المحاضرة السادسة: اركان الجريمة الالكترونية و سبل الوقاية منها وإجراءات التحقيق فيها

_أولا- أركانها :_ان للجريمة الالكترونية اركان ثلاثة وتتمثل في :

* الركن الشرعي: وهو الصفة الغير مشروعة للـفعل، وتتمثل في قاعدة التجريم والعقاب فيها من خلال ما ورد النص عليه في القانون المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بالتكنولوجيا الاعــلام والاتصال ومكافحتها.

* الركن المادي: يتمثل في ماديات الجريمة التي تبرز بها الى العالم الخارجي.

* الركن المعنوي: وهي إرادة التي يقترن بها الفعل سواء في صورة القصد او الخطأ.

كما ان للجريمة الالكترونية كغيرها من الجرائم اطراف تتمثل في:

* الجاني او المجرم الالكتروني: وبهذا المعني يكون الجاني شخصا طبيعيا ذا أهلية وقدرة على تحمل العقوبة او حتى شخصا معنوي .

* المجني عليه: يكون في الغالب شخص معنوي كالبنوك والشركات وغيرها من المنظمات والهيئات التي تعتمد في انجاز اعمالها على الحاسب الالي .

* المحل: ان للجريمة الالكترونية محلا يتمثل في المعلومات ،أجهزة ، الأشخاص والجهات. (رشاد، 2018، صفحة 451)

ثانيا- سبل مكافحة الجريمة الالكترونية: توجد سبل متنوعة لمكافحة الجريمة الالكترونية ، حيث تتباين هذه السبل بدرجة فاعليتها وتعقيدها ، وذلك حسب البرامج المصممة لهذا الغرض، ومن بين هذه السبل:

- عمل نسخ من ملفات البيانات

Backups

- استخدام البرامج المضادة للفيروسات

Anti-Virus software

- برامج جدران النار

Firewalls software

نظام او برنامج حماية تحجز البيانات بين الشبكة الداخلية والشبكة الخارجية، أي هو الجهاز الذي يتحكم في تدفق المعلومات بين جهاز الحاسوب والانترنت، والهدف هو حجز كل ما هو غير مرغوب فيه من خارج البيئة المحمية، يستطيع اذن الخروج إلى عالم الانترنت ولكن لا يستطيع من في الخارج الدخول إلى الجهاز من خلاله.

– استخدام الخصائص الفسيولوجية

Biometzics Fingerprint

لحماية النظام مثل بصمة الابهام، حدقة العين ، الصوت وغيرها.

التشفير

Encryption

وتستخدم معظم نظم المعلومات الإدارية الشبكية برامج جدران النار، والبرامج المضادة للفيروسات بالإضافة إلى التشفير لحماية الرسائل والملفات المخفية، وهناك تشفير باستخدام المفتاح العام

Public Key Encryption

المعروف اختصارا باسم

(P K E)

وهو نظام تشفير يستخدم مفتاحين، مفتاح رئيس يمكن ان يستخدم أو أن يحصل عليه أي شخص ومفتاح خاص

Private Key

للشخص المستلم فقط. (قابوسة، 2019، صفحة 251)

بالإضافة الى هذا الإجراءات الوقائية يمكن ان يكون هناك بعض التوصيات فيما يخص الجريمة الالكترونية تتمثل في:

–ضرورة تدخل المشرع القانوني لمواجهة الجريمة الالكترونية (المعلوماتية) التي ترتكب في الفضاء الالكتروني.

– تأهيل العاملين في قطاع أمن المعلومات في المنظمات المالية من أجل حماية المنظومة الالكترونية، والتعامل باحتراف مع تكنولوجيا المعلومات والاتصالات.

-تفعيل الأجهزة الخاصة بالخبرة الجنائية للجريمة الالكترونية (المعلوماتية) يتكون أعضاؤها من فريق متخصص فنيا في تقنية الاتصالات والمعلومات، لأن اثبات الجريمة الالكترونية يتطلب قواعد خاصة للتعامل مع الأدلة في هذه الجرائم.

- العمل على إعادة النظر في المناهج الدراسية، وضرورة تضمينها مادة عامة عن الحاسب الآلي والشبكات المعلوماتية وكيفية التعامل مع الأجهزة الالكترونية، على سبيل المثال: يجب أن تتضمن كليات القانون قسما خاصا لدراسة الجرائم الالكترونية في مادة القانون العقوبات والمعاملات المالية، والتجارة الالكترونية، والصيرفة الالكترونية، والحكومة الالكترونية.

- الاهتمام باتفاقيات التعاون الدولية والإقليمية والعربية لمكافحة الجرائم الالكترونية (كاتفاقية بودابست 2001) والتنسيق فيما بينها لتعاون أجهزة الشرطة في تبادل البيانات والمعلومات اللازمة، والتصدي للاستخدامات غير المشروعة في المعاملات الالكترونية وملاحقة المتهمين هذه الجرائم. (قابوسة، 2019، صفحة 254)

- الاعتماد على أساليب وتقنيات متطورة للتمكن من كشف عن هوية مرتكب الجريمة والاستدلال عليه بأقل وقت ممكن.

- توعية الافراد ونصحهم لماهية الجرائم الالكترونية وكل ما يترتب عليها من مخاطر.

- الحرص على الحفاظ على سرية المعلومات الخاصة بالعناوين الالـكترونية كالحسابات البنكـية والبطاقات الائتمانية وغيرها.

- عدم الكشف عن كلمة سر نهائيا وتغيرها بشكل مستمر واختيار كلمات سر صعبة، تجنب تخـزين الصور الخاصة للأفراد على مواقع التواصل الاجتماعي وأجهزة الحاسوب.

- استمرار تحديث برامج الحماية الخاصة بجهاز الحاسوب.

- تأسيس منظمة خاصة لمكافحة الجرائم الالكترونية والحد منها.

- المسارعة في الإبلاغ للجهات الأمنية فور تعرض لجريمة.

- مواكبة التطورات المرتبطة بالجريمة الالكترونية والحرص على تطوير وسائل مكافحتها. (رشاد، 2018، صفحة 443)

ثالثا - إجراءات التحقيق في الجرائم الالكترونية: للتحقيق في الجرائم الالكترونية يجب الالمام والمعرفة الجيدة بمجال الحاسب الآلي والانترنت ، وكيفية الاستفادة من هذه المعرفة واستخدامها بكفاءة في التحقيق والتحري واستخلاص الأدلة، ثم معرفة ما يمكن استخدامه كدليل في المحكمة ، وأخيرا معرفة الخطوات اللازمة لتجريم المشتبه به من الناحية القانونية ، بالإضافة إلى ذلك لابد من توفر مجموعة من المتخصصين والمحققين لديهم معرفة وخبرة طويلة في مجال جرائم الحاسوب والانترنت، وكيفية التعامل مع الأدلة الجنائية الرقمية، حيث يتولى عملية التفتيش عن الأدلة خبير في الحاسوب والشبكات، وآخر في تدقيق الحاسبات وخبير في التصوير والبصمات ثم خبير الرسم التخطيطي ، وتساهم هذه الإجراءات جميعها في الوصول إلى الآتي:

- التأكد من وقوع الجريمة.

- تحديد نمط وطبيعة الجريمة المرتكبة.

- التعرف على التقنيات المستخدمة في ارتكابها.

- المساعدة في تحديد الجاني والجناة المحتملين أو المشتبه بهم.

- معرفة الأسباب والدوافع المحتملة لارتكاب الجريمة.

- الاستدلال على الشهود في حالة وجودهم.

- توضيح طبيعة الأدلة الجنائية ومصادرها.

ويحتاج فريق المحققين في الجرائم المعلوماتية إلى مجموعة من البرمجيات الخاصة بالتحقيق الجنائي منها:

برمجيات النسخ الاحتياطي الجنائي، برمجيات استعادة الملفات المحذوفة، برمجيات كسر كلمات سر بعض المستندات، برمجيات تتبع الاتصال الشبكي، برمجيات استعراض الصور، برمجيات عرض محتوى الملفات المختلفة.

وأخيرا، فيما يلي بعض النصائح التقليدية لخبراء الحاسوب بمكافحة الجريمة الالكترونية:

-اجتناب استخدام أجهزة الحاسوب في الأماكن العامة، كالمقاهي والفنادق وغيرها إلا للضرورة.

- ضرورة إقفال البريد الالكتروني بعد الاستخدام، وتجاهل الرسائل الواردة التي لا تعرف مصدرها، ومسح المراسلات الصادرة والواردة التي لا تحتاج الجوع اليها.

- الحرص على تغيير كلمة السر باستمرار، وأن تكون مزيجا من الحروف الصغيرة والكبيرة والأرقام والاشارات.

-ضرورة أن تكون كلمة السر بعيدة عن معلوماتك الشخصية والعائلية مثل الاسم، تاريخ الميلاد، رقم الهاتف الخاص بك، أو عن الأسماء الشهيرة مثل الاعبين أو الشخصيات السياسية.

- ألا يكون بريدك الالكتروني مكتوبا على بطاقتك التعريفية، فلا تسلم هذه البطاقة إلا لمن تعرف أنه لن يسئ استخدامها.

- نقل نسخة من عناوين الأشخاص الذين تتواصل معهم إلى مكان آخر وتحديثها باستمرار. (قابوسة، 2019، صفحة 253)