بسم الله الرحمن الرحيم

السلام عليكم ورحمة الله وبركاته

الجرائم المعلوماتية

دور وزارة الداخلية في مواجهة الجرائم المعلوماتية:

- التوعية المستمرة للضباط والعاملين في جميع جهات الوزارة
- عقد الندوات المتخصصة في بعض مجالات إساءة استخدام التكنولوجيا الحديثة
- تم إنشاء موقع على شبكة الإنترنت وتخصيص صفحة لتلقي بلاغات وشكاوي المواطنين

دور وزارة الداخلية في مواجهة الجرائم المعلوماتية:

التنسيق مع الجهات المعنية بإصدار التراخيص لمزاولة أشطة تكنولوجيا المعلومات

تم إنشاء قواعد بيانات تخدم أعمال المكافحة والملفات والسجلات الخاصة بذلك

التنسيق مع الأجهزة النوعية المختصة بأعمال المكافحة وتبادل المعلومات

دور وزارة الداخلية في مواجهة الجرائم المعلوماتية:

- المشاركة في وضع مقترحات التشريعات الجديدة لحماية استخدامات الحاسبات والانترنت
- صقل الخبرات العلمية والعملية للضباط والعاملين عن طريق الدورات التدريبية محلياً ودولياً
- المشاركة في المؤتمرات والندوات المنعقدة محلياً وعالمياً في مجال الجريمة المعلوماتية

أسباب مدى صعوبة الإثبات في هذه الجرائم

لاتترك أثر لها بعد ارتكابها

صعوبة الاحتفاظ الفني بآثارها إن وجُدت.

تحتاج إلى خبرة فنية ويصعب على المحقق التقليدي التعامل معها

أسباب مدى صعوبة الإثبات في هذه الجرائم

تعتمد على الخداع في ارتكابها والتضليل في التعرف على مرتكبيها

تعتمد على قمة الذكاء في ارتكابها

وسائل الجرائم الالكترونية وطرق الوقاية منها

صناعة ونشر الفيروسات وهي من أكثر الجرائم انتشاراً وشيوعاً على الإنترنت

النصب والاحتيال كبيع السلع أو الخدمات الوهمية

انتحال الشخصية

أهم طرق الوقاية من القرصنة والجرائم الالكترونية

1- أخذ الحيطة والحذر وعدم تصديق كل مايصل من إعلانات والتأكد من مصداقيتها عن طريق محركات البحث الشهيرة.

2- تجنب فتح أي رسالة إلكترونية مجهولة المصدر بل المسارعة إلى إلغائها.

3- وضع الرقم السري بشكل مطابق للمواصفات الجيدة التي تصعب من عملية القرصنة الوصول إليه من هذه المواصفات (بأن يحتوي على أكثر من ثمانية أحرف، أن يكون متنوع الحروف والرموز واللغات).

5- الحرص على المعلومات الشخصية والحاسب الشخصي وذلك بوضع برامج الحماية المناسبة.

التأمين الإلكتروني للبرامج والبيانات والاتصالات:

1) برامج الحماية من الفيروسات (Anti Virus Scanning) حماية الحواسب من الشبكات والرسائل الالكترونية والملفات التي يتم تحميلها من شبكة الانترنت أو أي مسخدك داخل الشبكة حيث تقوم هذه البرامج بمنع الفيروسات من الدخول لذاكرة الحاسب واكتشافها وإيقاف آثارها التدميرية.

2) أهمية استحداث وسائل تأمينية إلكترونية تمثلت في استخدام بصمات (أصابع – صوت – عين – خط) لتحديد هوية المستخدم ومنع أية محاولات نفاذ غير شرعية لنظم المعلومات الإلكترونية.

التأمين الإلكتروني للبرامج والبيانات والاتصالات:

3) التشفير للمعلومات والمقصود هو تغيير مظهرها بحيث يختفي معناها الحقيقي بحيث تكون غير مفهومه لمن يتلصص عليها من مرتكبي الجرائم التكنولوجية.

4) التوقيع الإلكتروني له أهمية في توفير الحماية اللازمة للتعاملات الاقتصادية والمالية على شبكة الإنترنت ويتم ذلك من خلال مجموعة من البرامج ومفاتيح الشفره الخاصة والعامة والتي تشكل منظومة أمنية دقيقة لضمان أمن وسرية أداء الصفقات الإلكترونية عبر الشبكة.