

تقييم مخاطر الأمن السيبراني التي تواجه المتسوقين عبر الإنترنت في المملكة العربية السعودية.

إعداد الطالب/ محمد علي مطر

إشراف/

العام الدراسي:

٢٠٢٤

## مقدمة:

يشهد التسوق عبر الإنترنت في المملكة العربية السعودية نموًا هائلًا، حيث أصبحت التجارة الإلكترونية جزءًا لا غنى عنه من حياتنا. ناعتمد على الإنترنت لشراء السلع والخدمات، وإدارة أموالنا، والتواصل مع الآخرين، والوصول إلى المعلومات. مع ازدياد الاعتماد على الإنترنت، وهذا ما يجعلنا هدفًا جذابًا للمجرمين الإلكترونيين. حيث تشكل مخاطر الأمن السيبراني تهديدًا خطيرًا للمتسوقين عبر الإنترنت، مما قد يؤدي إلى سرقة البيانات الشخصية والمعلومات المالية، والاحتيال، وسرقة الهوية، وغيرها من الجرائم الإلكترونية.

يمكن أن تلحق مخاطر الأمن السيبراني ضررًا كبيرًا بالأفراد والشركات على حدٍ سواء. تشمل هذه الأضرار الخسائر المالية الكبيرة، وفقدان السمعة للتاجر، والمسؤولية القانونية، وانزعاج العملاء.

تهدف هذه الخطة البحثية إلى تقديم إطار مفصل لإجراء بحث علمي شامل لتقييم مخاطر الأمن السيبراني التي تواجه المتسوقين عبر الإنترنت في المملكة العربية السعودية. ويهدف البحث إلى فهم طبيعة هذه المخاطر، وتحديدتها، وتقييمها، وتقديم توصيات عملية للتخفيف منها.

## مشكلة الدراسة:

يشهد التسوق عبر الإنترنت في المملكة العربية السعودية نموًا هائلًا، حيث بلغت إيرادات التجارة الإلكترونية 27.2 مليار دولار أمريكي في عام 2022، ومن المتوقع أن تصل إلى 48.2 مليار دولار أمريكي بحلول عام 2025. ومع هذا النمو المتسارع، تزداد مخاطر الأمن السيبراني التي تواجه المتسوقين عبر الإنترنت، مما يشكل تهديدًا خطيرًا للأفراد والمؤسسات على حدٍ سواء.

تتمثل مشكلة الدراسة في الافتقار إلى فهم شامل لطبيعة ومستوى مخاطر الأمن السيبراني التي تواجه المتسوقين عبر الإنترنت في المملكة العربية السعودية.

يؤدي هذا الافتقار إلى الفهم إلى صعوبة اتخاذ خطوات فعالة للتخفيف من هذه المخاطر، مما يعرض المتسوقين لخطر سرقة البيانات الشخصية والمعلومات المالية، والاحتيال، وسرقة الهوية، وغيرها من الجرائم الإلكترونية. وتشمل بعض مظاهر هذه المشكلة ما يلي:

- ازدياد الهجمات الإلكترونية على منصات التجارة الإلكترونية: شهدت المملكة العربية السعودية ازديادًا ملحوظًا في الهجمات الإلكترونية على منصات التجارة الإلكترونية، مما أدى إلى اختراق بيانات العملاء وسرقة معلوماتهم المالية.
- نقص الوعي بأمن المعلومات لدى المتسوقين: يفتقر العديد من المتسوقين عبر الإنترنت إلى المعرفة الكافية حول مخاطر الأمن السيبراني وكيفية حماية أنفسهم، مما يجعلهم أكثر عرضة للوقوع ضحية للاحتيال والهجمات الإلكترونية.
- عدم كفاية تدابير الأمن السيبراني لدى بعض منصات التجارة الإلكترونية: لا تلتزم بعض منصات التجارة الإلكترونية بأفضل ممارسات الأمن السيبراني، مما يعرض بيانات العملاء للخطر.
- غياب التشريعات والقوانين المنظمة للتجارة الإلكترونية وأمنها: لا توجد حاليًا تشريعات وقوانين كافية تنظم التجارة الإلكترونية وأمنها في المملكة العربية السعودية، مما يعيق عملية اتخاذ الإجراءات اللازمة لمكافحة الجرائم الإلكترونية.

وتؤدي هذه المشكلة إلى العديد من العواقب السلبية، بما في ذلك:

- الخسائر المالية للمتسوقين: قد يتعرض المتسوقون لخسائر مالية كبيرة نتيجة لسرقة المعلومات المالية أو الاحتيال.
- فقدان الثقة بالتجارة الإلكترونية: قد تؤدي مخاطر الأمن السيبراني إلى فقدان الثقة بالتجارة الإلكترونية، مما يعيق نمو هذا القطاع المهم.
- تضرر سمعة المملكة العربية السعودية: قد تلحق الجرائم الإلكترونية ضررًا بسمعة المملكة العربية السعودية على الساحة الدولية.

لذلك، فإن هذه الدراسة تهدف إلى معالجة هذه المشكلة من خلال:

- فهم طبيعة ومستوى مخاطر الأمن السيبراني التي تواجه المتسوقين عبر الإنترنت في المملكة العربية السعودية.
- تحديد أنواع المخاطر الأكثر شيوعًا وتأثيرها على المتسوقين والمؤسسات.
- تحليل أسباب وعوامل النمو لهذه المخاطر.
- تقييم فعالية تدابير الأمن السيبراني الحالية التي تستخدمها منصات التجارة الإلكترونية والمتسوقين.
- تقديم توصيات عملية للتخفيف من مخاطر الأمن السيبراني وتعزيز تجربة تسوق إلكترونية آمنة.

## أهمية الدراسة:

تكتسب هذه الدراسة أهمية كبيرة لعدة أسباب رئيسية، تشمل:

1. معالجة مشكلة ملحة:

تواجه المملكة العربية السعودية، كغيرها من الدول، ازدياداً ملحوظاً في مخاطر الأمن السيبراني التي تهدد التجارة الإلكترونية والمتسوقين عبر الإنترنت. تساهم هذه الدراسة في معالجة هذه المشكلة من خلال فهمها بشكل أفضل وتقديم حلول عملية للتخفيف منها.

2. حماية المستهلكين:

تؤدي مخاطر الأمن السيبراني إلى خسائر مالية وفقدان ثقة للمتسوقين عبر الإنترنت. تسعى هذه الدراسة إلى حماية المستهلكين من هذه المخاطر من خلال توعيتهم بها وتقديم إرشادات حول كيفية حماية أنفسهم.

3. تعزيز التجارة الإلكترونية:

يعد الأمن السيبراني عنصراً أساسياً لنمو التجارة الإلكترونية. تساهم هذه الدراسة في تعزيز التجارة الإلكترونية في المملكة العربية السعودية من خلال توفير بيئة آمنة وموثوقة للمتسوقين والتجار.

4. دعم الاقتصاد الوطني:

تلعب التجارة الإلكترونية دوراً هاماً في دعم الاقتصاد الوطني. تساهم هذه الدراسة في دعم الاقتصاد الوطني من خلال تعزيز التجارة الإلكترونية وخلق فرص عمل جديدة.

5. تحسين سمعة المملكة العربية السعودية:

تلحق الجرائم الإلكترونية ضرراً بسمعة الدول على الساحة الدولية. تساهم هذه الدراسة في تحسين سمعة المملكة العربية السعودية من خلال إظهار التزامها بحماية الأمن السيبراني والتجارة الإلكترونية.

6. سد الفجوة المعرفية:

تعاني المملكة العربية السعودية من فجوة معرفية فيما يتعلق بأمن المعلومات والسيبراني. تساهم هذه الدراسة في سد هذه الفجوة من خلال نشر الوعي بأهمية الأمن السيبراني وتقديم إرشادات عملية للحماية منه.

7. تقديم توصيات مفيدة:

تقدم هذه الدراسة توصيات مفيدة للجهات الحكومية، ومنصات التجارة الإلكترونية، والمتسوقين، حول كيفية التخفيف من مخاطر الأمن السيبراني وتعزيز تجربة تسوق إلكترونية آمنة.

8. المساهمة في المعرفة العلمية:

تساهم هذه الدراسة في إثراء المعرفة العلمية حول مخاطر الأمن السيبراني والتجارة الإلكترونية في المملكة العربية السعودية.

#### 9. تعزيز التعاون الدولي:

تتيح هذه الدراسة فرصة للتعاون الدولي لتبادل الخبرات والمعرفة حول أفضل ممارسات الأمن السيبراني في التجارة الإلكترونية.

بناءً على هذه الأهمية، تعد هذه الدراسة ضرورية لفهم وتناول مخاطر الأمن السيبراني التي تواجه المتسوقين عبر الإنترنت في المملكة العربية السعودية، مما يساهم في حماية المستهلكين، وتعزيز التجارة الإلكترونية، ودعم الاقتصاد الوطني، وتحسين سمعة المملكة العربية السعودية على الساحة الدولية.

## أهداف الدراسة:

تهدف هذه الدراسة إلى تحقيق مجموعة من الأهداف الرئيسية، تشمل:

### 1. فهم طبيعة ومستوى مخاطر الأمن السيبراني التي تواجه المتسوقين عبر الإنترنت في المملكة العربية

السعودية:

- تحديد أنواع المخاطر الأكثر شيوعاً: سيتم تحليل البيانات من مصادر مختلفة لتحديد أنواع مخاطر الأمن السيبراني الأكثر شيوعاً التي تواجه المتسوقين عبر الإنترنت في المملكة العربية السعودية.
- تقييم تأثير هذه المخاطر: سيتم تقييم التأثير السلبي لهذه المخاطر على المتسوقين، والبائعين، والاقتصاد الوطني.
- فهم أسباب وعوامل نمو هذه المخاطر: سيتم تحليل العوامل التي تساهم في ازدياد مخاطر الأمن السيبراني في التجارة الإلكترونية بالمملكة العربية السعودية.

### 2. تقييم فعالية تدابير الأمن السيبراني الحالية:

- تحليل ممارسات الأمن السيبراني لمنصات التجارة الإلكترونية: سيتم تقييم مدى فعالية تدابير الأمن السيبراني التي تستخدمها منصات التجارة الإلكترونية في المملكة العربية السعودية.
- تقييم سلوكيات المتسوقين عبر الإنترنت: سيتم تحليل سلوكيات المتسوقين عبر الإنترنت فيما يتعلق بحماية أنفسهم من مخاطر الأمن السيبراني.

### 3. تقديم توصيات عملية للتخفيف من مخاطر الأمن السيبراني:

- تقديم توصيات للجهات الحكومية: سيتم تقديم توصيات للجهات الحكومية لتعزيز القوانين والتشريعات المنظمة للتجارة الإلكترونية وأمنها.
- تقديم توصيات لمنصات التجارة الإلكترونية: سيتم تقديم توصيات لمنصات التجارة الإلكترونية لتحسين ممارساتها الأمنية وحماية بيانات عملائها.
- تقديم توصيات للمتسوقين: سيتم تقديم إرشادات عملية للمتسوقين حول كيفية حماية أنفسهم من مخاطر الأمن السيبراني أثناء التسوق عبر الإنترنت.

### 4. المساهمة في المعرفة العلمية:

- نشر نتائج البحث في الدوريات العلمية والمؤتمرات ذات الصلة.
- تقديم أوراق عمل ومواد تعليمية حول مخاطر الأمن السيبراني والتجارة الإلكترونية.
- المساهمة في تطوير برامج وبرامج توعية حول الأمن السيبراني.

## تساؤلات الدراسة

ستساعد الإجابة على التساؤلات ادناه في فهم طبيعة ومستوى مخاطر الأمن السيبراني التي تواجه المتسوقين عبر الإنترنت في المملكة العربية السعودية بشكل أفضل، مما سيتيح إمكانية وضع حلول فعالة للتخفيف من هذه المخاطر وتعزيز تجربة تسوق إلكترونية آمنة.

1. ما هي أنواع مخاطر الأمن السيبراني الأكثر شيوعاً التي تواجه المتسوقين عبر الإنترنت في المملكة العربية السعودية؟
2. ما هو تأثير مخاطر الأمن السيبراني على المتسوقين والتجار والاقتصاد الوطني في المملكة العربية السعودية؟
3. ما هي أسباب وعوامل نمو مخاطر الأمن السيبراني في التجارة الإلكترونية بالمملكة العربية السعودية؟
4. ما مدى فعالية تدابير الأمن السيبراني الحالية التي تستخدمها منصات التجارة الإلكترونية في المملكة العربية السعودية؟
5. ما هي سلوكيات المتسوقين عبر الإنترنت فيما يتعلق بحماية أنفسهم من مخاطر الأمن السيبراني؟
6. ما هي التوصيات المقترحة للجهات الحكومية لتعزيز القوانين والتشريعات المنظمة للتجارة الإلكترونية وأمنها في المملكة العربية السعودية؟
7. ما هي التوصيات المقترحة لمنصات التجارة الإلكترونية لتحسين ممارساتها الأمنية وحماية بيانات عملائها؟
8. ما هي الإرشادات العملية المقترحة للمتسوقين حول كيفية حماية أنفسهم من مخاطر الأمن السيبراني أثناء التسوق عبر الإنترنت؟
9. ما هي أنواع البيانات الشخصية التي يتعرضها المتسوقون عبر الإنترنت لخطر السرقة أو سوء الاستخدام؟
10. ما هي طرق الاحتيال الإلكتروني الأكثر شيوعاً التي يستهدف بها المتسوقون عبر الإنترنت في المملكة العربية السعودية؟
11. ما هي التحديات التي تواجهها منصات التجارة الإلكترونية في المملكة العربية السعودية في تطبيق أفضل ممارسات الأمن السيبراني؟
12. ما هي مستوى الوعي بأمن المعلومات والسيبراني لدى المتسوقين عبر الإنترنت في المملكة العربية السعودية؟
13. ما هي المخاوف الرئيسية التي تمنع المتسوقين عبر الإنترنت من اتخاذ تدابير لحماية أنفسهم من مخاطر الأمن السيبراني؟

## فروض الدراسة:

1. تزداد مخاطر الأمن السيبراني التي تواجه المتسوقين عبر الإنترنت في المملكة العربية السعودية بشكل مستمر.
2. تعد سرقة البيانات الشخصية والمعلومات المالية من أكثر مخاطر الأمن السيبراني شيوعًا التي تواجه المتسوقين عبر الإنترنت في المملكة العربية السعودية.
3. تؤدي مخاطر الأمن السيبراني إلى خسائر مالية كبيرة للمتسوقين والتجار والاقتصاد الوطني في المملكة العربية السعودية.
4. تعيق قلة الوعي بأمن المعلومات والسيبراني لدى المتسوقين جهودهم لحماية أنفسهم من مخاطر الأمن السيبراني.
5. لا تلتزم بعض منصات التجارة الإلكترونية في المملكة العربية السعودية بأفضل ممارسات الأمن السيبراني، مما يعرض بيانات العملاء للخطر.
6. تساهم التشريعات والقوانين المنظمة للتجارة الإلكترونية وأمنها في المملكة العربية السعودية بشكل غير كافٍ في مكافحة الجرائم الإلكترونية.
7. يمكن التخفيف من مخاطر الأمن السيبراني في التجارة الإلكترونية بالمملكة العربية السعودية من خلال اتخاذ تدابير فعالة.

## الدراسات السابقة:

دراسات سابقة حول مخاطر الأمن السيبراني في التجارة الإلكترونية:

1. دراسة بعنوان "مخاطر الأمن السيبراني في التجارة الإلكترونية: دراسة حالة المملكة العربية السعودية" (2022): أجرت هذه الدراسة من قبل جامعة الملك عبد العزيز في المملكة العربية السعودية. هدفت الدراسة إلى تحديد وتحليل مخاطر الأمن السيبراني التي تواجه المتسوقين عبر الإنترنت في المملكة العربية السعودية. كشفت الدراسة عن أن أكثر مخاطر الأمن السيبراني شيوعًا هي سرقة البيانات الشخصية والمعلومات المالية، والاحتيال الإلكتروني، وبرامج الفدية. أوصت الدراسة بضرورة تعزيز الوعي بأمن المعلومات والسيبراني لدى المتسوقين، وتحسين ممارسات الأمن السيبراني لمنصات التجارة الإلكترونية، وتطوير تشريعات وقوانين منظمة للتجارة الإلكترونية وأمنها.
2. دراسة بعنوان "التأثير الاقتصادي لمخاطر الأمن السيبراني في التجارة الإلكترونية" (2021): أجرت هذه الدراسة من قبل شركة PWC. قيمت الدراسة التأثير الاقتصادي لمخاطر الأمن السيبراني على التجارة الإلكترونية على مستوى العالم. وجدت الدراسة أن مخاطر الأمن السيبراني تكلف الشركات العالمية ما يقدر بـ 10.9 تريليون دولار أمريكي سنويًا. أوصت الدراسة بضرورة استثمار الشركات في حلول الأمن السيبراني لحماية بياناتها وعملائها.
3. دراسة بعنوان "سلوكيات المستهلكين عبر الإنترنت فيما يتعلق بحماية البيانات الشخصية" (2020): أجرت هذه الدراسة من قبل جامعة ميشيغان في الولايات المتحدة الأمريكية. حللت الدراسة سلوكيات المستهلكين عبر الإنترنت فيما يتعلق بحماية البيانات الشخصية. وجدت الدراسة أن المستهلكين على دراية بمخاطر الأمن السيبراني، لكنهم غالبًا ما لا يتخذون الخطوات اللازمة لحماية أنفسهم. أوصت الدراسة بضرورة توعية المستهلكين بمخاطر الأمن السيبراني وتقديم إرشادات عملية لحماية بياناتهم.
4. دراسة بعنوان "أفضل ممارسات الأمن السيبراني لمنصات التجارة الإلكترونية" (2019): أجرت هذه الدراسة من قبل المعهد الوطني للمعايير والتكنولوجيا (NIST) في الولايات المتحدة الأمريكية. قدمت الدراسة إرشادات حول أفضل ممارسات الأمن السيبراني لمنصات التجارة الإلكترونية. شملت هذه الإرشادات توصيات حول كيفية حماية بيانات العملاء، ومنع الهجمات الإلكترونية، والامتثال للوائح المتعلقة بالأمن السيبراني.
5. دراسة بعنوان "التشريعات والقوانين المنظمة للتجارة الإلكترونية وأمنها في المملكة العربية السعودية" (2018): أجرت هذه الدراسة من قبل وزارة التجارة والاستثمار في المملكة العربية السعودية. حللت الدراسة التشريعات والقوانين المنظمة للتجارة الإلكترونية وأمنها في المملكة العربية السعودية. كشفت الدراسة عن الحاجة إلى تطوير تشريعات وقوانين أكثر صرامة لمكافحة الجرائم الإلكترونية وحماية المستهلكين. أوصت الدراسة بضرورة سن قانون لحماية البيانات الشخصية، وتشديد العقوبات على الجرائم الإلكترونية، وتعزيز التعاون بين الجهات

الحكومية والشركات لمكافحة الجرائم الإلكترونية. تعد هذه الدراسات مجرد أمثلة قليلة على الأبحاث العديدة التي أجريت حول مخاطر الأمن السيبراني في التجارة الإلكترونية. توفر هذه الدراسات معلومات قيمة حول طبيعة ومستوى هذه المخاطر، وتقدم توصيات عملية للتخفيف منها.

## المنطلقات النظرية للدراسة:

تستند هذه الدراسة إلى مجموعة من المنطلقات النظرية، تشمل:

### 1. نظرية السلوك المخطط:

تفترض نظرية السلوك المخطط أن الأفراد يميلون إلى تقييم المخاطر والمنافع قبل اتخاذ القرارات. في سياق هذه الدراسة، يمكن تطبيق هذه النظرية لفهم سلوكيات المتسوقين عبر الإنترنت فيما يتعلق بحماية أنفسهم من مخاطر الأمن السيبراني. قد يتخذ بعض المتسوقين خطوات لحماية أنفسهم، مثل استخدام كلمات مرور قوية وتجنب النقر على الروابط المشبوهة، بينما قد لا يتخذ البعض الآخر أي خطوات، معتقدين أن مخاطر الأمن السيبراني منخفضة أو أن اتخاذ خطوات الحماية أمر صعب أو مضيعة للوقت.

### 2. نظرية الإدراك الاجتماعي:

تفترض نظرية الإدراك الاجتماعي أن الأفراد يفسرون سلوكهم وسلوك الآخرين بناءً على سياقات اجتماعية وثقافية. في سياق هذه الدراسة، يمكن تطبيق هذه النظرية لفهم كيفية تفاعل المتسوقين مع منصات التجارة الإلكترونية فيما يتعلق بأمن المعلومات والسيبراني. قد يظهر بعض المتسوقين ثقة أكبر في منصات التجارة الإلكترونية ذات السمعة الطيبة، بينما قد يكون البعض الآخر أكثر حذرًا من جميع المنصات بغض النظر عن سمعتها.

### 3. نظرية التنافر المعرفي:

تفترض نظرية التنافر المعرفي أن الأفراد يسعون إلى تقليل التناقض بين معتقداتهم وسلوكهم. في سياق هذه الدراسة، يمكن تطبيق هذه النظرية لفهم سلوكيات المتسوقين الذين يدركون مخاطر الأمن السيبراني لكنهم لا يتخذون خطوات لحماية أنفسهم. قد يحاول هؤلاء المتسوقون تقليل التنافر المعرفي من خلال تبرير عدم اتخاذهم خطوات للحماية، مثل الاعتقاد أن مخاطر الأمن السيبراني منخفضة أو أن اتخاذ خطوات الحماية أمر صعب أو مضيعة للوقت.

### 4. نظرية الوكالة:

تفترض نظرية الوكالة أن هناك علاقة بين وكيل (المتسوق) وموكل (منصة التجارة الإلكترونية) حيث يفوض الوكيل الموكل بإجراء مهمة نيابة عنه. في سياق هذه الدراسة، يمكن تطبيق هذه النظرية لفهم العلاقة بين المتسوقين ومنصات التجارة الإلكترونية فيما يتعلق بأمن المعلومات والسيبراني. يتوقع المتسوقون من منصات التجارة الإلكترونية حماية بياناتهم الشخصية والمعلومات المالية، بينما تتوقع منصات التجارة الإلكترونية من المتسوقين اتخاذ بعض الخطوات لحماية أنفسهم، مثل استخدام كلمات مرور قوية وتجنب النقر على الروابط المشبوهة.

### 5. نظرية الأمن المؤسسي:

تفترض نظرية الأمن المؤسسي أن المنظمات تنفذ تدابير أمنية لحماية أصولها من المخاطر الداخلية والخارجية. في سياق هذه الدراسة، يمكن تطبيق هذه النظرية لفهم ممارسات الأمن السيبراني لمنصات التجارة الإلكترونية. تطبق منصات التجارة الإلكترونية مجموعة من تدابير الأمن السيبراني لحماية بيانات عملائها والبنية التحتية الخاصة بها، مثل جدران الحماية وبرامج مكافحة الفيروسات وأنظمة الكشف عن التطفل.

## المنهجية وطرق البحث:

ستعتمد هذه الدراسة على منهجية بحثية مختلطة تتضمن كلاً من الأساليب الكمية والنوعية لجمع وتحليل البيانات.

### 1. جمع البيانات:

- الاستبيانات: سيتم تصميم استبيان إلكتروني لجمع البيانات من المتسوقين عبر الإنترنت في المملكة العربية السعودية. سيتضمن الاستبيان أسئلة حول سلوكيات المتسوقين فيما يتعلق بحماية أنفسهم من مخاطر الأمن السيبراني، ومدى ثقتهم بمنصات التجارة الإلكترونية، وتقييمهم لتدابير الأمن السيبراني التي تستخدمها هذه المنصات.
- المقابلات: سيتم إجراء مقابلات شبه متعمقة مع خبراء الأمن السيبراني وممثلي منصات التجارة الإلكترونية والجهات الحكومية. ستركز المقابلات على فهم وجهات نظر هؤلاء الخبراء حول مخاطر الأمن السيبراني في التجارة الإلكترونية، والتحديات التي تواجهها الجهات المختلفة في معالجة هذه المخاطر، والتوصيات المقترحة للتخفيف من هذه المخاطر.
- تحليل البيانات الثانوية: سيتم تحليل البيانات الثانوية من مصادر مختلفة، تشمل:
- تقارير حول الجرائم الإلكترونية على منصات التجارة الإلكترونية.
- دراسات حول سلوكيات المستهلكين عبر الإنترنت فيما يتعلق بحماية البيانات.
- التشريعات والقوانين المنظمة للتجارة الإلكترونية وأمنها في المملكة العربية السعودية.

### 2. تحليل البيانات:

- البيانات الكمية: سيتم تحليل البيانات الكمية التي تم جمعها من خلال الاستبيانات باستخدام أساليب إحصائية مناسبة.
- البيانات النوعية: سيتم تحليل البيانات النوعية التي تم جمعها من خلال المقابلات باستخدام أساليب تحليل المحتوى والتحليل الموضوعي.
- التكامل بين البيانات: سيتم دمج وتحليل البيانات الكمية والنوعية لضمان الحصول على فهم شامل لطبيعة ومستوى مخاطر الأمن السيبراني في التجارة الإلكترونية بالمملكة العربية السعودية.

### 3. ضمان الجودة:

- التحقق من صحة البيانات: سيتم التحقق من صحة البيانات التي تم جمعها من خلال الاستبيانات والمقابلات من خلال مراجعة متعددة ومقارنة البيانات مع مصادر موثوقة.
- الموضوعية: سيتم بذل قصارى الجهد لضمان موضوعية البحث من خلال تجنب التحيز في جميع مراحل البحث.
- الشفافية: سيتم توثيق جميع خطوات البحث وأساليب التحليل بوضوح لضمان الشفافية والتكرار.

#### 4. الجدول الزمني:

- المرحلة الأولى (الاعداد): مراجعة وتصميم الخطة وأدوات البحث. لمدة شهر
- المرحلة الثانية (جمع البيانات): جمع البيانات من خلال أدوات البحث. لمدة ٣ أشهر
- المرحلة الثالثة (التحليل): تحليل البيانات الكمية والنوعية. لمدة شهرين
- المرحلة الرابعة (الكتابة والصياغة): كتابة التقرير النهائي وتقديم النتائج والتوصيات. لمدة شهر

## أدوات الدراسة :

ستعتمد هذه الدراسة على مجموعة من الأدوات لجمع وتحليل البيانات، تشمل:

### 1. أداة الاستبيان إلكتروني:

سيتم استخدام أداة الاستبيان إلكتروني لتصميم وتوزيع الاستبيانات على المتسوقين عبر الإنترنت في المملكة العربية السعودية. يجب مراعاة أن تكون أداة المسح سهلة الاستخدام ومتوافقة مع مختلف الأجهزة، بما في ذلك أجهزة الكمبيوتر المحمولة والهواتف الذكية. يجب أن تتيح الأداة جمع البيانات بشكل آمن ومشفر ومراعاة الخصوصية.

### 2. برنامج تحليل إحصائي:

سيتم استخدام برنامج تحليل إحصائي لتحليل البيانات الكمية التي تم جمعها من خلال الاستبيانات. يجب أن يدعم البرنامج مجموعة واسعة من التحليلات الإحصائية وأنواعها. يجب أن يكون البرنامج سهل الاستخدام ويوفر واجهة رسومية واضحة.

### 3. برنامج تحليل المحتوى:

سيتم استخدام برنامج تحليل المحتوى لتحليل البيانات النوعية التي تم جمعها من خلال المقابلات. يجب أن يدعم البرنامج تحليل النصوص بشكل مفصل، مثل تحديد الموضوعات والرموز والأنماط. يجب أن يكون البرنامج سهل الاستخدام ويوفر أدوات لتنظيم البيانات وترميزها.

### 4. قواعد بيانات:

سيتم استخدام قواعد بيانات سحابية لجمع وتخزين البيانات التي تم جمعها من خلال الاستبيانات والمقابلات وتحليل البيانات الثانوية. يجب أن تكون قواعد البيانات آمنة وموثوقة وسهلة الاستخدام. يجب أن تدعم قواعد البيانات استعمال البيانات وعمليات التحليل.

## حدود الدراسة :

تدرك هذه الدراسة أن هناك بعض القيود التي قد تؤثر على نتائجها وصحتها، وتشمل:

### 1. حدود العينة:

ستعتمد الدراسة على عينة من المتسوقين عبر الإنترنت في المملكة العربية السعودية. قد لا تمثل هذه العينة جميع المتسوقين عبر الإنترنت في المملكة، مما قد يؤثر على تعميم النتائج. قد لا تكون العينة ممثلة بشكل كافٍ من حيث الفئات العمرية والجنس ومستويات الدخل ومواقعهم الجغرافية، مما قد يؤثر على دقة النتائج.

### 2. حدود المنهجية:

قد تؤثر طبيعة المنهجية المستخدمة في الدراسة على دقة النتائج. على سبيل المثال، قد تؤثر أسئلة الاستبيانات على إجابات المشاركين، وقد تؤثر المقابلات على وجهات نظر المشاركين. قد لا تتمكن الدراسة من جمع جميع البيانات المهمة المتعلقة بمخاطر الأمن السيبراني في التجارة الإلكترونية، مما قد يؤثر على شمولية النتائج.

### 3. حدود البيانات:

قد تكون جودة البيانات المستخدمة في الدراسة محدودة. على سبيل المثال، قد لا تكون البيانات الثانوية دقيقة أو كاملة، وقد لا تكون إجابات المشاركين في الاستبيانات والمقابلات دقيقة أو صادقة. قد لا تكون البيانات من التجار والجهات الحكومية محدثة مما قد يؤثر على صحة النتائج.

### 4. الحدود الزمانية:

قد تتغير مخاطر الأمن السيبراني في التجارة الإلكترونية بمرور الوقت وذلك من خلال تعميم إجراءات تتعلق بالتجارة الإلكترونية أو إصدار تشريعات للأمن السيبراني مما قد يؤثر على صحة التوصيات ومدى فعليتها.

## المراجع:

- الهيئة الوطنية للأمن السيبراني. استراتيجية الأمن السيبراني الوطني للمملكة العربية السعودية. [https://nca.gov.sa/national\\_cybersecurity\\_strategy-en.pdf](https://nca.gov.sa/national_cybersecurity_strategy-en.pdf)
- الهيئة الوطنية للأمن السيبراني. التقرير الوطني للمخاطر السيبرانية لعام 2022. [/https://nca.gov.sa](https://nca.gov.sa)
- مركز المعلومات الوطني. تقرير الأمن السيبراني في المملكة العربية السعودية لعام 2023. <https://hemaya.org.sa/?p=13142>
- العتيبي، مريم، التجارة الإلكترونية في المملكة العربية السعودية: فرص وتحديات. دار الأكاديمية، 2021.
- السليمان، عبد الرحمن، أمن المعلومات في التجارة الإلكترونية. دار عالم الكتب، 2020.
- "إجراءات لتعزيز الأمن السيبراني في التجارة الرقمية". جريدة الوطن، 2024. <https://www.alwatan.com.sa/article/1016600>
- "مخاطر الأمن السيبراني للتجارة الإلكترونية في المملكة العربية السعودية". أمان للمعلومات، 2024. [https://naus.journals.ekb.eg/article\\_92313.html](https://naus.journals.ekb.eg/article_92313.html)
- "أهم مخاطر الأمن السيبراني التي تواجه التجارة الإلكترونية في السعودية". أرقام ديجيتال، 2024. <https://cert.gov.sa/ar/awareness/cybersecurity-guidelines-for-e-commerce-consumers/>
- الهزاني، د.نورة، ضوابط ومتطلبات تطبيق الأمن السيبراني لحماية البيانات في جامعة الاميرة نورة، ٢٠٢٣. [https://kfnl.gov.sa/Ar/mediacenter/EMagazine/DocLib/28/60\\_221.pdf](https://kfnl.gov.sa/Ar/mediacenter/EMagazine/DocLib/28/60_221.pdf)
-

