**محاضرة 2: تكنولوجيا الاتصال ومكافحة الجريمة:**

استنادا إلى ما سبقت الإشارة إليه في المحاضرة السابقة حول الأضرار الجسيمة التي يمكن أن تخلفها الجريمة الالكترونية بشتى أنواعها كان لابد من وجود آليات وتدابير لحماية الأفراد والمؤسسات والدول على حد سواء من هذا النوع المستحدث من الجرائم وهذا ما سنتطرق إليه في هذه المحاضرة من خلال العناصر التالية:

1. **تدابير عامة للوقاية والحماية من جرائم الكمبيوتر والانترنت:**

**(كيفية حماية نفسك عبر الإنترنت من الجرائم الإلكترونية)**

نظرًا لانتشار الجرائم الإلكترونية، وجب على الأفراد المستخدمين لتكنولوجيا الإعلام والاتصال وبالتحديد الكمبيوتر والانترنت وقاية أنفسهم من مخاطر الجرائم الالكترونية وذلك من خلال اتخاذ عدة تدابير عامة تقترحها شركة Kaspersky المختصة في حماية أجهزة الكمبيوتر والبرامج الالكترونية والبيانات الشخصية. وهي كالآتي:

1. **إبقاء البرنامج ونظام التشغيل محدّثَين:**

يضمن إبقاء البرنامج ونظام التشغيل لديك محدّثَين استفادتك من أحدث تصحيحات الأمن لحماية جهاز الكمبيوتر الخاص بك.

1. **استخدام برنامج مكافحة الفيروسات وإبقائه محدّثًا**

يشكّل استخدام برنامج لمكافحة الفيروسات أو حل شامل لأمن الإنترنت طريقة ذكية لحماية النظام من الهجمات. يتيح لك برنامج مكافحة الفيروسات إمكانية فحص التهديدات واكتشافها وإزالتها قبل أن تصبح مشكلة. وجود هذه الحماية يساعد في حماية جهاز الكمبيوتر الخاص بك وبياناتك من الجرائم الإلكترونية، مما يمنحك راحة البال. أبقِ برنامج مكافحة الفيروسات محدَّثًا للحصول على أفضل مستوى من الحماية.

1. **استخدام كلمات مرور قوية**

تأكد من استخدام كلمات مرور قوية لا يمكن للأشخاص معرفتها ولا تقم بتسجيلها في أي مكان. يمكنك كذلك استخدم تطبيق مدير كلمات مرور حسن السمعة لإنشاء كلمات مرور قوية بشكل عشوائي لتسهيل الأمر عليك.

1. **عدم فتح المرفقات في رسائل البريد الإلكتروني العشوائية أبدًا**

تشكّل مرفقات البريد الإلكتروني في رسائل البريد الإلكتروني العشوائية طريقة تقليدية لإصابة جهاز الكمبيوتر ببرامج ضارة وغيرها من أشكال الجرائم الإلكترونية. لا تفتح أبدًا مرفقًا من مرسِل لا تعرفه.

1. **عدم فتح الروابط في رسائل البريد الإلكتروني العشوائية أو على مواقع الويب غير الموثوق بها**

توجد طريقة أخرى يصبح بها الأشخاص ضحايا للجرائم الإلكترونية، وهي فتح الروابط الموجودة في رسائل البريد الإلكتروني العشوائية أو الرسائل الأخرى أو المواقع الإلكترونية غير المألوفة. تجنّب القيام بهذا الأمر للحفاظ على أمنك على الإنترنت.

1. **عدم تقديم المعلومات الشخصية إلا إذا كنت آمنًا**

لا تقدم أبدًا بيانات شخصية عبر الهاتف أو عبر البريد الإلكتروني إلى أي جهة ما لم تكن متأكدًا تمامًا من أمان الخط أو البريد الإلكتروني. تأكد من أنك تتحدث إلى الشخص الذي تعتقد أنك تتحدث معه.

1. **الاتصال بالشركات مباشرةً بشأن الطلبات المشبوهة**

إذا اتصلت بك شركة وطلبت منك معلومات شخصية أو بيانات، أنه المكالمة بدون إعطائهم شيء، ثم أعد الاتصال بهم مرة أخرى باستخدام الرقم الموجود على الموقع الإلكتروني الرسمي الخاص بهم للتأكد من أنك تتحدث إليهم وليس مع مجرمي الإنترنت. الأفضل كذلك استخدام رقم هاتف مختلف لأن مجرمي الإنترنت يمكنهم إبقاء الخط مفتوحًا. عندما تعتقد أنك اتصلت بالشركة مجددًا، يمكنهم الادّعاء بأنهم من المصرف أو مؤسسة أخرى تعتقد أنك تتحدث معها.

1. **التنبّه لعناوين مواقع URL التي تزورها**

راقب عناوين مواقع URL التي تفتحها. هل تبدو مشروعة؟ تجنب الضغط على الروابط التي تحتوي على عناوين URL غير مألوفة أو التي تبدو كرسالة غير مرغوب فيها. إذا كان منتج أمن الإنترنت لديك يشمل وظائف لضمان أمن المعاملات عبر الإنترنت، فتأكد من تمكينها قبل تنفيذ المعاملات المالية عبر الإنترنت.

1. **مراقبة بياناتك المصرفية**

من المهم اكتشاف أنك وقعت ضحية جريمة إلكترونية بسرعة. راقب بياناتك المصرفية واستفسر عن أي معاملات غير مألوفة مع المصرف، ويمكن للمصرف التحقيق فيما إذا كانت احتيالية أم لا.

1. **مكافحة الجريمة الالكترونية من خلال التشريعات: (الجزائر نموذجا)**

إن من الموازنات الأساسية التي سعت مختلف التشريعات لتحقيقها هي التوفيق بين الحقوق والحريات خاصة الشخصية، وبين مقتضيات حفظ الأمن والنظام العام. وفي إطار مواجهة هذه الجريمة المستجدَّة أصدرت الجزائر القانون رقم 09-04 بتاريخ 14 شعبان 1430ه الموافق 5-8-2009م، والمتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. واستند هذا القانون على الدستور و6 قوانين، أوّلها قانون العقوبات وقانون الإجراءات الجزائية. وتضمّن 19 مادة موزَّعة على 6 فصول

كما أنشئت على مستوى محكمة مقر مجلس قضاء الجزائر، قطبا جزائيا متخصصا في المتابعة والتحقيق في الجرائم المتصلة بتكنولوجيا الاتصال والإعلام والهيئة بنص القانون رقم 09/04 أن "الهيئة مؤسسة عمومية ذات طابع إداري تتمتع بالشخصية المعنوية والاستقلال المالي توضع تحت سلطة وزارة الدفاع الوطني." والتي سميت بـ: " **الهيئة الوطنية للوقاية من الجرائم المتعلقة بتكنولوجيا الاتصال والإعلام ومكافحتها".**

1. **مفهوم الأمن السيبيراني:**

يشكل الأمن السيبيراني جزء أساسيا من أي سياسة أمنية وطنية فقد أصبحت الدول تصنف مسائل الدفاع السيبيراني كأولوية في سياساتها الدفاعية كما خصصت أكثر من 130 دولة أقساما خاصة بالأمن السيبيراني في فرقها الأمنية الوطنية، ويقصد بالأمن السيبيراني مجموع الأطر القانونية والتنظيمية والهياكل التنظيمية والوسائل التكنولوجية الوطنية والدولية التي تهدف إلى حماية الفضاء السيبيراني الوطني كما تركز على حماية بيانات الأفراد ومؤسسات الدولة من الاستخدام غير المصرح به أو أي أذى يلحق بشبكة البيانات. إذن فالأمن السيبيراني له 03 جوانب:

-حماية بيانات الأشخاص الالكترونية،

-ومن خلالها حماية الشركات ومؤسسات الدولة وبياناتها وعملائها،

-ثم حماية الأمن القومي وسلامة المواطنين ورفاهيتهم وخصوصيتهم لألا تستخدم هذه البيانات بطرق غير شرعية أو ضد أصحابها.