
دليل السلامة الرقمية
للمجتمعات الكويرية المصرية
الإصدار ١,٠
أطياف
mobaderon
مبادرون

دليـل الـسـلامـة الرقميـة للمجتمعات الكويرية المصرية

السياق الأمني والمجتمعي

يحتاج الجميع لمعرفة أساسيات السلامة الرقمية لتجنب المخاطر المحتملة، لكن تكون المعرفة بممارسات وأدوات السلامة الرقمية أمرا حرجا جدا بالنسبة لأفراد المجتمعات الكويرية في مصر، حيث تكون المخاطر الناجمة عن التعامل مع الفضاء الرقمي أكثر فداحة لدى الكويريين من غيرهم، وكذلك يتعرض الكويريون إلى تهديدات ومخاطر لا يتعرض لها غيرهم من الأساس، ويرجع ذلك إلى الوضع القانوني والاجتماعي الذي يهدد الكويريين على نحو خاص. ويمكن اعتبار جميع مستخدمي الإنترنت عرضة للمخاطر الرقمية لكن بدرجات متفاوتة، ففئة النساء في مصر، وفي العالم عموما، أكثر عرضة لتلك المخاطر من الرجال، وأفراد المجتمعات الكويرية في مصر كذلك أكثر عرضة لها من غير الكويريين، بل وإن الفئات المختلفة داخل المجتمعات الكويرية المصرية تتفاوت في المخاطر التي يتعرض لها أفرادها، فغالبا ما تكون النساء الترانس أكثر الفئات المتأثرة، بينما تتأثر النساء المثليات بدرجة أقل، وهو ما لا يعني أنهن لسن عرضة للخطر، فالجميع مستهدف، لكن لا مساواة في الظلم. ولهذا يجب الفصل بين الفئات المختلفة داخل المجتمعات الكويرية المصرية عند النظر إلى واقعها والمخاطر التي تواجهها، بل ويجب وضع عوامل أخرى في الاعتبار مثل التعليم والطبقة الاجتماعية ومكان السكن، لكن سنلجأ عند الحديث عن المجتمعات الكويرية في مصر إلى تقسيمها إلى فئات محددة تشترك في أشكال العنف والمخاطر القانونية والتمييز المجتمعي الواقعة عليها.

تواجه النساء الترانس وغير النمطيات/يين تحديات هائلة في المجتمع المصري، ترتبط بشكل أساسي باختلاف المعلومات الموجودة عن الجنس في البطاقة عن المظهر مما قد يعرضهن/م إلى عنف من قبل المجتمع ومشاكل قانونية وأشكالا عديدة من التمييز في التعليم والعمل والرعاية الصحية. يواجه المثليون كذلك ملاحقة الشرطة والعصابات وتواجه المثليات أحيانا الاغتصاب التصحيحي، كما يتعرض الأشخاص من مختلف التوجهات الجنسية والهويات الجندرية غير النمطية إلى عنف الأسرة والمجتمع وأحيانا إلى عنف طبي على شكل ممارسات العلاج التحويلي.

أبرز التهديدات

يحتوي هذا الجزء وصفا لممارسات عنيفة

تصيد الشرطة

تستخدم الشرطة المصرية تطبيقات المواعدة المنتشرة بين أفراد المجتمعات الكويرية للإيقاع بالرجال المثليين والنساء الترانس تحديدا وتوجه تهمًا أبرزها اعتياد ممارسة الفجور، وتبرع مباحث الآداب في تصيد المثليين والترانس عبر تطبيقات المواعدة من خلال الاتفاق على الالتقاء بالشخص في مكان محدد ثم تأتي الشرطة لإلقاء القبض عليه ومصادرة الهاتف في العادة، وقد كانت الشرطة في البداية تعمد إلى إثبات التهم باستخدام المحادثات التي يتفق فيها أفراد الشرطة مع الشخص على اللقاء، لكن في العديد من القضايا الأخيرة، صارت الشرطة تزيف محادثات لاستخدامها في إثبات التهمة، وفي عدة حالات كانت الشرطة تخدع المقبوض عليهم بإقناعهم بإمكانية إخلاء سبيلهم شرط مساعدة الشرطة في الإيقاع بآخرين لكن استجابة المقبوض عليهم لهذه الخدع في الواقع تزيد القضية تعقيدا عبر تحويلها إلى تهمة "تكوين شبكة لممارسة الفجور" في كثير من الأحيان.

العصابات

تنشط الكثير من العصابات في مصر للإيقاع بأفراد المجتمعات الكويرية، وعلى عكس الشرطة، فإن استهداف العصابات لا يقتصر على الرجال المثليين والنساء الترانس فحسب، بل يمتد إلى العديد من الفئات الأخرى، وتختلف كذلك أهداف تلك العصابات من تصيد أفراد المجتمعات الكويرية، فبعض العصابات تلجأ للابتزاز من أجل الحصول على المال، وبعضها يفعل ذلك بدافع أيديولوجي، وتتنوع أشكال العنف التي تمارسها العصابات بين التعدي بالضرب والاغتصاب والسرقة والتهديد وغير ذلك.

التهديد والتشهير

يتعرض الكثير من أفراد المجتمعات الكويرية للتهديد بواسطة أشخاص يتمكنون من الحصول على دليل على الهوية الكويرية، فيقومون إما بابتزاز أفراد المجتمع الكويري وتهديدهم

بفضحهم أمام أسرهم أو في أماكن عملهم أو دراستهم أو غيرها، ويقوم كذلك بعض المجموعات بالتشهير بأفراد المجتمعات الكويرية على منصات مثل إكس (تويتر سابقا) أو فيسبوك أو تليجرام، ويصل الأمر إلى محاولة جمع أكبر قدر من البيانات عن أولئك الأشخاص من أجل إلحاق الضرر بهم والتحريض ضدهم.

خطابات الكراهية

تعد خطابات الكراهية أكثر أشكال العنف انتشارا ووضوحا ضد المجتمعات الكويرية في مصر، ورغم النظر إليها على أنها تهديد أقل خطرا من التهديدات الأخرى، إلا أن انتشار خطابات الكراهية بشكل واسع على مواقع التواصل الاجتماعي يجعل من مجرد تصفح تلك المواقع تجربة صعبة لأفراد المجتمعات الكويرية، ويعاني الأفراد الكويريون من آثار انتشار خطابات الكراهية دون التحدث كثيرا عنها بصفتها أكثر التهديدات شيوعا والتي تؤثر على الصحة النفسية لعدد كبير من أفراد المجتمعات الكويرية.

الممارسات

حماية الهوية

لحماية هوياتنا عند استخدام الإنترنت نحاول تجنب ترك آثار تسمح للآخرين بتتبعنا، فنتجنب تسجيل الحسابات بأرقام هواتفنا المرتبطة ببطاقاتنا الشخصية، ونتجنب الإفصاح عن الكثير من المعلومات الشخصية أو تركها متاحة للعلن على منصات التواصل الاجتماعي، ولا تقتصر حماية الهوية على عدم الإفصاح عنها بشكل مباشر، فيمكن كذلك حمايتها عن طريق عدم ترك آثار تدل على الهوية الجنسية أو الجندرية في ملفات الهاتف أو الملاحظات أو تاريخ التصفح، ويجب ألا نخجل من الإصرار على عدم رغبتنا بمشاركة معلومات شخصية، لأن أماننا يجب أن يأتي في المرتبة الأولى دوما.

تأمين الهاتف

يمكن للهواتف في العادة الإفصاح عن الهويات الكويرية أكثر من أي شيء آخر بسبب احتوائها تطبيقات المواعدة وتطبيقات التراسل وتطبيقات التواصل الاجتماعي والمتصفحات (وبالتالي سجلات التصفح) وجهات الاتصال وسجل المكالمات والصور ومقاطع الفيديو، لهذا يجب تأمين الهواتف ومحتوياتها بحرص شديد، فيكون قفل الهاتف باستخدام كلمة سر (بدلا من البصمة أو الوجه أو النمط) لأن كلمة السر المعقدة هي أصعب الأشياء في تجاوزها عبر التلاعب أو اختراقها أو، في أسوأ الأحوال، إجبار المستخدم على تجاوزها، وتكون كلمة السر الجيدة معقدة تتكون من حروف كبيرة وصغيرة ورموز وأرقام، ويفضل إغلاق أكبر عدد من محتويات الهاتف أو وضع حواجز أمام الوصول إليها بشكل منفصل، فالكثير من التطبيقات تسمح بإغلاقها بشكل منفصل أو إغلاق أجزاء منها مثل تطبيق واتساب الذي يسمح بقفل محادثات معينة من اختيار المستخدم، ويمكن الاحتفاظ الصور في تطبيق لحفظ الملفات بشكل مشفر مثل Tella. وكلما تمكن المستخدم من وضع عراقيل أو حواجز أمام الوصول إلى محتويات الهاتف زادت قدرته على حماية هويته من أي شخص غير مرغوب فيه.

تطبيقات المواعدة

تعج تطبيقات المواعدة بأفراد الشرطة وأفراد العصابات إلى جانب الأشخاص الجيدين، وللأسف لا توجد طريقة سهلة للتمييز بينهم، لكن بشكل عام هناك بضعة أشياء تجعلنا

نشك في نوايا من نحادثهم عبر تطبيقات المواعدة مثل عرض الأموال (لأن هذا يدعم تهمة الفجور في القانون المصري للرجال المثليين والنساء الترانس وكثيرا ما يسعى أفراد الشرطة إلى إثباته)، ومثل الرغبة السريعة في المقابلة ومثل الاستجداء أو لعب دور الضحية، ويفضل عدم تقديم أي معلومات شخصية مهمة يمكن استخدامها للوصول إلينا وإمضاء وقت كاف في محادثة الشخص للتعرف عليه قبل لقائه، ويمكن كذلك قبل لقاء أي شخص مراسلة أحد الأصدقاء الموثوقين وإعطائه تفاصيل اللقاء مثل العنوان وغيره ليتمكن من التصرف في حالات الخطر، وعند استخدام تطبيقات المواعدة يجب وضع صحتنا النفسية في الاعتبار وعدم الاستجابة لأي ضغوط لدفعنا لفعل أو قول أي شيء لسنا واثقين من رغبتنا فيه، ويجب أن لا نخجل من رفض أي شيء غير مريح بالنسبة لنا من حظر أو الإبلاغ عن أي شخص يتسبب بالأذى.

الاتصال بالإنترنت

يمكن لشركات الاتصالات وأصحاب شبكات الواي فاي التي نتصل بها رؤية المواقع التي نزورها، لذا يجب استخدام شبكة خاصة افتراضية VPN لتشفير اتصالنا بالإنترنت وتفعيل خيارات الجدار الناري بها، وتساعدنا شبكات VPN في:

- منع شركات الاتصالات من معرفة المواقع التي نزورها
- منع أصحاب شبكات الواي فاي من التجسس علينا
- منع المواقع التي نزورها من معرفة موقعنا بناء على عنوان الـ IP (لكن هذا لن يمنعها من معرفة عنواننا الحقيقي إذا أعطيناها صلاحية الوصول إلى خدمة ال GPS)

التصفح

عند تصفح الإنترنت يمكن تشغيل وضع التصفح الخفي حتى لا يحتفظ المتصفح بسجل المواقع التي تمت زيارتها، ويجب الحرص على تجنب الضغط على الروابط غير الموثوقة وتحميل الملفات من مصادر غير رسمية فالتصيد عبر مواقع الإنترنت شائع جدا وكذلك البرمجيات الخبيثة على مواقع التحميل غير الرسمية، ويُفضَّل استخدام متصفحات أكثر احتراما للخصوصية مثل Firefox أو Brave مع تثبيت إضافات تعزز الحماية (على نسخة الحاسب) مثل uBlock origin.

الحسابات

حماية حساباتنا تكون عبر اختيار كلمات سر قوية يزيد عدد حروفها عن 14 حرفا وتحتوي حروفا كبيرة وصغيرة ورموز وأرقام، وعبر تفعيل المصادقة الثنائية، وهي إضافة طريقة أخرى للتحقق من الهوية بعد كلمة السر، وأشهر طريقة لفعل ذلك هي باستخدام أكواد التحقق من تطبيقات التحقق بخطوتين (وهناك أمثلة في قسم الأدوات)، فإذا تم تفعيل التحقق بخطوتين يكون الحساب محميا بطبقتين؛ الأولى هي كلمة السر، وفي حالة تمكن المهاجم من الحصول عليها يجب عليه تجاوز الطبقة الثانية حتى يصل إلى الحساب.

منصات التواصل الاجتماعي

مشكلة منصات التواصل الاجتماعي تكمن في كونها مصممة لجعل المستخدم يشارك أكبر قدر من المعلومات عن نفسه وهذا ما يعرض أفراد المجتمعات الكويرية في مصر إلى مخاطر كشف الهوية والتصيد. كلما كان المستخدم حريصا في المعلومات التي يشاركها زادت فرصته في حماية نفسه من تلك المخاطر، وتوفر معظم منصات التواصل الاجتماعي الآن خيار تحديد خصوصية المحتوى الذي ينشره المستخدم، ويُفضل ضبط الحسابات أو المنشورات على ألا تظهر سوى للأشخاص الموثوق فيهم ومراجعة قوائم الأصدقاء كل فترة للتأكد من خلوها من الحسابات غير الموثوق فيها والحسابات المهجورة.

التراسل

العامل الأول في أمان المراسلات هي عدم التحدث سوى إلى الأشخاص الذين نثق فيهم، والحذر الشديد مع أولئك الذين لا نعرفهم جيدا بعد، وحتى من نثق فيهم قد تقع هواتفهم في الأيادي الخطأ، لهذا يفضل اتخاذ احتياطات الأمان في كل الأحوال. والعامل الثاني هو استخدام تطبيقات تراسل توفر قدرا جيدا من الخصوصية والأمان، وعند اتخاذ قرار بشأن تطبيقات التراسل التي سنستخدمها يجب وضع بعض العوامل بعين الاعتبار، بالإضافة إلى احتياجاتنا الأخرى مثل عدد الأصدقاء على هذا التطبيق. التشفير الافتراضي يعني أن المحادثات بين الأطراف تستخدم تشفيرا قويا بشكل تلقائي، وقد صارت معظم التطبيقات توفر تلك الميزة لكن ليس كلها توفرها بشكل افتراضي. والشفافية الكاملة تعني أن بوسع أي شخص التحقق من الكود المصدري للتطبيق وطريقة عمله بحيث لا يمكن للتطبيق اتخاذ أي

قرارات تصميم أو اتخاذ أي إجراءات غير معلنة وهو ما يضمن التزام التطبيق بمعايير جيدة. وكلما كان التطبيق يجمع عن المستخدم بيانات أقل كان ذلك أفضل، فالبيانات يتم استخدامها في العادة لجمع أكبر قدر من المعلومات عن المستخدم، وفي أفضل الأحوال يتم استخدام تلك البيانات لاستهدافه بإعلانات موجهة. عند التسجيل لاستخدام أحد تطبيقات التراسل تطلب معظم تلك التطبيقات رقم الهاتف وتتحقق من ملكية صاحب الرقم له، وهذا من ناحية يضمن عدم امتلاك شخص واحد عددا كبيرا من الحسابات في نفس الوقت وإساءة استخدام الخدمة، لكنه من ناحية أخرى يعطي الخدمة وسيلة للتعرف على هوية المستخدم، وفي معظم الأحيان كذلك يعطي المستخدمين الآخرين وسيلة للبحث عن المستخدم باستخدام رقم الهاتف، وإن كانت بعض التطبيقات تقدم خيارا لمنع المستخدمين الآخرين من العثور على الحساب عند البحث باستخدام رقم الهاتف.

من أهم ما يجب البحث عنه في تطبيقات التراسل هي مزايا وخصائص الأمان التي يوفرها مثل المحادثات المؤقتة والرسائل ذاتية التدمير والصور التي لا يمكن عرضها سوى مرة واحدة مع منع التقاط صورة للشاشة، وقد صارت تلك المزايا متوفرة في معظم تطبيقات التراسل الشهيرة، وتسعى تلك الخصائص لتوفير الحماية للمستخدم من الطرف الآخر الذي يراسله، وهنا يجب التمييز بين قدرتنا على حماية أنفسنا ممن نراسلهم وبين قدرتنا على حماية أنفسنا من الأطراف الأخرى مثل شركات الاتصالات وخدمات جمع البيانات والشركات المالكة للتطبيقات أنفسها. فخصائص الأمان المتوفرة في معظم التطبيقات قد تساهم في حمايتنا ممن نراسلهم لكنها لا تعني حمايتنا من الأطراف الأخرى، ولهذا يجب علينا كذلك الاهتمام بالمعايير الأخرى مثل التشفير والشفافية وعدم جمع البيانات.

	تشفير افتراضي	شفافية كاملة	لا يجمع البيانات	يمكنه إخفاء رقم الهاتف	خصائص أمان
سيجنال	✅	✅	✅	⛔[1]	✅
واير	✅	✅	⛔	✅	✅
واتساب	✅	⛔	⛔	⛔	✅

[1] سيصبح إخفاء رقم الهاتف متاحا في النسخ القادمة من سيجنال

	تشفير افتراضي	شفافية كاملة	لا يجمع البيانات	يمكنه إخفاء رقم الهاتف	خصائص أمان
تليجرام	⛔	⛔	⛔	✅	✅
إنستجرام	⛔	⛔	⛔	✅	✅
مسنجر	ليس للكل	⛔	⛔	✅	قليلة
سنابشات	⛔	⛔	⛔	✅	✅

نخلص إلى أن سيجنال ووایر من أفضل الخيارات من حيث الخصوصية والأمان، بينما لا توفر معظم المنصات الشهيرة ذات القدر من الخصوصية، لكن حتى عند اضطرارنا إلى استخدامها يجب تفعيل أكبر قدر من خصائص الأمان المتاحة فيها.

تأمين الملفات

يمكن تأمين الملفات باستخدام برامج وتطبيقات التشفير على الهاتف والحاسوب، وتحتوي بعض الهواتف طرقا مدمجة لتشفير أو قفل الملفات بكلمة سر، ويمكن في نظام ويندوز تشفير قسم محدد من مساحة التخزين باستخدام BitLocker المدمج في بعض نسخ ويندوز، أو استخدام برمجيات مثل VeraCrypt أو Picocrypt وعلى الهاتف باستخدام تطبيق Tella (المزيد من التفاصيل في قسم الأدوات).

البيانات الوصفية

البيانات الوصفية هي معلومات يتم تخزينها مع الصور التي نلتقطها وقد تتضمن تفاصيل كثيرة عن ظروف التقاط الصورة مثل:

- وقت التقاط الصورة
- إحداثيات الموقع الجغرافي الدقيقة لمكان التقاط الصورة
- نوع وإصدار الجهاز أو الكاميرا المستخدمة لالتقاط الصورة

- الشركة المصنعة للكاميرا
- تفاصيل إعدادات الكاميرا والعدسة

بالإضافة إلى العديد من التفاصيل الأخرى والتي تختلف من صورة إلى أخرى حسب الجهاز والإعدادات والمستشعرات المفعلة وقت التقاط الصورة. ويجب إخفاء البيانات الوصفية من الصور قبل إرسالها إلى الآخرين.

قائمة الأدوات

❖ تعمية الاتصال والشبكة الخاصة الافتراضية

TOR	1.1.1.1	BeePass

تساعد الشبكات الخاصة الافتراضية في منع شركات الاتصالات وأصحاب شبكات الواي فاي التي نتصل بها من رؤية المواقع التي نزورها، ويمكن استخدام BeePass أو 1.1.1.1 لهذا الغرض، أما TOR فهو متصفح يتصل بالإنترنت عبر نظام توجيه يوفر تشفيرا قويا لكن خصائصه الأمنية القوية تجعله أبطأ وتجعل بعض المواقع لا تعمل عليه بسلاسة.

❖ المتصفح

Brave	Firefox

أهم المتصفحات التي توفر مزايا خصوصية جيدة هي Firefox و Brave، ويتميز Firefox على الهاتف بقدرته على تفعيل الإضافات مثل uBlock origin على عكس متصفحات الهواتف الشهيرة الأخرى، ويتميز Firefox على الحواسب أيضا بقدرته على صنع حاويات تعزل المواقع التي يزورها المستخدم عن بعضها.

❖ تطبيقات التحقق بخطوتين

ente Auth	Google Authenticator

عند تفعيل التحقق بخطوتين في الحسابات الإلكترونية يجب ربطه بأحد تطبيقات التحقق بخطوتين مثل Google Authenticator و ente Auth والذي يقوم بإصدار كود متغير كل 30 ثانية يجب على المستخدم إدخاله بعد كلمة السر عند تسجيل الدخول، ويتميز تطبيق Google Authenticator بمزامنة الأكواد باستخدام حساب جوجل، ويتميز تطبيق ente Auth بقدرته أيضا على عرض أكواد التحقق على سطح المكتب.

❖ **مدير كلمات السر**

Bitwarden

يساعد Bitwarden في إنشاء وحفظ كلمات السر المعقدة بحيث يمكن للمستخدم إنشاء كلمات سر قوية دون أن يضطر إلى تذكرها، ويعمل Bitwarden كتطبيق على معظم الأنظمة ويعمل أيضا كإضافة على المتصفحات على أجهزة الكمبيوتر.

❖ **تطبيقات التراسل**

Wire	Signal

يتميز سيجنال بموثوقيته وسرعته والشفافية وخصائص الأمان القوية التي يوفرها لكن أهم عيوبه هو ظهور رقم هاتف المستخدم للآخرين بينما يتميز واير بإمكانية التسجيل باستخدام البريد الإلكتروني وعدم إظهاره رقم الهاتف للآخرين.

❖ **تشفير الملفات على الهاتف**

Tella

يعمل Tella كخزنة مشفرة يمكن إغلاقها بكلمة سر أو رمز أو نمط ليحتفظ المستخدم بداخله بالملفات الحساسة، ويمكن التقاط الصور وتسجيل الصوت بداخل Tella حتى يتم إنشاء الملفات بداخله من البداية أو جلب الملفات من خارجه إليه.

❖ **تشفير الملفات على الحاسب**

Picocrypt	VeraCrypt

يساعد VeraCrypt في إعداد مجلد مشفر بكلمة سر يكون على شكل ملف يمكن فتحه وإغلاقه باستخدام البرنامج في أي وقت، ويمكنه كذلك تشفير أجهزة التخزين ووحدات التخزين في القرص الصلب. ويعتبر Picocrypt أبسط وأسهل في الاستخدام حيث يمكن استخدامه لإنشاء نسخ مشفرة من الملفات أو المجلدات ومن ثم فك تشفير تلك النسخ المشفرة باستخدام نفس كلمة السر المستخدمة عند إنشائها.

❖ **تصوير المحتوى الحساس**

Obscura Cam (Android)

يساعد هذا التطبيق على التقاط الصور مع تقديم خصائص تساعد في تمويه التفاصيل غير المرغوب فيها وهو لا يحتفظ بالبيانات الوصفية للصور الملتقطة من خلاله.

❖ **محو البيانات الوصفية**

Metapho (iOS)	**Exif Eraser** (Android)

لمحو البيانات الوصفية للصور قبل إرسالها على الهاتف يمكن استخدام تطبيق Exif Eraser على الهواتف التي تعمل بنظام أندرويد وتطبيق Metapho على هواتف أيفون.

تمارين

قد يُذكر هذا الجزء بعض القراء بأحداث أليمة

التوقيف بواسطة الشرطة

كانت سارة، وهي عابرة جندريا لم تغير أوراقها الرسمية حتى الآن، عائدة من منزل أحد الأصدقاء وكانت تمشي في الشارع حين استوقفها رجال الأمن. يحتوي هاتفها على صور خاصة لها وعلى محادثات بينها وبين العديد من أصدقائها الكويريين الآخرين.

فكروا في إجابات للأسئلة التالية:

ماذا كان بوسع سارة فعله قبل حدوث هذا الموقف لتجنب وقوع أكبر عدد من الأضرار؟

في لحظة الاستيقاف، ما الذي يجب على سارة فعله؟

شك الأهل

رأت والدة عزيز بالصدفة إشعارا برسالة دفعتها للشك بميول ابنها الجنسية، مما دفعها إلى فحص الهاتف بحثا عن أدلة أخرى كالمحادثات والصور ومقاطع الفيديو وسجل التصفح.

فكروا في إجابات للأسئلة التالية:

ماذا كان بوسع عزيز فعله لمنع حدوث هذا الموقف من الأساس؟ كيف كان بوسعه حماية كل نوع من الأدلة المحتملة؟

عند انكشاف دليل معين، ما الذي يمكن لعزيز فعله؟

ابتزاز باستخدام النودز

أثناء المراسلة بين شفيق وأحد الأشخاص على أحد تطبيقات المواعدة قام الاثنان بتبادل المعلومات الخاصة والصور الحميمية لنفسيهما، وبعد ذلك بدأت نبرة الشخص الآخر تتغير وأعاد إرسال إحدى صور شفيق العارية له مرة أخرى موضحا له أن تلك الصورة تحمل وجهه وأنه تمكن عبر حسابه من الوصول إلى أقاربه وطلب منه دفع مبلغ من المال حتى يحذف الصورة وإلا فسيرسلها إلى أقاربه.

فكروا في إجابات للأسئلة التالية:

ما الاحتياطات التي كان على شفيق اتخاذها في مراسلة ذلك الشخص؟

هل يجب أن يقوم شفيق بدفع المبلغ؟ وهل سيقوم في تلك الحالة بضمان عدم تكرار تهديد الشخص له مرة أخرى؟

ما التصرف الذي يجب على شفيق القيام به في هذا الموقف؟