات. يلعب مُنشِّط تمرين المحاكاة دور المشرف على العملية، حيث يتأكد أن التمرين يسير بسلاسة ويحقق أهدافه. يقوم مُنشِّط تمرين المحاكاة بتقديم التمرين والسياق وخلفية الأحداث؛ ويجيب على بعض الأسئلة الأساسية؛ ويضيف الإدخالات. تتضمن التوصيات الأخرى لتيسير تمرين المحاكاة ما يلي:

- التأكد من أنك على دراية تامة بتمرين المحاكاة.
- تذكُّر الغاية والأهداف من التعلم الخاصة بتمرين المحاكاة، ثم القيام بتوجيه النقاش حتى يتمكن المشاركون من تحقيق تلك الأهداف.
- التحدث عن الأدوار والتوقعات بوضوح في البداية وطوال تمرين المحاكاة.
- مراقبة الساعة عن كثب والتأكد من احترام الوقت الذي تقضيه مع المشاركين و الاستفادة منه.
- التأكد من أن الفضاء آمن ومُرحِّب وأن يشعر معظم الأشخاص بأن وجهات نظرهم مسموعة وموضوعة في الحسبان.
- عندما يشير أحد المشاركين إلى ممارسة جيدة، يجب القيام بتسليط الضوء عليها! يمكن لهذا أن يعزز الثقة بالنفس ويشجع على المزيد من المشاركة.
- عند الجهل بالجواب عن سؤال ما، فلا خوف من الاعتراف بذلك، ويكفي الالتزام بالرد عليه بعد تمرين المحاكاة. استخدم فضاءات المجتمع مثل Mattermost الخاص بـ Team CommUNITY للحصول على إجابات للأسئلة التي قد لا تتمكن من معرفتها بنفسك.
- إذا كان ممكنا، عليك بجمع الملاحظات طوال فترة المشاركة والاستعداد لإجراء تعديلات صغيرة. إذا كنت تخطط لاستضافة تمرين محاكاة ما مرات متكررة، فيمكنك أيضا جمع الملاحظات في نهاية الجلسة لفهم كيف يمكنك تحسينها للمرات القادمة.
- إذا بدأ تمرين المحاكاة ينحرف عن المسار الأصلي، فلا بأس بذلك! كن مرنا ولكن يجب التأكُّد من أنه يعالج أهداف التعلم في النهاية.

إذا كنت ترغب في الحصول على إرشادات أكثر تفصيلا، فيما يلي التعليمات المقترحة لمساعدتك في التنشيط، خطوة خطوة.

1. قم بتقديم نفسك (وأي مدربين مشاركين آخرين)، واشرح دورك (أو أدواركم)، وصِف الهدف العام لتمرين المحاكاة (مثلا: سنرى اليوم كيف يمكن لغرفة الأخبار الاستجابة لحدث أمني). هذا هو الوقت المثالي أيضا لوضع بعض القواعد الأساسية للمجموعة.
2. بعد ذلك، قم بتفصيل أكثر بوصف ما سيحدث أثناء تمرين المحاكاة. اشرح أن المقصود منه هو محاكاة موقف خيالي يقارب الحياة الحقيقية من أجل فهم أفضل لاستجاباتنا واستجابات مجتمعنا بشكل أوسع .
3. حسب عدد أفراد المجموعة ومكوناتها، قد ترغب في تقسيم المشاركين إلى مجموعات فرعية.
4. قم بعرض مقدمة المشهد على المشاركين، بما في ذلك أي قصة قد تكون ضرورية لفهم سياق الأحداث .
5. قم بسرد المشهد، توجيها تلو الآخر، بينما يتقدم المشاركون عبر تمرين المحاكاة. كن متأهبا في حال طرح أحد سؤالا وكذلك للمساعدة في استكشاف الأخطاء وإصلاحها إذا واجه المشاركون أي عقبة.
6. قم بتزويد الإدخالات حسب الحاجة.
7. شجع المشاركين على التفاعل والاستجابة للتوجيهات. اطلب منهم تدوين الملاحظات حيثما كان ذلك مناسبا أو مفيدا. استخدم إجاباتك المعدة مسبقا لمساعدة المشاركين في حالة مواجهتهم للصعوبات أو عند حاجتهم إلى أمثلة للبدء.
8. بعد أن يكمل المشاركون تمرين المحاكاة، اطلب منهم مناقشة ما تعلموه من التجربة وأفكارهم حول تمارين المحاكاة كأسلوب تدريب. يُعد هذا وقتا مناسبًا لتسجيل الملاحظات والتفكير في دمج التحسينات في الدورات التدريبية المستقبلية.
9. بمجرد اختتام تمرين المحاكاة، تحقق مما إذا كانت هناك أي مواد ختامية أو متابعات أو ملخصات يجب مشاركتها مع المشاركين.

الملحق 1: خلفية عن « سارة » (شخصية من تمارين المحاكاة)

لقد أنشأنا شخصية واحدة، « سارة »، لنجعلها أساس التجارب في أمثلة سيناريوهات تمارين المحاكاة. لقد ساعدنا هذا على إضفاء طابع من التناسق إلى تمارين المحاكاة وإعطاء الصحفيين نقطة انطلاقة جيدة للتفكير في التهديدات والتفكير في سياق أوسع. لقد قمنا بإدراج مقدمة عن « سارة » أدناه، والتي يمكن للمُنشِّطين استخدامها لتهيئة المشهد وتوفير السياق قبل بدء أحد الأمثلة لسيناريوهات تمارين المحاكاة الخاصة بنا.

« سارة » صحفية تبلغ من العمر 41 عاما. عملت في العديد من المؤسسات الإخبارية المحلية والدولية لعدة سنوات في البلد الذي وُلدَت فيه وفي البلدان المجاورة.

في العام الماضي، بدأت سارة العمل مع منظمة إخبارية استقصائية تسمى 'Free Press Now' في بلدها الأم، والتي تقدم عدة تقارير عن مجموعة من القضايا السياسية. تشمل هذه التقارير الانتهاكات المشتبه بها لحقوق الإنسان من قبل الحكومة الحالية، والمسؤولين الحكوميين الفاسدين، والسياسات الحكومية التي تجعل الحياة أكثر صعوبة بالنسبة للأقليات العرقية في البلاد.

بفضل تقاريرها الصادقة والموثوقة، أصبحت Free Press Now مصدرا موثوقا وشعبيا للمعلومات للسكان المحليين.

بعد الانتخابات الوطنية التي أُجريَت قبل خمسة أشهر، بدأت الحكومة الجديدة التي أخذت زمام السلطة في تقييد حريات الصحافة، وفي الأسبوع الماضي داهمت السلطات منازل ثلاثة صحفيين بارزين في العاصمة. ومؤخرا، تمت مداهمة منزل « سارة » أيضا، رغم أن منفذي المداهمة لم يأخذوا سوى عدة دفاتر.

.

السيناريو 1: جهاز مفقود

الهدف

مساعدة المشاركين على التخطيط والاستجابة في حال فقدان جهاز واحد أو أكثر من أجهزتهم - والذي قد يحتوي على معلومات حساسة.

أهداف التعلم

- تحديد مقاربات لضمان التواصل الآمن بين الصحفيين ومصادرهم البشرية.
- ترسيخ الوعي حول مخاطر فقدان جهاز مثل الهاتف أو الحاسوب.
- فهم أفضل الممارسات المتعلقة بحماية الأجهزة وأمنها
- مشاركة المقاربات الجيدة لالتحاق موظفي المنظمات بالوظيفة ومغادرتها، لاسيما فيما يتعلق بأمن الأجهزة.

المهارات والسلوكات التي يجب التدرب عليها قبل أو بعد تمرين المحاكاة

- تثبيت وإعداد واستخدام سيجنال (Signal) (أو أي تطبيق مراسلة آمن آخر)
- إعداد واستخدام برنامج مراسلة بديل مُعمَّى من طرف إلى طرف (مثل واتساب WhatsApp أو المحادثة السرية لفيسبوك ماسنجر Facebook Messenger Secret Chat)
- تثبيت وإعداد واستخدام Mailvelope (أو خيار آخر لتعمية البريد الإلكتروني)
- تعمية جهاز محمول (إعداد كلمة السر)
- تعيين كلمات سر لكل تطبيق على الجهاز المحمول
- إجراء نسخ احتياطي وتعمية البيانات على الأجهزة المحمولة (باستخدام الخدمات السحابية أو الأقراص الصلبة الخارجية)

السيناريو

اتصل سابقًا مصدر مجهول بـ « سارة » عبر فيسبوك ماسنجر (Facebook Messenger)، موضحا أن لديه معلومات حساسة يريد مشاركتها معها. يحتوي الملف الذي يريد مشاركته على معلومات حول الشؤون المالية لوزير الدفاع الحالي.

رغبة منها في الحفاظ على أمان المصدر، ترغب « سارة » في إقناعه بنقل المعلومات عبر برنامج مراسلة مُعمَّى من طرف إلى طرف.

س 1 - كيف يمكن لـ « سارة » شرح مفهوم التعمية من طرف إلى طرف لإقناع المصدر بأهمية ذلك المفهوم؟

- لن يتمكن أحد – ولا حتى الشركة التي تدير برنامج المراسلة – من الوصول إلى محتويات الرسالة. ولن يتم تخزين محتوى الرسالة بشكل غير مُعمّى على خوادم الشركة أيضًا
- لا يمكن لهيئات تنفيذ القانون الوصول إليه من مزود خدمة المحادثات
- إذا تمكن أحد المهاجمين من اختراق الحساب الذي تم استخدامه لإرسال الرسالة، فلن يتمكن من الوصول إلى محتويات الرسائل أيضا (ما لم تكن هناك نسخ احتياطية غير مُعمّاة)

س 2 - للتأكد من أن التواصل بينهما آمن من الآن فصاعدا، ما هي أشكال التواصل الرقمي التي يجب على « سارة » أن تفكر في استخدامها مع هذا المصدر؟

- برامج المراسلة مع التعمية من طرف إلى طرف والرسائل المختفية
- البريد الإلكتروني المُعمّى

ابتهج المصدر، لكون « سارة » تُركّز على التأكد من أمن تواصلهما، لكن المصدر لا يزال غير متأكد من الطريقة الأولى بالاختيار. طلب المصدر بعض النصائح من « سارة » حول تطبيقات المراسلة مثل سيجنال (Signal) و تيليجرام (Telegram) و فيسبوك ماسنجر (Facebook Messenger)، بالإضافة إلى بريده الإلكتروني.

س 3 (الاختيار) - من منظور الأمن الرقمي، ما هي بعض العوامل التي يجب مراعاتها عند اختيار تطبيقات المراسلة المختلفة واستخدامها؟

- - أرقام الهواتف: تتطلب معظم برامج المراسلة المُعمّاة من طرف إلى طرف أرقام الهواتف، وفي العديد من الأماكن يجب تسجيل أرقام الهواتف، إذَ بذلك تعرف الحكومة الشخص الذي يكون خلف أي رقم هاتفي. وهذا يعني أنه إذا بحثت الحكومة في هاتف « سارة » أو هاتف المصدر، فيمكنهم معرفة أنهم كانوا يتراسلون، حتى لو استخدموا أسماء مستعارة أو رسائل مختفية (وسيكون الحل الوحيد هو حذف الأسماء من جهات الاتصال وتطبيقات المراسلة ومن الأفضل مسح محتوى الهاتف)
- - المحادثات السرية: يوفر فيسبوك ماسنجر (Facebook Messenger) وتيليجرام (Telegram) وضعين إثنين، أحدهما فقط مُعمّى من طرف إلى طرف. يُطلق على هذا الوضع عادة اسم المحادثة السرية أو شيء مشابه، لكنه غالبا ما يكون مخفيا في الإعدادات
- - الرسائل المختفية: تحتوي جميع برامج المراسلة الحديثة تقريبا على ميزة الرسائل المختفية، لكن في بعض الحالات تكون متاحة فقط في وضع المحادثة السرية
- - حذف المحادثات: يُعد هذا أمرا بديهيًا، ولكن من المهم الإدراك أن بعض برامج المراسلة تقوم فقط بأرشفة المحادثات بدلا من حذفها
- - الوعي بلقطات الشاشة: يمكن لأي طرف ضار في المحادثة التقاط لقطة شاشة أو — إذا كانت ميزات برنامج المراسلة لا تسمح بذلك — يمكنه ببساطة التقاط صورة لشاشة هاتفه
- - الاستيثاق بعاملَين: يمكن للمهاجم الاستيلاء على حساب المراسلة عن طريق الاستيلاء على رقم الهاتف الذي تم استخدامه لتسجيل الحساب وإعادة إرسال رسالة التحقق القصيرة إليه. يسمح له ذلك بانتحال شخصية مالك الحساب، لكن لا يمنح عادة حق الوصول إلى سجل الرسائل. تتوفر معظم برامج المراسلة الآن على خيار طلب كلمة سر إضافية بالإضافة إلى الرمز المُرسَل عبر الرسائل القصيرة: هذا يعني أنه حتى لو تمكن أحد المهاجمين من الاستيلاء على رقم الهاتف، فلن يتمكن من الوصول بسهولة إلى الحساب
- - الرموز السرية أو العبارات السرية المتينة لتسجيل الدخول إلى الجهاز (الهاتف) نفسه

س 4 (الاختيار) - من منظور الأمن الرقمي، ما هي بعض العوامل التي يجب مراعاتها عند التواصل عبر البريد الإلكتروني؟

- يجب على المصدر إنشاء عنوان بريد إلكتروني جديد يستعمله فقط للتواصل مع « سارة »
- - يجب أن يحتوي البريد الإلكتروني الجديد على كلمة سر قوية وفريدة من نوعها واستيثاق متين بعاملَيْن
- - يجب على المصدر أيضا البحث عن هجمات التصيُّد واستخدام التقنيات التي يمكن أن تساعد في التقليل منها، مثل المفاتيح الأمنية الفعلية أو الملء التلقائي لمدير كلمات السر
- - على نحو مثالي، يجب أن يتواصل المصدر و« سارة » عبر PGP، على سبيل المثال باستخدام Mailvelope. وهذا يعني أنه حتى لو تم اختراق حساباتهم بطريقة ما، فسيظل المهاجم غير قادر على قراءة محتويات رسائلهم بدون مفتاح PGP الخاص بهم

يرسل المصدر الملف بشكل آمن إلى « سارة » وتراه على هاتفها المحمول. إنها سعيدة بالحصول على هذه المعلومات وتخرج مع أصدقائها للاحتفال بذلك. أثناء وجودها في حفلة ما، تفقد « سارة » هاتفها وتدرك أنها نسيت حمايته بكلمة السر.

أثناء حضورها إحدى الحفلات، فقدت هاتفها وأدركت أن لديها كلمة سر بسيطة جدا (1111).

س 5 - ماذا يمكن أن يحدث لهاتف « سارة » والمعلومات الموجودة بداخله؟

- يمكن لأي شخص يعثر الهاتف الوصول إلى المعلومات الحساسة إذا اكتشف مكانها
- - يمكن لأي شخص يجد الهاتف إرسال رسائل إلى جهات اتصال « سارة » والتظاهر بأنها هي
- - يمكن لأي شخص يبحث في المعلومات الموجودة على الهاتف أن يعرض هوية وسلامة جهات اتصال « سارة » للخطر أو أن يجمع معلومات يمكن استخدامها في الهندسة الاجتماعية
- - يمكن لـ « سارة » أن تفقد بشكل جدي مصداقيتها كصحفية

س 6 - ما الذي يمكن أن تفعله « سارة » الآن للحد من التأثير على أمنها الرقمي؟

- - يمكنها مسح محتوى هاتفها عن بعد، إذا كانت قد قامت بإعداد هذه الخاصية
- - يمكنها تسجيل الدخول إلى بريدها الإلكتروني وحسابات وسائل التواصل الاجتماعي على أجهزتها الأخرى، وتقوم بتغيير كلمة السر، وإذا أمكن، أن تضغط فوق رابط "تسجيل الخروج من جميع الأجهزة التي تم تسجيل الدخول إليها"

س 7 - ما هي إيجابيات وسلبيات إخبار المصدر أنها فقدت الهاتف؟

- نقاش بدون إجابات صحيحة ودقيقة.

أخبار جيدة! وجدت صديقة « سارة » و التي كانت معها في الحفلة الهاتف في معطفها. اتصلت بها وأعادت لها الهاتف في اليوم الموالي.

س 8 - الآن بعد أن استعادت « سارة » هاتفها، ما هي الخطوات التي يمكنها اتخاذها فيما يتعلق بتأمين جهازها رقميا في حال فقدانه مرة أخرى في المستقبل؟

- - فكر في استخدام فتح القفل باستخدام المقاييس الحيوية في بعض الأحيان. هناك مزايا (لا يمكن لأحد أن يختلس النظر بينما تقوم « سارة » بإدخال كلمة سرها، ولن يتم التقاطها بواسطة كاميرات المراقبة أيضا) وعيوب لذلك (من السهل إجبار « سارة » على فتح قفل جهازها)
- - قم باستخدام كلمات سر وعبارات سرية أطول لفتح قفل الهاتف. تجنب فتح القفل باستخدام الأنماط (مثل تلك التي تربط بين النقاط)، حيث يمكن تخمينها بسهولة من طرف الشخص الذي ينظر أو الكاميرا أو الآثار على الشاشة
- - قم بقفل التطبيقات (مثل برامج المراسلة) بكلمة سر إضافية أيضا، إذا كانت « سارة » متوجسة من احتمال مشاركة أو تمرير هاتفها في بعض الأحيان
- - قم بإعداد التطبيقات التي يمكنها تعقب الأجهزة وتحديد موقعها ومسحها عن بُعد

س 9 - من منظور التنظيمي، كيف يجب أن تبدو عملية التحاق موظف جديد بوظيفته من أجل تأمين أجهزة المنظمة، مثل الهواتف المحمولة والحواسيب؟

- التأكد من اتباع جميع الموظفين، بغض النظر عن مناصبهم، لإجراءات عملية الالتحاق وأن يدركوا أهميتها
- يجب على المنظمات أن تسرد بوضوح التوقعات المطلوبة من الموظفين بخصوص اتباع ممارسات الأمن الرقمي للمنظمة.
- تحديد الخطوات التي يجب اتخاذها عند التعرض للخطر (مثل سرقة الهاتف أو تعرض كلمة السر للاختراق)
- يجب تقديم الدعم التقني لجميع الموظفين الذين يحتاجون إليه.

Internews
Local voices. Global change.

Journalist Security Fellowship

السيناريو 2: الأمن في المنظمات والوعي بالروابط

الهدف

مساعدة المشاركين لضمان مستوى عالٍ من الوعي بالأمن الرقمي وضمان تطبيق أفضل الممارسات داخل منظمتهم، مع زملائهم في العمل، بل مع الصحفيين المستقلين.

أهداف التعلم

- نظريا، فهم مفهوم السلامة الرقمية كعملية متواصلة وليس كغاية.
- التحدث وتعليم وإقناع الآخرين بأهمية الأمن الرقمي
- مناقشة خيارات التواصل الآمن عبر جهازك المحمول بشكل عملي
- التأكد من أفضل الممارسات حول التعامل الآمن مع الملفات.
- الوعي بإعدادات الحساب لأجهزة الحاسوب المتصلة بالشبكة.
- فهم أهمية نمذجة التهديدات.

المهارات والسلوكات التي يجب التدرب عليها قبل أو بعد تمرين المحاكاة

- 1 - إعداد الصلاحيات وصيانتها في المنصات التعاونية (مثل جوجل درايف Google Drive)
- 2 - (إن كان ممكنا، نظرا لأن بعض هذه الميزات متوفرة فقط على منصات المؤسسات) الاطلاع على سجلات الوصول في المنصات التعاونية (مثل جوجل درايف Google Drive)
- 3 - إعداد واستخدام الاستيثاق بعاملَيْن، وعلى نحو مثالي مع المفاتيح الأمنية الفعلية أو آليات مماثلة ومقاومة لأساليب التصيُّد
- 4 - سياسات كلمات السر الجيدة (استخدام كلمات سر فريدة، واستخدام كلمات سر طويلة، واستخدام عبارات سرية) ومديري كلمات السر
- 5- تعمية المستندات (باستخدام Mailvelope وغيره)
- 6 - تثبيت وإعداد واستخدام تطبيق سيجنال Signal (أو أي تطبيق مراسلة آمن آخر)
- استخدام الميزات المتقدمة داخل تطبيق المراسلة الآمن (كمثال، حذف الرسائل المحدد بالوقت)
- 7 - تثبيت وإعداد واستخدام Mailvelope (أو خيار آخر لتعمية البريد الإلكتروني)
- 8- التعامل بشكل آمن مع الملفات والمستندات من المصادر الحساسة

السيناريو

تقوم « سارة » بتشكيل فريق من الصحفيين للتحقيق في الفساد المتعلق بالصفقات العمومية خلال كوفيد-19 والتي قامت بها وزارة الصحة. ليس لدى كل الصحفيين في الفريق نفس المستوى من المهارات الرقمية و المعارف و ممارسات السلامة. تعرف « سارة » أن مستوى أحد أعضاء فريقها ضعيف جدا في حماية الملفات.

تعلم « سارة » أن أحد أعضاء فريقها يتَّبع بعض الممارسات غير المبالية فيما يتعلق بحماية الملفات.

س 1 - كيف يمكن لـ « سارة » أن تشجع زملاءها على تحسين نهجهم في مجال السلامة الرقمية؟ ما الذي يجب أن تفعله « سارة » لضمان تطبيق ممارسات الأمن الرقمي عند تنظيم فريق تعاوني؟

- قم بشرح أهمية التمتع بالسلامة الرقمية الجيدة: يمكن أن يشمل ذلك التحدث عن كيف يمكن لضعف السلامة الرقمية أن يعيق بشكل كبير المسيرة المهنية للصحفي، وكيف من المرجح أن تثق بك المصادر والزملاء أكثر إذا كنت تتمتع بسلامة رقمية جيدة، والحاجة إلى حماية الناس من حولنا.
- قم بمناقشة الأجهزة التي يستخدمونها، وكيف يقومون بحماية حسابات مستخدميهم، وكيف يقومون بتخزين الملفات وكيف يتبادلونها، وكيفية وصولهم إلى شبكة عملهم (هل يستخدمون أجهزتهم الخاصة أم أنهم يعملون على حواسيب الشركة)، وإذا كانوا يستخدمون الاستيثاق بعاملَيْن لتأمين حسابات مستخدميهم وتنظيم كلمات سرهم (هل يعيدون استخدام كلمات السر، وهل يستخدمون مديري كلمات السر).
- تقرير كيف يجب على الفريق التواصل وكيف يجب عليهم تخزين الملفات والوصول إلى الملفات. الهدف من الخطوة الثانية هو التأكد من أن الجميع يتبع نفس البروتوكول المتعلق بالأنشطة المذكورة سابقا.
- الوضع بعين الاعتبار تدريب الفريق باستخدام البروتوكولات المعمول بها حديثا. بعد وضع القواعد يجب على الفريق أن يمر عبر تدريب تجريبي، ليختبر فعليا طرق التواصل الجديدة ومعرفة مكامن الخلل في العملية ، والتي يجب تسويتها.

س 2 - كيف ستقوم « سارة » وفريقها بتخزين ومشاركة الملفات الصوتية والمستندات من المصادر؟

- تقييد من يمكنه الوصول إلى الملفات والمجلدات المختلفة، واستخدام إعدادات المشاركة بعناية في منصات مثل جوجل درايف Google Drive
- ثني الأشخاص عن أخذ الملفات والمستندات من بيئة العمل (مفاتيح USB، مرفقات البريد الإلكتروني...) والذي قد يؤدي إلى توسيع مساحة الهجوم وزيادة خطر التسريبات والاختراقات.
- الطلب من الفريق استخدام حواسيب العمل فقط للوصول إلى ملفات العمل
- تقييد البرامج التي يمكن تثبيتها على حواسيب العمل، والتأكد دائما من وجود كلمات سر متينة وآخر التحديثات للبرامج

س 3 - كيف سيضمن كل من « سارة » و فريقها التواصل بشكل آمن؟

من خلال إلحاق الفريق بأكمله لنفس المنصة والتأكد من ارتياح الجميع عند استخدامها، يمكن لـ « سارة » مساعدة فريقها في إنشاء طريقة تواصل سالمة وآمنة فيما بينهم.

الوضع بعين الإعتبار:

- نقل معظم المحادثات إلى تطبيق سيجنال Signal، مع استخدام اختفاء الرسائل ونسخ الرسائل التي تحتاج إلى الأرشفة
- استخدام PGP في البريد الإلكتروني
- إنشاء قواعد أمنية متينة لحساب البريد الإلكتروني (كلمة سر فريدة، استيثاق بعاملَيْن)

قبل أسبوعين من نشر تقريرهم، تتلقى « سارة » مكالمة هاتفية من المصدر الحكومي الرئيس في هذا التحقيق. تعرف « سارة » المصدر جيدا وتثق به. في المكالمة، يقول المصدر ببساطة "الحكومة تعلم - لقد حدث تسريب" ثم يغلق الخط.

س 4 - من منظور الأمن الرقمي، ما هي الخطوات الأولى التي يجب على « سارة » اتخاذها للاستجابة للتسرب المحتمل للمعلومات؟

- طلب تغيير كلمات السر من جميع أفراد فريقها، فقط في حالة حصول أحد المهاجمين على كلمة السر لأحد حساباتهم.
- الأخذ بعين الاعتبار أن الحكومة لم تكن في حاجة إلى اقتحام غرفة التحرير التابعة لها؛ إذ أنه من الممكن أنهم اكتشفوا التسريب من خلال تحرّي ما يطبعه الموظفون الحكوميون مثلا.

- القيام بإجراء تحقيق صغير داخل غرفة الأخبار: التحقق مما إذا كان الجميع يتبعون البروتوكولات، ومن لديهم حق الوصول إلى الملفات والمعلومات التي تم تسريبها، وما الذي تم تسريبه بالضبط في المقام الأول. يمكن تتبع الوصول إلى كل جزء من البيانات التي تعمل عليها بطريقة أسهل من خلال استخدام ميزات التحكم في الوصول والتحكم في النُّسخ .
- التفكير فيما إذا كانت هناك حاجة إلى تسريع عملية النشر.

تدرك « سارة » أن التسريب جاء من داخل منظمتها. كان لدى المصمم حق الوصول إلى جوجل درايف Google Drive المشترك للمؤسسة. عرفت « سارة » هذا من خلال التحقق من ميزة التحكم في الوصول في جوجل درايف Google Drive، إذ أدركت أن فريق التصميم كان لديه حق الوصول إلى كل شيء على الشبكة بسبب طبيعة عملهم، ووجدت أن أحد المصممين قد قام عن طريق الخطأ بمشاركة مستند مع عميل مستقل لديه كان يعمل مع الحكومة، عوض مشاركته مع صديق في غرفة الأخبار يحمل نفس الاسم العائلي.

س 5 - ما الذي كان يمكن لفريق « سارة » أن يفعله بشكل مختلف في هذه الحالة؟

- يجب على « سارة » إنشاء بروتوكولات آمنة تنطبق على فريق التحقيق الخاص بها فقط. وينبغي لها التأكد من وجود نظام واضح لمنح التصريحات وأنه يتم اتباعه في الممارسة العملية.
- يجب أن يعمل الفريق مع المصممين بطريقة تجعلهم لا يملكون سوى المعلومات التي يحتاجون إليها: ولا ينبغي إعطاؤهم أي تفاصيل سرية أو حساسة إلا في حالة الضرورة القصوى للنشر.
- يجب على « سارة » أيضا أن تنظر إلى الأمن والخصوصية على أنها سيرورة للعمليات وليست حالة عرضية ؛ إنه شيء يجب تداوُله باستمرار.

السيناريو 3: المضايقة والتشهير

الهدف

مساعدة المشاركين على تصور أفضل طريقة للاستعداد والاستجابة للتشهير والمضايقات عبر الانترنت.

أهداف التعلم

- تحديد الأساليب والتدابير التخفيفية للصحفيين الذين يتعرضون للمضايقات والتشهير على وسائل التواصل الاجتماعي.
- فهم كيف يمكن جمع المعلومات من وسائل التواصل الاجتماعي وكيف يمكن استخدامها ضد الصحفيين وموظفي غرفة الأخبار.
- استكشاف العلاقة بين جنس الفرد والمضايقات التي يتعرض لها، والتبعات الأمنية لذلك.
- مناقشة الاعتبارات حول كيف يمكن لمؤسسة إعلامية القيام بوضع إجراءات وممارسات لحماية الموظفين والمتعاقدين الذين يتم
- استهدافهم من خلال المضايقات و التشهير.
- الوضع في الاعتبار خططا احترازية للصحفيين الذين ليس لديهم دعم من غرفة الأخبار (مثل العاملين لحسابهم الخاص والموظفين الخارجيين)
- السرد الأمني وإقناع الآخرين، كيف يمكن التحدث مع الأشخاص الذين لا يواجهون المضايقات بشكل تقليدي وإقناعهم بأنها مشكلة كبيرة تتطلب عملا ودعماً تنظيمياً مُنسَّقا.
- الأمن التنظيمي: إعداد السياسات داخل المنظمات، وتحديد الطرق التي يمكن للمنظمات من خلالها تقديم الدعم الأفضل للصحفيين الذين يواجهون هجمات المضايقة [1]

المهارات والسلوكات التي يجب التدرب عليها قبل أو بعد تمرين المحاكاة

- إدارة وتحديث إعدادات الخصوصية على منصات التواصل الاجتماعي الكبرى
- استخدام أدوات الأمان على منصات التواصل الاجتماعي الكبرى، مثل الإبلاغ والحظر. يتضمن هذا معرفة كيفية استخدام هذه الآليات وفهم ما تقوم به بالضبط
- إعداد واستخدام الاستيثاق بعاملَيْن، ومن الأفضل استخدامه مع مفاتيح الأمان الفعلية أو آليات مماثلة مقاومة للخداع

السيناريو

تعمل « سارة » على مقال جديد عن الأقليات العرقية في بلدها وكيف تؤدي السياسات الحكومية إلى زيادة تهميش هذه المجموعات. خلال الأسابيع الماضية لاحظت « سارة » ارتفاعا في عدد التعليقات على حساباتها في وسائل التواصل الاجتماعي، حيث تشارك أيضا أعمالها. بدأت أيضا تتلقى تعليقات بغيضة ومهينة من قبل مختلف مثيري الإزعاج على الانترنت الذين يستهدفونها مباشرة.

س 1 - ما هي بعض الخطوات التي يمكن أن تتخذها « سارة » لحظر والإبلاغ عن الأشخاص الذين يدلون بهذه التعليقات؟

- يمكنها الاتصال بشركات التواصل الاجتماعي الكبرى (مباشرة أو ربما من خلال منظمتها) للإبلاغ عن المضايقات واسعة النطاق.
- تعطيل المنشورات والردود على صفحتها الشخصية
- أن تكون أكثر انتقائية بشأن من يمكنه العثور عليها على وسائل التواصل الاجتماعي

[1] في معظم الدورات التدريبية، سيكون هذا هدفا تعليميا. إذا كنت ستدير جلسة مع مديري وسائل الإعلام أو غيرهم من صناع القرار وكان من الممكن قياس النتائج التنظيمية، فيمكنك أيضا استخدام هذا كمهارة

- اختيار عدم إمكانية وَسمِها على وسائل التواصل الاجتماعي

أدى بذل الجهود لحظر والإبلاغ عن بعض المحرضين الرئيسيين عبر الانترنت إلى إزعاج مجموعة من مثيري الإزعاج في الشبكة، مما أدى إلى زيادة المحتوى الذي يحض على الكراهية ضد « سارة ». تشير بعض التعليقات أيضا إلى التهديد والعنف تجاهها، بشكل مباشر وغير مباشر.

س 2 - ما هي بعض الطرق التي يمكن لـ « سارة » أن تحقق في هذا العدوان ضدها لتحديد ما إذا كان جزءً من حملة أكبر وأكثر تنسيقًا أو شيئا أكثر تنظيما.

- يمكنها التحقيق في الموقف بنفسها، ويمكنها كذلك طلب دعم الزملاء في التحقيق
- يمكنها التحقق من كون المزعجين يستخدمون نفس اللغة أو نفس الكلمات المفتاحية أو نفس الوسومات. إذا كان الأمر كذلك، فمن المرجح أن تكون حملة مُنسَّقة
- حسب المنصة. هناك خيارات عدة في « أنستغرام » لرؤية المعلومات المتعلقة بحسابات معينة — متى تم إنشاؤها، وعدد الأشخاص الذين يستخدمونها، وكم مرة تم تغيير اسمها، وما إلى ذلك.
- تحقق من كونه يتم تضخيمه من طرف وسائل الإعلام
- التحقق من أوقات النشر الأكثر شيوعا

تخبر زملاءها عن المنشورات، لكن يقول لها معظم أعضاء الفريق الذكور بمن فيهم رئيس تحريرها ألا تقلق وأن المشكلة ستختفي من تلقاء نفسها. إنها متوترة وتشعر أن فريقها لا يستمع لها ولا يدرك المشكلة.

س 3 - بدلاً من إخبار « سارة » بألا تقلق، ما هي بعض الطرق التي يمكن لفريقها ومنظمتها دعم « سارة » من خلالها، لا سيما فيما يتعلق بوجودها على الانترنت وأمنها الرقمي؟

- المساعدة في إجراء تقييم كامل للوضع
- مراجعة الممارسات الأمنية الرقمية مع « سارة » وتدابير السلامة المعمول بها، ومساعدتها في تحسين الوضع إذا لزم الأمر.
- الحصول على الممارسة والخبرة المشتركة من الآخرين في المنظمة
- السماح للأشخاص ذوي الثقة بإدارة الحساب أو الاطلاع عليه لتفادي التعرض مباشرة لتلك الكلمات والتهديدات لكن مع استمرار الوجود في الانترنت رغم ذلك
- يمكن للمنظمة المساعدة في البحث عن أنماط حدوث المضايقات
- تتبع كيفية حدوث المضايقات في منشورات المنظمة وليس منشورات « سارة » فقط
- رفع هذا الأمر إلى فريق الأمن والمساعدة في التحقيق

في أحد الأيام، سرب أحد مثيري الإزعاج في الشبكة صور « سارة » الشخصية على الانترنت. الصور التي نشرتها على مواقع التواصل الاجتماعي منذ سنوات، هي صور شخصية، وفي بعض الحالات تتضمن بعض المعلومات الحساسة.

أَدخِلْ - شارك من 1 إلى 4 صور مع المشاركين. (يمكن العثور على الصور في الملحق في هذه الوثيقة). تشمل أمثلة الصور ما يلي:

- « سارة » وكلبها يسيران خارج منزلها
- « سارة » تدخن سيجارة القنب الهندي
- « سارة » ومجموعة من أصدقائها المقربين في عطلة
- « سارة » وهي تعمل داخل غرفة الأخبار الخاصة بها

ناقش مع مجموعة المشاركين لماذا قد تكون كل صورة من هذه الصور حساسة.

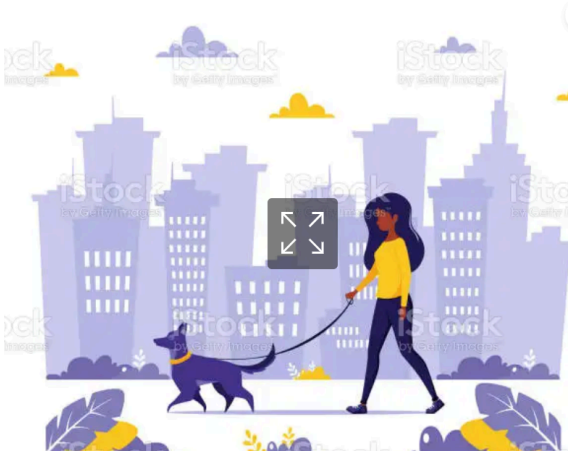
س 4 - ما هي بعض الطرق التي يمكن لشخص ما الوصول بها إلى معلومات « سارة » عبر الانترنت، مثل منشورات وسائل التواصل الاجتماعي القديمة؟

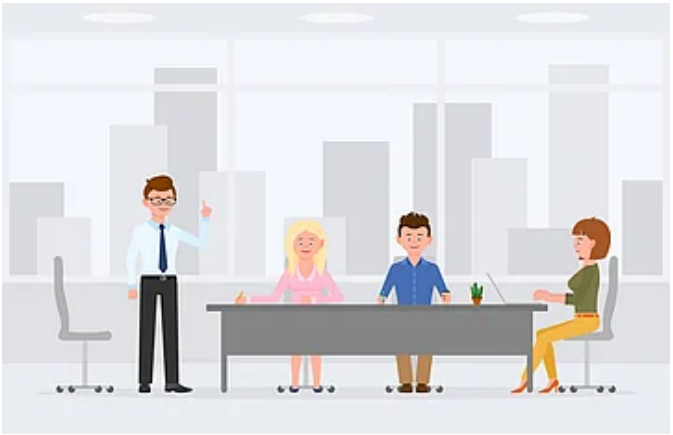
- قيام أصدقاء « سارة » بنشر صورها دون إعدادات خصوصية ملائمة

- القيام باختراق حسابات « سارة »
- احتمال قيام أحد معارف « سارة » من وسائل التواصل الاجتماعي بحفظ الصور لمشاركتها لاحقا
- إمكانية فهرسة صور « سارة » على وسائل التواصل الاجتماعي بواسطة محرك للبحث

س 5 - ما هي الخطوات التي يمكن أن تتخذها « سارة » لمحاولة منع تسريب المزيد من المعلومات عنها عبر الانترنت؟
- حذف الصور القديمة
- حذف الحسابات
- قفل الحسابات
- تحميل صور جديدة ولكن تسرب فقط القليل من المعلومات عنها
- الحصول على تقرير من شركة التواصل الاجتماعي والذي يلخص جميع البيانات التي لديهم عنها
- الإبلاغ عن الصور التي تم نشرها مؤخرا والإبلاغ عن الحسابات التي تم النشر منها
- الاستمرار في نشر المحتوى المتعلق بالعمل، حتى لو تم نشر محتوى شخصي أقل. إذا تم الانسحاب من الانترنت، فذلك يُعد فوزا للمزعجين على الانترنت
- أخذ لقطة شاشة للمنشورات، وتوثيقها قدر الإمكان. وتسجيل الأسماء المستعارة للمزعجين على الانترنت

س 6 - ما الخطوات التي كان من الممكن أن تتخذها « سارة » و منظمتها لمنع جمع هذه المعلومات وتسريبها عبر الانترنت، لاسيما فيما يتعلق بالأمن الرقمي؟
- إنشاء مجموعة من الأصدقاء المقربين كي يتمكنوا من رؤية الصور الشخصية والمنشورات الشخصية على وسائل التواصل الاجتماعي وحدهم فقط
- عدم نشر المعلومات الحساسة نهائيا (مثل الصورة المرفقة)
- عدم نشر الصور التي تكشف معلومات خاصة مثل الموقع
- إنشاء حسابات مهنية بحيث يكون لها وجود على الانترنت ليس له علاقة بحياتها الشخصية
- كلمة سر متينة وسياسات استيثاق بعاملَيْن لحسابات وسائل التواصل الاجتماعي





السيناريو 4: دخول السلطات لغرفة أخبار

الهدف

مساعدة المشاركين في الاستجابة النظرية والعملية لدخول السلطات إلى غرفة الأخبار الخاصة بهم

أهداف التعلم

- التأكد من وجود خطط احتياطية للتواصل ووجود مكونات تقنية في حال عدم التمكن من الوصول إلى غرفة الأخبار أو إلى الجهاز الشخصي.
- فهم أفضل الممارسات عندما يتعلق الأمر بتأمين الأجهزة الرقمية داخل غرفة الأخبار أو المنظمة.
- تحديد طرق لتأمين مختلف الملفات على جهاز رقمي، مثل الحاسوب أو الهاتف المحمول.
- التخطيط لتعرض المعلومات للخطر في حال دخول السلطات ومداهمتها لغرفة الأخبار.
- استكشاف المفاهيم المتعلقة بنمذَجة التهديدات والتخطيط المسبق للأفراد والمنظمات.

المهارات والسلوكات التي يجب التدرب عليها قبل أو بعد تمرين المحاكاة

- استخدام أداة مثل VeraCrypt أو ما يشبهها لتعمية البيانات الموجودة على الأقراص الصلبة والأقراص الخارجية
- نمذَجة التهديدات، وتحديدا ما يتعلق بالتعامل مع السلطات ومداهمة المكاتب: كيفية تقييم المخاطر، والاستعداد لها، واستخلاص العِبر بعد حدوثها
- الأمن التنظيمي والمجتمعي، وتحديدا كيفية العمل مع رؤساء التحرير والمديرين والمحامين أثناء المواقف العصيبة، وتحديد أي سؤال يجب رفعه إلى مَن بالضبط
- استخدام الإعدادات داخل Microsoft Office وجوجل درايف Google Drive لمعرفة آخر الملفات التي تم الوصول إليها ومتى
- (مهارة متقدمة) إذا كانت للمؤسسة سجلات وصول شاملة من خلال اشتراك في جوجل درايف Google Drive المُميَّز أو اشتراك O365، فيمكن الوصول إلى هذه السجلات والعمل بها
- الاطلاع على سجلات البحث وسجلات الوصول إلى الملفات في متصفحات الانترنت وأنظمة التشغيل الرائدة

السيناريو

تعمل « سارة » في غرفة أخبار بها حوالي 20 شخصا. إنه صباح يوم إثنين حافل، حيث يعمل 15 صحفيا وموظفون آخرون من غرفة الأخبار، مع 5 زملاء آخرين يعملون عن بُعد.

في الساعة 10 صباحا، وصل ما يقرب من 50 ضابط شرطة إلى غرفة الأخبار. لديهم مذكرة يظهرونها لرئيس التحرير، ثم يشقون طريقهم بينما يطالبون في نفس الوقت جميع الصحفيين والموظفين بالمغادرة على الفور.

تلتقي « سارة » وزملاؤها في الخارج ويناقشون سبل الحفاظ على عمل منظمتهم الإعلامية بطريقة سليمة و آمنة.

س 1 - ما هي بعض الأولويات في مثل هذا الموقف؟

- التواصل مع محامٍ للتشاور بشأن الخطوات التالية
- الاتصال بالزملاءً الذين يعملون عن بعد
- تدقيق في الذي يحمل هاتفه المحمول معه ومن تركه في المكتب

س 2 - ما هي بعض الطرق التي يمكن بها لـ « سارة » وزملائها التواصل بشكل آمن خلال هذا الموقف؟

- إنشاء محادثة جماعية على واتساب WhatsApp أو سيجنال Signal
- قد يكون من الجيد التواصل من خلال أرقام شخصية، بدل أرقام العمل. لكي لا تتم مزامنة المحادثة مع الأجهزة التي لا تزال في المكتب

س 3 - كيف ينبغي لـ « سارة » وزملائها إدارة حسابات المنظمة على الانترنت مثل المواقع الإلكترونية وحسابات وسائل التواصل الاجتماعي؟

- تغيير كلمات السر على الفور
- إذا كان من الممكن تسجيل الخروج عن بعد من الأجهزة التي لا تزال في المكتب، لكن يجب استشارة المحامين أولا حتى لا يعتبر ذلك تلاعبا بالأدلة (قد يعتمد هذا بشكل كبير على الموقع أو الولاية القضائية)
- التشاور مع المحامين قبل نشر شيء حول مداهمة الشرطة

تتذكر « سارة » أنها عندما كانت تغادر غرفة الأخبار، رأت الشرطة تبدأ بوضع الحواسيب والأجهزة والأوراق في أكياس. تمكنت « سارة » من المغادرة بهاتفها، لكن بقي حاسوبها المحمول في غرفة التحرير. قامت مجموعة الزملاء بتقييم سريع للمعلومات التي يمكن للشرطة الحصول عليها.

س 4 - كيف يجب تأمين الأجهزة في غرفة الأخبار؟

- تأمين الحواسيب بكلمات سر متينة
- تشغيل قفل الشاشة بعد فترة قصيرة من الوقت؟
- مفاتيح USB وأقراص صلبة خارجية مُعمّاة

أثناء مناقشتهم خارج المكتب، كشف رئيس التحرير أنه نسي قَفل جهاز حاسوبه عند مغادرة المكتب.

السؤال 5 - ما هي بعض الطرق التي يمكن لغرفة الأخبار من خلالها على الفور تقييم تأثير مداهمة السلطات ؟

- التحقق مما تمت مصادرته أو ما تم إعادة ترتيبه من الملفات الورقية (إذا تمت إعادة ترتيب الملفات، فهذا يعني أن الشرطة ربما تكون قد صوَّرتها)
- بما أن الحواسيب تحتوي عادةً على سجلات البحث والوصول إلى الملفات وكذلك تاريخ التصفُّح، فتحقق منها أيضا. يمكنك رؤية الملفات الحديثة في Microsoft Word وبعض تاريخ التصفح إذا كنت تستخدم Google Docs. إذا تم محو تاريخ التصفح، فهذا يعني أيضا أن شخصا ما حاول ربما مسح الآثار
- من غير المرجح أن يتم تثبيت أي برامج ضارة أثناء المداهمة، ولكن إذا كنت قلقا بشأن ذلك، فاستشر متخصصا في فحص البرامج الضارة

س6 - كيف ينبغي للمنظمة التأكد من عدم تعرضهم لمزيد من المخاطر بسبب مداهمة الشرطة هذه؟

- تغيير كلمات السر، فقط للاحتياط
- التحدث مع محامي حول ما كان مسموحا للشرطة بالوصول إليه وما كان غير مسموح لها أثناء المداهمة
- إذا كانوا يستخدمون أسماء مرموزة أو مستعارة من أجل أبحاثهم، فيجب تغييرها

بعد بضعة أسابيع، اتصل رئيس تحرير غرفة الأخبار بجميع الصحفيين والموظفين معا. إنهم يريدون فهم التهديدات المماثلة التي قد تواجهها غرفة الأخبار في المستقبل.

س 7 - فيما يتعلق بنمذجة التهديدات والأمن الرقمي، ما الذي يعتبره الأفراد والمنظمات تهديدات قد يواجهونها؟

- طرح أسئلة نمذَجة التهديدات القياسية: ما هي المعلومات التي لديهم، ومن قد يكون مهتما بالوصول إليها، وما هي العواقب إذا نجح خصومهم بذلك
- عند إدراج الخصوم، وجب التفكير في الدوافع (ماذا يرغبون في القيام به ولماذا) والقدرات (ما الذي يمكنهم فعله بالضبط، وما هي الوسائل التقنية والقانونية والتنظيمية والمالية التي يحظون بها؟)

السيناريو 5: دخول السلطات لمنزل صحفي

الهدف

إكساب الصحفيين المهارات النظرية والتقنية لضمان أفضل أمان رقمي ممكن في بيئتهم المنزلية

أهداف التعلم

- التعرف على كيفية تأمين الأجهزة الرقمية الموجودة في المنزل
- تطبيق إجراءات وقائية حول دفاتر الملاحظات الورقية
- البدء بحذف الملفات عن بعد وإيجابيات وسلبيات القيام بذلك.
- تقييد الوصول إلى المعلومات التي تعرضت للخطر
- التحضير لدخول السلطات لمنزل صحفي
- جعل المشاركين يفكرون في الأمن التنظيمي والمجتمعي، وتحديدا كيفية العمل مع رؤساء التحرير والمديرين والمحامين أثناء المواقف العصيبة، وتحديد أي سؤال يجب رفعه إلى مَن بالضبط

المهارات والسلوكات التي يجب التدرب عليها قبل أو بعد تمرين المحاكاة

- استخدام أداة مثل VeraCrypt أو ما يشبهها لتعمية البيانات الموجودة على الأقراص الصلبة والأقراص الخارجية
- نمذَجة التهديدات، وتحديدا ما يتعلق بالتعامل مع السلطات ومداهمة المنازل: كيفية تقييم المخاطر، والاستعداد لها، واستخلاص العِبر بعد حدوثها
- تفعيل الأدوات مثل أداة شركة آبل « Find My » أو الأداة « Samsung Find » في نظام أندرويد، والتي يمكن استخدامها لقفل الأجهزة أو مسح بياناتها عن بعد
- استخدام الإعدادات داخل Microsoft Office وجوجل درايف Google Drive لمعرفة آخر الملفات التي تم الوصول إليها ومتى
- (سلوك متقدم) إذا كانت للمؤسسة سجلات وصول شاملة من خلال اشتراك جوجل درايف Google Drive المميز أو اشتراك O365، فيمكن الوصول إلى هذه السجلات والعمل بها
- الاطلاع على سجلات البحث وسجلات الوصول إلى الملفات في متصفحات الانترنت وأنظمة التشغيل الشائعة

السيناريو

قبل 5 أشهر وبعد الانتخابات الوطنية، بدأت الحكومة الجديدة التي تتولى السلطة بتوجيه السلطات للحد من الحريات الصحفية، وقامت السلطات بمداهمة منازل ثلاثة صحفيين بارزين في العاصمة. استجابةً لذلك، اجتمعت « سارة » وبعض الزملاء معا وناقشوا طرقا لحماية أنفسهم ومعلوماتهم في حال مواجهة سيناريو مشابه.

س 1 - ما هي بعض الأشياء التي يجب على الصحفي الأخذ بعين الإعتبار عند اتخاذه قرار تخزين معلومات في منزله؟

- تخزين الأجهزة الموجودة في المنزل في مكان آمن
- تعمية وحماية كلمات سر جميع الأجهزة
- عدم إدراج معلومات المصادر الحساسة مثل أسمائهم في المستندات
- احتفظ بجرد لماهية ومكان الاحتفاظ بالمعلومات (ولكن احتفظ بهذا أيضا في مكان آمن!)
- المعلومات غير الرقمية: احذر من النسخ الملموسة
- عدم الاحتفاظ بأي شيء حساس في المنزل إذا كان ممكنا
- اتباع القوانين المحلية وكذلك سياسات المنظمة

- كن على دراية بالعواقب القانونية لتخزين المعلومات الحساسة في منزلك بدلا من مكتبك.
- التفكير في من يمكنه الوصول إلى منزلك وأجهزتك

س 2 (اختياري) - ما هي بعض أفضل الممارسات حول تخزين دفاتر الملاحظات الورقية في المنزل؟

- ضع في اعتبارك تدمير ما لا تحتاج إليه
- لا تحتفظ بجميع الملاحظات في مكان واحد – معلومات أقل للوصول إليها بسهولة
- إخفاء دفاتر الملاحظات
- خزينة، قفل ومفتاح، حافظ عليها آمنة!
- ما هو مستوى حساسية المعلومات التي يجب الاحتفاظ بها في المنزل؟
- استخدام الاختصارات والاختزالات – تكون منطقية لك فقط

س 3 - ما هي التدابير التي يمكن اتخاذها لتأمين الأجهزة الإلكترونية ما أمكن (الحواسيب والأقراص الصلبة ومفاتيح USB إلخ.)

- التعمية
- الحماية بكلمة السر
- النسخ الاحتياطي للبيانات خارج الموقع
- التفكير في التخلص من الأجهزة القديمة بشكل آمن، خاصة تلك التي لم تعد قيد الاستخدام

غادرت « سارة » اليوم منزلها في التاسعة صباحا لشرب قهوة وشراء البقالة. عندما عادت بعد ساعة كان باب شقتها مفتوحا. دخلت « سارة » شقتها لتجد رجلين يبحثان في مكتبها وغرفة نومها. كان أحد الرجال يقرأ دفتر ملاحظات « سارة » بينما كان الآخر يحمل حقيبة بداخلها حاسوب « سارة ». ترى « سارة » أن مفاتيح USB والأقراص الصلبة الخارجية التي كانت على مكتبها هي الآن مفقودة. يرتدي الرجلان ملابس مدنية، لكن « سارة » تفترض أنهما يعملان لحساب الحكومة بطريقة ما.

الخيار 1 - تتحدث « سارة » مع الرجلين لفترة وجيزة وتتمكن من مغادرة منزلها بأمان. تمشي إلى منزل صديق قريب لها.

س 4 (اختياري) - علمًا أن بعض معلومات « سارة » قد تم اختراقها، خاصة من دفتر ملاحظاتها الورقي، من ينبغي إبلاغه بهذا الحادث؟

- إبلاغ رئيس التحرير ومحامي غرفة التحرير
- قبل الاتصال بأي مصادر قد تكون مذكورة في دفتر الملاحظات، يجب التحدث أولا إلى رئيس التحرير وغرفة الأخبار على نطاق أوسع، وكذلك إلى المتخصصين في المجال الأمني (إذا تم ذكر المصادر بأسماء مستعارة فقط ولكنهم تلقوا مكالمة في اليوم التالي، فقد يسمح ذلك للأجهزة الأمنية بربط هوية المصادر بالأسماء المستعارة). قد يكون من الحكمة عدم التواصل معهم في البداية

س 5 - ما الذي يمكن أن تفعله « سارة » لمنع الوصول إلى معلوماتها الرقمية بينما لا يزال الرجلان داخل شقتها؟

- فعل كل ما في وسعك لاتباع القانون المحلي
- الإصرار على أن تتبع السلطات القانون المحلي أيضا (على سبيل المثال السماح بالتصوير ووجود الشاهد إلخ.)
- تقنيات تخفيف التصعيد
- اكتشاف من هما وما إذا كان لديهما تفويض
- تقييم الوضع من أجل سلامتها الشخصية
- طلب المشورة القانونية، الاتصال بغرفة الأخبار
- تقديم حسابات ووثائق مزورة (قد يتطلب ذلك بعض التحضير)
- تحريف المسار

الخيار 2 - « سارة » غير قادرة على مغادرة شقتها. يطلب منها الرجلان الجلوس ويطالبان منها إعطائهما كلمات السر لحاسوبها ولمفاتيح USB الخاصة بها. يهددانها بأخذها إلى مركز الشرطة إذا لم تقدم هذه المعلومات. تطلب « سارة » منهما إذا كان لديهما أمرا قضائيا لكنهما لا يقدمانه لها.

س 6 - علمًا أن لديها معلومات حساسة على حاسوبها، بما في ذلك تحديد هوية المصادر السرية، ما هي الخيارات التي تمتلكها « سارة » في هذه الحالة؟

- تقييم نقط الضعف وإعطاء الأولوية للقضايا الأكثر أهمية
- تسجيل الخروج عن بعد والحذف عن بعد للحسابات الحساسة
- تحديد كافة المعلومات المُخزَّنة في المنزل
- ضع في اعتبارك إيجابيات وسلبيات إبلاغ أعضاء الفريق والمصادر الذين قد يكونون في خطر. ربما اتخذْ هذا القرار بدعم من غرفة الأخبار.
- إمكانية حذف الملفات عن بعد

س 7 - تتوفر « سارة » على برنامج حذف ملفات عن بعد تم إعداده على حاسوبها. ما الذي يجب عليها مراعاته قبل حذف ملفات الحاسوب؟

- يمكن أن تكون مشكلة قانونية – إعاقة سير العدالة
- التفكير في التداعيات المحتملة، والتحدث مع محام أولاً إذا أمكن
- إذا لم يكن لدى « سارة » دليل على أن هؤلاء الأشخاص ينتمون إلى السلطات الأمنية، وكانوا يبدون وكأنهم دخلاء عاديين أو من قوات أمنية غير تابعة للدولة، فإن هذا يغير المجال القانوني ومدى التهديد

س 8 (اختياري) - علمًا أن بعض معلوماتها قد تعرضت للخطر، من يجب أن تبلغ « سارة » بهذا الحادث؟ هل يجب عليها اتباع تراتُبية معينة للأشخاص المعنيين بالتبليغ؟

- رئيس تحرير غرفة الأخبار
- أمن غرفة الأخبار وفريق تكنولوجيا المعلومات
- الفريق القانوني لغرفة الأخبار
- الوضع في الاعتبار الاتصال بالمصادر
- إذا كان هناك صحفي مستقل، يجب التفكير في مشاركة الموقف مع صحفيين مستقلين آخرين.

ترفض « سارة » في النهاية تقديم كلمات السر لأجهزتها. بعد البحث في شقتها لمدة 10 دقائق أخرى، غادر الرجلان ومعهما حاسوب « سارة » ومفاتيح USB ودفتر ملاحظاتها الورقي.

تمكنت « سارة » الآن من الوصول إلى شقتها مرة أخرى. ترى أن أحد حاسوبَيها قد تُرك مع أحد مفاتيح USB الخاصة بها. تم أخذ جميع دفاتر ملاحظاتها الورقية من الشقة.

س 9 - ما الذي يجب أن تفعله « سارة » الآن لضمان عدم تعرض معلوماتها وأمنها لمزيد من الخطر نتيجة لتصرفات الرجلين أثناء وجودهما في شقتها؟

- ربما قام هؤلاء بتثبيت برامج ضارة على أجهزة « سارة »؛ قد يكون من الجيد إرسال هذه الأجهزة إلى متخصص في التحقيق الجنائي الرقمي
- سؤال منظمتها عن نوع الدعم الذي يمكن أن تتلقاه منهم
- الوضع بعين الاعتبار إمكانية وضع أجهزة تنصت في شقتها
- التحدث إلى منظمتها وإلى المستشارين القانونيين والمستشارين الأمنيين، حول ما إذا كان معقولًا التحدث علنا عن المداهمة من منظور السلامة والأمن أم عدم التحدث عن ذلك

س 10 (اختياري) - بغض النظر عن جوانب الأمن الرقمي لهذا السيناريو، ما هي الاحتياطات والاستجابات الأخرى التي كان من الممكن أن تتخذها « سارة » للحفاظ على أمنها وأمان معلوماتها؟

- التعرف أكثر على كيفية عمل قوات حفظ الأمن في البلاد، وإذا كانت هناك مجموعات خارجة عن سلطة قوات حفظ الأمن تقوم بترهيب الصحفيين
- الاستعداد مع المحامين ورؤساء التحرير حول أفضل السبل للرد على مداهمات المنازل
- عدم الاحتفاظ بالمعلومات الحساسة في المنزل إذا كان هناك احتمال مداهمة للمنازل