

جرائم الذكاء الاصطناعي والحلول المقترحة –حالة شركة Uber Technologies – Artificial Intelligence Crimes and Proposed Solutions - Case of Uber Technologies –

فداوي أمينة*

جامعة الشاذلي بن جديد - الطارف، الجزائر

a.feddaoui@univ-eltarf.dz

- تاريخ الإرسال: 2025/02/28 - تاريخ القبول: 2025/04/26 - تاريخ النشر: 2025/09/22

الملخص: يمكن تعريف الذكاء الاصطناعي على أنه مجموع التقنيات والوسائل و الطرق الحديثة التي تهدف إلى محاكاة الذكاء البشري من خلال نماذج تصنيع وابتكار آلات وتطبيقات متطورة في العديد من المجالات، وفي ظل هذه المرتكزات هدفت هذه الدراسة إلى عرض الجوانب النظرية المختلفة للذكاء الاصطناعي، أهميته وأنواعه، وكذا التطرق إلى أهم الجرائم الناتجة عن الذكاء الاصطناعي، مع الالتفات إلى الهجمة السيبرانية التي كانت ضحيتها شركة Uber Technologies خلال سنة 2022م، وتوصلت الدراسة إلى مجموعة من النتائج أهمها أن جرائم الذكاء الاصطناعي عديدة أبرزها ما يعرف بتصيد المعلومات، برامج الفدية، سرقة الهوية، اختراق بيانات الشركات والبنوك، الهندسة الاجتماعية والقرصنة، كما توصلت الدراسة إلى مجموعة من الحلول المقترحة أهمها ضرورة التركيز على برامج الأمن السيبراني لحماية الأنظمة والشبكات والمواقع الإلكترونية للأفراد والشركات من أجل التصدي للهجمات الإلكترونية المختلفة.

الكلمات المفتاحية: جرائم، الذكاء الاصطناعي، الحلول، شركة Uber Technologies.

Abstract: Artificial intelligence defined as the sum of modern technologies, tools and methods that aim to simulate human intelligence through models of manufacturing and creating advanced machines and applications in many fields. In light of these foundations, this study aimed to present the various theoretical aspects of artificial intelligence, its importance and types, as well as to address the most important crimes resulting from artificial intelligence, with attention to the case of Uber Technologies during the year 2022. The study concluded a set of results, the most important of which is that artificial intelligence crimes are many, and the most notably known as phishing, ransom ware, identity theft, hacking companies and banks' data, and social engineering. The study also found a set of proposed solutions, the most important of which is the need to focus on cyber security programs to protect systems, networks, and websites for individuals and companies in order to confront various attacks.

Keywords : Crimes, Artificial Intelligence, Solutions, Uber Technologies.

* المؤلف المرسل: فداوي أمينة.

مقدمة:

تعتبر التكنولوجيا ضرورة حتمية في عالمنا المعاصر نتيجة للعولمة واقتصاد السوق الحرة، وقد تسابقت الدول في الآونة الأخيرة نحو تبني التكنولوجيا المتقدمة، وأبرز تلك الدول اليابان و الولايات المتحدة الأمريكية، فانتشرت استخدامات الانترنت و تطبيقات الهواتف الذكية، وكذلك الروبوتات التي تحاكي العقل البشري وهذا ما يسمى بالذكاء الاصطناعي، بحيث يقصد به كل التقنيات و الآليات الحديثة التي تعمل معا من أجل محاكاة العقل البشري من خلال برمجة الآلات والروبوت ليفكر و يستنتج ويصح ذاتيا مثل الإنسان، ويعتبر الذكاء الاصطناعي حديث الساعة نظرا لإيجابياته وفوائده الكثيرة، ولكن الذكاء الاصطناعي أيضا له مخاطر وسلبات تنجم عن عدم التحكم في التكنولوجيا مما يجعل منها طريقا خطرا في يد بعض المتسللين، فظهرت الجريمة الالكترونية أو ما يسميها البعض بالجريمة السيبرانية ونقشت بكثرة في قطاع الأعمال، فكثيرا ما نسمع عن جرائم سرقة الهوية، انتحال الشخصية، الهندسة الاجتماعية وبرامج الفدية، واختراق مواقع كبرى الشركات، وتعتبر شركة أوبر Uber technologies أحد كبرى الشركات التي وقعت ضحية هجمة سيبرانية ارتكبتها متسلل وقام باختراق بياناتها، وبهذا صار لابد من محاربة جرائم الذكاء الاصطناعي عن طريق عدة أساليب تكنولوجية في إطار ما يعرف بالأمن السيبراني، وفي ظل هذه المرتكزات إرتأينا إعتقاد موضوع هذه الدراسة، ولتحقيق أهداف هذه الدراسة تمت صياغة تساؤلها الرئيسي كمايلي: "ماهي جرائم الذكاء الاصطناعي وماهي الحلول المقترحة لمواجهتها بالنظر لحالة شركة Uber Technologies؟"

وللإجابة عن التساؤل الرئيسي للدراسة تم طرح الأسئلة الفرعية التالية:

- ما هو الذكاء الاصطناعي؟ وماهي أهميته؟ وأنواعه؟
- ما هو تعريف الجريمة الالكترونية؟ وماهي أنواع جرائم الذكاء الاصطناعي؟
- ماهي الحلول المقترحة لتفادي الوقوع كضحية للجرائم الناتجة عن الذكاء الاصطناعي؟
- كيف تعرضت شركة Uber Technologies للهجمة الالكترونية سنة 2022م وماهي الأسباب؟
- كيف استطاعت الشركة الخروج من أزمة وقوعها كضحية للهجمة الالكترونية بدون أضرار؟

وللإجابة عن التساؤل الرئيسي للدراسة تمت صياغة فرضية الدراسة كمايلي:

الفرضية الأولى: تمكنت شركة Uber Technologies من مواجهة الهجمة الالكترونية التي تعرضت لها من خلال الإجراءات الأمنية السيبرانية.

الفرضية الثانية: تمكنت شركة Uber Technologies من مواجهة الهجمة الالكترونية التي تعرضت لها من خلال الإجراءات القانونية.

وتتبع أهمية هذه الدراسة من أهمية مواجهة الجريمة بصفة عامة، والجريمة الالكترونية بصفة خاصة، لاسيما ونقشي استخدامها في المجتمع باستخدام الهواتف الذكية بمختلف التقنيات والأساليب الحديثة والتي باتت تشكل خطرا حقيقيا على حياة الفرد والمجتمع، كما تتبع أهمية الدراسة أيضا من أهمية التطرق لمخاطر التكنولوجيا وضرورة اتخاذ الإجراءات الوقائية من خلال الأمن السيبراني، كما تهدف هذه الدراسة إلى التطرق لمجموعة من العناصر وهي مفهوم الذكاء الاصطناعي، أهميته وأنواعه، ماهية الجريمة الالكترونية، أنواع جرائم الذكاء الاصطناعي، وكذا الحلول المقترحة لمواجهتها، ثم محاولة الاستفادة من حالة شركة Uber technologies سنة 2022م.

لقد تم الاعتماد في هذه الدراسة على المنهج الاستنباطي من خلال التحليل النظري المنطقي الاستدلالي لربط الجوانب النظرية المتعلقة بالذكاء الاصطناعي وأنواع الجرائم المتعلقة به والحلول المقترحة لتجنب الجريمة الالكترونية، كما تم الاعتماد على منهج دراسة الحالة من خلال تحليل حالة شركة Uber technologies، والاستفادة منها للخروج بتوصيات ضرورية لمواجهة مختلف أنواع الجرائم المتعلقة بالذكاء الاصطناعي. وقد اقتصر حدود هذه الدراسة على جرائم الذكاء الاصطناعي دون غيرها من الجرائم المختلفة، كما اقتصر حدودها المكانية على حالة شركة رائدة في مجال النقل ومتعددة الجنسيات وهي شركة Uber technologies ، أما بالنسبة للحدود الزمنية للدراسة فكانت متعلقة بسنة 2022م.

لقد تم تقسيم هذه الدراسة إلى ثلاث أقسام رئيسية بحيث تناول القسم الأول بعنوان "عموميات حول الذكاء الاصطناعي" مفهوم الذكاء الاصطناعي، أهميته وأنواعه، وتناول القسم الثاني بعنوان "أنواع الجرائم المتعلقة بالذكاء الاصطناعي والحلول المقترحة لمواجهتها" مفهوم الجريمة الالكترونية، أنواع الجرائم المتعلقة بالذكاء الاصطناعي، والحلول المقترحة لمواجهتها، كما تناول القسم الثالث بعنوان "دراسة حالة شركة Uber technologies"، تقديم الشركة محل الدراسة، ووقائع الجريمة السيبرانية التي وقعت ضحيتها، وكيفية مواجهتها لها، وفي خاتمة الدراسة تم عرض النتائج و الاقتراحات التي يمكن اعتبارها كتوصيات لتفادي الوقوع كضحية للجرائم المتعلقة بالذكاء الاصطناعي.

1- عموميات حول الذكاء الاصطناعي:

يعتبر الذكاء الاصطناعي من المفاهيم الحديثة التي انتشرت في عصر العولمة والتطور التكنولوجي، ويعني الذكاء الاصطناعي بصفة عامة مختلف التقنيات التي تسمح للأنظمة والآلات أن تفهم وتتفاعل وتستننتج بحيث تحاكي العقل البشري، وفي مايلي سيتم التطرق لمفهوم الذكاء الاصطناعي، أهميته وأنواعه.

1.1- مفهوم الذكاء الاصطناعي وأهميته:

بعد الثورة الصناعية في بريطانيا، توجهت دول العالم نحو التكنولوجيا الحديثة، فهي التي تعكس تطور معيشة ورفاهية البشر، فتحول العالم نحو البحث عن وسائل أكثر فعالية لتحقيق الراحة والرفاهية، فتطورت تقنيات وآليات الذكاء الاصطناعي، Artificial Intelligence واستخدام الروبوت الآلي، Robotics وتصارع استخدامها بشكل متصاعد في الحياة اليومية للأفراد والمجتمعات، وبات الذكاء الاصطناعي إلى جانب تقنيات التعلم الآلي جزءاً هاماً في حياتنا اليومية، إضافة إلى أجهزة الاستشعار¹. فتزايد استخدام تقنيات الذكاء الاصطناعي في المجتمع، بحيث يؤثر اقتصادياً واجتماعياً ومدنياً بشكل إيجابي على حياة المواطن والمستهلك على حد سواء²، ويتضمن الذكاء الاصطناعي تطوير أجهزة الكمبيوتر القادرة على الانخراط في عمليات التفكير الشبيهة بالإنسان مثل التعلم والتفكير المنطقي وتصحيح الذات، وهو المفهوم الذي يعني أنه يمكن تحسين الآلات لتتولى بعض القدرات التي يُعتقد عادةً أنها تشبه الذكاء البشري مثل التعلم والتكيف والتصحيح الذاتي وما إلى ذلك³.

ويعتقد البعض أن الذكاء الاصطناعي هو أي نوع من أنواع الذكاء، بينما يؤكد الآخرون أنه يجب أن تحاكي تقنيات الذكاء الاصطناعي الذكاء البشري⁴. كما يعرفه القاموس العالمي للذكاء الاصطناعي على أنه المجال الذي يهتم بتطوير التقنيات التي تسمح لأجهزة الكمبيوتر بالتصرف بطريقة تبدو وكأنها كائن ذكي مثل الإنسان⁵.

كما يعد علم الذكاء الاصطناعي أحد فروع علم الحاسب الآلي وإحدى الدعائم التي تقوم عليها التكنولوجيا العصرية، ويهدف إلى الوصول إلى أنظمة ذكية تحاكي تصرف الإنسان من حيث التعلم والتفكير، وتقدم أنظمة الذكاء الاصطناعي خدمات متنوعة كالتعليم والتوجيه والتفاعل مع الآخرين وغيرها⁶. ومن خلال ما سبق يمكن القول أن الذكاء الاصطناعي هو كل التقنيات والأساليب التكنولوجية الحديثة المطبقة على الآلة بحيث تهدف إلى محاكاة العقل البشري في التفكير والاستنتاج والمنطق.

¹ عبد الله موسى، أحمد حبيب بلال، الذكاء الاصطناعي، ثورة في تقنيات العصر، دار الكتب المصرية، مصر، 2019، ص15.

² محمد محمد الهادي، الذكاء الاصطناعي معالمه وتطبيقاته وتأثيراته التنموية والمجتمعية، الدار المصرية اللبنانية، مصر، 2021، ص79.

³ Joost Nico Kok, **Artificial Intelligence, encyclopedia of life support systems**, EOLSS publishers, United Kingdom, 2009, p2.

⁴ عبد الله موسى، أحمد حبيب بلال، الذكاء الاصطناعي، ثورة في تقنيات العصر، مرجع سبق ذكره، ص16.

⁵ William J. Raynor Jr, **The International Dictionary of Artificial Intelligence**, Glenlake Publishing Company, USA, 1999, p13.

⁶ مهدي حنا، الذكاء الاصطناعي والصراع الإمبريالي، الآن ناشرون وموزعون، الأردن، 2020، ص41.

ومما سبق يمكن القول أن الذكاء الاصطناعي يتميز بمايلي⁷:

- اكتساب المعلومات بالممارسة العملية، وإمكانية التمييز بين مختلف القضايا،
- إمكانية التفاعل والاستجابة للمتغيرات، أي المرونة ورد الفعل السريع،
- الإدراك الحسي واتخاذ القرارات السليمة، وذلك من خلال دراسة كل الاحتمالات الممكنة، والقدرة على اختيار القرارات المثلى التي تؤدي إلى النتائج المرغوبة،
- القدرة على اكتشاف الأخطاء وتصحيحها بسرعة ودقة.

كما تظهر أهمية الذكاء الاصطناعي من خلال قدرته على أن يحل محل العامل البشري في جميع الأنشطة والمجالات، وذلك من خلال التفكير الذكي وتحليل البيانات بدقة تفوق العقل البشري، وكمثال⁸ على ذلك نذكر برنامج (ألفا جو) التابع لشركة قوغل الرائدة والذي تمكن من هزيمة أكبر لاعب في العالم في اللعبة الصينية القديمة (جو)، كما اتسعت دائرة الذكاء الاصطناعي لتبرز في مجال الصحافة، المحاماة، البنوك، قيادة السيارات، الخدمات الصحية...الخ، كما برزت أهميته خلال جائحة كورونا، حين اعتمدت دولة الصين على الروبوت الآلي ذاتي القيادة المزود بتقنيات الشحن لتقديم الخدمات الصحية للمرضى، توصيل الأدوية والأغذية، وجمع القمامة الطبية دون انتشار العدوى، وينتج عن استخدام الذكاء الاصطناعي مزايا عديدة في تخفيض التكاليف وتقليل المخاطر خاصة في مجال الطب والبحث العلمي، كما أن استخدامه سيؤدي مستقبلا إلى التخلي عن العامل البشري ومناسته بقوة في العديد من الوظائف، ولو أن البعض يرى أن الذكاء الاصطناعي هو مكمل للعنصر البشري وليس بديلا عنه.⁹

2.1-أنواع الذكاء الاصطناعي:

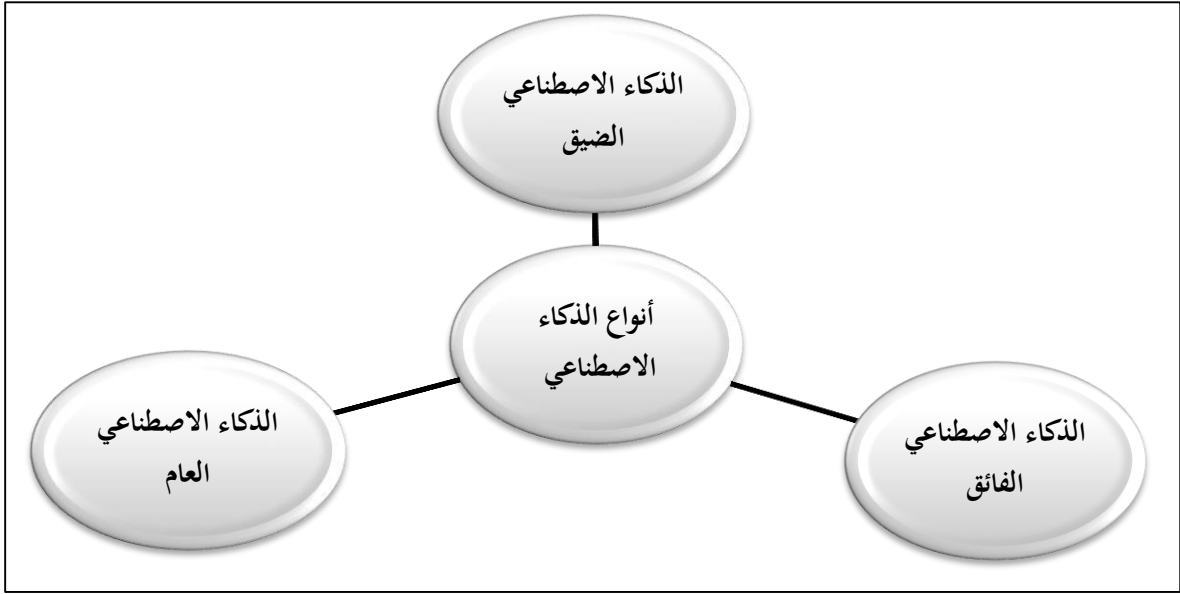
بصفة عامة يمكن تصنيف الذكاء الاصطناعي إلى ثلاث أنواع كما يوضحه الشكل الآتي:

⁷ بنت نبي ياسمين بلعسل، الحسين عمروش، الذكاء الاصطناعي ودوره في تحقيق التنمية المستدامة، مجلة الدراسات القانونية والاقتصادية، المجلد 05، العدد 01، المركز الجامعي بريك، 2022، ص1157.

⁸ محمد فتحي عبد العال، فانتازيا الجائحة، دراسة علمية، دار ديوان العرب للنشر والتوزيع، مصر، 2021، ص ص25-26.

⁹ محمد فتحي عبد العال، مرجع سبق ذكره، ص ص25-26.

الشكل رقم (01): أنواع الذكاء الاصطناعي.



المصدر: من إعداد الباحثة استنادا إلى: مهدي حنا، الذكاء الاصطناعي والصراع الإمبريالي، الآن ناشرون وموزعون، الأردن، 2020، ص49.

ومن خلال الشكل أعلاه يمكن تحليل أنواع الذكاء الاصطناعي كمايلي¹⁰:

1.2.1- الذكاء الاصطناعي الضيق أو الضعيف، Artificial narrow intelligence:

وهو من بين الأشكال البسيطة للذكاء الاصطناعي، بحيث تتم برمجة الآلة على القيام بمهام معينة داخل بيئة محدودة أو ضيقة، ويعتبر عملها كرد فعل على موقف محدد، ولا تعمل إلا في الظروف البيئية الخاصة بها، وذلك مثل الروبوت "ديب بلو" الذي صنعه شركة IBM والذي تغلب على "جاري كاسباروف" بطل الشطرنج الدولي.

2.2.1- الذكاء الاصطناعي العام أو القوي، Artificial general intelligence:

يتميز هذا النوع بقدرته على جمع وتحليل المعلومات وجمع الخبرات من المواقف المكتسبة، وذلك يمكن أن يؤهله لاتخاذ قرارات بشكل مستقل وذاتي، كالسيارات ذاتية القيادة، وروبوت الدردشة السريعة.

¹⁰ إيهاب خليفة، مجتمع ما بعد المعلومات، تأثير الثورة الصناعية الرابعة على الأمن القومي، العربي للنشر والتوزيع، مصر، 2019، ص ص42-

3.2.1- الذكاء الاصطناعي الخارق، Artificial super-intelligence:

هو عبارة عن نموذج حديث مازال قيد التجربة يهدف لمحاكاة البشر، ويتميز بنمطين أساسيين، الأول يسعى لمحاولة فهم أفكار العقل البشري، والانفعالات التي تؤثر على سلوكه، ويملك إمكانيات محدودة على التفاعل الاجتماعي، أما الثاني فهو نموذج لنظرية العقل، حيث يستطيع التعبير عن الحالة الداخلية، والتنبؤ بالمشاعر والمواقف، وهو الجيل القادم من الأنظمة الفائقة الذكاء.

2-جرائم الذكاء الاصطناعي والحلول المقترحة لها:

تعد الجريمة الالكترونية من أحدث الجرائم الناتجة عن استخدام التكنولوجيا الحديثة، كما تختلف جرائم الذكاء الاصطناعي تماما عن الجرائم التقليدية من حيث وقائعها وأهدافها وكيفية التصدي لها، وفيما يلي سيتم التطرق إلى ماهية الجريمة الالكترونية، ومختلف أنواع جرائم الذكاء الاصطناعي وكيفية مواجهتها.

1.2- ماهية الجريمة الالكترونية:

الجريمة لغة يقصد بها التعدي على الآخرين أو الذنب، وتعرف عموما على أنها فعل غير مشروع تقر له القوانين عقوبات تختلف حسب نوع الجريمة،¹¹ وقد تطور مفهوم الجريمة في العصر الحديث، فانقلبت من الجريمة بصفتها تقليدية أبعادها محدودة إلى الجريمة بمفهومها الحديث والتي تعتمد على الطرق والأساليب الحديثة في تنفيذ الفعل الاجرامي بطرق مبتكرة أو باستخدام التكنولوجيا الحديثة¹²، وهذا ما يسمى بالجريمة الإلكترونية أو الجريمة السيبرانية، وتُعرف الجريمة السيبرانية بأنها الجريمة التي تستخدم أجهزة الحوسبة، بما في ذلك الهواتف الذكية، وأجهزة التكنولوجيا القابلة للارتداء وغيرها للاحتيال على ممتلكات المجتمع وسرقتها ومضايقتها وتدميرها¹³.

2.2-أنواع الجرائم المتعلقة بالذكاء الاصطناعي والحلول المقترحة لمواجهتها:

تختلف جرائم الذكاء الاصطناعي باختلاف دوافع المجرم، وكذا طرق تنفيذه للهجمات وطبيعة الثغرات التي تتيح له ذلك، لذلك لابد من التعرف على مختلف جرائم الذكاء الاصطناعي واقتراح الإجراءات الضرورية

¹¹ أيمن عبد الله فكري، الجرائم المعلوماتية، دراسة مقارنة في التشريعات العربية والأجنبية، مكتبة القانون والاقتصاد، الرياض، 2014، ص82.

¹² ناصر بن محمد البقمي، مكافحة الجرائم المعلوماتية وتطبيقاتها في دول مجلس التعاون لدول الخليج العربية، مركز الامارات للدراسات والبحوث الاستراتيجية، الامارات العربية المتحدة، 2008، ص3.

¹³ Karabo Pilane, Zainab Ruhwanya, Irwin Brown, **Factors Influencing Cybercrime Reporting Behavior In South African State-Owned Entities**, Human Aspects of Information Security and Assurance, 16th IFIP WG 11.12 International Symposium, HAISA 2022, Mytilene, Lesbos, Greece, July 6–8, 2022, Proceedings, Springer , Switzerland, 2022, p285.

لتقادي الوقوع كضحية لها، وفيما يلي سيتم عرض مختلف أنواع جرائم الذكاء الاصطناعي والحلول المقترحة لمواجهتها:

1.2.2- أنواع جرائم الذكاء الاصطناعي:

للذكاء الاصطناعي العديد من الميزات التي تساعد على الارتقاء بمستوى حياة الأفراد، لكن له عيوباً أيضاً إذا ما تم استخدامه بشكل إيجابي، لذلك لابد من سن ضوابط صارمة لمنع حدوث مخاطر استخدامه، فبالرغم من الفرص التي يتيحها والتي يمكن أن تساعد على تحسين مستوى معيشة الأفراد، إلا أن مخاطره متعددة، فهو يسمح بانتشار المعلومات المحرفة، ناهيك عن أنه يسهل عمليات التجسس، وقد تتمكن آلياته مستقبلاً من خلق كائنات قد تسبب الأمراض..، ولذلك بدأ العلماء المسؤولون عن تطوير تقنيات الذكاء الاصطناعي في الآونة الأخيرة بدق ناقوس الخطر حول سلبات استخدام الذكاء الاصطناعي ومخاطره الحديثة¹⁴. ومن بين مخاطر الذكاء الاصطناعي ما يعرف بجرائم الذكاء الاصطناعي، ويمكن تصنيفها كما يلي:

- **التجسس الإلكتروني:** ويستهدف التجسس الرقمي عادة الشركات المختلفة،¹⁵
- **هجمات الحرمان من الخدمات:** يتم استخدام هذه الهجمات من خلال عدد كبير من الحواسيب التي يتم التحكم بها عن بُعد باستخدام تردد مشترك لمجموعة من الأشخاص، ويكون الهدف من تنفيذ هذه الهجمات إغراق موقع معين بكميات كبيرة من البيانات في وقت واحد، مما يُسبب إعاقة في الوصول إليه،
- **التصيد الاحتيالي:** وهو الأكثر انتشاراً، ويتم من خلال إرسال جماعي لرسائل عبر البريد الإلكتروني تتضمن روابط مختلفة لمواقع إلكترونية أو ملفات مرفقة ضارة بالحاسوب، وبمجرد النقر عليها يتم تحميل برامج حاملة لفيروسات مخربة لبيانات الكمبيوتر،
- **مجموعات الاستغلال:** وهي برامج مصممة لاستغلال أي أخطاء أو ثغرات في أجهزة الحاسوب، كما يمكن للقراصنة استخدام هذه التقنية لاختراق مختلف مواقع الويب واستخدامها بطرق سلبية.
- **برامج الفدية:** وهي عبارة عن برامج تمنع مستخدم جهاز الكمبيوتر من الوصول إلى بياناته المخزنة، ثم يشترط المهاجم على الضحية دفع مبلغ من المال كفدية ليتمكن من استرجاع ملفاته،¹⁶

¹⁴ فورين أفيروز، كيف يمكننا تقادي كارثة من صنع الذكاء الاصطناعي؟، مقال منشور بتاريخ 16-08-2023، على الرابط:

<https://www.aljazeera.net/news/presstour/2023/8/16/> ، تاريخ الاطلاع: 02-11-2023، 11:00.

¹⁵ فيصل محمد عبد الغفار، الحرب الإلكترونية، الجندرية للنشر والتوزيع، الأردن، 2015، ص ص 10-11.

¹⁶ احذر أنواع الجرائم الإلكترونية، مقال منشور بتاريخ 04-11-2023، على الرابط:

<https://www.tuniscopie.com/ar/article/367519/arabe/actu-arabe/piratage-340921> ، تاريخ الاطلاع: 02-11-2023،

11:00.

- **القرصنة الإلكترونية:** يمكن تعريفها على أنها تتبع أو استعمال العنوان الإلكتروني بنية تحقيق المداخل الخاصة بشهرة علامة تجارية خاصة ومملوكة لمشروع معين.¹⁷ كما تُعرف القرصنة على أنها وصول غير شرعي إلى بيانات ومعلومات تتواجد على أجهزة الحاسوب أو شبكات الويب من خلال استغلال الثغرات المتواجدة في هذه الأنظمة،
- **سرقة الهوية:** وتحدث عندما يتمكن شخص ما من الحصول على البيانات الشخصية لفرد آخر بشكل غير شرعي ويستخدمها لارتكاب أفعال غير قانونية كالنصب والاحتيال،
- **الهندسة الاجتماعية:** يعتمد هذا النوع من الجرائم على التلاعب النفسي بالضحية لإجبارها على تنفيذ أعمال غير شرعية أو الإفصاح عن بيانات سرية، ويستخدمها مجرمو الإنترنت للقيام بالاحتيال على الآخرين،
- **قرصنة البرمجيات:** وهي إعادة توزيع أو استعمال برامج معينة دون ترخيص من المؤسسة المالكة لها، كإنتاج برامج مزيفة أو استخدام العلامة التجارية للبرنامج الأصلي،
- **البرمجيات الخبيثة:** وهي البرامج التي يمكن أن تسبب تأثيرا سلبيا على أداء جهاز الكمبيوتر، ومن بين هذه البرامج نذكر ما يلي¹⁸:
- ✓ **الفيروسات:** وهو برنامج يُلحق اضرارا بنظام الحاسوب بحيث يؤدي إلى إتلاف نظام التشغيل؛ كحذف البيانات أو الملفات أو تعطيلها،
- ✓ **دودة الحاسوب:** وتشبه دودة الحاسوب الفيروسات ولكنها لا تُعدّل على نظام الحاسب الآلي بل تتكاثر بشكل مستمر مما يبطئ نظام تشغيل الكمبيوتر بحيث يُمكن التحكم بها عن بُعد عكس الفيروسات،
- ✓ **حصان طروادة:** وهو جزء مخفي في برنامج الحاسوب يعمل على سرقة معلومات المستخدم، بحيث يتتبع ويسرق المعلومات التعريفية للبريد الإلكتروني عند محاولة المستخدم الولوج إليه عبر متصفح الانترنت،
- ✓ **برمجيات أخرى:** وتشمل برامج الإعلانات، التجسس ومختلف البرمجيات الخبيثة الهجينة.

2.2.2- الحلول المقترحة للوقاية من جرائم الذكاء الاصطناعي:

من بين الحلول التي يمكن اقتراحها للوقاية من جرائم الذكاء الاصطناعي مايلي¹⁹:

¹⁷ خالد ممذوح إبراهيم، الحماية القانونية للعلامات التجارية مدنيا وجنائيا في القانون الاتحادي لدولة الإمارات العربية المتحدة رقم 37 لسنة

1992 المعدل بالقانون رقم 8 لسنة 2002، دار الفكر الجامعي، مصر، 2019، ص 215.

¹⁸ احذر أنواع الجرائم الإلكترونية، مرجع سبق ذكره.

¹⁹ ما هي طرق وأساليب الوقاية المستخدمة في الجرائم الإلكترونية؟، مقال منشور على الرابط: <https://lawmaroc.com/>، تاريخ الاطلاع:

2023-11-02، 11:00.

- **ضرورة تحديث البرامج:** وذلك لمنع وتقليل مخاطر الهجمات السيبرانية، فغالبًا ما يتم استخدام نقاط الضعف في البرامج القديمة للوصول إلى الأجهزة وأنظمتها،
- **استخدام كلمات مرور قوية يصعب تخمينها:** وذلك لمنع استخدام أدوات كسر كلمات المرور الضعيفة، ويجب أن تكون كلمة المرور القوية مزيجًا من ثمانية أحرف على الأقل، تتكون من الأحرف الكبيرة والصغيرة، الأرقام والحروف.
- **استخدام المصادقة ثنائية العامل، 2FA:** وذلك كاحتراز أمني إضافي ويستوجب تقديم شكلين من أشكال الهوية، مثل كلمة المرور والرمز المرسل إلى الهاتف للوصول إلى الحساب،
- **استخدام والتحديث المستمر لبرمجيات مكافحة الفيروسات:** وذلك لتسهيل اكتشاف وإزالة البرامج الضارة من أجهزة الحاسوب،
- **الحد من إمكانية الوصول إلى المعلومات الحساسة:** بحيث يجب أن يقتصر الوصول إليها على الأفراد الذين يستخدمونها في مسؤولياتهم المهنية،
- **الاعتماد على البيانات الاحتياطية:** وذلك من خلال الاحتفاظ المستمر بنسخ احتياطية حديثة من البيانات المهمة لتسهيل استعادة المفقودة منها وتقليل تأثير أية هجمات محتملة.
- **استخدام الشبكات الافتراضية الخاصة:** يمكن أن تساعد هذه الشبكات في السيطرة على الهجمات الإلكترونية عن طريق تشفير حركة المرور عبر الإنترنت، وتعتبر شبكة VPN الافتراضية مثال لهذا النوع من الشبكات،
- **مراقبة النشاط المشبوه:** إذ يجب على المؤسسات مراقبة أنظمتها الإلكترونية وترقب أية نشاطات مشبوهة أو هجمات إلكترونية محتملة وذلك من أجل الكشف المبكر ومنع الأضرار،
- **القيام بإجراءات تدقيق أمنية منتظمة:** وتهدف هذه الإجراءات إلى تحديد نقاط الضعف في أنظمتها الأمنية،
- **استخدام التشفير:** يعرف التشفير على أنه تحويل النص إلى رموز غير مفهومة لمنع الاطلاع عليها إلا للأفراد المرخص لهم بذلك وينقسم إلى ما يعرف بالتشفير المتماثل والتشفير الغير متماثل.²⁰ ويمكن أن يساعد التشفير في منع الجريمة السيبرانية من خلال منع الوصول إلى البيانات الحساسة خاصة المالية منها كمعلومات بطاقات الائتمان،
- **اليقظة والحذر:** إن توخي اليقظة وإدراك التهديدات المحتملة هو جزء مهم من منع مختلف الهجمات الإلكترونية، ويشمل ذلك اليقظة عند فتح رسائل البريد الإلكتروني أو النقر على الروابط الغير معروفة، أو عند مشاركة المعلومات الحساسة.²¹

²⁰ محمد أحمد كاسب خليفة، الاثبات والالتزامات في العقود الإلكترونية، دار الفكر الجامعي، مصر، 2019، ص283.

²¹ ما هي طرق وأساليب الوقاية المستخدمة في الجرائم الإلكترونية؟، مرجع سبق ذكره.

3- دراسة حالة شركة Uber Technologies:

تعتبر شركة Uber technologies من أكثر الشركات رواجاً في مجال النقل على المستوى الدولي بحيث تستخدم في تقديم خدماتها تطبيق أوبر عن طريق الهاتف الذكي لمحاولة ربط السائق بالزبون، إلا أن هذه الشركة وقعت ضحية قرصنة إلكترونية خلال سنة 2022م، وفيما يلي سيتم تقديم الشركة ونشاطها، وكيفية تعرضها للاختراق وأسلوب مواجهتها لتلك الحادثة.

1.3- تقديم شركة Uber Technologies:

شركة أوبر، Uber Technologies Inc (Uber) هي شركة خدمات نقل الركاب، تقدم خدماتها من خلال منصاتها التكنولوجية مثل تطبيقات الهاتف المحمول والمواقع الإلكترونية، وتقوم شركة Uber بربط الركاب بالسائقين أو موفري الرحلات المستقلين، كما تقدم الشركة خدمات الاستقبال والنقل إلى المطارات في عدة دول، كما توفر الشركة من خلال منصتها التكنولوجية خدمات توصيل الطعام والوجبات، تقدم أوبر أيضاً خدمات الشحن والخدمات اللوجستية، وخدمات لقطاع الشركات للتنقل اليومي وتربط المستهلكين بشبكات النقل العام، وتمتلك الشركة عمليات في عدة مدن عبر أمريكا وأوروبا والشرق الأوسط وأفريقيا وآسيا، يقع المقر الرئيسي لشركة أوبر في سان فرانسيسكو، كاليفورنيا، الولايات المتحدة.²²

وقد حققت شركة Uber Technologies نجاحاً ملحوظاً منذ تأسيسها في عام 2009م، حيث نمت بسرعة من خدمة نقل محلية إلى شبكة نقل دولية تقدم خدمات عبر 90 دولة حول العالم، فكان لها تأثير كبير في خلق السمعة الاستراتيجية والحفاظ عليها كشركة رائدة في صناعة النقل.²³ وتعمل Uber اليوم على وضع استراتيجيات لتحقيق أقصى قدر من الأرباح في اقتصاد عالمي ديناميكي وتنافسي، فقد أثار دخول أوبر إلى سوق سيارات الأجرة العديد من الصراعات، والتحديات القانونية، حيث تطورت الشركة منذ تأسيسها للحفاظ على مكانتها، فخلال العقد الأول من وجودها، أصبحت أوبر مزوداً بارزاً في قطاع الخدمات، حيث ضمت 110 مليون مستخدم شهرياً في الولايات المتحدة بحلول عام 2019م، واعتباراً من أوائل عام 2023م ازداد عدد مستخدمي أوبر شهرياً إلى 130 مليوناً، وتعمل أوبر في 72 دولة، حيث تم تنفيذ أكثر من 24 مليار رحلة، وفي عام 2022م حققت الشركة ما يقارب 32 مليار دولار أمريكي من صافي الإيرادات، وازداد إجمالي حجم الحجز في أوبر على أساس سنوي حتى ظهور جائحة كوفيد19،

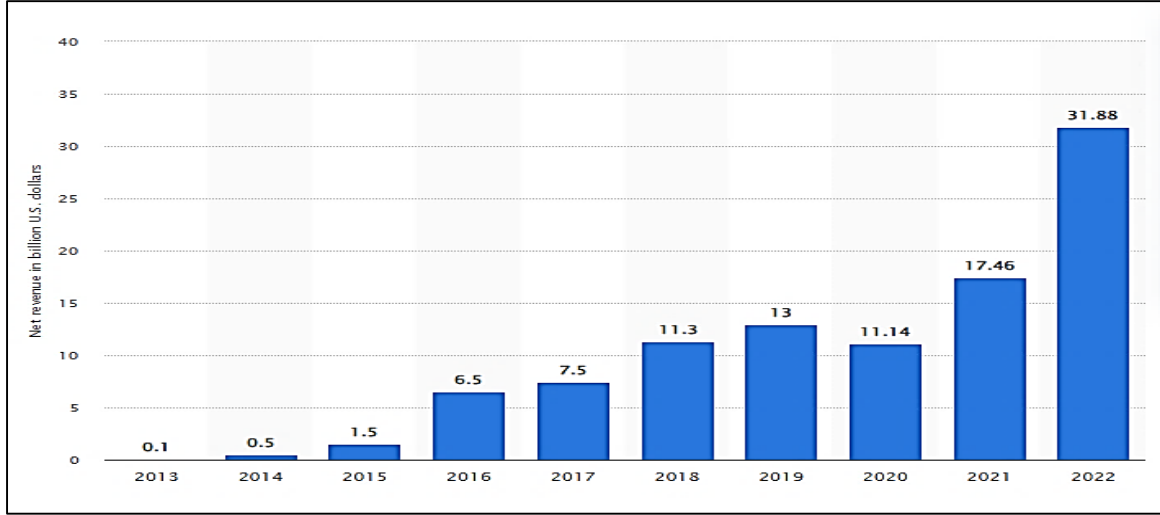
²² Uber Technologies Inc: Overview, website: <https://www.globaldata.com/company-profile/uber-technologies-inc/>, Access date: 03-11-2023, 11:00.

²³ Daniel Pereira, Uber Mission and Vision Statement, article published in 25-06-2023, Website: <https://businessmodelanalyst.com/uber-mission-and-vision-statement/>, Access date: 03-11-2023, 11:00.

²⁴ Statista Research Department, Uber Technologies- statistics & facts, article published in 31-08-2023, website: <https://www.statista.com/topics/4826/uber-technologies/#topicOverview>, Access date: 03-11-2023, 11:00.

ثم سرعان ما تعافت الشركة على الرغم من انخفاض إجمالي الحجزات خلال فترة الجائحة إلى ما يزيد قليلاً عن عشرة مليارات دولار أمريكي في الربع الثاني من عام 2020م ، وفي الربع الأول من عام 2023م حققت أوبر إجمالي حجزات بقيمة 31.41 مليار دولار أمريكي في جميع أنحاء العالم.²⁵ ويوضح الشكل الآتي إجمالي المداخل التي حققتها شركة أوبر اعتباراً من سنة 2013م إلى غاية سنة 2022م:

الشكل رقم (02): تطور مداخل شركة أوبر خلال الفترة 2013م-2022م(بليون دولار).



المصدر: Statista Research Department, **Uber's net revenue worldwide 2013-2022**, article published in 29-08-2023, website: <https://www.statista.com/statistics/550635/uber-global-net-revenue/> , Access date: 03-11-2023, 11:00.

ومن خلال الشكل أعلاه يتضح أن مداخل الشركات تطورت منذ 2013م بشكل متصاعد بلغ 13 بليون دولار سنة 2019م، ثم شهدت تراجعاً خلال فترة جائحة كوفيد إلى 11,14 بليون دولار، وسرعان ما استعادت المداخل عافيتها بارتفاع بلغ أقصاه سنة 2022م بقيمة 31,88 بليون دولار.

وتمتلك أوبر Uber تطبيقاً عبر الهاتف يقوم باستخدام نظام GPS بين السائقين والزبائن المتواجدين في أقرب نقطة بحيث يستطيع الزبون تقييم أداء السائق عند كل رحلة، كما يقوم السائق بتقييم الراكب مما يساعد الراكب على اختيار السائق المناسب، ويقوم السائق أيضاً بتقييم الراكب حتى يتم تسجيل البيانات مستقبلاً في حال تعرضه لأية مساءلة، كما يتوفر تطبيق أوبر في جميع أنواع الهواتف مثل الأيفون ونظام اندرويد ونظام ويندوز، وتعمل شركة أوبر Uber طبقاً للقوانين الخاصة بكل دولة، وتصنف كشركة مواصلات لا تمتلك أية سيارات أو سائقين بل تعرف الراكب بالسائق عبر تطبيقها، وتصنف الشركة الخدمة أنها حل للتشارك بالسيارات والسماح للسائقين غير المهنيين بالعمل.²⁶

²⁵ Statista Research Department, **Uber Technologies- statistics & facts**, op cit.

²⁶ نبذة عن شركة أوبر Uber ، مقال منشور على الرابط: <https://driversuber.com/> ، تاريخ الاطلاع: 03-11-2023، 11:00.

جرائم الذكاء الاصطناعي والحلول المقترحة - حالة شركة Uber Technologies-

ويمكن شرح عمل تطبيق شركة أوبر وفق الخطوات المبينة في الجدول الآتي:

الجدول رقم (01): خطوات استخدام تطبيق أوبر.

الخطوات	شرح الخطوات
الخطوة الأولى: يفتح الراكب التطبيق.	يقوم الراكب بإدخال وجهته في مربع "إلى أين؟"؛ ثم يقوم بمراجعة كل خيار رحلة فيما يتعلق بحجم السيارة وسعرها ووقت النزول المقدر؛ يختار الخيار المطلوب؛ ثم يؤكد الالتقاط.
الخطوة الثانية: يتم مطابقة الراكب مع السائق.	يرى سائق قريب طلب الركوب الخاص بالراكب ويختار قبوله، ثم يتم إخطار الراكب تلقائيًا عندما تكون سيارة السائق على بعد حوالي دقيقة واحدة.
الخطوة الثالثة: السائق يلتقط الراكب.	يتحقق السائق والراكب من أسماء بعضهما البعض والوجهة ثم يبدأ السائق بالرحلة.
الخطوة الرابعة: يأخذ السائق الراكب إلى الوجهة.	يمنح التطبيق السائق خيار الوصول إلى الاتجاهات خطوة بخطوة.
الخطوة الخامسة: يترك السائق والراكب التقييمات والمراجعات	في نهاية كل رحلة، يمكن للسائقين والركاب تقييم بعضهم البعض من 1 إلى 5 نجوم. يتوفر للركاب أيضًا خيار تقديم تحيات للسائق وإكرامية مباشرة في التطبيق.

المصدر:

How to use the Uber app, website: <https://www.uber.com/it/en/about/how-does-uber-work/?uclid=394cd80b-27da-49b6-a8ef-a529123cdb96> , Access date: 03-11-2023, 11:00.

2.3 - وقائع الجريمة السيبرانية التي وقعت ضحيتها Uber Technologies سنة 2022م:

خلال شهر سبتمبر 2022م، تم اختراق قواعد البيانات الداخلية لشركة Uber الأمريكية، ويقال أن المتسلل تمكن من الوصول إلى بيانات أوبر الأمانة من خلال "الهندسة الاجتماعية"، وهو ما يعني التلاعب أو خداع شخص ما، غالبًا عن طريق البريد الإلكتروني أو المكالمات الهاتفية، للوصول إلى معلومات شخصية أو مالية، فقد أصبحت أساليب التلاعب هذه شائعة في عالم الجرائم الإلكترونية، ووفقًا لشركة Uber، فبعد اختراق المتسلل لكلمة مرور الشركة، أرسل طلبات تسجيل دخول متكررة إلى حسابه وتمكن بعد ذلك من تجاوز مصادقة تسجيل الدخول الثنائية الخاصة بـ Uber، وعندما تمت المصادقة، تم قبول المتسلل في حساب Uber Slack ونشر رسالة نصها: "أعلن أنني متسلل وأن Uber تعرضت لاختراق البيانات"،²⁷ وقد قام خبير أمني بتقسيم اختراق Uber إلى تنسيق سهل الفهم لمساعدة زملائه من قادة الأمن وجميع المتخصصين في فهم مدى سهولة حدوث ذلك لأي شخص وكيف تم تنفيذ اختراق بهذا الحجم بالضبط وذلك كمايلي²⁸:

1.2.3 - خلفية عملية الإختراق:

في 15 سبتمبر، تمكن أحد المتسللين من الوصول غير المقيد إلى شبكة أوبر، فأصدرت أوبر بيان تقول فيه أنها "تستجيب لحادث" وأنه لم يتم الحصول على أية بيانات حساسة للمستخدم، ثم تم إخطار فريق أوبر من قبل المتسلل، مباشرة على تطبيق Slack الداخلي الخاص بهم، ومن خلال حساب المسؤول، تمكن المتسلل من الوصول إلى لوحة إدارة Slack ولوحة معلومات Sentinel One وحساب AWS والمزيد.

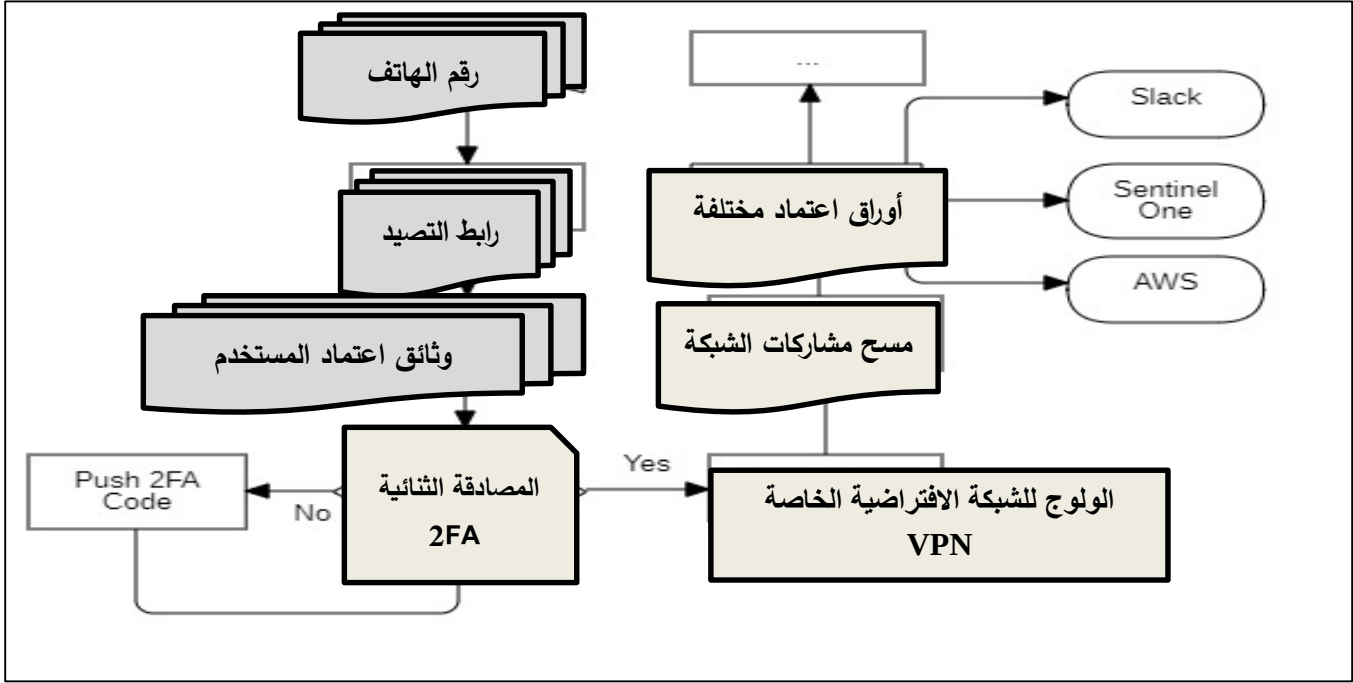
ويمكن شرح مخطط الهجمة السيبرانية التي تعرضت لها أوبر من خلال المخطط التالي:

²⁷Lindsay Shachnow, Uber Users: What You Need to Know about Last Month's Data Breach, article published in 11-10-2022, website: <https://www.bu.edu/articles/2022/what-you-need-to-know-about-uber-data-breach/>, access date: 03-11-2023,11:00.

²⁸ Uber's Recent Breach, article published in 04-12-2022,

Website: <https://www.breachlock.com/resources/blog/uber-breach/>, access date: 03-11-2023,11:00.

الشكل رقم (03): مخطط الهجمة السيبرانية لشركة أوبر.



المصدر:

Uber's Recent Breach, article published in 04-12-2022,

Website: <https://www.breachlock.com/resources/blog/uber-breach/> , access date: 03-11-2023,11:00.

ويمكن شرح خطوات الاختراق الموضحة في الشكل أعلاه كمايلي²⁹:

- الحصول على بيانات اعتماد المستخدم: تمكن المتسلل إرسال روابط التصيد، ثم تمكن من الحصول على بيانات اعتماد المستخدم، هذا هو المكان الذي ظهرت فيه الطبقة الدفاعية الأولى، وهي المصادقة الثنائية (FA2)، ثم الاتصال بشبكة VPN، وقد استخدمت Uber المصادقة الثنائية المستندة إلى الدفع مما يسمح بمضايقة الضحية بإشعارات FA2 حتى يوافق، ويُعرف هذا باسم إرهاب المصادقة الثنائية (FA2)،

-مسح الشبكة الداخلية للشركة: أثناء الاتصال بشبكة VPN، تمكن المتسلل من الوصول إلى الشبكة الداخلية وبدأ في فحص الشبكة الداخلية بحثاً عن مشاركات الشبكة.

²⁹ Uber's Recent Breach, Op cit.

2.2.3- الإجراءات المتبعة لمواجهة عملية الاختراق:

نسقت شركة أوبر بشكل وثيق جهود التعافي والاستجابة مع مكتب التحقيقات الفيدرالي ووزارة العدل، وتعهدت الشركة أيضًا بتعزيز سياساتها وممارساتها وتقنياتها السيبرانية لتحسين دفاعاتها، كما أكدت الشركة أنها اتخذت إجراءات وقائية متعددة ردًا على الهجوم كما يلي:³⁰

- تم تحديد الحسابات المخترقة أو التي يحتمل أن تكون مخترقة وتم حظرها أو طلب إعادة تعيين كلمة المرور لاستعادة الوصول إليها، ثم تم تعطيل العديد من الأدوات الداخلية.

- تمت إعادة تعيين معلومات الوصول في العديد من خدمات Uber الداخلية عبر تناوب المفاتيح.

- تم إغلاق قاعدة التعليمات البرمجية الخاصة بالشركة، مما منع أي تغييرات جديدة في التعليمات البرمجية.

- عندما استعادت أوبر إمكانية الوصول إلى الأدوات الداخلية، طلبت من الموظفين إعادة مصادقة بيانات الاعتماد.

- انطلاقًا من الشكل (03) الموضح سابقًا والمتضمن تطور إيرادات شركة أوبر يتضح أن مداخل الشركة سنة 2022م لم تتأثر بحادثة الاختراق بل تمكنت أوبر من تجاوز الأزمة بسرعة، وسجلت مبلغ عائدات مرتفع بدرجة كبيرة مقارنة بالسنوات الماضية.

- بتاريخ 23 سبتمبر 2022م وفي نفس الشهر الذي اكتشفت فيه حادثة الاختراق، تم القبض على المتسلل.³¹

خاتمة:

من خلال هذه الدراسة يمكن استخلاص مجموعة من النتائج أبرزها أن الذكاء الاصطناعي هو مجموع التقنيات التكنولوجية الحديثة المستخدمة لتحويل الأنظمة والآلات إلى ما يحاكي العقل البشري في التفكير والاستدلال وتصحيح الذات، وتبرز أهميته في نقل التكنولوجيا الحديثة وإحلال الآلة محل اليد العاملة ومواكبة العولمة وتطوير كافة القطاعات، كما خلصت الدراسة إلى ما يلي:

³⁰ Matt Kapko, **Uber details how it got hacked, claims limited damage**, article published in 19-09-2022, website: <https://www.cybersecuritydive.com/news/uber-attack-details/632193/>, access date: 03-11-2023, 11:00.

³¹ شيما عبد المنعم، عمره 17 عاما وقائد عصابة خطيرة ضبط الهاكر مخترق أوبر و GTA 6، مقال منشور بتاريخ: 2023-09-24، على الرابط: <https://www.elbalad.news/5454434>، تاريخ الاطلاع 2023-10-03، 11:30.

جرائم الذكاء الاصطناعي والحلول المقترحة - حالة شركة Uber Technologies-

- الذكاء الاصطناعي له العديد من الإيجابيات إلا أنه لا يخلو من السلبيات التي تجعله عرضة لعدة مخاطر أبرزها ما يعرف بالجريمة السيبرانية،
- الجريمة السيبرانية هي استغلال الثغرات التي يمكن أن تتواجد في التطبيقات الذكية والآلات والبرامج والمواقع الإلكترونية من أجل ارتكاب عدة هجمات إلكترونية،
- من أخطر الجرائم المتعلقة بالذكاء الاصطناعي برامج الفدية، سرقة الهوية، الهندسة الاجتماعية، والاختراق أو القرصنة وكذا البرامج الخبيثة،
- كانت شركة Uber Technologies الأمريكية إحدى ضحايا الجريمة السيبرانية خلال سنة 2022م، بحيث تم اختراق موقعها الإلكتروني باستخدام ما يعرف بالهندسة الاجتماعية، ثم تم الدخول لبياناتها الحساسة،
- سرعان ما تفتنت شركة Uber Technologies للجريمة وقامت بمجموعة من الإجراءات الأمنية السيبرانية المستعجلة لتغيير المعلومات السرية وإعادة برمجة موقعها الإلكتروني،
- تفادت شركة Uber Technologies عملية الاختراق و استطاعت تجاوز الأزمة بفضل الإجراءات الوقائية السيبرانية وكذا الإجراءات القانونية للقبض على المتسلل، مما يؤكد صحة الفرضيتين الأولى والثانية للدراسة،
- واستنادا للنتائج السابقة يمكننا تقديم مجموعة من الاقتراحات العامة المتعلقة بتفادي جرائم الذكاء الاصطناعي، ومن أهمها:
- ضرورة استخدام كلمات مرور قوية بحيث يصعب تخمينها أو تجاوزها بسهولة،
- ضرورة استخدام المصادقة ثنائية العامل، 2FA وبرامج وتقنيات التشفير،
- ضرورة استخدام وتحديث برنامج مكافحة الفيروسات والتفطن للبرامج المشبوهة،
- ضرورة استخدام البيانات الاحتياطية والشبكات الخاصة، مع ضرورة التوعية باليقظة والحذر خاصة لموظفي الشركات ذات السمعة العالمية، والبنوك والمؤسسات المالية.