معهد العراب العالي للتدريب

109 سيبر

التحليل الجنائي الرقمي والجرائم الرقمية

م/نورة الحربي

نبذة عن المقرر

يهدف هذا المقرر الى التعرف على مفهوم الجرائم الالكترونية والرقمية وخصائصها وطرق الحماية منها وتشمل تلك الجرائم سرقة الهوية والتشفير والابتزاز ويتطلب ذلك كوادر فنية عالية التدريب لكشف الجرائم الالكترونية، يشمل المحتوى عن قوانين الجرائم المعلوماتية السعودي العقوبات والتشريعات. أيضًا يشمل على موجز عن مواقع التواصل الاجتماعي وكيفية اختراقها وطرق الحماية من الاختراقات

معهد العراب العالي للتدريب

الأهداف العامة والتفصيلية من المقرر

- إكساب المتدرب المعارف والمهارات للتعرف و اكتشاف ومواجهة الجرائم الرقمية

1. يكتسب مفهوم التحري الجنائي الرقمي في الجرائم الرقمية
2. يتحرى في الجرائم الرقمية وتقنية المعلومات
3. يعدد خصائص وسمات مرتكبو الجرائم الرقمية
4. يحدد اشكال الجرائم الرقمية
5. يتوصل الى الدوافع التي تؤدي الى ارتكاب الجرائم الرقمية
6. يعدد طرق مكافحة الجرائم الرقمية
7. يستخدم نظرية التحقق في التحري الجنائي الرقمي
8. يستخدم تقنيات وتحليل الحوادث الجنائية الرقمية للحواسيب عبر اداة Forensics Tool Kit – FTK
9. يستخدم تقنيات وتحليل الحوادث الجنائية الرقمية للجوالات عبر اداة Forensics Tool Kit – FTK
10. يعدد جرائم وسائل التواصل الاجتماعي وآلية اختراقها
11. يطبق قانون الجرائم المعلوماتية السعودي والعقوبات والتشريعات

معهد العراب العالي للتدريب

د. موضي الجامع

مدير عام تطوير كفاءات الاتصالات وتقنية المعلومات STCفي أكاديمية

مستقبل الأمن السيبراني كبير بحكم أننا في كل يوم نعزز علاقتنا مع التقنية وكل تقنية جديدة هي المستقبل

ماهر التحليل الجنائي الرقمي

التحليل الجنائي الرقمي: هوعملية لجمع الأدلة الرقمية و تحليلها لاستخراج المعلومات اللازمة للكشف عن الجرائم المرتكبة باستخدام التقنية الرقمية، مثل الاختراقات والاحتيال اللإلكتروني و التزوير والقرصنة والتجسس الإلكتروني والجرائم المرتبطة بالانترنت. يستخدم المحققون الجنائيون العديد من التقنيات والأدوات المتخصصة لجمع الأدلة وتحليلها.

أهمية التحليل الجنائي

الحفاظ على الأدلة الرقمية	• يتم جمع الأدلة الرقمية خلال التحقيق الجنائي، ويتم استخدامها لتحديد هوية الجاني وجمع الأدلة لإحالته إلى العدالة
الحد من الجرائم الإلكترونية	• يتم التحقيق الجنائي الرقمي للكشف عن الجرائم الإلكترونية وتحديد اساليب الهجوم المستخدمة وبناء الوعي الأمني للأفراد والؤسسات للحد من هذه الجرائم
الحفاظ على الخصوصية	• يتم التحقيق الجنائي الرقمي بطرق تحافظ على خصوصية البيانات الشخصية والمعلومات الحساسة حيث يتم جمع الأدلة بطريقة قانونية ومتوافقة مع الأنظمة القانونية المحلية والدولية
الدفاع عن الشركات والمؤسسات	• يتم التحقيق الجنائي الرقمي لحماية الشركات والمؤسسات من الهجمات الإلكترونية والاختراقات وتحديد نقاط الضعف في الأنظمة الأمنية وتعزيزها
الحفاظ على الأمن القومي	• يتم التحقيق الجنائي الرقمي للحفاظ على الأمن القومي وحماية الأسرار الحكومية والاقتصادية والتجارية

ادوات التحليل الجنائي

برامج استعادة البيانات	• تتيح هذه البرامج استعادة البيانات المحذوفة او المفقودة من الأجهزة الرقمية مثل الحواسيب او الهواتف الذكية والاقراص الصلبة
برامج النحليل الرقمي	• تاعد هذه البرامج على تحليل الأدلة الرقمية المجمعة، وتتضمن برامج التحليل الأحصائي والتحليل النفسي والجيولوجي وتحليل النصوص
برامج الاستعادة الجنائية	• تساعد هذه البرامج على استعادة الأدلة الرقمية المحذوفة أو المتلفة بشكل متعمد
برامج التجسس والاختراق	• تساعد هذه البرامج على الوصول الى الإجهزة الرقمية والشبكات اللاسلكية وجمع الادلة الرقمية المتعلقة بالجريمة
برامج التشفير وفك التشفير	• تستخدم هذه البرامج لتشفير البيانات وفك التشفير وقد يتم استخدامها للوصول الى بيانات مشفرة بشكل غير قانوني
برامج التصوير الرقمي	• تستخدم هذه البرامج لتحلي الصور الرقمية والفيديو الوصت واستخلاص الأدلة الرقمية المتعلقة بالجريمة

مؤهلات المحلل الجنائي الرقمي

يحتاج المحققون من أجل تنفيذ مهامهم بشكل فعال إلى التمتع بمجموعة من المهارات والصفات الشخصية، كالتالي:

- الفهم المتعمق لكافة القوانين والإجراءات القانونية المتعلقة بالجرائم والأدلة.
- مهارات تواصل كتابية وشفوية ممتازة.
- إجادة استخدام الحاسوب وقدرة على التعامل مع برامج مايكروسوفت أوفيس.
- قدرة عالية على الاستماع وتحليل المعلومات بشكل دقيق.
- يجب أن يمتلك عقلا تحليليا واعيا وقادرا على اتخاذ قرارات حكيمة.
- قدرة عالية على تفسير الأدلة والنتائج.
- الإلمام التام بجميع أنواع الأدلة والفهم المتعمق لعمليات التحقيق حسب ظروف كل حالة.
- مهارات مقابلة واستجواب ممتازة.
- يجب أن يمتلك مستويات عالية من السرية والنزاهة والتمتع ببعض الصفات الشخصية كالصدق والأخلاق وعدم التحيز وغيرها.
- يفضل أن يكون حاصلا على درجة البكالوريوس في القانون أو علوم الطب الشرعي أو العمل كضابط شرطة أو أي مجال آخر ذات صلة.
- مهارات التفكير النقدي والقدرة على حل المشكلات.
- لديه قدرة على الجلوس والعمل لفترات طويلة حيث إن طبيعة عمله مكتبية.
- يجب أن يتمتع بالذكاء والفطنة وقدرة على الانتباه لأدق التفاصيل.
- القدرة على مراقبة كافة التفاصيل الخاصة بالجناة أثناء إجراء التحقيقات.
- مهارات تنظيمية عالية وقدرة على إدارة الوقت.

مؤهلات المحلل الجنائي الرقمي

محقق جنائي رقمي - Digital Forensic Investigator :
هذا هو الوظيفة الرئيسية في مجال التحليل الجنائي الرقمي. يقوم محقوق الجرائم الرقمية بجمع واستعادة الأدلة الرقمية من أجهزة الكمبيوتر والأجهزة الإلكترونية وتحليلها لاستخدامها في التحقيقات الجنائية.

خبير أمان سيبراني - Cybersecurity Analyst:
يعمل خبراء الأمان سيبراني على حماية البنية التحتية الرقمية للمؤسسات والشركات من الهجمات السيبرانية. يمكن لهؤلاء الخبراء أيضًا أن يلعبوا دورًا في تحليل الجرائم الإلكترونية.

محلل تهديد سيبراني - Cyber Threat Analyst:
يقوم محللو التهديدات سيبرانية بمراقبة وتحليل الأنشطة السيبرانية المشبوهة وتقديم تقارير عنها. يعملون على تحديد الهجمات المحتملة والتصدي لها.

مؤهلات المحلل الجنائي الرقمي

متخصص في استجابة الطوارئ السيبرانية - Incident Responder:
يتعامل متخصصو استجابة الطوارئ السيبرانية مع الهجمات السيبرانية في الوقت الفعلي، ويتخذون إجراءات لوقف الهجمات واستعادة البيانات.

محلل جرائم إلكترونية - Cybercrime Analyst:
يقوم محللو الجرائم الإلكترونية بتحليل الأنشطة الإلكترونية غير القانونية ومحاولة تحديد الجناة وفهم دوافعهم.

خبير تقني في مجال الأمان - Security Technical Expert:
يعمل هؤلاء الخبراء على تصميم وتنفيذ تقنيات الأمان والحلول الرقمية المتقدمة لحماية الأنظمة والبيانات.

مؤهلات المحلل الجنائي الرقمي

مسؤول تقنية المعلومات - IT Manager:
يقوم مسؤولو تقنية المعلومات بدورهم بإدارة البنية التحتية الرقمية للمؤسسات وضمان أمانها وتشغيلها بكفاءة.

محلل بيانات - Data Analyst:
يمكن أن يكون محللو البيانات ذوو أهمية كبيرة في تحليل البيانات الكبيرة والمعلومات الرقمية للكشف عن الأنماط والتحليلات ذات الصلة بالجرائم.

مدير تحليل البيانات الرقمية - Digital Data Analysis Manager:
يشرف على فرق التحليل الجنائي الرقمي وينسق عمليات التحقيق والتحليل.

عقوبات الجرائم الإلكترونية

- الجرائم التي تهدف إلى التشهير والوصول بطريقة غير مشروعة والاختراق لخصوصياتهم.

السجن لمدة لا تتعدى العام الواحد أو غرامة مالية قد تصل حتى 500.000 ريال سعودي.

- جرائم الهاكر والقرصنة والعمل على اختراق المعلومات الشخصية. السجن لمدة لا تتعدى 4 سنوات إضافة للغرامة المالية تصل حتى 3000.000 ريال سعودي.
- التحريض للغير أو تقديم المساعدة والاتفاق معه لارتكاب أي من الجرائم التي ذكرت سابقاً بذات العقوبة للجرم المرتكب بما لا يتعدى الحد الأعلى لها.
- الشروع للقيام بإحدى الجرائم الواردة في نظام الجرائم الإلكترونية في السعودية والتي لا تتعدى عقوبتها نصف الحد الأعلى لذات العقوبة.

اشهر الكورسات بمجال التحليل الجنائي

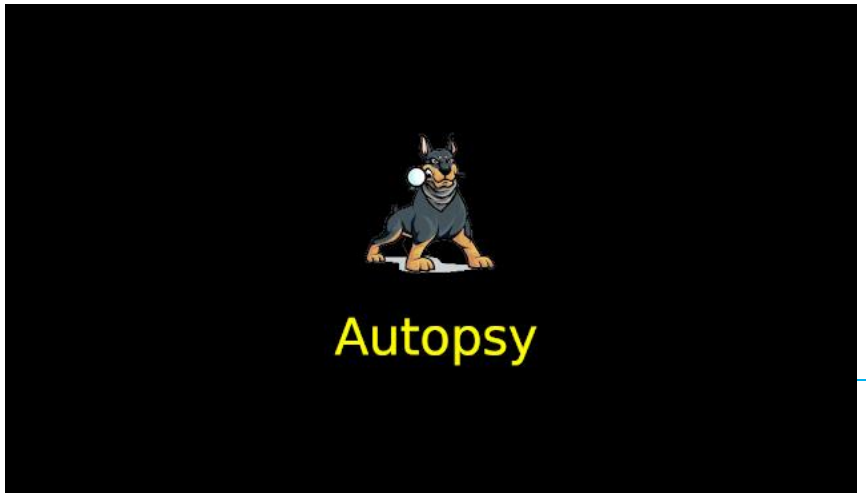
ماهي شهادة CHFI؟

شهادة CHFI هي اختصار لـ" Computer Hacking Forensic Investigator " وهي شهادة مهنية تعني أن حاملها لديه المعرفة والمهارات المطلوبة للتحقيق في الهجمات الإلكترونية وجمع الأدلة الرقمية وتحليلها وتقديم التقارير الفنية المتعلقة بها

نبذة عن برنامج autoposy

Autopsy هذه الاداة تقوم بعمل تحليل على نظام المجرم, كي ابسط الامور أكثر يقوم المحقق الرقمي باخذ نسخة من نظام المتهم باستخدام أدوات مثل اداة dd ومن ثم يستخدم اداة Autopsy لعمل تحليل, هذه الاداة عندما يتم تشغيلها تقوم بفتح بورت 9999 ويمكنك الاتصال عبر هذا البورت من المتصفح وعمل قضية (وفتح محضر تحقيق) ومن ثم المباشرة في التحقيق والتدقيق.

https://www.autopsy.com/download/



خصائص و سمات مرتكبو الجرائم الرقمية

١. مجرم متخصص، له قدرة فائقة في المهارة التقنية، ويستغل مداركه ومهاراته في اختراق الشبكات، وكسر كلمات
المرور، أو الشفرات، ويسبح في عالم الشبكات، ليحصل على البيانات والمعلومات الموجودة في أجهزة الحواسب، ومن خلال الشبكات.

2. مجرم يعود إلى الإجرام. فما يميز المجرم المعلوماتي أنه يعود للجريمة دائمًا، فهو يوظف مهاراته في كيفية عمل الحواسيب، وكيفية تخزين البيانات والمعلومات، والتحكم في أنظمة الشبكات في الدخول غير المصرح به مرات عدة. فهو قد لا يحقق جريمة الاختراق بهدف الإيذاء، وإنما نتيجة شعوره بقدرته ومهارته في الاختراق.

3. مجرم محترف، له من القدرات والمهارات التقنية ما يؤهله لأن يوظف مهاراته في الاختراق والسرقة والنصب والاعتداء على حقوق الملكية الفكرية، وغيرها من الجرائم، مقابل المال.

4. مجرم ذكي، حيث يمتلك من المهارات ما يؤهله للقيام بتعديل الأنظمة الأمنية وتطويرها، حتى لا تستطيع أن تلاحقه وتتبع أعماله الإجرامية من خلال الشبكات، أو داخل أجهزة الحواسيب. فالإجرام المعلوماتي هو إجرام الذكاء، ودونما حاجة إلى استخدام القوة والعنف، وهذا الذكاء هو مفتاح المجرم المعلوماتي لاكتشاف الثغرات واختراق البرامج المحصنة.

دوافع ارتكاب الجريمة الرقمية

- دوافع مادية: ويقصد بها الحصول على مكاسب مادية، فهي من أكثر وأشهر الدوافع لارتكاب الجرائم وأكثرها ثراء في الحصول على المال والربح الكبير والمجدي، فيكون السبب وراء هذا الدافع هو وقوع الأفراد في ضيق مالي؛ ممّا يدفعهم إلى سرقة الأموال وتحوليها إلى حساباتهم الشخصية.

- دوافع شخصية: ويقصد بهذه الدوافع هو رغبة الأفراد في التعلم، فيقضون أغلب أوقاتهم في التعلم على كيفية اختراق الممنوعات والتقنيات الأمنية.

- دوافع ذهنية أو نمطية: ويقصد بها الدوافع التي يكون للأفراد من خلالها الرغبة في إثبات ذاتهم والعمل على تحقيق الانتصارات، فيما يخص التقنيات المتعلقة بالأنظمة المعلوماتية.

- دافع الانتقام: ويقصد به الدافع الذي يدفع الأفراد في الانتقام، فهو من أخطر الدوافع المتعلقة في ارتكاب الجرائم الإلكترونية. وتزيد خطورتها عند يمتلك هؤلاء الأفراد معلومات كبيرة عن شركات أو مؤسسات معينة.

- دافع التسلية: ويقصد بذلك قيام الأفراد بارتكاب الجرائم الإلكترونية بهدف التسلية فقط.

- دافع سياسي: ويقصد بذلك قيام الأفراد بارتكاب الجرائم الإلكترونية؛ بهدف تلفيق الأخبار والمعلومات أو حتى الاستناد إلى أجزاء بسيطة من الحقيقة. وبالتالي يتم نسخ الأخبار الملفقة وتتم هذه الجرائم في المواقع السياسية المعادية للحكومات، مع أهمية التركيز على قدرتهم في إبراز المحاولات الدولية لاختراق الشبكات الحكومية في مختلف أنحاء العالم.

اشكال الجرائم الرقمية

•أنواع الجرائم الإلكترونية يُمكن تصنيف أنواع الجرائم الإلكترونية كما يأتي
• ADVERTISINGهجمات الحرمان من الخدمات: يُرمز لها بالرمز ((DDoS، وتُنفّذ هذه الهجمات باستخدام مجموعات كبيرة من أجهزة الكمبيوتر يُتحكَّم بها عن بُعد بواسطة أشخاص يستخدمون نطاق ترددي مشترك، وتهدف هذه الهجمات لإغراق الموقع المستهدف بكميّات هائلة من البيانات في آن واحد، ممّا يُسبّب بطئاً وإعاقةً في وصول المستخدمين للموقع.
•التصيد الاحتيالي: يُعتبر هذا النوع من الجرائم الإلكترونية الأكثر انتشاراً، وهو إرسال جماعي لرسائل تصل عبر البريد الإلكتروني تحتوي على روابط لمواقع أو مرفقات ضارّة، وبمجرّد نقر المستخدم عليها فإنّه قد يبدأ بتحميل برامج ضارة بجهاز الكمبيوتر الخاص به.
•مجموعات الاستغلال: يعرّف هذا النوع على أنّه استخدام برامج مصمّمة لاستغلال أيّ أخطاء أو ثغرات أمنية في أجهزة الكمبيوتر، ويُمكن الحصول على هذه البرامج من شبكة الإنترنت المظلمة، كما يُمكن للقراصنة اختراق مواقع ويب شرعية واستخدامها للإيقاع بضحاياهم. برامج الفدية: تمنع هذه البرامج صاحب الجهاز من الوصول إلى ملفّاته المخزّنة على محرّك الأقراص الصلبة، ويشترط المجرم على الضحيّة دفع مبلغ ماليّ كفدية لإتاحة استعادة ملفاته التي يحتاجها. القرصنة: تُعرّف القرنصة على أنّها وصول غير شرعي إلى بيانات ومعلومات موجودة على أجهزة الكمبيوتر أو شبكات الإنترنت من خلال استغلال نقاط ضعف وثغرات في هذه الأنظمة

اشكال الجرائم الرقمية

- **سرقة الهويّة:** يحدث هذا النوع من الجرائم عندما يحصل شخص ما على المعلومات الشخصية لشخص آخر بشكل غير قانونيّ ويستخدمها لأغراض غير شرعية مثل الاحتيال والسرقة
- **الهندسة الاجتماعية:** يعتمد هذا النوع من الجرائم على العنصر البشري في التلاعب النفسي بالضحية لإرغامها على القيام بأعمال غير قانونية أو إفشاء معلومات سريّة، وهي من الأساليب التي يستخدمها مجرمو الإنترنت للقيام بأعمال الاحتيال
- **قرصنة البرمجيات:** تُعرّف قرصنة البرمجيات على أنّها إعادة توزيع واستخدام لبرمجيات دون تصريح من الشركة المالكة للبرمجية، وهناك عدّة أشكال لهذه القرصنة كالآتي إنتاج برمجيات تجارية مزيّفة واستخدام العلامة التجارية للبرمجية الأصلية. تحميل نسخ غير قانونية من البرمجيات. انتهاك اتفاقيات استخدام البرمجيات التي تحدّ من عدد مستخدمي النسخة الواحدة من البرنامج.
- **البرمجيات الخبيثة:** تُعرف البرمجيات الخبيثة بأنّها البرمجيات التي تؤثّر على الأداء الطبيعيّ لأجهزة الكمبيوتروفي ما يأتي أشهر أنواع هذه البرمجيات
- **الفيروس:** وهو برنامج كمبيوتر أو برنامج مرتبط ببرنامج كمبيوتر آخر يُلحق ضرراً مباشراً بنظام الكمبيوتر، وعند تشغيل هذا البرنامج فإنّه سيؤدي إلى ضرر بنظام التشغيل؛ كحذف ملفّات من النظام أو تعطيلها.
- **دودة الحاسوب:** تُعدّ برامج كمبيوتر مثل الفيروسات ولكنّها لا تُعدّل على نظام الكمبيوتر، بل تتكاثر باستمرار ممّا يؤدي لإبطاء نظام التشغيل، وعلى عكس الفيروسات فإنّ دودة الحاسوب يُمكن التحكّم فيها عن بُعد.
- **حصان طروادة:** يُعدّ جزءاً خفيّاً في برمجية الكمبيوتر يسرق معلومات المستخدم المهمّة، حيث إنّه يُمكن أن يُراقب ويسرق المعلومات التعريفية للبريد الإلكتروني أثناء محاولة المستخدم الدخول له عبر متصفّح الويب.
- **برامجيات أُخرى:** تتضمّن برمجيات الإعلانات، وبرمجيات التجسس، وبرمجيات خبيثة هجينة تضمّ أكثر من نوع من البرمجيات السابقة في الوقت ذاته.

طرق مكافحة الجرائم الرقمية

تحديد إجراءات واضحة وتطوير السياسات للموظفين.

- وضع خطط استجابة لحوادث الأمن السيبراني.
- عدم الوثوق بالروابط المجهولة وفتحها إلّا بعد أن تسأل المرسل عنها وتتأكّد من أمانها.
- تحديث البرامج وتثبيت برامج لمكافحة الفيروسات والحماية.
- إنشاء كلمات مرور قوية تتكوّن من أحرف وأرقام ورموز يصعب فكّها وتغييرها بانتظام.
- الابتعاد قدر الإمكان عن الاتصال بالشبكات العامة، وإن كنت مضطرّاً لذلك، تجنّب إجراء معاملات سريّة.
- فحص عناوين الـ URL قبل فتح الروابط، والتأكّد من أمانها ومصداقيتها.
- تجاهل الرسائل غير المرغوب بها في رسائل البريد الإلكتروني.

طرق مكافحة الجرائم الرقمية

رسم سياسات دولية تفرض عقوبات صارمة على مرتكبي جرائم الإنترنت إذ يستلزم التدخل الحكومي والدولي نظراً للخطورة الجسيمة للأمر.
– الاعتماد على أساليب وتقنيات متطوّرة للتمكن من الكشف عن هوية مرتكب الجريمة والاستدلال عليه بأقل وقت ممكن.
– توعية الأفراد ونصحهم لماهية الجرائم الإلكترونية وكل ما يترتب عليها من مخاطر.
– الحرص على الحفاظ على سرية المعلومات الخاصة بالعناوين الإلكترونية كالحسابات البنكية، والبطاقات الائتمانيّة وغيرها.
– عدم الكشف عن كلمة السر نهائياً وتغييرها بشكل مستمر واختيار كلمات سر صعبة. تجنب تخزين الصور الخاصة بالأفراد على مواقع التواصل الاجتماعي وأجهزة الحاسوب.
– تجنّب تحميل أي برنامج مجهول المصدر.
– استمرارية تحديث برامج الحماية الخاصة بأجهزة الحاسوب ومنها ، MCafee, Norton.
–تأسيس منظمة خاصة لمكافحة الجرائم الإلكترونية والحد منها.
– المسارعة في الإبلاغ للجهات الأمنية فور التعرض لجريمة إلكترونية.
– مواكبة التطورات المرتبطة بالجريمة الإلكترونية والحرص على تطوير وسائل مكافحتها.
– استخدام برمجيات آمنة ونظم تشغيل خالية من الثغرات.

طرق مكافحة الجرائم الرقمية

حرص على استخدام كلمات سرية للوصول إلى البرامج الموجودة على جهاز الحاسوب.
– عدم ترك جهاز الحاسوب مفتوحاً.
– فصل اتصال جهاز الحاسوب بشبكة الإنترنت في حال عدم الاستخدام.
– أخذ الحيطة والحذر وعدم تصديق كل ما يصل من إعلانات والتأكد من مصداقيتها عن طريق محركات البحث الشهيرة.
– وضع الرقم السري بشكل مطابق للمواصفات الجيدة التي تصعّب من عملية القرصنة عليه من هذه المواصفات بأن يحتوي على أكثر من ثمانية أحرف أن يكون متنوع الحروف والرموز واللغات إلخ.
– يفضل تغيير كلمة المرور الخاصة بك بصفة دورية
– لا تضع معلومات علي الانترنت لا تحب أن يراها الجميع من تعرفهم ولا تعرفهم وتذكر أنه بمجرد أن تضع معلومات علي الانترنت لن تتمكن أبدا من ارجاعها مرة أخرى حتى لو قمت بحذفها
– معلوماتك الخاصة (اجعلها خاص) ان معلوماتك الخاصة مثل اسمك بالكامل ورقم هاتفك ورقم الهوية ورقم بطاقتك الائتمان وايضا عنوانك بالتفصيل هي معلومات خاصة لا يجب ان تتاح للجميع علي الانترنت لا شخص لا تعرفه فلا تفصح له عنها او تضعها علي اي موقع لا تثق به .

نظرية التحقيق في التحري الجنائي الرقمي

التحقيق الجنائي الرقمي هوعلم يهدف الى تجميع وتحليل وتقييم الادلة المتواجدة في الاجهزة ويتضمن امكانية استرجاع البيانات في حال فقدانها". والهدف منه هو "استخدامه كوسيلة لادانة شخص او جهة في عدة عمليات مثل الدخول الغير مصرح فيه للاجهزه ، انتحال الشخصية الإلكترونيا ، عمليات السرقة وايضا تدخل فيها جرائم القتل وما الى ذلك".

نظرية التحقيق في التحري الجنائي الرقمي

آلية التحقيق_الجنائي_الرقمي :

- identificationمعرفة نوع الهجمة وفهمها ومن هنا يبدا في جمع السجلات واخذ نسخه احتياطية من الاجهزه للعمل عليها.
- containmentلابد من عمل scanعلى كل الاجهزة لمعرفة مدى انتشار هذه الهجمه والمحاولة في فهم التقنيات وجميع الملفات المتعلقة بها.
- eradicationيتم هنا ازاله الملفات الخاصة بالهجمة مثلًا عند وجود ملف مشبوه يتم حذفه وايضا في حال التواصل مع عنوان مشبوه يتم رفع طلب لمنع الوصول لهذا العنوان.
- recoveryيتم هنا ارجاع الاجهزه لحالتها السابقة من خلال استخدام ال backupsولابد التاكد من ان النسخ الاحتياطية لا تحتوي على مسببات الهجمة مثال لو كانت تستخدم ثغرة متواجدة في النسخ الاحتياطية لا نستطيع استخدامها.
- lessons learnedيتم هنا مراجعه ما حدث وكيفية تجنب حدوثه في المستقبل.

لابد من كتابة تقرير لكل مرحلة، تُفصّل فيه جميع الادلة، التي تم ايجادها من خلال التحليل.

تقنيات وتحليل الحوادث الجنائية الرقمية للحواسيب عبر أداة Forensics Toolkit-FTK

FORENSICS TOOL KIT:

هي أداة تحليل رقمية تستخدم أساسًا لتطبيقات القضايا الجنائية. تتيح هذه الأداة للمحققين القدرة على تحليل مجموعات كبيرة من البيانات والعثور على الجرائم الإلكترونية.

يمكنه إنشاء نسخ من البيانات دون إجراء تغييرات على الدليل الأصلي أي ما نطلق عليه bit by bit . من المهم ان تعرف بأن في النسخ عند عملية التحقيق لا يتم بالشكل العادي ولكن يتم عمل نسخ لكل بت موجود على القرص وهذا أحد ميزات هذا البرنامج.

تقنيات وتحليل الحوادث الجنائية الرقمية للحواسيب عبر أداة Forensics Toolkit-FTK

https://youtu.be/lfUmo1mH9v4?si=qjAopD4xEXv3iaVu

تقنيات وتحليل الحوادث الجنائية الرقمية للجوالات عبر أداة Forensics Toolkit-FTK

https://youtu.be/gUVP__oRlXs?si=QeZDP25awUi7AmZd
https://youtu.be/-UZo1wP_4GY?si=cckmh_IHY2TGAk5T
https://youtu.be/R2dDWW-sYvM?si=zO0yQ4rwUwPkXYOy
https://youtu.be/fh6B65usZJM?si=mOs9dvSaUAtHJEXq

معهد العراب العالي للتدريب

تطبيق عملي

جرائم وسائل التواصل الاجتماعي

***النوع الأول/ جرائم ضد ألافراد، وأبرزها:**

١- جرائم السب والقذف:

حيث تعتبر جرائم السب والقذف والتشهير، أكثر الجرائم التى انتشرت عبر مواقع التواصل الاجتماعي، "كالفيس بوك أو الواتس أو التويتر أو الانستجرام"، وتتشدد القوانين العربية بالعقاب لجريمتي السب والقذف على مواقع التواصل الاجتماعي؛ لأن المجني عليه يتأذى من ذكر ما يشينه علانية، وتتحقق هذه العلانية في القول أو بالفعل أو بالكتابة، وبألفاظ تخدش الشرف أو الاعتبار بطريقة علنية.

٢- إنتحال الشخصية:

وفيها يستدرج المجرم الضحية، ويستخلص منه المعلومات بطرق غير مباشرة، ويستهدف فيها معلومات خاصة من أجل الإستفادة منها واستغلالها لتحقيق مكاسب مادية، أو التشهير بسمعة أشخاص بعينهم وقلب الوسط رأساً على عقب، وإفساد العلاقات سواءً الإجتماعية أو في العمل.

جرائم وسائل التواصل الاجتماعي

*٣- تهديد الأفراد:

يصل المجرم من خلال القرصنة وسرقة المعلومات إلى معلومات شخصية، وخاصة جداً بالنسبة للضحية، ثم يقوم بابتزازه من أجل كسب الأموال، وتحريضه للقيام بأفعال غير مشروعة قد يصاب فيها بأذى.

٤- تشويه السمعة:

يقوم المجرم باستخدام المعلومات المسروقة، وإضافة بعض المعلومات المغلوطة، ثم يقوم بارسالها عبر الوسائط الإجتماعية، أو عبر البريد الإلكتروني للعديد من الأفراد، أو عبر أي وسيلة للتواصل الاجتماعي، بغرض تشويه سمعة الضحية وتدميره نفسيًا، إضافة الى الفاظ تدخل في حكم التشهير أو الإهانة، طعنًا فى الأفراد أو خدشًا لسمعة العائلات.

٥) التحريض على أعمال غير مشروعة:

وفيها يقوم المجرم باستخدام المعلومات المسروقة، عن أفراد بعينهم واستغلالها في إبتزاز الضحايا، بالقيام بأعمال غير مشروعة، تتعلق بالدعارة وتجارة المخدرات وغسيل الأموال، أو جرائم القتل أو العنف، أو الاعمال الارهابية.

٦- إنتهاك الحياه الخاصة:

ويتعمد فيها الجاني على نشر الصور، إذا كانت هذه الصورة تُعد إساءة لأشخاص أو تنتهك حرمة الحياة الخاصة، أو تحتوى على معلومات أو أخبار كاذبة، أو مفبركة وتمثل إساءة لصاحبها.

النوع الثاني/ جرائم ضد المؤسسات، وأبرزها:

١- اختراق الأنظمة:

وتتسبب هذه الجرائم بخسائر كبيرة للمؤسسات والشركات، المتمثلة في الخسائر المادية والخسائر في النظم، بحيث يقوم المُجرم باختراق أنظمة الشبكات الخاصة بالمؤسسات والشركات، والحصول على معلومات قيّمة وخاصة بأنظمة الشركات، ومن ثم يقوم باستخدام المعلومات من أجل خدمة مصالحه الشخصية، والتي تتمثل في سرقة الأموال وتدمير أنظمة الشركة الداعمة للإدارة، مما يسبب خسائر جسيمة للشركة أو المؤسسة.

النوع الثاني/ جرائم ضد المؤسسات، وأبرزها:

٢- تدمير النظم:

يكون هذا النوع من التدمير، باستخدام الطرق الشائعة، وهي الفيروسات الإلكترونية التي تنتشر في النظام وتسبب الفوضى والتدمير، ويتسبب ذلك في العديد من الخسائر المرتبطة بالملفات المدمرة، ومدى أهميتها في إدارة وتنظيم الشركات والمؤسسات، أو تدمير الخادم الرئيسي الذي يستخدمه جميع من بالمؤسسة من أجل تسهيل الأعمال، ويتم ذلك من خلال إختراق حسابات الموظفين بالمؤسسة الخاصة بالشبكة المعلوماتية للمؤسسة، والدخول على الحسابات جميعاً في نفس الوقت، ويتسبب ذلك في عطل تام للخادم مما يؤدي إلى تدميره، وبالتالي تعطّل الأعمال بالشركات.

٣- إستخدام "البروكسي" للدخول للمواقع المحجوبة:

يعرف "البروكسي" بأنه: "برنامج وسيط يقوم بحصر إرتباط جميع مستخدمي الإنترنت في جهة واحدة ضمن جهاز موحد". والمعنى المتعارف عليه لدي مستخدمي الانترنت للبروكسي، هو ما يستخدم لتجأوز المواقع المحجوبة، حيث يستخدم البروكسي لتجأوز المواقع المحجوبة، سواءً كانت مواقع جنسية أو سياسية معادية للدولة، وقد يتم حجب بعض المواقع التي لا يفترض حجبها، كبعض المواقع العلمية والتي تنشر إحصائيات عن الجرائم، ومن هنا، فاستعمال البروكسي للدخول إلى المواقع المحجوبة، يعتبر امراً مخالفًا لقوانين مكافحة الجريمة الالكترونية.

النوع الثالث: جرائم ضد الأموال، وأبرزها:

١- الإستيلاء على حسابات البنوك:

وهي إختراق الحسابات البنكية والحسابات المتعلقة بمؤسسات الدولة وغيرها من المؤسسات الخاصة، كما يتم أيضاً سرقة البطاقات الإئتمانية، ومن ثم الإستيلاء عليها وسرقة ما بها من أموال.

٢- أنتهاك حقوق الملكية الفكرية والأدبية:

وهي صناعة نسخ غير أصلية من البرامج، وملفات المالتيميديا ونشرها من خلال الإنترنت، ويتسبب ذلك في خسائر فادحة في مؤسسات صناعة البرامج والصوتيات.

النوع الرابع: جرائم ضد أمن الدول، وأبرزها:

١- برامج التجسس:

تنتشر العديد من برامج التجسس والمستخدمة لأسباب سياسية، والتي تهدد أمن وسلامة الدولة، ويقوم المجرم بزرع برنامج التجسس داخل الأنظمة الإلكترونية للمؤسسات، فيقوم أعداء الوطن بهدم أنظمة النظام والإطلاع على مخططات عسكرية تخص أمن البلاد، لذلك فهي تعتبر من أخطر الجرائم المعلوماتية.

٢- استخدام المنظمات الإرهابية لأسلوب التضليل:

ويعتمد الإرهابيون على إستخدام وسائل الإتصال الحديثة وشبكة الإنترنت، من أجل بث ونشر معلومات مغلوطة أو كاذبه، والتي قد تؤدي لزعزعة الإستقرار في البلاد وإحداث الفوضى، من أجل تنفيذ مصالح [illegible]اسية ومخططات إرهابية، وتضليل عقول الشباب من أجل الإنتفاع بمصالح شخصية.

تطبيق قانون الجرائم المعلوماتية السعودي والعقوبات والتشريعات

نظام مكافحة جرائم المعلوماتية
١٤٢٨ هـ

بسم الله الرحمن الرحيم

مرسوم ملكي رقم م/١٧ بتاريخ ٨ / ٣ / ١٤٢٨

بعون الله تعالى
نحن عبد الله بن عبد العزيز آل سعود
ملك المملكة العربية السعودية
بناء على المادة (السبعين) من النظام الأساسي للحكم، الصادر بالأمر الملكي رقم (أ/٩٠) وتاريخ ٢٧ / ٨ / ١٤١٢ هـ.
وبناء على المادة (العشرين) من نظام مجلس الوزراء، الصادر بالأمر الملكي رقم (أ/١٣) وتاريخ ٣ / ٣ / ١٤١٤ هـ.
وبناء على المادة (الثامنة عشرة) من نظام مجلس الشورى، الصادر بالأمر الملكي رقم (أ/٩١) وتاريخ ٢٧ / ٨ / ١٤١٢ هـ.
وبعد الاطلاع على قرار مجلس الشورى رقم (٦٨ /٤٣) وتاريخ ١٦ / ٩ / ١٤٢٧ هـ.
وبعد الاطلاع على قرار مجلس الوزراء رقم (٧٩) وتاريخ ٧ / ٣ / ١٤٢٨ هـ.

رسمنا بما هو آت:

أولًا: الموافقة على نظام مكافحة جرائم المعلوماتية، بالصيغة المرافقة.
ثانيًا: على سمو نائب رئيس مجلس الوزراء والوزراء – كل فيما يخصه – تنفيذ مرسومنا هذا.

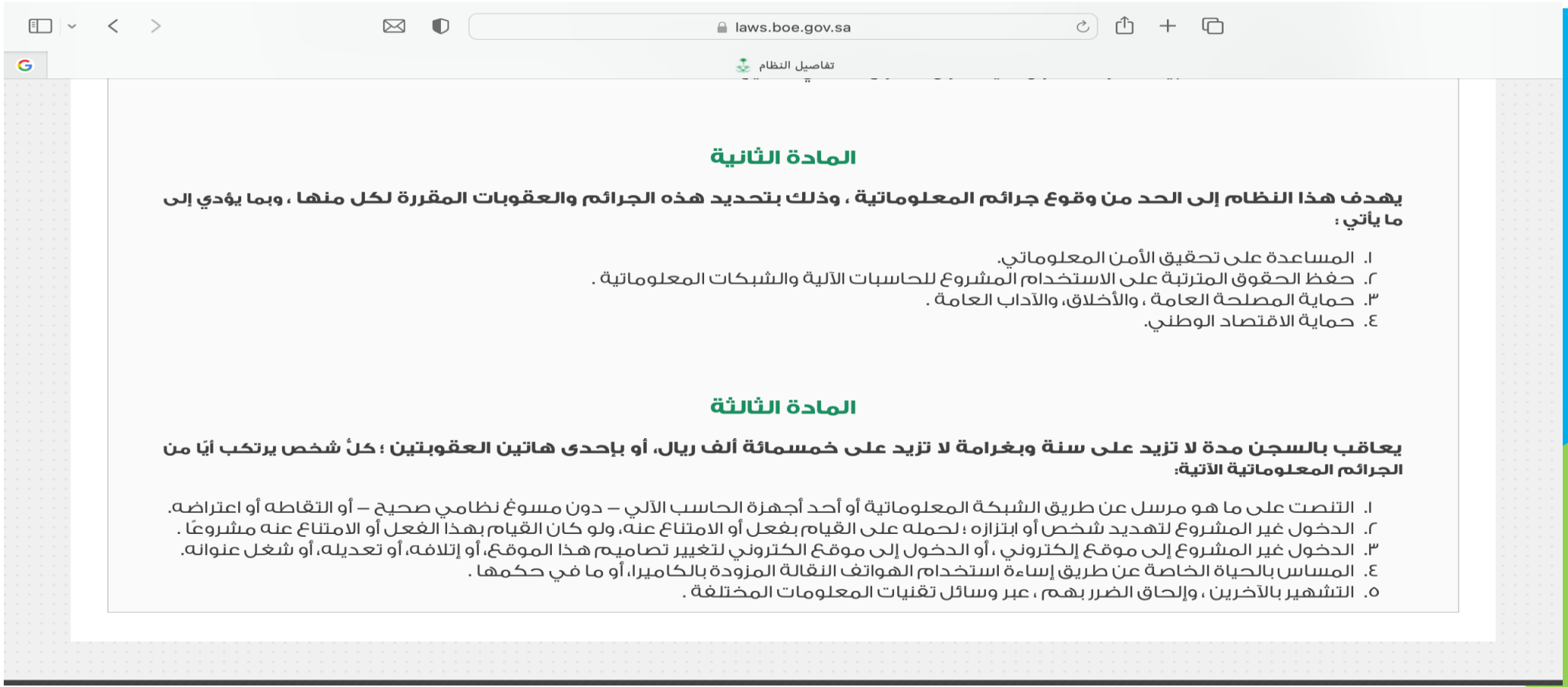
عبد الله بن عبد العزيز

بسم الله الرحمن الرحيم

قرار مجلس الوزراء رقم ٧٩ بتاريخ ٧ / ٣ / ١٤٢٨

إن مجلس الوزراء
بعد الاطلاع على المعاملة الواردة من ديوان رئاسة مجلس الوزراء برقم ٤٧٦٧٥/ب وتاريخ ٢٤ / ١٠ / ١٤٢٧ هـ، المشتملة على خطاب معالي وزير الاتصالات

تطبيق قانون الجرائم المعلوماتية السعودي والعقوبات والتشريعات



المادة الثانية

يهدف هذا النظام إلى الحد من وقوع جرائم المعلوماتية ، وذلك بتحديد هذه الجرائم والعقوبات المقررة لكل منها ، وبما يؤدي إلى ما يأتي :

١. المساعدة على تحقيق الأمن المعلوماتي.
٢. حفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية .
٣. حماية المصلحة العامة ، والأخلاق، والآداب العامة .
٤. حماية الاقتصاد الوطني.

المادة الثالثة

يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على خمسمائة ألف ريال، أو بإحدى هاتين العقوبتين ؛ كلُّ شخص يرتكب أيًا من الجرائم المعلوماتية الآتية:

١. التنصت على ما هو مرسل عن طريق الشبكة المعلوماتية أو أحد أجهزة الحاسب الآلي – دون مسوغ نظامي صحيح – أو التقاطه أو اعتراضه.
٢. الدخول غير المشروع لتهديد شخص أو ابتزازه ؛ لحمله على القيام بفعل أو الامتناع عنه، ولو كان القيام بهذا الفعل أو الامتناع عنه مشروعًا .
٣. الدخول غير المشروع إلى موقع إلكتروني ، أو الدخول إلى موقع الكتروني لتغيير تصاميم هذا الموقع، أو إتلافه، أو تعديله، أو شغل عنوانه.
٤. المساس بالحياة الخاصة عن طريق إساءة استخدام الهواتف النقالة المزودة بالكاميرا، أو ما في حكمها .
٥. التشهير بالآخرين ، وإلحاق الضرر بهم ، عبر وسائل تقنيات المعلومات المختلفة .

نظام مكافحة الجرائم المعلوماتية السعودي

https://laws.boe.gov.sa/BoeLaws/Laws/LawDetails/25df73d6-0f49-4dc5-b010-a9a700f2ec1d/1

معهد العراب العالي للتدريب

شكرا