KING HUSSEIN FOUNDATION مؤسسة الملك الحسين
مركز المعلومات والبحوث
INFORMATION AND RESEARCH CENTER

دليل إرشادي تفاعلي للحد من العنف الرقمي

للأساتذة الجامعيين

قائـــمة المحتويـــات

مركز المعلومات والبحوث – مؤسسة الملك الحسين IRCKHF

يعتبر مركز المعلومات والبحوث - مؤسسة الملك الحسين والذي تأسس في عام ١٩٩٥ بمثابة عامل محفّز للتغير الاجتماعي-الاقتصادي من خلال إجراء البحوث الشاملة، حملات كسب التأييد القائمة على الأدلة، ونشر المعرفة مع الممارسين وصانعي السياسات والمجتمع المدني حول قضايا حقوق الإنسان، والمساواة بين الجنسين والعدالة الاجتماعية ، وتمكين المجتمع المدني.

مؤسسة "سيكديف (The SecDev Foundation)

هي منظمة غير حكومية كندية تُعنى بتعزيز المرونة الرقمية لدى المجتمعات المستضعفة - وخاصة النساء والشباب ومنظمات المجتمع المعرضة للخطر، تعمل المؤسسة في أكثر من ٢٠ دولة، بما في ذلك دول منطقة الشرق الأوسط وشمال إفريقيا، حيث تمكّن الأفراد من التفاعل الآمن والفعّال مع الفضاء الرقمي.

في منطقة الشرق الأوسط وشمال إفريقيا، لعبت مؤسسة «سيك ديف» دوراً محورياً في التصدي للعنف القائم على النوع الاجتماعي عبر الفضاء الرقمي، خاصة من خلال برنامج «سلام@» الذي نفذته بالشراكة مع منظمات محلية لتعزيز الوعي وتطوير استراتيجيات لمواجهة التهديدات الرقمية.

المركز الدولي لأبحاث التنمية (IDRC)

تم تنفيذ هذا العمل بمساعدة منحة من مركز بحوث التنمية الدولية، أوتاوا، كندا. الآراء الواردة هنا لا تمثل بالضورة آراء المركز الدولي لبحوث التنمية أو أعضاء مجلس إدارته.
يستثمر المركز الدولي لبحوث التنمية الدولية في البحوث عالية الجودة في البلدان النامية، وتبادل المعرفة مع الباحثين وصانعي السياسات من أجل زيادة استيعابها واستخدامها، ويحشد التحالفات العالمية لبناء عالم أكثر استدامة وشمولاً.

فريق العمل

قام فريق مركز المعلومات والبحوث بإعداد وتصميم هذا الدليل.

إعداد الدليل:

أ.د. أيمن هلسا – مدير مركز المعلومات والبحوث – مؤسسة الملك الحسين

أ. سوسن زايدة – رئيسة قسم البحوث في مركز المعلومات والبحوث - مؤسسة الملك الحسين

أ. روان الربيحات – باحثة رئيسية في مركز المعلومات والبحوث - مؤسسة الملك الحسين

م. سوزان وائل سيف - عضو اللجنة الاستشارية في مشروع الحد من العنف الرقمي وضابط تمكين المرأة في وزارة الاقتصاد الرقمي والريادة

مراجعة الدليل:

الجامعات:

د. خلود الزعبي خصاونة – محاضرة غير متفرغ في عدد من الجامعات الأردنية

د. عبيدة علي الربابعة – كلية الاعلام – جامعة البترا

أ. صادق محمد السحيمات – كلية تكنولوجيا المعلومات – جامعة الشرق الأوسط

د, مرسيل عيسى الجوينات – كلية الاعلام – جامعة اليرموك

د. نشوان عبدالله نشوان – كلية الآداب – جامعة الإسراء

د.نور توفيق مبيضين – كلية الآداب - جامعة الإسراء

أعضاء اللجنة الاستشارية:

ملازم أول م. أمينة علي عربيات – ضابط تحقيق وحدة الجرائم الإلكترونية

أ. سينياميس كلمات – الجمعية الأردنية للمصدر المفتوح

أ. شيرا محمد القطارنة – مديرة وحدة برامج تمكين المرأة اللجنة الوطنية لشؤون المرأة

د. محمد نشأت الطراونة – مدير وحدة شؤون المفوضين هيئة تنظيم قطاع الاتصالات

تقديم

يهدف هذا الدليل إلى مساعدة الأساتذة الجامعيين في تقديم مادة تعليمية متكاملة وشاملة للحد من العنف الرقمي، وذلك بطريقة تفاعلية وجذابة لتعزيز فهم الطلبة لهذا الموضوع المهم. يوفر الدليل محتوى علمي دقيق، إلى جانب استراتيجيات تدريس مبتكرة تشمل الأنشطة الصفية والمناقشات التفاعلية، لضمان تفاعل الطلبة وإثراء معرفتهم بالموضوع.

يتناول الدليل الجانب القانوني والتشريعي للعنف الرقمي، بالإضافة إلى استراتيجيات الوقاية والحماية الرقمية، مما يجعله أداة تعليمية قيمة ليس فقط في المساقات الجامعية، ولكن أيضًا في ورش العمل وحملات التوعية التي تستهدف الطلبة والشباب بشكل عام.

لمن هذا الدليل

تم تصميم هذا الدليل خصيصًا للأساتذة الجامعيين، الذين يقومون بتدريس المواد الإجبارية أو الاختيارية التي تهدف إلى تزويد الطلبة الجامعيين بمهارات حياتية أو قانونية. يمكن للأساتذة الاستفادة منه لتغطية ثلاث محاضرات أو أقل حول موضوع العنف الرقمي ضمن المقررات الدراسية، كما يمكن استخدامه كمرجع لتنظيم ورش توعوية تفاعلية لطلبة الجامعات، لتعزيز وعيهم حول المخاطر الرقمية وطرق الحماية.

محتوى الدليل

◆ المحاضرة الأولى: فهم العنف الرقمي

تقدم هذه المحاضرة نظرة شاملة حول العنف الرقمي، حيث تشمل:

- تعريف العنف الرقمي وفق المعايير الدولية.
- أشكاله المختلفة مثل التحرش الإلكتروني، الابتزاز، التشهير، والتجسس الرقمي.
- التأثير النفسي والاجتماعي للعنف الرقمي على الضحايا.

أنشطة مقترحة:
تحليل دراسات حالة واقعية.
مناقشات تفاعلية حول تجارب الطلبة مع الأمان الرقمي.

◆ المحاضرة الثانية: الأطر القانونية والتشريعية للعنف الرقمي في الأردن

تركز هذه المحاضرة على القوانين التي تنظم الجرائم الإلكترونية في الأردن، مع مقارنة بالتشريعات الدولية، وتشمل:

- قانون الجرائم الإلكترونية الأردني رقم (١٧) لسنة ٢٠٢٣ وأبرز مواده ذات الصلة بالعنف الرقمي
- التحديات القانونية التي تواجه الضحايا، مثل صعوبة الإثبات وقلة الوعي القانوني.
- الآليات المتاحة للضحايا، مثل الإبلاغ عن الجرائم الرقمية ودور مؤسسات الحماية.
- الاجراء القانوني المتبع في حاله التبليغ عند التعرض لاي شكل من اشكال العنف الرقمي.
- العقوبات التي قد تقع على من يرتكب هذا الفعل.

أنشطة مقترحة:
محاكاة محكمة لمناقشة قضية عنف رقمي.
تحليل نصوص قانونية ومناقشة مدى فعاليتها.
مناظرة طلابية حول مدى كفاية القوانين الحالية.

◆ المحاضرة الثالثة: الوقاية والحماية من العنف الرقمي

تتناول هذه المحاضرة استراتيجيات الحماية الرقمية لضمان بيئة إلكترونية آمنة، وتشمل:

- كيفية ضبط إعدادات الخصوصية على منصات التواصل الاجتماعي.
- أساليب التعامل مع التهديدات الرقمية والإبلاغ عنها.
- استخدام أدوات الأمان السيبراني مثل كلمات المرور القوية، والمصادقة الثنائية، وشبكات VPN.
- الدعم النفسي والاجتماعي للضحايا، ودور المجتمع في مكافحة العنف الرقمي.

أنشطة مقترحة:

الاستعانه بفيديو توضيحي للحماية مثل ضوابط منصات التواصل الاجتماعي
ورشة عمل حول إعدادات الأمان في وسائل التواصل الاجتماعي.
تمرين الأمن الرقمي: تحليل سيناريوهات تهديد إلكتروني.
مشروع طلابي لإنشاء حملات توعوية لمكافحة العنف الرقمي.

التوصيات لنجاح استخدام هذا الدليل

- اعتماد نهج تفاعلي.
- دمج التجارب الواقعية من خلال تقديم أمثلة حقيقية ودراسات حالة لزيادة وعي الطلبة.
- احترام حساسية الموضوع من خلال توفير بيئة آمنة للنقاش دون إصدار أحكام على المشاركين.
- ربط المحتوى بالسياق المحلي من خلال التأكيد على القوانين الأردنية وأمثلة من الواقع المحلي لتعزيز فهم الطلبة.

دليل الاستخدام

- تم إعداد هذا الدليل ضمن إطار التعاون بين مركز المعلومات والبحوث – مؤسسة الملك الحسين (IRCKHF) ومؤسسة SecDev الكندية، بهدف دعم الأساتذة الجامعيين في تعزيز الوعي الرقمي والحد من العنف الإلكتروني في الجامعات الأردنية.

التواصل والاستفسارات

- للملاحظات، أو طلبات الاستخدام، أو الإبلاغ عن أي انتهاك لحقوق الملكية الفكرية، يُرجى التواصل عبر البريد الإلكتروني: info@irckhf.org
- كما يمكن متابعة التحديثات المستقبلية للدليل والاطلاع على الموارد الإضافية حول الأمان الرقمي والعنف الإلكتروني عبر موقع منصة حقي (https://haqqi.info/ar)، المنصة الوطنية التابعة لمركز المعلومات والبحوث – مؤسسة الملك الحسين، والتي تُعد مصدرًا موثوقًا للمعرفة القانونية وحقوق الإنسان في الأردن، إضافة إلى صفحات المؤسسة الرسمية على وسائل التواصل الاجتماعي.

المحاضرة الأولى: فهم العنف الرقمي

الأهداف:

- تعريف العنف الرقمي وأشكاله المختلفة.
- فهم العوامل التي تساهم في انتشاره.
- تحليل تأثيره النفسي والاجتماعي على النساء.

المحتوى العلمي:

١. **مقدمة حول العنف الرقمي:**
   - تعريف العنف الرقمي وفق الأمم المتحدة.
   - الفرق بين العنف الرقمي والعنف التقليدي.
   - لماذا يعتبر العنف الرقمي قضية خطيرة؟
٢. **أشكال العنف الرقمي:**
   - التحرش الإلكتروني (رسائل غير مرغوبة، تعليقات مسيئة).
   - التنمر الإلكتروني والتشهير.
   - الابتزاز ونشر الصور دون موافقة.
   - انتهاك الخصوصية والتجسس الإلكتروني.
   - النصب والاحتيال الالكتروني.
٣. **تأثير العنف الرقمي على الضحايا:**
   - التأثير النفسي (القلق، الاكتئاب، اضطراب ما بعد الصدمة).
   - التأثير الاجتماعي (العزلة، فقدان الثقة بالنفس، الخوف من الفضاء الرقمي).
   - التأثير الاقتصادي (التشهير الذي يؤدي لفقدان الوظيفة، الابتزاز المالي).

طرق التدريس والأنشطة التفاعلية المقترحة:

- عرض فيديوهات قصيرة تعرض حالات حقيقية للعنف الرقمي.
- تحليل دراسات حالة (قصص حالات تعرضت للعنف الرقمي وتأثيره عليهن)
- نقاش مفتوح: هل سبق للطلبة أن واجهوا أو سمعوا عن مثل هذه الحالات؟
- استطلاع رأي فوري حول مدى شعور الطلبة بالأمان عند استخدام الإنترنت

المحتوى التعليمي المقترح

١. مقدمة حول العنف الرقمي

◆ تعريف العنف الرقمي

العنف الرقمي هو شكل من اشكال الجرائم الالكترونية هو مصطلح شامل لجرائم تنفذ من خلال تكنولوجيا المعلومات والاتصالات بغرض ممارسة العنف ويشمل عددًا كبيرًا من الجرائم المختلفة. ويأخذ العنف الإلكتروني اشكالا متعددة، منها مثلًا العنف الجنسي (مثل التحرش الالكتروني والابتزاز الإلكتروني، تواصل البالغين مع الأطفال والمراهقين عبر الإنترنت بغرض التمهيد للممارسات الجنسية) أو الجرائم بحق الممتلكات (مثل التصيد، والمتاجر الزائفة) أو جرائم العنف (مثل التنمر الإلكتروني، والمطاردة الإلكترونية) أو المراقبة الرقمية.

يتمثل العامل المشترك بين كل هذه الجرائم في استخدام الانترنت بغرض ممارسة العنف. عادةً ما يكون مرتكبو/مرتكبات الجرائم مجهولين/مجهولات الهوية، حيث يمكنهم التفاعل مع الآخرين دون الإفصاح عن هوياتهم، مثلًا عن طريق اسم مستعار.

تشير نتائج دراسة السلامة الرقمية لليافعين في الأردن (٢٠٢٤)، التي أجرتها مؤسسة إنقاذ الطفل، إلى أن التحرش الرقمي يشكل أحد أكثر أشكال العنف شيوعًا بين الفئات العمرية من ١٠ إلى ١٧ عامًا، مع تباين في أنماط التعرض له بحسب الجنس والعمر. وقد أبلغت نسبة أعلى من الفتيات مقارنة بالفتيان عن تعرضهن لمواقف مزعجة أو مؤذية عبر الإنترنت، من بينها تلقي صور غير لائقة أو رسائل مزعجة أو التعرض للملاحقة والمراقبة الإلكترونية[1].

العنـــف الرقمي

يحدث في الفضاء الإلكتروني من خلال الرسائل، الصور، الفيديوهات، والبرمجيات الضارة.

يمكن أن يحدث عن بُعد دون الحاجة إلى الاتصال المباشر.

يمكن أن ينتشر على نطاق واسع وبسرعة فائقة عبر الإنترنت.

يمكن تتبعه رقميًا، ولكن غالبًا ما يكون مرتكبه مجهول الهوية.

العنـــف التقليدي

يحدث في الواقع الفعلي، مثل العنف الجسدي أو العنف النفسي داخل الأسرة أو المجتمع.

يتطلب وجودًا ماديًا للمعتدي والضحية في نفس المكان.

ينحصر غالبًا في نطاق محدود جغرافيًا.

يمكن توثيقه بصعوبة ويتطلب شهادات الشهود.

◆ لماذا يعتبر العنف الرقمي قضية خطيرة؟

١. الانتشار السريع: يمكن أن تنتشر الإساءات والاعتداءات الرقمية بسرعة كبيرة، ما يؤدي إلى تعرض الضحية لضغوط نفسية واجتماعية واسعة. [2]

٢. إمكانية الوصول المستمرة: المعتدون يمكنهم مضايقة الضحايا على مدار الساعة عبر الإنترنت، مما يجعل العنف الرقمي أكثر إزعاجًا من العنف التقليدي.[3]

٣. إخفاء الهوية: يمكن للمعتدين استخدام هويات مزيفة أو إخفاء أنفسهم، مما يصعّب ملاحقتهم قانونيًا.[4]

٤. التأثيرات النفسية والجسدية: التعرض المستمر للعنف الرقمي يمكن أن يؤدي إلى اضطرابات نفسية مثل الاكتئاب، القلق، واضطراب ما بعد الصدمة.[5]

٥. التأثير على السمعة الشخصية والمهنية: يمكن أن يؤدي التشهير الإلكتروني إلى الإضرار بسمعة الضحايا، مما يؤثر على حياتهم المهنية والاجتماعية.[6]

٢. أشكال العنف الرقمي

أ. التحرش الإلكتروني

التحرش الإلكتروني يشمل الرسائل غير المرغوبة، التعليقات المسيئة، إرسال صور أو فيديوهات غير لائقة، أو الملاحقة عبر الإنترنت.[7]

◆ أمثلة على التحرش الإلكتروني[8]

- تلقي رسائل متكررة ذات طابع جنسي عبر البريد الإلكتروني أو وسائل التواصل الاجتماعي.
- نشر تعليقات مسيئة أو مهينة على حسابات النساء على الإنترنت.
- إرسال صور أو مقاطع فيديو غير لائقة دون موافقة المستلم.

١ مؤسسة إنقاذ الطفل – الأردن. (2024). الفضاءات الرقمية: هل نعلم حقًا ما يحدث خلف الشاشات؟ دراسة حول السلامة الرقمية لليافعين في الأردن (١٠–١٧ عامًا). بدعم من DANIDA

٢ ICRC Humanitarian Law & Policy Blog (2024) · Online violence: real life impacts on women and girls in humanitarian settings.

٣ سلاما@ (٢٠٢٣)، دليل مواجهة العنف الرقمي لطالبات الجامعات في الأردن.

٤ Vagia Polyzoidou (2024). Digital Violence Against Women: Is There a Real Need for Special Criminalization? Int J Semiot Law 37:1777–1797

٥ ICRC Humanitarian Law & Policy Blog (2024) · Online violence: real life impacts on women and girls in humanitarian settings.

٦ European Institute for Gender Equality (2022). Cyber Violence against Women and Girls Key Terms and Concepts.

٧ الاسكوا (بدون تاريخ). تعريف مصطلح التحرش الالكتروني.

٨ Stopbulling.gov. (2024). What Is Cyberbullying.

- التأثيرات
  - نفسية: القلق، الخوف، فقدان الثقة بالنفس.
  - اجتماعية: العزلة الاجتماعية، التوقف عن استخدام الإنترنت.
  - مهنية: التأثير على بيئة العمل أو التوظيف.
- إحصائيات

وفقًا لدراسة أجرتها منظمة الأمم المتحدة للمرأة، أفادت 73% من النساء بأنهن تعرضن لشكل من أشكال التحرش الإلكتروني، بينما لم تقم سوى ٤٪ منهن بالإبلاغ عن الجريمة.[9]

في دراسة على طالبات الجامعات الأردنيات، 50% من المشاركات تعرضن للتحرش الإلكتروني، بينما 78% لم يبلغن عنه بسبب الخوف من العواقب.[10]

ب. التنمر الإلكتروني والتشهير[11]

التنمر الإلكتروني هو استخدام الإنترنت لإلحاق الضرر العاطفي أو النفسي بشخص ما عن طريق الإهانة، التشهير، أو نشر محتوى مهين.

- أمثلة على التنمر الإلكتروني
  - نشر صور محرجة أو شخصية للضحية دون إذن.
  - إنشاء حسابات وهمية لنشر إشاعات أو تهديدات.
  - استخدام الفوتوشوب أو الذكاء الاصطناعي لإنشاء صور مُحرّفة للتشهير بالضحايا.
- التأثيرات
  - نفسية: اضطرابات القلق، الاكتئاب، الانعزال الاجتماعي.
  - أكاديمية: تراجع الأداء الدراسي أو الانسحاب من التعليم.
  - اقتصادية: فقدان الوظيفة أو تأثر السمعة المهنية.
- إحصائيات

أظهرت دراسة أوروبية أن 60% من النساء اللواتي تعرضن للتنمر الإلكتروني عانين من فقدان الثقة بالنفس والخوف من التفاعل الاجتماعي.[12]

ج. الابتزاز ونشر الصور دون موافقة[13]

يشمل الابتزاز الإلكتروني التهديد بنشر صور أو معلومات خاصة بهدف الحصول على أموال أو خدمات جنسية.

- أمثلة على الابتزاز الإلكتروني
  - تهديد النساء بنشر صور شخصية إذا لم يدفعن المال للمبتز.
  - التلاعب بالعلاقات العاطفية عبر الإنترنت للحصول على صور أو معلومات حساسة ثم استخدامها للابتزاز.
  - استخدام برامج الاختراق لسرقة البيانات الخاصة وتهديد الضحية.
- التأثيرات
  - نفسية: شعور بالذنب، الخوف، القلق الدائم.
  - اجتماعية: العزلة، فقدان الثقة بالمجتمع.
  - قانونية: قد لا يكون هناك وعي قانوني لدى الضحايا حول كيفية الإبلاغ والتعامل مع هذه الحالات.

٩ European Institute for Gender Equality (2022). Cyber Violence against Women and Girls Key Terms and Concepts.
١٠ سلاما@ (٢٠٢٣)، دليل مواجهة العنف الرقمي لطالبات الجامعات في الأردن.
١١ الطبي (٢٠٢٤). التنمر الالكتروني.
١٢ سلاما@ (٢٠٢٣)، دليل مواجهة العنف الرقمي لطالبات الجامعات في الأردن.
١٣ وفاء محمد صقر (٢٠٢٤). جريمة الابتزاز الالكتروني، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة بني سويف، الملد ٣٦ – العدد ٢.

◆ إحصائيات

أفاد ٤٥٪ من النساء في منطقة الشرق الأوسط وشمال إفريقيا بأنهن تعرضن لشكل من أشكال الابتزاز الإلكتروني، ومعظمهن لم يبلغن عن الحوادث خوفًا من الوصمة الاجتماعية.[١٤]

د. انتهاك الخصوصية والتجسس الإلكتروني[١٥]

يشمل محاولات اختراق الأجهزة، التنصت على المحادثات، تتبع الموقع الجغرافي، وسرقة البيانات الشخصية.

◆ أمثلة على انتهاك الخصوصية

- استخدام برامج التجسس للوصول إلى الرسائل والصور دون إذن.
- تتبع موقع الضحية عبر تطبيقات GPS دون علمها.
- نشر معلومات شخصية مثل العنوان أو رقم الهاتف على الإنترنت دون موافقة.

◆ التأثيرات

- نفسية: الشعور بعدم الأمان، اضطرابات النوم.
- مهنية: قد يؤثر تسريب البيانات الخاصة على فرص العمل.
- قانونية: يصعب تتبع المجرمين بسبب استخدامهم تقنيات إخفاء الهوية.

◆ إحصائيات

تسجيل حالات تعرض نساء لمراقبة أجهزتهن الذكية من قبل أزواجهن السابقين بهدف التحكم والسيطرة.[١٦]

وفي ضوء تعدد أشكال العنف الرقمي وانتشاره المتزايد، تتخذ الحكومة الأردنية عدة خطوات لمواجهته والحد من آثاره، وذلك من خلال سن تشريعات وقوانين تهدف إلى التصدي للعنف الرقمي وتعزيز حماية الضحايا. كما تعمل على توسيع نطاق التوعية المجتمعية عبر إدماج التربية الإعلامية والمعلوماتية في المدارس والجامعات، وتنظيم ورش عمل توعوية لتعريف الطلبة بأساليب الحماية الرقمية ومخاطر الانتهاكات الإلكترونية. وتقوم وحدة الجرائم الإلكترونية، إلى جانب جهات رسمية أخرى، بتنفيذ زيارات ميدانية دورية للمؤسسات التعليمية بهدف نشر الوعي بأفضل الممارسات الرقمية، وتمكين الأفراد، خاصة الفئات الشابة، من مواجهة التحديات الرقمية بوعي ومعرفة.

١٤ Vagia Polyzoidou (2024). Digital Violence Against Women: Is There a Real Need for Special Criminalization? Int J Semiot Law 37:1777–1797

١٥ دياب البداينة (٢٠٢٨). الجرائم الإلكترونية المفهوم والأسباب. ورقة علمية مقدمة في الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية الدولية، كلية العلوم الاستراتيجية، قطر.

١٦ سلاما@ (٢٠٢٣)، دليل مواجهة العنف الرقمي لطالبات الجامعات في الأردن.

المحاضرة الثانية:

الأطر القانونية والتشريعية للعنف الرقمي في الأردن

الأهداف:

- التعرف على القوانين الأردنية الخاصة بالعنف الرقمي.
- فهم التحديات القانونية التي تواجه الضحايا.
- تحليل أوجه القصور التشريعي والحلول الممكنة.

المحتوى العلمي:

١. القوانين والتشريعات ذات الصلة:
   - قانون الجرائم الإلكترونية الأردني (أبرز المواد المتعلقة بالعنف الرقمي).
   - التشريعات الدولية: مقارنة بين الأردن ودول أخرى.
٢. تحديات إنفاذ القانون:
   - صعوبة إثبات الجريمة الرقمية.
   - ضعف الوعي القانوني لدى الضحايا.
   - غياب الدعم النفسي والقانوني الكافي.
٣. الآليات المتاحة للضحايا:
   - كيفية الإبلاغ عن الجرائم الرقمية.
   - دور مراكز الحماية والمؤسسات القانونية.

طرق التدريس والأنشطة التفاعلية:

- محاكاة محكمة: يتم توزيع الطلبة لأدوار (محامي، قاضي، ضحية، شرطة) لمناقشة قضية افتراضية.
- تحليل نصوص قانونية: استعراض مواد قانون الجرائم الإلكترونية وتفسيرها بطريقة مبسطة.
- مناظرة طلابية حول جدوى القوانين الحالية ومدى فعاليتها.
- عصف ذهني

المحتوى العلمي المقترح للمحاضرة الثانية

١. مقدمة

يعد قانون الجرائم الإلكترونية الأردني رقم (١٧) لسنة ٢٠٢٣ من أهم التطورات القانونية في مواجهة العنف الرقمي. ومع تزايد استخدام الإنترنت، باتت الحاجة إلى قوانين واضحة وقوية لحماية الأفراد من الجرائم الرقمية ضرورية.

٢. القوانين والتشريعات ذات الصلة

أ. قانون الجرائم الإلكترونية رقم (١٧) لسنة ٢٠٢٣

أبرز المواد القانونية المرتبطة بالعنف الرقمي ضد النساء:

١. الابتزاز والتهديد الرقمي

المادة (١٨): يعاقب كل من هدد شخصًا أو ابتزه بالسجن من سنة إلى ثلاث سنوات وغرامة بين ٣٠٠٠ و٦٠٠٠ دينار.

إذا كان التهديد يتعلق بأمور خادشة للشرف، تصل العقوبة إلى الأشغال المؤقتة وغرامة بين ٥٠٠٠ و١٠٠٠٠ دينار.

٢. نشر أو مشاركة محتوى خاص دون إذن

المادة (٢٠): أي شخص يقوم بنشر أو مشاركة صور أو تسجيلات شخصية بدون إذن يعاقب بالسجن من ٣ أشهر إلى سنتين وغرامة تصل إلى ٥٠٠٠٠ دينار.

٣. انتحال الهوية الرقمية

المادة (٥): يعاقب بالحبس لمدة لا تقل عن ٣ أشهر وغرامة بين ١٥٠٠ و١٥٠٠٠ دينار من يقوم بانتحال هوية شخص آخر عبر الإنترنت.

ب. مقارنة مع تشريعات دولية

الدولة	ابرز التشريعات المتعلقة بالعنف الرقمي	العقوبات
الأردن	قانون الجرائم الإلكترونية رقم ١٧ لسنة ٢٠٢٣	غرامات تصل إلى ٥٠٠٠٠ دينار وسجن حتى ٥ سنوات
الاتحاد الأوروبي	اللائحة العامة لحماية البيانات (GDPR)[17]	غرامات تصل إلى ملايين اليوروهات وسجن يصل إلى ٥ سنوات
الولايات المتحدة الأمريكية	قانون الجرائم الإلكترونية الفيدرالي[18]	سجن حتى ٥ سنوات وغرامات تصل إلى ٢٥٠,٠٠٠ دولار
تونس	قانون العنف ضد المرأة لسنة ٢٠١٧[19]	سجن حتى ٤ سنوات وغرامات
المغرب	قانون العنف ضد المرأة لسنة ٢٠١٩[20]	سجن حتى ٣ سنوات

٣. تحديات إنفاذ القانون

- ضعف التبليغ عن الجرائم الرقمية بسبب الخوف من الوصمة الاجتماعية.
  صعوبة تعقب الجناة عند استخدام حسابات مزيفة أو تقنيات إخفاء الهوية.
  نقص في تدريب القضاة على التعامل مع قضايا الجرائم الرقمية.
- طول الوقت الذي تأخذه الاجراءات الشكوى لحين صدور الحكم القانوني.

٤. الآليات المتاحة للضحايا

◆ الإبلاغ عن الجرائم الرقمية:

- من خلال وحدة مكافحة الجرائم الإلكترونية في مديرية الأمن العام.
- عبر تقديم بلاغ رسمي إلى النيابة العامة.

◆ دعم المجتمع المدني:

- منظمات غير حكومية تساعد الضحايا في الحصول على المشورة القانوني.

طرق التدريس والأنشطة التفاعلية

١. محاكاة محكمة

يتم توزيع الطلبة على أدوار (قاضٍ، محامٍ، ضحية، متهم).
يتم تقديم قضية ابتزاز رقمي مشابهة لقضية رنا لمناقشتها قانونيًا.
الطلبة يستخدمون مواد قانون الجرائم الإلكترونية الأردني رقم ١٧ لسنة ٢٠٢٣ لصياغة الأحكام.

---

١٧ التعليمات العامة لحماية البيانات (General Data Protection Regulation) هي إطار قانوني صادر عن الاتحاد الأوروبي يهدف إلى حماية البيانات الشخصية للأفراد داخل الاتحاد الأوروبي والمنطقة الاقتصادية الأوروبية (EEA). دخلت هذه اللائحة حيز التنفيذ في ٢٥ مايو ٢٠١٨، وتعد من أكثر القوانين صرامة فيما يتعلق بحماية الخصوصية الرقمية وتنظيم كيفية جمع البيانات الشخصية ومعالجتها وتخزينها.

١٨ قانون الاحتيال وإساءة استخدام الحاسوب (CFAA - Act Abuse and Fraud Computer) هو القانون الفيدرالي الأساسي في الولايات المتحدة الأمريكية الذي ينظم الجرائم الإلكترونية، بما في ذلك الاختراق، الاحتيال عبر الإنترنت، وانتهاك الخصوصية الرقمية. تم إقراره في عام ١٩٨٦ وتم تعديله عدة مرات لمواكبة التطورات في الجريمة السيبرانية.

١٩ قانون أساسي عدد ٥٨ لسنة ٢٠١٧ مؤرخ في ١١ أوت ٢٠١٧ يتعلق بالقضاء على العنف ضد المرأة.

٢٠ القانون رقم ١٠٣,١٣ المتعلق بمحاربة العنف ضد النساء

قضية دراسية:
ابتزاز فتاة عبر وسائل التواصل الاجتماعي

ملخص القضية

في عام ٢٠٢٣، تعرضت رنا، وهي طالبة جامعية في عمان، لعملية ابتزاز رقمي عبر وسائل التواصل الاجتماعي. بدأت القصة عندما تعرفت رنا على شخص يدعى أحمد من خلال منصة إنستغرام، حيث تواصل معها لفترة وأظهر اهتمامه بها. بعد عدة أشهر من التفاعل، أقنعها بإرسال صور شخصية في سياق محادثات خاصة. بعد فترة، انتهت العلاقة بينهما، لكن أحمد استخدم الصور التي أرسلتها له سابقًا لابتزازها.

تفاصيل الابتزاز

- بدأ أحمد في إرسال رسائل تهديدية إلى رنا عبر تطبيق واتساب، مطالبًا إياها بدفع ٣٠٠ دينار أردني مقابل عدم نشر صورها على الإنترنت.
- هددها بإرسال الصور إلى عائلتها وأصدقائها إن لم تستجب لطلباته.
- مع استمرار التهديدات، شعرت رنا بالرعب والتوتر النفسي وقررت عدم إبلاغ عائلتها خوفًا من اللوم أو الوصمة الاجتماعية.

كيف تم التعامل مع القضية؟

١.الإبلاغ عن الجريمة

- لجأت رنا إلى إحدى صديقاتها المقربات، التي شجعتها على التحدث مع وحدة مكافحة الجرائم الإلكترونية في مديرية الأمن العام.
- قام ضباط الوحدة بمراجعة رسائل التهديد وأدلة الابتزاز، ووجهوا رنا إلى تقديم شكوى رسمية وفق قانون الجرائم الإلكترونية الأردني رقم (١٧) لسنة ٢٠٢٣.

٢.التدخل القانوني

- استندت الشرطة إلى المادة (١٨) من القانون، التي تنص على أن الابتزاز الإلكتروني يعاقب بالسجن لمدة تتراوح بين سنة وثلاث سنوات، وغرامة بين ٣٠٠٠ و٦٠٠٠ دينار.
- تم تعقب الحسابات الرقمية التي استخدمها أحمد، مما أدى إلى تحديد موقعه والقبض عليه.
- خلال التحقيق، اعترف أحمد بفعلته، وتمت إحالته إلى القضاء.

٣.الدعم النفسي والاجتماعي

- تلقت رنا دعمًا نفسيًا من إحدى الجمعيات النسوية التي تقدم استشارات للنساء المتضررات من العنف الرقمي.
- تم توعيتها حول أساليب الحماية الرقمية، مثل ضبط إعدادات الخصوصية، عدم مشاركة الصور الشخصية، والإبلاغ الفوري عن أي تهديدات مماثلة.

النتائج

- تم الحكم على أحمد بالسجن لمدة سنتين ودفع غرامة قدرها ٥٠٠٠ دينار أردني.
- رنا استطاعت تجاوز الأزمة بعد تلقيها الدعم النفسي والمعنوي.
- القضية تبرز أهمية التوعية الرقمية للفتيات حول حماية خصوصيتهن وعدم الوقوع ضحية الابتزاز الرقمي.

مناقشة مع الطلبة

- ما الذي كان يمكن أن تفعله رنا بشكل مختلف لحماية نفسها؟
- ماذا يمكن أن يحدث لو لم تتجه رنا لوحدة الجرائم الالكترونية؟
- هل تعتقد ان هناك عوائق تمنع رنا من الإبلاغ؟
- ما الإجراءات التي يمكن أن تتخذها الجامعات لحماية الطالبات من العنف الرقمي؟

إضاءة:

يمكن تسليط الضوء على أساليب الابتزاز الأخرى والمنتشرة حاليا مثل الايهام في توفير فرص عمل للضحية وطلب المعلومات الخاصة بها وايضا من خلال تقديم مساعدات ماليه وتقديم قروض لطالبات الجامعات.

٢. تحليل نصوص قانونية

- يتم توزيع نصوص قانونية متعلقة بالعنف الرقمي على الطلبة.
- تتم مناقشة مدى كفاية هذه القوانين في حماية الضحايا.

٣. مناظرة طلابية

الموضوع: "هل قوانين الجرائم الإلكترونية الأردنية كافية لحماية النساء من العنف الرقمي؟"

- فريق مؤيد للقوانين الحالية.
- فريق يدعو إلى تعديلات تشريعية تأخذ بعين الاعتبار خصوصية الجرائم الالكترونية المرتكبة ضد النساء

المحاضرة الثالثة: الوقاية والحماية من العنف الرقمي

الأهداف:

- تطوير مهارات الحماية الرقمية لدى الطلبة.
- معرفة كيفية التعامل مع العنف الرقمي عند حدوثه.
- تعزيز ثقافة المواطنة الرقمية المسؤولة.
- نشر الوعي في البيئة المحيطة للطالب.

المحتوى العلمي:

١. **أساليب الحماية الرقمية:**
   - كيفية ضبط إعدادات الخصوصية على وسائل التواصل الاجتماعي.
   - استخدام كلمات مرور قوية والتأكد من حماية الحسابات.
   - التعرف على أساليب الاحتيال الرقمي.
٢. **كيفية الإبلاغ عن العنف الرقمي:**
   - آليات الإبلاغ في منصات التواصل الاجتماعي.
   - التواصل مع الجهات القانونية المختصة.
٣. **دور المجتمع في مواجهة العنف الرقمي:**
   - مسؤولية الأفراد في التبليغ والدعم.
   - أهمية التوعية والمناصرة لخلق بيئة رقمية آمنة.

طرق التدريس والأنشطة التفاعلية:

- ورشة عمل تقنية: تطبيق عملي على كيفية ضبط إعدادات الخصوصية في حسابات الطلبة.
- تمرين الأمن الرقمي: يقوم الطلبة بمراجعة إعدادات أمان حساباتهم وتطبيق النصائح الواردة.
- مشروع توعوي: يكلف الطلبة بإعداد فيديو أو حملة رقمية للتوعية بالعنف الرقمي.

محتوى علمي مقترح للمحاضرة الثالثة

١. مقدمة

العنف الرقمي، بما في ذلك التحرش، الابتزاز، وانتهاك الخصوصية، يؤثر سلبًا على الصحة النفسية والاجتماعية للضحايا، خاصة النساء. لذا، من الضروري التركيز على الوقاية والحماية الرقمية لضمان بيئة إلكترونية آمنة. تشير الدراسات إلى أن 75% من النساء اللواتي تعرضن للعنف الرقمي لم يكن لديهن معرفة كافية بوسائل الحماية الرقمية، مما يؤكد الحاجة إلى تعزيز الوعي والمهارات الرقمية.[٢١]

٢١ European Institute for Gender Equality (2022). Cyber Violence against Women and Girls Key Terms and Concepts.

٢. أساليب الحماية الرقمية

أ. إعدادات الخصوصية على وسائل التواصل الاجتماعي

تشير الإحصائيات إلى أن 68% من النساء اللاتي تعرضن للعنف الرقمي لم يستخدمن إعدادات الخصوصية بشكل كافٍ.[٢٢] لذلك، ينبغي توعية الأفراد بكيفية ضبط إعدادات الأمان على المنصات المختلفة:

فيسبوك:

- تفعيل ميزة المصادقة الثنائية (Two-Factor Authentication).
- الحد من يمكنه رؤية المنشورات والصور الشخصية.
- استخدام خيار «المراجعة قبل النشر» للصور التي يتم الإشارة إليك فيها.
- التواصل مع الأشخاص المعروفين في الواقع او البيئة المحيطة فقط والذين لا يحملون أسماء وهمية أو مستعارة.

إنستغرام:

- ضبط الحساب على الوضع الخاص لمنع الغرباء من رؤية المحتوى.
- منع الغرباء من إرسال رسائل مباشرة عبر إعدادات المراسلة.
- الإبلاغ عن الحسابات المسيئة وحظر المتحرشين رقميًا.

تويتر (X):

- تمكين خاصية إخفاء الردود المسيئة تلقائيًا.
- ضبط من يمكنه الرد على التغريدات الخاصة بك.

واتساب:

- تفعيل خيار عدم إظهار آخر ظهور إلا للأصدقاء الموثوقين.
- منع غير المسجلين في قائمة جهات الاتصال من رؤية الصورة الشخصية أو الحالة.

* من الضروري عند تغيير رقم الهاتف وشراء خط جديد حذف الرقم القديم من جميع الحسابات المرتبطة به، حيث انه غالباً ما تُخترق اغلب الحسابات بهذه الطريقة .

ب. كيفية التعامل مع التهديدات الإلكترونية والإبلاغ عنها

تشير التقارير إلى أن نسبة ضئيلة فقط من النساء المتضررات يقمن بالإبلاغ عن العنف الرقمي بسبب الخوف من الانتقام أو الوصمة الاجتماعية. لذا، من المهم تقديم خطوات واضحة للإبلاغ عن الجرائم الرقمية:

- ◆ الإبلاغ عبر منصات التواصل الاجتماعي: توفر معظم المنصات خاصية الإبلاغ عن:
  - الحسابات المسيئة.
  - الرسائل المزعجة أو التهديدات.
  - المنشورات التي تحتوي على محتوى غير لائق.
- ◆ الإبلاغ عبر وحدة مكافحة الجرائم الإلكترونية في الأردن:
  - يمكن تقديم بلاغ رسمي عبر موقع وحدة الجرائم الإلكترونية في مديرية الأمن العام الأردني.
  - يجب تقديم أدلة رقمية (لقطات شاشة، رسائل تهديد، حسابات الجناة).
  - عند تقديم شكوى جرائم الالكترونية، يجب إحضار لائحة شكوى من المدعي العام من المحكمة المختصة وثم التوجه للجرائم الإلكترونية.
- ◆ اللجوء إلى المساعدة القانونية:
  - التواصل مع منظمات المجتمع المدني التي توفر استشارات قانونية للضحايا.

٢٢ سلاما@ (٢٠٢٣)، دليل مواجهة العنف الرقمي لطالبات الجامعات في الأردن.

- طلب الحماية القانونية من خلال رفع دعوى رسمية في المحاكم المختصة.

٣. استراتيجيات الحماية الشخصية عبر الإنترنت

أ. استخدام كلمات مرور قوية وتقنيات الأمان السيبراني

- استخدام كلمات مرور معقدة تحتوي على أحرف كبيرة وصغيرة وأرقام ورموز خاصة.
- عدم إعادة استخدام نفس كلمة المرور عبر مواقع متعددة.
- تحديث كلمات المرور بشكل دوري، خاصة بعد التعرض لأي محاولة اختراق.

ب. تفعيل المصادقة الثنائية:

وتسمى أيضاً التحقق بخطوتين، هذه الخاصية تضيف طبقة حماية إضافية عند تسجيل الدخول إلى حسابك بعد استخدام كلمة المرور

ج. استخدام الأدوات التكنولوجية للحماية

- VPN (الشبكة الخاصة الافتراضية): يخفي عنوان IP ويحمي البيانات الشخصية.
- برامج مكافحة الفيروسات: تمنع اختراق الأجهزة وسرقة المعلومات.
- تشفير البيانات: يضمن حماية الملفات والمعلومات الحساسة من الوصول غير المصرح به.

د. حماية الهواتف الذكية والأجهزة الشخصية

- تفعيل خاصية القفل بالبصمة أو التعرف على الوجه لزيادة الحماية.
- تجنب تحميل تطبيقات من مصادر غير موثوقة، حيث قد تحتوي على برامج تجسس.
- إيقاف تشغيل خاصية الموقع الجغرافي في التطبيقات غير الضرورية لتجنب التتبع.
- تحديث البرامج بانتظام، من المهم تحديث نظام التشغيل والبرامج والتطبيقات بالنظام لسد الثغرات الأمنية.
- عدم مشاركة الرمز الموحد مع أي شخص وخاصه في الحوالات البنكية OTP.

هـ. استخدام التطبيقات المشفرة وذات المصدر المفتوح

- استخدام تطبيقات التواصل الإلكتروني المشفرة مثل تطبيق Signal.
- استخدام تطبيقات إدارة كلمات المرور مثل Bitwarden.
- استخدم مواقع موثوقة للتحقق من الروابط والملفات قبل النقر عليها وفتحها. مثل Virustotal.

٤. الدعم النفسي والاجتماعي للضحايا

أ. تأثير العنف الرقمي على الصحة النفسية

أظهرت دراسات حديثة أن العنف الرقمي يؤدي إلى زيادة معدلات القلق والاكتئاب والعزلة الاجتماعية، حيث أبلغ 80% من الضحايا عن آثار نفسية سلبية طويلة الأمد.لذا، من المهم توفير خدمات دعم نفسي متخصصة للضحايا، مثل:

- جلسات دعم نفسي فردية أو جماعية للنساء المتضررات.
- توفير خط دعم نفسي سري يمكن للضحايا اللجوء إليه عند الحاجة.
- توعية المجتمع حول الأثر النفسي للعنف الرقمي لتشجيع بيئة داعمة للضحايا.

ب. دور المجتمع المدني في دعم الضحايا

يلعب المجتمع، بأفراده ومؤسساته، دورًا محوريًا في الوقاية من العنف الرقمي والاستجابة له، من خلال تعزيز بيئة رقمية آمنة، وتوفير الدعم للضحايا، ورفع الوعي المجتمعي. وتتوزع الأدوار على أربعة محاور رئيسية:

◆ **أولا: مسؤولية الأفراد في التبليغ والدعم**

- يشكل وعي الأفراد وحسهم بالمسؤولية حجر الأساس في التصدي للعنف الرقمي.
- التبليغ عن حالات العنف وعدم الصمت يُعدّ دعمًا مباشرًا للضحايا وردعًا للجناة.
- دعم الضحايا نفسيًا ومعنويًا، وتجنب اللوم المجتمعي، يساعد في تقليل الآثار السلبية ويشجع على الإبلاغ.

◆ **ثانيا: أهمية التوعية والمناصرة**

- تنظيم حملات توعوية في الجامعات والمجتمع المحلي حول مخاطر العنف الرقمي وسبل الحماية القانونية والتقنية.

- إطلاق مبادرات طلابية ومجتمعية لنشر ثقافة «المواطنة الرقمية المسؤولة» واستخدام المنصات الرقمية بشكل آمن.
- مناصرة حقوق الضحايا في الإعلام ومنصات التواصل، وتغيير النظرة النمطية للنساء المتضررات من العنف الرقمي.

◆ ثالثا: دور الأسرة في الحماية والاحتواء

- تشكل الأسرة خط الدفاع الأول، لا سيما في المجتمعات التقليدية، حيث يتطلب الأمر دعمًا لا لومًا للضحايا من الأبناء، خصوصًا الفتيات.
- يساهم الحوار المفتوح والمبني على الثقة بين الأهل والأبناء في الكشف المبكر عن حالات العنف وتقديم المساندة.
- من الضروري توعية الوالدين بأدوات الحماية الرقمية وآليات الإبلاغ، خاصة مع الاستخدام الواسع للتكنولوجيا من قبل الشباب.

◆ رابعا: دور المجتمع المدني والمؤسسات الداعمة

- تقدم منظمات المجتمع المدني خدمات قانونية ونفسية متخصصة للنساء المتضررات من العنف الرقمي.
- تنفذ برامج توعية رقمية تستهدف الطلبة في المدارس والجامعات لتعزيز ثقافة الأمان الرقمي والوقاية.
- تطلق حملات إلكترونية تشجع النساء على التبليغ دون خوف، وتعمل على إزالة الحواجز الاجتماعية والثقافية التي تعيق ذلك.

طرق التدريس والأنشطة التفاعلية

١. ورشة عمل تطبيقية حول إعدادات الأمان

يقوم الطلبة بفتح هواتفهم وضبط إعدادات الخصوصية على تطبيقات مثل واتساب، فيسبوك، وإنستغرام.
يتم إجراء تقييم لمستوى الحماية لكل طالب، وتقديم نصائح لتعزيز الأمن الرقمي.

٢. تمرين الأمن الرقمي

يتم تقديم سيناريوهات مختلفة للطلبة حول التهديدات الرقمية، مثل:

- تلقي رسالة تهديد عبر الإنترنت.
- التعرض لمحاولة تصيد احتيالي (Phishing).
    - يقوم الطلبة بتحليل السيناريوهات وتحديد أفضل طرق التصرف بناءً على المعلومات التي تعلموها.

مثال تطبيقي:
تحليل سيناريوهات التهديدات الرقمية

السيناريو الأول:
تلقي رسالة تهديد عبر الإنترنت

الموقف:

تتلقى مريم، طالبة جامعية، رسالة عبر إنستغرام من حساب مجهول يقول فيها:

"أنا أعرف كل شيء عنك، لدي صور لك، وإذا لم ترسلي لي ٢٠٠ دينار خلال ٤٨ ساعة، سأقوم بنشرها للجميع."

الأسئلة للنقاش مع الطلبة:

١. ما هو نوع التهديد الذي تعرضت له مريم؟
٢. ما هي الإجراءات الفورية التي يجب أن تتخذها مريم لحماية نفسها؟
٣. كيف يمكن لمريم التأكد مما إذا كانت هذه الرسالة خدعة أو تهديد حقيقي؟
٤. كيف يمكنها الإبلاغ عن هذا التهديد عبر القنوات القانونية؟

الإجابة المثالية:

- عدم الرد على المرسل وعدم إرسال أي أموال.
- حفظ أدلة التهديد عبر أخذ لقطات شاشة للرسائل.
- لإبلاغ عن الحساب على منصة إنستغرام لحظره.
- التوجه إلى وحدة مكافحة الجرائم الإلكترونية الأردنية وتقديم بلاغ رسمي استنادًا إلى المادة (١٨) من قانون الجرائم الإلكترونية رقم ١٧ لسنة ٢٠٢٣.

السيناريو الثاني:
التعرض لمحاولة تصيد احتيالي (Phishing)

الموقف:

يتلقى أحمد، طالب جامعي، رسالة بريد إلكتروني من عنوان يبدو رسميًا:

"عزيزي المستخدم، لقد تم اختراق حسابك البنكي. يرجى تحديث بياناتك فورًا من خلال الرابط أدناه لحماية حسابك من الإغلاق." www.bank-secure-login.com

الأسئلة للنقاش مع الطلبة:

١. ما هي علامات الاحتيال في هذه الرسالة؟
٢. لماذا يُعد النقر على هذا الرابط خطرًا على بيانات أحمد؟

٣.ما الذي يجب أن يفعله أحمد عند تلقي مثل هذه الرسالة؟
٤.كيف يمكنه التأكد مما إذا كانت الرسالة حقيقية أم مزيفة؟

الإجابة المثالية:

عدم النقر على الرابط، حيث يمكن أن يكون موقعًا مزيفًا لسرقة بياناته الشخصية.
التأكد من صحة البريد الإلكتروني المرسل عبر التواصل المباشر مع البنك.
استخدام برامج الحماية من التصيد الاحتيالي مثل Google Safe Browsing.
الإبلاغ عن البريد الإلكتروني الاحتيالي إلى البنك المعني والجهات المختصة مثل وحدة مكافحة الجرائم الإلكترونية.

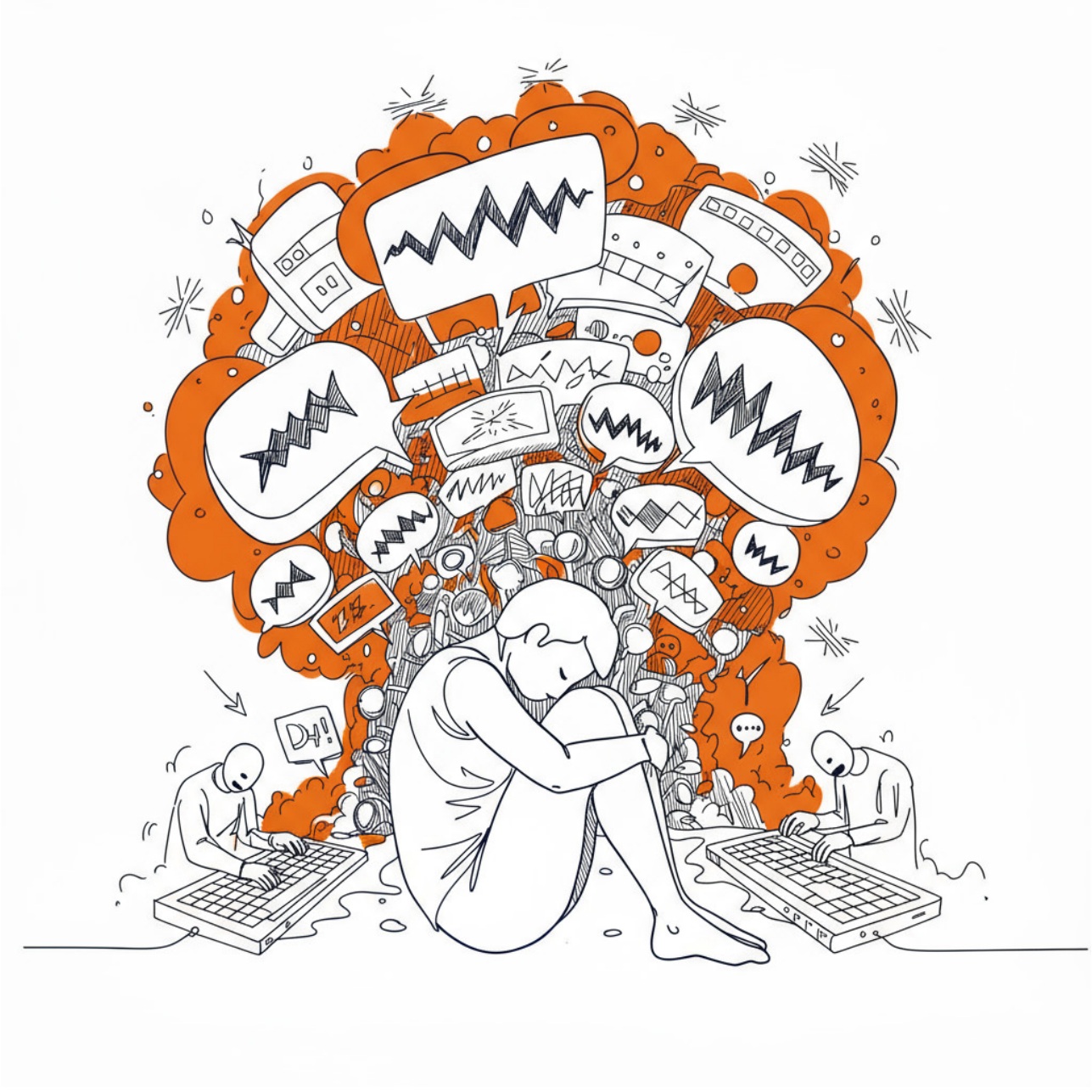
الهدف من النشاط:

تعزيز الوعي الرقمي لدى الطلبة حول التهديدات الإلكترونية.
تعليمهم كيفية التحقق من مصداقية الرسائل والتصرف بشكل آمن عبر الإنترنت.
تدريبهم على استخدام أدوات الإبلاغ والحماية الرقمية.

٣. مشروع توعوي: إنشاء حملات إلكترونية لمكافحة العنف الرقمي

يتم تقسيم الطلبة إلى مجموعات لإنشاء حملة رقمية توعوية تتضمن:

- منشورات توعوية حول العنف الرقمي.
- مقاطع فيديو قصيرة تشرح كيفية الحماية الرقمية.
- مواد إرشادية حول كيفية الإبلاغ عن الجرائم الإلكترونية.



الفـــبركة العميـــقة

(Deepfake) تقنية الذكاء الاصطناعي التي تُمكن من تعديل الصور ومقاطع الفيديو والصوت بطريقة تجعلها تبدو واقعية، وتُستخدم في:

تزوير صور وفيديوهات للضحايا بغرض التشهير أو الابتزاز.
خلق محتوى إباحي مزيف للنساء باستخدام صورهن الأصلية.
نشر أخبار كاذبة ومضللة تستهدف شخصيات عامة أو مؤثرة.

كيف يمكن كشفها؟

استخدام أدوات التحقق من الفيديوهات مثل InVID.
البحث عن تشوهات في حركة الفم أو الأعين، حيث تكون غير طبيعية في الفيديوهات
رفع الفيديو إلى خبراء تقنيين أو جهات مختصة مثل وحدة الجرائم الإلكترونية في الأردن.

كيف تحمي نفسك؟

تجنب نشر صور شخصية بجودة عالية على الإنترنت، حيث يمكن استخدامها للفبركة.
عدم مشاركة صور أو فيديوهات خاصة عبر الإنترنت، حتى مع الأصدقاء المقربين.
الإبلاغ فورًا في حال الاشتباه في استخدام تقنيات Deepfake للإساءة إليك.

الذكاء الاصطناعي والتحرش الرقمي

يستخدم المجرمون برامج الذكاء الاصطناعي لإنشاء حسابات وهمية وانتحال شخصيات حقيقية لخداع الضحايا.

إنشاء حسابات وهمية على إنستغرام وفيسبوك تحمل صورًا مزيفة لشخصيات جذابة للإيقاع بالضحايا.
استخدام الذكاء الاصطناعي في الدردشة التلقائية (Chatbots) لخداع الضحايا وإقناعهم بمشاركة صور أو معلومات شخصية.
سرقة الهوية الرقمية باستخدام صور الضحايا ونشرها على مواقع مزيفة.

كيف تحمي نفسك؟

لا تتحدث مع حسابات مجهولة تطلب معلومات خاصة أو صورًا شخصية.

المراقبة الرقمية والتجسس الإلكتروني

استخدام تطبيقات أو برامج لاختراق الهواتف وأجهزة الكمبيوتر لمراقبة الأشخاص دون علمهم

كيف يحدث؟
عبر تطبيقات التجسس التي يمكن تثبيتها على هاتف الضحية بدون علمها.
من خلال الواي فاي العام، حيث يمكن للمجرمين سرقة البيانات عند الاتصال بشبكة غير آمنة.
عبر إرسال روابط خبيثة لسرقة بيانات المستخدمين.

كيف تحمي نفسك؟
إزالة أي تطبيق مشبوه لم تقم بتثبيته بنفسك.
عدم الاتصال بشبكات WiFi عامة دون استخدام VPN.
تحديث الهاتف باستمرار لحظر الثغرات الأمنية.

حالات وأمثلة مستوحاة من الواقع

حالة ١:
فبركة صور فتاة جامعية عبر الذكاء الاصطناعي (Deepfake)

القصة:
"رُبى"، طالبة جامعية في عمان، كانت تنشر صورًا عادية على إنستغرام. تفاجأت يومًا برسائل تهديد من حساب مجهول يدّعي أنه يملك "صورًا غير لائقة لها" وسيقوم بنشرها إن لم تدفع مبلغ ٥٠٠ دينار. بعد التحقيق، تبيّن أن الصور تم تعديلها بتقنية الذكاء الاصطناعي Deepfake، حيث استخدم شخص مجهول صورة وجهها وألصقها على جسد مختلف.

كيف تم التعامل مع المشكلة؟
أبلغت ربى وحدة الجرائم الإلكترونية الأردنية، والتي تعاملت مع الموقف بجدية.
قدمت بلاغًا رسميًا، وتم تحليل الصور بواسطة خبراء تقنيين أثبتوا أنها مزورة.
تم تتبع الحساب المجهول، وكان خلفه شخص من داخل الجامعة، وتم توقيفه قانونيًا وفق المادة ٢٣ من قانون الجرائم الإلكترونية.

الدروس المستفادة للطلبة:
أي شخص يمكن أن يكون ضحية للفبركة العميقة (Deepfake)، حتى لو لم ينشر صورًا غير لائقة.
لا يجب الاستجابة للابتزاز أو دفع المال، لأن ذلك قد يزيد من الابتزاز.
الإبلاغ الفوري عن هذه الحالات يمكن أن ينقذ الضحية ويمنع انتشار الصور.

ورشة تفاعلية مقترحة

ورشة تفاعلية مقترحة

حالة ٢:
مراقبة فتاة عبر برامج التجسس من قبل شريكها السابق

القصة:
"ليان"، طالبة جامعية، لاحظت أن شريكها السابق يعرف تفاصيل لا يمكنه معرفتها عن حياتها اليومية، مثل مكان وجودها والمحادثات التي أجرتها مع صديقاتها. بعد فحص هاتفها، اكتشفت أن تطبيق تجسس مخفي كان يعمل في الخلفية، ويرسل بيانات موقعها ورسائلها إلى شخص مجهول.

كيف تم التعامل مع المشكلة؟
استعانت بصديقة متخصصة في الأمن السيبراني، والتي قامت بفحص هاتفها واكتشفت التطبيق المخفي
أبلغت وحدة الجرائم الإلكترونية، وتم تتبع الجاني الذي كان يستخدم البرنامج للتجسس عليها
تم اتخاذ إجراءات قانونية ضده وفق قانون الجرائم الإلكترونية، انتحال الهوية الرقمية والمراقبة غير القانونية).

الدروس المستفادة للطلبة:
يجب فحص الهاتف بانتظام للتأكد من عدم وجود تطبيقات تجسس غير معروفة.
تجنب مشاركة الهاتف مع الآخرين، حتى لو كانوا أصدقاء مقربين.
يمكن معرفة التطبيقات المشبوهة عبر التحقق من التطبيقات التي تستهلك البطارية والإنترنت بشكل غير طبيعي.

حالة ٣:
نصب واحتيال عبر الذكاء الاصطناعي والمحادثات المزيفة

القصة:
"خالد"، طالب جامعي، تلقى رسالة على إنستغرام من فتاة تبدو حقيقية، تبادلا الحديث لفترة، ثم طلبت منه إرسال بيانات حسابه البنكي "لتحويل مبلغ مكافأة دراسية". بعد ذلك، تم سحب ٢٠٠ دينار من حسابه. لاحقًا، اكتشف أن الحساب كان يُدار بواسطة روبوت ذكاء اصطناعي (Chatbot) يستخدم صورًا مزيفة، وأن المجرم كان يستهدف ضحايا آخرين بالطريقة نفسها.

كيف تم التعامل مع المشكلة؟
توجه خالد للبنك وأوقف جميع التعاملات المشبوهة.
أبلغ منصة إنستغرام عن الحساب الوهمي، وتم حذفه.
نشر تجربته بين زملائه لتوعيتهم ضد عمليات النصب الرقمي.

الدروس المستفادة للطلبة:
لا تثق بأي شخص يطلب منك معلومات شخصية أو بنكية عبر الإنترنت.
استخدم البحث العكسي عن الصور (Google Reverse Image Search) لمعرفة إذا كانت الصورة تخص شخصًا حقيقيًا أو مزيفة.
احذر من الحسابات الجديدة التي لا تملك سجلًا طويلًا من النشاط.

النشاط: "هل تستطيع كشف الفبركة العميقة؟"

الأهداف:

تدريب الطلبة على التعرف على الصور والفيديوهات المزيفة.
رفع مستوى الوعي بالذكاء الاصطناعي وتأثيره في العنف الرقمي.

الخطوات:

يعرض الأستاذ ٥ صور أو فيديوهات، بعضها حقيقي وبعضها مفبرك باستخدام Deepfake.
يُطلب من الطلبة تحديد أيها حقيقي وأيها مزيف، مع تقديم مبررات لاختياراتهم.
بعد كل صورة أو فيديو، يشرح الأستاذ العلامات التي تدل على التزوير، مثل:
- عدم تطابق تعابير الوجه بشكل طبيعي.
- خلل في حركة الفم والعينين.
- جودة الصورة المتغيرة في مناطق معينة.
في النهاية، يقدم الأستاذ أدوات كشف الفبركة التي يمكن للطلبة استخدامها مثل InVID و Deepware.

الفائدة:

يكتسب الطلبة مهارات عملية في كشف المحتوى المزيف.
يصبح لديهم وعي أعمق بمخاطر Deepfake والذكاء الاصطناعي في العنف الرقمي.

المصادر

المصادر العربية:

- البداينة، دياب. (٢٠١٤). الجرائم الإلكترونية: المفهوم والأسباب. ورقة علمية مقدمة في الملتقى العلمي حول الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية الدولية، كلية العلوم الاستراتيجية، قطر.
- اللجنة الاقتصادية والاجتماعية لغربي آسيا – الإسكوا. (بدون تاريخ). تعريف مصطلح التحرش الإلكتروني.
- عبدالكريم، أ.، وهاب، ت.، عبدالأمر، م.، حسين محمد، ج.، وجمعة، م. (2025). الدليل الشامل للتعامل مع قضايا العنف الرقمي ضد النساء في العراق. مؤسسة أنسم للحقوق الرقمية، ومؤسسة SecDev. رخصة المشاع الإبداعي
- الطبي. (2024). التنمر الإلكتروني.
- سلاما@. (2023). دليل مواجهة العنف الرقمي لطالبات الجامعات في الأردن.
- صقر، وفاء محمد. (٢٠٢٤). جريمة الابتزاز الإلكتروني. مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة بني سويف، ٣٦(2).

المصادر الأجنبية:

- European Institute for Gender Equality. (2022). Cyber violence against women and girls: Key terms and concepts.
- ICRC Humanitarian Law & Policy Blog. (2024). Online violence: Real life impacts on women and girls in humanitarian settings.
- Polyzoidou, V. (2024). Digital violence against women: Is there a real need for special criminalization? International Journal for the Semiotics of Law, 37, 1777–1797.
- Stopbullying.gov. (2024). What is cyberbullying?

الملحقات

لمزيد من المعلومات وللاستزادة من التحديثات الجارية:

١. الحماية الرقمية (عربي) - معلومات أمنية وأدلة تدريبية وأدوات موصى بها باللغة العربية.

2. Security-in-a-Box (باللغتين العربية والإنجليزية) - معلومات حول الأمن الرقمي وأدلة تدريبية وموارد أخرى.

٣. FrontLine Defenders (باللغتين العربية والإنجليزية) - معلومات ودعم بشأن المخاطر الرقمية وغيرها من المخاطر الأمنية للمدافعين عن حقوق الإنسان.

٤. سلامة تك (عربي) - أخبار الأمن الرقمي، مصادر التعلم الذاتي، الدعم الفني، التدريب والمساعدة العاجلة.

٥. الدفاع عن النفس ضد المراقبة (باللغتين العربية والإنجليزية): نصائح وأدوات وإرشادات لاتصالات أكثر أماناً عبر الإنترنت، تديرها مؤسسة Electronic Frontier Foundation.

6. Safe Sisters (بالإنجليزية) - برنامج زمالة وموارد تستهدف بشكل خاص المدافعات عن حقوق الإنسان والصحفيات أو العاملات في مجال الإعلام والناشطات للتدريب على تحديات الأمن الرقمي.

تقييم وتطوير الدليل

رأيك مهم!

ندعوك لتقييم دليل « دليل إرشادي تفاعلي للحد من العنف الرقمي « عبر الاستبيان التالي لمساعدتنا في تطوير أدوات أكاديمية فعّالة لحماية الطلبة وتعزيز وعيهم حول العنف الرقمي.

امسح رمز QR أدناه للمشاركة:

https://docs.google.com/forms/d/1_hOLLSIansJnnKDR8LkMoAGRH6tcpQ9XBcgOAJAlg2o/preview

يستغرق الاستبيان أقل من ٥ دقائق. شكراً لمساهمتك في بناء بيئة جامعية أكثر أمانًا ومسؤولية.