وزارة التنميـــــة الاجتماعيـــــة والأســـــرة
Ministry of Social Development and Family
State of Qatar • دولـــة قطـــر

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency



الحملة الدولية السنوية لمناهضة العنف ضد المرأة

الأمـــن الرقمـــي للمـــرأة

الشريحة المستهدفة
المرأة



الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy



الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

الحملة الدولية السنوية لمناهضة العنف ضد المرأة

الأمـــن الرقمـــي للمـــرأة

الشريحة المستهدفة

المرأة

كُتَيّب المُدَرّب

الموضوع	رقم الصفحـة
المحور الأول: مبادئ الأمن الرقمي	6
مفهوم الأمن الرقمي	7
أهمية الخصوصية الرقمية	8
الاستخدام الآمِن للأجهزة	9
إعدادات الخصوصية	10
حماية البيانات	11
السؤال التفاعلي الأول	12
المحور الثاني: أبرز التهديدات الرقمية للنساء والفتيات	13
أبرز أشكال التهديدات الرقمية للفتيات	14
من وسائل وقاية الفتيات من التهديدات الرقمية	16
أبرز أشكال التهديدات الرقمية للسيدات	17

الموضوع	رقم الصفحـة
من وسائل وقاية السيدات من التهديدات الرقمية	18
أبرز أشكال التهديدات الرقمية لكبيرات القَدْر	19
من وسائل وقاية كبيرات القَدْر من التهديدات الرقمية	20
أبرز أشكال التهديدات الرقمية لعاملات المنازل	21
من وسائل وقاية عاملات المنازل من التهديدات الرقمية	22
السؤال التفاعلي الثاني	23
السؤال التفاعلي الثالث	24
المحور الثالث: الإبلاغ عن التهديدات	25
توثيق الأدلة الرقمية	26
الإبلاغ عن التهديدات	27
السؤال التفاعلي الرابع	28

الموضوع	رقم الصفحـة
المحور الرابع: تمكين المرأة رقميًّا	29
تعزيز الوعي بحقوق المرأة في الفضاء السيبراني	30
مبادرات لدعم النساء في مجالات الأمن السيبراني	31
دور الأكاديمية الوطنية للأمن السيبراني في تمكين المرأة رقميًّا	33
السؤال التفاعلي الخامس	37
إجابات الأسئلة التفاعلية	38
المراجع	40



المحور الأول

مبادئ الأمن الرقمي

مفهوم الأمن الرقمي

الأمن الرقمي هو القدرة على استخدام التقنيات الحديثة والإنترنت بشكلٍ آمِن ومسؤول يحمي خصوصية المرأة ويصون بياناتها من أيّ تهديد أو إساءة.
يهدف إلى تمكين النساء من التفاعل مع العالم الرقمي بثقة ودون خوف من الاستغلال أو التتبُّع.



- يشمل حماية الأجهزة والبيانات الشخصية
- يُعزّز الثقة في التعامل مع المنصات الإلكترونية
- يَحُدّ من المخاطر قبل وقوعها من خلال الوعي والممارسات الوقائية

أهمية الخصوصية الرقمية

الخصوصية الرقمية تعني الحفاظ على المعلومات الشخصية من الوصول غير المُصرَّح به، سواء من أفراد أو جهات خارجية.
بالنسبة للمرأة، تُعدّ الخصوصية الرقمية أساس الأمان النفسي والاجتماعي.

من وسائل المحافظة على الخصوصية الرقمية



- تجنّب مشاركة الصور والمعلومات الحساسة على المنصات العامة
- عدم قبول طلبات الصداقة من أشخاص مجهولين
- مراجعة إعدادات الخصوصية بانتظام في كلّ تطبيق
- التفكير قبل النشر؛ فالمحتوى الرقمي لا يختفي بسهولة

الاستخدام الآمِن للأجهزة

الأجهزة الذكية أصبحت جزءًا لا يتجزّأ من حياة المرأة اليومية، لذلك فإنّ تأمينها يُعدّ أولوية.

قفل الجهاز ببصمة أو كلمة مرور قوية

تحديث نظام التشغيل والتطبيقات باستمرار

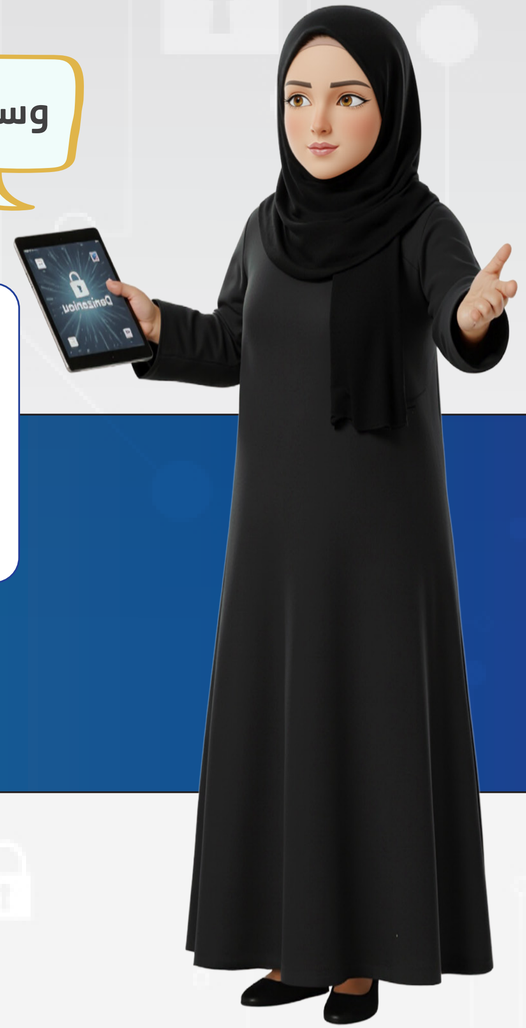
تفعيل خاصية "العثور على الجهاز" للمساعدة عند فقدان الجهاز أو سرقته

تجنّب تثبيت التطبيقات من مصادر مجهولة



إعدادات الخصوصية

وسائل التواصل تُمثِّل مساحة للتعبير، لكنّها أيضًا بيئة مفتوحة قد تُعرِّض المرأة للمخاطر إذا لم يتم إدارتها بوَعْي.



- تفعيل المصادقة الثنائية لحماية الحسابات
- تحديد مَن يمكنه رؤية المنشورات والتفاعل معها
- إلغاء أذونات التطبيقات غير الموثوقة المرتبطة بالحساب
- تجنّب مشاركة الموقع الجغرافي في أثناء التنقل أو السفر
- مراجعة إعدادات الحسابات الاجتماعية، وتحديد مَن يمكنه رؤية المنشورات
- حَصْر قبول طلبات الصداقة بالأشخاص المعروفين
- عدم مشاركة تفاصيل الحياة اليومية بشكلٍ متكرّر

حماية البيانات



تُعدّ الصور والمحادثات العائلية من أكثر أنواع البيانات حساسية.

- استخدام تطبيقات مراسلة آمِنَة بتقنية التشفير الطرفي
- حَذْف الرسائل القديمة، أو التي تتضمَّن بيانات شخصية
- تجنّب إرسال الصور أو المستندات الحساسة عبر البريد أو الرسائل العامة
- الاحتفاظ بنُسَخ احتياطية مُشفَّرة للبيانات الهامة
- عدم تخزين الصور الحساسة على الأجهزة المتصلة بالإنترنت
- استخدام تطبيقات تشفير لحِفْظ الصور الخاصة
- حَذْف الصور المُكرَّرة أو غير الضرورية بانتظام

السؤال التفاعلي الأول



1 ما أفضل ممارسة لحماية حساباتك الرقمية؟

أ. استخدام كلمة مرور واحدة لكل الحسابات

ب. تفعيل المصادقة الثنائية، وتغيير كلمة المرور دوريًّا

ج. مشاركة كلمة المرور مع صديقة موثوقة

د. ترك الحسابات مفتوحة على الأجهزة العامة



المحور الثاني

أبرز التهديدات الرقمية للنساء والفتيات

أبرز أشكال التهديدات الرقمية للفتيات



التحرُّش الرقمي

عبر إرسال رسائل غير مرغوبة، أو صور مسيئة

الابتزاز عبر الإنترنت

التهديد بنشر صور أو تزوير مقاطع صوت أو فيديو

المُلاحَقة الإلكترونية

رسائل مُزعِجَة ومحاولة اختراق الحسابات

أبرز أشكال التهديدات الرقمية للفتيات



التنمُّر الإلكتروني

تعليقات جارحة أو مسيئة

سرقة الهوية الرقمية

اختراق الحسابات وسرقة البيانات الشخصية

التلاعب العاطفي عبر الإنترنت

وعود زائفة واستغلال الثقة لأغراض ضارَّة

من وسائل وقاية الفتيات من التهديدات الرقمية

عدم مشاركة المعلومات الشخصية على مواقع التواصل الاجتماعي

تجاهل الرسائل المسيئة، وحظر المُرسِل

ضبط إعدادات الخصوصية في حسابات التواصل الاجتماعي

عدم قبول طلبات صداقة من أشخاص مجهولين



إبلاغ مركز مكافحة الجرائم الالكترونية في وزارة الداخلية

إطلاع الأهل على أيّ تهديدات رقمية

توثيق التهديدات من خلال الاحتفاظ بصور للرسائل المزعجة

أبرز أشكال التهديدات الرقمية للسيدات



الاحتيال المالي

مواقـع تسـوُّق وهميـة لسـرقة البيانـات الماليـة

سرقة البيانات الشخصية

عبـر تحميـل تطبيقـات غيـر آمِنَـة أو مشـاركة البيانـات الشـخصية

البرمجيات الخبيثة

تحميل تطبيقات من مواقع غير موثوقة قد يؤدي إلى سرقة البيانات الشخصية أو المالية

الاختراق المنزلي

الأجهـزة الذكيـة مثـل الكاميـرات المتصلـة بالإنترنت يمكن اختراقهـا؛ إن لم تكن محمية بكلمـات مرور قويـة

من وسائل وقاية السيدات من التهديدات الرقمية

- عدم مشاركة البيانات الشخصية على مواقع التواصل الاجتماعي
- تحميل التطبيقات من المواقع الرسمية الموثوقة
- حماية الأجهزة المنزلية الذكية بكلمات مرور قوية
- الشراء من المواقع الإلكترونية الموثوقة والرسمية
- تفعيل المصادقة الثنائية لحسابات التواصل الاجتماعي
- عدم النقر على الروابط المجهولة
- الإبلاغ عن أيّ تهديد رقمي



أبرز أشكال التهديدات الرقمية لكبيرات القَدْر



الاحتيال المالي

مثل مكالمات أو رسائل مُزيَّفة تطلب تحويل أموال أو بيانات مالية

الروابط الاحتيالية

روابط مُزيَّفة على منصات التواصل الاجتماعي مثل واتساب أو فيسبوك

ضعف المعرفة التقنية

يجعل بعض النساء هدفًا سهلًا لهجمات الهندسة الاجتماعية

من وسائل وقاية كبيرات القَدْر من التهديدات الرقمية

عدم الضغط على أيّ رابط مجهول المصدر

عدم تقديم أيّ بيانات شخصية أو مالية عبر منصات التواصل الاجتماعي



يُفضَّل سؤال أحد أفراد الأسرة قبل القيام بأيّ إجراء تقني جديد

الإبلاغ عن أيّ تهديد رقمي

أبرز أشكال التهديدات الرقمية لعاملات المنازل

الاحتيال المالي
روابط تحويل وهمية أو طلبات مساعدة مُزيَّفة من "أصدقاء"

الابتزاز الإلكتروني
عبر استغلال صورها أو مكالماتها

نشر معلومات عن العائلة أو المنزل دون قصد
وهذا يُشكِّل خطرًا أمنيًّا على الأسرة



من وسائل وقاية عاملات المنازل من التهديدات الرقمية

- عدم التصوير داخل المنزل
- عدم الضغط على روابط مجهولة
- عدم مشاركة البيانات الشخصية على مواقع التواصل الاجتماعي
- الاستئذان قبل نشر أيّ معلومات جديدة
- الإبلاغ عن أيّ تهديد رقمي



السؤال التفاعلي الثاني



2 ما هو أول تصرّف يجب القيام به عند التعرّض لرسائل تهديد أو ابتزاز عبر الإنترنت؟

أ. حذف الحساب فورًا

ب. إرسال المال للمبتز

ج. توثيق الرسائل والاحتفاظ بها كدليل، ثم إبلاغ الجهات المختصة

د. تجاهل التهديد وعدم إخبار أحد

السؤال التفاعلي الثالث



3 أيٌّ من الخيارات التالية يُعتبر سلوكًا آمِنًا يحمي من الاحتيال المالي عبر الإنترنت؟

أ. إدخال رقم البطاقة في أيّ موقع يعرض تخفيضات مُغْرية

ب. الشراء فقط من المواقع الإلكترونية الموثوقة

ج. مشاركة معلومات البطاقة مع صديقة لتساعد في الشراء

د. حفظ كلمة المرور في الملاحظات على الهاتف



المحور الثالث

الإبلاغ عن التهديدات

توثيق الأدلة الرقمية

توثيق الأدلة يُعدّ أهمّ خطوة قانونية في التعامل مع العنف الإلكتروني.

- تصوير الشاشة مع حفظ التاريخ والوقت
- عدم حذف الرسائل أو الحساب المسيء
- حفظ روابط الصفحات والمحادثات الأصلية
- التواصل مع الجهات المختصة في الدولة



الإبلاغ عن التهديدات

الاتصال بالرقم الساخن
66815757

الاتصال بالرقم
2347444



تطبيق وزارة الداخلية
"مطراش2"

البريد الإلكتروني
cccc@moi.gov.qa

السؤال التفاعلي الرابع



4 في حال تلقّي تهديد رقمي داخل دولة قطر، فأيّ ممَّا يلي يُعدّ مِن الطُّرق الرسمية للتبليغ؟

أ. التواصل عبر تطبيق وزارة الداخلية "مطراش2"

ب. نشر القصة على وسائل التواصل الاجتماعي

ج. طلب المساعدة من صديق عبر الإنترنت

د. تجاهل التهديد وانتظار أن يختفي



المحور الرابع

تمكين المرأة رقميًّا

تعزيز الوعي بحقوق المرأة في الفضاء السيبراني

تتمتع المرأة بحقوق رقمية أساسية؛ تشمل: الخصوصية، والحرية في التعبير، والحماية من الاستغلال أو التتبُّع.

الوعي بهذه الحقوق يُعزّز قدرتها على المطالبة بالحماية القانونية عند انتهاكها

الاطلاع على سياسات المنصات الرقمية المتعلّقة بحماية المستخدمين

الإبلاغ عن أيّ محتوى يَنتهك الخصوصية أو يُستخدَم دون إذن

دعم المبادرات التي تُعنَى بالمساواة الرقمية وتمثيل المرأة في الفضاء السيبراني



مبادرات لدعم النساء في مجالات الأمن السيبراني

المبادرات الوطنية



المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

مَنَاهِج **الأَمْن السِّيبْرَانِيّ** التَّعْلِيمِيَّة
Cyber Security Curricula Education

CyberEco

المخيـــم الشبابي
السيبراني الصيفي

مبادرات لدعم النساء في مجالات الأمن السيبراني



المبادرات الدولية

Women4Cyber Foundation

منظمة أوروبية غير ربحية تدعم مشاركة النساء في التدريب والتوظيف، وإنشاء فروع وطنية في عدة دول أوروبية.

She@Cyber (Erasmus+ Program)

مشروع أوروبي لتدريب النساء من خلفيات غير تقنية على أساسيات الأمن السيبراني عبر منصات تعليمية مجانية.

Cynder Project (OAS)

مبادرة في أمريكا والبحر الكاريبي لدَمْج المرأة في سياسات الأمن السيبراني، وتعزيز مهارات النساء والفتيات رقميًّا.

دور الأكاديمية الوطنية للأمن السيبراني في تمكين المرأة رقميًّا



تعمل الأكاديمية الوطنية للأمن السيبراني على تمكين المرأة رقميًّا من خلال البرامج والمبادرات التي أطلقتها، وهي:

- المبادرة الوطنيّة للسلامة الرقميّة
  Digital Safety National Initiative
- مَنَاهِج الأَمْن السِّيبْرَانِيّ التَّعْلِيمِيَّة
  Cyber Security Curricula Education
- CyberEco
- المخيـــم الشبابي السيبراني الصيفي



المبادرة الوطنيّة للسلامة الرقميّة
Digital Safety National Initiative

تَستهدف مختلف شرائح المجتمع

المرأة والأسرة من الشرائح الرئيسة المستهدَفة

تقديم محتوى توعية يُعزّز من الأمان الرقمي للنساء

يتم تقديم محتوى التوعية للنساء من خلال:

- دليل السلامة الرقمية
- كُتَيّب السلامة الرقمية للأسرة
- لعبة إلكترونية (البيت السيبراني)
- ورش توعية

مَنَاهِج **الأَمْن السِّيبْرَانِيّ** التَّعْلِيمِيَّة
Cyber Security Curricula Education

يستهدف الطلبة في مختلف المراحل التعليمية

يقدم محتوى توعية للطالبات

يُعزّز من قدرة الفتيات على التعامل الآمِن مع الإنترنت

حصل المشروع على عدة جوائز دولية



يتم نقل التجربة إلى دول مجلس التعاون لدول الخليج العربية

تم تطبيق المشروع في 433 مدرسة

استفاد من محتوى التوعية 583,000 طالب وطالبة

CyberEco

- يستهدف الطلبة في مختلف المراحل التعليمية
- يدمج التعليم بالترفيه
- يقدم محتوى توعية للطالبات
- تم تطبيق المشروع في 207 مدارس
- يُعزّز من قدرة الفتيات على التعامُل الآمِن مع الإنترنت
- استفاد من المشروع 10,608 من الطلاب والطالبات



المخيَّم الشبابي السيبراني الصيفي

يستهدف الطلبة والطالبات الشباب

يتبنّى ويُطوّر المواهب السيبرانية



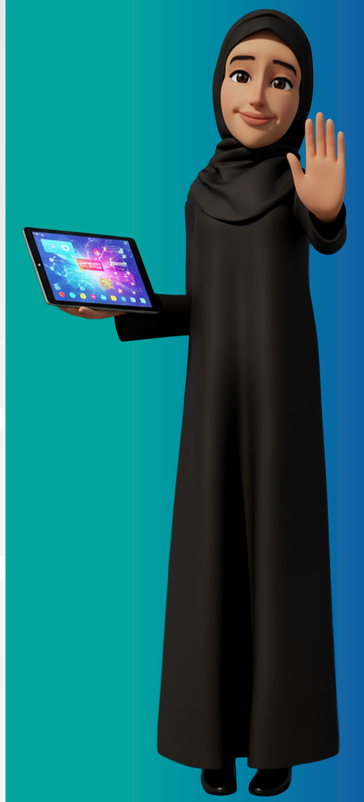
يُقدّم محتوى توعية وتدريب للطالبات

استفاد من المشروع 200 طالبة

يُعزّز الوعي بمفاهيم الأمن السيبراني

يتضمَّن أدوات توعية وتدريب متنوّعة

السؤال التفاعلي الخامس



5 أيٌّ ممَّا يلي يُعدّ مِن الحقوق الأساسية للمرأة في الفضاء السيبراني؟

أ. مشاركة جميع بياناتها علنًا

ب. التنازل عن خصوصيتها مقابل استخدام المنصات

ج. الخصوصية، والحماية من التتبُّع والاستغلال

د. نشر معلومات الآخرين بحُرّية



إجابات الأسئلة التفاعلية

01 **إجابة السؤال التفاعلي الأول**

ب. تفعيل المصادقة الثنائية، وتغيير كلمة المرور دوريًّا

02 **إجابة السؤال التفاعلي الثاني**

ج. توثيق الرسائل والاحتفاظ بها كدليل، ثم إبلاغ الجهات المختصة

03 **إجابة السؤال التفاعلي الثالث**

ب. الشراء فقط من المواقع الإلكترونية الموثوقة

04 **إجابة السؤال التفاعلي الرابع**

أ. التواصل عبر تطبيق وزارة الداخلية «مطراش2»

05 **إجابة السؤال التفاعلي الخامس**

ج. الخصوصية، والحماية من التتبُّع والاستغلال

المراجع

1. ernest, nonum et al. SOCIAL ENGINEERING: UNDERSTANDING HUMAN FACTORS IN CYBER SECURITY. International Journal of Convergent and Informatics Science Research. May 2025, on site: https://harvardpublications.com/hijcisr/article/view/326
2. eSafety Commissioner (Australia). Staying safe: Cyberstalking, on site: https://www.esafety.gov.au/key-topics/staying-safe/cyberstalking
3. European Institute for Gender Equality. Cyber violence against women, on site: https://www.eige.europa.eu/gender-based-violence/cyber-violence-against-women
4. European Parliament. (2023). IPOL_STU(2023)743341_EN [PDF]. on site: https://www.europarl.europa.eu/RegData/etudes/STUD/2023743341//IPOL_STU(2023)743341_EN.pdf
5. IBM. What is malware?, on site: https://www.ibm.com/think/topics/malware
6. Karnouskos, Stamatis. Artificial Intelligence in Digital Media: The Era of Deepfakes, IEEE TRANSACTIONS ON TECHNOLOGY AND SOCIETY, June 2020, on site: https://ieeexplore.ieee.org/document/9123958

7. Kosinski, Matthew. IBM. What is phishing?, on site: https://www.ibm.com/think/topics/phishing
8. Kosinski, Matthew. IBM. What is ransomware? Retrieved, on site: https://www.ibm.com/think/topics/ransomware
9. National Cyber Security Centre. Password policy: updating your approach. November 2018, on site: https://www.ncsc.gov.uk/collection/passwords/updating-your-approach
10. Startup Defense. Fake software update prompts. on site: https://www.startupdefense.io/cyberattacks/fake-software-update-prompts
11. UN Women. FAQs: Digital abuse, trolling, stalking and other forms of technology-facilitated violence against Iwomen. February 2025, on site: https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women
12. United Nations Office on Drugs and Crime. Handling of digital evidence (Module 6), on site: https://www.unodc.org/e4j/ar/cybercrime/module-6/key-issues/handling-of-digital-evidence.html

الأكاديمية الوطنية للأمن السيبراني
National Cyber Security Academy

الوكالة الوطنية للأمن السيبراني
National Cyber Security Agency

للتواصل مع الأكاديمية الوطنية للأمن السيبراني

16555 - 40466379 - 51045944

www.ncsa.gov.qa academy@ncsa.gov.qa