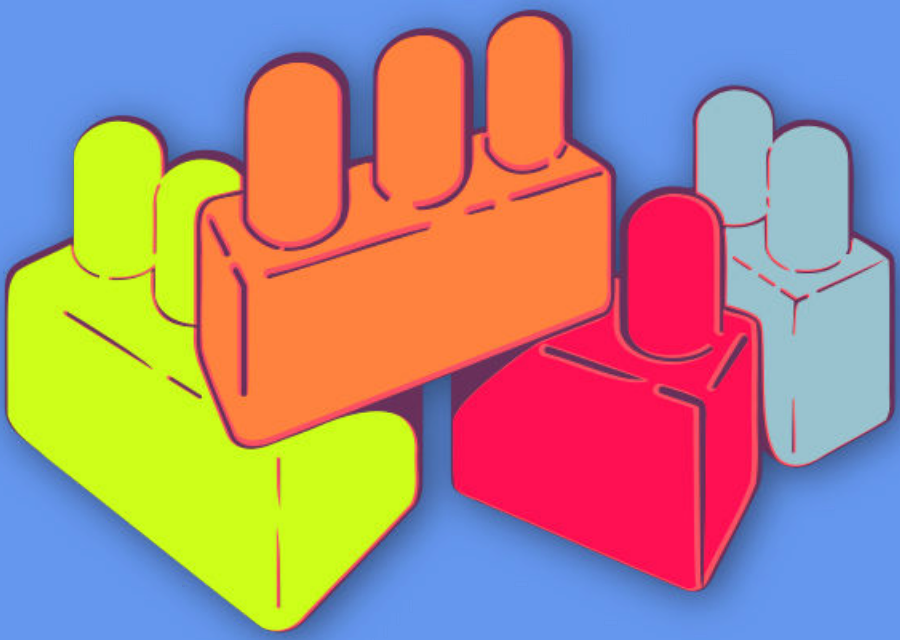

أسس الأمن الرقمي الجولة الأولى

التصفّح الآمن

INSTITUTE FOR
WAR & PEACE REPORTING

https://iwpr.net/

المحتويات

باب ١

التصفّح الآمن

- **الأهداف:** توفر هذه الجلسة مقدمة حول ممارسات تصفّح الإنترنت الآمنة، بما في ذلك لمحة عامة عن البرامج المضافة والمنافع الأخرى الممكن استخدامها لإنشاء بيئة تصفّح أكثر أمانًا.
- **الطول:** 45 دقيقة
- **الشكل:** جلسة
- **مستوي المهارة:** أساسي
- **المعرفة المطلوبة:**
  - غير ضرورية
- **جلسات/تمارين ذات صلة:**
  - كيف يعمل الإنترنت؟[١]
  - كيفية حماية حاسوبكن[٢]
- **المواد اللازمة:**
  - شرائح (مع النقاط المفتاحية الواردة أدناه)

---

[١] https://vrr.im/7ba9
[٢] https://vrr.im/ac95

- حاسوب محمول/حاسوب والتجهيزات الخاصة بجهاز العرض
- إمكانية اتصال بشبكة إنترنت لاسلكي

إدارة الجلسة

الجزء الأول – إختيار المتصفّح

١. إبدأن الجلسة بسؤال المشاركات عن متصفحات الإنترنت التي يستخدمنها والخيارات الأخرى التي سمعن عنها. قدمن لهن متصفّح فايرفوكس Firefox – إشرحن فوائد استخدامه وناقشن بإيجاز الفرق بينه وبين المتصفحات الشائعة الأخرى من قبيل غوغل كروم Google Chrome أو إنترنت إكسبلورير Internet Explorer.

إختياري: عند العمل مع النساء الناطقات باللغة العربية، قد تجدن هذا الفيديو مفيدا لبدء النقاش.

https://www.youtube.com/watch?v=cTrN1OAMYkM

الجزء الثاني – ممارسات التصفّح الأكثر أمانًا

٢. تتوفر بعض ممارسات التصفّح الأكثر أمانًا التي يمكنكن مناقشتها مع المشاركات – ومع أنكن غير مضطرات للتحدث عنها جميعها معهن، يوصى بأن تشاركن ما يكفي لإعطاء المشاركات خيارات متنوعة (لا تنسين أيضًا أن تحرصن على أن يكون المحتوى مناسبًا ومهماً لبيئة المشاركات).

٣. إشرحن للمجموعة أنكن ستقمن بمراجعة بعض ممارسات التصفّح الآمن معهن، ولكن لن تركزن الآن على أدوات محددة غير المتصفحات بحد ذاتها. بعض المشاركات قد يرغبن منذ هذه اللحظة بتغيير المتصفحات التي يستخدمنها ولكن الأخريات قد لا يكن جاهزات لذلك – لذا قبل مناقشة بعض الأدوات المحددة كالبرامج المضافة إلى

المتصفحات، لابد من إبقاء تركيز النقاش على الممارسة في البدايةً.
إليكن بعض الممارسات التي يمكنكن طرحها للنقاش:

البقاء متيقظات تجاه محاولات التصيّد والتصيّد المستهدف.
حجب الإعلانات المضمنة (embedded ads) والإعلانات المفاجئة. (pop-up ads)
معرفة كيفية عمل ملفات تعريف الإرتباط (كوكيز) – إحرصن على التحدث عن مدى تسهيلها للتصفّح ولكن أيضًا عن سلبياتها.
تعطيل ومحو ملفات تعريف الإرتباط من المتصفحات.
محو سجل التصفّح؛
عدم حفظ كلمات السرّ في إعدادات متصفحكن.
التحقق من البرامج المضافة التي قمتن بإضافتها إلى متصفحكن.
تشغيل خيار "عدم التعقّب" (Do Not Track) في متصفحكن.
استخدام بدائل عن محرّك بحث غوغل (مثل دك دك غو Duck Duck Go)
معرفة من يقوم بالتعقّب على الإنترنت ولماذا؟ (كلا الرابطين الموردين أدناه جيدين عن هذه المسألة https://trackography.org/
و https://www.mozilla.org/es-MX/lightbeam/)؛
ناقشن الفرق بين HTTP و HTTPS؛
ما هي الشبكات الإفتراضية الخاصة ومتى يجب إستخدامها؟
كيف يعمل بالظبط التصفّح المتخفي (Incognito Mode or Private Browsing)، ومتى يجب استخدامه؟

الجزء الثالث – الأدوات والبرامج المضافة من أجل تصفّح أكثر أمانًا

٤. إشرحن، بعد أن عالجتن بعض الممارسات الأساسية للتصفّح الآمن، أنه يمكنكن أيضًا إقتراح أدوات معيّنة – البرامج المضافة بالتحديد – التي قد تساعد أو تسهّل عملية إعتماد بعض تلك الممارسات تلقائيًا.

٥. قدمن لهن الأدوات التالية، شارحاتٍ لهن كيفية عمل كل واحدة منها، ولا تنسين أيضًا مشاركة الروابط اللازمة لتنزيلها مع المشاركات. لابد أن تفهم المشاركات أهمية وفائدة كل أداة تمت مشاركتها معهنّ؛ ففي حال لم تشرحنها بشكلٍ واضح، قد يؤدي ذلك إلى إتخاذ المشاركات قرارات مبنية على معلومات خاطئة بشأن خصوصيتهن أوإخفاء هويتهن على الإنترنت.

أدوات متصفح سطح المكتب

أداة "نو سكريبت" [٣](NoScript)

أداة "آدبلوك بلس" [٤](AdBlock Plus)

أداة "برايفيسي بادجر" [٥](Privacy Badger)

أداة "إيتش تي تي بي إس إفريوير" [٦](HTTPS Everywhere)

أداة "كليك أند كلين" [٧](Click & Clean)

متصفّح "تور" [٨](Tor)

---

[٣] https://noscript.net/
[٤] https://adblockplus.org/es/
[٥] https://www.eff.org/es/privacybadger
[٦] https://www.eff.org/https-everywhere
[٧] https://www.hotcleaner.com/
[٨] https://www.torproject.org/download/download-easy.html.en

أداة "يوبلوك" [٩](uBlock)

أداة "ديسكونكت" [١٠](Disconnect)

أداة "يومايتركس" [١١](uMatrix)

أدوات متصفحات الهواتف المحمولة

أداة "إيتش تي تي بي إس إفريوير" [١٢](HTTPS Everywhere)

مكافح الفيروسات "أفاست" [١٣]Avast

أداة "أورفوكس" [١٤](Orfox)

أداة "أوربوت" [١٥](Orbot)

متصفح "تور" [١٦](Tor) لهاتف آيفون

ممارسات وميزات أخرى

التصفّح المتخفي (Incognito Mode/InPrivate Mode)

غالبًا ما تتسبب هذه الميزة بالإلتباس لأنها غير مفهومة بشكلٍ مناسب – وقد لا يتوفر لدى المشاركات فكرة واضحة عن كيفية عمل التصفّح المتخفي كميزة من ميزات المتصفحات ومتى يكون استخدامها مفيدًا. فسّرن لهن كيفية عمل ميزة التصفّح (والميزات المشابهة)، وقدمن لهن بعض الأمثلة عن الحالات التي قد تكون فيها هذه الميزات مفيدة فعليًا.

---

[٩] https://www.ublock.org/

[١٠] https://disconnect.me/

[١١] https://addons.mozilla.org/es/firefox/addon/umatrix/

[١٢] https://www.eff.org/https-everywhere

[١٣] https://www.avast.com

[١٤] https://guardianproject.info/apps/orfox/

[١٥] https://www.torproject.org/docs/android.html.en

[١٦] https://mike.tig.as/onionbrowser/

الممارسات الآمنة على شبكة الإنترنت اللاسكي

ختامًا، ناقشن لبعض الوقت، وقدمن شرحًا إذا أمكن، لبعض الممارسات الآمنة الأساسية الخاصة بالإتصال بشبكات الإنترنت اللاسكي - يتضمن ذلك ممارسات كتغيير كلمات السرّ المحددة مسبقًا الخاصة بالمودم، وشرح كيفية مراقبة الأجهزة المتصلة بشبكة الإنترنت اللاسلكي الخاصة بهن.

المراجع

- https://myshadow.org/ckeditor_assets/attachments/189/datadetoxkit_optimized_01.pdf
- https://myshadow.org/train
- https://myshadow.org/how-to-increase-your-privacy-on-firefox
- https://securityinabox.org/en/guide/firefox/linux/