University of Mohamed khider- Biskra
Faculty of Law & Political Science
Department of Law
Speciality : Business Law
Level : Master 1-Sem2

English legal terminology

2021-2022

Topic 4

The title : Cybercrime

1-Deinition of Cybercrime :

Cybercrime is the use of a computer as an instrument to further illegal ends, Cybercrime has grown in importance as the computer has become central to commerce, entertainment, and government.

Cybercrime is any criminal activity that involves a computer, networked device or a network. While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them. Others use computers or networks to spread malware, illegal information, images or other materials. Some cybercrimes do both, target computers to infect them with a computer virus, which is then spread to other machines and, sometimes, entire networks.

A primary effect of cybercrime is financial. Cybercrime can include many different types of profit-driven criminal activity, including ransomware attacks, email and internet fraud, and identity fraud, as well as attempts to steal financial account, credit card or other payment card information.

Cybercriminals may target an individual's private information or corporate data for theft and resale. As many workers settle into remote work routines due to the Corona pandemic, making it important to protect backup data.

Cybercrime can cause direct harm or indirect harm to whoever the victim is. However, the largest threat of cybercrime is on the financial security of an individual as well as the government.

1-تعريف الجريمة الالكترونية:

الجرائم الإلكترونية هي استخدام الكمبيوتر كأداة لتحقيق غايات أخرى غير قانونية، وقد ازدادت أهمية الجرائم الإلكترونية، حيث أصبح الكمبيوتر مركزًا للتجارة والترفيه والحكومة.

الجرائم الإلكترونية هي أي نشاط إجرامي يشمل جهاز كمبيوتر أو جهاز متصل بشبكة أو شبكة، بينما يتم تنفيذ معظم الجرائم الإلكترونية من أجل جني الأرباح لمجرمي الإنترنت، يتم تنفيذ بعض الجرائم الإلكترونية ضد أجهزة الكمبيوتر أو الأجهزة مباشرة لإتلافها أو تعطيلها. يستخدم الآخرون أجهزة الكمبيوتر أو الشبكات لنشر البرامج الضارة أو المعلومات غير القانونية أو الصور أو المواد الأخرى. تقوم بعض الجرائم الإلكترونية بكلا الأمرين، وتستهدف أجهزة الكمبيوتر لإصابتها بفيروس الكمبيوتر، والذي ينتشر بعد ذلك إلى أجهزة أخرى، وأحيانًا إلى شبكات كاملة.

التأثير الأساسي للجريمة الإلكترونية هو التأثير المالي. يمكن أن تشمل الجرائم الإلكترونية أنواعًا مختلفة من الأنشطة الإجرامية التي يحركها الربح، بما في ذلك هجمات برامج الفدية والاحتيال عبر البريد الإلكتروني والإنترنت والاحتيال في الهوية، فضلاً عن محاولات سرقة الحساب المالي أو بطاقة الائتمان أو معلومات بطاقة الدفع الأخرى.

قد يستهدف مجرمو الإنترنت المعلومات الخاصة بالفرد أو بيانات الشركة بغرض السرقة وإعادة البيع. نظرًا لأن العديد من العمال يستقرون في إجراءات العمل عن بُعد بسبب وباء كورونا، فمن المتوقع أن تزداد جرائم الإنترنت وتكرارها في عام 2021، مما يجعل من المهم حماية البيانات الاحتياطية.

يمكن أن تسبب الجرائم الإلكترونية ضررًا مباشرًا أو ضررًا غير مباشر لمن هو الضحية. ومع ذلك، فإن أكبر تهديد للجرائم الإلكترونية هو على الأمن المالي للفرد وكذلك الحكومة.

2-Types of Cybercrime :

The major types of cybercrime are :

-Computer virus : ***Computer virus, a portion of a computer program code that has been designed to furtively copy itself into other such codes or computer files. It is usually created by a prankster or vandal to effect a nonutilitarian result or to destroy data and program code or, in the case of ransomware, to extort by payment.***

-Hacking : ***It is an illegal practice by which a hacker breaches the computer"s security system of someone for personal interest. Software piracy is an attack that involves the unlawful copying, distribution and use of software programs with the intention of commercial or personal use. Trademark violations, copyright infringements and patent violations are often associated with this type of cybercrime.***

-Unwarranted mass-surveillance: ***Mass surveillance means surveillance of a substantial fraction of a group of people by the authority especially for the security purpose, but if someone does it for personal interest, it is considered as cybercrime.***

-Child pornography : ***It is one of the most heinous crimes that is brazenly practiced across the world. Children are sexually abused and videos are being made and uploaded on the Internet.***

-Child grooming and taking care of a child electronically to groom him for illegal purposes : ***It is the practice of establishing an emotional connection with a child especially for the purpose of childtrafficking and child prostitution.***

-Copyright infringement : ***If someone infringes someone"s protected copyright without permission and publishes that with his own name, is known as copyright infringement.***

-Money laundering : ***Illegal possession of money by an individual or an organization is known as money laundering. It typically involves transfers of money through foreign banks and/or legitimate business. In other words, it is the practice of transforming illegitimately earned money into the legitimate financial system.***

-Cyber-extortion : ***When a hacker hacks someone"s email server, or computer system and demands money to reinstate the***

system, it is known as cyber-extortion.

-Cyber-terrorism : ***Normally, when someone hacks government"s security system or intimidates government or such a big organization to advance his political or social objectives by invading the security system through computer networks, it is known as cyber-terrorism.***

-Cyber Security : ***Cyber security is a potential activity by which information and other communication systems are protected from and/or defended against the unauthorized use or modification or exploitation or even theft.***

Likewise, cyber security is a well-designed technique to protect computers, networks, different programs, personal data, etc., from unauthorized access.

-Cryptojacking: ***An attack that uses scripts to mine cryptocurrencies within browsers without the user's consent. Cryptojacking attacks may involve loading cryptocurrency mining software to the victim's system if the user's browser has a tab or window open on the malicious site.***

-Identity theft: ***An attack that occurs when an individual accesses a computer to glean a user's personal information, which they then use to steal that person's identity or access their valuable accounts, such as banking and credit cards. Cybercriminals buy and sell identity information for gain.***

-Credit card fraud: ***An attack that occurs when hackers infiltrate retailers' systems to get the credit card and/or banking information of their customers. Stolen payment cards can be bought and sold in bulk on darknet markets.***

-Cyberespionage: ***A crime involving a cybercriminal who hacks into systems or networks to gain access to confidential information held by a government or other organization. Attacks may be motivated by profit or by ideology. Cyberespionage activities can include every type***

of cyberattack to gather, modify or destroy data, as well as using network-connected devices, like webcams or closed-circuit TV (CCTV) cameras, to spy on a targeted individual or groups and monitoring communications, including emails, text messages and instant messages.

-Exit scam: The dark web, not surprisingly, has given rise to the digital version of an old crime known as the exit scam. In today's form of this crime, dark web administrators divert virtual currency held in marketplace escrow accounts to their own accounts - essentially, criminals stealing from other criminals.

2-أشكال الجريمة الالكترونية:

-فيروس الكمبيوتر: فيروس الكمبيوتر هو جزء من رمز لبرنامج الكمبيوتر الذي تم تصميمه لنسخ نفسه خلسة إلى رموز أو ملفات كمبيوتر آخر. عادةً ما يتم إنشاؤه بواسطة المخادع أو المخرب لإحداث نتيجة غير عسكرية أو لتدمير البيانات ورمز البرنامج أو في حالة برامج الفدية، للابتزاز بالدفع.

-القرصنة :إنها ممارسة غير قانونية يقوم من خلالها المتسلل باختراق نظام أمان الكمبيوتر لشخص ما لمصلحته الشخصية. وقرصنة البرامج هو هجوم يتضمن نسخ البرامج وتوزيعها واستخدامها بشكل غير قانوني بقصد استخدام تجاري أو شخصي. غالبًا ما ترتبط انتهاكات العلامات التجارية وانتهاكات حقوق النشر وانتهاكات براءات الاختراع بهذا النوع من الجرائم الإلكترونية.

-المراقبة الجماعية غير المبررة: تعني المراقبة الجماعية مراقبة جزء كبير من مجموعة من الأشخاص من قبل السلطة خاصة لأغراض أمنية، ولكن إذا قام شخص ما بذلك لمصلحة شخصية، فإنها تعتبر جريمة إلكترونية.

-استغلال الأطفال في المواد الإباحية: إنها واحدة من أبشع الجرائم التي تُمارس بوقاحة في جميع أنحاء العالم. يتعرض الأطفال للاعتداء الجنسي ويتم إنشاء مقاطع الفيديو وتحميلها على الإنترنت.

-العناية بالطفل الكترونيا لاستمالته لأغراض غير قانونية: إنها ممارسة إقامة علاقة عاطفية مع الطفل خاصة لغرض الاتجار بالأطفال وبغاء الأطفال.

-انتهاك حقوق الملكية: إذا انتهك شخص ما حقوق الطبع والنشر المحمية لشخص ما دون إذن ونشر ذلك باسمه، فيعرف ذلك بانتهاك حقوق النشر.

-غسيل الأموال: يُعرف الحيازة غير القانونية للأموال من قبل فرد أو منظمة باسم غسيل الأموال. عادة ما يتضمن تحويل الأموال من خلال البنوك الأجنبية و / أو الأعمال التجارية المشروعة. بمعنى آخر، إنها ممارسة تحويل الأموال المكتسبة بطريقة غير مشروعة إلى نظام مالي شرعي.

-الابتزاز الإلكتروني: عندما يخترق أحد المتطفلين خادم البريد الإلكتروني أو نظام الكمبيوتر الخاص بشخص ما ويطالب بالمال لإعادة النظام، يُعرف باسم الابتزاز الإلكتروني.

-الإرهاب السيبراني: عادة، عندما يقوم شخص ما باختراق نظام الأمن الحكومي أو تخويف الحكومة أو مثل هذه المنظمة الكبيرة للنهوض بأهدافه السياسية أو الاجتماعية من خلال غزو نظام الأمان من خلال شبكات الكمبيوتر، فإنه يُعرف باسم الإرهاب السيبراني.

-الأمن السيبراني: الأمن السيبراني هو نشاط محتمل يتم من خلاله حماية المعلومات وأنظمة الاتصال الأخرى و / أو الدفاع عنها ضد الاستخدام غير المصرح به أو التعديل أو الاستغلال أو حتى السرقة. وبالمثل، فإن الأمن السيبراني هو أسلوب جيد التصميم لحماية أجهزة الكمبيوتر والشبكات والبرامج المختلفة والبيانات الشخصية وما إلى ذلك، من الوصول غير المصرح به.

-الهجوم النصي: هجوم يستخدم البرامج النصية لتعدين العملات المشفرة داخل المتصفحات دون موافقة المستخدم. قد تتضمن هجمات Cryptojacking تحميل برنامج تعدين العملات المشفرة إلى نظام الضحية إذا كان متصفح المستخدم به علامة تبويب أو نافذة مفتوحة على الموقع الضار.

-سرقة الهوية: هجوم يحدث عندما يقوم شخص ما بالوصول إلى جهاز كمبيوتر للحصول على المعلومات الشخصية للمستخدم، والتي يستخدمها بعد ذلك لسرقة هوية هذا الشخص أو الوصول إلى حساباته القيمة، مثل البنوك وبطاقات الائتمان. يشتري مجرمو الإنترنت معلومات الهوية ويبيعونها للربح،

-الاحتيال على بطاقة الائتمان: هجوم الكتروني يحدث عندما يتسلل المتسللون إلى أنظمة تجار التجزئة للحصول على بطاقة الائتمان و / أو المعلومات المصرفية لعملائهم. يمكن شراء بطاقات الدفع المسروقة وبيعها من أجل الربح بكميات كبيرة في أسواق الشبكة المظلمة.

-التجسس الإلكتروني: جريمة تنطوي على مجرم إلكتروني يخترق أنظمة أو شبكات للوصول إلى المعلومات السرية التي تحتفظ بها حكومة أو منظمة أخرى. قد يكون الدافع وراء الهجمات هو الربح أو الأيديولوجية. يمكن أن تشمل أنشطة التجسس الإلكتروني كل نوع من أنواع الهجمات الإلكترونية لجمع البيانات أو تعديلها أو تدميرها، بالإضافة إلى استخدام الأجهزة المتصلة بالشبكة.

مثل كاميرات الويب أو كاميرات الدوائر التلفزيونية المغلقة (CCTV) ، للتجسس على فرد أو مجموعات مستهدفة ومراقبة الاتصالات ، بما في ذلك رسائل البريد الإلكتروني والرسائل النصية والرسائل الفورية.

-احتيال الخروج: ليس من المستغرب أن الويب المظلم قد أدى إلى ظهور نسخة رقمية من جريمة قديمة تُعرف باسم احتيال الخروج. في شكل اليوم لهذه الجريمة، يقوم مسؤولو الويب المظلم بتحويل العملة الافتراضية الموجودة في حسابات الضمان الخاصة بالأسواق إلى حساباتهم الخاصة بشكل أساسي، المجرمين الذين يسرقون من المجرمين الآخرين.

3-Effects of cybercrime on businesses :

While the financial losses due to cybercrime can be significant, businesses can also suffer other disastrous consequences as a result of criminal cyberattacks, including the following:

-Damage to investor perception after a security breach can cause a drop in the value of a company.

-In addition to potential share price drops, businesses may also face increased costs for borrowing and greater difficulty in raising more capital as a result of a cyberattack.

-Loss of sensitive customer data can result in fines and penalties for companies that have failed to protect their customers' data. Businesses may also be sued over the data breach.

-Damaged brand identity and loss of reputation after a cyberattack undermine customers' trust in a company and that company's ability to keep their financial data safe. Following a cyberattack, firms not only lose current customers, but they also lose the ability to gain new customers.

-Businesses may also incur direct costs from a criminal cyberattack, including increased insurance premium costs and the cost of hiring cybersecurity companies to do incident response and remediation, as well as public relation and other services related to an attack.

3-آثار الجرائم الإلكترونية على الأعمال التجارية:

يمكن أن تعاني الشركات من عواقب وخيمة أخرى نتيجة للهجمات الإلكترونية الإجرامية، بما في ذلك ما يلي:

-يمكن أن يتسبب الضرر الذي يلحق بتصور المستثمر بعد حدوث خرق أمني في انخفاض قيمة الشركة. بالإضافة إلى الانخفاضات المحتملة في أسعار الأسهم، قد تواجه الشركات أيضًا زيادة في تكاليف الاقتراض وصعوبة أكبر في جمع المزيد من رأس المال نتيجة للهجوم الإلكتروني.

-يمكن أن يؤدي فقدان بيانات العملاء الحساسة إلى فرض غرامات وعقوبات على الشركات التي فشلت في حماية بيانات عملائها. يمكن أيضًا مقاضاة الشركات بسبب خرق البيانات.

-يؤدي تلف هوية العلامة التجارية وفقدان السمعة بعد هجوم إلكتروني إلى تقويض ثقة العملاء في الشركة وقدرتها على الحفاظ على أمان بياناتهم المالية. بعد هجوم إلكتروني، لا تفقد الشركات العملاء الحاليين فحسب، بل تفقد أيضًا القدرة على اكتساب عملاء جدد.

-قد تتكبد الشركات أيضًا تكاليف مباشرة من هجوم إلكتروني إجرامي، بما في ذلك زيادة تكاليف أقساط التأمين وتكلفة توظيف شركات الأمن السيبراني للقيام بالاستجابة للحوادث ومعالجتها، فضلاً عن العلاقات العامة والخدمات الأخرى المتعلقة بالهجوم.

4- Prevent the cybercrime :

To prevent the cybercrime, various laws and legislation have been enacted in addition to the agencies that have been established to deal with cybercrime. In 2015, the United Nations Office on Drugs and Crime (UNODC) released the cybercrime repository, which is a central database that includes legislation, previous findings and case law on cybercrime and electronic evidence. The intention of the cybercrime repository is to assist countries and governments in their attempts to prosecute and stop cybercriminals.

Legislation dealing with cybercrime can be applicable to the general public, or it can be sector-specific, extending only to certain types of companies to protecte private information from threats and unauthorized access and use. Other legislation has been established

to deal with specific cybercrimes, such as cyberbullying and online harassment.

4-منع الجريمة الإلكترونية:

لمكافحة الجريمة الإلكترونية تم سن قوانين وتشريعات مختلفة في أغلب الدول بالإضافة إلى الوكالات التي تم إنشاؤها للتعامل مع الجرائم الإلكترونية. في عام 2015، أصدر مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC) مستودع الجرائم الإلكترونية، وهو قاعدة بيانات مركزية تتضمن التشريعات والنتائج السابقة والسوابق القضائية بشأن الجرائم الإلكترونية والأدلة الإلكترونية. الهدف من مستودع الجرائم الإلكترونية هو مساعدة البلدان والحكومات في محاولاتها لملاحقة المجرمين الإلكترونيين ووقفهم. ويمكن أن تكون التشريعات التي تتعامل مع الجرائم الإلكترونية قابلة للتطبيق على عامة الناس، أو يمكن أن تكون خاصة بقطاع معين أو شركات أو مؤسسات معينة، حيث يتم حماية المعلومات الخاصة من التهديدات والوصول والاستخدام غير المصرح بهما. كما يتم وضع تشريعات أخرى للتعامل مع جرائم الإنترنت المحددة، مثل التسلط عبر الإنترنت والمضايقات عبر الإنترنت.

References :

-Aaron Dennis Michael, Cybercrime, available on the link :

https://www.britannica.com/topic/cybercrime

-Brush Kate, Cybercrime, available on the link :

https://www.techtarget.com/searchsecurity/definition/cybercrime

-Cybercrime and its effect on businesses, Clickatell, available on the link :

https://www.clickatell.com/articles/information-security/cybercrime-effect-businesses/

-Desmet Niles, Cybercrime Effects on Business, available on the link :

https://www.linkedin.com/pulse/cybercrime-effects-business-why-you-should-care-nils-desmet

-Minahan Bill, Effects of cyber attacks on business, available on the link :

https://www.anetworks.com/effects-of-cyber-attacks-on-business/

-Narasimha rao B.V. L., Lecture notes on business laws and ethics, available on the link:

https://www.iare.ac.in/sites/default/files/Business%20Law%20%26Ethics%20Noes.pdf

-S Joseph, Lecture notes for business laws, available on the link :

https://josephscollege.ac.in/lms/Uploads/pdf/material/BLAW.pdf