جـامـعـة الدكتور يـحـي فـارس بـالـمـديـة

كلية العلوم الإنسانية والاجتماعية

قسم علوم الاعلام والاتصال

استخدامات الشباب الجامعي للفضاء السيبراني ومخاطر الجريمة الالكترونية

دراسة مسحية على عينة من طلبة قسم علوم الاعلام والاتصال بجامعة المدية المستخدمين لموقع الفيسبوك

خلال الفترة الممتدة من الفاتح جانفي إلى 20 أفريل 2024

مذكرة مكملة لنيل شهادة ماستر في علوم الاعلام والاتصال

تخصص: سمعي بصري

- الطالبتين :

بن صحصاح نور الهدى

بوستة بشرى

- إشراف :

د. شايب نبيل

السنة الجامعية: 2024/2023


بِسْمِ اللَّهِ الرَّحْمَٰنِ الرَّحِيمِ

شكر وتقدير

بسم الله الرحمن الرحيم:

الحمد لله الذي هدانا لهذا وما كنا لنهتدي لولا أن هدانا الله.

نتقدم بالشكر الجزيل والحمد لله الكثير في الأول والأخير للخالق تبارك وتعالى والذي بعونه ومشيئته تم إنجاز هذه المذكرة.

كما نتقدم بأسمى معاني الشكر والتقدير إلى أستاذنا

"شايب نبيل"

الذي تفضل بقبول الإشراف علينا والذي كان له كل الفضل في إنجاز هذا العمل من خلال توجيهاتهونصائحه .

وشكري الموصول إلى جميع الأساتذة الأفاضل بقسم علوم الإعلام والإتصال جامعة المدية خاصة الأستاذة الفاضلة "**فندوشي ربيعة**".

و الشكر موصول كذلك إلى جميع زملائي في الدراسة ماستر 2 سمعي بصري 2024/2023

الذين لم يبخلو علي بالمساعدة رغم كل مسؤولياتهم.

الإهداء:

لم تكن الرحلة قصيرة ولا ينبغي لها أن تكون، لم يكن الحلم قريب ولا الطريق محفوفا بالتسهيلات

لـــكنني فعلتها.....

بعد مسيرة دامت سنوات ها أنا اليوم أقف على عتبة تخرجي أقطف ثمار تعبي وأرفع قبعتي بكل فخر.

فالحمد لله حبا وشكراوإمتنانا، فما كنت لأفعل هذا لولا فضل الله

فالحمد لله على البدء والحمد لله على الختام.

أهدي هذا النجاح لنفسي أولا ثم إلى كل من سعى معي لإتمام هذه المسيرة

دمتم لي سندا لا عمرا.

إلى من شرفني بحمل إسمه والدي العزيز من بذل الغالي والنفيس واستمديت منه قوتي واعتزازي بذاتي،

الرجل الذي سعى طوال حياته لكي نكون أفضل منه.

أبي الغالي (جمال) حفضه الله.

إلى معنى الحب والحنان التي وهبتني الحياة والأمل، احتضنتني بقلبها قبل يدها

وسهلت لي الشدائدبدعائها.

والدتي الحبيبة (رشيدة) حفضها الله.

إلى الساندين والذين راهنو على نجاحي وكانو مصدر قوتي إلى من كانو خلفي مؤمنون بأني أستطيع

النجاح، من عشنا سويا حلو الحياة ومرها.

إخوتي وأخواتي (وليد، وهيبة، أحمد، عبد الله)

إلى صديقي ورفيقة دربي حين ظن الجميع أني بلا أصدقاء، هي التي آمنت بي حين اعترى الآخرون،

زميلتي في إنجاز مذكرة التخرج (بشرى)

ولا أنسى رفقاء الروح صديقاتي العزيزات، أصحاب الشدائد والأزمات (شهيناز، إحسان)

بن صحصاح نور الهدى

إهداء:

(وآخر دعواهم أنَ الحَمدُ لله رب العالمين)

الحمد لله حباً وشكراً وامتناناً على البدء والختام لم تكن الرحلة قصيرة ولا ينبغي لها أن تكون، لم يكن العلم قريباً ولا الطريق كان محفوفاً بالتسهيلات لكني فعلتها...

أهدي هذا النجاح لنفسي أولاً، ثم الي كل من سعى معي للإتمام هذه المسيرة دمتم لي سنداً لا عُمر له

الى ركني العظيم في الحياة الى من كلله الله بالهيبة والوقار الى من أحمل أسمه بكل فخر الى ذلك الرجل العظيم الذي بذل كل ما بوسعه مأمني الوحيد وفرحتي الدائمة

والدي الحبيب "السبتي" متعه الله بالصحة والعافية.

الى من وهج حياتي الى معنى الحب و الى معنى الحنان الى بسمة الحياة وسر الوجود الى من كان دعائها سر نجاحي وحنانها بلسم جراحي داعمي الأول ووجهتي التي أستمد منها القوة والدتي الحبيبه "سمية" متعها الله بالصحة والعافية.

إلى الأعمدة الثابتة في الحياة، الداعمين السائدين أرضي الصلبة وجداري المتين الى من مدت أياديهم في أوقات الضعف ويؤمنوا بشجاعتي مهما ضعفت وارتخيت واقفين خلفي

الى من شد الله بهم عضدي فكانوا خير معين اخوتي سفيان، سهير، بسمة.

الى ملائكة رزقني الله بهم لأعرف من خلالهم طعم الحياة الجميلة الذين غيرو مفاهيم الحب والصداقة والسند في حياتي " شهيناز، إحسان"

وأحب أن اختم الإهداء الى صاحبة الفضل العظيم صديقة الرحلة و النجاح الى من وقفت بجانبي كلما أوشكت ان أتعثر " نور الهدى".

بوستة بشرى

خطة الدراسة

مقدمة

الإطار المنهجي

1) إشكـالية الـدراسة
2) تساؤلات الـدراسـة
3) أسبـاب إختيار المـوضوع
4) أهـداف الـدراسـة
5) أهمـية الدراسـة
6) منـهج الـدراسة و أدواتها
7) مجتمع البحث وعينة الدراسة
8) مفاهيم و مصطلحات الدراسة
9) الـدراسات السـابقة وحدود الإستفادة منها

الإطار النظري

الفصل الأول: مدخل عام للفضاء السيبراني

تمهيد

📖 المبحث الأول: مفهوم الفضاء السيبراني .

📖 المبحث الثاني: خصائص الفضاء السيبراني .

📖 المبحث الثالث: أنواع الفضاء السيبراني .

📖 المبحث الرابع: مخاطر الفضاء السيبراني .

📖 المبحث الخامس: سبل ردع الهجمات السيبرانية .

خلاصة الفصل

الفصل الثاني :الجريمة الالكترونية : المفهوم ،الخصائص، الأنواع والأهداف

تمهيد

📖 المبحث الأول: مفهوم الجريمة الإلكترونية.

📖 المبحث الثاني: خصائص الجريمة الإلكترونية.

📖 المبحث الثالث: أنواع الجريمة الالكترونية .

📖 المبحث الخامس: سبل مكافحة الجريمة الإلكترونية والتشريعات القانونية.

خلاصة الفصل

الفصل الثالث: المقـترب النـظري للدراسة

تمهيد

📖المبحث الأول: مفهوم نظرية الإستخدامات و الإشباعات.

📖المبحث الثاني: نشأة النظرية .

📖المبحث الثالث: فروض النظرية .

📖المبحث الرابع: أهداف النظرية .

📖المبحث الخامس: إنتقادات النظرية .

خلاصة الفصل

الإطار التطبيقي

تمهيد

📖**أولا:** تحديد خصائص العينة المبحوثة

📖**ثانيا:** التحليل الكمي و الكيفي لبيانات الدراسة

📖**ثالثا** : عرض الإستنتاجات العامة و الجزئية للدراسة

خلاصة

ملخص الدراسة

عالجت هذه الدراسة إستخدامات طلبة قسم علوم الإعلام و الإتصال بجامعة يحي فارس بالمدية للفضاء السيبراني و مخاطر الجريمة الإلكترونية عبر موقع الفيسبوك، حيث تهدف هذه الأخيرة إلى التعرف على كيفية ممارسة الجريمة الالكترونية في موقع الفيسبوك، والوقوف على العوامل المساعدة على انتشارها، والكشف عن سبل مجابهتها من منظور الطلبة . وتصنف هذه الدراسة ضمن الدراسات المسحية التي حاولنا فيها رصد وجهات النظر المختلفة حول إستخدامات طلبة الجامعة للفضاء السيبراني ومخاطر الجريمة الالكترونية عن طريق أداة بحثية متمثلة في إستمارةالإستبيان التي احتوت على مجموعة من الأسئلة والتي وزعت على 120 مفردة من المجتمع الاصلي . وتمثلت عينة الدراسة في طلبة قسم علوم الإعلام والإتصال جامعة يحي فارس المدية .و بعد القيام بالقراءة الكمية و الكيفية لبيانات الدراسة وفق الأساليب الاحصائية المناسبة تم التوصل للنتائج العامة للدراسة المتمثلة في: أن جرائم القرصنة الإلكترونية من أكثر الجرائم شيوعا بين الطلبة من منظور هم، التي ترتكب عن طريق الروابط المشبوهة والبريد الالكتروني، والتي تعود بشكل سلبي عليهم من خلال تضرر سمعتهم وسرقة هويتهم الشخصية، وموقع الفيسبوك من أكثر المواقع التي تطبق عليه هذه الجرائم مقارنة بمواقع التواصل الاجتماعي الأخرى، خاصة بعد إفصاح الطلبة عن هوياتهم الشخصية وتسجيل الدخول عبر أجهزة الهواتف المحمولة والكمبيوتر ما يزيد من درجة التعرض لجرائم المعلوماتية لكونها أجهزة متصلة بالأنترنت، ما يسهل عمليات التهكير وسرقة البيانات ومنه التهديد والابتزاز.

كما أن معظم المبحوثين أي عينة الدراسة لم يتعرضو لأي جريمة إلكترونية لمعرفتهم الجيدة بالمخاطر الشائعة لهذه الجرائم، و بأن للوعي الرقمي وتحديث القوانين و الرقابة على إستخدامالفيسبوك دور جد هام في مجابهة الجرائم الإلكترونية، كذلك إستخدامهم كلمات مرور قوية و برامج مضادة للفيروسات.وأخيرا ثقافة الإبلاغ.

• **الكلمات المفتاحية:** الجريمة الإلكترونية، الفضاء السيبراني، الطلبة، الإستخدام، القرصنة .

Abstract

This study looks at university students' use of internet and the hazards of cybercrime on Facebook. Its goal is to analyse how cybercrime is perpetrated on Facebook, identify the variables that lead to its spread, and investigate solutions to counteract it from the students' perspective. We gathered various perspectives on university students' use of cyberspace and the risks of cybercrime using a research technique known as a survey. The Survey had a series of questions and was delivered to 120 people from the original community. The study sample included students from Yahia Fares University's Department of Media and Communication Sciences in Medea.

Following a quantitative and qualitative analysis of the study data using proper statistical methodologies, the survey's overall findings revealed that cyber hacking offences are among the most common crimes, according to the students. These crimes are frequently performed through questionable websites and emails, harming students' reputations and stealing their identities. Facebook is one of the most affected sites when compared to other social networking sites, especially after students reveal their personal identities and log in via mobile phones and computers, increasing their vulnerability to cybercrime due to these devices' internet connectivity, facilitating hacking and data theft, and ultimately leading to threats and blackmail.

Furthermore, because of their knowledge of the common risks connected with cybercrime, the majority of the survey participants had never been exposed to one. They recognised that digital awareness, updating regulations, and monitoring Facebook usage are critical in preventing cybercrime. Furthermore, they employed secure passwords and antivirus software. Finally, they stressed the need of reporting events.

Keywords: Cybercrime, Cyberspace, Students, Usage, Hacking.

مقدمة

مقدمة:

بينما يشهد العصر الحالي تطورات هائلة في مجال التكنولوجيا والإتصالات، تزداد أهمية الفضاء السيبراني كوسيلة حيوية لتبادل المعرفة والتواصل بين الأفراد والمؤسسات، إذ يعد الفضاء السيبراني بيئة غير محدودة تسمح بالوصول إلى معلومات متنوعة وتبادلها عبر الانترنت، فهو عبارة عن أهم البيئات الإفتراضية في العصر الحالي، يشكل بيئة رقمية متكاملة تتسم بالتنوع والديناميكية تشكلها شبكة الانترنت وأنظمة الحاسوب والأجهزة الذكية والأنظمة المتصلة بالانترنت، حيث تسهم في تفعيل هذا الفضاء الرقمي الواسع مجموعة من التقنيات الرقمية كأنظمة الدفع الإلكتروني، أنظمة إدارة المحتوى، تطبيقات ذكية، البريد الإلكتروني، الشبكات الإجتماعية، مواقع الويب وغيرها من التقنيات الأخرى.....

هذا ما جعله محط إهتمام الطلاب الجامعيين لإستخداماته المتعددة في مختلف المجالات الأكاديمية والإجتماعية، إذ تتميز الجامعات بكونها مراكز حيوية للتعليم والبحث حيث يلجأ طلاب الجامعة إلى الفضاء السيبراني لتبادل الموارد التعليمية وإجراء أبحاثهم والتواصل مع زملائهم وأساتذتهم .فضلا عن ذلك يستخدم الطلاب الفضاء السيبراني لأغراض شخصية وترفيهية مثل التواصل الإجتماعي ومشاركة المحتوى خاصة على موقع الفيسبوك، إذ يعتبر واحدا من أبرز الأدوات الإجتماعية عبر الانترنت الأكثر إستخداما من طرف طلبة الجامعة.

مع ذلك لا يخلو الفضاء السيبراني من التحديات والمخاطر المتزايدة التي يتعرض لها الطلبة من جرائم الانترنت على موقع الفيسبوك خاصة والهجمات السيبرانية عامة من بين هذه الجرائم المعلوماتية نجد الإحتيال الإلكتروني والقرصنة الإلكترونية وسرقة الهوية وإنتهاك الخصوصية وغيرها ...ما يأثر سلبا على هذه الفئة.

ليصبح من الضروري فهم هذه المخاطر وتحديدها لتطوير إستراتيجيات أمنية فعالة لحماية طلاب الجامعة أثناء إستخدامهم لموقع الفيسبوك والفضاء السيبراني بشكل عام، كذلك تعزيز الثقافة الرقمية لحمايتهم الشخصية ومعلوماتهم على الانترنت .

ومن أجل إبراز مخاطر الجريمة الإلكترونية عبر موقع الفيسبوك التي يتعرض لها الطلبة قمنا بتقسيم دراستنا من خلال خطة البحث التي إشتملت على مقدمة والإطار المنهجي والإطا ر النظري والإطار التطبيقي .حيث جاء في الإطار المنهجي: إشكالية الدراسة، وتساؤلات الدراسة مع الوقوف على

أهم أسباب إختيار الموضوع وأهداف الدراسة وأهميتها بالإضافة إلى تحديد أهم المفاهيم الإجرائية المتعلقة بالإطار العام للدراسة، كذلك الدراسات السابقة، المنهج المستخدم وتحديد مجتمع البحث والعينة، وأدوات جمع البيانات .

أما الإطار النظري للدراسة: قمنا بتخصيص له 3 فصول الفصل الأول بعنوان الفضاء السيبراني الذي جاء تحته خمسة مطالب متضمنة: مفهوم الفضاء السيبراني، خصائصه، أنواع الفضاء السيبراني، المخاطر وسبل ردع الهجمات السيبرانية . الفصل الثاني بعنوان الجريمة الإلكترونية الذي جاء تحته ستة مطالب متضمنة: مفهوم الجريمة الإلكترونية، الخصائص، أنواع الجريمة الإلكترونية، أهدافها، سبل مكافحة الجريمة الإلكترونية وكمطلب أخير بعنوان التشريعات القانونية لمكافحة جرائم الانترنت.

الفصل الثالث بعنوان مقترب نظري لنظرية الإستخدامات والإشباعات الذي جاء تحته خمسة مطالب متضمنة مفهوم النظرية، نشأة النظرية، فروض النظرية، أهداف النظرية وفي الأخير الإنتقادات الموجهة لنظرية.

أما بالنسبة للإطار التطبيقي تضمن إستمارة إستبيانية ودراستها كميا وكيفيا مع التحليل، مكونة من 4 محاور المحور الأول متعلق بالبيانات الشخصية لطلبة، المحور الثاني بعنوان: ممارسة الجريمة الإلكترونية في موقع الفيسبوك من منظور الطلبة، المحور الثالث بعنوان: العوامل المساعدة على إنتشار الجريمة الإلكترونية عبر الفيسبوك من منظور الطلبة، المحور الرابع بعنوان: سبل مجابهة الجريمة الإلكترونية من منظور الطلبة .

خلصنا بذلك إلى عرض النتائج والإجابة على أسئلة الدراسة.

الإطار المنـــهـجي لـلدراســة

1) إشكـــــالية الـــــدراسة
2) تســـاؤلات الـــــدراســـة
3) أسبـــاب إختيار المـــــوضوع
4) أهـــــداف الـــدراســـة
5) أهمـــــــية الدراســـــة
6) منهج الدراسة و أدواتها
7) مجتمع البحث وعينة الدراسة
8) مفاهيم ومصطلحات الدراسة
9) الدراسات السابقة وحدود الإستفادة منها

1) إشكالية الدراسة.

يعتبر الفضاء السيبراني ذلك العالم الإفتراضي الذي يتكون من شبكات الكمبيوتر المترابطة، ويشمل المواقع الإلكترونية، وسائل التواصل الاجتماعي، البريد الإلكتروني وألعاب الفيديو وغيرها من المنصات الرقمية التي تضبطها مجموعة من الممارسات والتقنيات لحماية تلك الانظمة، الشبكات، البرامج والبيانات كذلك حماية خصوصية الأفراد والأمن القومي من الهجمات الالكترونية ما يسمى بالدفاع السيبراني خط الدفاع الأول، حيث أصبح ضروريا أكثر من أي وقت مضى وهو ممارسة حماية الأنظمة الإلكترونية من الهجمات يشمل ذلك حماية الأجهزة من الوصول غير المصرح به أو الإستخدام أو التعديل أو الإتلاف أو السرقة.

كما يعد الفضاء السيبراني فضاءا إفتراضيا مفتوحا يوفر العديد من الإيجابيات أهمها كونه يسهل التواصل بين الناس من جميع أنحاء العالم بغض النظر عن الموقع الجغرافي والزمن، يتيح التواصل عبر الأنترنيت، التعلم عن بعد، مشاركة المعلومات والأفكار والتواصل مع المعلميين والطلاب، إضافة إلى مجالات أخرى كالتجارة والأعمال، المشاركات السياسية، الوعي الثقافي وغيرها .

لكنه يأتي أيضا مع العديد من السلبيات نذكر منها الجرائم الإلكترونية كالقرصنة الإلكترونية بإختراق أنظمة الكمبيوتر وسرقة البيانات، الإدمان الإلكتروني، إنتشار معلومات مضللة، التأثير على الرأي العام، فقدان الخصوصية، التشهير والتهديد كذلك التحرش الجنسي عبر مواقع التواصل الإجتماعي وغيرها من جرائم المعلوماتية الأخرى.

فالطالب الجامعي من أكثر الفئات إستخداما للفضاء السيبراني والمواقع الإلكترونية حيث ان هؤلاء هم الأكثر إستخداما لها حيث يمتلكون المهارات الحاسوبية، ولديهم إطلاع واسع على الكمبيوتر واستخداماته وشبكات الانترنت، خاصة بعد تطورات التكنولوجيا الحديثة وظهور تقنيات جديدة مثل الذكاء الإصطناعي، كون هذا الفضاء يساهم بشكل كبير في حياة الطالب من خلال الدراسات والأبحاث الأكاديمية، التعلم عن بعد، الإبداع والتعبير، الترفيه وأهم من ذلك الترويج للمشاريع الشخصية، ما يقابله مجموعة من المخاطر نذكر منها إهدار الوقت، التنمر الإلكتروني وسرقة الهوية .

ولعل أكثر ما يواجه الطالب أو يتعرض له في هذا العالم الإفتراضي هو الجريمة الإلكترونية بكل أنواعها خاصة على موقع الفيسبوك كونه أكثر شيوعا عند الطلبة الجامعيين .

ومن هنا فإن السؤال الجوهري الذي سنحاول معالجته من خلال هذه الدراسة يمكن وضعه وفق الصياغة التالية:

ما هي إنعكاسات مخاطر الجريمة الإلكترونية على طلبة الإعلام والإتصال بجامعة المدية المستخدمين لموقع الفيسبوك ؟

2) تساؤلات الدراسة.

- كيف تمارس الجريمة الإلكترونية في موقع الفيسبوك ؟
- ماهي العوامل المساعدة على انتشار الجريمة الإلكترونية عبر الفيسبوك ؟
- ماهي سبل مجابهة الجريمة الإلكترونية ؟

3) أسباب إختيار الموضوع.

1) أسباب ذاتية:

- الإهتمام الشخصي بالموضوع.
- الإهتمام بكل ما يتعلق بوسائل التواصل الإجتماعي خاصة.
- الرغبة في حل مشكلة التعرض للجريمة الإلكترونية على موقع الفيسبوك.
- إعتبار الجريمة الإلكترونية مشكلة العصر.
- التعرض لهذا النوع من الإجرام من خلال موقع الفيسبوك.

2) أسباب موضوعية:

- كون الجرائم الإلكترونية ظاهرة مستحدثة تعرف تطورا مستمرا .
- إنتشار إستخدام منصة الفيسبوك بين الطلبة الجامعيين، إذ يعتبر الفيسبوك من اكثر المنصات شيوعا بين هذه الفئة .
- تزايد حالات التعرض لهذه الجرائم الإلكترونية خاصة عبر الفيسبوك.
- زيادة الوعي الأمني لدى الطلبة وتزويدهم بالمعرفة .
- الموضوع المطروح متعلق بتخصصي اي تخصص إعلام وإتصال .

4) أهداف الدراسة .

يمكن تلخيص أهداف الدراسة في ما يلي:

- معرفة إستخدامات الطلبة الجامعيين للفضاء السيبراني وتسليط الضوء على مخاطر الجريمة الإلكترونية التي يتعرضون لهاعبرموقع الفيسبوك بغرض تطوير سياسات فعالة للتعامل مع هذه الإشكالية.
- إضافة دراسة جديدة تركز على جانب مهمش من جوانب الجريمة الإلكترونيية وهي الجرائم الواقعة على الطلبة.

- نهدف إلى التعرف على الجوانب السلبية للتقنية الحديثة وتأثيرهاعلى فئة الطلبة الجامعيين.

5) أهمية الدراسة.

- تعد هذه الدراسة من بين الدراسات الحديثة التي يعيشها العصر الحالي خاصة أن الطلبة الجامعيين يستخدمون بكثرة مواقع التواصل الإجتماعي على رأسها موقع الفيسبوك .
- إضافة معرفة علمية جديدة ووجهات نظر جديدة متعلقة بجرائم الأنترنيت وإنعكاساتها على الطالب الجامعي.
- تعمل هذه الدراسة على توعية الطالب لحماية بياناته الشخصية وخصوصياته الفردية.

6) منهج الدراسة وأداوتها :

منهج الدراسة: إن طبيعة الظاهرة أو ميدان البحث هما اللذان يفرضان على الباحث المنهج المناسب لإستقصاء تفاصيل الموضوع كلها وجمع المعلومات والتوصل الى إستنتاجات مرضية.[1]

تعريف المنهج المسحي:

تعريف هوينتي: المسح الإجتماعي هو محاولة منظمة للإبلاغ عن الوضع الحالي لنظام إجتماعي أو مجموعة أو بيئة معينة وتحليله وشرحه، يركز على الوقت الحاضر بدلا من اللحظة الحالية . كما يهدف إلى الحصول على بيانات قابلة للتصنيف والتفسير ومصممة للإستفادة منها مستقبلا خاصة للأغراض العلمية.[2]

تعليل إستخدام المنهج المسحي:

- لتحليل البيانات وجمعها من مختلف المصادر مثل الإستبيانات .
- لجمع البيانات الكمية حول إستخدامات الطلاب الجامعي بولاية المدية لموقع الفيسبوك، ومعرفة كيفية إستخدامهم للفضاء السيبراني والانشطة التي يقومون بها، والمخاطر التي يتعرضون لها .
- الزيادة من دقة وصحة النتائج .

---

1 عامر قنديلجي: البحث العلمي وإستخدام مصادر المعلومات، دار اليازوري العلمية للنشر والتوزيع، الاردن، 1999، ص 31.

2 د.عبود عبد الله العسكري: منهجية البحث العلمي في العلوم النفسية والتربوية، دار النمير، 2006، ص 112.

- إكتشاف علاقات جديدة بين المتغيرات المختلفة .
- لفهم الظاهرة بشكل أفضل والحصول على صورة شاملة لظاهرة .
- قلة التكلفة: يعد المنهج المسحي من أرخص مناهج البحث العلمي ولا يتطلب موارد مادية كبيرة .
- لا يتطلب مهارات تقنية عالية.

أدوات الدراسة:

تعرف على أنها: تلك الوسائل التي يستخدمها الباحث في جمعه للمعلومات والبيانات المستهدفة في بحثه ضمن إستخدامه لمنهج معين أو أكثر .[1]

فقد إعتمدنا في دراستنا على **أداة الإستبيان** لأنها تتلائم مع طبيعة وأهداف ومنهج الدراسة.

تعريف الإستمارة: يعرفها رشيد زرواتي: "هي عبارة عن مجموعة من الاسئلة المرتبة حول موضوع معين يتم وضعها في إستمارة وتقدم إلى أشخاص معينيين قصد الحصول على أجوبة الأسئلة الواردة، كما أن الإستمارة هي الوسيلة العلمية التي تساعد الباحث على جمع الحقائق والمعلومات عن المبحوث من خلال عملية المقابلة ".[2]

محاور الإستمارة: الإستمارة الإستبيانية تقسم إلى 3 أبولب رئيسية:

الباب الأول: يجب أن يحتوي الفصل الأول على معلومات عن الجهة التي تجري البحث في الصفحة الاولى ثم بعدها يذكر عنوان الدراسة، متبوعا بإسم الباحث أو الفريق البحثي المشرف على الدراسة، ثم في نهاية زاوية الصفحة يحدد تاريخ إجراء المقابلة وإسم المقابل، يمكننا أيضا كتابة العبارة التالية على الصفحة الأولى: "إن المعلومات التي تزودنا بها لن يطلع عليها أي شخص أو أي جهة، ولن تستخدم إلا في أغراض هذا البحث العلمي مهما كانت الأحوال "

يمكن لمثل هذه الملاحظات أن تشجع المشاركين علر تجاوز القلق والتردد.

الباب الثاني: ويغطي جميع المعلومات العامة أو الشخصية ذات الصلة بالمبحوث: عمره، مستواه التعليمي، التخصص...

---

[1] أحمد بن مرسلي: مناهج البحث العلمي في علوم الإعلام والإتصال، ديوان المطبوعات الجامعية، الجزائر، ط3، 2007، ص202.

[2] رشيد زرواتي: منهجية البحث العلمي في البحوث الإجتماعية، دار الكتاب الحديث،، 2004

الباب الثالث: يتعلق بالأسئلة المتخصصة التي يدور حولها البحث أو موضوع الدراسة.[1]

7) مجتمع البحث وعينة الدراسة:

1) مجتمع البحث:

يعرف مجتمع البحث على أنه: "مجموعة المفردات التي تستهدف الباحث دراستها لتحقيق نتائج الدراسة بمعنى جميع الوحدات التي يرغب الباحث في دراستها، ويمثل المجتمع الكل أو المجموع الأكبر الذي يستهدف دراسته ويتم تعميم نتائج الدراسة على كل مفرداته، إلا أنه يصعب الوصول هذا المجتمع المستهدف، فيتم التركيز على المجتمع المتاح أو الممكن الوصول إليه أو الإقتراب منه لجمع البيانات .[2]

فيما يخص دراستنا يتمثل أفراد مجتمع بحثنا المتعلق بإستخدامات طلبة الجامعة للفضاء السيبراني ومخاطر الجريمة الإلكترونية في طلبة كلية العلوم الإنسانية والإجتماعية بجامعة المدية، حيث اقتصرت الدراسة على طلبة قسم علوم الإعلام والإتصال ضمن طور ليسانس وماستر 1و2 من ذكور وإناث للعام الدراسي 2024/2023، إذ بلغ عددهم الإجمالي 551 بين طلبة الإعلام، إتصال وعلاقات عامة وسمعي بصري .

وتمثلت خصائص أفراد مجتع بحثنا في إختلاف جنسهم والقرب المكاني والزماني منهم، وبالتالي سهولة التواصل معهم بصفة مباشرة.

2) عينة الدراسة:

عرفت العينة على أنها: "جزء من وحدات المجتمع لها نفس خواص المجتمع الأصلي وعليه فإن اختيار العينة وقياس المتغيرات موضوع البحث تكون ممثلة لوحدات المجتمع الأصلي ".[3]

و عليه فقد إعتمدنا في هذه الدراسة على العينة الحصصية وهي أكثر أنواع العينات غير العشوائية استخداما في البحوث الاجتماعية ،وتقوم على أساس وجود عدم تجانس بين مفردات مجتمع البحث ، مما

---

[1] عبد الغني عماد: منهجية البحث في علم الإجتماع: الإشكاليات، التقنيات، المقاربات، دار الطليعة للطباعة والنشر، ط1، بيروت، 2008، ص63-64.

[2] عامر مصباح: منهجية البحث في العلوم السياسية والإعلام، ديوان المطبوعات الجامعية، 2008، ص49.

[3] لحسن عبد الله باشيوة، وآخرون، البحث العلمي: مفاهيم-أساليب-تطبيقات، ط1، مؤسسة الوراقة، عمان، 2010، ص258.

يتطلب من الباحث ان يقوم بتحديد الخصائص التي تتصف بها عناصر المجتمع ، وبعد تقسيم عناصر المجتمع الى قطاعات حسب تلك الخصائص يتم اختيار العينة ، بحيث تتوفر فيها تلك الخصائص بنفس نسبة وجودها في المجتمع.[1]

تمثلت عينة الدراسة في طلبة الإعلام والإتصال بجامعة يحي فارس المدية كونهم الفئة أكثر إلماما بالمعلومات المتعلقة بدراستنا بحكم تخصصهم وتمكنهم من الإجابة على الأسئلة بشكل أفضل .وعلى هذا الأساس اخترنا 120 مفردة متكونة من طلبة السنة الثالثة ليسانس تخصص إعلام، طلبة الماستر 1و2 تخصص سمعي بصري وإتصال وعلاقات عامة، حيث يتكون مجتمع البحث من حوالي 551 طالب المكون من 5 طبقات: حجم الطبقة الاولى 247 طالب من قسم الإعلام للسنة الثالثة ليسانس ، الطبقة الثانية 100طالب سنة اولى ماستر اتصال وعلاقات عامة، الطبقة الثالثة 114طالب سنة ثانية ماستر اتصال وعلاقات عامة، الطبقة الرابعة 25 طالب سنة اولى ماستر سمعي بصري والطبقة الخامسة 65 طالب سنة ثانية ماستر سمعي بصري.

8) مفاهيم ومصطلحات الدراسة:

يعتبر تحديد المفاهيم والمصطلحات أمرا ضروريا في البحث العلمي، تساعد على فهم الموضوع بشكل دقيق وواضح وأمم من ذلك التقرب من الاهداف الحقيقية للموضوع .

أولا: السيبرانية:

لغويا: مأخوذة من كلمة (سيبر) وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الإفتراضي فالسيبرانية تعني (فضاء الانترنت).[2]

وهي كلمة مشتقة من الكلمة اليونانيةkybernetesالتي وردت بداية في مؤلفات الخيال العلمي، وكان يقصد بها قيادة ربان السفينة.[3]

---

[1] د.خليفي رزقي،د.شيقارة هجيرة:"منهجية تحديد نوع وحجم العينة في البحوث العلمية"،مجلة المعارف،العدد23،،جامعة امحمد بوقرة بومرداس ،ديسمبر 2017،ص286.

[2] أحمد عبيس نعمة الفتلاوي: الهجمات السيبرانية مفهومها والمسؤولية الدولية الناشئة عنها في ضوء التنظيم المعاصر، بحث مقبول للنشر في مجلة المحقق الحلي، العراق، جامعة الكوفة، كلية القانون، 2016، ص05.

[3] رمزي منير البعلبكي: المورد الحديث، لبنان، دار العلم الحديث، د.س، ص307.

إصطلاحا: عرف قاموس مصطلحات الأمن المعلوماتي السيبرانية انها هجوم عبر الفضاء الإلكتروني يهدف الى السيطرة على مواقع إلكترونية او بنية محمية الكترونيا لتعطيلها او تدميرها او الإضرار بها .

وعرف قاموس المصطلحات العسكرية الامريكية السيبرانية بأنها "اي فعل يستخدم عن طريق شبكات الكترونية بهدف السيطرة أو التعطيل لبرامج إلكترونية أخرى".[1]

إجرائيا:

السيبرانية هي علم يخص الشبكات الإلكترونية الحاسوبية وشبكة الانترنت أو بمعنى شامل كل ما يتعلق بالواقع الإفتراضي، تتحكم في الأنظمة المغلقة والآلات (القيادة والتحكم)، كما تهدف إلى السيطرة على المواقع الإلكترونية وغيرها بتعطيلها وسرقة كل من المعلومات والبيانات الشخصية منها ما يسمى بالهجوم الإلكتروني.

ثانيا: الجريمة:

لغويا: كلمة جريمة من جرم أي الكسب المستهجن والمكروه والجرم: التعدي والجرم، كذلك هو الذنب

والجمع إجرام وجروم وهو الجريمة .[2]

الجريمة crime: نمط من السلوك حددت عناصره بدقة يتضمن جزاءا عقابيا، انتهاك لمعيار يتضمن جزاءا عقابيا، انتهاك لمعيار يعتقد أنه يشكل تهديدا للمجتمع .[3]

إصطلاحا: عرفها الأستاذ محي الدين عوض بقوله: "الجريمة هي عمل او إمتناع طارىء له مظهر خارجي ليس إستعمالا لحق ولا قياما بواجب يجرمه القانون ويفرض عليه عقابا ويقوم به إنسان أهل لتحمل المسؤولية الجنائية.[4]

---

[1] أحمد عبيس نعمة الفتلاوي، مرجع سابق، ص713.

[2] عمار مساعدي: مكافحة الاجرام والإجرام المنظم، ورقة مقدمة لمؤتمر العمل التطوعي والامن في الوطن العربي، اكاديمية نايف الرياض، 2000، ص2.

[3] مصلح الصالح "الشامل، قاموس مصطلحات العلوم الإجتماعية انجليزي .عربي"دار علم الكتب للطباعة والنشر والتوزيع، ط1، السعودية، 1999، ص129- 130.

[4] محمد محي الدين عوض: القانون الجنائي مبادئه الاساسية ونظرياته العامة، مكتبة جامعة القاهرة، مصر، 1981، ص95.

إجرائيا: الجريمة هي كل فعل او إمتناع عن فعل يجرمه القانون ويرد علية بعقوبة جزائية، او هي سلوك ينتهك قواعد الأخلاق والمبادىء الإنسانية يخل بالنظام الإجتماعي ويؤثر على القيم والمعايير داخل المجتمع .

ثالثا: الفيسبوك:

لغويا: والفيسبوك هو كلمة أعجمية مكونة من جزأين: فيس face وبوك book، وهي تعني كتاب الوجوه مثلما أراد بها مؤسس الفيسبوك.[1]

إصطلاحا: واحد من أهم مواقع التشبيك الاجتماعي وهو لايمثل منتدى اجتماعيا فقط، وإنما أصبح قاعدة تكنولوجية سهلة بإمكان اي شخص ان يفعل ما يشاء عن طريقها، وتقوم آلية التواصل وإرسال الأخبار في الفايسبوك على مجموعة من السمات التي تتيح للمستخدميين إمكانية التواصل مع بعضهم البعض.[2]

إجرائيا: الفيسبوك هو موقع تواصل إجتماعي الأكثر شهرة في العالم يسمح للأشخاص بالتواصل ومشاركة المحتوى مع الآخرين عبر الأنترنيت بهدف التعرف على أحداث وأخبار جديدة.

رابعا: الطالب الجامعي:

لغويا:

" طالب، يطالب، مطالبة وطلابا، فهو مطالب، والمفعول مطالب.

طالبه بالشيء: سأل بإلحاح مايعتبره حقا له، طالبه بنصيبه: طلب منه ان يمنحه نصيبه ".[3]

إصطلاحا:

عرف محمد إبراهيم الطالب على انه: " الفرد الذي اختار مواصلة الدراسة الأكاديمية والمهنية، ويأتي الى الجامعة محملا معه جملة القيم وتوجيهات صقلتها المؤسسات التربوية الأخرى والجامعة من المفروض أن تحضره للحياة العليا ".[1]

---

[1] قمجية حسان أحمد: الفيس بوك تحت المجهر، دار النخبة للنشر والتوزيع، ط1، مصر، 2017، ص24.

[2] د.عباس مصطفى صادق: صناعة الخبر بين الإعلام التقليدي والجديد، مؤتمر وسائل التواصل الإجتماعي، جامعة الإمام محمد بن سعود الإسلامية، كلية الإعلام والإتصال، أبو ظبي، ص17 www.academid.edu/33451664/

[3] معجم المعاني الجامع – معجم عربي عربي، دون مكان، دون سنة، ص24.

إجرائيا: الطالب الجامعي هو الشخص الذي يدرس في الجامعة للحصول على شهادة جامعية، حيث يتبع برنامج دراسي يشمل مواد مختلفة في تخصصه، ويشارك في الدروس والمحاضرات والأعمال والبحوث . بهدف الحصول على المعرفة والمهارات اللازمة لممارسة مهنة معينة أو مواصلة التعليم العالي .

[1] محمد إبراهيم: دور التربية في مستقبل الوطن العربي، دار مجدلاوي، عمان، ط1، 2003، ص222-223.

9) الدراسات السابقة:

هناك العديد من الدراسات التي عالجت موضوع أثر الأنترنت على الشباب والجريمة الإلكترونية من زوايا مختلفة . نذكر منها:

الدراسة الأولى: للطالب دحماني سمير.

دراسة حول **أثر شبكة الانترنت لدى الشباب في ظل العولمة الإعلامية**، عبارة عن مذكرة ماجستير مناقشة بقسم علوم الإعلام والإتصال جامعة الجزائر3 2008- 2009.

إشكالية الدراسة: هل يمكن أن يكون لإستخدام شبكة الانترنت أثر على الهوية لدى الشباب الجامعي الجزائري في ظل العولمة الإعلامية ؟ واي إتجاهات تحملها هذه الفئة نحو ذلك ونحو هويتهم الثقافية ؟

أهداف الدراسة: دراسة تأثير إستخدام الانترنت على إتجاهات الشباب الجامعي تجاه هوياتهم الإجتماعية والثقافية للشباب، وتحديد الإرتباطات بين تأثير إستخدام الانترنت على الهويات الثقافية للشباب، وتحديد بعض الأسباب التي تؤدي الى ذلك .

المنهج: المنهج المسحي من خلال العينة العربية عدد أفرادها 340 فرد .

الأداة: الملاحظة المقصودة والمنتظمة .

حدود الإستفادة منها: تركز الدراسة على تحليل إستخدام الشباب الجامعي للهوية الإفتراضية في مواقع التواصل داخل الشبكات الإجتماعية، وتسلط الضوء على تأثير شبكة الأنترنت على الشباب في ظل العولمة . تحققت الدراسة من العديد من النقاط التي يمكن أن تفيدنا في الدراسة خاصة فيما يتعلق " بتأثير إستخدام الشباب لفيسبوك على هويتهم الفردية ".

الدراسة الثانية: دراسة كلير وآخرون .

دراسة بعنوان "**مواقع التواصل الإجتماعي وأثرها على الحالة النفسية للطالب الجامعي** "

مشكلة الدراسة: تناولت مشكلة الدراسة الأسئلة التالية:

س1- ماهي التأثيرات النفسية لإستخدام وسائل التواصل الإجتماعي على هؤلاء الطلاب ؟

س2- ما الذي يدفع الطلاب الجامعي في مختلف البلدان العربية الى إستخدام مواقع التواصل الإجتماعي؟

س3- هل تختلف الإشباعات المحققة من إستخدام مواقع التواصل الإجتماعي من بلد غلى آخر؟

أهداف الدراسة:

العلاقة ما بين معدل إستخدام الشباب الجامعي لمواقع التواصل الإجتماعي .

دوافع هؤلاء الشباب من إستخدام هذه المواقع .

أكثر مواقع التواصل الإجتماعي إستخداما بين الشباب الجامعي .

المنهج: المنهج الوصفي الارتباطي، كانت العينة عشوائية تتكون من 227 فرد من الشباب الجامعي في البلدان العربية .

نتائج الدراسة: توصل الباحثون الى:

وجود فروقات ذات دلالة إحصائية بين خصائص البيئة لشباب الجامعي العربي وفق البلد بالنسبة للإشباعات المحققة عبر إستخدام مواقع التواصل الإجتماعي، كذلك تبين ان إستخدام هذه المواقع يعزز الإحساس بالحضور الإجتماعي، كما ظهر وجود علاقة ذات دلالة إحصائية ما بين المعدل اليومي لإستخدام مواقع التواصل الإجتماعي والتغير والإحباط.

حدود الإستفادة منها: توافقت دراستنا مع دراسة كلير الحلو في التركيز على مواقع التواصل الإجتماعي كجزء من موضوع البحث، وكذلك إستهدفت الطلبة الجامعيين ومع ذلك إختلفت الدراسة في أنها أجريت في بعض البلدان العربية، وهذا يمثل إختلافا في سياق الدراسة عن دراستنا .

الدراسة الثالثة: لطالبة قمقاني فاطمة الزهراء

دراسة ميدانية لتأثير الانترت على عينة من الشباب بالجزائر العاصمة بعنوان: **الجريمة الإلكترونية والشباب في الجزائر.**

عبارة عن أطروحة لنيل شهادة دكتوراه علوم في علم الاجتماع التربوي 2015-2016

إشكالية الدراسة:

ما هي أسباب إنتشار الجريمة الإلكترونية في أوساط الشباب عبر شبكة الانترنت ؟

أهداف الدراسة:

- التعرف على الجرائم الإلكترونية التي تنتشر بين الشباب عبر شبكة الانترنت .
- لسد ثغرة في الدراسات الإجتماعية في مجال إستخدام التكنولوجيا والشباب.

المنهج: المنهج الوصفي التحليلي والمنهج الإحصائي.

الاداة: الملاحظة، الإستمارة، المقابلة .

نتائج الدراسة: توصلت الباحثة الى:

ان السبب الاول لكثرة الجرائم الإلكترونية يعود الى قلة الرقابة والتوعية من طرف الأسرة والمؤسسات التعليمية .

السبب الثاني يعود الى ضعف القيم الدينية والإجتماعية عند فئة الشباب .

حدود الاستفادة منها: ركزت الدراسة على أسباب إنتشار الجريمة الإلكترونية في اوساط الشباب الجزائري، هذا ما سيفيدنا في دراستنا خاصة وان عينة الدراسة أو مجتمع بحثنا متعلق بطلبة جامعة يحي فارس قسم علوم الإعلام والإتصال المستخدمين لموقع الفيسبوك ومخاطر الجريمة الإلكترونية.

الفصـل الأول

مدخل عام للفضاء السيـبرانـي

تمهيد

- 🕮 المبحث الأول: مفهوم الفضاء السيبراني .
- 🕮 المبحث الثاني: خصائص الفضاء السيبراني .
- 🕮 المبحث الثالث: أنواع الفضاء السيبراني .
- 🕮 المبحث الرابع: مخاطر الفضاء السيبراني .
- 🕮 المبحث الخامس: سبل ردع الهجمات السيبرانية .

خلاصة الفصل

تمهيد:

تعد الثورة الرقمية التي نعيشها في الوقت الراهن خطوة كبيرة غيرت من نمط حياتنا وطريقة تفاعلنا مع من حولنا في العالم، إذ يشكل الفضاء السيبراني جزءا من هذه الثورة بحيث يمثل المجال الإفتراضي الذي يجمع بين الأنظمة الحاسوبية والشبكات، البيانات، إضافة إلى البرمجيات .حيث يعتبر فهم الفضاء السيبراني وما يخلفه من أثر في مجتمعنا عامة وحياتنا اليومية خاصة أمر بالغ الأهمية في ظل تزايد إستخدام التكنولوجيا الرقمية في مختلف جوانب الحياة.

سنتطرق من خلال هذا الفصل الذي جاء تحت عنوان مدخل عام للفضاء السيبراني إقتباس جزء بسيط من الدراسات لإعطاء نظرة شاملة عن مفهوم الفضاء السيبراني، خصائصه، أنواع الهجمات السيبرانية وإستراتيجيات الردع لها، ومخاطر هذا الفضاء.

1) مفهوم الفضاء السيبراني:

تعريف الفضاء:

لغة: مصدر مأخوذ من الفعل الثلاثي (فضا، يفضو، فضوا، فهو فاض) والفضاء هو المكان الواسع والفضاء الخارجي الفارغ الواسع من الأرض، يقال: أفضيت إذ خرجت إلى الفضاء .

إصطلاحا: هو كل ما يقع خلف الغلاف الجوي للأرض، أو هو كل ما يقع في الإرتفاع حوالي (1000كم) فوق سطح البحر، فهو يضم سائر الأجرام السماوية في الكون بما فيها الشمس والقمر والمذنبات .[1]

تعريف السيبرانية:

لغة: مشتقة من كلمة سيبرنتيك أو كيبرنتيك وهي مفردة مشتقة من اللغة الإغريقية القديمة من كيبرنتسين أي القائد أو قائد السفينة كما قد تكون مشتقة من كيبرنتيكا أي فن قيادة السفن .[2]

إصطلاحا: أصل المصطلح " السيبرنتيك " وهو مصطلح له أصل يوناني قديم في بداية كان يعني إدارة القوارب، وبعد القرن التاسع عشر إستعمله العالم الفرنسي الشهير " أمبير " لتعبير عن علم خاص للإدارة الإجتماعية السياسية .[3]

الفضاء السيبراني: بالرجوع إلى عام **1982**، وهو تاريخ ظهور هذا المصطلح .صياغ كاتب الخيال العلمي "ويليام جيبسون " William Gibson تصورا غريبا، هلوسة جماعية يشترك فيها مليارات المشغلين يوميا، في كل دولة كتمثيل للبيانات المستخلصة من بنوك المعلومات في جميع أجهزة الكمبيوتر في العالم .

---

[1] عبد الله عبد الطائي، عبيد: أحكام الفضاء في الفقه الإسلامي، بيروت، دار الكتب العلمية، د ت، ص14.

[2] د م، سيبر نتيك، على الموقع: https: //m.marefa.org تم الإطلاع يوم: 24-2-2024، 21: 20 سا .

[3] م يانكوف، ل يوتوفا، السيبر نتيك والإعلام، ترجمة: (برهان العلى)، بيروت، دار الطليعة، ط 1، 1979، ص07.

ولتسمية هذه الفكرة جمع جيبسون كلمة cybernetics (التي تعني علم التحكم الآلي) مع كلمة الفضاء space، لتصبح الفضاء السيبراني cyber space الذي أصبح حقيقة مع إنتشار شبكة الانترنت على نطاق العالم .[1]

فالفضاء السيبراني cyber space إذن مصطلح حديث، ظهر نتيجة لثورة تكنولوجيا المعلومات ويشمل جميع الحواسيب والمعلومات التي بداخلها والأنظمة والبرامج والشبكات المفتوحة لإستعمال الجمهور العام أو تلك الشبكات التي صممت لإستعمال فئة محددة من المستعملين ومنفصلة عن شبكة الانترنت العامة .[2] فالفضاء السيبراني هو العالم المادي والمفاهيمي الذي توجد فيه جميع هذه الأنظمة .[3]

ويتكون الفضاء السيبراني من:

1) المكون الأول: الطبيعي أو المادي وهو الذي يتمثل في الأسلاك والمحولات والبنية التحتية كالكبلات.
2) المكون الثاني: يتمثل في المحتوى الذي يعكس شكل المعرفة في عالم الفضاء السيبراني .
3) المكون الثالث: يتمثل في عملية التوصيل بين المعلومات والبشر وحركة التفاعل ما بين البرمجيات والمعدات، والإرتباط بتصورات وقيم وسلوك المستخدمين، كما أصبحت المعلومات لها قيمة إقتصادية وقيمة ميدانية بالنسبة إلى الجهات وكلما زادت فعالية إدارة تلك المعلومات زادت الفائدة التي يمكن الحصول عليها وأصبح تفوق المعلومات إحدى القيم الأساسية للقوة العسكرية وأصبحت المعلومات مجالا للسيطرة والتحكم، ويتعلق ذلك بعمليات المعلومات التي تشير للبيئة التي يمكن من خلالها شن عمليات الهجوم والدفاع والتي تكون متصلة ومستخدمة عبر الشبكات .[4]

---

[1] بيتر سينجر، دروس الحروب الماضية واللإتجاهات التكنولوجية المستقبلية، الحروب المستقبلية في القرن الحادي والعشرين، ط 1، مركز الإمارات للدراسات والبحوث الإستراتيجية، 2014، ص83.

[2] محمود محارب: إسرائيل والحرب الإلكترونية، قراءة في كتاب حرب الفضاء الإلكتروني، إتجاهات وتأثيرات على إسرائيل، سلسلة مراجعة كتب صادرة عن المركز العربي للأبحاث ودراسة السياسات، 2011، ص01.

[3] حمدون توريه: الفضاء السيبراني وتهديد الحرب السيبرانية، البحث عن السلام السيبراني، الإتحاد الدولي للإتصالات، جانفي2011، ص 9-12.

[4] عادل عبد الصادق: الفضاء الإلكتروني وتهديدات جديدة للأمن القومي، ص03.

2) خصائص الفضاء السيبراني:

الفضاء السيبراني هو مجال إفتراضي يعتمد على أنظمة الكمبيوتر وشبكات الانترنت ومخزون كبير من البيانات والمعلومات، حيث يمكن الإتصال بهذا المجال دون قيود جغرافية . وينفرد الفضاء السيبراني بمجموعة من الخصائص التي تميزه عن البر، البحر، الجو والفضاء ويمكن إجمال هذه الخصائص فيما يلي:

- **المجال الكهرومغناطيسي:** فبدون هذا المجال تفقد تكنولوجيا المعلومات والإتصالات (HCT) القدرة على العمل.
- **توفر البدائل:** في الفضاء السيبراني تتوفر البدائل بإستمرار على عكس الجو، البحر، الفضاء والذي يوجد فيه ميدان واحد، ففي ميدان الجو مثلا يحسم الأمر بتدمير طائرة العدو، في حين أن في الفضاء السيبراني عند إغلاق مواقع الأشخاص مثلا تبقى أمال هؤلاء إمكانية فتح موقع جديد بإسم مختلف في ساعات قليلة.
- سهولة إصلاح الشبكات وإعادة بنائها بفضل قلة تكلفة الأجهزة وتوفرها .
- **أسبقية الهجوم:** الهجوم في الفضاء السيبراني يحدث بسرعة، ومن الصعب تحديد مصدره أو المسؤول عنه .[1]
- **الطبقات الأربعة:** يتكون الفضاء السيبراني من أربع طبقات، والسيطرة على إحداهما لا يعني السيطرة على بقية الطبقات، نعرض منها بإختصار ما يلي:

1) الطبقة المادية: وتتكون من الأجهزة المادية كأجهزة الكمبيوتر والشبكات والأسلاك وأجهزة التوجيه (routers).و تقع هذه الأجهزة المادية ضمن ولاية السلطات القضائية وهو أمر مهم لإنفاذ القانون عندما يتم البحث عن الأجهزة المستخدمة للقيام بالجرائم السيبرانية .

2) طبقة المعلومات: تتضمن هذه الطبقة إنشاء معلومات وتوزيعها والتفاعل بين المستخدمين، ويمكن للمستخدمين إنشاء هذه المعلومات من خلال إنشاء مواقع الويب، والربط بمواقع ويب أخرى، ونشر المعلومات على مواقع التواصل الإجتماعي مثل Twitter أو Facebook.

[1] أنديرا عراجي: القوة في الفضاء السيبراني، فصل عصر من التحدي والإستجابة، رسالة لنيل دبلوم دراسات عليا في العلوم السياسية والإدارية، جامعة لبنان: كلية الحقوق والعلوم السياسية والإدارية، 2015-2016، ص18.

3) الطبقة المنطقية: وتمثل هذه الطبقة الجهاز العصبي المركزي للفضاء السيبراني، وهي مسؤولة عن توجيه حزم البيانات إلى وجهاتها النهائية، بشكل أساسي عبر أنظمة أسماء النطاقات (DNS)، وبروتوكولات الانترنت والمتصفحات ومواقع الويب والبرامج، كلها تعتمد على كابلات الألياف البصرية والأسس المادية .

4) طبقة الأشخاص: لا يعد الأشخاص مجرد مستخدمين سلبيين للفضاء السيبراني، فهم يحددون ويشكلون شخصيته بالطرق التي يختارونها لإستخدامه، فيعد الأشخاص وشخصياتهم والتي قد تختلف من مكان لآخر جزءا مهما من بنية الفضاء السيبراني .

- يستبدل الفضاء السيبراني مفهوم الوقتية شبه اللحظية بالتوقيتات التقليدية في إشارة لسرعة التي تتمتع بها الأنشطة الجارية في هذا الفضاء.
- يتجاوز قيود الجغرافيا والموقع المادي .
- يتجاوز الحدود التقليدية والسلطات القضائية، أي المفاهيم التقليدية لنظريات الحدود والسيادة الوطنية للدول القومية.
- يحجب هويات الفاعلين وروابط التعامل أو التعاطي فيما بينهم، وقد ساهمت هذه الخاصية في تعاظم دور الجرائم السيبرانية لما لها من أثر في مجريات التحقيقات الجنائية، إذ أن الوصول للجناة في هذا العالم يعد من الصعوبة وذلك على النطاقين الداخلي والدولي.
- يتجاوز آليات المسؤولية المعهودة من حيث تعيين الفاعل ونسبة الفعل إليه.[1]

[1] وليد مرزة حمزة المخزومي، ط محمد خزعل عباس: أمن الفضاء السيبراني، قراءة في المفهوم القانوني، مجلة العلوم القانونية، المجلد 37، الجزء الثاني، شباط 2023، ص 09-10.

3) أنواع الهجمات السيبرانية:

إن الهجمات السيبرانية تبدأعندما يتمكن المجرم الإلكتروني من إيقاع ضحيته في المصيدة بعد إقناعه أن المصدر أو الملف المرسل موثوق به، إذ يتم إرسالها على شكل بريد إلكتروني أو رسالة نصية، وحينما يتم إستقبال المتلقي للرسالة وينقر على الرابط يتم تثبيت برامج ضارة على جهازه أو تجميد النظام كجزء من هجوم برامج أو إختراق الخصوصية الخاصة به .

و يرى محمد فهمي بأن الهجمات الإلكترونية تشمل أشكال كثيرة من سرقة المعلومات، والتجسس، ونشر معلومات سرية وفضح الأنظمة السياسية لأغراض التحريض ونشر أفكاره مضادة .[1]

و عليه تأتي هذه الهجمات على الأشكال التالية:

1) **الإختراق:** هو القدرة على الوصول للبيانات والمعلومات الخاصة بشخص ما، فالهجمات هدفها الأساسي تغيير المعطيات أو محو معلومات، أو الهجمات الحرمان من الخدمة هذا النوع عموما سهل التنفيذ وعادة لايسبب إلا القليل من الضرر.

2) **حرب المعلومات الشخصية: (التجسس):** يقصد بالتجسس تلك الطرق لإختراق المواقع الإلكترونية ومن ثم سرقة بعض الكلمات والتي قد تكون في قائمة الأهمية والخطورة للطرف المتلقي والمسروق منه، وذلك بإستخدام أحصنة طروادة وبرامج التجسس بهدف سرقة المعلومات السرية التي يتم تأمينها بشكل صحيح يمكن أن يتم إعتراضها أيضا وقرصنتها .[2]

و يوصف هذا المستوى بأنه تجاوز لحدود الخصوصية الإلكترونية الفردية، مما يشكل إعتداء على الحقوق الشخصية للفرد، وإنتهاك لحرمة الحياة الخاصة، ومنها سرقة البيانات المالية ونشرها عبر الشبكة الإلكترونية للمعلومات أو لقيام أحد الأشخاص بتكوين ملف عن طريق الحاسب الآلي يحتوي على معلومات تخص شخصا آخر بغير علمه أو إذنه .[3]

---

[1] صلاح حيدر عبد الواحد: حروب الفضاء الإلكتروني، دراسة في مفهومها وخصائصها وسبل مواجهتها، رسالة مقدمة للحصول على درجة الماجستر في العلوم السياسية، كلية الآداب والعلوم، جامعة الشرق الأوسط، 2021، ص23.

[2] محمد الصغير كاوجة: الهجمات السيبرانية بين الواقع وسبل المواجهة، مجلة الرسالة للدراسات الإعلامية، مجلد 06، العدد03، سبتمبر2022، ص 111-112.

[3] طلال ياسين العيسى، عدي محمد عناب: المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث والدراسات الإنسانية، المجلد 19، العدد1، 2019، ص85.

3)**سرقة كلمات المرور والتسلل لنظام:** وتتمثل في التخمين والخداع والبرمجيات الخبيثة والنفاذ لملف تخزين كلمات المرور .

4)**هجمات رفض أداء الخدمة:** وهي هجمات إنكار الخدمة "هجمات دوس (DDOS) تستخدم لزيادة التحميل على الانترنت مما يؤدي للضغط على الشبكات ويمنع المستخدمين من الوصول للمنتجات والخدمات .[1]

4) مخاطر الفضاء السيبراني:

أحدث الفضاء السيبراني تغيرات في مفاهيم العلاقات الدولية، كمفهوم القوة والصراع والحرب، حيث إنتشرت القوة بين الفاعلين الدوليين، وتحول الصراع من المادي إلى الإفتراضي، ما نتج عنه ظهور تهديدات جديدة تتزايد في الحجم والشدة .فكلما زاد التشابك والإعتماد، زادت التهديدات السيبرانية.

ويلاحظ أيضا أن التهديدات السيبرانية لا تستهدف الإضرار بالبشر بصورة مباشرة، فهي تؤثر في الأنظمة والشبكات والأجهزة التي يستخدمها الفرد، وتعتمد عليها الدول، ومن ثم تؤثر في أسلوب الحياة ذاتها بشكل يهدد أمن الدولة ككل.

فيمكن القول أن المخاطر الناشئة من الفضاء السيبراني تتسم بثلاث سمات رئيسية، هي:

- إتساع نطاق وتعدد مستوياتها.
- عدم إمكان إيقاف مخاطر تلك التهديدات كليا.
- تنوع المخاطر السيبرانية، سواء من حيث طبيعتها، أو مصدرها، فقد تشنها دول، أو منظمات إجرامية، أو أفراد، أو إرهابيون وغيرهم.

فطبيعة الفضاء السيبراني جعلت المخاطر الأمنية الناتجة عن التفاعل فيه مختلفة كليا عن التهديدات الأمنية التقليدية .ويعزز من هذا الإختلاف امتناع نطاق الفضاء السيبراني، حيث انه يتخطى الحواجز الجغرافية والمكانية، ومن ثم يجمع مختلف الفواعل الدولية، التي تمتلك مصالح ورؤى إستراتيجية متنوعة كما أن العولمة أصبحت من الأمور الحتمية وإعتماد الدول المتزايد على الأنظمة الإلكترونية لم

[1] سامي محمد بونيف، دور الإستراتيجيات الإستباقية في مواجهة الهجمات السيبرانية–الردع السيبراني نموذجا–، المجلة الجزائرية للحقوق والعلوم السياسية المجلد04، العدد07، جامعة أحمد بن يحي الونشريسي، 2019، ص124_125.

يعد أيضا ممكنا التراجع عنه، مايزيد من المخاطر التي قد تتعرض لها الفواعل نتيجة لهذا الإعتماد المتزايد.

كما أن معدلات التطور في الفضاء السيبراني مرتفعة، و من ثم يترتب على كل تطور ظهور نقاط ضعف جديدة تهدد أمن الدولة، أي أن الفضاء السيبراني يتسم بديناميكية متشابكة.

كما أن عدم القدرة على التأكد من هوية الفاعل الدولي القائم بالهجوم هو أحد أهم العوائق التي تواجه الدولة في التعامل مع التهديدات السيبرانية، وهو ما يختلف عن التهديدات التقليدية .و يتمثل التحدي الأكبر في الفضاء السيبراني في صعوبة إسناد الهجوم لفاعل بعينه، ما يمثل مصدر قوة للفواعل الدولية، حيث تتسم عملياتهم بالسرية وعدم قدرة التعرف على هويتهم، ومن ثم معاقبتهم أو رد الهجمات، خاصة إذا كان مصدرها أكثر من جهاز إلكتروني ومقدم للخدمة في أكثر من دولة.

بصفة عامة، تنقسم مخاطر الفضاء السيبراني التي تواجهها الدول إلى أنماط رئيسية، هي:

1) **هجمات الحرمان من الخدمة:** حيث يتم إطلاق حزمة كبيرة من الطلبات والمهمات على خوادم الضحية بصورة تفوق قدرة الخادم أو الجهاز على معالجتها والإستجابة لها، ما يؤدي إلى توقفه بصروة جزئية أو كلية، أو إبطاء عمله، ما يسبب ضررا للمستخدم النهائي . وهي تستعمل كثيرا ضد مواقع الانترنت أو البنوك أو المؤسسات، من أجل التأثير فيها، أو لدفع فدية مالية.

2) **إتلاف المعلومات أو تعديلها:** ويقصد بها الوصول إلى معلومات الضحية عبر شبكة الانترنت أو الشبكات الخاصة، والقيام بعملية تعديل البيانات المهمة دون أن يكتشف الضحية ذلك .فالبيانات تبقى موجودة، لكنها مضللة، ما قد يؤدي إلى نتائج كارثية، خاصة إذا كانت خططا عسكرية، أو مواعيد، أو خرائط سرية.

3) **التجسس على الشبكات:** و يقصد به الدخول غير المصرح، والتجسس على شبكات الخصم، دون تدمير أو تغيير في البيانات، يكون الهدف منه الحصول على معلومات قد تكون خططا عسكرية، أو أسرارا حربية، أو إقتصادية، أو مالية، أو سياسية، ما يؤثر سلبا في مهام الخصم .

4) **تدمير المعلومات:** ويتم في هذه الحالة مسح وتدمير كامل للأصول والمعلومات والبيانات الموجودة على الشبكة، يصطلح عليه "تهديد لسلامة المحتوى"، ويعنى به إحداث تغيير في البيانات سواء بالحذف أو التدمير من قبل أشخاص غير مخولين.

وعليه، فلم يقتصر إهتمام الدول بالأمن السيبراني على البعد التقني فحسب، بل تجاوزه إلى أبعاد أخرى، مثل الأبعاد الثقافية والإجتماعية والإقتصادية والعسكرية وغيرها، وهو ما عمل على دعم حقيقة أ الإستخدام غير السلمي للفضاء السيبراني يؤثر في الرخاء الإقتصادي والإستقرار الإجتماعي لجميع الدول التي أصبحت تعتمد على النية التحتية الكونية للمعلومات .

إضافة إلى أن تصاعد دور الفاعلين من غير الدول في العلاقات الدولية قد أثر بدوره في سيادة الدول، خاصة مع بروز دور الشركات التكنولوجية العابرة للحدود الدولية، وبروز أخطار القرصنة والجريمة السيبرانية والجماعات الإرهابية.

لقد أصبحت المصالح القومية التي ترتبط بالبنية التحتية الحيوية عرضة لخطر الهجوم، حيث جعل الفضاء السيبراني تلك المصالح مرتبطة ببعضها بعضا في بيئة عمل واحدة . ومن ثم، فإن أي هجوم على إحدى تلك المصالح يكون سببا في حدوث عدم توازن إستراتيجي، وتهديد خطير للأمن القومي، ما دفع العديد من الدول إلى إدخال الأمن السيبراني ضمن إستراتيجياتها للأمن القومي .

إن "ترسيم الخطوط الفاصلة بين الحرب والسلام يمكن أن يتآكل بسهولة في الفضاء السيبراني، فيمكن أن يتم إلحاق أضرار مهما تكن طبيعتها بالخصم، وذلك دون تجاوز الخط الفاصل بين الحرب والسلام بشكل رسمي .[1]

[1] حازم محمد خليل: إستغلال الفضاء السيبراني في الحروب غير التقليدية، دراسة في الوكالة السيبرانية والإرهاب السيبراني، المجلة العلمية لكلية الدراسات الإقتصادية والعلوم السياسية بجامعة الإسكندرية، العدد الخامس عشر، كلية الإقتصاد والعلوم السياسية جامعة القاهرة، يناير 2023، ص272-274.

5) سبل ردع الهجمات السيبرانية:

تتعدد سبل مواجهة الهجمات السيبرانية والتي من شأنها تفلدي مثل هذه الهجمات التي تنجر عنها مخاطرعديدة والتي يمكن تلخيصها على النحو التالي:

1) جدران الحماية: تعد من أقوى السبل الوقائية لمثل هذه الهجمات الحادة والخطرة التي تمس أنظمة الكمبيوتر والشبكات، والتي يعرف أيضا بتسمية "الجدران النارية " Firewallأما عن بداية هذه التقنية فقد ظهرت في أواخر عقد الثمانينات من القرن الماضي، وذلك إستجابة لعدد من الإختراقات لشبكة الانترنت المستجدة حينذاك، وقد ظهر منها عدة أجيال: الجيل الأول يعرف ب مرشحات العبوة (Packet Filters)و يقوم مبدأ علمه على فلترة (ترشيح) العبوة والتي تمثل الوحدة الأساسية المخصصة لنقل البيانات بين الحواسيب على الانترنت فإذا كانت العبوة تطابق مجموعة شروط الجدار، فإنه يسمح بمرور العبوة، أو يرفضها ويتخلص منها .

2) التطبيقات المضادة للفيروسات: مضاد الفيروسات هو برنامج يتم إستخدامه لإكتشاف البرمجيات الضارة ومنعها من إلحاق الضرر بالحاسوب أو سرقة البيانات الشخصية، وذلك عن طريق إزالتها أو إجراء التعديلات عليها وإصلاحها، بحيث يمكن لهذا البرنامج أن يتصدى لبرنامج التجسس وبرامج أحصنة طروادة .

3) أنظمة كشف التسلل: كما تتألف أنظمة التسلل من عدة مكونات هي: جهاز استشعار ينبه على وقوع الأحداث ولوحة تحكم لمراقبة الأحداث والتنبيهات والتحكم بأجهزة الإستشعار، ومحرك يقوم بتسجيل إدخالات الأحداث المتلقاة من خلال أجهزة الإستشعار في قاعدة البيانات، وتكون أنظمة كشف التسلل مصنفة بالإعتماد على نوع وموقع أجهزة الإستشعار والمنهجيات المستخدمة على المحرك.[1]

4) الإستعانة بجدار حماية قوي بإمكانه التصدي لهذا النوع من الهجمات الخطرة.

5) الإستمرار في تحديث البرامج والتطبيقات الخاصة بمكافحة الفيروسات .

6) إستخدام شبكة إفتراضية خاصة .

7) الإعتماد على كلمات مرور قوية وغير المألوفة.

8) عدم فتح المرفقات والروابط الصادرة من جهات غير الموثوقة أو عن جهات مجهولة .

[1] صلاح حيدر عبد الواحد، مرجع سبق ذكره، ص59-60.

9) تجنب إستخدام أو تنزيل البرامج او الملفات في جهاز الكمبيوتر الخاص بك دون تأكد من مصداقيتها .[1]

[1] محمد الصغير كاوجة، مرجع سبق ذكره، ص116.

خاتمة الفصل:

يعتبر الفضاء السيبراني بيئة حيوية تشهد نموا متسارعا، وهو مجال شديد التطور والتعقيد، إذ أنه أعطى مفهوما جديدا للزمان والمكان، يؤثر بشكل كبير على حياة الأفراد والمجتمعات والدول سواء بالإيجاب أو السلب، إذ يجب تعزيز التوعية بمخاطر الفضاء السيبراني والتي تتمثل في الإختراق وسرقة المعلومات الشخصية والبيانات وإنتهاك خصوصية الآخرين، هذا ما إستدعى خلق إستراتيجيات وسبل ردع لهذه المخاطر، من خلال تبني سلوكيات سيبرانية آمنة ومسؤولة مثل تأمين أجهزتنا وحساباتنا الإلكترونية والإبتعاد عن المواقع والأنشطة الخطيرة عبر الأنترنت.

الفـــصـل الثـانـي

الجريمةالإلكترونية:المفهوم،الخصائص الأنواع والأهداف

تمهيد

- 🕮 المبحث الأول: مفهوم الجريمة الإلكترونية.
- 🕮 المبحث الثاني: خصائص الجريمة الإلكترونية.
- 🕮 المبحث الثالث: أنواع الجريمة الالكترونية .
- 🕮 المبحث الرابع: أهداف الجريمة الإلكترونية .
- 🕮 المبحث الخامس: سبل مكافحة الجريمة الإلكترونية والتشريعات القانونية.

خلاصة الفصل

تمهيد:

في عصرنا الرقمي وخاصة بعد تطور تكنولوجيا المعلومات تعد الجريمة الإلكترونية ظاهرة عالمية ذات أبعاد علمية وتقنية وتشريعية وإجتماعية وإقتصادية، أصبحت تمثل تحديا كبيرا للأفراد والشركات والمجتمعات والدول وتهدد أمنهم وسلامتهم وإستقرارهم . مما دفع معظم الدول للإجتهاد ومحاولة إيجاد حلول للحد من إنتشارها على الصعيد الأمني والعسكري خصوصا العلمي . وبدورنا نحن كباحثين سنحاول من خلال دراستنا تفسيرها والوصول الى نتائج من شأنها التقليل منها .

سنتطرق من خلال هذا الفصل الذي جاء تحت عنوان الجريمة الإلكترونية إقتباس جزء بسيط من الدراسات لإعطاء نظرة شاملة عن الجريمة الإلكترونية من تعريفات، خصائص، أنواعها، أهدافها والأهم من ذلك سبل مكافحتها والتشريعات القانونية الخاصة بها .

1) مفهوم الجريمة الإلكترونية:

من خلال هذا المبحث سأحاول التعرف إلى التعاريف المختلفة للجريمة الإلكترونية:

الجرائم الإلكترونية: جرائم مستحدثة شكلت ثورة على نظم الجريمة المختلفة، وإن تشابهت مع الجريمة التقليدية من حيث الأركان العامة والخاصة وإحتياجها لجاني ومجني عليه والموضوع والوسيلة، إلا أنها اختلفت عنها من حيث الفاعل وميزاته وطبيعة السلوك الجرمي المتميز بخاصية فريدة ومسرح للجريمة ذي طابع معنوي، بالإضافة الى تشعب وتنوع أصنافها وعدم قدرة النصوص الجنائية العقابية التقليدية على الإحاطة بهذه الصورة الجديدة التي إبتكرها عقل الفاعل والتي لاتنسجم وقاعدة التكييف المعروفة، وقد إختلفت تسميات هذا النوع من الإجرام وتعددت تبعا لتطور المفهوم، حيث يمكن إرجاع سبب التباين في المفاهيم إالى نشأة، تاريخ وتطور تكنولوجيا المعلومات، إختلاف وتعدد هذه الجرائم وتباين وجهات النظر بين المختصين في مجال الإعلام والقانون وعلم الإجتماع والنفس وحتى بين التقنيين.[1]

من بين هذه التسميات نذكر: " جرائم إساءة إستخدام الكمبيوتر، جرائم إحتيال الكمبيوتر، الجرائم المرتبطة بالكمبيوتر، جرائم التقنية العالية، جرائم الهاكرز، الإحتيال المعلوماتي، الغش المعلوماتي، التعسف في إستعمال الحاسب الآلي، جرائم الانترنت، الجرائم السيبرانية، السيبر كرايم، الجريمة المعلوماتية.....الخ ".[2]

تعرف الجريمة الإلكترونية على انها: أي فعل ضار يأتيه المواطن عبر إستعماله الوسائط الإلكترونية مثل الحواسيب، أجهزة الموبايل، شبكات الإتصالات الهاتفية، شبكات نقل المعلومات، شبكة الأنترنت، أو الإستخدامات غير القانونية للبيانات الحاسوبية أو الإلكترونية.[3]

---

[1] جعفر حسن جاسم الطائي: جرائم تكنولوجيا المعلومات، دار البداية ناشرون وموزعون، الأردن، ط1، 2007، ص107.

[2] حسن بن أحمد الشهري: نحو قانون دولي موحد لمكافحة الجرائم المعلوماتية، مجلة دراسات وأبحاث، العدد1، جامعة الجلفة، 2009، ص192.

[3] د.عبد السلام محمد المايل، د.عادل محمد الشربحي، د.على قابوسة: الجريمة الإلكترونية في الفضاء الإلكتروني "المفهوم، الأسباب، سبل المكافحة مع التعرض لحالة ليبيا "، مجلة أفاق للبحوث والدراسات سداسية، دولية محكمة، االعدد4، المركز الجامعي ايليزي، 2019، ص245.

فهي كل جريمة تتم بوسيلة إلكترونية كالحاسوب مثلا، وذلك بإستخدام شبكات الانترنت من خلال غرف الدردشة، وإختراق البريد الإلكتروني ومختلف وسائل التواصل الإجتماعي، بهدف إلحاق الضرر لفرد أو مجموعة من الأفراد، وحتى لدولة من الدول تكون ضمن برنامج الإستهداف الحربي أو الإقتصادي

أو الإضرار بسمعتها أو العكس، ويبقى الهدف واحد، وهو الكشف عن قضايا مستتر عليها، أو نشر معلومات لفائدة طرف أو أطراف أخرى من باب التسريب.[1]

أما بالنسبة للتعريف القانوني للجريمة الإلكترونية فقد اصطلح المشرع الجزائري على تسميتها بمصطلح الجرائم المتصلة بكنولوجيا الإعلام والإتصال وعرفها بموجب أحكام **المادة 2** من القانون رقم **09-04**[2] على أنها: "جرائم المساس بأنظمة المعالجة الآلية للمعطيات المحددة في قانون العقوبات، وأي جريمة أخرى ترتكب أو يسهل إرتكابها عن طريق منظومة معلوماتية، أو نظام للإتصالات الإلكترونية."

وحسب المشرع الجزائري فإنه قد تتحقق الجريمة الإلكترونية بمجرد أن ترتكب الجريمة، أو يسهل إرتكابها عن طريق منظومة معلوماتية أو نظام الإتصالات الإلكترونية، مما يجعل هذا التعريف يشمل عدد كبير من الجرائم، كما أن التعريف تضمن تكرار كون أن مفهوم نظام الإتصالات الإلكترونية يندرج ضمن مصطلح المنظومة المعلوماتية.[3]

2) خصائص الجريمة الإلكترونية:

تتميز الجريمة الإلكترونية بخصائص تميزها عن الجريمة التقليدية نذكر منها:

1-جريمة عابرة للحدود: تتسمالجريمة الإلكترونية بالطابع الدولي، ذلك لأن الطابع العالمي لشبكة الانترنت جعل معظم دول العالم في حالة إتصال دائم على الخط، وبهذا فالجريمة الالكترونية لا تعترف بالحدود بين الدول لذلك وصفت بالجرائم العابرة للقارات، وهو ما يعني أن مسرح الجريمة لم يعد محلي بل

---

[1] سميرة بيطام: الجريمة الإلكترونية وتقنية الإجرام المستحدث، 3أكتوبر2015.
www.alukah.net، 04/202402/، 2 45. 2h

[2] القانون رقم 09-04، الصادر في 05أوت 2009، يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والإتصال ومكافختها، ج ر العدد47.

[3] سوير سفيان: جرائم المعلوماتية، مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام جامعة أبو بكر بلقايد، تلمسان، 2010-2011، ص من 14-16.

عالمي، مع عدم اشتراط تواجد الفاعليين على مسرح الجريمة اي عدم التواجد المادي للمجرم الإلكتروني في مكان الجريمة .[1]

2-جرائم صعبة الإثبات: تتم الجريمة الإلكترونية في بيئة غير تقليدية حيث تقع خارج إطار الواقع المادي الملموس لتقوم اركانها في بيئة التقنيات التكنولوجية الحديثة مما يجعل الأمور تزداد تعقيدا لدى سلطات الأمن وأجهزة التحقيق والملاحقة، ففي هذه البيئة تكون البيانات والمعلومات عبارة عن نبضات إلكترونية غير مرئية تنساب عبر النظام المعلوماتي مما يجعل امر طمس الدليل ومحوه كليا من قبل الفاعل أمرا في غاية السهولة. وتجدر الأشارة الى ان وسائل المعاينة وطرقها التقليدية لا تفلح غالبا في إثبات هذه الجرائم نظرا لطبيعتها الخاصة التي تختلف عن الجريمة التقليدية، فالاخيرة لها مسرح تجري عليه الأحداث مخلفة آثارا مادية تقوم عليها الادلة لكن فكرة مسرح الجريمة في هذا النوع من الجرائم يتضاءل دوره في الافصاح عن الحقائق المؤدية للادلة المطلوبة وذلك بسبب ان الجرائم الإلكترونية لا تخاف آثارا مادية حتى ان إكتشافها والتحقيق فيها يتم في الغالب بعد فترة طويلة نسبيا، الأمر الذي يعطي مجالا للجناة ان يغيروا او يتلفوا الآثار المادية ان وجدت مما يؤدي الى ولوج الشك في صحة الأدلة المستقاة من المعاينة، بالاضافة الى ذلك فان نقص الخبرة الفنية والتقنية لدى الشرطة وجهات الادعاء والقضاء يشكل عائقا أساسيا امام إثبات الجريمة الإلكترونية ذلك ان هذا النوع من الإجرام يتطلب تأهيل وتدريب هذه الجهات في مجال تقنية المعلومات وكيفية جمع الأدلة والتفتيش والملاحقة في بيئة التقنيات التكنولوجيا الحديثة.[2]

3-جرائم سهلة الإرتكاب: تتميز هذه الجرائم بأنها جرائم ناعمة أو كما يطلق عليها الفقه "جرائم ذوي الياقات البيضاء" كناية على أنها لا تحتاج الى أدنى مجهود عضلي او الى سلوكيات مادية فيزيائية لتحقيق النتيجة فيها، طالما توافرت لدى الفاعل التقنية اللازمة والوسيلة المناسبة .[3]

4- جرائم صعبة الإكتشاف: تتميز الجريمة الإلكترونية بصعوبة إكتشافها واذا اكتشفت فإن ذلك يكون بمحض الصدفة عادة، حيث انه من الواضح ان عدد الحالات التي تم فيها استكشاف هذه الجرائم قليلة

---

[1] خالد ممدوح إبراهيم: الجرائم المعلوماتية، دار الفكر الجامعي، مصر، 2009، ص77.

[2] نهلة عبد القادر المومني: الجرائم المعلوماتية، دار الثقافة للنشر والتوزيع، الاردن، ط1، 2008، ص56-57.

[3] جلال محمد الزعبي، أسامة أحمد المناعسة: جرائم تقنية المعلومات الالكترونية، دار الثقافة للنشر والتوزيع، الاردن، ط1، 2009، ص92.

اذا ما قورنت بما يتم اكتشافه من الجرائم التقليدية، ويمكن رد الأسباب التي تقف وراء الصعوبة في إكتشاف هذا النوع من الإجرام الى عدم ترك هذه الجريمة لاي أثر خارجي بصورة مرئية كما ان الجاني له القدرة على تدمير دليل الإدانة في أقل من ثانية مما يشكل عاملا إضافيا في صعوبة إكتشاف هذا النوع من الإجرام، حيث تصل أدلة الإدانة فيها الى حدود 20%.[1]

3) أنواع الجريمة الإلكترونية:

سنتناول في هذا المبحث أنواع الجريمة الإلكترونية مع التركيز على جريمة القرصنة الإلكترونية التي أصبحت تشكل تهديدا متزايدا على الطلبة الجامعيين خاصة:

1- القرصنة الإلكترونية:

⇦ مفهوم الهكرز أو التجسس:

بدأت كلمة hackers ككلمة تحمل معنى يختلف تماما عما تحمله هذه الايام، فقد بدأت كصفة تشير لعبقرية مبرمجي الكمبيوتر وقدرتهم على إبتكار انظمة وبرامج حاسوب أكثر سرعة، ومن أشهر من إكتسب هذه الصفة (دينيس ريتش) و(كين تومسون) اللذان صمما برامج اليونكس عام 1969.

أما الهكرز بالمفهوم السيء فلم يكن لهم وجود قبل عام 1981، وهو عام ظهور أول حاسوب شخصي من انتاج شركة IBM.

ذلك ان عملية القرصنة الإلكترونية كانت غاية في الصعوبة لعدة اسباب منها ان النسخ الأولي للحواسيب كانت ضخمة، وتحتاج الى غرف كبيرة ذات درجات حرارة ثابتة، اما انتهاك خصوصية الآخرين فكانت تأخذ اشكالا أخرى كالتلصص على هواتف الآخرين من خلال شركات الهواتف المحلية وتعمد تداخل الخطوط لإضفاء المزيد من المرح والتسلية على الامر، ناهيك عن التلصص على أسرار

[1] حسين صابر دويب: القوانين العربية وتشريعات تجريم الجرائم الإلكترونية وحماية المجتمع، المؤتمر السادس لجمعية المكتبات والمعلومات، السعودية، 06-07 أفريل 2010.

المنتهكين وأحيانا إبتزازهم، وقد حدث ذلك بإحدى الشركات المريكية الى فصل مجموعة الشباب العاملين وإستبدالهم بطاقم من الفتيات .[1]

- **الإختراق:** هو القدرة على الوصول لهدف معين والدخول على الأجهزة بطريقة غير مشروعة عن طريق ثغرات في نظام الحماية الخاص بها بهدف التطفل على خصوصيات الأخرين وإلحاق الضرر بهم.

ويطلق على المخترق مصطلح Hacker وحينما يتمكن المخترق من إحداث الاضرار كحذف ملفات أو تشغيل ملفات مؤذية او وضع او زراعة ملفات تجسسية (أحصنة طروادة) او فيروسات او أي نوع من هذه الأنواع فهو مخرب (Cracker).

ويتم الإختراق عن طريق معرفة الثغرات الموجودة في النظام والتي غالبا ما تكون في المنافذ او(Ports) الخاصة بالجهاز .ويمكن وصف هذه المنافذ بأها بوابات للكمبيوتر على الشبكة العالمية تسمح لها بالدخول .[2]

و يمكن تعريف القرصنة الإلكترونية على انها عملية إختراق لأجهزة الحاسوب او المواقع تتم عبر شبكة الانترنت غالبا لان أغلب حواسيب العالم مرتبطة عبر هذه الشبكة او حتى عبر شبكات داخلية يرتبط بها أكثر من جهاز حاسب ويقوم بهذه العملية شخص أو عدة أشخاص متمكنيين من إختراق برامج الحاسوب وطرق إدارتها أي انهم مبرمجون ذو مستوى عالي يستطيعون بواسطة برامج مساعدة إختراق حاسوب معين للتعرف على محتوياته ومن خلالها يتم إختراق باقي الأجهزة المرتبطة معها في نفس الشبكة.[3]

- **أسباب جريمة القرصنة الإلكترونية:** تتشارك جريمة القرصنة الإلكترونية مع الجريمة المعلوماتية في أغلب الاسباب بطبيعة الحال لانها صورة من صورها من بين هذه الاسباب نذكر:

---

[1] بشرى حسين الحمداني: القرصنة الإلكترونية أسلحة الحرب الحديثة، دار أسامة للنشر والتوزيع، الأردن –عمان، ط1، 2014، ص12.

[2] بشرى حسين الحمداني: ، مرجع سبق ذكره، ص13.

[3] عبابسة فاروق، عبوب خديجة: القرصنة الإلكترونية وأثرها على المستخدم، مذكرة لنيل شهادة الماستر تخصص إعلام وإتصال، جامعة عبد الحميد ابن باديس مستغانم، 2016/2015، ص43.

الدوافع الشخصية: حيث ان الدافع لارتكاب جرائم الكمبيوتر يغلب عليه الرغبة في قهر الناس اكثر من شهوة الحصول على الربح، ويميل مرتكبوا جرائم نظم المعلومات الى إظهار تفوقهم ومستوى ارتقاء براعتهم لدرجة انه إزاء ظهور اي تقنية مستحدثة فإن مرتكبوا هذه الجرائم لديهم شغف الآلة يحاولون إيجاد الوسيلة الى تحطيمها بل والتفوق عليها، فقد اثبتت إحدى الدراسات ان القراصنة يتملكهم جميعا شعور البحث عن القوة ويؤدي ارتكابهم للجرائم بواسطة الكمبيوتر الى تعويضهم عن الحساس بالدونية.[1]

حب التعلم: يعتبر حب التعلم والإستطلاع من الأسباب الرئيسية التي تدفع لإرتكاب مثل هذه الجرائم لان المخترق يعتقد ان اجهزة الحاسوب والانظمة هي ملك للجميع ويجب ان لا تبقى في المعلومات حكرا على احد اي ان للجميع الحق بالتعرف والاستفادة من هذه المعلومات.

التسلية واللهو: عدد غير قليل من مخترقي الانظمة يعتبرون من عملهم هذا وسيلة للمرح والتسلية وتقضية اكبر وقت ممكن في مواقع وحواسيب آخرين ويكون هذا الإختراق غالبا سلبيا يحدث تاثيرا على المستخدم.[2]

- **أهم طرق اختراق الحاسوب:** تتم أغلب عمليات الإختراق عن طريق زرع برنامج معين في جهاز الضحية، يقوم هذا البرنامج بعمل معين كما يلي:

1) **الفيروسات:** هو برنامج له القدرة على نسخ نفسه اكثر من مرة ويمتاز بقدرته على التخفي وله آثار تدميرية على أنظمة تشغيل الحاسوب لان عملية النسخ والتكرار الدائم لملفاته تجعل هاته الملفات تحل محلات الملفات الأصلية الموجودة على القرص الصلب للحاسوب.

2) **أحصنة طروادة:** هو برنامج تجسسي بعمل معين يحدده الشخص الذي صممه أو زرعه في جهاز الضحية يمكنه من الحصول على مبتغاه.

3) **الديدان:** هو برنامج ينتقل غالبا عبر البريد الالكتروني ويمتاز بقدرته على التنقل عبر شبكات الانترنت لغرض تعطيلها او التشويش عليها عن طريق شل قدرتها على تبادل المعلومات .

4) **القنبلة المعلوماتية:** information Bomb: هو برنامج يصنعه مصمم النظام بنفسه لغرض انهاء مدة عمل ذلك النظام خلال وقت معين، او في حال إستخدام أرقام او أحرف معينة يحددها المصمم.

---

[1] رابحي لخضر، بن بعلاش خاليدة: هعالجة الجرائم المعلوماتية في ظل التعاون الدولي والإستجابة الدولية، الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية والمكافحة، 16-2015/11/17، جامعة محمد خيضر، ص4.

[2] بشرى حسين الحمداني: مرجع سبق ذكره، ص69-70.

5) **الفخ: Trappe:** هو منفذ يتركه مصمم البرنامج يسهل له عملية الدخول اليه وقت مايشاء وإجراء التعديلات التي يريدها.[1]

2- جرائم الإعتداء على الأشخاص: المقصود بالإعتداء هذا هو السب والقذف والتشهير وبث أفكار وأخبار من شأنها الإضرار الأدبي او المعنوي بالشخص او الجهة المقصودة من خلال الحاسب الآلي. هذا وتتنوع طرق الإعتداء بداية من الدخول على الموقع الشخصي للشخص المشهر به وتغيير محتوياته والذي يندرج تحت الجرائم التي تتم ضد الحواسيب والشبكات او عمل موقع آخر يتم نشر اخبار ومعلومات غير صحيحة والذي يندرج تحت الجرائم بإستخدام الحواسب الآلية والشبكات والذي غالبا ما يتم من خلال إحدى مواقع الإستضافة المجانية لصفحات الانترنت والتي اصبح عددها بالآلاف في آفة الدول المتصلة بالانترنت.[2]

3- جريمة الإبتزاز الإلكتروني:

- **مفهوم الإبتزاز:** هو تلك الأفعال التي تدفع بالفرد إلى التهديد بكشف معلومات معينة عن شخص، أو فعل شيء ليؤذي الشخص المهدد، إن لم يقم الشخص المهدد بالإستجابة إلي بعض الطلبات، كما يمكن أن تكون هذه المعلومات عادة محرجة أو ذات طبيعة مدمرة اجتماعيا، وهو بمعنى الحصول على أهداف غير مشروعة بإتباع وسائل غير مشروعة أيضا، وغالبا مايكون هذا الهدف أو هذه الأهداف ذات بعد مؤثر سلبي للحياة الإجتماعية، وقد يستخدم الإبتزاز في أي وظيفة مهما كان نوعها للتأثير على الشخص الذي يكون عرضة لهذا الفعل لتحقيق مكاسب نوعية وغبر مشروعة.
- **مفهوم الإبتزاز الإلكتروني:** هو كل فعل يقوم به الفرد بإستعمال تقنيات عالية الدقة في الإعلام الآلي وبإستخدام شبكة الانترنت وكذا البرامج التي تتيح للفرد محو آثاره بعدما يقوم بعملية الإبتزاز من أجل تحقيق غاية معينة، حيث نشير هنا إلى إختلاف الغايات بإختلاف الأفراد وبإختلاف العوامل التي قد يتعرض لها هؤلاء الأفراد.

---

[1] عبابسة فاروق، عبوب خديجة: مرجع سبة ذكره.

[2] محمد علي قطب: الجرائم المعلوماتية وطرق مواجهتها، جزء2، الأكاديمية الملكية للشرطة، مملكة البحرين، 2010، ص7.

أشكال الإبتزاز الإلكتروني:

1. إبتزاز إلكتروني عاطفي: نقصد به تلك الأفعال التي يقوم به المبتز الذي لديه معلومات كافية عن الشخص المراد إبتزازه عاطفيا من أجل تحقيق هدف معين، هذا الهدف قد حدده المبتز من أول لقاء بينه وبينضحيته وبالتالي تحديد الطرق الكفيلة بإيقاع الضحية لهذا الفخ، ثم المضي قدما في تحقيق ما حدده سابقا مع توخي أقصى درجات الحيطة والحذر.

2. إبتزاز إلكتروني مادي: و الغرض منه تحقيق المنفعة المادية أي الربح المادي أو نيل المبالغ المالية عن طريق إيهام الضحية بفضح بعض الحقائق الشخصية المتعلقة به مثل تركيب الصورة الشخصية للضحية بإستخدام برامج تحسين وتعديل الصور بصورة إباحية أو في أوضاع مخلة بالحياء وبالتالي الناتج من ذلك التهديد يؤدي بالضحية للإنصياع والرضوخ لمطالب المجرم المبتز الذي يقوم بطلب مستمر للمبالغ المالية وفي حالة إعلان الرفض من طرف الضحية سيكون هناك التهديد بنشر هذه الصور والحقائق زورا وبهتانا على مستوى شبكات التواصل وعلى مستوى المواقع التي تكون الضحية مشتركة فيها.[1]

4- الجرائم الإباحية الإلكترونية: تعد الجرائم الإباحية الإلكترونية إحدى اهم واكثر الجرائم تاثيرا على الأشخاص والمجتمعات لما لها من اثر مادي ومعنوي يمس شخوص المجني عليهم اوقيمهم او أعراضهم، بالإضافة للاثر السلبي المترتب على المجتمع ان لم تعالج هذه المعضلة بصورة قانونية واقية.

و تتمثل الجريمة الإلكترونية الإباحية بإرسال او نشر عمل إيباحي او تمثل بإعداد او حفظ او معالجة او عرض او طباعة او نشر او ترويج انشطة او اعمال إباحية او اتصال بالدعارة او الأعمال الإباحية، والذي تم بصورة قصدية بواسطة إستخدام نظام معلومات أو الشبكة المعلوماتية او ما يماثلها من الوسائل الإلكترونية.[2]

[1] سعيد زيوش، "ظاهرة الإبتزاز الإلكتروني وأساليب الوقاية منها –قراءة سوسيولوجية وأراء نظرية–"، مجلة العلوم الإجتماعية، العدد22، جامعة الشلف، الجزائر، 2017، ص71-72-73.

[2] أحمد محمد اللوزي، محمد عبد المجيد الذنيبات: الجريمة الإباحية الإلكترونية كما نظمها قانون الجرائم انظمة المعلومات الكويتي، دراسات علوم الشريعة والقانون، المجلد42، العدد3، 2014، ص835.

4) أهداف الجريمة الإلكترونية:

- الوصول الى المعلومات بشكل غير قانوني، كسرقة المعلومات أو الإطلاع عليها أو حذفها أو تعديلها بما يحقق هدف المجرم .
- الوصول إلى الأجهزة الخادمة الموفرة للمعلومات وتعطيلها أو تخريبها وعادة ما تتم هذه العملية على مواقع الانترنت.
- الحصول على معلومات تغيير عناوين مواقع الانترنت بهدف التخريب على المؤسسات العامة وإبتزازها.
- للوصول الى الأشخاص أو الجهات المستخدمة للتكنولوجيا بغرض التهديد أو الإبتزاز كالبنوك أو الدوائر الحكومية والأجهزة الرسمية بكافة أشكالها.
- الإستفادة من تقنية المعلومات من أجل كسب مادي او معنوي او سياسي غير مشروع كعمليات تزوير بطاقات الإئتمان وعمليات إختراق المواقع الإلكترونية على الشبكة العنكبوتية.
- إستخدام التكنولوجيا في دعم الإرهاب والأفكار المتطرفة أو نشر الأفكار التي يمكن ان تؤسس الى الفكر تكفيري.[1]

5) سبل مكافحة الجريمة الإلكترونية والتشريعات القانونية :

توجد سبل متنوعة لمكافحة الجريمة الإلكترونية، حيث تتباين هذه السبل بدرجة فاعليتها وتعقيدهاوذلك حسب البرامج المصصمة لهذا الغرض ومن بين هذه السبل:

- عمل نسخ من ملفات البيانات Backups.
- إستخدام 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 المستخدم إذن الخروج الى عالم الانترنت ولكن لايستطيع من في الخارج الدخول الى الجهاز من خلاله.

[1] محمد شاكر السعيد، خالد بن عبد العزيز الحرفش: مفاهيم أمنية، ط1، جامعة نايف للعلوم الأمنية، الرياض، 2010، ص75.

- إستخدام الخصائص الفسيولوجية fingerprint، Biometrics لحماية النظام مثل بصمة الإبهام، حدقة العين، الصوت وغيرها . التشفير Encryption.

وتستخدم معظم نظم المعلومات الإدارية الشبكية برامج جدران النار، والبرامج المضادة للفيروسات بالإضافة الى التشفير Encryption لحماية الرسائل والملفات المخفية، وهناك تشفير بإستخدام المفتاح العام Public Key Encryption المعروف اختصارا باسم (PKE)وهو نظام تشفير يستخدم مفتاحين، مفتاح رئيس يمكن ان يستخدم او ان يحصل عليه أي شخص ومفتاح خاص Private Key للشخص المستلم فقط.[1]

التشريعات القانونية لمكافحة الجريمة الإلكترونية:

1) الجرائم الإلكترونية في الشريعة الإسلامية: من المسلم به ان الشريعة الإسلامية شريعة عامة لكل زمان ومكان، وان الناس مختلفون في ضبط نفوسهم، فلا بد من وجود عقاب رادع يضبط اصحاب النفوس الضعيفة من الوقع في الجرائم حتى يسلم المجتمع من الفساد ظاهرا وباطنا من أجل الك حاربت الشريعة الإسلامية الجرائم بشتى صورها، لان شريعة الإسلام تفترض ان الإنسان يجب ان يعيش من طريق شريف، وان يحيا على ثمرات كفاحه وجهده الخاص. والشريعة الإسلامية لا تجعل أي فعل من الأفعال جريمة إلا ما فبه ضرر محقق للفرد والجماعة، ويظهر هذا الضرر فيما يمس الدين، أو العرض، أو النفس، أو النسل، أو المال، أو العقل، وهذه الكليات مقصد مهم من مقاصد الشريعة الإسلامية التي شرعت من أجل الحفاظ عليها.[2]

و قد تميزت الشريعة الإسلامية بمنهجها الفريد في مكافحة الجريمة واستئصالها من جذورها من خلال خطتين متلازمين ومتوازيين وهما:

أولا: الجانب الوقائي: ومن أهم ملامحه إصلاح الجاني، وفتح ابواب التوبة أمامه على مصراعيها، وعدم تيئيسه من رحمة الله، وحثه على الإقلاع والندم، وعدم التمادي في الباطل، فالشريعة بداهة تكره

[1] عبد السلام محمد المايل، عادل محمد الشربجي، مرجع سبق ذكره، ص251.

[2] إبراهيم رمضان إبراهيم عطايا: الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية والانظمة الدولية(دراسة تحليلية تطبيقية)، العدد 30، ج2، كلية الشريعة والقانون بطنطا، 2015، ص384.

الجريمة، وتتوعد عليها بالنكال في الدنيا والآخرة وتهدد اقواما يرتكبونها سرا ثم يبرزون للناس وكأنهم أطهار شرفاء.[1]

قال تعالى(وَلَا تُجَٰدِلْ عَنِ ٱلَّذِينَ يَخْتَانُونَ أَنفُسَهُمْ إِنَّ ٱللَّهَ لَا يُحِبُّ مَن كَانَ خَوَّانًا أَثِيمًا يَسْتَخْفُونَ مِنَ ٱلنَّاسِ وَلَا يَسْتَخْفُونَ مِنَ ٱللَّهِ وَهُوَ مَعَهُمْ إِذْ يُبَيِّتُونَ مَا لَا يَرْضَىٰ مِنَ ٱلْقَوْلِ وَكَانَ ٱللَّهُ بِمَا يَعْمَلُونَ مُحِيطًا)[2]

فدور الشريعة في الجانب الوقائي تجاه الجريمة لا يقتصر على وضع عقاب رادع للجاني فحسب، بل تتخذ كل الإجراءات والتدابير التي من شانها الحيلولة دون وقوع الجريمة، فالتربية الإسلامية المستمرة بالحكمة والموعظة الحسنة ثم التوعية المستمرة بالجريمة وأخطارها من كافة الجهات المعيشية، وأيضا سد الأبواب والمنافذ التي تؤدي الى إقتراف الجريمة.

ثانيا: الجانب العلاجي:

وهذا الجانب يلي الجانب الوقائي في مواجهة الجريمة بصفة عامة والجريمة الإلكترونية بصفة خاصة وبما أن الجريمة سلوك شاذ يهدد امن الافراد وإستقرار المجتمعات ويقوض أركان الدولة والبلاد فإن أحكام الشريعة الإسلامية الغراء بعدلها القويم ومبادئها الشاملة يدور حول صيانة الضرورات الأساسية التي لا يستطيع الإنسان ان يستغني عنها ويعيش بدونها، فوضغت العقوبات الشرعية الجازرة والأليمة لكل من يتعدى على هذه الضرورات الأساسية وينتهك حرمتها، فوضعت لكل جريمة من الجرائم العقوبات المناسبة للحد من إرتكاب هذه الجريمة، كل هذه الخطوات تؤدي الى مكافحة الجريمة وتقي المجتمع من أخطارها، وبذلك فقد تكلفت التشريعات الجنائية الإسلامية على عاتقها عبء مكافحة الجريمة والتصدي لها .

وهناك حقان ترعاهما الشريعة الإسلامية هما:

1. حق المخطىء في فرصة يتوب منها، ويستأنف ملكا أنظف.
2. حق المجتمع في صيانة كيانه من نزوات العصيان وتخبطه الذي يصيب الأبرياء والغافلين .

[1] محمد الغزالي: هذا ديننا، ط3، القاهرة، ص229.

[2] النساء 106-108.

إن مما لا شك فيه أن الشريعة الإسلامية أفردت لكل جريمة من الجرائم العقوبة التي تلائمها، ونصت على الضوابط والشروط والأحكام التي تخص كل جريمة وعقوبتها في الجرائم والعقوبات التقليدية، لكن في هذا العصر ظهرت جرائم كثيرة مرتبطة بالتقدم في جميع مجالات التقنية في مجال الحاسب الآليوالانترنت، فكان لزاما على المشتغلين بالفقه الإسلامي ان يتعرفوا على هذا النوع من الجرائم ويضعوا له العقوبات التي تناسبه .

لذلك اعتبرت الجرائم التقليدية كجريمة السرقة والقذف والنصب مثلها مثل الجرائم التي ارتكبت عن طريق الانترنت مثال عن ذلك السرقة بواسطة الانترنت بإستخدام بطاقات الائتمان المسروقة، حيث ان هذه البطاقات تعد مالا.

هذا اذا سهل على المتخصصين في العلوم الشرعية إلحاق وصف الجريمة الإلكترونية بوصف الجريمة التقليدية لإختلال شرط من الشروط مثلا، فان ميدان العقوبة التعزيرية ميدان واسع لمواجهة هذه الجريمة، يختار القاضي فيه ما هو مناسب وملائم لحال المجرم وجسمانة ضرره، وباعثه، و زمانه ومكانه.

فالعقوبات التعزيرية: عقوبات غير مقدرة تجب حقا لله أو لآدمي في كل معصية ليس فيها حد ولا كفارة.فهي كا لحدود في الزجر والتأديب للأمة، واذا كانت العقوبة التعزيرية غير مقدرة فللحاكم او القاضي ان يفرض العقوبة التي يراها مناسبة، فقد تكون توبيخا او ضربا وقد تكون حبسا، وقد تكون مصادرة على الا تبلغ حدا من الحدود عند جمهور الفقهاء، خلافا للحنفية والمالكية يرون ان العقوبة التعزيرية قد تصل في بعض الاحيان اللر القتل.[1]

2)الجريمة الإلكترونية في التشريع الجزائري: أصدر المشرع الجزائري مجموعة من التشريعات لمواجهة الجريمة الإلكترونية على إختلافها من ذلك نذكر:

المرسوم التنفيذي رقم 98-257 المؤرخ في 3 جمادى الأولى عام 1419هـ الموافق 25غشت سنة 1998م الضابط لشروط وكيفيات إقامة الخدمات "أنترنت"و إستغلالها: ألقى هذا المرسوم المسؤولية القانونية المباشرة على مزودي خدمة الانترنت بمقتضى **المادة 14**في ما يتعلق بالمضامين والمواد المنشورة والمواقع التي يقومون بإستضافتها مع الإلتزام بسرية كل المعلومات المتعلقة بحياة المشتركين

[1] إبراهيم رمضان إبراهيم عطايا: مرجع سبق ذكره، ص387-389.

الخاصة، وعدم الإدلاء بها إلا في الحالات المنصوص عليها في القانون، أي حالات الدفاع عن الامنوالنظام العام كما ألزمهم بضرورة إتخاذ كافة الإجراءات المطلوبة للتأكد من وجود رقابة دائمة على المحتوى لمنع الوصول الى المواد التي تتعارض مع الأخلاق أو النظام العام.[1]

القانون رقم 04-15المؤرخ في 27 رمضان عام 1425هـ الموافق 10 نوفمبر 2004م المعدل والمتمم للأمر 66-156المؤرخ في 18 صفر عام 1386هـ الموافق 8 يونيو سنة 1966م والمتضمن قانون العقوبات: تعتبر الخطوة البارزة التي خطاها المشرع الجزائري في مجال مكافحة الإجرام الإلكتروني تعديل قانون العقوبات لعام 2004 وتحديدا من خلال القسم السابع مكرر تحت عنوان " المساس بأنظمة المعالجة الآلية للمعطيات " يشمل المواد من 394مكرر إلى 394مكرر07.[2]

المرسوم الرئاسي رقم 06-473المؤرخ في 20ذي القعدة عام 1427هـ الموافق 11ديسمبر سنة 2006م المتضمن التصديق على الإتفاق بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الكنفدرالية السويسرية حول التعاون القضائي في المجال الجزائي: تهدف هذه الإتفاقية إلى تدعيم التعاون بين الجزائر وسويسرا في مجال مكافحة جميع أشكال الجريمة منها الجريمة الإلكترونية التي تعد أحد أنواعها ومتابعتها وقمعها والبحث عن أدلة الإثبات أو تسليم الملفات والمعلومات والوثائق .[3]

القرار الوزاري المشترك المؤرخ في 26 ربيع الاول عام 1428هـ الموافق 14 أفريل سنة 2007م المتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي:

---

[1] الجريدة الرسمية للجمهورية الجزائرية الديموقراطية الشعبية: مرسوم تنفيذي رقم 98-257مؤرخ في 03جمادى الأولى عام 1419هـ الموافق25أوت 1998م يضبط شروط وكيفيات إقامة خدمات "انترنت "و إستغلالها، العدد63، يوم 26أوت1998، ص08.

[2] الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية: قانون رقم 04-15مؤرخ في 27رمضان عام 1425هـ الموافق 10 نوفمبر 2004م يعدل ويتمم الأمر رقم 66-156المؤرخ في 18 صفر عام 1386هـ الموافق 08يونيو سنة 1966م والمتضمن قانون العقوبات، العدد71، يوم10نوفمبر 2004م، ص11.

[3] الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية: مرسوم رئاسي رقم 06-437مؤرخ في 20ذي القعدة عام 1427هـ الموافق 11ديسمبر سنة 2006م يتضمن التصديق على الاتفاق بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية وحكومة الكنفدرالية السويسرية حول التعاون القضائي في المجال الجزائي، العدد83، يوم20ديسمبر2006م، ص11.

بموجب المادة الخامسة من هذا القرار انشىء مخبر متخصص في الدلائل المعلوماتية وجرائم الكمبيوتر ومخبر لإستغلال الهواتف المحمولة في إطار مكافحة الجريمة الإلكترونية تقنيا.[1]

3)العقوبات الأصلية لجريمة القرصنة الإلكترونية: تعتبر عقوبة جرائم القرصنة الإلكترونية من العقوبات المشددة لان العقوبة فيها تكون مضاعفة عن العقوبة الأصلية:

أولا: عقوبة الشخص الطبيعي: يعاقب بالحبس من ثلالة اشهر الى سنة واحدة وبغرامة من 50.000دج ألى 100.000دج كل من يدخل او يبقى عن طريق الغش في كل جزء من منظومة للمعالجة الآلية للمعطيات او يحاول ذلك، تضاعف العقوبة اذا ترتب عن ذلك حذف او تغيير لمعطيات المنظومة.

و اذا ترتب عن ذلك الافعال المذكورة اعلاه تخريب نظام اشتغال المنظومة تكون العقوبة الحبس من ستة اشهر إلى سنتين والغرامة من 50.000الى 150.000دج.[2]

المادة تتضمن صور جريمة القرصنة الإلكترونية في الصورة المشددة لهذه الجريمة لانها تتضمن مضاعفة العقوبة وذلك عند حذف او تغيير لمعطيات المنظمة.

يعاقب بالحبس من ستة اشهر الى ثلاث سنوات وبغرامة من 5000.000دج الى 2.000.000دج كل من أدخل بطريق الغش المعطيات التي يتضمنها .[3]

ثانيا: عقوبة الشخص المعنوي: مبدأ مساءلة الشخص المعنوي وارد في **المادة 12** من إتفاقية بودابست، بحيث يسأل الشخص المعنوي عن هذه الجرائم سواء بصفته فاعلا أصليا او شريكا او متدخلا كما يسأل عن الجريمة التامة او المشروع فيها، كل ذلك بشرط أن تكون الجريمة قد ارتكبت لحساب الشخص المعنوي بواسطة أحد أعضائه او ممثليه.[4]

---

[1] الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية: قرار وزاري مشترك مؤرخ في 26ربيع الاول عام 1428هـ الموافق 14أفريل سنة 2007م، يتعلق بتنظيم الأقسام والمصالح والمخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي، العدد36، يوم 03جوان 2007م، ص16.

[2] المادة 394مكرر، ق ع ج.

[3] 394مكرر 1، نفسه.

[4] عطاء الله قشار: مواجهة الجريمة المعلوماتية في التشريع الجزائري، الملتقى المغاربي حول القانون والمعلوماتية، أكاديمية الدراسات العليا، ليبيا، أكتوبر 2009، ص25.

وقد نص المشرع الجزائري في **المادة 51** مكرر من قانون العقوبات الجزائري على مسائلة الشخص المعنوي وذلك وفق شروط:

1. أن ترتكب إحدى الجرائم المنصوص عليها قانونا.
2. أن تكون بواسطة أحد أعضاء او ممثلي الشخص المعنوي.
3. أن ترتكب الجريمة لحساب الشخص المعنوي.[1]

كما نص المشرع في **المادة 18** مكرر من نفس القانون على ان العقوبات التي تطبق على الشخص المعنوي في مواد الجنايات والجنح هي:

– الغرامة التي تساوي من مرة الى خمس مرات الحد الأقصى للغرامة المقررة للشخص الطبيعي في القانون الذي يعاقب على الجريمة.

و يعاقب الشخص المعنوي الذي يرتكب إحدى الجرائم المنصوص عليها في هذا القسم بغرامة تعادل خمس مرات الحد الاقصى للغرامة المقررة للشخص الطبيعي.[2]

ثالثا: عقوبة الإشتراك: خصص قانون العقوبات الجزائري لجريمة الإشتراك في الجرائم الماسة بأنظمة المعالجة الآلية للمعطيات التي نت بين شروطها الإتفاق الجنائي مادة معينة والتي جاء في نصها ما يلي: "كل من شارك في مجموعة او اتفاق تألف بغرض الإعداد لجريمة او أكثر من الجرائم المنصوص عليها في هذا القسم وكان هذا التحضير مجسدا بفعل أو عدة أفعال مادية، يعاقب بالعقوبات المقررة للجريمة ذاتها "[3]

رابعا: عقوبة الشروع: الشروع في الشيء هو البدء في القيام به والشروع في الجريمة ينصرف الى البدء في تنفيذها .[4]

---

[1] ختير مسعود: الحماية الجنائية لبرامج الكمبيوتر، أساليب وثغرات، دار الهدى للنشر والتوزيع، الجزائر، ط2010، ص 100-101.

[2] 394مكرر4، ق ع ج.

[3] المادة 394مكرر5، نفسه.

[4] علي حسن الشرفي: شرح الأحكام العامة للتشريع العقابي اليمني وفقا لمشروع القانون الشرعي للجرائم والعقوبات، دار المنار، القاهرة، 1993، ص254.

جاء في نص **المادة 30** من ق ع ج ما يلي: " كل محاولات لإرتكاب جناية تبتدىء بالشروع في التنفيذ او بافعال لا لبس فيها تؤدي مباشرة الى ارتكابها تعتبر كالجناية اذا لم تتوقف او لم يخب أثرها الا نتيجة لظروف مستقلة عن إرادة مرتكبها حتى لو لم يكن بلوغ الهدف المقصود بسبب ظرف مادي يجهله مرتكبها "

خاتمة الفصل:

وختاما من دراستنا لهذا الفصل يمكننا القول أن الجرائم المعلوماتية من أخطر الجرائم لصعوبة إكتشافها وإثباتها، وتنوع أهدافها وأساليبها .

مما جعل المشرع الجزائري يقوم بالإجراءات المناسبة للتصدي للجريمة المعلوماتية عامة، وجريمة القرصنة الإلكترونية خاصة، وذلك بتعديل القوانين وإستحداث قوانين جديدة لمكافحة هذا النوع من الإجرام.

الفـصـل الثـالث

المقـترب النـظري للدراسة

تمهيد

📖المبحث الأول: مفهوم نظرية الإستخدامات و الإشباعات.

📖المبحث الثاني: نشأة النظرية .

📖المبحث الثالث: فروض النظرية .

📖المبحث الرابع: أهداف النظرية .

📖المبحث الخامس: إنتقادات النظرية .

خلاصة الفصل

تمهيد:

تعتبر نظرية الإستخدامات والإشباعات نظرية تواصلية تركز على فهم الأسباب التي يستخدم بها الأفراد وسائل الإعلام والتكنولوجيا، وكيفية تلبية إحتياجاتهم ورغباتهم الشخصية بدلا من إعتبار الأفراد مجرد مستهلكين يتلقون المحتوى الإعلامي، كما تركز هذه النظرية على دور الفرد في إختيار إستخدامه وسائل الإعلام والتكنولوجيا وكيفية الإستفادة منها .

ولفهم النظرية أكثر سنتطرق من خلال هذا الفصل إلى بعض المفاهيم المتعلقة بنظرية الإستخدامات والإشباعات، تعريفها، النشأة، الأهداف، الفروض وإنتقادات النظرية الموجهة لها .

1) مفهوم نظرية الإستخدامات و الإشباعات:

الإستخدام: قد قام العديد من الباحثين عدة مفاهيم لمفهوم الإستخدام من بينهم " لوكواديك" الذي عرف الإستخدام على أنه "نشاط إجتماعي يتحول إلى نشاط عادي في المجتمع بفضل التكرار والقدم، وقد أصبح ضروريا من أجل سد حاجة وهي الحاجة إلى المعلومات . أما "La croix" هو الآخر إقترح تعريفا لمفهوم الإستخدام، حيث يقول: " أن الإستخدامات الإجتماعية هي أنماط إستخدام تظهر وتبرز بصورة منتظمة على نحو كاف، بحيث تشكل عادات في يوميات إستخدام تفرض نفسها في قائمة الممارسات الثقافية، القائمة مسبقا وتعيد إنتاج نفسها وربما مقاومة الممارسات الأخرى المنافسة لها أو المرتبطة بها " .[1]

الإشباع: عرفت الإشباعات على أنها حاجات ملحة تنوب الفرد لسد نقص إما داخلي أو خارجي [2].و في نظرية التحليل النفسي فالإشباع يعني خفض التنمية والتخلص من التوتر بعد الوصول وتحقيق المبتغى .[3]ووفقا لنظرية الإستخدامات والإشباعات يتم وصف أفراد الجمهور بإعتبارهم مدفوعين بمؤثرات نفسية وإجتماعية لإستخدام وسائل الإعلام بغية الحصول على نتائج خاصة يطلق عليها الإشباعات .[4]

الدافع: يشار إلى مفهوم الدافع في اللغة الإنجليزية بكلمة motive ومعناها يحرك فكلمة دافع مأخوذة من الفعل الثلاثي دفع أي حرك الشيء من مكانه إلى مكان آخر وفي إتجاه معين .[5]و عرف على أنه: " عامل إنفعالي حركي وفطري أو مكتسب شعوري أو لا شعوري يسير نشاط الفرد للأداء والإنجاز، أو تحقيق غاية، وينشأ داخل الفرد كنتيجة لخبراته السابقة توجهه لتحقيق هدف معين " [6]

---

[1] عبد الوهاب بوخوفة: التلميذ، المدرسة، المعلم وتكنولوجيا الإعلام والإتصال، التمثل والإستخدامات، أطروحة دكتوراه، جامعة الجزائر كلية العلوم السياسية والإعلام، 2007، ص35.

[2] إبراهيم قائد أحمد: إستخدامات الطلبة اليمنيين للفيسبوك والإشباعات المتحققة منه، النسخة الإلكترونية، مجلة دراسات وأبحاث، العدد 26، السنة التاسعة، ديسمبر 2017، ص 05.

[3] إبتسام رايس: نظرية الإستخدامات والإشباعات وتطبيقاتها على الإعلام الجديد، النسخة الإلكترونية، مجلد دراسات وأبحاث، العدد25، السنة الثانية، ديسمبر 2016، ص 503.

[4] عبد الرزاق الديلمي: إستخدامات الشباب الجامعي الأردني لمواقع التواصل الإجتماعي وإشباعاتها، النسخة الإلكترونية، مجلة علوم الإنسان والمجتمع، العدد 12، نوفمبر 2014، ص 123.

[5] إبراهيم قائد أحمد، مرجع سبق ذكره، ص 05.

[6] ريحانة بوطي: دوافع إستخدام الشباب للهوية الإقتراضية في الشبكات الإجتماعية وأثرها على الفرد، رسالة ماجستير، جامعة الحاج لخضر باتنة، ص 19.

الحاجة: حسب بن تونس فإن الحاجة هي " الدافع الطبيعي والميل الفطري الذي يدفع الإنسان إلى تحقيق غاية ما داخلية كانت أو خارجية، شعورية أو لا شعورية .[1]

أما نظرية الإستخدامات والإشباعات: فيأخذ منظور الإستخدامات والإشباعات وجهة نظر المستخدم لوسائل الإعلام ويبحث في كيفية إستخدام الناس لوسائل الإعلام والإشباعات التي يحققونها من إستخدامهم لتلك الوسائل، حيث تهتم نظرية الإستخدامات والإشباعات بدراسة الإتصال الجماهيري دراسة وظيفية منظمة، وتنحصر رؤيتها للجماهير على أنها فعالة في إنتقاء أفرادها لرسائل ومضمون وسائل الإعلام ووفقا لنظرية الإستخدامات والإشباعات فإن وسائل الإعلام تشكل موردا لتلبية إحتياجات الجمهور المختلفة، وتحول السؤال **من ما الذي تفعله وسائل الإعلام بالجمهور ؟ إلى ما الذي يفعله الجمهور بوسائل الإعلام ؟**[2]

[1] ساجية مخوف بن تونس: إستخدام الشباب للأنترنت وآثارها على الحياة النفسية والإجتماعية في وسائط الإتصال بين الإستعمال والإستخدام، مخلوف (الجزائر مخبر إستخدامات وتمقي المنتجات الإعلامية والثقافية في الجزائر 2015)، ص 23.

[2] مصطفى علي سيد النبي، الإتجاهات الحديثة لنظرية الإستخدامات والإشباعات، المجلة المصرية للدراسات المتخصصة، العدد23، يوليو 2019، ص41.

2) نشأة النظرية:

تعود الجذور التاريخية لنظرية الإستخدامات والإشباعات إلى الطرح الذي قدمه " إليهو كاتز " سنة 1959 في مقال رد فيه على رؤية " برناردبيرلسون " الذي حكم على أبحاث حقل الإعلام بالموت في حين رد عليه كاتز أن حقل الأبحاث المرتبطة بالإقناع هو الذي مات [1] وتطور مفهوم الإستخدامات والإشباعات في دراسة " كاتز وبلومر "1969 للإنتخابات العامة البريطانية عام 1964 ومن خلال الدراسة تم التعرف على أسباب مشاهدة أو عدم مشاهدة الحملات الإنتخابية .[2]

وقد إهتمت نظرية الإستخدامات والإشباعات بدراسة الإتصال الجماهيري دراسة وظيفية منظمة فخلال عقد الأربعنيات من القرن العشرين، أدى إدراك عواقب الفروق الفردية، والتباين الإجتماعي على إدراك السلوك المرتبط بوسائل الإعلام إلى بداية منظور جديد للعلاقة بين الجماهير ووسائل الإعلام .[3]كان ذلك تحولا من رؤية الجماهير على أنها عنصر سلبي غير فعال، إلى رؤيتها على أنها فعالة في إنتقاء أفرادها لرسائل ومضمون وسائل الإعلام . ويشير "ويرنر" و" تانكرد "إلى أن البحث في أنواع الإحتياجات التي يحققها إستخدام وسائل الإعلام قد بدأ منذ وقت مبكر من الثلاثينيات، حيث أجريت دراسات عديدة من هذا المنظور: على قراءة الكتب، ومسلسلات الراديو، والصحف اليومية، والموسيقى الشعبية، وأفلام السينما وذلك للتعرف على أسباب إستخدام الناس لوسائل الإعلام والنتائج التي تترتب عن ذلك.[4]

ويذهب " إدلستاين وزملاءه " إلى أن تأسيس نموذج الإستخدامات والإشباعات جاء كرد فعل لمفهوم قوة وسائل الإعلام الطاغية ويضفي هذا النموذج صفة الإيجابية على جمهور وسائل الإعلام، فمن خلال منظور الإستخدامات لم تعد الجماهير مجرد مستقبلين سلبيين لوسائل الإتصال الجماهيري، وإنما يختار الأفراد بوعي وسائل الإتصال التي يتعرضون لها ونوع المضمون الذي يلبي حاجاتهم النفسيةوالإجتماعية،

---

[1] إبتسام رايس، مرجع سبق ذكره، ص510.

[2] ريحانة بوطي، مرجع سبق ذكره، ص33.

[3] حسن عماد المكاوي، ليلى حسين السييد: الإتصال ونظرياته المعاصرة، ط10 (القاهرة: الدار اللبنانية، د.ت.ط)، ص239.

[4] محمد منير حجاب: نظريات الإتصال (القاهرة: دار الفجر، 2010)، ص 297.

[1] وقد أشارت هويت لوجود عوامل تدفع بالأفراد لإستخدام وسائل كما أن إحتياجات الأفراد يمكن أن تشبع من التعرض لوسائل الإتصال ومن هنا إنبثق مصطلح الإشباعات .[2]

3) فروض النظرية:

1- جمهور المتلقين هو جمهور نشط، وإستخدامه لوسائل الإعلام هو إستخدام موجه لتحقيق أهداف معينة .

2- يمتلك أعضاء الجمهور المبادرة في تحقيق العلاقة بين إشباع الحاجات وإختيار وسائل معينة يرى أنها تشبع حاجاته .

3- تنافس وسائل الإعلام مصادر أخرى لإشباع الحاجات .

4- الجمهور وحده هو القادر على تحديد الصورة الحقيقية لإستخدام وسائل الإعلام .

5- الجمهور نفسه هو الذي يحدد الأحكام حول قيمة العلاقة بين الحاجات والإستخدام .

6- الأفراد يستخدمون وسائل الإعلام لحل مشاكلهم فيما يتعلق بالبحث عن المعلومات والإتصال الإجتماعي والتعلم الإجتماعي والتطور .

7- يختار الأفراد من مضمون وسائل الإعلام ما يتناسب مع إحتياجاتهم سواء كان متعلقة بالمعلومات الأساسية أو التسلية أو التعلم .[3]

4) أهداف النظرية:

تسعى نظرية الإستخدامات والإشباعات إلى تحقيق ثلاث أهداف رئيسية هي:

1. التعرف على كيفية إستخدام الأفراد لوسائل الإعلام، وذلك بالنظر إلى الجمهور النشط الذي يستخدم الوسيلة التي تشبع حاجاته وأهدافه.
2. توضيح دوافع إستخدام وسيلة بعينها من وسائل الإعلام، و التفاعل مع نتيجة هذا الإستخدام .
3. التركيز على أن فهم عملية الإتصال الجماهيري يأتي نتيجة لإستخدام وسائل الإتصال الجماهيري[1]

---

[1] أديب خضور، "السلوك الإتصالي لقرية سورية"، مجلة جامعة الأقصى، المجلد 19، العدد1، 2015، ص 45.

[2] فاطمة ميدان "إستخدامات الشباب لوسائل الإتصال الحديثة: دراسة ميدانية في المؤسسة التربوية "، مجلة العلوم الإنسانية، العدد10، 2016، ص168.

[3] مصطفى علي سيد عبد النبي، مرجع سبق ذكره، ص 42.

5) إنتقادات النظرية:

أهم الإنتقادات الموجهة لنظرية الإستخدامات والإشباعات:

1. أن هذه النظرية تتبنى مفاهيم تتسم بشيء من المرونة، مثل الدافع، الإشباع، الهدف، الوظيفة، وهذه المفاهيم ليس لها تعريفات محددة، وبالتالي فمن الممكن أن تختلف النتائج التي نحصل عليها من تطبيق النظرية تبعا لإختلاف التعريفات .
2. أن الحاجات الخاصة بالفرد متعدد ما بين فسيولوجية ونفسية وإجتماعية، وتختلف أهميتها من فرد لآخر، ولتحقيق تلك الحاجات تتعدد أنماط التعرض لوسائل الإعلام وإختيار المحتوى .
3. تقوم النظرية على إفتراض أن إستخدام الفرد لوسائل الإعلام إستخدام متعمد ومقصود وهادف، والواقع يختلف في أحيان كثيرة عن ذلك، فهناك أيضا إستخدامات غير هادفة .
4. تنظر البحوث التي تستند إلى نظرية الإستخدامات والإشباعات إلى وظائف وسائل الإتصال من منظور فردي يستخدم الرسائل الإتصالية، في حين أن الرسالة الإتصالية قد تحقق وظائف لبعض الأفراد وتحقق إختلالا وظيفيا للبعض الآخر .[2]

[1] محمود حسن إسماعيل: مبادىء علم الإتصال ونظريات التأثر، ط1، دار العالمية للنشر والتوزيع، مصر، 2003، ص 255.

[2] محمود حسن إسماعيل، مرجع سبق ذكره، ص 257.

خاتمة الفصل:

نستنتج مما تطرقنا إليه أن نظرية الإستخدامات والإشباعات تقدم إطارا قويا لفهم سلوكيات الجمهور الإعلامي، وتركز النظرية على الدور النشط الذي يلعبه الأفراد في إختيار وإستخدام وسائل الإعلام لتلبية إحتياجاتهم ورغباتهم، وتشير إلى أن الجمهور ليس سلبيا يتلقى ببساطة رسائل من وسائل الإعلام بل هم فاعلون يبحثون عن محتوى يلبي إهتماماتهم.

الفصل الرابع

الاطار التطبيقي للدراسة

تمهيد

📖**أولا:** تحديد خصائص العينة المبحوثة

📖**ثانيا:**التحليل الكمي والكيفي لبيانات الدراسة

📖**ثالثا:** عرض الإستنتاجات العامة والجزئية للدراسة

خلاصة

تمهيد:

تعتبر الدراسة الميدانية مكملة للدراسة النظرية في إجراء البحوث، حيث تساعد الباحث للوصول إلى نتائج وحقائق تفسر و توضح وتكشف عن تساؤلات البحث، وتبين مدى ارتباط الجانب النظري بالجانب الموجود في الواقع.

وبعد أن تعرفنا في الفصل السابق على المعلومات المتعلقة بموضوع الدراسة وحاولنا ضبطها نظريا، سوف نعرض في هذا الفصل تحليل نتائج الدراسة وفق إجابات أفراد العينة، و ذلك بالإعتماد على الأساليب الإحصائية المناسبة لطبيعة الدراسة.

و يتضمن الفصل التطبيقي للدراسة 3 مباحث يتناول الأول تحديد خصائص العينة المبحوثة، المبحث الثاني يتم فيه التحليل الكمي والكيفي لبيانات الدراسة وفي المبحث الأخير يتم فيه عرض الإستنتاجات العامة والجزئية للدراسة .

أولا :تحديد خصائص العينة المبحوثة :

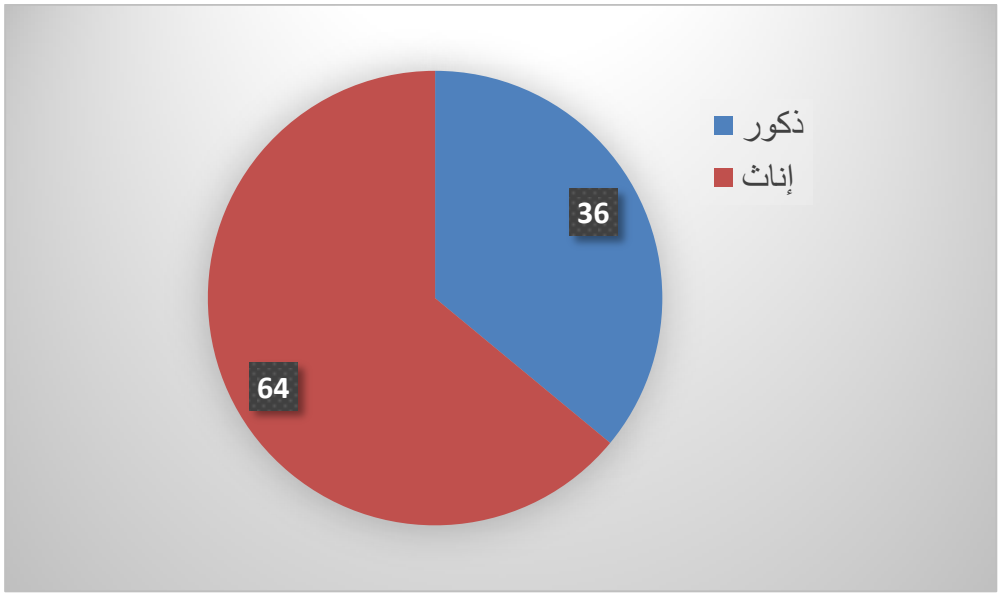
تمثلت العينة المبحوثة في طلبة قسم علوم الإعلام والإتصال بجامعة يحي فارس المدية كونهم الفئة أكثر إلماما بالمعلومات المتعلقة بدراستنا بحكم تخصصهم وتمكنهم من الإجابة على الأسئلة بشكل أفضل ومشاركة تجاربهم وآرائهم حول إستخدامهم للفضاء السيبراني ومدى تعرضهم للجرائم الالكترونية والتي يمكن ان تساهم في فهم أفضل لتحليل السلوك السيبراني ومخاطره ،وعلى هذا الأساس اخترنا 120 مفردة متكونة من طلبة السنة الثالثة ليسانس تخصص إعلام، طلبة الماستر 1و2 تخصص سمعي بصري وإتصال وعلاقات عامة، حيث يتكون مجتمع البحث من حوالي 551 طالب المكون من 5 طبقات: حجم الطبقة الاولى 247 طالب من قسم الإعلام للسنة الثالثة ليسانس ، الطبقة الثانية 100طالب سنة اولى ماستر اتصال وعلاقات عامة، الطبقة الثالثة 114طالب سنة ثانية ماستر اتصال وعلاقات عامة، الطبقة الرابعة 25 طالب سنة اولى ماستر سمعي بصري والطبقة الخامسة 65 طالب سنة ثانية ماستر سمعي بصري.

ثانيا: التحليل الكمي والكيفي لبيانات الدراسة :

الجدول رقم1: يمثل العينة المبحوثةحسب متغير الجنس:

متغير الجنس	التكرار	النسبة
ذكور	43	%36
إناث	77	%64
المجموع	120	%100

الشكل رقم 1 يمثل العينة المبحوثة حسب متغير الجنس



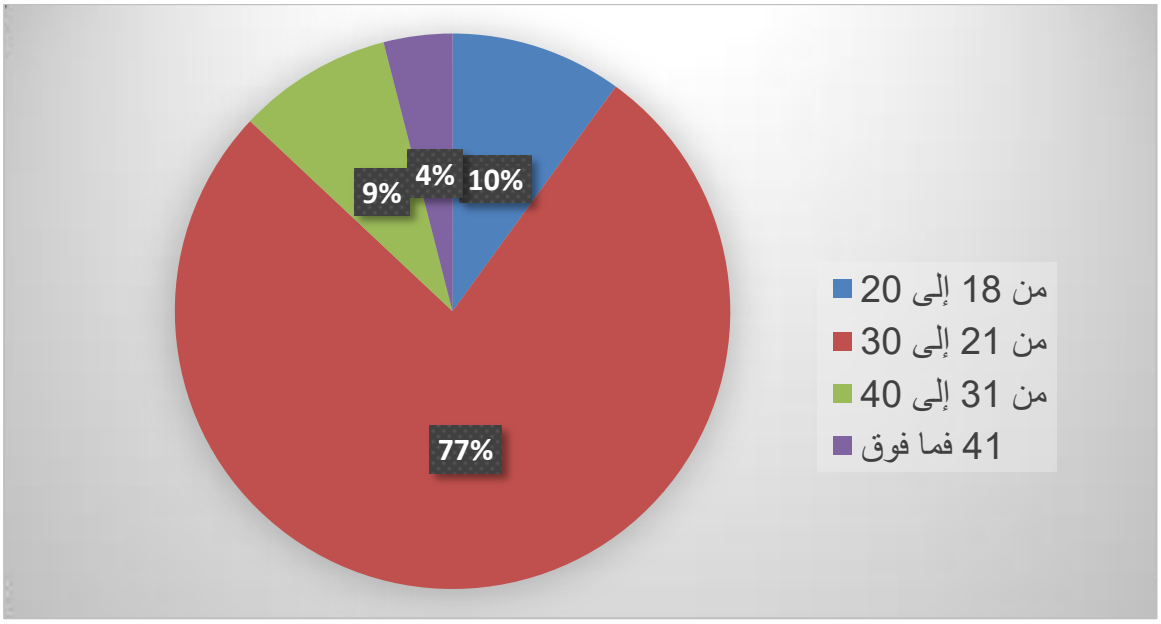
نلاحظ من خلال معطيات الجدول رقم 1 التي تخص العينة المبحوثة حسب متغير الجنس ،أن فئة الإناث هي الفئة الغالبة والتي قدرت ب :64% أي ما يعادل 77 مبحوثا ،ثم تليها فئة الذكور و التي قدرت بنسبة 36% بمعدل 43 مبحوثا ، وهذا ما يوصلنا إلى أن فئة الإناث مرتفعة عن الذكور .

ويرجع ارتفاع نسبة الاناث مقابل الذكور الى عدة عوامل يمكن ابرازها في الشكل التالي :ذلك ان الاناث يقبلن على تخصص الاعلام والاتصال أكثر من الذكور ، وان تعداد الاناث اكثر في المجتمع لذلك نجد ان اغلبية الطلبة في هذا الميدان هم الاناث.

الجدول رقم 2: يمثل العينة المبحوثةحسب متغير السن:

متغير السن	التكرار	النسبة
من 18 إلى 20	12	%10
من 21 إلى 30	92	%77
من 31 إلى 40	11	%9
41 فما فوق	5	%4
المجموع	120	%100

الشكل رقم 2 يمثل العينة المبحوثة حسب متغير السن



اتضح لنا من خلال الجدول 2 الخاص بمتغير السن بعد اعتمادنا على التقسيم الديموغرافي العالمي للسن أن الفئة العمرية الأكثر شيوعا هي من 21 إلى 30 سنة حيث بلغت نسبتها 77% بتكرار 92 مرة وهي النسبة الأعلى بين الفئات العمرية من حيث المشاركة ، في حين بلغت النسبة الموالية المحددة من 18 إلى 20 نسبة 10% بتكرار 12 مرة، تليها فئة من 31 إلى 40 التي قدرت بنسبة 9% بتكرار 11 مرة وفي الأخير كآخر فئة عمرية قدرت بنسبة 4% بتكرار 5 مرات وهي فئة من 41 سنة فما فوق.

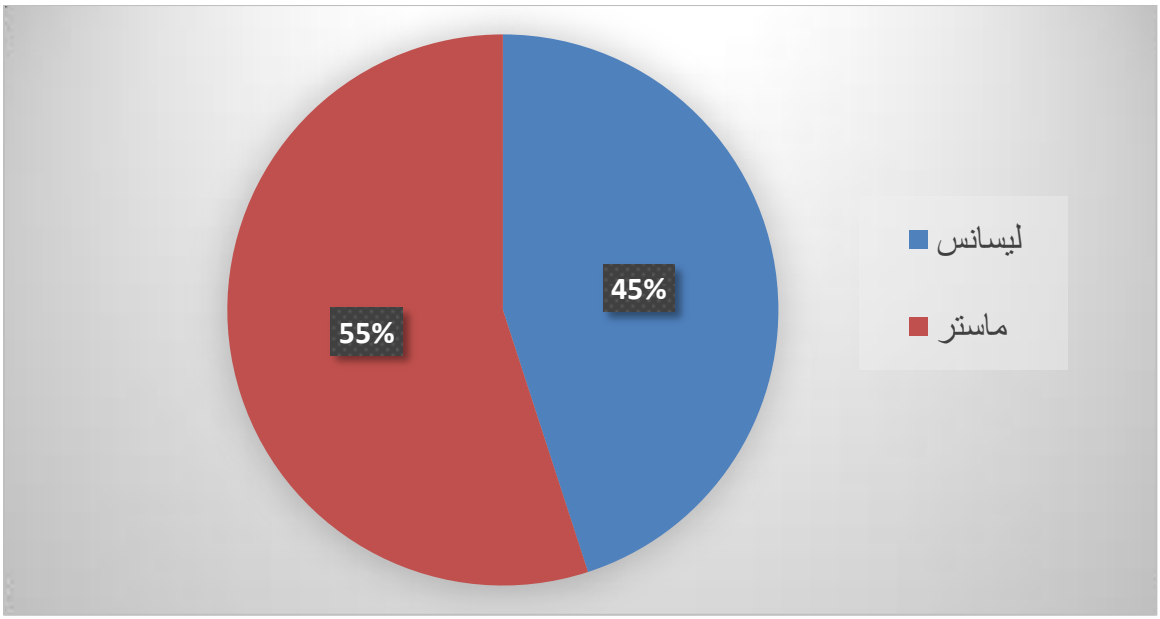
ومن هنا نستنتج أن فئة الشباب المتداولة من 21 إلى 30 هي الفئة الغالبة في عينة دراستنا المحددة بـ 120 مفردة من طلبة السنة الثالثة ليسانس تخصص إعلام وطلبة الماستر 1و2تخصص

سمعي بصري وإتصال وعلاقات عامة ،وهذا راجع إلى أن كون أغلب الطلبة يتحصلون على شهادة ليسانس في حدود 21سنة وشهادة الماستر في حدود 23سنة كما يوجد منهم من يعيد في مقاعد الجامعة خاصة في السنة الاولى ليسانس وهذا بسبب عديد من التغيرات التي تحصل على مختلف البناءات المرتبطة بمسار الطالب الجامعي .

الجدول رقم 3: يوضح العينة المبحوثة حسب متغير المستوى التعليمي

متغير المستوى التعليمي	التكرار	النسبة
ليسانس	54	%45
ماستر	66	%55
المجموع	120	%100

الشكل رقم 3 يوضح العينة المبحوثة حسب متغير المستوى التعليمي



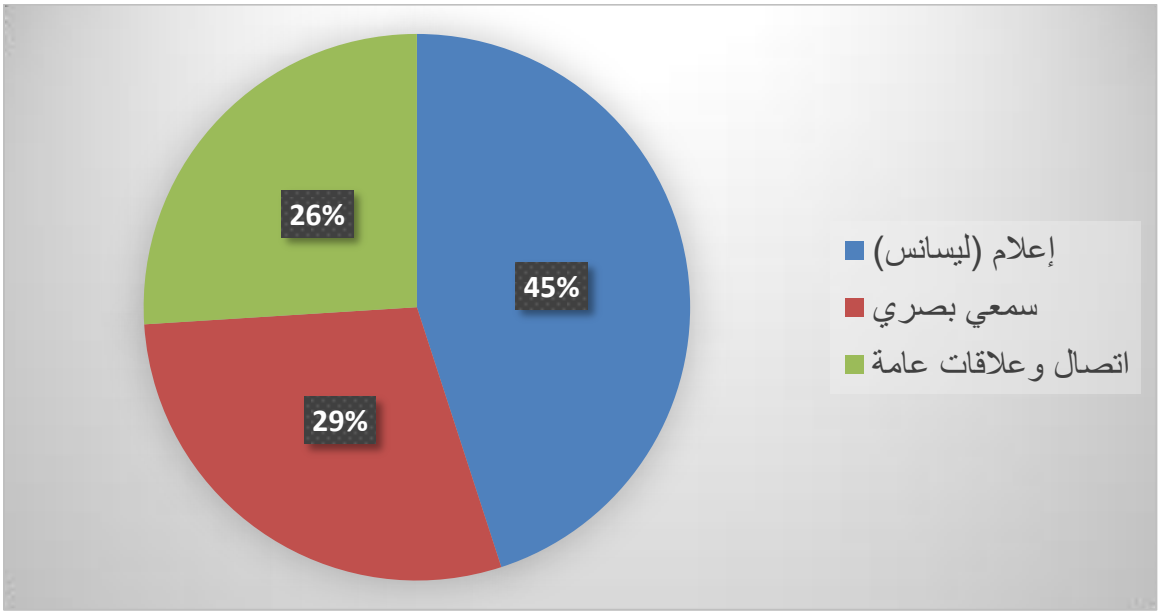
الجدول رقم 3 يوضح متغير المستوى التعليمي حيث بلغت نسبة طلبة الماستر 55% بتكرار 66 مرة من أصل طلبة الماستر 1 تخصص سمعي بصري وإتصال وعلاقات عامة، وطلبة الماستر 2 تخصص سمعي بصري وإتصال وعلاقات عامة، في حين أن نسبة ليسانس إعلام قد بلغت 45% بتكرار 54 مرة.

ومنه فإن نسبة طلبة الماستر كانت الفئة الغالبة على العينة المبحوثة ، فنجد طلبة الماستر يفضلون درجات عليا لتحسين مهاراتهم وتطوير خبراتهم والحصول على ترقيات و وظائف برواتب أعلى وهذا ما يساهم في زيادة نسبة طلبة الماستر مقارنة بطلبة ليسانس .

الجدول رقم 4: يمثل العينة المبحوثةحسب متغير التخصص:

متغير التخصص	التكرار	النسبة
إعلام (ليسانس)	54	%45
سمعي بصري	35	%29
اتصال وعلاقات عامة	31	%26
المجموع	120	%100

الشكل رقم 4 يمثل العينة المبحوثةحسب متغير التخصص



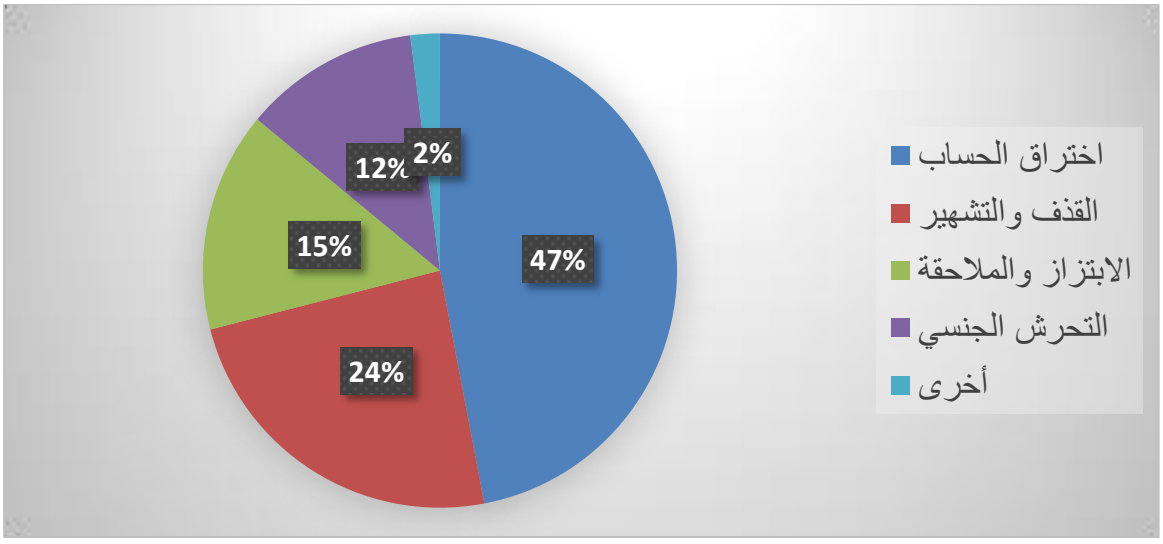
تبين لنا من خلال الجدول رقم 4 الذي يمثل العينة المبحوثة حسب متغير التخصص أن تخصص إعلام لطلبة ليسانس السنة الثالثة هو التخصص الغالب على العينة المبحوثة حيث بلغ نسبة 45% بتكرار 54 مفردة لان عدد افراد هذا التخصص كان أكبر من عدد طلبة التخصصات الاخرى حيث بلغ 247طالب من أصل 551 من مجتمع البحث حسب الاحصائيات المقدمة من طرف إدارة الجامعة ، ثم

يليها تخصص سمعي بصري لكل من ماستر 1 وماستر 2 بنسبة 29% بتكرار 35 مرة، وفي الأخير يأتي تخصص إتصال وعلاقات عامة لكل من ماستر 1 و2 كأقل نسبة بتقدير 26% بتكرار 31 مرة حيث أن طبيعة العينة طبقية.

الجدول رقم 5: يمثل أنواع الجرائم الالكترونية الأكثر انتشارا بين الطلبة.

أنواع الجرائم الإلكترونية	التكرار	النسبة
اختراق الحساب الشخصي	57	%47
القذف والتشهير	29	%24
الابتزاز والملاحقة	18	%15
التحرش الجنسي	14	%12
أخرى	2	%2
المجموع	120	%100

الشكل رقم 5 يمثل أنواع الجرائم الالكترونية الأكثر انتشارا بين الطلبة



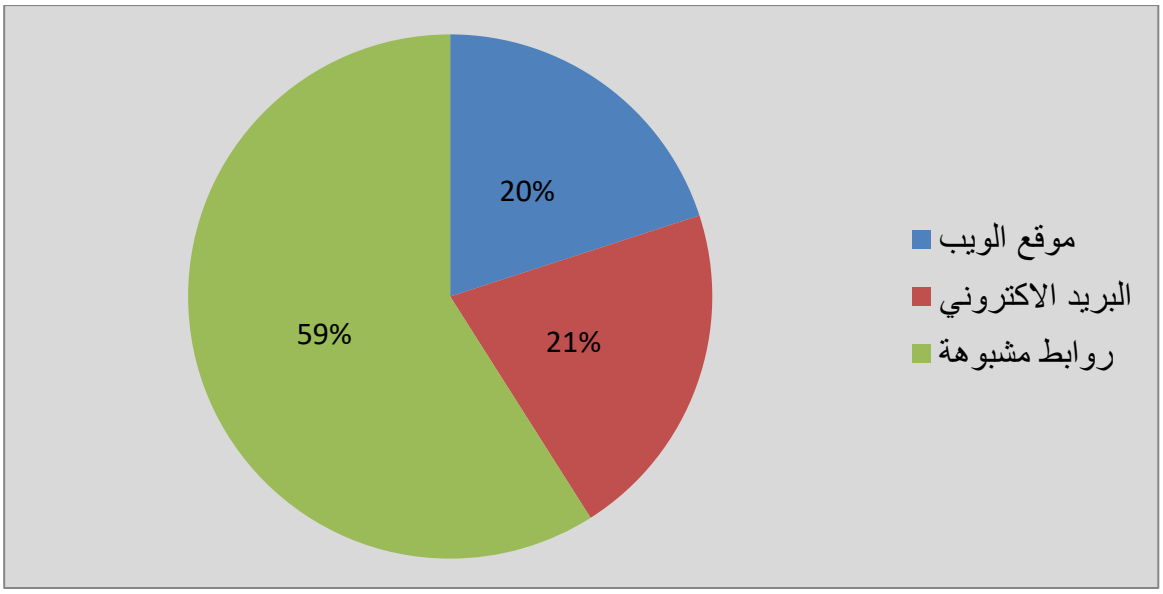
يؤكد الجدول رقم 5 الذي يمثل أنواع الجرائم الالكترونية التي يتعرض لها الطلبة عبر موقع الفيسبوك أن جريمة الاختراق وسرقة البيانات الشخصية هي الأكثر انتشارا بينهم حيث بلغت نسبة 47% بتكرار 57 مرة لانها جرائم سهلة الحدوث بدون أي تخطيط مسبق خاصة مع إنتشار استخدام الانترنت

والهواتف الذكية واجهزة الكمبيوتر. اما في المرتبة الثانية تأتي جريمة القذف والتشهير بنسبة 24% بتكرار 29 مرة بنشر معلومات او أخبار كاذبة عن شخص ما بقصد الضرر بسمعته وكرامته .تليها جريمة الابتزاز والملاحقة بنسبة 15% بتكرار 18 مرة وهو سلوك اجرامي يتمثل في مضايقة الافراد بشكل متكرر ما يسبب الشعور بالخوف أو القلق أو عدم الامان . ثم جريمة التحرش الجنسي حيث بلغت نسبة 12% بتكرار 14 مرة والتي اختيرت من طرف الإناث اكثر من الذكور وهذا يدل على أن الإناث هي الفئة الأكثر تعرض لهذا النوع من الإجرام وتشمل التصرفات غير المرغوب فيها بإرسال رسائل أو صور أو فيديوهات إباحية دون موافقة الشخص الآخر. أما الجرائم الأخرى فقد كانت في المرتبة الأخيرة بنسبة 2% بالتقريب بتكرار 2 مرات، تمثلت هذه الجرائم في المتاجرة بالمخدرات عبر موقع الفيسبوك وانتحال شخصية المستخدم وفتح حساب وهمي بإسمه والعمل به.

الجدول رقم 6: يمثل الوسائط التي يتم عن طريقها ارتكاب الجريمة الالكترونية :

الوسائط التي يتم عن طريقها ارتكاب الجريمة الإلكترونية	التكرار	النسبة
موقع الويب	24	%20
البريد الالكتروني	25	%21
روابط مشبوهة	71	%59
المجموع	120	%100

الشكل رقم 6 يمثل الوسائط التي يتم عن طريقها ارتكاب الجريمة الالكترونية

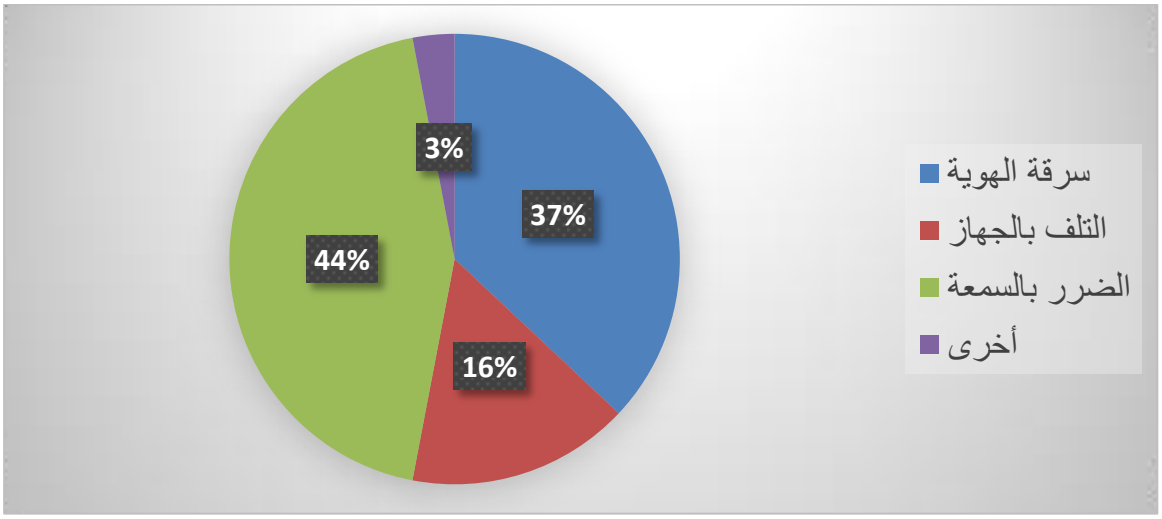


يشير الجدول رقم 6 الذي جاء تحت عنوان الوسائط التي يتم عن طريقها ارتكاب الجريمة الالكترونية أن الروابط المشبوهة من أكثر الوسائط التي ترتكب بواسطتها هذه الجرائم حيث بلغت نسبتها 59% بتكرار 71 مرة، وهي عبارة عن روابط غير آمنة تحتوي على برامج ضارة مثل الفيروسات مثال على ذلك فيروس phishing "فيشينغ" الذي يعمل عن طريق إنشاء روابط غير آمنة تبدو وكانها صفحات ويب شرعية ،ولكنها في الواقع تحاول إختراق معلومات الدخول الخاصة بالمستخدمين مثل اسم المستخدم وكلمة المرور . في المرتبة الثانية يأتي البريد الالكتروني بنسبة 21% بتكرار 25 مرة وهو الوسيلة التي تستخدم للإرسال والاستقبال بين الأشخاص وهو ما يحدد هوية الأشخاص على موقع الفيسبوك، في المرتبة الثالثة حددت نسبة 20% لموقع الويب بتكرار 24 مرة وهي مجموعة من الصفحات التي تتضمن محتوى متنوعا مثل الصور والفيديوهات والروابط وغيرها ، تكون متصلة ببعضها البعض عبر روابط تسمح للمستخدمين بالتنقل بينها بسهولة عن طريق المتصفح الالكتروني وهنا تنفذ الجرائم الالكترونية بشكل فعال وغير مرئي .

الجدول رقم 7: يوضح الانعكاس الذي ينتج عن الجريمة الإلكترونية :

الانعكاس الذي ينتج عن الجريمة الإلكترونية	التكرار	النسبة
سرقة الهوية	44	%37
التلف بالجهاز	19	%16
ضرر بالسمعة	53	%44
أخرى	4	%3
المجموع	120	%100

الشكل رقم 7 يوضح الانعكاس الذي ينتج عن الجريمة الإلكترونية



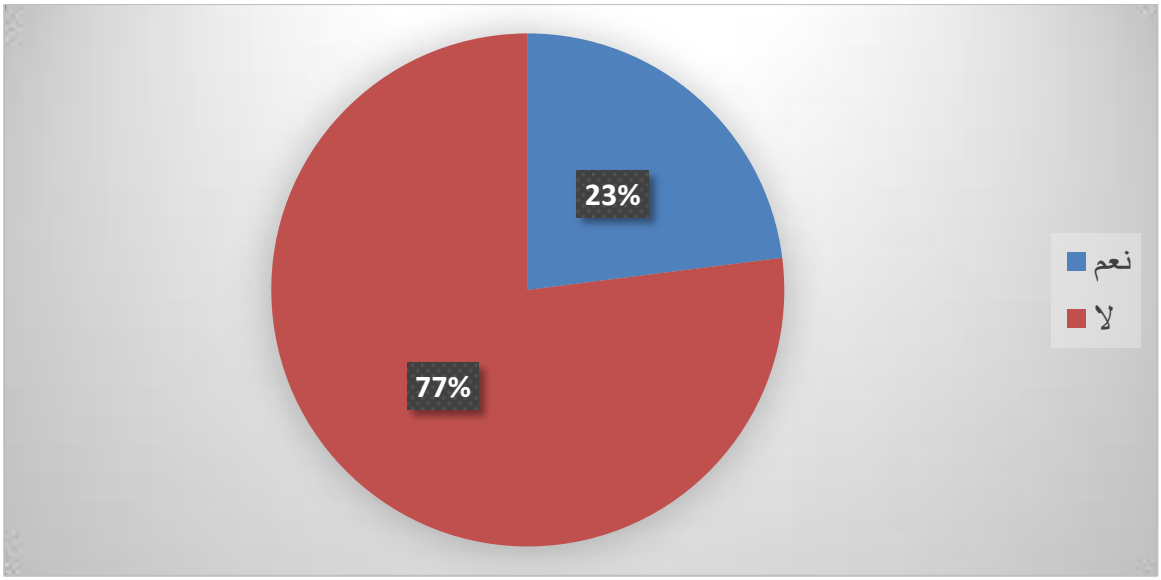
يكشف الجدول رقم 7 المتعلق بالانعكاس الذي ينتج عن الجريمة الالكترونية أن الضرر بالسمعة هو أكثر إنعكاس تسببه هذه الجرائم على الطلبة حيث قدر بنسبة 44% بتكرار 53 مرة و الذي يشير إلى الأذى الذي يلحق بسمعة الشخص وينتج عنه فقدان ثقة الآخرين وتأثيره السلبي على علاقاته الشخصية والدراسية، ثاني إنعكاس كان سرقة الهوية بنسبة 37% بتكرار 44 مرة وإستغلالها في التشهير أو الاساءة للشخص المنسوب اليه. وثالث تضرر كان التلف بجهاز الهاتف و الكمبيوتر بنسبة 16% بتكرار 19 مرة وذلك بفقدان البيانات المخزنة مثل الملفات الهامة وعدم القدرة على الوصول إلى المعلومات كذلك تكلفة الإصلاح أو الاستبدال. ومن الأضرار الأخرى المذكورة في الاستمارة الموزعة على

الطلبة بلغت نسبة 3% بتكرار 4 مرات المتمثلة في الضرر النفسي، الخوف، أضرار مادية، وانعدام الثقة في مواقع التواصل الاجتماعي .

الجدول رقم 8 :يوضح مدى تعرض الطلبة للجريمة الالكترونية:

مدى تعرض الطلبة للجريمة الإلكترونية	التكرار	النسبة
نعم	28	%23
لا	92	%77
المجموع	120	%100

الشكل رقم 8 يوضح مدى تعرض الطلبة للجريمة الالكترونية



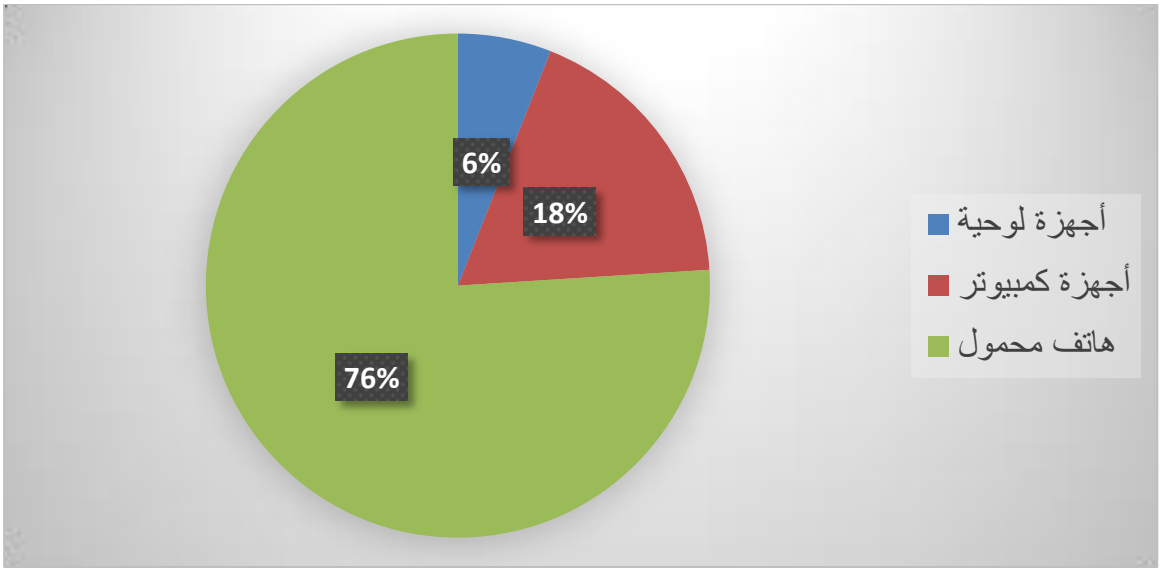
يثبت الجدول رقم 8 المتعلق بمدى تعرض طلبة قسم علوم الإعلام والاتصال بجامعة المدية للجريمة الالكترونية أن نسبة الطلاب الذين لم يتعرضوا لأي نوع من هذه الجرائم قد بلغت نسبة77% بتكرار 92 مرة ويرجع ذلك إلى إستخدامهم لكلمات مرور قوية وفريدة وتجنب إستخدام معلومات شخصية سهلة التخمين مثل تاريخ الميلاد ، كذلك تثبيت برامج مكافحة الفيروسات وتحديثها بشكل دوري وتجنب النقر على الروابط او فتح المرفقات من رسائل البريد الالكتروني . في حين أن نسبة الطلبة الذين تعرضوا للجريمة الالكترونية أو جرائم الانترنت بلغت 23% بتكرار 28 مرة، تمثلت هذه الجرائم في القرصنة

الالكترونية بالدرجة الأولى حيث بلغ عدد الطلبة الذين تعرضوا لقرصنة حسابهم الشخصي18 من أصل 28 طالب لعدم إمتلاكهم لمهارات حماية بياناتهم ومعلوماتهم الشخصية من السرقة والإختراق وعدم إستخدامهم للمصادقة الثنائية التي يتم عن طريقها إرسال رمز تأكيد إلى الهاتف او البريد الالكتروني بعد إدخال كلمة المرور الخاصة به ، باقي الطلبة واجهوا جرائم أخرى كسرقة البريد الالكتروني، التحرش الجنسي خاصة عند الإناث، كذلك انتحال شخصية بإنشاء حساب وهمي بمعلومات الضحية إضافة إلى التهديد والنصب والاحتيال عبر موقع الفيسبوك.

الجدول رقم9: يمثل الأداة المستخدمة للولوج إلى الفيسبوك:

الأداة المستخدمة	التكرار	النسبة
أجهزة لوحية	07	%6
أجهزة كمبيوتر	22	%18
هاتف محمول	91	%76
المجموع	120	%100

الشكل رقم 9 يمثل الاداة المستخدمة للولوج إلى الفيسبوك



يبين الجدول رقم 09 الأداة المستخدمة للولوج إلى الفيسبوك حيث أكدت النتائج على أن الأداة المستخدمة بكثرة بين الطلبة هي الهاتف المحمول بنسبة 76% بتكرار 91 مرة لأنها تعتبر الأداة الرئيسية

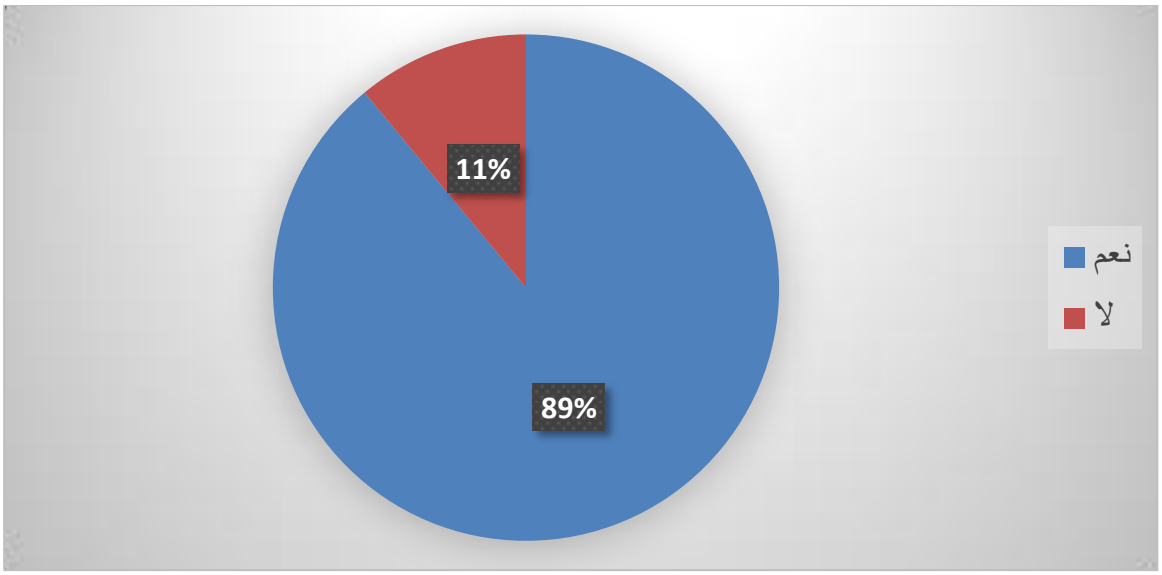
التي يفضلها الطلبة للوصول إلى الفيسبوك وذلك لصغر حجمه ما يجعله مناسب للإستخدام اليومي وإدارة المهام كذلك لامتلاكه خاصية التقاط الصور و الفيديوهات بجودة إحترافية، في المرتبة الثانية أجهزة الكمبيوتر بنسبة 18% بتكرار 22 مرة للإعتماد عليه في إنجاز البحوث ومذكرات التخرج خاصة طلبة السنة الثالثة ليسانس تخصص إعلام وطلبة الماستر 2سمعي بصري وإتصال وعلاقات عامة، تليها أجهزة لوحية بنسبة 6% بتكرار 07 مرات ويرجع ذلك لسيطرة الهواتف الذكية والمنافسة من أجهزة الكمبيوتر المحمولة كما انها نطاق ضيق الخدمة تستخدم بشكل أساسي للترفيه.

في حين يرى معظم الطلبة أن هذه الأجهزة قد تزيد من فرص التعرض للجريمة الالكترونية، حيث يمكن استخدامها لوسائل غير قانونية خاصة بعد استعمال الجهاز وبيعه، ولكونها أجهزة متصلة بالأنترنت ما يزيد من خطورتها وعدم أمانها.

الجدول رقم 10: يبين مدى تعرض موقع الفيسبوك للجريمة الإلكترونية مقارنة بالمواقع الأخرى:

مدى تعرض الفيسبوك للجريمةالالكترونية مقارنة بالمواقع الاخرى	التكرار	النسبة
نعم	107	%89
لا	13	%11
المجموع	120	%100

الشكل رقم 10 يبين مدى تعرض موقع الفيسبوك للجريمة الالكترونية مقارنة بالمواقع الاخرى



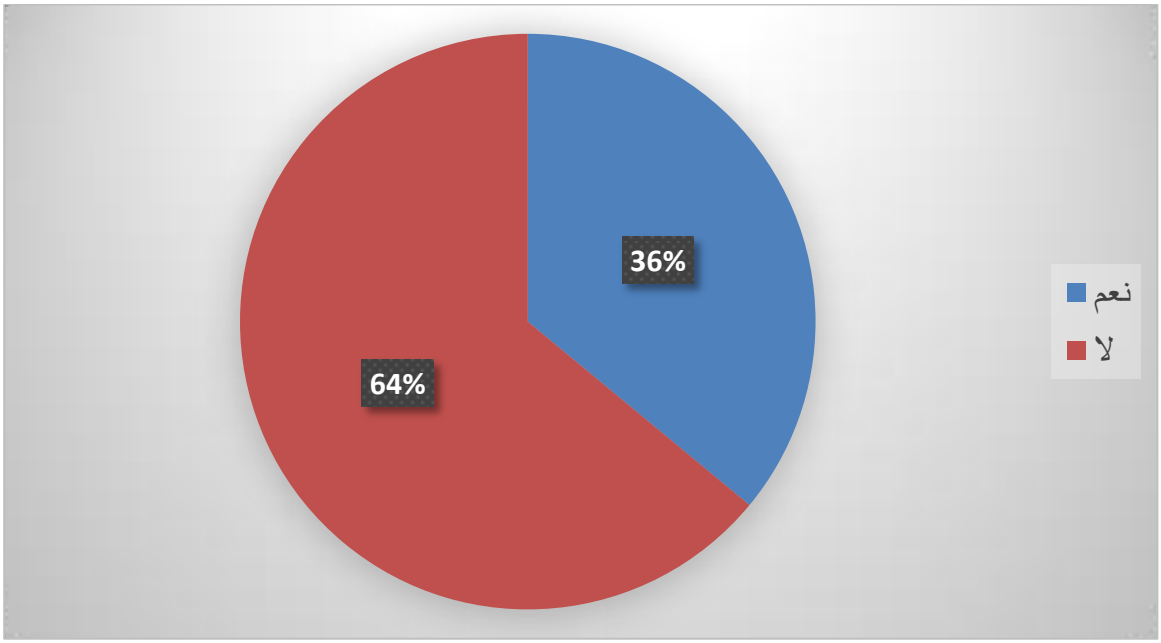
أظهر الجدول رقم 10 الذي يبين مدى تعرض الفيسبوك للجريمة الالكترونية مقارنة بالمواقع الأخرى، حيث بلغت نسبة 89% بمعدل 107 مبحوثا يرون بأن موقع الفيسبوك أكثر عرضة لجرائم المعلوماتية أو جرائم الحاسوب مقارنة بالمواقع الأخرى كالأنستغرام والتيك توك وغيرها ، لأن الفيسبوك يملك أكبر عدد من المستخدمين كونه من أقدم المواقع التي يستخدمها الأفراد يوميا ، كذلك لإمتلاكه خاصية الصور التي تمكن المستخدمين من تحميل الالبومات والصور من أجهزتهم إلى الموقع وخاصية الحالة statuts التي تتيح إمكانية إبلاغ أصدقائهم بأماكنهم وما يقومون به من أعمال والمشاركة في الرسائل ،لهذا نجح الفيسبوك في كسب العديد من المستخدمين من خلال تنوع الخدمات التي ينتجها وبالتالي زيادة التعرض للجرائم الإلكترونية .

في حين أن نسبة 11% بمعدل 13 مبحوثا يرون بأن الفيسبوك مثله مثل التطبيقات الأخرى أي بنفس درجة التعرض خاصة إذا كانت كلمة المرور موحدة لكل مواقع التواصل الإجتماعي مثال عن ذلك عندما يتعرض الفيسبوك للقرصنة فتتعرض كل المواقع الاخرى للقرصنة بسبب عدم وعي الطلبة الكافي بإستخدام هذا الموقع .

الجدول رقم11: يمثل إنعكاس مدة الإستخدام في زيادة الجرائم الإلكترونية:

مدة الإستخدام	التكرار	النسبة
نعم	43	%36
لا	77	%64
المجموع	120	%100

الشكل رقم 11 يمثل إنعكاس مدة الإستخدام في زيادة الجرائم الإلكترونية



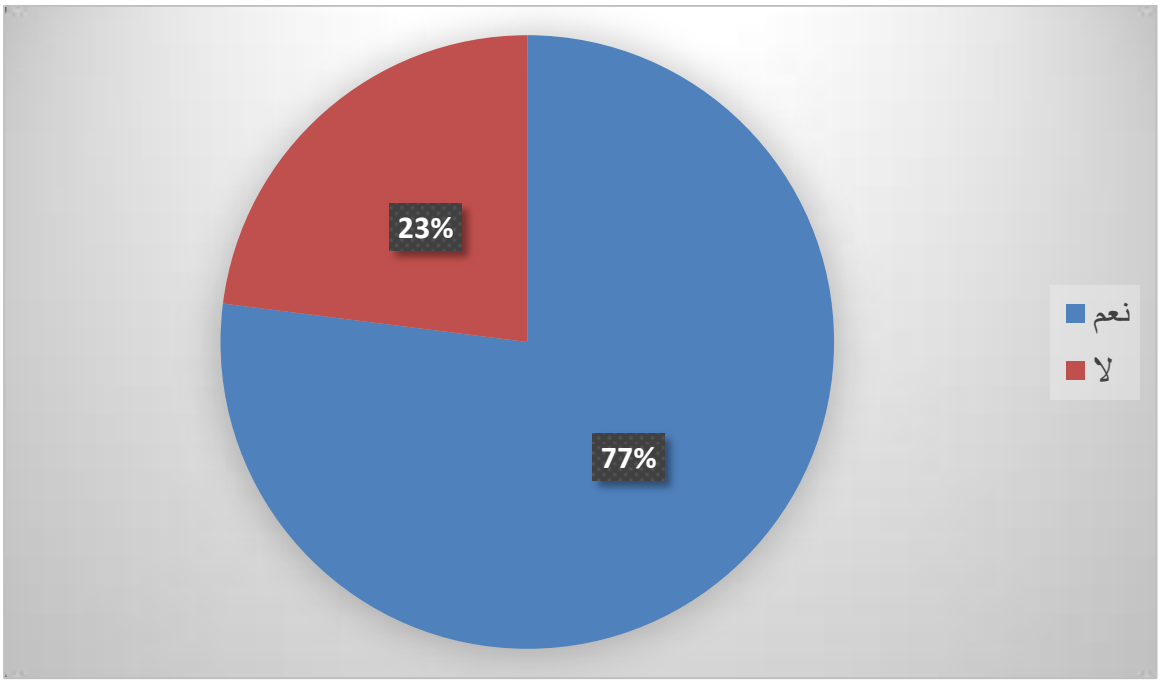
أثبت الجدول رقم 11 المتمثل في إنعكاس مدة إستخدام الفيسبوك في زيادة الجريمة الإلكترونية أن نسبة 64% ما يعادل77 مبحوثا ترى بأن مدة الإستخدام لا تعني بالضرورة أن الطلبة سيكونون أكثر عرضة للجريمة الالكترونية.في الواقع التعرض لمخاطر الانترنت يعتمد أكثر على كيفية إستخدام الشخص للمنصة وليس فقط على المدة الزمنية ، إذا كان الطلبة مدركين المخاطر ويتبعون ممارسات آمنة مثل عدم مشاركة المعلومات الحساسة وضبط إعدادات الخصوصية بشكل صحيح فإن الوقت قد لا يكون العامل الحاسم في تعرضهم للجريمة. في حين أن نسبة 36% مايعادل 43 مبحوثا تشير إلى وجود إرتباط بين المدة التي يقضيها الطلبة على هذا الموقع والتعرض للجريمة مثل الإحتيال و الإختراق والسرقة

الإلكترونية ، خاصة مع وجود عوامل مثل مشاركة المعلومات الشخصية والتفاعل مع الغرباء و النقر على الروابط المشبوهة بالإضافة إلى تأثير الإدمان على وسائل التواصل الإجتماعي الذي يقلل من اليقظة و الوعي بمخاطر الجرائم.

الجدول رقم 12: يمثل إنعكاسات الإفصاح عن الهوية على الفيسبوك :

إنعكاسات الإفصاح عن الهوية	التكرار	النسبة
نعم	92	77%
لا	28	23%
المجموع	120	100%

الشكل رقم 12 يمثل إنعكاسات الإفصاح عن الهوية على الفيسبوك



يوضح الجدول رقم12إنعكاسات الإفصاح عن الهوية على الفيسبوك ، حيث أكدت نسبة 77% بتكرار 92 مرة أن الإبلاغ عن الهوية يزيد من درجة التعرض ، من خلال الإفصاح بالإسم الكامل وتاريخ الميلاد وعنوان السكن ورقم الهاتف، إضافة إلى تفاصيل العمل أو الدراسة وحتى الصورة الشخصية، كذلك ميل الطلاب إلى مشاركة موقعهم الحالي و خطط السفر وتفاصيل حياتهم اليومية مما تجعلهم أهدافا سهلة

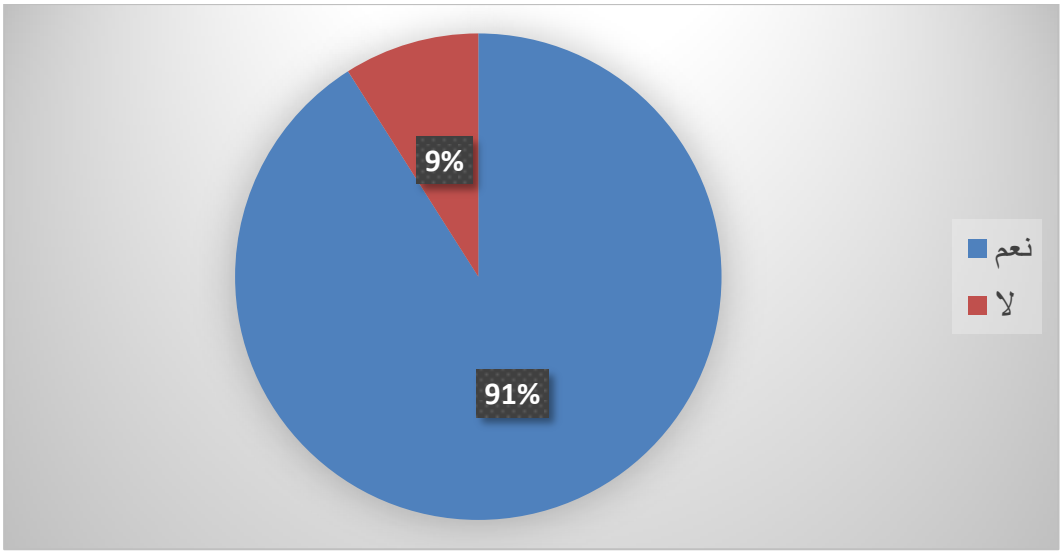
للتتبع والاستغلال و محفوفة بالمخاطر للأسباب التالية: سرقة الهوية، التصيد الاحتيالي، الاختراق، التهديد والتشهير بعد الحصول على صور فيديوهات ومحادثات شخصية، كما أنه في بعض الأحيان تكون هناك عداوة بين المجرم الالكتروني والمتضرر فيكون من السهل الوصول إليه عن طريق المعلومات الموجودة على حسابه الشخصي.

في حين أن نسبة 23% بتكرار 28 مرة ترى أن الإفصاح عن الهوية لا يزيد من درجة التعرض لأن الهوية الرقمية من الصعب ان تتسم بالإستقرار و الثبات وإنما هي على الدوام في حالة تغيير وتطور مستمرين حسب طبيعة التفاعل الإجتماعي للأفراد عبر الشبكات الإجتماعية .فنادرا ما يعرض المستخدمون لمواقع التواصل ملفاتهم الشخصية وأسمائهم الحقيقية ومعلوماتهم الحقيقية المكونة لهويتهم بل يلجئون في تشكيل الهوية الافتراضية المطابقة للحقيقة خاصة الإناث خوفا من العادات و التقاليد بنشر صورهم أو أسمائهم الحقيقية.

الجدول رقم13: يوضح دور تفقد البيانات الشخصية :

تفقد البيانات الشخصية	التكرار	النسبة
نعم	109	%91
لا	11	%9
المجموع	120	%100

الشكل رقم 13 يوضح دور تفقد البيانات الشخصية



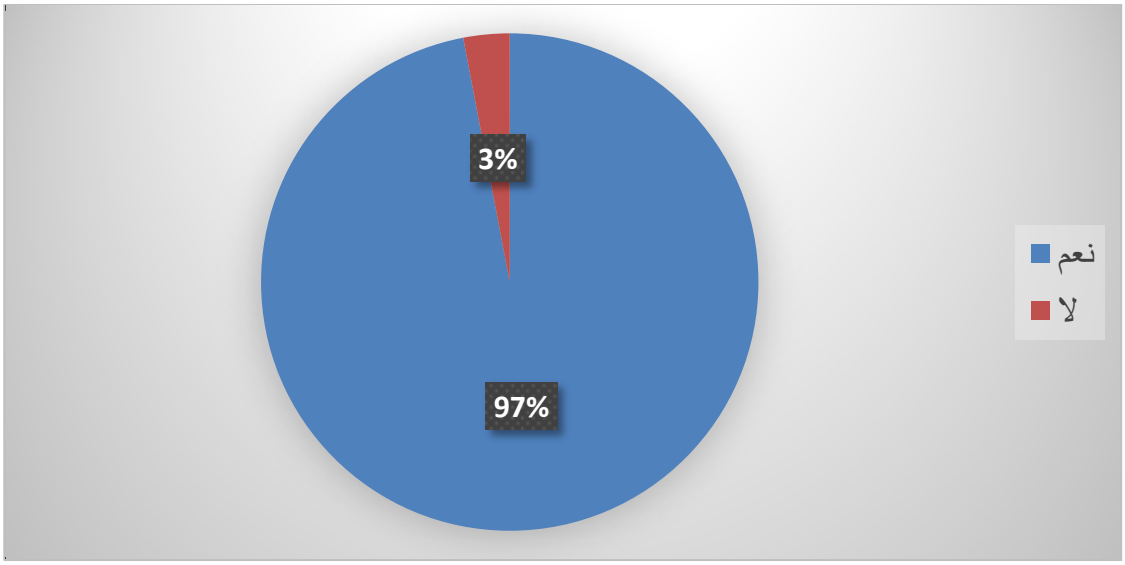
يبرز الجدول رقم 13 المتعلق بدور تفقد البيانات الشخصية في التقليل من نسبة التعرض للجريمة الالكترونية أن تفقد البيانات الشخصية بشكل دوري يمكن أن يلعب دورا هاما في التقليل من هذه الجرائم بنسبة 91% بتكرار 109 مبحوثا ، حيث أن العالم اليوم يعتمد بشكل متزايد على التكنولوجيا لتصبح البيانات الشخصية معرضة للإختراقات و الهجمات الالكترونية .فمن خلال مراجعة الطلبة لبياناتهم بانتظام يمكن الكشف عن التغييرات الغير عادية أو نشاطات مشبوهة بشكل سريع ، هذا الوعي المبكر يسمح لهم بإتخاذ الاجراءات الوقائية الضرورية مثل تغيير كلمات المرور، تنشيط ميزات الامان الإضافية، أو حتى التواصل مع الجهات المعنية لإيقاف أي محاولات إحتيال محتملة.

في حين أن نسبة 9% بتكرار 11 مبحوثا يعتقدون أن تفقد البيانات الشخصية ليس كافيا لتقليل الجرائم الإلكترونية وأن الحلول التقليدية ليست كافية لمعالجة هذه المشكلة المتزايدة ،وإنما هناك عوامل أخرى تلعب دورا أكبر في مكافحة الجرائم الإلكترونية مثل تعزيز الوعي الأمني من خلال برامج تعليمية وتدريبية مستمرة وتطوير تقنيات حماية أكثر فعالية وتطبيق قوانين صارمة .

الجدول رقم 14: يمثل دور الوعي الرقمي في مكافحة الجرائم الالكترونية:

دور الوعي الرقمي في مكافحة الجريمة الإلكترونية	التكرار	النسبة
نعم	116	%97
لا	4	%3
المجموع	120	%100

الشكل رقم 14 يمثل دور الوعي الرقمي في مكافحة الجرائم الالكترونية



يفسر الجدول رقم 14 دور الوعي الرقمي عند الطلبة في مكافحة الجرائم الالكترونية حيث بلغت نسبة 97% بتكرار 116 مرة وهي نسبة جد عالية تؤكد على أن الوعي الرقمي له دور هام في مكافحة الجرائم الالكترونية من خلال تمكين الطلبة بالمعرفة و الادوات اللازمة لحماية أنفسهم في الفضاء السيبراني. فعندما يكون الطلبة على دراية بمخاطر الانترنت وكيفية التعامل معها يمكنهم تقليل فرص تعرضهم للجريمة الالكترونية كالوعي بمحاولة التصيد الإحتيالي ومنحهم ثقافة الإبلاغ عنها وعدم الخوف منها ومواجهتها وتعزيز الوعي بين بعضهم البعض.

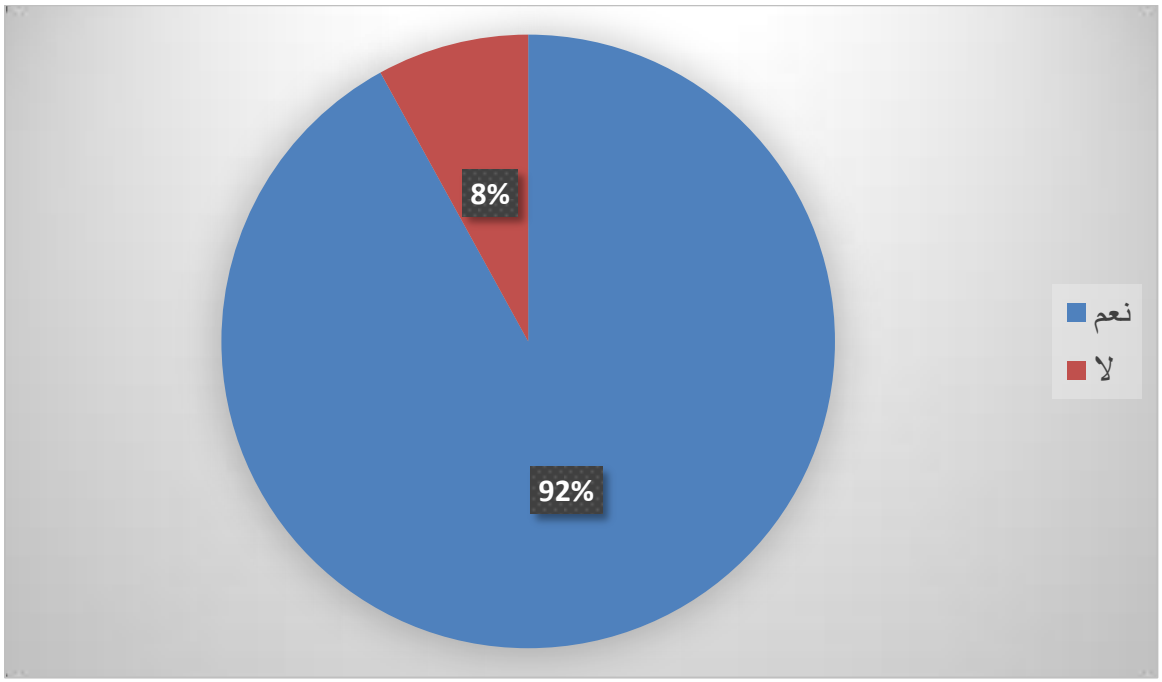
كما أن نسبة 3% بتكرار 4 مرات وهي نسبة جد قليلة يرون الوعي الرقمي وحده ليس كافيا للحد من الجرائم الالكترونية بسبب تعقيد وتطور هذه الجرائم بشكل مستمر . على الرغم من أهمية الوعي

الرقمي في تعليم الطلبة كيفية حماية أنفسهم من بعض التهديدات أو الهجمات ،الى أن الجرائم تتطلب إجراءات متعددة الأبعاد لمكافحتها بفعالية كمواكبة أساليب الهجوم الجديدة التي يعتمدها المجرمون و التقنيات المتقدمة مثل الذكاء الإصطناعي والتعليم الآلي .

الجدول رقم 15: يمثل فعالية القوانين في التقليل من الجرائم الالكترونية:

فعالية القوانين في التقليل من الجريمة الإلكترونية	التكرار	النسبة
نعم	110	%92
لا	10	%8
المجموع	120	%100

الشكل رقم 15 يمثل فعالية القوانين في التقليل من الجرائم الالكترونية



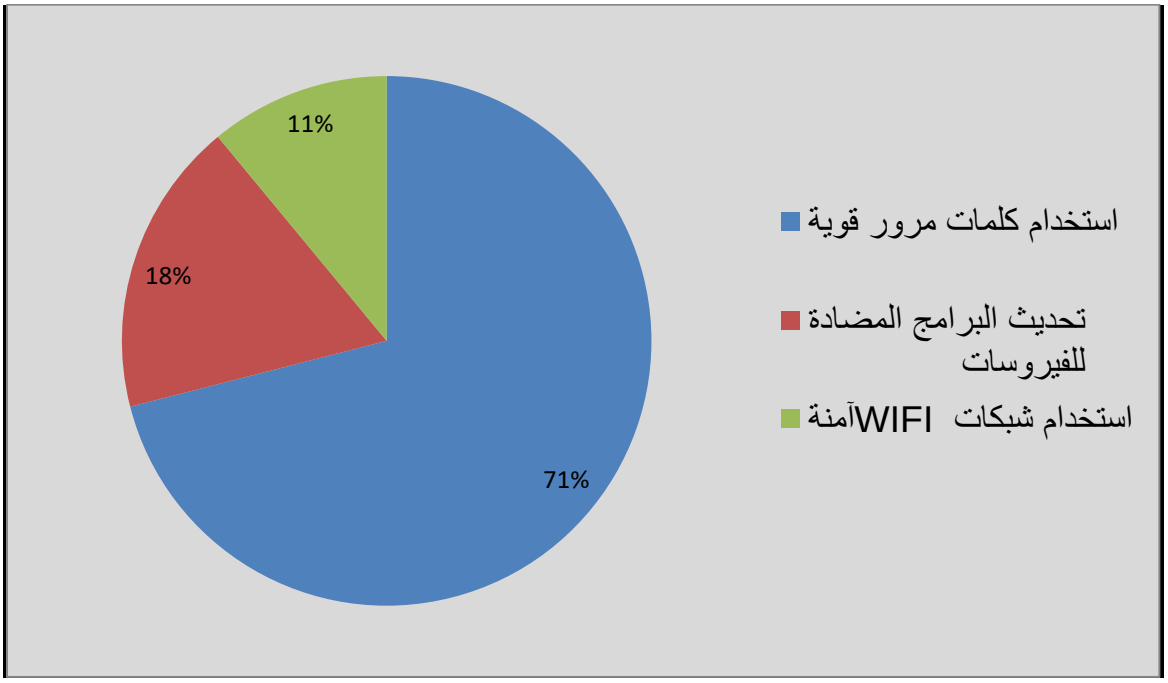
يظهر الجدول رقم 15 دور تحديث القوانين المتعلقة بالجرائم الالكترونية في التقليل من جرائم الحاسوب، حيث فاقت نسبة 92% بتكرار 110 مرة تؤكد ضرورة تحديث القوانين المتعلقة بالجرائم الالكترونية لأنها أصبحت ظاهرة جديرة بالنظر و الإعتبار تخترق المجتمع وتهدد دعائمه وهو ما دعا

إلى سن تشريعات تتماشى مع المستجدات على الساحة الإجرامية ووضع نصوص وقوانين مشددة واضحة فيها عقوبة الجاني وتفسير هذه التشريعات وشرحها للحد منها والتقليل من آثارها وزيادة الوعي بمخاطر هذه الجريمة وتحديد لكل فعل منها جزاء، وبأخذ الحذر والحيطة في الإستخدام .في حين أن نسبة 8% بتكرار 10 ترى بأنها جرائم صعبة الإثبات لأن الجاني لا يترك أي آثار يمكن أن يستدل عليه من خلالها ، هذا ما يصعب على المحققين الكشف عن هاته الجرائم وإلقاء القبض على مرتكبيها و للتعرف أكثر على الآليات والإجراءات التي تتخذ للكشف عن هذه الجريمة .

الجدول رقم 16: يمثل الإجراءات الأمنية للوقاية من الجرائم الالكترونية:

الإجراءات الأمنية لحماية الطلبة	التكرار	النسبة
استخدام كلمات مرور قوية	85	%71
تحديث البرامج المضادة للفيروسات	22	%18
استخدام شبكات WIFI آمنة	13	%11
المجموع	120	%100

الشكل رقم 16 يوضح الإجراءات الأمنية للوقاية من الجرائم الالكترونية



يبين الجدول رقم 16 الإجراءات الأمنية التي يتخذها طلبة جامعة المدية بقسم علوم الاعلام والاتصال لحماية أنفسهم من الجرائم الالكترونية : بداية بأعلى نسبة 71% بتكرار 85 مرة الخاصة بإجراء استخدام كلمات مرور قوية، يأتي بعدها إجراء تحديث البرامج المضادة للفيروسات بنسبة 18% بتكرار 22 مرة، يليها اجراء استخدام شبكات WIFI آمنة بنسبة تقدر بـ 11% بتكرار 13 مرة.

إذن، ومن خلال ماسبق يمكن ان نستنتج ان المبحوثين يستخدمون كلمات مرور قوية والتي تحتوي على مجموعة متنوعة من الاحرف الكبيرة والصغيرة والأرقام والرموز وتكون طويلة بما يكفي، وعدم مشاركتها مع أي شخص آخر لتأمين حساباتهم والوقاية من الجرائم الالكترونية، كذلك تحديث برامج .مضادة للفيروسات مثل "Avast free Antivirus" إذ يعتبر واحدا من برامج مكافحة الفيروسات المجانية الأكثر استخداما، وفي الأخير استخدام شبكات WIFI آمنة وعدم استخدام شبكات مفتوحة مثل التي يجدها في الأماكن العامة مثل المقاهي فإنه يمكن للمهاجمين الالكترونيين استخدام هذه الفرصة للوصول غير مصرح إلى جهازهم وبياناتهم الشخصية.

ثالثا: عرض الإستنتاجات العامة والجزئية للدراسة:

1-الإستنتاجات الجزئية :

قد توصلنا من خلال هذه الدراسة التي تتمحور حول استخدامات الشباب الجامعي للفضاء السيبراني ومخاطر الجريمة الالكترونية إلى جملة من النتائج نحاول من خلالها الإجابة على الإشكالية والتساؤلات المطروحة في الدراسة:

- **المحور الاول :ممارسة الجريمة الإكترونية في موقع الفيسبوك .**

*أجمع افراد العينة المبحوثة على أن جريمة القرصنة الإلكترونية من أكثر الجرائم التي يتعرض لها الطلبة بنسبة 47% تلتها جريمة القذف والتشهير بنسبة 24%.

* أظهرت الدراسة أن الروابط المشبوهة من أبرز الوسائط التي تتم عن طريقها إرتكاب الجريمة الإلكترونية وذلك ما تعكسه نسبة 59% ويليها البريد الالكتروني بنسبة 21%.

*نستنتج أن الانعكاس الذي ينتج عن التعرض للجريمة الالكترونية يعود بشكل كبيرالى التضرر بالسمعة بنسبة 44% يليها سرقة الهوية بنسبة 37%.

*تبين لنا أن أغلبية طلبة قسم علوم الاعلام والاتصال بجامعة المدية لم يتعرضوا لأي جريمة إلكترونية بنسبة 77% ونسبة 32% قد تعرضو للبعض منها كالاختراق و التحرش الجنسى.

المحور الثاني : العوامل المساعدة على انتشار الجريمة الالكترونية عبر الفيسبوك .

*يتضح لنا أن أكثر أداة يستخدمها الطلبة للولوج الى الفيسبوك هي الهاتف المحمول بنسبة 76% وذلك لكونها أسرع وأسهل اداة كذلك لما تتميز به دون غيرها، تلتها أجهزة كمبيوتر بنسبة 18.%

*دلت نتائج الدراسة أن موقع الفيسبوك أكثر عرضة للجريمة الالكترونية مقارنة بالمواقع الأخرى بنسبة89% كونه اقدم موقع والأكثر انتشارا بين الطلبة، تلتها نسبة11% ترى أن للفيسبوك نفس درجة التعرض مع المواقع الأخرى .

*أكدت نتائج الدراسة أن مدة إستخدام الفيسبوك ليس لها أي علاقة بالتعرض للجريمة الالكترونية بنسبة 64% و انما يرجع السبب لقلة الوعي الرقمي وإنعدام الرقابة على موقع الفيسبوك.

*وضحت الدراسة أن الافصاح عن الهوية على الفيسبوك يزيد من درجة التعرض للجريمة الالكترونية فكان بنسبة 77% ، تليها نسبة 23%يرون بأن الإفصاح لا يزيد من درجة التعرض .

المحور الثالث :سبل مجابهة الجريمة الإلكترونية .

*أثبتت الدراسة أن تفقد البيانات الشخصية على الفيسبوك يقلل من التعرض للجريمة الالكترونية بنسبة 91% .

*كشفت الدراسة أن الوعي الرقمي يساهم في مكافحة الجرائم الالكترونية بنسبة97.%

*أظهرت الدراسة أن تحديث القوانين المتعلقة بالجرائم الالكترونية يساهم في التقليل منها بنسبة 92.%.

* تبين لنا أن أكثر إجراء أمني يتخذه الطالب لحماية نفسه من جرائم المعلوماتية هو استخدام كلمات مرور قوية بنسبة71%، يليها إجراء تحديث البرامج المضادة للفيروسات بنسبة 18%.

2- الاستنتاجات العامة :

*أظهرت نتائج الدراسة أن فئة الإناث في أفراد عينتنا أكثر من الذكور وهذا بنسبة 64% مقابل 36 % للذكور وذلك لأن المجتمع الجزائري تغلب فيه فئة الإناث وإقبال الإناث على تخصص إعلام و إتصال.

*بينت نتائج الدراسة أن أغلب أفراد العينة يتراوح سنهم من 21-30 سنة بنسبة 77% وهي الفئة الشبابية.

*دلت الدراسة أن أغلب أفراد العينة من طلبة المستوى التعليمي ماستر بنسبة 55%.

*كشفت الدراسة أن تخصص إعلام للسنة الثالثة ليسانس بنسبة 45% هو التخصص الغالب على عينة الدراسة.

*أكدت نتائج الدراسة أن اختراق الحساب الشخصي من أكثر الجرائم شيوعا بين الطلبة عبر موقع الفيسبوك بنسبة 47% و إستخدامها للوصول لحسابات أخرى مرتبطة بالطالب مثل البريد الإلكتروني .

* كشفت نتائج الدراسة أن الروابط المشبوهة من أكثر الوسائط التي يتم عن طريقها إرتكاب الجريمة الالكترونية بنسبة 59%، إذ تحتوي هذه الروابط على برامج ضارة تثبت على جهاز المستخدم دون علمه يمكن أن تشمل على فيروسات أو برامج تجسس تقوم بسرقة المعلومات الشخصية أو التحكم في الجهاز.

* بينت نتائج الدراسة أن الانعكاس السلبي للجريمة الالكترونية هو التضرر بالسمعة بالدرجة الاولى بنسبة 44% بتسريب ونشر صور و فيديوهات ومحادثات خاصة تحتوي على معلومات حساسة أو محرجة، أو إستخدام حسابات الطالب لنشر محتوى غير لائق أو مسيء مما يؤدي إلى التضرر بسمعته بين عائلته و أصدقائه .

*وضحت نتائج الدراسة أن معظم المبحوثين لم يتعرضوا لأي جريمة الكترونية بنسبة 77%، لإمتلاكهم مزيج من الوعي ، التعليم ، والتقنيات الحديثة التي توفر حماية فعالة ضد معظم الهجمات الالكترونية.

* أظهرت نتائج الدراسة أن معظم المبحوثيين يستخدمون أجهزة الهاتف المحمول لدخول لموقع الفيسبوك بنسبة 76% ،لانها خفيفة الوزن وسهلة الحمل ومتاحة في أي وقت وأي مكان .

* تشير نتائج الدراسة أن موقع الفيسبوك من أكثر المواقع تعرضا للجريمة الالكترونية مقارنة بمواقع التواصل الاجتماعي الاخرى بنسبة 89% ، فهو يحتل أكبر قاعدة من المستخدمين كما يسمح بإستخدام تطبيقات طرف ثالث ، مما يمكن أن يفتح ثغرات أمنية إذا لم تكن هذه التطبيقات آمنة.

* تأكد نتائج الدراسة أن مدة إستخدام الفيسبوك ليس لها علاقة بتعرض الطالب للجريمة الالكترونية بنسبة 64% ، لان مدة إستخدام فيسبوك ليست العامل الرئيسي الذي يحدد تعرض الطلبة للجرائم الالكترونية .

* بينت نتائج الدراسة أن الإفصاح عن الهوية على موقع الفيسبوك يزيد من درجة التعرض للجريمة الالكترونية بنسبة 77% ،لان الإفصاح عن الهوية الشخصية يزيد بشكل كبير من درجة التعرض .عندما يشارك الافراد معلومات حساسة مثل الأسماء الكاملة ،تواريخ الميلاد ، العناوين وغيرها ...يصبح من السهل إستغلال هذه البيانات لإرتكاب جرائم متنوعة.

* وضحت نتائج الدراسة أن تفقد البيانات الشخصية على موقع الفيسبوك يقلل من التعرض لجرائم المعلوماتية بنسبة 91% فمن خلال مراجعة الطلبة لبياناتهم بانتظام يمكن الكشف عن التغييرات الغير عادية أو النشاطات المشبوهة بشكل سريع.

* تشير نتائج الدراسة أن الوعي الرقمي لدى الطلبة يساهم في مكافحة الجرائم الالكترونية بنسبة 97% من خلال تعزيز السلوك المسؤول مثل توخي الحذر عند فتح رسائل البريد الالكتروني والمرفقات الغير معروفة وتعلم ممارسات الامان السليمة لحماية أنفسهم .

* أظهرت نتائج الدراسة أن تحديث القوانين المتعلقة بالجرائم الالكترونية بإمكانها الحد منها بنسبة 92% لان تحديث القوانين يسمح بفرض عقوبات رادعة والحرص على التطبيق الفعال للقوانين الجديدة التي تثني المجرمين عن إرتكاب جرائمهم .

* تشير نتائج الدراسة المتعلقة بالإجراءات الامنية التي يستخدمها الطلبة لحماية أنفسهم من الجرائم الالكترونية أن إستخدام كلمات مرور قوية بنسبة 71% هو الإجراء الاكثر تداولا بينهم ، لانها بمثابة خط الدفاع الاول ضد المتسللين و الهجمات الالكترونية ، كلما كانت كلمات المرور قوية زادت صعوبة إختراق الحساب و الوصول على البيانات.

خاتمة

خاتمة

في ختام دراسة استخدمات الفضاء السيبراني من قبل الشباب الجامعي ومخاطر الجرائم الالكترونية يتضح أن التكنولوجيا أصبحت جزءا لا يتجزأ من حياتهم اليومية والتي تحمل في طياتها مجموعة من المخاطر كالجرائم الإلكترونية عبر موقع الفيسبوك المتمثلة في القرصنة والقذف والتشهير و التحرش الجنسي وغيرها من الجرائم الاخرى وهذا ما يهدد خصوصية وأمن الطلبة.

ومن خلال تحليلنا الكمي والكيفي لمضمون الإستمارة المتمثلة في دراسة مسحية على عينة من طلبة قسم علوم الاعلام و الاتصال بجامعة المدية خلصنا في الأخير الى النتائج العامة والتي تجيب على الاسئلة وقد إستنتجنا بأن جرائم الاختراق هي الاكثر شيوعا بين الطلبة التي تكون بواسطة روابط مشبوهة والذي ينعكس سلبا بتضرر سمعتهم، خاصة وان موقع الفيسبوك من أكثر المواقع إنتشارا فتكثر فيه هذه الجرائم على غرار المواقع الأخرى وذلك بعد الإفصاح عن الهوية الشخصية للطلبة باستخدام اجهزة كالهواتف والكمبيوتر المتصلة بالأنترنت مما يزيد من احتمالية تعرضهم للجرائم. وعلى الرغم من ذلك، فإن معظم الطلاب لم يتعرضوا لأي جريمة لوعيهم بمخاطرها، ومعرفة الدور الذي يلعبه الوعي الرقمي وتحديث القوانين والرقابة في تقليل احتمالية التعرض لهذه الجرائم الالكترونية.

قائمة المصادر و المراجع

قائمة المصار و المراجع

***قرآن الكريم**

المعاجم والقواميس:

صلح الصالح "الشامل، قاموس مصطلحات العلوم الإجتماعية انجليزي .عربي"دارعلم الكتب للطباعة والنشر و التوزيع، ط1، السعودية، 1999.

معجم المعاني الجامع – معجم عربي عربي، دون مكان، دون سنة.

الكتب

1) أحمد بن مرسلي: مناهج البحث العلمي في علوم الإعلام و الإتصال، ديوان المطبوعات الجامعية، الجزائر، ط3، 2007.

2) بشرى حسين الحمداني: القرصنة الإلكترونية أسلحة الحرب الحديثة، دار أسامة للنشر و التوزيع، الأردن عمان، ط1، 2014.

3) بيتر سينجر، دروس الحروب الماضية و اللإتجاهات التكنولوجية المستقبلية، الحروب المستقبلية في القرن الحادي و العشرين، ط 1، مركز الإمارات للدراسات و البحوث الإستراتيجية، 2014، ص83.

4) جعفر حسن جاسم الطائي: جرائم تكنولوجيا المعلومات، دار البداية ناشرون وموزعون، الأردن، ط1، 2007.

5) جلال محمد الزعبي، أسامة أحمد المناعسة: جرائم تقنية المعلومات الالكترونية، دار الثقافة للنشر والتوزيع، الاردن، ط1، 2009.

6) حسن عماد المكاوي، ليلى حسين السييد: الإتصال و نظرياته المعاصرة، ط10 (القاهرة: الدار اللبنانية، د.ت.ط).

7) حمدون توريه: الفضاء السيبراني وتهديد الحرب السيبرانية، البحث عن السلام السيبراني، الإتحاد الدولي للاتصالات، جانفي2011.

8) خالد ممدوح إبراهيم: الجرائم المعلوماتية، دار الفكر الجامعي، مصر، 2009.

9) ختير مسعود: الحماية الجنائية لبرامج الكمبيوتر، أساليب و ثغرات، دار الهدى للنشر و التوزيع، الجزائر، ط2010، ص 100-101.

10) د.خالد يوسف العمار: أبجديات البحث و إعداد الرسائل الجامعية في العلوم النفسية والتربوية و الاجتماعية، دار الإعصار العلمي للنشر والتوزيع، عمان، 2014.

11) د.عبود عبد الله العسكري: منهجية البحث العلمي في العلوم النفسية والتربوية، دار النمير، 2006

12) رشيد زرواتي: منهجية البحث العلمي في البحوث الاجتماعية، دار الكتاب الحديث، ، 2004

13) رمزي منير البعلبكي: المورد الحديث، لبنان، دار العلم الحديث، د.س.

14) عادل عبد الصادق: الفضاء الإلكتروني و تهديدات جديدة للأمن القومي.

15) عامر قنديلجي: البحث العلمي واستخدام مصادر المعلومات، دار اليازوري العلمية للنشر و التوزيع، الاردن، 1999.

16) عامر مصباح: منهجية البحث في العلوم السياسية و الإعلام، ديوان المطبوعات الجامعية، 2008.

17) عبد الغني عماد: منهجية البحث في علم الاجتماع: الإشكاليات، التقنيات، المقاربات، دار الطليعة للطباعة و النشر، ط1، بيروت، 2008.

18) عبد الله عبد الطائي، عبيد: أحكام الفضاء في الفقه الإسلامي، بيروت، دار الكتب العلمية، د ت،

19) علي حسن الشرفي: شرح الأحكام العامة للتشريع العقابي اليمني و فقا لمشروع القانون الشرعي للجرائم و العقوبات، دار المنار، القاهرة، 1993.

20) قمجية حسان أحمد: الفيس بوك تحت المجهر، دار النخبة للنشر والتوزيع، ط1، مصر، 2017.

21) لحسن عبد الله باشيوة، وآخرون، البحث العلمي: مفاهيم–أساليب–تطبيقات، ط1، مؤسسة الوراقة، عمان، 2010.

22) م يانكوف، ل يوتوفا، السيبرنتيك و الإعلام، ترجمة: (برهان العلى)، بيروت، دار الطليعة، ط 1، 1979.

23) محمد إبراهيم: دور التربية في مستقبل الوطن العربي، دار مجدلاوي، عمان، ط1، 2003.

24) محمد الغزالي: هذا ديننا، ط3، القاهرة.

25) محمد شاكر السعيد، خالد بن عبد العزيز الحرفش: مفاهيم أمنية، ط1، جامعة نايف للعلوم الأمنية، الرياض، 2010.

26) محمد علي قطب: الجرائم المعلوماتية و طرق مواجهتها، جزء2، الأكاديمية الملكية للشرطة، مملكة البحرين، 2010.

27) محمد محي الدين عوض: القانون الجنائي مبادئه الأساسية ونظرياته العامة، مكتبة جامعة القاهرة، مصر، 1981.

28) محمد منير حجاب: نظريات الاتصال، القاهرة: دار الفجر، 2010.

29) محمود حسن إسماعيل: مبادئ علم الاتصال و نظريات التأثر، ط1، دار العالمية للنشر و التوزيع، مصر، 2003.

30) محمود محارب: إسرائيل و الحرب الإلكترونية، قراءة في كتاب حرب الفضاء الإلكتروني، اتجاهات و تأثيرات على إسرائيل، سلسلة مراجعة كتب صادرة عن المركز العربي للأبحاث ودراسة السياسات، 2011.

31) نهلة عبد القادر المومني: الجرائم المعلوماتية، دار الثقافة للنشر و التوزيع، الأردن، ط1، 2008،

المجلات العلمية

1) إبتسام رايس: نظرية الاستخدامات و الإشاعات و تطبيقاتها على الإعلام الجديد، النسخة الإلكترونية، مجلد دراسات و أبحاث، العدد25، السنة الثانية، ديسمبر 2016.

2) إبراهيم رمضان إبراهيم عطايا: الجريمة الإلكترونية وسبل مواجهتها في الشريعة الإسلامية و الانظمة الدولية(دراسة تحليلية تطبيقية)، العدد 30، ج2، كلية الشريعة و القانون بطنطا، 2015.

3) إبراهيم قائد أحمد: إستخدامات الطلبة اليمنيين للفيسبوك و الإشباعات المتحققة منه، النسخة الإلكترونية، مجلة دراسات و أبحاث، العدد 26، السنة التاسعة، ديسمبر 2017.

4) أحمد عبيس نعمة الفتلاوي: الهجمات السيبرانية مفهومها و المسؤولية الدولية الناشئة عنها في ضوء التنظيم المعاصر، بحث مقبول للنشر في مجلة المحقق الحلي، العراق، جامعة الكوفة، كلية القانون، 2016.

5) أحمد محمد اللوزي، محمد عبد المجيد الذنيبات: الجريمة الإباحية الإلكترونية كما نظمها قانون الجرائم انظمة المعلومات الكويتي، دراسات علوم الشريعة و القانون، المجلد42، العدد3، 2014.

6) أديب خضور، "السلوك الإتصالي لقرية سورية"، مجلة جامعة الأقصى، المجلد 19، العدد1، 2015.

7) حازم محمد خليل: إستغلال الفضاء السيبراني في الحروب غير التقليدية، دراسة في الوكالة السيبرانية و الإرهاب السيبراني، المجلة العلمية لكلية الدراسات الإقتصادية و العلوم السياسية بجامعة الإسكندرية، العدد الخامس عشر، كلية الإقتصاد و العلوم السياسية جامعة القاهرة، يناير 2023، ص272-274.

8) حسن بن أحمد الشهري: نحو قانون دولي موحد لمكافحة الجرائم المعلوماتية، مجلة دراسات وأبحاث، العدد1، جامعة الجلفة، 2009.

9) د.عبد السلام محمد المايل، د.عادل محمد الشربحي، د.علىقابوسة: الجريمة الإلكترونية في الفضاء الإلكتروني "المفهوم، الأسباب، سبل المكافحة مع التعرض لحالة ليبيا "، مجلة أفاق للبحوث والدراسات سداسية، دولية محكمة، االعدد4، المركز الجامعي ايليزي، 2019.

10) راويه بنت أحمد القحطاني، سعود بن ضحيانالضحيان: "النمطية المنهجية في الرسائل الجامعية"، مجلة كلية الخدمة الإجتماعية للدراسات و البحوث الإجتماعية، العدد عشرون، جامعة الفيوم، ص445.

11) سامي محمد بونيف، دور الإستراتيجياتالإستباقية في مواجهة الهجمات السيبرانية–الردع السيبراني نموذجا–، المجلة الجزائرية للحقوق و العلوم السياسية المجلد04، العدد07، جامعة أحمد بن يحي الونشريسي، 2019.

12) سعيد زيوش، "ظاهرة الإبتزاز الإلكتروني و أساليب الوقاية منها –قراءة سوسيولوجية وأراء نظرية–"، مجلة العلوم الإجتماعية، العدد22، جامعة الشلف، الجزائر، 2017.

13) طلال ياسين العيسى، عدي محمد عناب: المسؤولية الدولية الناشئة عن الهجمات السيبرانية في ضوء القانون الدولي المعاصر، مجلة الزرقاء للبحوث و الدراسات الإنسانية، المجلد 19، العدد1، 2019.

14) عبد الرزاق الديلمي: إستخدامات الشباب الجامعي الأردني لمواقع التواصل الإجتماعي و إشباعاتها، النسخة الإلكترونية، مجلة علوم الإنسان و المجتمع، العدد 12، نوفمبر 2014.

15) فاطمة ميدان "إستخدامات الشباب لوسائل الإتصال الحديثة: دراسة ميدانية في المؤسسة التربوية "، مجلة العلوم الإنسانية، العدد10، 2016.

16) كلير الحلو و آخرون: مواقع التواصل و أثرها على الحالة النفسية للطالب الجامعي، المجلة الدولية للدراسات التربوية و النفسية، المجلد3، العدد2، لبنان، 2018.

17) محمد الصغير كاوجة: الهجمات السيبرانية بين الواقع و سبل المواجهة، مجلة الرسالة للدراسات الإعلامية، مجلد 06، العدد03، سبتمبر2022..

18) مصطفى علي سيد النبي، الإتجاهات الحديثة لنظرية الإستخدامات و الإشباعات، المجلة المصرية للدراسات المتخصصة، العدد23، يوليو 2019.

19) وليد مرزة حمزة المخزومي، ط محمد خزعل عباس: أمن الفضاء السيبراني، قراءة في المفهوم القانوني، مجلة العلوم القانونية، المجلد 37، الجزء الثاني، شباط 2023،.

رسائل جامعية

1) أنديرا عراجي :القوة في الفضاء السيبراني ،فصل عصر من التحدي و الإستجابة ،رسالة لنيل دبلوم دراسات عليا في العلوم السياسية و الإدارية ،جامعة لبنان :كلية الحقوق و العلوم السياسية و الإدارية ،2015-2016.

2) ريحانة بوطي : دوافع إستخدام الشباب للهوية الإقتراضية في الشبكات الإجتماعية و أثرها على الفرد ، رسالة ماجستير ، جامعة الحاج لخضر باتنة .

3) سوير سفيان:جرائم المعلوماتية ،مذكرة لنيل شهادة الماجستير في العلوم الجنائية وعلم الإجرام جامعة أبو بكر بلقايد،تلمسان،2010-2011.

4) صلاح حيدر عبد الواحد : حروب الفضاء الإلكتروني ،دراسة في مفهومها و خصائصها و سبل مواجهتها ،رسالة مقدمة للحصول على درجة الماجستر في العلوم السياسية ، كلية الآداب و العلوم،جامعة الشرق الأوسط،2021،.

5) عبابسة فاروق،عبوبخديجة:القرصنة الإلكترونية وأثرها على المستخدم،مذكرة لنيل شهادة الماستر تخصص إعلام و إتصال،جامعة عبد الحميد ابن باديس مستغانم،2016/2015.

6) عبد الوهاب بوخوفة : التلميذ،المدرسة،المعلم وتكنولوجيا الإعلام و الإتصال ،التمثل و الإستخدامات ،أطروحة دكتوراه ،جامعة الجزائر كلية العلوم السياسية و الإعلام ،2007،.

قوانين و أوامر

1) القانون رقم 09-04،الصادر في 05أوت 2009،يتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام و الإتصالومكافختها، ج ر العدد47.

2) الجريدة الرسمية للجمهورية الجزائرية الديموقراطية الشعبية:مرسوم تنفيذي رقم 98-257مؤرخ في 03جمادى الأولى عام 1419هـ الموافق25أوت 1998م يضبط شروط و كيفيات إقامة خدمات "انترنت "و إستغلالها،العدد63،يوم 26أوت1998.

3) الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية: قانون رقم 04-15مؤرخ في 27رمضان عام 1425هـ الموافق 10 نوفمبر 2004م يعدل و يتمم الأمر رقم -66156المؤرخ في 18 صفر عام 1386هـ الموافق 08يونيو سنة 1966م و المتضمن قانون العقوبات ،العدد71،يوم10نوفمبر 2004م.

4) الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية: مرسوم رئاسي رقم 06-437مؤرخ في 20ذي القعدة عام 1427هـ الموافق 11ديسمبر سنة 2006م يتضمن التصديق على الاتفاق بين حكومة الجمهورية الجزائرية الديمقراطية الشعبية و حكومة الكنفدرالية السويسرية حول التعاون القضائي في المجال الجزائي ،العدد83،يوم20ديسمبر 2006م.

5) الجريدة الرسمية للجمهورية الجزائرية الديمقراطية الشعبية :قرار وزاري مشترك مؤرخ في 26ربيع الاول عام 1428هـ الموافق 14أفريل سنة 2007م،يتعلق بتنظيم الأقسام و المصالح و المخابر الجهوية للمعهد الوطني للبحث في علم التحقيق الجنائي ،العدد36،يوم 03جوان 2007م.

المؤتمرات و الملتقيات :

1) مار مساعدي :مكافحة الاجرام و الإجرام المنظم ،ورقة مقدمة لمؤتمر العمل التطوعي والامن في الوطن العربي ،اكاديمية نايف الرياض،2000،.

2) رابحي لخضر،بنبعلاش خاليدة:معالجة الجرائم المعلوماتية في ظل التعاون الدولي و الإستجابة الدولية ،الملتقى الوطني حول الجريمة المعلوماتية بين الوقاية و المكافحة،16-2015/11/17،جامعة محمد خيضر.

3) عطاء الله فشار:مواجهة الجريمة المعلوماتية في التشريع الجزائري،الملتقى المغاربي حول القانون و المعلوماتية ،أكاديمية الدراسات العليا،ليبيا،أكتوبر 2009.

المواقع الالكترونية:

1) د.عباس مصطفى صادق:صناعة الخبر بين الإعلام التقليدي و الجديد،مؤتمر وسائل التواصل الإجتماعي ،جامعة الإمام محمد بن سعود الإسلامية،كلية الإعلام و الإتصال،أبو ظبي:
www.academid.edu/33451664/

2) د م ، سيبر نتيك، على الموقع : https://m.marefa.org تم الإطلاع يوم : 24-2-2024 ، 21:20 سا .،المركز الجامعي ايليزي،2019.

3) سميرة بيطام : الجريمة الإلكترونية وتقنية الإجرام المستحدث،3أكتوبر 2015.

www.alukah.net ،02/04/2024،22h 45

الملاحق

وزارة التعليم العالي والبحث العلمي

جامعة يحي فارس بالمدية

كلية العلوم الانسانية والاجتماعية

قسم علوم الإعلام والإتصال

إستمارةاستبيانية حول موضوع
استخدامات الشباب الجامعي للفضاء سيبراني ومخاطر الجريمة الإلكترونية.
دراسة مسحية على عينة من طلبة قسم علوم الإعلام والاتصال
-جامعة المدية-
الفيسبوك نموذجا

في إطار إعداد مذكرة تخرج لنيل شهادة الماستر في علوم الاعلام والإتصال –تخصص سمعي بصري- حول موضوع استخدامات طلبة الجامعة للفضاء السيبراني ومخاطر الجريمة الالكترونية. نقدم إليكم هذا الاستبيان ونرجو منكم قراءة مضمونه والاجابة على أسئلته من خلال وضع علامة (X) في المكان المناسب.

كما نحيطكم علما أن معلومات هذه الاستمارة سرية (دون ذكر الاسم واللقب) ولا تستعمل إلا لأغراض علمية.

إعداد الطالبتين: اشراف:

بن صحصاح نور الهدى د. شايب نبيل

بوستة بشرى

الموسم الجامعي 2024/2023

المحور الأول: البيانات الشخصية

1- الجنس:

ذكر ☐ أنثى ☐

2- السن:

من 18إلى 20 ☐ من 21إلى 30 ☐ من 31إلى40 ☐ فما فوق ☐

3- المستوى التعليمي:

ليسانس ☐ ماستر ☐

4- التخصص:

إعلام ☐ سمعي بصري ☐ إتصال وعلاقات عامة ☐

المحور الثاني: ممارسة الجريمة الإلكترونية في موقع الفيسبوك من منظور الطلبة.

5- ماهي أنواع الجرائم الالكترونية التي يتعرض لها الطلبة

إختراق الحساب ☐

القذف والتشهير ☐

الابتزاز والملاحقة ☐

التحرش الجنسي ☐

أخرى أذكرها.....

6- ماهي الوسائط التي يتم عن طريقها ارتكاب الجريمة الالكترونية

موقع ويب ☐

بريد إلكتروني ☐

عبر روابط مشبوهة ☐

أخرى أذكرها.....

7- حسب اعتقادك ما هو الإنعكاس الذي ينتج عن التعرض للجريمة الإلكترونية؟

سرقة الهوية ☐

التلف بجهاز الكمبيوتر أو الهاتف الذكي ☐

تضرر السمعة ☐

أخرى أذكرها.....

8- انت كطالب هل تعرضت سابقا لجريمة إلكترونية؟

نعم ☐

لا ☐

إذا كانت الاجابة نعم حدد نوع الجريمة

.....

المحور الثالث: العوامل المساعدة على إنتشار الجريمة الإلكترونية عبر الفيسبوك من منظور الطلبة

9- ما هي الأداة المستخدمة للولوج إلى الفيسبوك؟

أجهزة كمبيوتر ☐

أجهزة لوحية ☐

هاتف محمول ☐

هل ترى ان هذه الاجهزة تكون سببا للتعرض إلى الجريمة الالكترونية؟

.....

10- هل تعتقد أن الفيسبوك أكثر عرضة للجريمة الالكترونية مقارنة بالمواقع الأخرى؟

نعم ☐

لا ☐

لماذا.....

11- هل مدة استخدامك للفيسبوك تجعلك أكثر عرضة للجريمة الالكترونية؟

نعم ☐

لا ☐

لماذا.....

12- هل الافصاح عن الهوية على الفيسبوك يزيد من درجة التعرض للجريمة الالكترونية؟

نعم ☐

لا ☐

برر لماذا.....

13- هل تعتقد أن تفقد بياناتك الشخصية على موقع الفيسبوك يقلل من درجة التعرض للجريمة الالكترونية؟

نعم ☐

لا ☐

لماذا.....

المحور الرابع: سبل مجابهة الجريمة الالكترونية من منظور الطلبة.

14- هل تعتقد أن الوعي الرقمي يساهم في مكافحة الجرائم الالكترونية؟

نعم ☐

لا ☐

كيف ذلك.....

15- هل تعتقد أن تحديث القوانين المتعلقة بالجرائم الالكترونية يمكن أن يساهم في التقليل من جرائم معلوماتية؟

نعم ☐

لا ☐

وضح ذلك.....

16- ماهي الاجراءات الأمنية التي تتخذها لحماية نفسك من الجرائم الالكترونية؟

استخدام كلمات مرور قوية ☐

تحديث البرامج المضادة للفيروسات ☐

استخدام شبكات wifiأمنة ☐

اخرى أذكرها.....

17- هل لديك أي اقتراحات حول كيفية تعزيز الحماية من الجرائم الالكترونية؟

.....

الفهرس

الفهرس

مقدمة: ..... أ
1)إشكالية الدراسة..... 4
2)تساؤلات الدراسة..... 6
3)أسباب إختيار الموضوع..... 6
4)أهداف الدراسة 6
5)أهمية الدراسة..... 7
6)منهج الدراسة وأداوتها :..... 7
(7مجتمع البحث وعينة الدراسة: 9
8)مفاهيم ومصطلحات الدراسة:..... 10
9)الدراسات السابقة:..... 14
الفصل الأول : مدخل عام للفضاء السيبراني
تمهيد:..... 18
1)مفهوم الفضاء السيبراني:..... 19
2)خصائص الفضاء السيبراني: 21
3)أنواع الهجمات السيبرانية: 23
4)مخاطر الفضاء السيبراني: 24
5)سبل ردع الهجمات السيبرانية: 27
خاتمة الفصل:..... 29
الفصل الثاني : الجريمة الالكترونية : المفهوم ،الخصائص، الأنواع والأهداف
تمهيد..... 31
1)مفهوم الجريمة الإلكترونية:..... 32
2)خصائص الجريمة الإلكترونية:..... 33
3)أنواع الجريمة الإلكترونية:..... 35
3- جريمة الإبتزاز الإلكتروني: 38

4)أهداف الجريمة الإلكترونية: 40
5)سبل مكافحة الجريمة الإلكترونية والتشريعات القانونية : 40
خاتمة الفصل: 48

الفصل الثالث : المقترب النظري للدراسة

تمهيد: 50
1)مفهوم نظرية الإستخدامات و الإشباعات: 51
2)نشأة النظرية: 53
3)فروض النظرية: 54
4)أهداف النظرية: 54
5)إنتقادات النظرية:..... 55
خاتمة الفصل: 56

الإطار التطبيقي

تمهيد: 58
ثانيا: التحليل الكمي والكيفي لبيانات الدراسة : 60
ثالثا: عرض الإستنتاجات العامة والجزئية للدراسة:..... 79
خاتمة..... 84
قائمة المصار و المراجع 86
الفهرس 100