

مفاهيم الأمن الرقمي وحماية البيانات

الأهداف التعليمية:

- التعرف على مفهوم الأمن الرقمي وأهميته.
- فهم المخاطر الرقمية الشائعة.
- مناقشة استراتيجيات وقائية لحماية المعلومات الشخصية.
- تعزيز الممارسات اليومية للأمن الرقمي.

المقدمة

الأمن الرقمي
وحماية
البيانات



- المدربة تبدأ بسؤال:
- "ما أول شيء يخطر في ذهنك عند سماع كلمة الأمن الرقمي؟"
- جمع الإجابات على السبورة أو ورق فلب شارت.
- التوضيح أن الأمن الرقمي = حماية المعلومات والاتصالات والأجهزة من المخاطر الرقمية.

أساسيات الأمن الرقمي

أ. ما هو الأمن الرقمي؟

هو جميع الممارسات والأدوات التي تحمي خصوصيتنا ومعلوماتنا من الاختراق أو الاستغلال.



ب. المخاطر الرقمية الشائعة:

- البرمجيات الخبيثة (Malware).
- التصيد الإلكتروني (Phishing).
- سرقة الهوية.
- الابتزاز الإلكتروني.

ج. القواعد الأساسية للأمن الرقمي:

- كلمات مرور قوية وفريدة.
- المصادقة الثنائية (FA٢).
- تحديث البرامج والأنظمة بانتظام.
- التحقق من الروابط والرسائل قبل النقر عليها.
- استخدام الشبكات الآمنة (تجنب Wi-Fi العامة المفتوحة).

تمرين



نقاش جماعي - "كيف نحمي أنفسنا؟"

خلاصة وتلخيص

إعادة عرض النقاط الأساسية:

- الأمن الرقمي = حماية المعلومات + الأجهزة + الخصوصية.
- المخاطر: تصيد، اختراق، سرقة هوية، ابتزاز.
- الوقاية: كلمات مرور قوية، FA٢، تحديثات، تحقق من الروابط.

رسالة ختامية:

"الأمن الرقمي يبدأ من عادات صغيرة يومية، لكنها تصنع فرقًا كبيرًا في حمايتنا وحماية أسرنا."



المخرجات:

- وعي بالمخاطر الرقمية الشائعة.
- معرفة أساليب الحماية الأساسية.
- قائمة جماعية بممارسات يومية لتعزيز الأمن الرقمي.

حماية البيانات الشخصية وحسابات التواصل الاجتماعي

الأهداف:

- تعريف المشاركات بماهية البيانات الشخصية ولماذا هي مهمة.
- إبراز المخاطر الشائعة عند مشاركة البيانات على الإنترنت.
- تقديم خطوات عملية لحماية حسابات التواصل الاجتماعي.
- تمكين المشاركات من ممارسة إعدادات الخصوصية والأمان.

مقدمة تفاعلية

سؤال افتتاحي:

- "ما هي آخر مرة طُلب منك إدخال بيانات شخصية عبر الإنترنت؟ وكيف تعاملت معها؟"
- الهدف: ربط الموضوع بتجربة يومية لكل مشاركة.



حماية البيانات الشخصية

ما هي البيانات الشخصية؟

- الاسم الكامل، رقم الهاتف، البريد الإلكتروني.
- الصور والموقع الجغرافي.
- كلمات المرور والمعلومات البنكية.



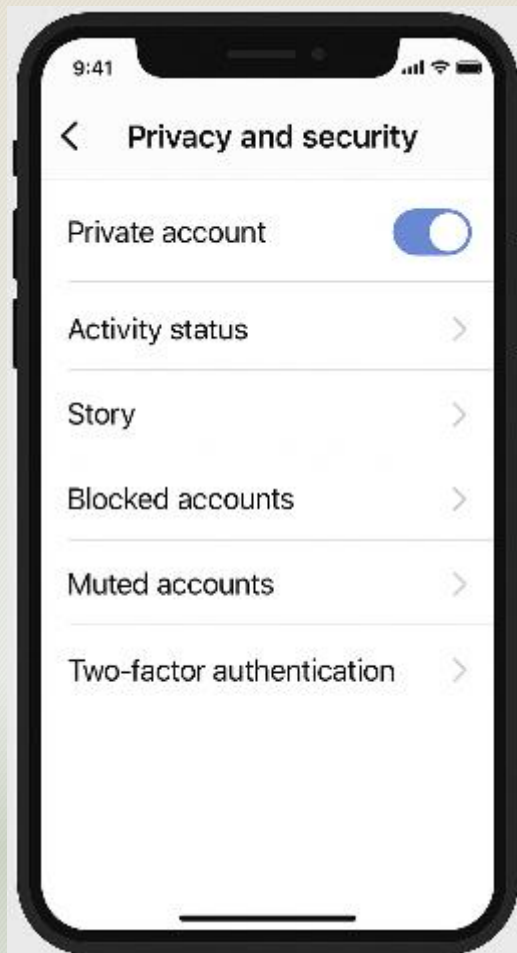
المخاطر:

- سرقة الهوية.
- بيع البيانات لأطراف ثالثة.
- الابتزاز الإلكتروني.

طرق الحماية:

- عدم مشاركة المعلومات الحساسة (العنوان، رقم الهاتف، الصور الخاصة) بشكل علني.
- تشفير الأجهزة وحمايتها بكلمة مرور.
- الحذر عند استخدام شبكات Wi-Fi عامة.

حماية حسابات التواصل الاجتماعي:



المخاطر:

- اختراق الحسابات.
- انتحال الهوية.
- التتمر أو التهديد.

خطوات عملية للحماية:

- كلمات مرور قوية وفريدة لكل حساب.
- تفعيل المصادقة الثنائية (FA٢).
- مراجعة إعدادات الخصوصية:
- من يمكنه رؤية المنشورات.
- من يمكنه إرسال طلبات صداقة.
- التحكم في من يرى المعلومات الشخصية.

تمرين عملي - "تأمين حسابي"



الهدف:

- تطبيق عملي لفحص إعدادات الخصوصية والأمان.

خلاصة وتوصيات

النقاط الأساسية:

- البيانات الشخصية ثمينة مثل المال.
- حسابات التواصل عرضة للمخاطر إذا لم نحصنها.
- الحماية تبدأ من الوعي والإعدادات الصحيحة.

رسالة ختامية:

"كل ضغطة زر على وسائل التواصل هي مسؤولية، فاحمي نفسك قبل أن تشاركى."



المخرجات:

- فهم المخاطر المرتبطة بالبيانات الشخصية.
- خطوات عملية لحماية الحسابات الرقمية.
- تطبيق مباشر لإعدادات الخصوصية والأمان.

آليات التبليغ والإحالة عند التعرض للتهديدات

■ الأهداف التعليمية:

- فهم معنى التبليغ والإحالة وأهميتهما في الحماية الرقمية والمجتمعية.
- التعرف على قنوات وآليات التبليغ (رقمية، محلية، مؤسسية).
- تجربة عملية لمحاكاة سيناريو تهديد وتطبيق خطوات الإحالة الصحيحة.

مقدمة

المدربة تطرح سؤالاً:

- "لو تعرضت لتهديد عبر الإنترنت، ما أول خطوة ستقومين بها؟".
- الهدف: معرفة خبرات المشاركات السابقة وبناء النقاش عليها.



آليات التبليغ



على منصات التواصل الاجتماعي:

- استخدام زر Report/إبلاغ للإبلاغ عن الرسائل المسيئة أو الحسابات المزيفة.
- حظر المرسل لمنع أي تواصل إضافي.

المستوى المحلي:

- الشرطة المجتمعية أو الجهات الأمنية المختصة.
- مراكز الدعم المجتمعي أو الجمعيات النسوية.

على مستوى المنظمات:

- آليات الإحالة (Referral) لجهات تقدم دعم قانوني أو نفسي أو اجتماعي.
- تفعيل سياسات الحماية مثل PSEA (منع الاستغلال والاعتداء الجنسي).

مفهوم الإحالة

- التبليغ = خطوة أولى لإيقاف التهديد أو تسجيل الحالة.

- الإحالة = ربط الناجية بجهة مختصة تقدم الخدمة المطلوبة:

- قانونية (محامون، استشارات قانونية).

- نفسية اجتماعية (أخصائيات، جلسات دعم).

- خدمات حماية (مأوى، خطوط مساعدة).

- مبدأ السرية والأمان: مشاركة المعلومات تكون بموافقة الضحية فقط.



Law



Health



Psychosocial
support



Police

تمرين عملي - محاكاة تبليغ



الهدف:

تجربة تفاعلية تحاكي سيناريو
واقعي لتهديد عبر الإنترنت
وتطبيق آليات التبليغ والإحالة.

الخلاصة



- التبليغ يحمي من التهديد المباشر.
- الإحالة تضمن حصول الضحية على دعم شامل (قانوني، نفسي، اجتماعي).
- السرية والموافقة عنصران أساسيان في أي عملية إحالة.
- العمل الجماعي بين الأفراد، المنصات، والجهات المحلية يعزز الحماية.

المخرجات:

- فهم الفرق بين التبليغ والإحالة.
- معرفة القنوات الرسمية وغير الرسمية للتبليغ.
- ممارسة خطوات عملية عبر تمرين محاكاة.

نهاية اليوم الثاني

شكرا لكم