**الجرائم المستحدثة كيفية إثباتها ومواجهتها**

نظرا للتطور السريع فى مجال نظم المعلومات و الاتصالات و ارتباطه بأدق تفاصيل الحياة اليومية للمواطنين سواء من خلال الانتشار الهائل لشبكة الإنترنت أو نظم ميكنة الدورات المستندية وإدارة المشروعات ، وما ترتب على ذلك من ظهور أشكال عديدة ومستحدثة من الجرائم الإلكترونية والتى تحاكى فى شكلها العام العديد من أشكال الجرائم العادية مثل جرائم السب و القذف و التشهير و جرائم النصب و الاحتيال و التزوير وجرائم الملكية الفكرية وجرائم الأموال العامة و الإرهاب بصوره المختلفة.

وفى ظل إصدار قانون التوقيع الإلكترونى و ترقب صدور قانون تأمين الفضاء الإلكترونى و مع ازدياد الخدمات المقدمة تحت مظلة الحكومة الإلكترونية تبدو الضرورة الملحة للتوعية بالأنواع المختلفة لهذه الجرائم والأساليب المستخدمة لتنفيذها بما يمكن رجال الشرطة و الجهات التشريعية لفهم الطبيعة الخاصة لهذه الجرائم و لاسيما علم الأدلة الرقمية ، أو ما يمكن ان نسميه الطب الشرعى المعلوماتى (Digital Forensics)، و الذى يمثل حجر الزاوية للتعامل الفاعل لهذه النوعية من الجرائم .

وبناء عليه ، قام المركز القومى للبحوث الاجتماعية والجنائية بعقد هذا المؤتمر لاستعراض الملامح الرئيسة للجرائم الإلكترونية وأشكالها المختلفة كما يعرض لعلم الدليل الرقمى و آليات التعامل معه .

## موضوعات المؤتمر :

١- **مقدمه عن الجرائم الإلكترونية**
يتم استعراض الأشكال المختلفة والمتجددة من الجرائم الإلكترونية مثل سرقة كلمات السر و الهوية الرقمية والتصنت علي شبكات المعلومات وجرائم الاحتيال للحصول على أرقام بطاقات الائتمان وادعاء شخصية الغير و جرائم اصتياد الضحايا (Fishing) لسرقة كلمات المرور الخاصة بالبريد الإلكترونى وجرائم الاحتيال النفسى والمخدرات الرقمية كأحد الجرائم المستحدثة.

٢- **أنواع الثغرات الأمنية فى نظم المعلومات و أساليب اختراقها**
يتم استعراض الأنواع المختلفة للثغرات الأمنية في مكونات نظم الحاسبات المختلفة مثل ثغرات نظام التشغيل وثغرات خوادم مواقع الإنترنت وثغرات التطبيقات والبرامج على اختلافها ، كما يتعرض لأهم ثغرة وهى توعية الأفراد (Human Factor) بالثغرات الخاصة بالسياسيات الأمنية للمؤسسات .

٣- **انتهاك الخصوصية الأفراد (شبكات التواصل الاجتماعى)**
يتم استعراض كيفية انتهاك خصوصية الأفراد في شبكات التواصل الاجتماعى مثل Face Book, twitter ,Linked in واستعراض الأساليب الاحتيالية المستخدمة فى هذا الصدد.

٤- **جرائم أجهزة المحمول**
يتم التعرض لبعض الأساليب التى يستخدمها الشخص المحتال للحصول على معلومات شخصية أو معلومات تخص الحسابات البنكية لمالك جهاز المحمول كما يتعرض لأساليب استخدام المحمول فى عمليات النصب والتهديد وإمكانية عدم إظهار رقم الطالب وإرسال رسائل من أرقام خادعة.

٥- **برامج التجسس الإلكترونى و سرقة الهوية الرقمية**
يتم التعرض في هذه الجزئية لإختراق الشبكات السلكية واللاسلكية للحصول على المعلومات المتداولة من خلالها ، أيضا التعرض لبعض الأساليب المتقدمة (Man in the Middle- web proxy- DNS Poisson) والتى يقع ضحاياتها الآلاف من مستخدمى شبكة الإنترنت .

٦- **أساليب إخفاء البيانات و استخدامها كأداة من قبل الإرهابيين أو الهاكرز**
يستعرض التقنيات المختلفة لإخفاء البيانات التي يمكن استخدامها من قبل العصابات الإلكترونية أو المجموعات الإرهابية حيث يتم التعرض لتقنيات إخفاء البيانات داخل صور أو ملفات فيديو أو ملفات صوت ، والعديد من الأنواع المختلفة لبرامج الوسائط المتعددة ( Multimedia – stenography) هذا بالإضافة لتقنيات ال(Alternate Data Stream – ADS) الخاصة بنظم تشغيل الويندوز.

**٧- طبيعة الدليل الرقمى و كيفية التحفظ عليه**

يعرض هذا الموضوع للخصائص العامة المميزة للأدلة الرقمية مع إلقاء الضوء على الأماكن التى قد توجد فيها أشكال مختلفة من البيانات والملفات والتى يمكن استخدامها كدليل رقمي لإثبات أو نفى جريمة إلكترونية ما، كما تتعرض للأساليب والخطوات الإجرائية اللازمة للتحفظ علي الدليل الرقمى بما يضمن سلامته وحجيته في الإثبات.

**٨- أساليب إتلاف و إخفاء الدليل الرقمى وإفساد حجيته فى الإثبات و تقنيات الإتلاف و التضليل**

يتم شرح التقنيات المختلفة التى يستخدمها المخترقون أو المحترفين من الجناة فى الجرائم الإلكترونية لإفساد أو إتلاف أو تغير أو مسح الدليل الرقمى ومنها علي سبيل المثال: تقنيات البروكسي (Proxy)، والتعامل مع نظم الحاسبات الافتراضية (Virtualization) واستخدام برامج إخفاء الدليل الرقمى مثل( Evidence Eliminator)

**٩- مفهوم التأمين الشامل (Defense in Depth)**

نتعرض هنا لمفهوم التأمين بمنظور شامل حيث لا يقتصر الحديث فقط على أنظمة الجدران النارية (Firewall)، أو أنظمة التنبؤ بالهجمات الإلكترونية ومنعها (Intrusion Prevention Systems - IPS) ، وأيضا يتم استعراض أهم النقاط التي يجب وضعها في الحسبان ليكون هناك تصور شامل لتأمين نظم الحاسبات بداية من الكابلات وأجهزة الشبكة وانتقالاً إلى نظم التشغيل ومرورا بضوابط تأمين التطبيقات والبرامج ، وانتهاء بالعنصر الأهم علي الاطلاق وهو توعية العنصر البشرى (المتعاملين مع هذه النظم).

**١٠- نماذج عملية**

لإتمام الاستفادة مما سبق عرضه من موضوعات يأتي هذا الجزء لتقديم نماذج عملية عن بعض الموضوعات سابقة الذكر سواء فى تنفيذ بعض أشكال الجرائم الإلكترونية أو فى بعض النماذج العملية المتعلقة بالدليل الرقمى وأيضا الإجابة على استفسارات السادة الحضور فى أى من الموضوعات المطروحة.

**المستهدفون بالحضور:**

المخابرات العامة ورجال الشرطة بكافة تخصصاتهم – السادة الضباط بالجهات الأمنية المختلفة – السادة وكلاء النيابة و القضاة – السادة أعضاء هيئة الرقابة الإدارية والنيابة الإدارية – المعنيين بالجوانب التشريعية – القائمين على إدارة مراكز المعلومات بالجهات الحكومية –البنوك- الوزارت المختلفة المعنية بحفظ البيانات أو التى لها مواقع على الإنترنت من مصر والدول العربية.