أدى الإنترنت والتطور الرقمي إلى إحداث تحول جذري في أساليب التواصل وتبادل المعلومات بين الأفراد. فنحن نقضي فترات طويلة من الزمن على منصات التواصل الاجتماعي، أصبحت غالبية المؤسسات تعتمد بشكل أساسي على نظم إدارة إلكترونية لمتابعة أعمالها وإدارة حساباتها، مما جعل العمليات الإدارية تُدار بشكل كبير عبر الإنترنت. علاوة على الأجهزة المنزلية التي أصبح التحكم بها ممكنًا من خلال تقنيات الاتصال الرقمي. في ظل هذا الاعتماد المتزايد على الإنترنت، والسؤال الذي يطرح نفسه هو: ماذا يمكن أن يحدث إذا تمكن أحد المهاجمين من اختراق حاسوبك أو هاتفك المحمول؟ أو السيطرة على بريدك الإلكتروني أو حساباتك على منصات التواصل الاجتماعي؟ بل والأخطر، ماذا لو تمكن من الوصول إلى حساباتك المالية لا شك أن الإنترنت جلب فوائد كبيرة إلى حياتنا اليومية، ومع ذلك، حيث يتطلب التعامل مع الفضاء الإلكتروني قدراً عالياً من الوعي بمخاطره وكيفية الاستفادة المثلى منه. كونه عالمًا مفتوحًا بلا قيود صارمة، أخلاقية وأمنية. تُعرف هذه الجوانب السلبية بمخاطر الإنترنت، لذلك تُعتبر هذه الهجمات أخطر من الحروب التقليدية مثل النووية والعسكرية أو حتى الاقتصادية. الهجمات السيبرانية باتت الساحة الجديدة للصراع بين الدول، ومع هذا الاستخدام المتزايد للتكنولوجيا في مختلف نواحي الحياة، تصاعدت الهجمات الإلكترونية الموجهة ضد مستخدمي الشبكة العالمية بشكل ملحوظ. الأمن السيبراني يُعد مسؤولية مشتركة تقع على عاتق الجميع، حيث يمكن أن يؤدي الاختراق الذي يصيب جهازًا أو نظامًا تقنيًا معينًا إلى تهديد أنظمة وأجهزة أخرى مرتبطة به. يرتبط الأمن السيبراني بحماية الهواتف الذكية، أجهزة الحاسوب والأجهزة اللوحية، بالإضافة إلى تأمين البريد الإلكتروني والخدمات المصرفية الإلكترونية والمعلومات الشخصية المخزنة على هذه الوسائل من السرقة أو الاحتيال أو التجسس. أما بالنسبة للمؤسسات والشركات، فإنه عنصر أساسي للحفاظ على سلامة البيانات والأنظمة والأجهزة الخاصة بها. مما يجعل الالتزام بأعلى معايير الأمن السيبراني ضرورة لا غنى عنها للحفاظ على استمرارية الأعمال وسلامتها. مما يفتح آفاقًا للتعامل مع تقنيات الذكاء الاصطناعي ومقتضيات الثورة الصناعية الرابعة. لذلك، إلى جانب صيانة البنية التحتية الحساسة والقطاعات الحيوية والخدمات الحكومية ذات الأولوية شكل التكنولوجيا المالية عنصرًا رئيسيًا في الحياة اليومية بالمملكة، حيث شهد هذا القطاع نموًا هائلًا في السنوات الأخيرة، مما يسهم في تحسين كفاءة العمليات وزيادة معدلات الشمول المالي. يتزامن التوسع في استخدام التطبيقات الرقمية للمعاملات المالية مع ارتفاع التحديات المرتبطة بالأمن السيبراني. حيث تؤثر بشكل مباشر على ثقة المستخدمين في هذه الخدمات. لذلك، أثبتت دراسة لمحمد البحر وزملائه (2024) أن تثقيف العملاء حول قضايا الأمن السيبراني ينعكس إيجابًا على رضاهم وثقتهم بالخدمات المصرفية الرقمية، كما شددت دراسة أخرى (2024) حول التهديدات الأمنية في قطاع التكنولوجيا المالية على ضرورة تنفيذ استراتيجيات متكاملة لحماية البيانات، أظهرت دراسات إضافية كذلك أن إدراك المستخدمين لمستوى الأمان يؤثر بشكل كبير على نيتهم لاستعمال منصات الدفع الرقمية. تركز هذه الدراسة على مفاهيم نظرية أساسية مثل مفهوم "الأمن السيبراني"، تُعنى الدراسة بمفهوم "وعي المستخدم"، تهدف الدراسة إلى تعزيز الأمن السيبراني في تطبيقات الدفع عبر الهاتف المحمول بالمملكة عبر تحديد أبرز المخاطر المرتبطة بهذه الأنظمة، مع التركيز على الهجمات الإلكترونية الشائعة وتأثيراتها. وستعمل الدراسة على تقييم كفاءة التدابير الأمنية المستخدمة حاليًا وتقديم توصيات لتحسين هذه التدابير لتصبح أكثر قدرة على مواجهة المخاطر المستقبلية.

تسعى هذه الدراسة إلى تعزيز الأمن السيبراني في تطبيقات الدفع عبر الهاتف المحمول في المملكة العربية السعودية، من خلال تحديد المخاطر الأمنية المرتبطة بتطبيقات الدفع، مع التركيز على الهجمات الإلكترونية الشائعة وتأثيراتها على مستوى الأمان. كما تعمل الدراسة على تقييم فعالية التدابير الأمنية الحالية المستخدمة في تطبيقات الدفع، حيث ستقوم بتقديم توصيات لتحسين هذه التدابير لمواجهة التهديدات المتزايدة. بالإضافة إلى ذلك، مما يساعد على تطوير استراتيجيات لرفع هذا الوعي وتعزيز فهم المستخدمين لمخاطر الأمن السيبراني. علاوة على ذلك،