مارك طويل المادة: الحاسوب

10 – أ الموضوع: الجرائم الإلكترونية

1. **ما هي الجرائم الإلكترونية؟ وما هي أمثلة عليها**؟

الجريمة الإلكترونية هي نشاط غير مشروع موجه للوصول الى المعلومات المخزنة داخل الحواسيب أو الاجهزة الإلكترونية سعياً الى نسخها أو تغييرها أو حذفها. ويمكن اختصار مفهوم الجريمة الإلكترونية بأنها الجريمة التي تستهدف التقنية الإلكترونية بصورة كليه أو جزئية.من الامثلة:

* استخدام الحواسيب وشبكة الانترنت للتخطيط لجريمة مثل السرقة.
* اقتحام المواقع الإلكترونية على الشبكة مثل ايقافها عن العمل.
* جرائم القرصنة مثل استخدام البرامج المقرصنة.
* تشويه السمعة والتشهير بها في المواقع الإلكترونية والبريد الإلكتروني.
* انتحال شخصية فرد أو شركة بهدف الاحتيال مثلاً من خلال البريد الإلكتروني.
* تزوير التوقيع الإلكتروني.
* جرائم الاموال مثل الاختلاس من البنوك.
* الجرائم الماسة بالأمن والاقتصاد الوطني.
* جرائم التغرير والاستدراج .
1. **كيف يمكن للأفراد حماية انفسهم من الإحتيال الإلكتروني**؟
* الحذر من مراسلة الغرباء مثلاً عدم فتح الملفات التي تُرسَل عبر الشبكة العنكبوتية الا بعد التأكد من هوية مرسلها وحماية الحاسوب من الفيروسات وذلك باستخدام برامج أصلية مضادة للفيروسات وتحديث هذه البرامج بشكل دوري.
* مسح محتويات الهاتف عند بيعه باستخدام برامج متخصصة (Wipping Programs) لمسح وحدات التخزين وبطاقات الذاكرة حيث ان الأوامر (Delete) و (Format) ليست كفيلة بحذف محتوى الأقراص الصلبة أو الذاكرة الخارجية بشكل كامل.
* استخدام كلمات سر معقدة بحيث تشمل احرفاً وارقاماً ورموزاً وتغييرها باستمرار كما ينصح باستعمال نظام جدار الحماية (Firewalls).
* الحذر من مواقع التواصل الاجتماعي حيث ينصح بعدم إرسال الصور الشخصية والفيديوهات الخاصة أو أية معلومات حساسة إلى الغرباء عبر مواقع التواصل الاجتماعي.
* عدم ترك الأجهزة الخاصة مع شخص غريب لانه بالإمكان وخلال ثوانٍ معدودةٍ زرع برنامج تجسس أو إنشاء حساب للدخول على الجهاز من الخارج.

1. **كيف يمكن للأفراد التبليغ عن الجرائم الإلكترونية؟ ولمن يجب الإتصال**؟

يمكن للأفراد مراسلة وحدة مكافحة الجرائم الإلكترونية عبر البريد الإلكتروني cyber.crimes@psd.gov.jo أو الاتصال بالرقم المجاني 911 حيث تُقدَّم المساعدة وتُتخذ الاجراءات بشكل سري ومباشر.

1. **ما هي مخاطر مشاركة المعلومات الشخصية عبر وسائل التواصل الاجتماعي؟**

إنعدام الخصوصية وتسريب المعلومات الشخصية إلى اشخاص غرباء ويمكن إساءة استخدام هذه المعلومات وابتزاز اصحابها عن طريق التهديد. كما يمكن للقراصنة إنشاء حساب وهمي يشبه حساب المستخدم المستهدف والإستفادة من الشبكة الاجتماعية كالعمل على اكتساب الثقة من الأصدقاء والدائرة الاجتماعية للحصول على المعلومات وتحقيق انتحال الهوية.

1. **ما هي السلوكيات الآمنة عبر الانترنت التى يجب إتباعها؟**
* إحذر من أن تكون كلمة المرور مطابقة لمعلوماتك الشخصية مثل رقم الهاتف أو تاريخ الميلاد.
* تجنب زيارة المواقع المشبوهة.
* احرص على عدم كشف أرقام حساباتك البنكية للمواقع الغير آمنة.
* تجاهل الرسالة البريدية مجهولة المصدر.
* احرص على ان تكون كلمة المرور خليط من الأرقام والأحرف والرموز.
* لا تشارك صوراً لنفسك أو لعائلتك أو لبيتك مع أي اشخاص تلتقي بهم عبر الانترنت.