تأثير جرائم الإنترنت على التسوق الإلكتروني بالتطبيق على طلاب جامعة الزقازيق

إعداد

أ. د. وفقى السيد الإمام
أستاذ التسويق
بكلية التجارة – جامعة المنصورة

أحمد رشاد محمد عبد العال
باحث ماجستير
كلية التجارة – جامعة المنصورة

د. عمر أحمد عثمان حجازى
مدرس إدارة الأعمال
بكلية التجارة – جامعة المنصورة

مجلة راية الدولية للعلوم التجارية

دورية علمية محكمة

المجلد (٤) ـ العدد (١٣) ـ يناير ٢٠٢٥

https://www.rijcs.org/

معهد راية العالي للإدارة والتجارة الخارجية بدمياط الجديدة

المنشأ بقرار وزير التعليم العالي رقم ٤٨٩٠ بتاريخ ٢٢ أكتوبر ٢٠١٨ بجمهورية مصر العربية

تأثير جرائم الإنترنت على التسوق الإلكتروني بالتطبيق على طلاب جامعة الزقازيق

إعداد

أ. د. وفقى السيد الإمام
أستاذ التسويق
بكلية التجارة – جامعة المنصورة

أحمد رشاد محمد عبد العال
باحث ماجستير
كلية التجارة – جامعة المنصورة

د. عمر أحمد عثمان حجازى
مدرس إدارة الأعمال
بكلية التجارة – جامعة المنصورة

المستخلص

استهدفتْ هذه الدراسة التعرفَ على تأثير جرائم الإنترنت (التصيد الاحتيالي، القرصنة، البرامج الضارة) على التسوق الإلكتروني لطلاب جامعة الزقازيق،

واعتمدتْ الدراسة على قائمة استقصاء موجهة إلى عينة من طلاب جامعة الزقازيق، وتم جمع البيانات من ٣٩٤ مفردة، وتمَّ تطبيق أسلوب تحليل المسار لاختبار فروض الدراسة عن طريق استخدام البرنامج الإحصائي (Amos V.25). وتوصلتْ الدراسة إلى وجود تأثير لجرائم الإنترنت (التصيد الاحتيالي، القرصنة، البرامج الضارة) على أبعاد التسوق الإلكتروني (الفوائد المدركة، المخاطر المدركة، سهولة الاستخدام، الثقة والأمن). حيث يوجد تأثير معنوي سلبي للتصيد الاحتيالي على الفوائد المدركة وسهولة الاستخدام، ووجود تأثير معنوي إيجابي للتصيد الاحتيالي على المخاطر المدركة، بينما يوجد تأثير غير معنوي للتصيد الاحتيالي على الثقة والأمن. كما يوجد تأثير معنوي سلبي للبرامج الضارة على سهولة الاستخدام، وتأثير معنوي إيجابي للبرامج الضارة على المخاطر المدركة والثقة والأمن، بينما يوجد تأثير غير معنوي للبرامج الضارة على الفوائد

المدركة، وأيضاً يوجد تأثير معنوي إيجابي للقرصنة الرقمية على الفوائد المدركة وسهولة الاستخدام والثقة والأمن، وتأثير معنوي سلبي للقرصنة الرقمية على المخاطر المدركة.

كلمات مفتاحية: جرائم الإنترنت، التصيد الاحتيالي، البرامج الضارة، القرصنة الرقمية، التسوق الإلكتروني.

تمهيد:

يعتبر تثقيف المستهلكين في العصر الرقمي حول التسوق عبر الإنترنت أمراً ضرورياً، حيث يزداد عدد الأشخاص الذين يلجأون إلى الإنترنت لإجراء عمليات الشراء(Mariyappan& Sangeetha, 2024). فلقد تغيرت سلوكيات ومواقف المستهلكين بشكل كبير نتيجة لتطور الإنترنت، حيث ظهر التسوق الإلكتروني الذي يستخدم الكلمات والصور والفيديوهات لشرح وعرض المنتجات والخدمات على المواقع المختلفة، لذلك يُعتبر التسوق الإلكتروني مستقبل الاقتصاد، وكان لهذا التطور تأثير كبير على التجارة الإلكترونية، بما في ذلك المخاطر التي تؤثر سلبًا على نموها (Ahmed et al. 2022). ويُعد سلوك شراء المستهلكين أحد أهم مجالات الدراسة المرغوبة في مجال التسوق، بهدف فهم ومعرفة أنماط شراء المستهلكين وبالتالي زيادة إيرادات المنظمات وتعزيز نموها، فقد تمكنت المنظمات من خلال قدرتها على التنبؤ بدقة عالية من خلال استخدام عدة تقنيات وأدوات أن توجه السوق العالمية (Kaur et al., 2021).

ولكن في السنوات الأخيرة، شعرت الحكومة والشركات والمستهلكون بالقلق بشأن الشبكات والأنظمة والبنية التحتية لتكنولوجيا المعلومات، فقد أدى الانتشار السريع للإنترنت في شتى المجالات الاقتصادية والسياسية والاجتماعية إلى ظهور نمط إجرامي جديد أثر سلباً على تنمية الاقتصاد (Olivia, 2022). حيث يستخدم العديد من الأشخاص التسوق عبر الإنترنت لتلبية احتياجاتهم، وقد أدى ذلك إلى انتعاش بيئة التجارة الإلكترونية بما تحمله من مخاطر، ويؤثر السلوك الإيجابي للمستهلكين في تخفيف حدة تلك الآثار السلبية (Michels et al., 2022). لذلك، من الضروري توفير أنظمة أمان عالية كأحد الوسائل للتصدي لجرائم الإنترنت، فهناك

٩٨% من المعاملات عبر الإنترنت غير مشفرة، وبذلك قد تتعرض البيانات السرية والشخصية لخطر البرامج الضارة والتصيد الاحتيالي (Reddy et al., 2020).

ومن زاوية أخرى أشار (الهديف وشنيب، ٢٠٢٢) إلى أن جرائم الإنترنت متنوعة ولها أبعاد دولية تتجاوز الحدود الجغرافية، حيث تسهم قلة وعي المستهلكين وغياب اهتمام مؤسسات الدولة بتطبيق القوانين للحد منها في تفاقم المشكلة، حيث يتميز القائمون بهذه الجرائم بالدهاء والمهارات العالية في استخدام الحاسوب بغرض الحصول على مكاسب بطرق غير أخلاقية، وأدت التطورات التكنولوجية إلى انتقال المستهلكين من التسوق التقليدي إلى التسوق الإلكتروني، مما زاد من قلق العديد من المستهلكين بشأن الأمان والموثوقية وحماية معلوماتهم الشخصية، وقد زادت جرائم الاحتيال عبر الإنترنت بشكل كبير نتيجة لذلك (Boskovic& Kaurin, 2020).

ولتحديد فجوة الدراسة قام الباحثون بمراجعة العديد من الدراسات السابقة التي تناولت متغيرات الدراسة. حيث أوضح (DAY, 2024) أن إحدى الفجوات البحثية تكمن في استكشاف الدور الذي تلعبه القرصنة الرقمية في الدراسة الجامعية، خاصة بالنسبة للطلاب الذين قد يعانون من نقص في الموارد المؤسسية ومهارات استرجاع المعلومات، بالإضافة إلى الدخل المتاح لهم. كما تبين أن البحوث السائدة قد أغفلت، إلى حد كبير، التهديدات المحتملة والنتائج غير المرغوب فيها الناتجة عن التحول الرقمي (Halttunen, 2024).

من هذا المنطلق لاحظ الباحثون أن الأبحاث العلمية والدراسات السابقة تناولت العديد من أشكال جرائم الإنترنت وكيفية تأثيرها على التسوق الإلكتروني ولكن مجال البحث لا يزال يحتاج كثير من الدراسات التي توضح طرق الوقاية والحماية منها فى بيئة الوطن العربى بشكل عام والبيئة المصرية بشكل خاص، فجرائم الإنترنت تتطور مع تطور التكنولوجيا ويختلف تاثيرها حسب البيئة. فعلى الرغم من أن قرصنة البرمجيات تُعد مصدر قلق عالمي، فإن مظاهرها تختلف حسب المنطقة، ففي الدول المتقدمة تفرض اللوائح الصارمة لمكافحة القرصنة وحقوق

النشر عقبات كبيرة أمام الحصول على البرمجيات المقرصنة، ومع ذلك يشجع الانتشار الواسع للإنترنت عال السرعة بعض المستخدمين إلى اللجوء إلى مواقع غير مشروعة، كما أن تطبيق قوانين مكافحة القرصنة في المناطق النامية أقل صرامة، مما يجعل الحصول على البرمجيات المقرصنة أكثر سهولة (Iqbal et al., 2024). كما لاحظ الباحثون وجود ندرة في الدراسات العربية والأجنبية التي تناولت الأشكال الثلاثة لجرائم الإنترنت(التصيد الاحتيالي، القرصنة، البرامج الضارة) مع الأبعاد الأربعة(الفوائد المدركة، المخاطر المدركة، سهولة الاستخدام، الثقة والأمن) للتسوق الإلكتروني معًا، مما يجعل من هذه الدراسة محاولة لسد هذه الفجوة البحثية.

وبناء على ما سبق وفي ضوء الفجوة البحثية والدراسة الاستطلاعية(الملحق١) قام الباحثون بصياغة مشكلة الدراسة في: " ما تأثير جرائم الإنترنت على التسوق الإلكتروني لطلاب جامعة الزقازيق؟ " **الأمر الذى ينبثق منه التساؤلات الآتية:**

١- ما تأثير التصيد الاحتيالي كأحد أشكال جرائم الإنترنت على أبعاد التسوق الإلكتروني (الفوائد المدركة، المخاطر المدركة، سهولة الاستخدام، الثقة والأمن) لطلاب جامعة الزقازيق؟

٢- ما تأثير البرامج الضارة كأحد أشكال جرائم الإنترنت على أبعاد التسوق الإلكتروني لطلاب جامعة الزقازيق؟

٣- ما تأثير القرصنة الرقمية كأحد أشكال جرائم الإنترنت على أبعاد التسوق الإلكتروني لطلاب جامعة الزقازيق؟

وللإجابة عن هذه التساؤلات تتبنى الدراسة الحالية مجموعة من الأهداف، والتي تساهم في إضافة علمية للدراسات السابقة وهى:

١- قياس تأثير التصيد الاحتيالي كأحد أشكال جرائم الإنترنت على أبعاد التسوق الإلكتروني (الفوائد المدركة، المخاطر المدركة، سهولة الاستخدام، الثقة والأمن) لطلاب جامعة الزقازيق.

٢- قياس تأثير البرامج الضارة كأحد أشكال جرائم الإنترنت على أبعاد التسوق الإلكتروني (الفوائد المدركة، المخاطر المدركة، سهولة الاستخدام، الثقة والأمن) لطلاب جامعة الزقازيق.

٣- قياس تأثير القرصنة الرقمية كأحد أشكال جرائم الإنترنت على أبعاد التسوق الإلكتروني (الفوائد المدركة، المخاطر المدركة، سهولة الاستخدام، الثقة والأمن) لطلاب جامعة الزقازيق.

أهمية الدراسة: تم تقسيم أهمية الدراسة إلى جانبين هما:

أ- الأهمية العلمية: تساهم هذه الدراسة في سد الفجوة في الدراسات السابقة التي تناولت العلاقة بين جرائم الإنترنت بأنواعها المختلفة والتسوق الإلكتروني، حيث تأتى المساهمة الأولى في معرفة تأثير أنواع جرائم الإنترنت (التصيد الاحتيالي، القرصنة الرقمية، البرامج الضارة)على التسوق الإلكتروني. حيث يُعتبر التصيد الاحتيالي تهديدًا كبيرًا على الإنترنت، لأنه يعتمد على خداع الأشخاص للحصول على معلوماتهم الحساسة، لذا فإن فهم كيفية تأثير ساعات تصفح الإنترنت وعادات الشراء عبر الإنترنت على وعي المستخدم بالأمن السيبراني يمكن أن يساعد في تقليل المخاطر المرتبطة بهجمات التصيد الاحتيالي(Kuraku& Kalla, 2023). ثم المساهمة الثانية في تحديد تأثير أشكال جرائم الإنترنت كمتغير متعدد الأشكال على التسوق الإلكتروني، وذلك فى ضوء الفحص الذي تم للدراسات النظرية والبحوث الميدانية تم تكوين إطار مفاهيمي مبسط لمجموعة العلاقات والروابط التي تربط بين جرائم الإنترنت بأنواعها المذكورة والتسوق الإلكتروني، ثم المساهمة الأخيرة في التعرف على التطورات التكنولوجية وما نجم عنها من تأثيرات تتمثل فى جرائم الإنترنت وتأثيرها على التسوق الإلكتروني لطلاب جامعة الزقازيق، مما يساعد المهتمين والباحثين بدراسة هذه الأنواع من الجرائم.

ب- الأهمية التطبيقية: تتجلى الأهمية التطبيقية لهذه الدراسة في فهم تأثير جرائم الإنترنت على سلوكيات طلاب جامعة الزقازيق ومدى إدراكهم للمخاطر المتعلقة بالتسوق الإلكتروني، كما تسعى إلى دراسة تأثير هذه الجرائم على تسوق الطلاب عبر الإنترنت وتعزيز وعيهم بضرورة اتخاذ احتياطات أمنية، كما تساهم الدراسة أيضًا في تطوير استراتيجيات

توعية فعالة للشركات لتعزيز الثقة في التسوق الإلكتروني والحماية من المخاطر المحتملة. كما تهدف الدراسة إلى مساعدة الباحثين في تحديد أنواع جرائم الإنترنت المرتبطة بالتسوق الإلكتروني، وتطوير إجراءات أمان وحماية للطلاب والقطاع التجاري على حد سواء، كما تركز الدراسة على تحسين أنظمة الدفع الإلكتروني وتطوير تقنيات تشفير البيانات، وتعزيز الوعي بجرائم الإنترنت وأساليب التكنولوجيا المستخدمة في التسوق الإلكتروني لطلاب جامعة الزقازيق، أخيرًا، تسعى الدراسة إلى تمكين الطلاب من اتخاذ إجراءات احترازية عند التسوق عبر الإنترنت، وتحفيز تحسين التشريعات والسياسات الحكومية لمواجهة هذه الجرائم، مما يعزز الأمان والثقة في التسوق عبر الإنترنت.

أولاً: التعريف بالمفاهيم الأساسية للدراسة :

(١) جرائم الإنترنت (Internet crimes): هى سلوكيات غير أخلاقية وغير قانونية تؤثر على الفرد والمنظمات والمجتمع، وتتم من خلال الأجهزة المتصلة بالإنترنت بهدف تحقيق منافع شخصية لمرتكبها، وتتطور هذه الجرائم بتقدم التكنولوجيا وتتنوع بين عدة أشكال منها القرصنة، والبرامج الضارة، والتصيد الاحتيالي، وغيرها، وتؤثر بشكل سلبي على التسوق الإلكتروني. فقد أظهرت نتائج (Elisanti et al., 2024) أن احتمالات وقوع الجرائم الإلكترونية في معاملات الشراء والبيع عبر التجارة الإلكترونية قد زادت بشكل ملحوظ، وذلك بسبب قلة المعرفة، إهدار الأموال، الانجذاب للهدايا المزيفة، ارتفاع معدلات البطالة والفقر، والسياسات الأمنية الحكومية غير الصارمة. وعرف (Rahayu et al., 2021) جرائم الإنترنت بأنها تلك الجرائم التي تُرتكب عبر الإنترنت، وتشمل هذه الجرائم مجموعة واسعة من الأنشطة غير القانونية، بما في ذلك تلك التي تحدث في مجال التجارة الإلكترونية بما في ذلك التسوق الإلكتروني.

وتناولت العديد من الدراسات (Reyns, 2015; Leukfeldt& Yar, 2016; Natadimadja et al., 2020; Kuraku& Kalla, 2023;Neves,2022; Akdemir& Lawless, 2020; Ting et al., 2024; Iqbal et al., 2024; Elisanti et al., 2024) ، ويتفق الباحثون مع دراسة (Reyns,

2015; Akdemir& Lawless, 2020) ويسلط الضوء على ثلاثة أشكال لجرائم الإنترنت وهي(التصيد الاحتيالي، والقرصنة الرقمية، ، والبرامج الضارة) حيث يرى الباحثون أنها أكثر الأشكال شمولاً وإستخدامًا فى الدراسات السابقة، والأكثر ارتباطًا بمفهوم جرائم الإنترنت، والأكثر تناسبًا مع بيئة المجتمع المصرى عامة ولفئة الشباب الجامعى خاصة فقد أظهرت نتائج دراسة (Eze-Michael, 2020) أن أغلب الشباب المتورطين في جرائم الاحتيال عبر الإنترنت أما في مؤسسات التعليم العالى أو تخرجوا منها.

أ- **التصيد الاحتيالي (Phishing):** هو أسلوب احتيالي يتم من خلاله استخدام البريد الإلكتروني، الرسائل النصية، أو مواقع الويب المزيفة لسرقة حسابات المستخدمين والحصول على معلومات شخصية حساسة مثل كلمات المرور والتفاصيل الشخصية، ويتم تمثيل المرسل كشخص أو مؤسسة موثوقة لإقناع الضحية بتقديم المعلومات المطلوبة، مما يؤدي إلى تعرض الأفراد لخطر فقدان البيانات الشخصية والاستخدام غير المشروع لها. حيث تتطور مشهد الأمن السيبراني بشكل مستمر، حيث تظل هجمات التصيد الاحتيالي تهديدًا دائمًا وديناميكيًا في العالم الرقمي(Kuraku& Kalla, 2023). وتستمر مشكلة التصيد الاحتيالي في الزيادة، حيث يتفوق المهاجمون على الجهود المبذولة من الشركات والخبراء والباحثين في تطوير طرق لاكتشاف هجمات التصيد وتحسين مقاومة الأفراد لها، ففي عام ٢٠١٩ وصفته شركة مايكروسوفت بأنه شهد تطورًا ملحوظًا في التصيد الاحتيالي، مع إدخال المهاجمين ابتكارات جديدة في الأساليب التقنية والاجتماعية لجعل الهجمات أكثر فعالية ونجاحًا(Abdelhamid, 2020). وعرف (Natadimadja et al., 2020) التصيد الاحتيالي بأنه نشاط يقوم به المتصيدون من أجل سرقة البيانات الشخصية لمستخدمي الإنترنت، بهدف استخدامها لمصالحهم الشخصية، مثل بيانات المستخدم، وكلمات المرور، والحسابات المصرفية. وبالتالي تأثير التصيد الاحتيالي على الثقة في التجارة الإلكترونية يكون كبيرًا، حيث يشكل تهديدًا للأمان الشخصي ويؤدي إلى تدني مستويات الثقة في المنصات الإلكترونية. حيث أظهرت نتائج (Hussin et al., 2023) أن مستويات الثقة في

التجارة الإلكترونية تكون منخفضة إذا تمكن المحتالون من الوصول إلى المعلومات الشخصية عن طريق التصيد الاحتيالي.

ب- البرامج الضارة (Malware): البرامج الضارة تؤثر سلبًا على التسوق الإلكتروني من خلال سرقة المعلومات الشخصية والمالية مثل بيانات بطاقات الائتمان، وتعطيل مواقع التسوق مما يعوق إتمام المعاملات، كما تسهم في فقدان ثقة المستخدمين في الأمان الإلكتروني وتزيد من القلق حول أمان التسوق عبر الإنترنت، كما أن الشركات قد تواجه أيضًا تكاليف كبيرة تتعلق بتعافي البيانات وتعزيز الأمان، فضلاً عن الخسائر المالية الناتجة عن تلك البرامج الضارة.

وتعرف البرامج الضارة بأنها برامج غير قانونية وغير أخلاقية يتم تصميمها لإلحاق الضرر عمدًا بالأجهزة الإلكترونية، بهدف تحقيق منافع شخصية، وتتسم البرامج الضارة بسلوك ضار يستغل نقاط الضعف المخفية لاختراق الأجهزة، وتشمل الأمثلة عليها فيروسات الكمبيوتر، وأحصنة طروادة، وبرامج التجسس. فالبرامج الضارة هي برامج غير مرغوب فيها وغير أخلاقية يستخدمها مجرمو الإنترنت بشكل متكرر لتحقيق منافع شخصية، وتتميز هذه البرامج بالتطور والتغير المستمر، وقد أدت تقنيات الإخفاء إلى صعوبة اكتشافها، وتمثل متغيرات البرامج الضارة تهديدًا خطيرًا للمستهلكين (Aslan& Yilmaz, 2021). حيث أظهرت نتائج (Oki& Ngotshane, 2021) أن Covid-19 قد أثر بالفعل سلبًيا على الأشخاص وخاصة المتسوق الإلكتروني من خلال زيادة عدد حالات الاحتيال التي تنطوي على جرائم إلكترونية، حيث يمكنها أن تنتشر عن طريق البرامج الضارة مثل الفيروسات أو برامج حصان طروادة أو الفيروسات المتنقلة أو برامج التجسس. وتتزايد معدلات البرامج الضارة بما يشكل خطرًا على مستخدمي المواقع الإلكترنية، حيث تم إجراء العديد من الدراسات حول أساليب الكشف عن هذه البرامج، ومع ذلك، لا تزال هناك صعوبة كبيرة في اكتشافها، فهي تتجاوز بسهولة وحدة التشغيل كجدار حماية وبرامج مكافحة الفيروسات، ويمكنها أيضًا الاختباء باستخدام تقنيات التعتيم المختلفة، وبسبب تعدد أشكالها، لا توجد طريقة واحدة قادرة على كشف كل أنواع البرامج الضارة (Aslan& Samet, 2020). ومما لا شك فيه أن تلك البرامج تؤثر بشكل كبير على المستهلكين أثناء قيامهم بالتسوق

الإلكتروني. حيث يشهد الوضع الحالي لأنشطة الجرائم الإلكترونية يشهد تصاعداً في التهديدات والأحداث المتنوعة، حيث تتضمن هذه الأحداث اختراقات للثغرات الأمنية، وانتهاكات كبيرة للبيانات الشخصية، بالإضافة إلى حالات تسريب المعلومات التي تستهدف مختلف الجهات، بما في ذلك المشاهير والقادة السياسيين، مما يبرز هشاشة الأمان الرقمي في الوقت الحالي، كما تواجه المؤسسات التعليمية تعطيل أجهزة الكمبيوتر الخاصة بالطلاب من قبل المتسللين الذين يطالبون بفدية مالية لإعادة فتح النظام، مما يبرز تأثيرات مدمرة تتركز في تهديدات البرامج الضارة الحديثة (Ijaz et al., 2024).

ج- **القرصنة الرقمية (Digital piracy):** هي عملية غير قانونية تستغل الثغرات في أنظمة الكمبيوتر أو الشبكات للوصول غير المصرح به إلى البيانات الشخصية أو التنظيمية بهدف تحقيق منافع شخصية، مثل تحميل أو نسخ البرمجيات، الفيديو، الموسيقى، أو أي محتوى رقمي آخر محمي بحقوق الطبع والنشر. كماعرف (Day, 2024) القرصنة الرقمية بأنها تمثل سرقة المواد الفكرية المحمية بحقوق الطبع والنشر باستخدام تقنيات الويب، مما يؤثر على الدراسة والبحث الأكاديمي بشكل ملحوظ ويؤدي إلى تغيير مساحات التعلم في الجامعات. فقد شهد التسوق الإلكتروني زيادة كبيرة في قرصنة صور المنتجات، مما يعتبر انتهاكاً لحقوق الملكية الفكرية، ويستغل بعض التجار صور المنتجات المقرصنة كأداة للخداع، مما يؤدي إلى تشجيع المستهلكين على معاملات غير عادلة عبر الإنترنت، فبرغم من جهود الحكومات في تعزيز القوانين، إلا أن سياسات منصات التجارة الإلكترونية غير المنظمة تساهم في استمرار هذه الممارسات الضارة، ويمكن تحسين حماية حقوق المستهلك والملكية الفكرية من خلال تشديد الرقابة على استخدام الصور بشكل غير قانوني وتنظيم سلوكيات شركات التجارة الإلكترونية غير الأخلاقية، مما يسهم في حماية السوق الرقمي وضمان نزاهته (Francisco, 2024).

(٢) التسوق الإلكتروني (Electronic shopping): التسوق الإلكتروني هو شكل من أشكال التجارة الإلكترونية الذي يتيح للمستهلكين شراء السلع والخدمات عبر وسائل إلكترونية مثل

الإنترنت، ويتشابه التسوق الإلكتروني إلى حد كبير مع التسوق التقليدي، إلا أنه يتميز بالراحة والسرعة حيث يمكن للمشترين تصفح ومقارنة المنتجات بسهولة، والشراء بسرعة ودون الحاجة للانتقال بين المتاجر الفعلية، حيث يعرف (Singh, 2019) التسوق الإلكتروني بأنه أسلوب جديد للتسوق ظهر نتيجة للتطورات التكنولوجية المختلفة فهو يشبه التسوق التقليدي ولكن بشكل أكثر فاعلية. وللتسوق الإلكتروني عدة ابعاد تتمثل في (الفوائد المدركة، والمخاطر المدركة، وسهولة الاستخدام، والثقة والأمن). وتناولت العديد من الدراسات (Malhotra& Singh, 2013; Aditya et al., 2020; Iriani& Andjarwati, 2020; Grudicek& Dobrinic, 2021; Meixner et al., 2022; Hlatshwayo, 2022; Soares et al., 2023)، وقد وجد الباحثون أن الأبعاد التي وضعها(Hlatshwayo, 2022;Malhotra& Singh, 2013; Aditya et al., 2020) كانت شاملة في مضمونها ومفهومها، وأكثر تفسيرًا للأبعاد التي وضعها الباحثون الآخرون، والأكثر استخدامًا فى الدراسات السابقة والأكثر ارتباطًا بمفهوم التسوق الإلكتروني، ولمتغيرات الدراسة الحالية، وللبيئة التطبيقية للدراسة. حيث أشار(Malhotra& Singh, 2013) أن هناك أربعة أبعاد رئيسية للتسوق عبر الإنترنت تم اكتشافها تؤثر على تصورات الشباب للتسوق عبر الإنترنت كما يشاهدها الشباب هى الفوائد المدركة، المخاطر المدركة، والثقة المدركة، وسهولة الاستخدام . وفى ضوء ذلك سوف يعتمد الباحثون في هذه الدراسة على الأبعاد التالية:١-الفوائد المدركة ٢- المخاطر المدركة ٣- سهولة الاستخدام ٤- الثقة وأمن المعلومات.

أ- الفوائد المدركة: الفوائد المدركة تشير إلى التصورات الإيجابية التي يحملها المستهلكون حول التسوق عبر الإنترنت، مثل الراحة في الشراء من أي مكان وفي أي وقت، وتنوع المنتجات، وتوفير الوقت والجهد، وإمكانية مقارنة الأسعار بسهولة، والوصول إلى تقييمات وآراء المستخدمين الآخرين حول المنتجات. وعرف (Forsythe et al., 2006) الفوائد المدركة للتسوق عبر الإنترنت بانها التصور الشخصي للمستهلك للربح من التسوق عبر الإنترنت.

ب- المخاطر المدركة: المخاطر المدركة للتسوق الإلكتروني تعرف بأنها المخاوف والقلق الذي يشعر به المستهلكون عند إجراء عمليات التسوق الإلكتروني، وتشمل هذه المخاطر القلق من

التعرض للبرامج الضارة أو التصيد الاحتيالي وغيرها، ووجود مشاكل في جودة المنتج أو الخدمة، ومخاوف من عدم وصول المنتجات أو تأخير الشحن، وهذه المخاوف تؤثر على الثقة والأمن في منصات التسوق الإلكتروني وتؤدي إلى تردد بعض المستهلكين في القيام بالتسوق الإلكتروني. بينما عرف (Ahadiat et al., 2021) المخاطر مدركة بأنها هى التصور أو الوعي بالآثار السلبية المحتملة المرتبطة بموقف أو قرار معين.

ج- **سهولة الاستخدام:** سهولة الاستخدام للتسوق الإلكتروني هى مدى إدراك المستخدم لسهولة وراحة تجربة التسوق عبر الإنترنت، وتشمل هذه السهولة سهولة التنقل في الموقع أو التطبيق، وضوح واجهة المستخدم، سرعة الأداء، سهولة إتمام المعاملات، وجود دعم فعال للعملاء، وتوافق الموقع مع مختلف الأجهزة، وتؤثر سهولة الاستخدام المدركة على رضا المستهلكين وتجربتهم العامة، مما يساهم في تعزيز رغبتهم في العودة لاستخدام المنصة أو التوصية بها للآخرين. كما عرف (Davis, 1989) سهولة الاستخدام المدركة بأنها الدرجة التي يعتقد فيها الشخص أن استخدام نظام معين سيكون خالٍ من المجهود الجسدي والعقلي، حيث تعبر هذه السهولة عن المستوى الذي يعتقد فيه المستخدم أن التكنولوجيا أو النظام يمكن استخدامه بسهولة ودون مشاكل، ويتمثل تكرار الاستخدام والتفاعل المتكرر بين المستخدمين مع النظام في إظهار سهولة الاستخدام، حيث يؤكد النظام الذي يتم استخدامه بشكل متكرر أنه معروف بسهولة تشغيله وفعاليته وسهولة استخدامه من قبل مستخدميه.

د- **الثقة والأمن:** الثقة والأمان في التسوق الإلكتروني هما الشعور بالحماية والاطمئنان الذي يشعر به المتسوق بشأن معلوماته الشخصية والمالية أثناء إجراء عمليات التسوق عبر الإنترنت، مع تأكيد عدم استخدام بياناته بطرق غير أخلاقية أو غير قانونية، بالإضافة إلى الاعتقاد الإيجابي للمتسوق بأن الموقع أو المنصة التي يتعامل معها ستقدم له المنتجات أو الخدمات المعلنة بشكل صحيح وفي الجودة المتوقعة، وستحترم خصوصيته وتعامله بنزاهة وشفافية. فالأمان هو الشعور الذي يشعر به المستهلكون عند استخدام المتاجر عبر الإنترنت عندما

يعلمون أن بياناتهم الشخصية المقدمة للمتجر محمية ولن يتم الوصول إليها من قبل أطراف ثالثة (Strzelecki& Rizun, 2022).

(٣) العلاقة بين متغيرات الدراسة واستنباط الفروض:

(أ)- العلاقة بين جرائم الإنترنت والتسوق الإلكتروني: تتأثر تجربة التسوق الإلكتروني بشكل كبير بجرائم الإنترنت، مثل التصيد الاحتيالي والبرامج الضارة والقرصنة الرقمية، فهذه الجرائم تثير مخاوف بشأن أمان المعلومات الشخصية والمالية للمستخدمين، مما يؤدي إلى ترددهم في استخدام المنصات الإلكترونية، وتسعى الشركات لتعزيز الأمان لحماية بيانات المستخدمين وبناء ثقة أكبر في البيئة الرقمية، مما يساهم في تحسين تجربة التسوق عبر الإنترنت. كما أظهرت نتائج دراسة (Rahayu et al., 2021) أن الجرائم الإلكترونية تسبب أضرارًا كبيرة للمستخدمين، مثل فقدان الوقت والمال والبيانات، واستجاب المشاركون في الدراسة بمعدل ٨٦.٢%، مما يشير إلى أنهم يعتبرون هذه الجرائم خطيرة، ونتيجةً لهذه المشكلات، انخفضت الثقة في التجارة الإلكترونية بما في ذلك التسوق الإلكتروني وفقًا لردود المشاركين التي سجلت ٧٣.٨%، ويبدو أن مستخدمي التجارة الإلكترونية لا يثقون في الأمان والمصداقية في هذا المجال. ومن هذا المنطلق، هدف (Toso et al., 2023) إلى قياس مستوى الوعي بجرائم الإنترنت بين طلاب المرحلة الثانوية في جامعة ميساميس، وأظهرت نتائج الدراسة أن الطلاب يمتلكون درجة عالية من المعرفة والفهم حول بعض جرائم الإنترنت مثل القرصنة والتصيد الاحتيالي والتنمر، إلا أن معرفتهم بأنواع أخرى قد تكون محدودة. كما أظهرت نتائج (Garcia et al., 2023) أن خبرة المتسوقين مع إنستغرام كأحد مواقع التسوق الإلكتروني أثرت على قدرتهم في التمييز بين الإعلانات الاحتيالية والإعلانات الشرعية، ومع ذلك لم يكن المستخدمون الأكثر تكرارًا لاستخدام إنستغرام أقل عرضة للإعلانات الاحتيالية من المستخدمين الأقل تكرارًا، فلم تؤثر تقنيات التدريب الحالية على تقييم المشاركين للإعلانات الاحتيالية والشرعية، ويشير ذلك إلى أن الخبرة مع المنصة لا تكفي وحدها للحماية من الإعلانات الاحتيالية، وأن هناك حاجة لتطوير استراتيجيات تدريبية أكثر فعالية. كما أظهرت دراسة (Rezk et al., 2017) أن جرائم الإنترنت تؤثر على التجارة

الإلكترونية، وتوصلت النتائج إلى أن الوقوع ضحية للجريمة الإلكترونية ليس فقط له تأثير سلبي على التجارة الإلكترونية، ولكن الخوف من الجريمة الإلكترونية يجعل المستخدمين لا يثقون في التجارة الإلكترونية لإكمال عملية الشراء. بينما أظهرت نتائج (Buil-Gil et al., 2021) أن الجرائم الإلكترونية زادت خلال تفشي فيروس كورونا (كوفيد-١٩)، وكانت كبيرة بشكل ملحوظ مع سياسات وإجراءات الإغلاق الأكثر صرامة، خصوصًا الزيادة الكبيرة في عدد الجرائم المرتبطة بالتسوق الالكتروني و المزادات عبر الإنترنت، واختراق وسائل التواصل الاجتماعي بالبرامج الضارة والتصيد الاحتيالي، وهما أكثر فئات الجرائم الإلكترونية شيوعًا في المملكة المتحدة، وركزت تلك الجرائم على الأفراد أكثر من المؤسسات. بينما تناول (Siahaan& Nasution, 2018) ظاهرة جريمة الإنترنت وضحايا الاحتيال في المتجر الإلكتروني، وتوصل إلى أن الجرائم الإلكترونية تؤثر على الأمن القومي وثقة المستهلك و ينتج عنها خسائر مالية. فقد أشارت العديد من الدراسات أن الجرائم الإلكترونية والأضرار بالضحايا مرتبطين ارتباطًا وثيقًا(Bossler& Holt, 2009).

(ب)- العلاقة بين التصيد الاحتيالي و أبعاد التسوق الإلكتروني: التصيد الاحتيالي يؤثر على أبعاد التسوق الإلكتروني من خلال زيادة المخاوف المتعلقة بالأمان، مما يقلل من الفوائد المدركة، ويصعب عملية الاستخدام، ويضعف الثقة في منصات التسوق، هذه التأثيرات تجعل تجربة التسوق عبر الإنترنت أقل أماناً وموثوقية بالنسبة للمستخدمين. بينما هدف (Kuraku& Kalla, 2023) إلى تعزيز الوعي بالأمن السيبراني وتقليل مخاطر التصيد الاحتيالي من خلال فهم العلاقة بين عادات تصفح الإنترنت ووعي الأمان وتأثير عادات الإنفاق عبر الإنترنت والوقت الذي يقضيه الأفراد في التصفح على وعيهم بهجمات التصيد الاحتيالي، وأظهرت الدراسة أن الأفراد الذين يقضون وقتاً أطول على الإنترنت يكونون أكثر عرضة للتصيد الاحتيالي، حيث غالباً ما يقع هؤلاء الأفراد ضحايا للتكتيكات الخادعة التي يستخدمها المحتالون، كما أظهرت النتائج أن الأفراد الذين يتبنون عادات إنفاق أكثر مسؤولية وسلوكيات واعية بالأمن قدرة أفضل على

التعرف على محاولات التصيد الاحتيالي وإيقافها بفعالية. أظهرت نتائج (Aribake& Mat Aji, 2020) أن هناك تأثيرًا إيجابيًا كبيرًا بين المخاطر المدركة لمستخدمي الخدمات المصرفية عبر الإنترنت و التصيد الاحتيالي في القطاع المصرفي. تشير نتائج الدراسة إلى أن المخاطر المدركة تؤدي إلى زيادة التعرض لهجمات التصيد الاحتيالي؛ فكلما زاد ميل الأفراد إلى المخاطرة، زادت فرص تعرضهم لهذه الهجمات (Abdelhamid, 2020). كما أظهرت نتائج (De Kimpe et el., 2018) أن التصيد الاحتيالي يؤثر على أمن وثقة الشراء عبر الإنترنت، كما أظهرت النتائج انه لا ينبغي اعتبار استهداف التصيد الاحتيالي بمثابة حجة ضد الشراء عبر الإنترنت، بل كعلامة تحذيرية لمستخدمي الإنترنت الذين يشترون المنتجات او الخدمات عبر الإنترنت بانتظام. كما أظهرت نتائج (Perrault, 2018) أن ما يقرب من ٤ من كل ١٠ طلاب الذين شملتهم الدراسة لا يعرفون ما هو التصيد الاحتيالي ولا التهديدات التي يشكلها، كما أن الطلاب يبالغون في تقدير ثقتهم وأمانهم في التعرف على محاولات التصيد الاحتيالي ويقللون من تقدير احتمالية تعرضهم للهجوم. وبناءً على ما سبق من الدراسات، يتوقع الباحثون وجود علاقة بين التصيد الاحتيالي وأبعاد التسوق الإلكتروني، حيث يمكن صياغة فرض الدراسة الرئيسي الأول كالتالي:

H1: يوجد تأثير معنوي للتصيد الاحتيالي كأحد أشكال جر ائم الإنترنت على أبعاد التسوق الإلكتروني.وينقسم هذا الفرض إلى الفروض الفرعية التالية:

H1/a: يوجد تأثير معنوي للتصيد الاحتيالي على الفوائد المدركة.

H1/b: يوجد تأثير معنوي للتصيد الاحتيالي على المخاطر المدركة.

H1/c: يوجد تأثير معنوي للتصيد الاحتيالي على سهولة الاستخدام.

H1/d: يوجد تأثير معنوي للتصيد الاحتيالي على الثقة والأمن.

(ج)- العلاقة بين البرامج الضارة و أبعاد التسوق الإلكتروني: البرامج الضارة تؤثر بشكل كبير على التسوق الإلكتروني من خلال زيادة مخاطر وتهديدات الأمان والخصوصية، مما يقلل من ثقة المستخدمين في المواقع الإلكترونية، كما تؤثر على تجربة التسوق بتسببها في بطء الأداء وتداخلات مزعجة، ولمواجهة هذه التهديدات، قد تتخذ المنصات الإلكترونية إجراءات أمان قد

تعقد عملية التسوق، مما يؤثر سلبًا على سهولة الاستخدام، في الوقت نفسه يعزز الوعي بالبرامج الضارة من تبني المستخدمين لممارسات أمان أفضل، مثل استخدام برامج مكافحة الفيروسات. كما تناولت دراسة (Strzelecki& Rizun, 2022) أهمية حماية بيانات المستهلكين وتأثير الحوادث الأمنية الناتجة عن البرامج الضارة على الثقة وسلوك التسوق عبر الإنترنت، وأظهرت النتائج انخفاضًا كبيرًا في ثقة المستهلكين تجاه متجر Morele.net بشكل خاص، حيث تراجعت الثقة بشكل ملحوظ بعد حادث اختراق البيانات، ومع ذلك لم يؤثر هذا التراجع على مواقفهم وثقتهم تجاه التسوق عبر الإنترنت بشكل عام، فقد قرر واحد من كل ثلاثة مستهلكين تأثروا بالحادث التوقف عن التسوق عبر هذا الموقع، ومع ذلك لم يغيروا سلوكهم في التسوق عبر الإنترنت بشكل عام، بل انتقلوا إلى متاجر إلكترونية أخرى، كما أظهرت النتائج أن الحادث أدى إلى زيادة وعي المستهلكين بأهمية أمان وحماية بياناتهم، حيث أصبحوا أكثر حذرًا في تقديم بياناتهم لأي موقع ويب بعد الحادث. كما هدفت دراسة (Hlatshwayo, 2022) إلى التحقق من مدى تأثير المخاطر المدركة والثقة والمخاطر الأمنية على سلوك التسوق عبر الإنترنت من منظور جنوب إفريقي في ظل مخاطر الأمن السيبراني، وتؤكد نتائج الدراسة إلى أهمية الثقة والأمان في التسوق عبر الإنترنت قد تزيد بشكل ايجابي من وعي المستخدمين حول أهمية الحماية من البرامج الضارة، كما يمكن أن يدفع هذا الوعي الأفراد إلى تبني ممارسات أكثر أمانًا، مثل تثبيت برامج مكافحة الفيروسات وتحديثها بانتظام، ايضاً معرفة أن المستهلكين يهتمون بالأمان قد تشجع الشركات على تعزيز إجراءات الأمان الإلكتروني، وهذا قد يشمل استخدام تقنيات التشفير الأقوى وتطبيقات الحماية ضد البرامج الضارة، كما توضح الدراسة أن المخاطر المدركة تؤثر على سلوك التسوق عبر الإنترنت، فقد تؤدي إلى زيادة ايجابية على وعي المستهلكين حول التهديدات الأمنية، بما في ذلك البرامج الضارة، وهذا الوعي يمكن أن يشجعهم على اتخاذ احتياطات أمان أكثر صرامة، كما توضح أن تطبيق إجراءات أمان مشددة لحماية الموقع من البرامج الضارة مثل طلبات التحقق المفرطة أو إجراءات الأمان المعقدة يعيق سهولة الاستخدام

للتسوق عبر الإنترنت، قد يتسبب ذلك في تجربة تسوق أقل سلاسة للمستخدمين، مما يؤثر سلبًا على رضاهم واستمرارهم في استخدام المنصات الإلكترونية، أخيرًا توثر الفائدة المدركة إيجابي على مواقف التسوق عبر الإنترنت (SA). كما تُشير نتائج دراسة (Balapour et al., 2020) إلى أن المخاطر المدركة للخصوصية تؤثر سلبًا على تصورات الأمان في ظل وجود البرامج الضارة لتطبيقات الهواتف المحمولة، مما يزيد من المخاطر المدركة مع تزايد البرامج الضارة، كما تعزز هذه المخاطر وعي المستخدمين بأهمية الأمان الشخصي، مما يدفعهم إلى اتخاذ خطوات إضافية لحماية أنفسهم، وبالتالي ازدياد البرامج الضارة يزيد من حذر وتحوط المتسوقين بشأن معلوماتهم الشخصية عند التسوق عبر الإنترنت. بينما تناول (Hariharan et al., 2023) تصورات المستهلكين للأمان والخصوصية والثقة نتيجة للهجمات الإلكترونية على المنصات الرقمية وتأثيرها على سمعة المؤسسات ضمن الاقتصاد الرقمي، و أظهرت النتائج أن حوالي ٨٢% من المشاركين أعربوا عن أن مخاوف الخصوصية كانت الأكثر تأثرًا بسبب الهجوم الإلكتروني، حيث أن المستهلكين غير المخلصين كانوا أكثر قلقًا بشأن الأمان بنسبة تصل إلى ١٠% عند الشراء من المواقع الإلكترونية، بينما المستهلكين المخلصين تأثروا عاطفيًا أكثر بنسبة تصل إلى ١٣% مقارنة بغير المخلصين، ونتيجة للهجمات الإلكترونية بما في ذلك تلك التي تتضمن برامج ضارة، يزيد وعي المستهلكين بأهمية حماية بياناتهم الشخصية، فهذا الوعي يعزز اهتمامهم بتحسين الأمان الشخصي، مما يساهم في تعزيز إجراءات الأمان وحماية البيانات، كما ان الهجمات الإلكترونية بما في ذلك البرامج الضارة تجعل المستهلكين أكثر إدراكًا للمخاطر المتعلقة بالأمان والخصوصية، فهذه المخاوف تعزز حرصهم على حماية بياناتهم وتقديرهم لمستوى الأمان في المواقع التي يتعاملون معها. كما أظهرت دراسة (Hassan& Ahmed, 2023) أن المؤسسات تواجه تحديًا كبيرًا في تحقيق توازن بين إجراءات الأمن القوية وسهولة استخدام واجهات المواقع وذلك لتحسين تجربة المستهلكين وحماية بياناتهم الحساسة، إن تحقيق توازن جيد بين الأمان وسهولة الاستخدام يعزز ثقة المستهلكين، فعندما يصبح المستخدمون أكثر وعيًا بأفضل الممارسات الأمنية، فإنهم يصبحون أقل عرضة للهجمات التي تستخدم البرامج الضارة،

مما يزيد الوعي من قدرة المستخدمين على التعرف على التهديدات وتجنب الوقوع في فخ البرمجيات الضارة، فالمستخدمون الذين يثقون بالمنصة يكونون أقل عرضة للابتعاد عنها حتى في حالة وجود تهديدات متزايدة من البرامج الضارة، كما أشارت الدراسة إلى أن تحسين سهولة استخدام واجهة المنصة قد يؤدي إلى تقديم ميزات غير آمنة أو تبسيط إجراءات الأمان بشكل قد يفتح ثغرات يمكن للبرامج الضارة استغلالها، فإذا كانت الواجهة سهلة الاستخدام للغاية دون مراعاة الأمان، فقد تتعرض المنصة للهجمات. كما أشار (Anwar et al., 2021) إن المستهلكون يدركون بعض الفوائد والمخاطر المرتبطة بالتسوق عبر الإنترنت، كما تؤثر المخاطر المدركة سلبًا على سلوك الشراء عبر الإنترنت، مما يجعل المستخدمين أكثر وعيًا بمخاطر البرامج الضارة، فمع زيادة الوعي بالمخاطر المدركة الناتجة عن تزايد هجمات البرامج الضارة، قد يصبح المستهلكون أكثر حذرًا في تعاملهم مع المواقع غير المأمونة، مما يقلل من تعرضهم للبرامج الضارة، وهذا الوعي بالمخاطر يمكن أن يساهم في تعزيز التدابير الوقائية ضد التهديدات المتزايدة للبرامج الضارة، حيث يتخذ المستهلكون خطوات إضافية لتجنب المواقع المشبوهة التي قد تصاب بالبرامج الضارة. وبناءً على ما سبق من الدراسات، يتوقع الباحثون وجود علاقة بين البرامج الضارة وأبعاد التسوق الإلكتروني، حيث يمكن صياغة فرض الدراسة الرئيسي الثاني كالتالي:

H2: يوجد تأثير معنوي للبرامج الضارة كأحد أشكال جرائم الإنترنت على أبعاد التسوق الإلكتروني. وينقسم هذا الفرض إلى الفروض الفرعية التالية:

H2/a: يوجد تأثير معنوي للبرامج الضارة على الفوائد المدركة.

H2/b: يوجد تأثير معنوي للبرامج الضارة على المخاطر المدركة.

H2/c: يوجد تأثير معنوي للبرامج الضارة على سهولة الاستخدام.

H2/d: يوجد تأثير معنوي للبرامج الضارة على الثقة والأمن.

(د)- العلاقة بين القرصنة الرقمية وأبعاد التسوق الإلكتروني: تشير نتائج دراسة (Hoy, 2017) أن التكاليف المرتفعة للمقالات العلمية دفعت العديد من الباحثين إلى استخدام مواقع

"القرصنة" مثل "ساي-هب" (Sci-Hub)، الذي يوفر وصولًا فوريًا لأكثر من ٥٨ مليون مقال، فعلى الرغم من سهولة الاستخدام والفوائد المدركة للحصول على مقالات مجانية، لا يدرك المستخدمون أن هذه المقالات غالبًا ما يتم الحصول عليها بطرق غير قانونية عن طريق القرصنة الرقمية، أيضًا سهولة الوصول والفوائد المدركة تعزز من استخدام هذه المواقع، مما يشجع على مزيد من القرصنة الرقمية، فالمستخدمون يفضلون الواجهات البسيطة والوصول السريع، مما يزيد من تأثير هذه المواقع السلبي على النظم القانونية والأمنية، ويعزز من استخدام القرصنة الرقمية رغم المخاطر القانونية والأمنية، أيضًا تساهم الثقة والامن في هذا الموقع إلى تشجيع المزيد من الأفراد على استخدام هذه المواقع رغم المخاطر القانونية والأمنية، مما يؤدي إلى زيادة القرصنة الرقمية. كما تسلط دراسة (Saeed, 2023) الضوء على أن مخاوف المستهلكين بشأن استخدام بطاقات الائتمان، ومخاوفهم المتعلقة بأمان المعلومات، والعوامل التحفيزية للتسوق التي تقدمها المؤسسات التجارية، وثقة المستهلكين، ومشاعر المستخدمين حول سمعة التجارة الإلكترونية وتأثير ذلك على تصورهم لأمان البيانات عبر الإنترنت وثقتهم في تطبيق التجارة الإلكترونية، وأشارت الدراسة أن عندما يشعر المستهلكين بثقة عالية في أمان المنصات الإلكترونية، قد يقدّمون معلومات شخصية ومالية بشكل أكثر تكراراً عبر الإنترنت، وهذا يمكن أن يزيد من حجم البيانات المستهدفة من قبل القراصنة، حتى مع وجود أمان قوي، فالقراصنة قد يستهدفون هذه المنصات لأنهم يعرفون أن المستخدمين يثقون بها ويقدمون بيانات حساسة، أيضًا زيادة المخاوف المدركة من المخاطر يمكن أن تجعل المستهلكين أكثر حذرًا وتجنبهم التفاعل مع المنصات الإلكترونية غير الآمنة، هذا الحذر قد يقلل من تعرضهم للقرصنة لأنهم يتجنبون التعامل مع المواقع غير المحمية. ومن زاوية أخرى أظهرت نتائج(Hampton-Sosa, 2017) أن الفوائد المدركة وسهولة الاستخدام والثقة والأمان تلعب دورًا مهمًا في الحد من القرصنة الرقمية، عندما يدرك المستهلكون فوائد واضحة من خدمات الاشتراك في الموسيقى، مثل الوصول السهل إلى المحتوى، ويجدون الخدمة سهلة الاستخدام، ويثقون في أمان الخدمة، فإنهم يكونون أقل ميلاً للقرصنة، فتحسين هذه العوامل في خدمات الاشتراك يمكن أن يشجع

على الدفع مقابل المحتوى بدلاً من اللجوء إلى الطرق غير القانونية للقرصنة للحصول على الموسيقى، مما يقلل من انتشار القرصنة الرقمية. وتختلف هذه النتائج مع دراسة (KARAHAN& KAYABASI, 2019) الذى أسفرت عن وجود علاقة ايجابية بين المخاطر المدركة والقرصنة الرقمية، حيث أن الأفراد الذين يدركون المخاطر المرتبطة بالقرصنة الرقمية يكون لديهم موقف أكثر إيجابية تجاهها، والسبب أن الأفراد في تركيا إما يفتقرون إلى المعلومات الكافية حول المخاطر القانونية المرتبطة بالقرصنة الرقمية، أو لا يشعرون بالقلق من العقوبات حتى وإن كانوا يرون أن القوانين المتعلقة بالقرصنة الرقمية قد تكون كافية أو لا، كما أظهرت النتائج ان هناك علاقة سلبية بين الفوائد المدركة والقرصنة الرقمية، فالأفراد في تركيا رغم أنهم يقدّرون فوائد القرصنة الرقمية مثل التوفير والراحة والمتعة، إلا أن هذه الفوائد لا تُعتبر عوامل حاسمة في قراراتهم المتعلقة بالقرصنة الرقمية. من زاوية أخرى أظهرت دراسة (Liao et al., 2010) أن هناك علاقة سلبية بين المخاطر المدركة والقرصنة الرقمية. كما أظهرت دراسة (Yoon, 2011) أن هناك علاقة سلبية بين المخاطر المدركة والقرصنة الرقمية، وأن هناك علاقة إيجابية بين الفوائد المدركة والقرصنة الرقمية. كما أظهرت العديد من الدراسات السابقة إلى وجود علاقة إيجابية بين الفوائد المدركة والقرصنة الرقمية، مما يعني أن الأفراد قد يكونون أكثر ميلاً إلى ممارسة القرصنة الرقمية إذا اعتبروا أنها تقدم لهم فوائد ملموسة (Chiou et al., 2005; Goles et al., 2008; Peace et al., 2003). كما أظهرت دراسة(Ahadiat et al., 2021) تؤثر الفوائد المدركة بشكل إيجابي على القرصنة الرقمية، حيث يميل الأفراد الذين يرون فوائد من هذا السلوك إلى ممارسته، فالعلاقة بين القرصنة الرقمية والمخاطر المدركة هي سلبية، إذ تُقوض المخاطر المدركة المواقف الفردية تجاه القرصنة. هذا يعني أن الأفراد قد لا يأخذون المخاطر بعين الاعتبار عند اتخاذ قراراتهم، مما يقلل من تأثيرها على نيتهم للقرصنة. ومع زيادة المخاطر مثل العقوبات القانونية أو الأضرار المحتملة لأجهزتهم أو بياناتهم، يصبح الأفراد أكثر حذراً وأقل ميلاً للقرصنة الرقمية. كما أظهرت نتائج (Kos Koklic et al., 2016) أن العلاقة بين

القرصنة الرقمية والمخاطر المدركة سلبية، فكلما زاد إدراك الأفراد للمخاطر الشخصية المرتبطة بالقرصنة الرقمية، قل احتمال انخراطهم في هذا السلوك. كما اظهرت دراسة (Alleyne et al., 2015) أن العلاقة بين القرصنة الرقمية والمخاطر سلبية، حيث أن "إدراك خطر العقوبات" يؤثر بشكل كبير على نية الأفراد في الانخراط في القرصنة، مما يعني أن المخاطر المدركة تؤدي إلى تقليل نية الأفراد للقرصنة الرقمية. كما تشير دراسة (Sardanelli et al., 2019) أن المخاطر الأخلاقية والسلوكيات السابقة تلعب دورًا في تقليل استخدام القرصنة الرقمية وتحفيز الدفع للخدمات القانونية، مما يعكس علاقة سلبية بين المخاطر المرتبطة بالقرصنة الرقمية ورغبة الأفراد في استخدام الخدمات القانونية. كما أشار (Jaramillo et al., 2023) أن العلاقة بين القرصنة الرقمية والمخاطر يمكن أن تكون سلبية في سياق تأثير المخاطر المدركة، فالتهديد بالعقوبات يمكن أن يقلل من رغبة الأفراد في ارتكاب القرصنة الرقمية لأنه يزيد من الوعي بالمخاطر والعواقب القانونية المحتملة، لذا يتجلى التأثير السلبي هنا في تقليل احتمالية الانخراط في القرصنة الرقمية بسبب الخوف من العقوبات. وبناءً على ما سبق من الدراسات، يتوقع الباحثون وجود علاقة بين القرصنة الرقمية وأبعاد التسوق الإلكتروني، حيث يمكن صياغة فرض الدراسة الرئيسي الثالث كالتالي:

H3: يوجد تأثير معنوي للقرصنة الرقمية كأحد أشكال جرائم الإنترنت على أبعاد التسوق الإلكتروني.

وينقسم هذا الفرض إلى الفروض الفرعية التالية:

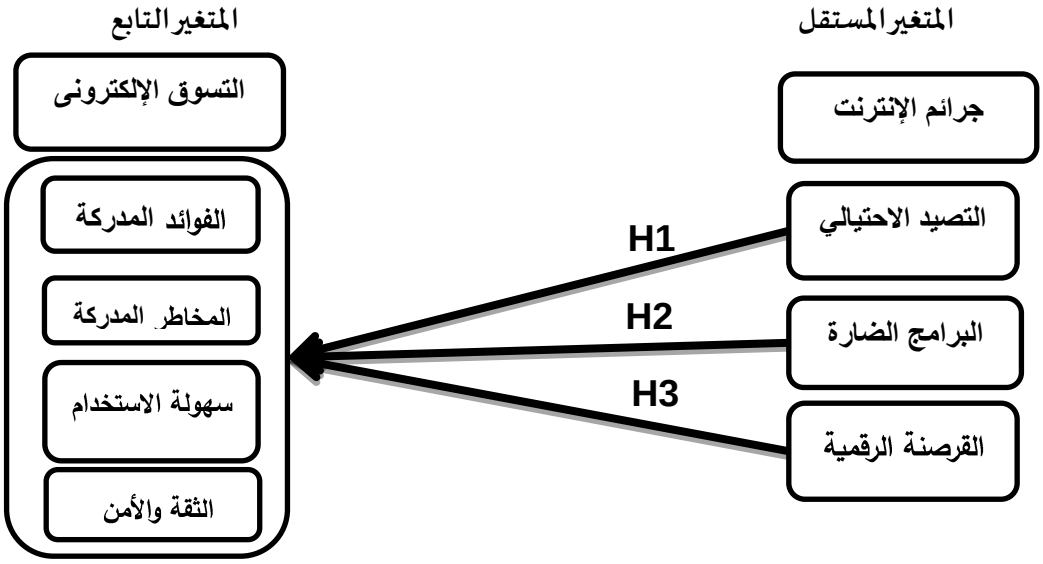
H3/a: يوجد تأثير معنوي للقرصنة الرقمية على الفوائد المدركة.

H3/b: يوجد تأثير معنوي للقرصنة الرقمية على المخاطر المدركة.

H3/c: يوجد تأثير معنوي للقرصنة الرقمية على سهولة الاستخدام.

H3/d: يوجد تأثير معنوي للقرصنة الرقمية على الثقة والأمن.

وتَمَّ تصوير العلاقات المفترضة بين المتغيرات في الإطار المفاهيمي في الشكل رقم (١).



شكل رقم (١/١) الإطار المفاهيمي المقترح للعلاقة بين متغيرات الدراسة

المصدر: إعداد الباحثين.

ثانيًا: منهجية الدراسة:

تم الاعتماد على المنهج الوصفي، ويذكر (الإمام، ٢٠٢٢) أنه أكثر ملاءمة لفهم الظاهرة ومقارنتها وتفسيرها، ومن ثم إجراء التحليل المتعمق الذي يقود الباحث إلى استخلاص العلاقات واقتراح الحلول لمشكلة الدراسة، كما يهتم بتقييم الوضع الحالي من أجل التنبؤ بالمستقبل، فضلاً عن وصف خصائص الظاهرة موضع البحث وتحديد طبيعة العلاقات بين المتغيرات. وقد اعتمد الباحثون هذا المنهج لمناسبته لطبيعة هذه الدراسة. وتتضمن طريقة البحث النقاط التالية:

(١) مجتمع وعينة الدراسة: يتكون مجتمع الدراسة من طلاب جامعة الزقازيق بجمهورية مصر العربية، والبالغ عددهم ١٦٣,٧٠٩ مفردة، وفقاً للموقع الرسمي للجامعة ، ونظرًا لصعوبة إجراء

هذه الدراسة بأسلوب الحصر الشامل لكبر حجم المجتمع، حدد الباحثون حجم العينة على أنه ٣٨٣ مفردة، ويستند هذا الحجم إلى ما تشير إليه الجداول الإحصائية من أن حجم العينة المناسب في حالة ما إذا كان مجتمع الدراسة أكثر من مائة ألف عند معامل ثقة ٩٥% هو ٣٨٣ مفردة (الإمام، ٢٠٢٢). ويعتمد الباحثون على عينة طبقية، حيث سيتم توزيعها طبقيًا على كليات الجامعة لضمان التمثيل المناسب.

(٢) قياس متغيرات الدراسة:

أداة الدراسة التي تم استخدامها في جمع بيانات الدراسة الميدانية من مصادرها الأولية لهذه الرسالة هي قائمة الاستقصاء، والتي تم إعدادها لهذا الغرض، وقد حرص الباحثون على تنظيم عبارات الاستقصاء وترتيبها بشكل منطقي ومراجعتها من حيث اللغة والشكل والمضمون، كما اهتم باختبار الاستقصاء وتحكيمه للكشف عن مدى ملاءمته لتحقيق أهداف الدراسة وتحديد درجة استجابة المستقصى منهم، واكتشاف أي أخطاء في الشكل أو المضمون. وقد اشتملت القائمة على (٣١عبارة) تغطي المتغيرين الرئيسيين للبحث، وتم وضعها على مقياس ليكرت الخماسي / من الموافقة التامة / إلى الرفض التام.

(أ) المتغير الأول (جرائم الإنترنت): وتم قياس هذا المتغير من خلال ثلاثة أشكال وهي: (التصيد الاحتيالي، البرامج الضارة، القرصنة الرقمية)، وقام الباحثون بتصميم مقياس لكل نوع من جرائم الإنترنت كما يلي:

التصيد الاحتيالي: قام الباحثون بالاعتماد على المقياس الموضح في دراسة كلاً من (Neves, 2022; De Kimpe et el., 2018; Reyns,2015; Choi, 2008; Leukfeldt, 2014) وبناءً على هذه المقاييس، قام الباحثون بتصميم مقياس ملائم لمجال الدراسة، ويشمل هذا المقياس (٤) عبارات تم قياس الوزن النسبي لكل منها باستخدام مقياس ليكرت الخماسي.

البرامج الضارة: قام الباحثون بتصميم مقياس ملائم لمجال الدراسة بالاعتماد على المقياس الموضح في دراسة كلاً من (Reyns,2015; Leukfeldt& Yar,2016; Neves, 2022)، ويشمل هذا المقياس (٤) عبارات تم قياس الوزن النسبي لكل منها باستخدام مقياس ليكرت الخماسي.

القرصنة الرقمية: وقام الباحثون بتصميم مقياس للقرصنة الرقمية استنادًا إلى المقياس الموضح في دراسة (Cronan & Al-Rafee, 2008)، وهو من المقاييس الأكثر استخدامًا في الدراسات السابقة التي ثبتت صدقها وثباتها. تم تعديل صياغة بعض العبارات وإضافة وحذف بعض العبارات الأخرى لتتناسب مع عينة الدراسة والبيئة المصرية بناءً على ملاحظات المحكمين، وليصبح المقياس معبرًا بشكل صحيح عن ما يجب قياسه. يشمل هذا المقياس (٤) عبارات تم قياس الوزن النسبي لكل منها باستخدام مقياس ليكرت الخماسي.

(ب)المتغير الثاني(التسوق الإلكتروني): ويتم قياس هذا المتغير من خلال أربعة أبعاد وهي: (الفوائد المدركة، المخاطر المدركة، الثقة والأمن، سهولة الاستخدام). قام الباحثون بتصميم مقياس لكل بعد منها كما يلي:

الفوائد المدركة: قام الباحثون بتصميم مقياس للفوائد المدركة استنادًا إلى المقياس الموضح في دراسة (Forsythe et al., 2006)، وهو من المقاييس الأكثر استخدامًا في الدراسات السابقة التي ثبتت صدقها وثباتها. يشمل هذا المقياس (٥) عبارة تم قياس الوزن النسبي لكل منها باستخدام مقياس ليكرت الخماسي.

المخاطر المدركة: قام الباحثون بتصميم مقياس للمخاطر المدركة استنادًا إلى المقياس الموضح في دراسة (Forsythe et al., 2006)، وهو من المقاييس الأكثر استخدامًا في الدراسات السابقة التي ثبتت صدقها وثباتها، ويشمل هذا المقياس (٥) عبارات تم قياس الوزن النسبي لكل منها باستخدام مقياس ليكرت الخماسي.

سهولة الاستخدام: قام الباحثون بتصميم مقياس لسهولة الاستخدام استنادًا إلى المقياس الموضح في دراسة (Davis, 1989)، وهو من المقاييس الأكثر استخدامًا في الدراسات السابقة التي ثبتت صدقها وثباتها. يشمل هذا المقياس (٥) عبارات تم قياس الوزن النسبي لكل منها باستخدام مقياس ليكرت الخماسي.

الثقة والأمن: قام الباحثون بتصميم مقياس للثقة والأمن استنادًا إلى المقياس الموضح في دراسة (Swinyard & Smith, 2003)، وهو من المقاييس الأكثر استخدامًا في الدراسات السابقة التي ثبتت صدقها وثباتها. يشمل هذا المقياس (٤) عبارات تم قياس الوزن النسبي لكل منها باستخدام مقياس ليكرت الخماسي.

ثالثاً: تحليل البيانات:

اعتمد الباحثون على أسلوب تحليل المسار لاختبار الفروض باستخدام برنامج(AMOS .25 V) ويعتمد هذا البرنامج على نموذجين وهما القياسي والهيكلي ويمكن توضيحهما كما يلي:

(١) تقييم نموذج القياس: قام الباحثون في هذا الجزء باستخدام نموذج المعادلة الهيكلية Structural Equation Modeling (SEM)، للتأكد من الصدق البنائي لمقياس الدراسة، ومن صحة النموذج وصلاحيته والتأكد من مطابقته لبيانات الدراسة قبل إجراء اختبار الفروض وذلك من خلال اتباع الخطوات التالية:

أ. تحديد اعتمادية معاملات التحميل Loadings) ويتضح من جدول (١) أن جميع معاملات التحميل مقبولة، حيث يرى (Hair et al. 2010) أن قيم معاملات التحميل المقبولة لابد أن تكون مساوية أو أكبر من ٠,٥٠.

ب.حساب معامل الثبات المركب (Composite Reliability) ومعامل ألفا كرونباخ (Cronbach's alpha) للوقوف على ثبات الاتساق الداخلي للمقياس، وكما هو موضح بجدول (٢) أظهرت نتائج اختبار الثبات أن معامل ألفا لكرونباخ لكل من التصيد الاحتيالي، البرامج الضارة، القرصنة الرقمية كان٠.٨٤١، ٠.٨٧٣، ٠.٨٣٦، بينما كان للفوائد المدركة، المخاطر المدركة، الثقة والأمن، سهولة الاستخدام كان ٠.٨٤٨، ٠.٨٦٨، ٠.٨٨٩، ٠.٨٤٤ على الترتيب، ومن ثم فإن جميع معاملات ألفا لكرونباخ مقبولة حيث يرى (Hair et al.، 2010) أن قيم ألفا المقبولة الى تكون أكبر من ٠,٧ تشير إلى درجة عالية من الاعتمادية على المقاييس المستخدمة. اما عن ثبات المكونات Composite Reliability (CR) فقد أظهرت نتائج التحليل الإحصائي والتي

يوضحها جدول (١) أن قيم (CR) مقبولة، حيث يرى أن قيم (CR) المقبولة لابد أن تكون مساوية أو أكبر من ٠.٧٠ (Hair et al.، ٢٠١٠).

ج. **قياس الصدق التقاربي convergent Validity** ويشير إلى المدى الذي تتقارب فيه العبارات التي تقيس البعد أو المتغير، أو يمكن تحميلها معاً على بعد أو متغير واحد، ويتم قياسه عن طريق متوسط التباين المستخرج Average variance extracted (AVE)، والذي لابد أن تزيد قيمته عن ٠,٥٠ لكل بعد أو متغير يتم قياسه. وقد أظهرت نتائج التحليل الإحصائي والتي يوضحها الجدول رقم (١) أن جميع قيم (AVE) مقبولة.

د. **الصدق التمايزي Discriminant Validity** ويشير إلى المدى الذي يكون فيه كل بعد أو كل متغير مختلف عن البعد أو المتغير الآخر، ويتم قياسه عن طريق الجذر التربيعي لمتوسط التباين المستخرج (square root of AVE)، حيث أنه لابد أن يزيد ارتباط البعد أو المتغير بنفسه عن قيمه ارتباطه بباقي متغيرات الدراسة الأخرى. وقد أظهرت نتائج التحليل الإحصائي والتي يوضحها الجدول رقم (٢) أن جميع القيم مقبولة.

جدول (١) معاملات التحميل والثبات والصدق التقاربي

Construct		loading	(AVE)	(α)	(CR)
PH	PH1	.742	.552	0.841	.830
	PH2	.815			
	PH3	.763			
	PH4	.642			
MW	MW1	.810	.630	0.873	.872
	MW2	.805			
	MW3	.761			
	MW4	.798			

تابع جدول (١) معاملات التحميل والثبات والصدق التقاربي

Construct	(CR)	(α)	(AVE)	loading	Construct
.831	0.836	.552	.745	DP1	DP
			.803	DP2	
			.722	DP3	
			.697	DP4	
.842	0.848	.517	.737	PB1	PB
			.700	PB2	
			.778	PB3	
			.629	PB4	
			.742	PB5	
.862	0.868	.557	.748	PR1	PR
			.722	PR2	
			.695	PR3	
			.738	PR4	
			.821	PR5	
.851	0.889	.593	.821	TS1	EU
			.901	TS2	
			.641	TS3	
			.690	TS4	
.838	0.844	.510	.679	EU1	TS
			.742	EU2	
			.772	EU3	
			.730	EU4	
			.641	EU5	

(PH) التصيد الاحتيالي،(MW) المخاطر المدركة،(DP) القرصنة الرقمية، (PB) الفوائد المدركة، (PR) المخاطر المدركة، (EU) سهولة الاستخدام، (TS) الثقة والأمن.

المصدر: إعداد الباحثين اعتماداً على نتائج التحليل الإحصائي.

جدول (٢) مصفوفة الارتباط بين المتغيرات والجذر التربيعي لـ (AVE)

	PB	PR	EU	TS	PH	MW	DP
PB	0.719						
PR	-0.259***	0.746					
EU	0.422***	-0.539***	0.714				
TS	-0.006	-0.085	0.007	0.770			
PH	-0.175**	0.493***	-0.332***	0.112†	0.743		
MW	-0.108†	0.487***	-0.380***	0.176**	0.660***	0.794	
DP	0.236***	-0.432***	0.548***	0.237***	-0.160**	-0.187**	0.743

المصدر: إعداد الباحثين اعتماداً على نتائج التحليل الإحصائي. Significance: *< 0.05, **< 0.01, *< 0.001**

(٢) **تقييم النموذج الهيكلي**: قام الباحثون باستخدام البرنامج الإحصائي AMOS V.25، وتم اختبار فروض الدراسة ومعرفة معاملات المسار بين متغيرات الدراسة ومستوى معنوية العلاقات بين متغيرات الدراسة. ويتضح في جدول (٣) أن مؤشرات جودة تطابق النموذج كانت مقبولة. كما يتضح في جدول (٣) نتائج اختبار التحليل الإحصائي للنموذج الهيكلي للدراسة، حيث يوضح العلاقة بين أشكال جرائم الإنترنت(التصيد الاحتيالي، البرامج الضارة، القرصنة الرقمية)، وأبعاد التسوق الإلكترونى(الفوائد المدركة، المخاطر المدركة، الثقة والأمن، سهولة الاستخدام).

جدول (٣) نتائج تحليل معاملات المسار

الفرض	المتغير المستقل	المتغير التابع	معامل المسار	قيمة المعنوية	النتيجة
H_{1a}	التصيد الاحتيالي	الفوائد المدركة	-.274	.040	قبول الفرض
H_{1b}	التصيد الاحتيالي	المخاطر المدركة	.398	.001	قبول الفرض
H_{1c}	التصيد الاحتيالي	سهولة الاستخدام	-.208	.064	قبول الفرض
H_{1d}	التصيد الاحتيالي	الثقة والأمن	.012	.912	رفض الفرض
H_{2a}	البرامج الضارة	الفوائد المدركة	.077	.614	رفض الفرض
H_{2b}	البرامج الضارة	المخاطر المدركة	.365	.001	قبول الفرض
H_{2c}	البرامج الضارة	سهولة الاستخدام	-.357	.006	قبول الفرض
H_{2d}	البرامج الضارة	الثقة والأمن	.352	.007	قبول الفرض
H_{3a}	القرصنة الرقمية	الفوائد المدركة	.294	.001	قبول الفرض
H_{3b}	القرصنة الرقمية	المخاطر المدركة	-.377	.001	قبول الفرض
H_{3c}	القرصنة الرقمية	سهولة الاستخدام	.577	.001	قبول الفرض
H_{3d}	القرصنة الرقمية	الثقة والأمن	.281	.001	قبول الفرض
Model Fit Indices					
$\chi 2$ (8.903) =3, $\chi 2/df$ = 2.968, CFI=.989, SRMR.071, RMSEA=0.071.					

مستوى المعنوية: $p < 0.001$ ***, $p < 0.010$ **, $p < 0.050$ *, $p < 0.100$ †

(PH) التصيد الاحتيالي، (MW) المخاطر المدركة، (DP) القرصنة الرقمية، (PB) الفوائد المدركة، (PR) المخاطر المدركة، (EU) سهولة الاستخدام، (TS) الثقة والأمن.

المصدر: إعداد الباحثين اعتماداً على نتائج التحليل الإحصائي.

وفقًا لنتائج التحليل الإحصائى يوجد تأثير معنوي سلبى للتصيد الاحتيالي على الفوائد المدركة بمعامل مسار (-٢٧٤.) عند مستوى معنوية (٠٤٠.)، كما يوجد تأثير معنوي سلبى للتصيد الاحتيالي على سهولة الاستخدام بمعامل مسار (-٢٠٨.) عند مستوى معنوية (٠٦٤.)، كما يوجد تأثير معنوي إيجابي للتصيد الاحتيالي على المخاطر المدركة بمعامل مسار (٣٩٨.)، بينما يوجد تأثير غير معنوي للتصيد الاحتيالي على الثقة والأمن بمعامل مسار (٠١٢.)، ومن النتائج السابقة يتبين **قبول الفرض** (H1c, H1b, H1a)، بينما يتم **رفض الفرض** (H1d). كذلك توصلت الدراسة لوجود تأثير معنوي سلبى للبرامج الضارة على سهولة الاستخدام بمعامل مسار (-٣٥٧.) عند مستوى معنوية (٠٠٦.)، كما يوجد تأثير معنوي إيجابي للبرامج الضارة على المخاطر المدركة بمعامل مسار (٣٦٥.) عند مستوى معنوية (٠٠٠١.)، كما يوجد تأثير معنوي إيجابي للبرامج الضارة على والثقة والأمن بمعامل مسار (٣٥٢.) عند مستوى معنوية (٠٠٧.)، بينما يوجد تأثير غير معنوي للبرامج الضارة على الفوائد المدركة بمعامل مسار (٠٧٧.)، ومن النتائج السابقة يتبين **قبول الفرض** (H1d, H1c, H1b)، بينما يتم **رفض الفرض** (H1a). كذلك توصلت الدراسة لوجود تأثير معنوي ايجابي للقرصنة الرقمية على الفوائد المدركة بمعامل مسار (٢٩٤.) عند مستوى معنوية (٠٠١.)، كما توصلت الدراسة لوجود تأثير معنوي إيجابي للقرصنة الرقمية على سهولة الاستخدام بمعامل مسار (٥٧٧.) عند مستوى معنوية (٠٠١.)، كذلك توصلت الدراسة لوجود تأثير معنوي ايجابي للقرصنة الرقمية على الثقة والأمن بمعامل مسار (٢٨١.) عند مستوى معنوية (٠٠١.)، كما يوجد تأثير معنوي سلبي للقرصنة الرقمية على المخاطر المدركة بمعامل مسار (-٣٧٧.) عند مستوى معنوية (٠٠٠١.)، ومن النتائج السابقة يتبين **قبول الفرض** (H1a, H1b, H1c, H1d).

رابعًا مناقشة النتائج:

توصلت الدراسة الحالية إلى وجود **تأثير معنوي سلبى للتصيد الاحتيالي على الفوائد المدركة** بمعامل مسار (-٢٧٤.) عند مستوى معنوية (٠٤٠.)، وتتفق نتائج الدراسة الحالية مع دراسة (Perrault, 2018; De Kimpe et al., 2018) فوجود تأثير معنوي سلبي بين التصيد الاحتيالي والفوائد المدركة للتسوق الإلكتروني يعني أن اى زيادة في محاولات التصيد الاحتيالي تؤدي إلى انخفاض الفوائد التي يدركها الطلاب من التسوق عبر الإنترنت، فعندما يواجه الطلاب تهديدات متكررة من التصيد الاحتيالي، مثل محاولات خداعهم للحصول على معلوماتهم الشخصية أو المالية، فإن ذلك يقلل من ثقتهم في منصات التسوق الإلكتروني، وهذه الثقة المنخفضة تؤدي إلى انخفاض تقديرهم للفوائد المحتملة التي يمكن أن يحصلوا عليها من التسوق عبر الإنترنت، مثل الراحة والتوفير والاختيارات الواسعة، كلما زادت مشكلات التصيد الاحتيالي، ينخفض رضا الطلاب عن التسوق الإلكتروني ويقل إدراكهم للفوائد المرتبطة به. كما يوضح(De Kimpe et al., 2018) أن زيادة التصيد الاحتيالي يمكن أن تقلل من الفوائد المدركة للتسوق الإلكتروني، حيث قد يرى المستخدمون أن مخاطر التعرض للجرائم الإلكترونية تفوق الفوائد المحتملة للتسوق عبر الإنترنت، مما قد يؤثر سلبًا على تصورهم لجودة التسوق الإلكتروني. كما يوضح (Perrault, 2018) أن تصاعد هجمات التصيد الاحتيالي قد يقلل من الفوائد المدركة للتسوق الإلكتروني، بسب أن المستخدمون يشعرون بعدم الأمان أو الخوف من فقدان معلوماتهم.

كما تظهر النتائج وجود **تأثير معنوي سلبى للتصيد الاحتيالي على سهولة الاستخدام** بمعامل مسار (-٢٠٨.) عند مستوى معنوية (٠٦٤.) وتتفق نتائج الدراسة الحالية مع نتائج دراسة (Perrault, 2018)، فوجود تأثير معنوي سلبي بين التصيد الاحتيالي وسهولة الاستخدام للتسوق الإلكتروني يعني أن زيادة في محاولات التصيد الاحتيالي تؤدي إلى انخفاض في تقييم الطلاب لسهولة استخدام منصات التسوق عبر الإنترنت، فعندما يتعرض الطلاب لتهديدات التصيد الاحتيالي، مثل الرسائل الإلكترونية الاحتيالية التي تهدف إلى سرقة معلوماتهم، فإن ذلك يجعلهم يشعرون بأن منصات التسوق الإلكتروني أقل أمانًا وسهولة في الاستخدام، كما أن هذه

تهديدات التصيد الاحتيالى تولد شعورًا بعدم الأمان وتعقيدًا في عملية التسوق، حيث قد يحتاج الطلاب إلى اتخاذ خطوات إضافية للتحقق من سلامة المواقع ووسائل الدفع، مما يجعل تجربة التسوق أكثر تعقيدًا وأقل سهولة، وبالتالي كلما زادت محاولات التصيد الاحتيالي، زادت الصعوبات التي يواجهها الطلاب في استخدام منصات التسوق، مما يقلل من سهولة الاستخدام التي يشعرون بها. حيث ان المستخدمون يصبحون أكثر حذرًا ويتطلبون إجراءات أمان إضافية عند زيادة التصيد الإحتيالى، مما قد يجعل عملية التسوق أكثر صعوبة وبطئًا(Perrault, 2018).

كما تظهر النتائج ووجود **تأثير معنوي إيجابي للتصيد الاحتيالي على المخاطر المدركة** بمعامل مسار (٣٩٨.) عند مستوى معنوية (٠.٠٠١)، وتتفق نتائج الدراسة مع نتائج دراسة (Kuraku& Kalla, 2023; Aribake& Mat Aji, 2020; Perrault, 2018; Abdelhamid, 2020; De Kimpe et al., 2018) فوجود تأثير معنوي إيجابي للتصيد الاحتيالي على المخاطر المدركة للتسوق الإلكتروني يعني أن اى زيادة في معدلات التصيد الاحتيالي ستؤدي إلى زيادة في إدراك الطلاب للمخاطر المرتبطة بالتسوق الإلكتروني وبالتالي يؤثر ذلك سلبياً على تسوقهم الإلكتروني، فاذا كان الموقع الإلكتروني يحتوى على رسائل تصيدية على سبيل المثال فسينتج عن ذلك ارتفاع في المخاطر لدى الطلاب تجاه ذلك الموقع وبالتالي سيتسوقون بشكل أقل، كما ان تعرض الطلاب لتهديدات التصيد الاحتيالي مثل سرقة المعلومات الشخصية أو الاحتيال المالي بشكل أكبر، ينتج عن ذلك وعيًا بالمخاطر الأمنية التي قد تواجههم عند التسوق عبر الإنترنت مرة أخرى بشكل أكبر، مما يجعلهم أكثر حذرًا ويقظة أثناء استخدام المنصات الإلكترونية. فالتصيد الاحتيالي يزيد من المخاطر المدركة المتعلقة بالتسوق الإلكتروني، حيث يشعر المستخدمون بقلق أكبر حول حماية معلوماتهم الشخصية والمالية، وهذه المخاوف تجعلهم أكثر حذرًا وترددًا في إجراء عمليات شراء عبر الإنترنت(De Kimpe et al., 2018).

بينما يوجد **تأثير غير معنوي للتصيد الاحتيالي على الثقة والأمن** بمعامل مسار (٠١٢.)، يعني أن التصيد الاحتيالي لا يظهر بشكل ملحوظ تأثيرًا مباشرًا على كيفية إدراك الأفراد

لثقتهم وأمانهم أثناء التسوق عبر الإنترنت، وهذا يشير إلى أن تصيد الاحتيالي على الرغم من كونه تهديدًا معروفًا، إلا أنه لا يؤثر بشكل كبير على الشعور العام بالثقة والأمان لدى الطلاب في الوقت الحالي، وقد يكون ذلك نتيجة لثقة الطلاب في مواقع التسوق الإلكتروني على الرغم من وجود التصيد الاحتيالي، حيث يشعر الطلاب بالأمان أثناء التسوق لأنهم يعتقدون أن المواقع تتمتع بمستويات عالية من الأمان تحميهم من مخاطر التصيد الاحتيالي، كما قد تكون المواقع الإلكترونية قد حسنت سياساتها وإجراءاتها الأمنية بشكل فعال، مما يقلل من تأثير التصيد الاحتيالي على ثقة الطلاب وأمانهم. كما قد يكون لدى الطلاب معلومات وإرشادات حول كيفية التعرف على التصيد الاحتيالي وتجنب الوقوع فيه، أيضًا يمكن أن تكون تجارب الطلاب الشخصية أو تجارب أصدقائهم أو أقاربهم مع التصيد الاحتيالي قد جعلتهم أكثر حذرًا، مما جعلهم لا يتسوقون إلا من خلال المواقع التسويقية الموثوقة فقط، والتي توفر حماية عالية ضد مخاطر التصيد الاحتيالي. وتختلف نتائج الدراسة مع دراسة (Hussin et al., 2023) حيث أظهرت نتائج أن مستويات الثقة في التجارة الإلكترونية تكون منخفضة إذا تمكن المحتالون من الوصول إلى المعلومات الشخصية عن طريق التصيد الاحتيالي. ومن النتائج السابقة يتبين قبول الفرض (H1c, H1b, H1a)، بينما يتم رفض الفرض (H1d).

كذلك توصلت الدراسة لوجود **تأثير معنوي سلبي للبرامج الضارة على سهولة الاستخدام** بمعامل مسار (-٣٥٧.) عند مستوى معنوية (٠٠٠.)، وتتفق نتائج الدراسة الحالية مع دراسة (Hlatshwayo, 2022; Hassan& Ahmed, 2023) ان هناك تاثير سلبي بين البرامج الضارة وسهولة الاستخدام، فيمكن أن يكون للبرامج الضارة تأثير سلبي واضح على سهولة الاستخدام في التسوق الإلكتروني، فعندما يصاب نظام أو جهاز ببرامج ضارة، فإنها غالباً ما تتسبب في بطء الأداء وتعطيل الوظائف الأساسية، مما يعرقل استخدام الطلاب لتلك المواقع بل ويجعل من الصعب التفاعل مع الموقع أو التطبيقات بكفاءة، فالبرمجيات الضارة كالفيروسات مثلاً يمكنها أن تؤدي إلى ظهور مشكلات متعددة مثل بطء أو التوقف المفاجئ أثناء التسوق في الموقع، مما يجعل الاستخدام اليومي أكثر تعقيداً، كما قد يتطلب التعامل مع

البرامج الضارة تدخلاً تقنياً مكثفاً وإجراءات إصلاحية قد تكون مرهقة للطلاب ومكلفة لاصحاب الموقع، مما يقلل من سهولة الاستخدام ويزيد من التعقيدات التي يواجهها الأفراد في التسوق الإلكتروني.

كما يوجد **تأثير معنوي إيجابي للبرامج الضارة على المخاطر المدركة** بمعامل مسار (٠.٣٦٥) عند مستوى معنوية (٠.٠٠١)، وتتفق نتائج الدراسة الحالية مع دراسة (Balapour et al., 2020; Hariharan et al., 2023; Hlatshwayo, 2022; Anwar et al., 2021؛) التى درست علاقة البرامج الضارة بالمخاطر المدركة أثناء التسوق الإلكتروني، حيث ان هناك تأثير ايجابى بين البرامج الضارة والمخاطر المدركة، حيث تؤدي زيادة البرامج الضارة إلى زيادة المخاطر المدركة في بيئة التسوق الإلكتروني بشكل ملحوظ، فكلما زاد عدد البرامج الضارة، يتزايد حجم التهديدات الأمنية التي يتعرض لها المستخدمون، مما يعزز الوعي بالمخاطرالمدركة، فالبرامج الضارة، مثل الفيروسات وبرامج التجسس، تقوم بتسريب المعلومات الشخصية، وتعرض الأنظمة للخطر، مما يجعل المستخدمين أكثر يقظة بشأن أمن بياناتهم، وهذا الوعي المتزايد يعزز إدراكهم للمخاطر المحيطة ويشجعهم على اتخاذ إجراءات احترازية إضافية، مثل تحسين الحماية الأمنية وتحديث البرمجيات بشكل دوري، وبالتالي يسهم في تقليل فرص التعرض للأضرار الناجمة عن هذه البرامج.

كما يوجد تأثير معنوي إيجابي للبرامج الضارة على والثقة والأمن بمعامل مسار (٠.٣٥٢) عند مستوى معنوية (٠.٠٠٧)، كما تتفق نتائج الدراسة الحالية مع دراسة (Balapour et al., 2020; Hassan& Ahmed, 2023; Hariharan et al., 2023; Hlatshwayo, 2022؛)، على وجود تأثير ايجابى بين البرامج الضارة والثقة والأمن، وذلك من خلال دفع الأفراد والمؤسسات إلى تعزيز إجراءات الأمان وحماية البيانات عند التسوق الإلكتروني، فعند مواجهة تهديدات البرامج الضارة، يدرك المستخدمون أهمية اتخاذ تدابير وقائية أكثر فعالية مثل استخدام برامج مكافحة الفيروسات، وتحديث أنظمة الحماية بانتظام، وتعزيز التشفير، وهذا الوعي المتزايد

يدفعهم إلى تحسين ممارسات الأمان، مما يؤدي إلى بناء بيئة إلكترونية أكثر أماناً، وبالتالى يزداد مستوى الثقة في المنصات الإلكترونية، حيث يصبح الأفراد أكثر ارتياحاً وثقة في أن بياناتهم محمية بشكل جيد ضد التهديدات المحتملة. وبالتالى قد تعمل البرامج الضارة كعامل محفز لتحسين معايير الأمان وتعزيز الثقة في الاستخدام الرقمي.

كما تتفق نتائج الدراسة الحالية مع نتائج (Strzelecki& Rizun, 2022) التي أوضحت أن حادث الاختراق بسبب البرامج الضارة أدى إلى زيادة وعي المستهلكين بأهمية أمن وحماية بياناتهم، فقد أصبحوا أكثر حذرًا في تقديم بياناتهم لأي موقع ويب بعد الحادث، وبالتالي فإن البرامج الضارة تأثيرت إيجابيًا على أمن وحماية المستهلكين، حيث جعلتهم أكثر انتباهًا عند تقديم بياناتهم للمواقع الإلكترونية بعد الحادث. كما تختلف نتائج تلك الدراسة مع نتائج(Strzelecki& Rizun, 2022) التي أظهرت انخفاضًا كبيرًا في ثقة المستهلكين تجاه متجر Morele.net بشكل خاص، حيث تراجعت الثقة بشكل ملحوظ بعد حادث اختراق البيانات، ومع ذلك لم يؤثر هذا التراجع على مواقفهم وثقتهم تجاه التسوق عبر الإنترنت بشكل عام.

بينما يوجد تأثير غير معنوي للبرامج الضارة على الفوائد المدركة بمعامل مسار (.٠٧٧)، و يعني هذا أن العلاقة بين البرامج الضارة والفوائد المدركة ليست قوية بما يكفي لتكون ذات دلالة إحصائية، فبرغم من وجود تأثير للبرامج الضارة على الفوائد المدركة، إلا أن هذا التأثير ليس كافياً ليكون ملموساً أو مؤثراً بشكل كبير، قد يكون السبب في ذلك هو أن البرامج الضارة لا تؤثر بشكل مباشر أو ملموس على كيفية إدراك المستخدمين للفوائد، أو أن هناك عوامل أخرى مثل جودة الخدمة أو إجراءات الحماية قد تكون لها تأثير أكبر، كما قد يكون التأثير موجودًا ولكنه خفي بسبب عوامل أخرى تؤثر على العلاقة، فيمكن أن تؤثر عوامل خارجية مثل دعم المستهلكين أو تصميم واجهة المستخدم على الفوائد المدركة بشكل أقوى من البرامج الضارة. ومن النتائج السابقة يتبين قبول الفرض (H1d, H1c, H1b)، بينما يتم رفض الفرض (H1a).

كذلك توصلت الدراسة لوجود تأثير **معنوي ايجابي للقرصنة الرقمية** على الفوائد المدركة بمعامل مسار (٢٩٤.) عند مستوى معنوية (٠٠١.)، تتفق نتائج الدراسة مع دراسة (Hoy, 2017; Ahadiat et al., 2021; Yoon, 2011; Chiou et al., 2005; Goles et al., 2008; Peace et al., 2003) أن هناك علاقة ايجابية بين القرصنة الرقمية و الفوائد المدركة، ويمكن توضيح ذلك بان استخدام القرصنة الرقمية يمنح الطلاب وصولاً غير محدود إلى محتويات مجانية مثل تحميل البرامج والموسيقى والفديو والكتب الدراسية المحمية بحقوق ملكية فكرية بدون اى تكاليف او بتكاليف قليله جدا، حيث تعرض هذه المواد المقرصنة على مواقع أخرى غير رسمية، وذلك دون الأخذ في الاعتبار الجانب الأخلاق والقانونى، مما يعزز فهمهم لقيمة الموارد الرقمية وكيفية الاستفادة منها، كما أن الوعي المتزايد لكيفية قرصنة تلك المواد يجعل الطلاب يقدّرون أكثر الفوائد التي يقدمها التسوق الإلكتروني، حيث يمكنهم العثور على منتجات وخدمات تلبي احتياجاتهم بسهولة، كما ان استخدام القرصنة الرقمية قد يعزز اهتمام الطلاب بالتكنولوجيا ويزيد من استعدادهم لاستكشاف المزيد من فوائد التسوق الإلكتروني وذلك دون الأخذ في الاعتبار الجانب الأخلاق والقانونى. وتختلف نتائج الدراسة مع (Hampton-Sosa, 2017) الذى وضح أن الفوائد المدركة من استخدام خدمات الاشتراك في الموسيقى (MSS) تؤثر بشكل إيجابي على نية شراء الاشتراك وتقلل من القرصنة الرقمية لها، فعندما يرى المستهلكون فوائد ملموسة، مثل الحصول على محتوى مفيد وسهل الوصول إليه، يصبحون أقل ميلاً للقرصنة لأنهم يجدون قيمة في الدفع مقابل الخدمة. كما تختلف مع دراسة (KARAHAN& KAYABASI, 2019) التي أظهرت نتائجها ان هناك علاقة سلبية بين الفوائد المدركة والقرصنة الرقمية، فالأفراد في تركيا رغم أنهم يقدّرون فوائد القرصنة الرقمية مثل التوفير والراحة والمتعة، إلا أن هذه الفوائد لا تُعتبر عوامل حاسمة في قراراتهم المتعلقة بالقرصنة الرقمية.

كذلك توصلت الدراسة لوجود تأثير **معنوي إيجابي للقرصنة الرقمية على سهولة الاستخدام** بمعامل مسار (٥٧٧.) عند مستوى معنوية (٠٠١.)، وتتفق نتائج الدراسة مع دراسة

(Hoy, 2017) ويمكن تفسير ذلك العلاقة الإيجابي للقرصنة الرقمية على سهولة الاستخدام في التسوق الإلكتروني في أن الزيادة في سهولة الوصول إلى المواد الرقمية المقرصنة، مثل الكتب والفيديو والموسيقى والبرامج، تساهم في زيادة استخدام القرصنة الرقمية، فعندما تكون المنصات الرقمية سهلة الاستخدام، يصبح من الأسهل على الطلاب الوصول إلى هذه المواد المقرصنة، مما يعزز من انتشارها، وبالتالي كلما زادت سهولة استخدام المواقع الإلكترونية للحصول على هذه المواد، يزداد إقبال الطلاب على القرصنة الرقمية، وهذا يعني أن تحسين سهولة الاستخدام في المواقع الرقمية يمكن أن يعزز من حجم القرصنة الرقمية بنفس القدر. وتختلف نتائج الدراسة مع دراسة (Hampton-Sosa, 2017) الذى أشار أن سهولة استخدام خدمات الاشتراك في الموسيقى (MSS) ترتبط بشكل إيجابي بنية شراء الاشتراك، فعندما تكون الخدمة سهلة الاستخدام، يقل احتمال التوجه إلى القرصنة بسبب تجربة المستخدم السلسة التي توفرها الخدمة القانونية مقارنةً بالطرق غير القانونية التي قد تكون أكثر تعقيدًا.

كذلك توصلت الدراسة لوجود تأثير **معنوي ايجابي للقرصنة الرقمية على الثقة والأمن** بمعامل مسار (٠.٢٨١) عند مستوى معنوية (٠.٠٠١)، فزيادة الثقة والأمن في المواقع الإلكترونية التي تقدم مواد مقرصنة يساهم في زيادة معدل الوصول إلى المواد الرقمية المقرصنة، فعندما يتمتع الطلاب بثقة عالية في أمان موقع إلكتروني معين، فإنهم يشعرون بالراحة في استخدام هذه المنصات، مما قد يسهل عليهم العثور والوصول إلى مواد مقرصنة مثل الكتب والفيديو والموسيقى والبرامج، مما يزيد من فرص استخدام هذه المنصات للبحث عن المواد المقرصنة، لذلك كلما زادت ثقة الأفراد في أمان الموقع الإلكتروني، قد يرتفع معدل الوصول إلى المحتوى المقرصن المطلوب.وتختلف تلك الدراسة مع (Hampton-Sosa, 2017) الذي أشار ان تعزيز الأمان والثقة في خدمة الاشتراك في الموسيقى (MSS) يمكن أن يقلل من القرصنة الرقمية لها، فإذا كانت الخدمة موثوقة وآمنة، فإن المستهلكين يكونون أكثر استعدادًا للدفع بدلاً من اللجوء إلى مصادر غير قانونية.

كما يوجد **تأثير معنوي سلبي للقرصنة الرقمية على المخاطر المدركة** بمعامل مسار (-٣٧٧.) عند مستوى معنوية (٠.٠٠١)، وتتفق نتائج الدراسة الحالية مع دراسة (Saeed, 2023; Liao et al., 2010; Yoon, 2011; Ahadiat et al., 2021; Kos Koklic et al., 2016; Sardanelli et al., 2019; Jaramillo et al., 2023) فوجود تأثير معنوي سلبي للقرصنة الرقمية على المخاطر المدركة للتسوق الإلكتروني يعني أن زيادة المخاطر التي تسببها القرصنة الرقمية تقلل من احتمالية دخول الطلاب إلى المواقع التي توفر مواد رقمية مقرصنة، فكلما زادت المخاطر المرتبطة بالقرصنة الرقمية، يتجنب الطلاب هذه المواقع لتفادي المخاطر الأمنية مثل الفيروسات والبرامج الضارة، وبالتالي يقل إدراكهم للمخاطر المتعلقة بالتسوق الإلكتروني لأنه قد يكون لديهم تجربة سلبية أو قلق أكبر من التهديدات المحتملة التي قد تنشأ من استخدام مثل هذه المواقع، مما يجعلهم أقل عرضة لاستخدامها.

وتختلف نتائج الدراسة مع دراسة (KARAHAN& KAYABASI, 2019) التي أشارت إلى وجود علاقة إيجابية بين المخاطر المدركة والقرصنة الرقمية، حيث أن الأفراد الذين يدركون المخاطر المرتبطة بالقرصنة الرقمية يظهرون مواقف أكثر إيجابية تجاهها، مما يدل على أن إدراك المخاطر قد لا يكون كافيًا لردعهم عن ممارسة القرصنة الرقمية، وذلك بسبب أن هناك نقص في المعلومات حول المخاطر القانونية للقرصنة الرقمية في تركيا مما تسبب في قلة الوعي بالمخاطر أو عدم الاهتمام بالعقوبات المحتملة، ومن النتائج السابقة يتبين قبول الفرض (H1a, H1b, H1c, H1d).

خامسًا: مساهمات الدراسة:

- **فهم تأثير جرائم الإنترنت**: توضح الدراسة تأثير جرائم الإنترنت على سلوكيات طلاب جامعة الزقازيق ومدى إدراكهم للمخاطر المتعلقة بالتسوق الإلكتروني.
- **تعزيز وعي الطلاب**: تسعى الدراسة إلى دراسة تأثير هذه الجرائم على تسوق الطلاب عبر الإنترنت وتعزيز وعيهم بضرورة اتخاذ احتياطات أمنية.

- **تطوير استراتيجيات توعية**: تساهم الدراسة في تطوير استراتيجيات توعية فعالة للشركات لتعزيز الثقة في التسوق الإلكتروني وحماية المستهلكين من المخاطر المحتملة.
- **تحديد أنواع الجرائم**: تساعد الدراسة الباحثين في تحديد أنواع جرائم الإنترنت المرتبطة بالتسوق الإلكتروني.
- **تطوير إجراءات أمان وحماية**: تسهم الدراسة في تطوير إجراءات أمان وحماية للطلاب والقطاع التجاري على حد سواء.
- **تحسين أنظمة الدفع وتشفير البيانات**: تركز الدراسة على تحسين أنظمة الدفع الإلكتروني وتطوير تقنيات تشفير البيانات.
- **تعزيز الوعي بجرائم الإنترنت**: تعزز الدراسة الوعي بجرائم الإنترنت وأساليب التكنولوجيا المستخدمة في التسوق الإلكتروني لطلاب جامعة الزقازيق.
- تمكين الطلاب واتخاذ إجراءات احترازية: تهدف الدراسة إلى تمكين الطلاب من اتخاذ إجراءات احترازية عند التسوق عبر الإنترنت.
- **تحفيز تحسين التشريعات**: تسعى الدراسة إلى تحفيز تحسين التشريعات والسياسات الحكومية لمواجهة جرائم الإنترنت، مما يعزز الأمان والثقة في التسوق عبر الإنترنت.

وبناءً على ما أسفرت عليه نتائج الدراسة **يمكن للباحثين تقديم مجموعة من التوصيات، كما هو موضح في جدول(٤)** التالي:

جدول(٤) توصيات الدراسة

التوصية	آليات التنفيذ	المسؤول عن التنفيذ
تطوير المناهج الدراسية	إدراج مواد دراسية متخصصة في أمن المعلومات وجرائم الإنترنت ضمن المناهج الدراسية، وتشجيع الأبحاث والدراسات حول أمن التسوق الإلكتروني ومخاطره من خلال منح بحثية داخلية أو التعاون مع مؤسسات بحثية.	كلية الحاسبات والمعلومات، وكلية إدارة الأعمال
تعزيز الوعي الأمني بين الطلاب	تنظيم ورش عمل ودورات تدريبية بالتعاون مع خبراء في أمن المعلومات، وتوزيع مواد تعليمية وإرشادية عبر البريد الإلكتروني أو المنصات التعليمية الرقمية حول كيفية التسوق بأمان عبر الإنترنت ومخاطر جرائم الإنترنت.	إدارة شؤون الطلاب، قسم الأمن السيبراني.
التعاون مع الجهات المختصة	تعزيز التعاون بين الجامعة والجهات الأمنية المختصة بمكافحة جرائم الإنترنت، وإقامة -ندوات ومحاضرات بالشراكة مع خبراء أمن المعلومات.	إدارة العلاقات العامة، قسم الأمن السيبراني.
توعية الطلاب بالسياسات القانونية	تعريف الطلاب بالقوانين المحلية والدولية المتعلقة بجرائم الإنترنت وحماية المستهلك الإلكتروني من خلال ورش توعية وندوات، وتوزيع كتيبات قانونية توضح العقوبات المترتبة على الجرائم الإلكترونية وأهمية الإبلاغ عنها.	إدارة الشؤون القانونية، قسم الأمن السيبراني.

تابع جدول(٤) توصيات الدراسة

توفير أدوات حماية فعالة	تعريف الطلاب بالقوانين المحلية والدولية المتعلقة بجرائم الإنترنت وحماية المستهلك الإلكتروني من خلال ورش توعية وندوات، وتوزيع كتيبات ومصادر قانونية توضح العقوبات المترتبة على الجرائم الإلكترونية وأهمية الإبلاغ عنها.	قسم تكنولوجيا المعلومات، إدارة الجامعة.
تحسين البنية التحتية التقنية	تحسين شبكة الإنترنت داخل الجامعة لضمان حماية البيانات الشخصية للطلاب، وتوفير موارد تقنية متقدمة تساعد في اكتشاف ومنع الهجمات الإلكترونية.	المسؤول: إدارة تكنولوجيا المعلومات، قسم البنية التحتية التقنية.
تحفيز البحث العلمي	تشجيع الطلاب على إجراء أبحاث حول تأثير جرائم الإنترنت على التسوق الإلكتروني من خلال تقديم منح بحثية للمشاريع ذات الصلة، وتنظيم مؤتمرات بحثية وتشجيع الطلاب على تقديم أبحاثهم حول موضوع الجرائم الإلكترونية.	عمداء ووكلاء البحث العلمي في الكليات.
تشجيع التسوق من المواقع الموثوقة	تقديم قائمة بالمواقع الإلكترونية الآمنة والموثوقة التي يمكن للطلاب التسوق منها، وتوجيه الطلاب لتقييم المواقع الإلكترونية قبل الشراء والتأكد من وجود شهادات أمان في الموقع.	إدارة الشؤون الطلابية، قسم تكنولوجيا المعلومات.
تطوير سياسات الجامعة	وضع سياسات وإجراءات واضحة للتعامل مع جرائم الإنترنت داخل الحرم الجامعي، إنشاء وحدة مختصة بأمن المعلومات تتولى تقديم الدعم الفني والتوعوي للطلاب.	إدارة الشؤون الإدارية، قسم الأمن السيبراني.
التوعية بالتقنيات الحديثة	توعية الطلاب بالتقنيات الحديثة المستخدمة في الحماية الإلكترونية مثل التشفير والمصادقة الثنائية من خلال ورش عمل ودورات تدريبية، وتقديم مواد تعليمية حول كيفية استخدام هذه التقنيات بشكل فعال.	إدارة تكنولوجيا المعلومات، مركز التدريب.

المصدر: إعداد الباحثين.

قائمة المراجع

(١) المراجع العربية

(١) الإمام، وفقي السيد (٢٠٢٢)، "إعداد مشروع البحث وكتاية التقرير النهائي"، ط٦، ***المكتبة العصرية***، المنصورة.

(٢) الهديف، مفتاح ميلاد ؛ شنيب، جمعة عبد الحميد (٢٠٢٢)، "الجرائم الالكترونية"، ***مجلة التربوى***، (٢٠)، ١٤١-١٥٥.

(٢) المراجع الأجنبية:

1. Abdelhamid, Mohamed (2020), "The role of health concerns in phishing susceptibility: Survey design study", ***Journal of medical Internet research***, 22(5), 1-10.

2. Aditya, Christian, Kusmiantini, Titik, and Liestyana, Yuli (2020), "Analisis Faktor-Faktor Yang Mempengaruhi Penentu Belanja Online". ***Jurnal Ekonomi dan Ilmu Sosial***, 5(2), 130-142.

3. Ahadiat, Ayi et al. (2021), "The theory of planned behavior and marketing ethics theory in predicting digital piracy intentions", ***WSEAS Transactions on Business and Economics***, 18, 679-702.

4. Ahmed, Sraboni, Munir, Mohammad S, and Islam, Tamjida (2022), "Online Shopping: A Survey on Consumer Buying Behavior in Bangladesh", ***European Scientific Journal***, 18(15), 93- 105.

5. Akdemir, Naci, and Lawless, Christopher J (2020), "Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach", ***Internet Research***, 30(6), 1665-1687.

6. Alleyne, Philmore, Soleyn, Sherlexis, and Harris, Terry (2015), "Predicting accounting students' intentions to engage in software and music piracy", ***Journal of Academic Ethics***, 13, 291-309.

7. Anwar, Usama et al. (2021), "Benefits and risks of online shopping with consumer's perspective: a case study of Pakistan", ***International Journal of Academic Research in Accounting, Finance and Management Sciences***, 11(1), 499-511.

https://doi.org/10.1016/j.techfore.2023.123028.

8. Aribake, Fadare O, and Mat Aji, Zahurin (2020), "The mediating role of perceived security on the relationship between internet banking users and their determinants", ***International Journal of Advanced Research in Engineering and Technology (IJARET***), 11(2),296-318.

9. Aslan, Omer, and Yilmaz, Abdullah A (2021), "A new malware classification framework based on deep learning algorithms", ***Ieee Access***, 9, 87936-87951,

Digital Object Identifier 10.1109/ACCESS.2021.3089586.

10. Balapour, Ali, Nikkhah, Hamid R., and Sabherwal, Rajiv (2020), "Mobile application security: Role of perceived privacy as the predictor of security perceptions", ***International Journal of Information Management***, 52, 102063,1-13.

11. Boskovic, Aleksandar, and Kaurin, Tanja (2020), "Customer Satisfaction Assessment by Online Shopping Service: A Case Study of Serbia", ***Tehnički vjesnik***, 27(5), 1631-1637.

12. Bossler Adam M, and Holt, Thomas J (2009), "On-line activities, guardianship, and malware infection: An examination of routine activities theory". ***International Journal of Cyber Criminology***, 3(1),400-420.

13. Buil-Gil, David et al. (2021), "Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK", ***European Societies***, 23(1), 47-59.

14. Chiou, Jyh-Shen, Huang, Chien-yi, and Lee Hsin-hui (2005), "The antecedents of music piracy attitudes and intentions, ***Journal of Business Ethics***, 57, 161-174.

15. Choi Kyung-shick (2008), "Computer crime victimization and integrated theory: An empirical assessment", ***International Journal of Cyber Criminology***, 2(1),308-333.

16. Cronan, Timothy P, and Al-Rafee, Sulaiman (2008), "Factors that influence the intention to pirate software and media" ***Journal of business ethics***, 78, 527-545.

17. Davis, Fred D (1989), "Perceived usefulness, perceived ease of use, and user acceptance of information technology", ***MIS quarterly***, 13(3),319-340.

18. DAY, MICHAEL J (2024), "Digital divides in Chinese HE: leveraging AI as Student's Partner (AIasSP) to reduce piracy" ***Quantum Journal of Social Sciences and Humanities***, 5(1), 165-183.

19. De Kimpe, Lies et al.(2018), "You've got mail! Explaining individual differences in becoming a phishing target", ***Telematics and Informatics***, 35(5), 1277-1287.

20. Elisanti, Evi et al. (2024), "Analysis of Cybercrime Potential in E-Commerce Buying and Selling Transactions", ***AL-MANHAJ: Jurnal Hukum dan Pranata Sosial Islam***, 6(1), 163-180..

21. Eze-Michael, Ezedikachi (2020), "Internet fraud and its effect on Nigeria's image in international relations", ***Covenant Journal of Business and Social Sciences***, 12(1), 1-24.

22. Forsythe, Sandraet al. (2006)," Development of a scale to measure the perceived benefits and risks of online shopping", ***Journal of interactive marketing***, 20(2), 55-75.

23. Francisco, Gaile (2024), Consumers and Businesses: An In-Depth Analysis of Copyright Law on Stolen Product Photographs on E-Commerce Platforms and its Implications on Consumer Protection, Available at SSRN***. Ph.D. thesis***, Marketing and Law Department, Ateneo de Manila University.

24. Garcia, Katherine R et al. (2023, September), "Phishing in Social Media: Investigating Training Techniques on Instagram Shop", ***In Proceedings of the Human Factors and Ergonomics Society Annual Meeting***,67(1),1850-1855.

25. Goles, Tim et al. (2008), "Softlifting: Exploring determinants of attitude", ***Journal of business ethics***, 77, 481-499.

26. HAIR JUNIOR, Joseph F et al. (2010), "SEM: An introduction", ***Multivariate data analysis: A global perspective***, 5(6), 629-686.

27. Halttunen, Veikko (2024), "How do digital threats change requirements for the software industry", ***arXiv***,1-8,
https://doi.org/10.48550/arXiv.2402.14588.

28. Hampton-Sosa, William (2017), "An exploration of essential factors that influence music streaming adoption and the intention to engage in digital piracy", ***International Journal of Electronic Commerce Studies***, 8(1), 97-134.

29. Hariharan, Jagdish et al. (2023, June), "Customers' perception of cybersecurity risks in E-commerce websites", ***In International Conference on AI and the Digital Economy (CADE 2023)***,1-8,
https://doi.org/10.1049/icp.2023.2565

30. Hassan, Amina, and Ahmed, Kareem (2023), "Cybersecurity's impact on customer experience: an analysis of data breaches and trust erosion", ***Emerging Trends in Machine Intelligence and Big Data***, 15(9), 1-19.

31. Hlatshwayo, Mthokozisi (2022)," The influence of perceived risk, trust and security on the online shopping behaviour: A South African perspective"*, **Master's thesis*** in Business Administration, Faculty of Commerce , Law, and Management, University of the Witwatersrand, Johannesburg.

32. Hoy, Matthew B (2017)," Sci-Hub: What librarians should know and do about article piracy", ***Medical reference services quarterly***, 36(1), 73-78.

33. Hussin, Harniyati et al. (2023, June), "Perceptions of phishing information access on e-commerce in Malaysia", ***In AIP Conference Proceedings***,26(1),
https://doi.org/10.1063/12.0014781.

34. Ijaz, Aqsaet al.(2024), "Innovative Machine Learning Techniques for Malware Detection" ***Journal of Computing & Biomedical Informatics***, 7(1), 403-424.

35. Iqbal, Asifet al. (2024)," Unveiling the Connection Between Malware and Pirated Software in Southeast Asian Countries: A Case Study", IEEE Open Journal of the Computer Society,5,62-72,
https://doi.org/10.1109/OJCS.2024.3364576.

36. Iriani, Sri S., and Andjarwati, Anik (2020)", Analysis of perceived usefulness, perceived ease of use, and perceived risk toward online shopping in the era of Covid-19 pandemic", ***Systematic Reviews in Pharmacy***, 11(12), 313-320.

37. Jaramillo, Fernando, Yang, Zhiyong, and Wang, Jingguo (2023), Effect of Perceived Sanction Risk on Digital Piracy Behavior: A Meta-Analytic Structural Equation Modeling Approach, ***Ph.D. thesis*** in Legal Management, Marketing and Law Department, University of South Florida - College of Business Administration.

38. KarAhan, Mehmet O, and Kayabasi, Aydin (2019)," The effect of the theory of planned behavior and the theory of ethics in digital piracy", ***Business & Management Studies: An International Journal***, 7(4), 1751-1775.

39. Kaur, Komalpreet et al. (2021)," Impact of E-marketing on Consumer Purchase Behaviour: An empirical study" ***IJRAR-International Journal of Research and Analytical Reviews (IJRAR)***, 8(1).387- 408.

40. Kos Koklic, Mateja, Kukar-Kinney, Monika, and Vida, Irena (2016), "Three-level mechanism of consumer digital piracy: Development and cross-cultural validation", ***Journal of Business Ethics***, 134, 15-27.

41. Kuraku, Dr Sivaraju, and Kalla, Dinesh (2023), "Impact of phishing on users with different online browsing hours and spending habits", ***International Journal of Advanced Research in Computer and Communication Engineering***, 12(10),34-41.

42. Leukfeldt, Eric R (2014), "Phishing for suitable targets in the Netherlands: Routine activity theory and phishing victimization" ***Cyberpsychology, Behavior, and Social Networking***, 17(8), 551-555.

43. Leukfeldt, Eric R., and Yar, Majid (2016)," Applying routine activity theory to cybercrime: A theoretical and empirical analysis", ***Deviant Behavior***, 37(3), 263-280.

44. Liao, Chechen, Lin, Hong-Nan, and Liu, Yu-Ping (2010), "Predicting the use of pirated software: A contingency model integrating perceived risk with the theory of planned behavior", ***Journal of Business Ethics***, 91, 237-252.

45. Malhotra, Meenakshi, and Singh, Dr Jashandeep (2013), "Factors affecting the adoption of online shopping in youngsters-an empirical study", ***International Journal of Management and Behavioral Sciences***, 2(1),44-54.

46. Mariyappan, N., and Sangeetha, G. (2024)," A Study On Consumer Education Towards External Stimuli Affecting Online Shopping Behavior–Analysis Using Jamovi", ***Educational Administration: Theory and Practice***, 30(4), 5985-5991.

47. Meixner, Oliver, Dittmann, Julian and Haas, Rainer (2022)," Online food shopping under COVID-19–a technology acceptance model to evaluate consumption motives and barriers", ***Proceedings in Food System Dynamics***, 64-74.

https://doi.org/10.18461/pfsd.2022.2206.

48. Michels, Leonard et al. (2022)," Empowering consumers to make environmentally sustainable online shopping decisions: A digital nudging approach",***ALSEL***,4707-4716,

https://hdl.handle.net/10125/79911.

49. Natadimadja, Muhammad R., Abdurohman, Maman, and Nuha, Hilal H (2020)," A survey on phishing website detection using hadoop" ***Jurnal Informatika Universitas Pamulang***, 5(3), 237-246.

50. Neves, Raquel A (2022), Vitimação por phishing: um estudo empírico, ***Master's thesis***, Faculty of Law, University of Porto.

51. Oki, Olukayode, and Ngotshane, Sipesande (2021, October), "Investigating the Effects of Covid-19 on Online Shopping Cybercrime in Buffalo City", ***In 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering***,1-6,
https://www.researchgate.net/publication/356133118

52. Olivia, Onwugbenu E (2022), "Examining the Effect of the Elevated Rate of Cybercrime on the Growth and Sustainable development of Nigeria's Economy", ***Journal of Commercial and Property Law***, 9(1), 32-43.

53. Peace, A. Graham, Galletta, Dennis F., and Thong, James Y (2003), "Software piracy in the workplace: A model and empirical test", ***Journal of Management Information Systems***, 20(1), 153-177.

54. Perrault, Evan K (2018), "Using an interactive online quiz to recalibrate college students' attitudes and behavioral intentions about phishing', ***Journal of Educational Computing Research***, 55(8), 1154-1167.

55. Rahayu, Siti K et al.(2021), "Cybercrime dan dampaknya pada teknologi e-commerce", ***JISAMAR (Journal of Information System, Applied, Management, Accounting and Research)***, 5(3), 632-637.

56. Reddy Maddikunta, Praveen K et al (2020), "Predictive model for battery life in IoT networks ***", IET Intelligent Transport Systems***, 14(11), 1388-1395.

57. Reyns, Bradford W (2015)," A routine activity perspective on online victimisation: Results from the Canadian General Social Survey" ***Journal of Financial Crime***, 22(4), 396-411.

58. Rezk, Amira, Barakat, Sherif, and Saleh, Hossam (2017), "The impact of cyber crime on E-Commerce", ***International Journal of Intelligent Computing and Information Sciences***, 17(3), 85-96.

59. Saeed, Saqib (2023), "A customer-centric view of E-commerce security and privacy", ***Applied Sciences***, 13(2), 1-22.

60. Sardanelli, Domenico et al. (2019)," Lowering the pirate flag: a TPB study of the factors influencing the intention to pay for movie streaming services", ***Electronic Commerce Research***, 19, 549-574.

61. Nasution, Muhammad D et al. (2018)," The Phenomenon of Cyber-crime and Fraud Victimization in Online Shop", ***International Journal of Civil Engineering and Technology***,9(6),1583-1592.

62. Singh, Uma S. (2019), "Buyers Perception on Online Shopping in Kurdistan Region", ***European Journal of Business and Management***,11(15),18-25.

63. Soares, João C et al. (2023), "Assessing the effects of COVID-19-related risk on online shopping behavior", ***Journal of Marketing Analytics***, 11(1), 82-94.

64. Strzelecki, Artur, and Rizun, Mariia (2022), "Consumers' change in trust and security after a personal data breach in online shopping", ***Sustainability***, 14(10), 1-17.

65. Swinyard, William R, and Smith, Scott M (2003), "Why people (don't) shop online: A lifestyle study of the internet consumer", ***Psychology & marketing***, 20(7), 567-597.

66. Ting, Tin T et al. (2024), "Validation of cyber security behaviour among adolescents at Malaysia university: Revisiting gender as a role", ***International Journal of Innovative Research and Scientific Studies***, 7(1), 127-137.

67. Toso, Christian H et al.(2023), "Cybercrime Awareness Among Senior High School Students", ***Mediterranean Journal of Basic and Applied Sciences (MJBAS),*** 7(2), 160-176.

68. Yoon, Cheolho (2011), "Theory of planned behavior and ethics theory in digital piracy: An integrated model", ***Journal of business ethics***, 100, 405-417.

ملحق رقم(١)إطار المقابلة الشخصية

قام الباحث في هذه المرحلة بإجراء مقابلات شخصية مع (٣٠) مفردة من طلاب جامعة الزقازيق. **ودار الحوار معهم حول:**

- ما مدى معلوماتك عن جرائم الإنترنت وأشكالها المختلفة؟
- ما مدى معلوماتك عن التسوق الإلكتروني؟
- ما مدى تعرضك لشكل او اكثر من أشكال جرائم الإنترنت أثناء التسوق الإلكتروني ؟ أذكر ما تعرضت له؟
- هل تدرك المخاطر التي قد تتعرض لها أثناء التسوق الإلكتروني؟ اذا كانت الإجابة نعم اشرحها وكيف ترى سبل الوقاية منها؟
- ما مدى شعورك بالأمان عند التسوق الإلكتروني ؟