إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق "Deep Fake" وعلاقته باستخدامهم الآمن لتلك المواقع

د. ولاء محمد محروس الناغي*

د. ياسر محمد محروس الناغي **

ملخص الدراسة:

تهدف الدراسة التعرف **علي مدي إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق "الديب فيك" وعلاقته باستخدامهم الآمن لتلك المواقع، وذلك من خلال** قياس عدة متغيرات منها مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق، والكشف عن مستوى الاستخدام الأمن لمستخدمي مواقع التواصل الإجتماعي و تحديد مستوى ثقة مستخدمي مواقع التواصل الاجتماعي في قدرتهم على كشف التزييف العميق (الثقة المزيفة)، وتوضيح الفروق في مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وفقاً للمتغيرات الديمجرافية (النوع – العمر – المستوى العلمي)، وتنتمي الدراسة الي الدراسات الوصفية التي اعتمدت علي منهج المسح الاعلامي، وتم التطبيق علي عينة قوامها (600 مفردة) من مستخدمي مواقع التواصل الاجتماعي بمحافظات (القاهرة،بورسعيد، اسيوط، الدقهلية)، وتم الاستعانة بالاستقصاء الالكتروني كأداة لجمع البيانات وتوصلت الدراسة لعدة نتائج اهمها:

1. توجد علاقة إرتباطية طردية ذات دلالة إحصائية بين مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وبين مستوى استخدامهم الأمن لتلك المواقع.

2- توجد علاقة إرتباطية عكسية ذات دلالة إحصائية بين مستوى ثقة مستخدمي مواقع التواصل الاجتماعي في قدرتهم على كشف التزييف العميق (الثقة المزيفة) وبين مستوى استخدامهم الأمن لتلك المواقع

3- توجد فروق ذات دلالة إحصائية في مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وفقاً للمتغيرات الديمجرافية (النطاق الجغرافي – النوع – المستوى التعليمي).

الكلمات المفتاحية: مستخدمي مواقع التواصل الاجتماعي، التزييف العميق، الاستخدام الآمن

---

* المدرس بقسم الإعلام بكلية التربية النوعية- جامعة بورسعيد

** المدرس بقسم الإعلام بكلية التربية النوعية- جامعة بورسعيد

Social media users' perception of Deepfake threats and its relationship to their safe use of those sites

Abstract:

The study aims to identify the extent of social media users' perception of Deepfake threats and its relationship to their safe use of social media, by measuring several variables, including the level of social media users' perception of Deepfake threats, Detecting the level of safe use of social media users, Determining the level of confidence of social media users in their ability to detect Deepfake (fake confidence) and clarifying the differences In the level of perception of the users of social media about the threats of Deep Fake according to the demographic variables (gender - age - educational level).

The study also belongs to the descriptive studies that relied on the media survey method, the study was applied to a sample of (600 individuals) of users of social media in the governorates of (Cairo, Port Said, Assiut, Dakahlia).

The study used the electronic questionnaire to collect data from the study sample, the study revealed several results, the most important of which are:

There is a statistically significant direct correlation between the level of social media users' perception of Deepfake threats and the level of safe use of social media.

There is a statistically significant inverse correlation between the level of confidence of social media users in their ability to detect Deepfake (fake confidence) and the level of their safe use of social media.

There are statistically significant differences In the level of perception of social media users of Deepfake threats according to demographic variables (geographical scope - gender - educational level).

Keywords: Social media users- Deepfake- safe use

مقدمة

تعتبر تقنيات الذكاء الاصطناعي كغيرها من التقنيات الأخرى سلاح ذو حدين فعلى الرغم من الإيجابيات والتسهيلات التي توفرها هذه التقنيات لمجال الاعلام، إلا أن بعض هذه التقنيات تحمل العديد من السلبيات و المخاطر والتهديدات الجسيمة خاصة فيما يتعلق بالمعلومات والبيانات المزيفة والتي تشكل المادة الخام لحروب الجيل الرابع والخامس.

ومن أبرز بصمات تقنيات الذكاء الاصطناعي في مجال الاعلام و الذي أحدث طفرة حقيقية وخطيرة في صناعة الوسائط المتعددة لتقنية التزييف العميق Deepfakes التي اتاحت تصنيع وتزييف تلك الوسائط بشكل يبدو واقعياً، مما يدفعنا إلى إدراك مهم ومقلق، بأن الاعتقاد الراسخ والمتأصل بتوثيق الصوت والفيديو للواقع، وكونه دليل على مصداقية المعلومات والبيانات قد أصبح اعتقاد يشوبه الشك.

كما زودت تقنية التزييف العميق Deepfakes مجرمي الإنترنت بقدرات احتيالية متطورة تمثل تهديدات جديدة على مستوى الأفراد والمؤسسات والمجتمعات سواء من خلال تصنيع المواد الإباحية المزيفة والتي اكدت الدراسات أن نسبة 96% من اجمالي المقاطع المزيفة بتقنية الديب فيك كانت للمحتوى الاباحي لأغراض تصفيه وتشويه شخص ما أو الانتقام أو الابتزار المالي أو الجنسي، أو من خلال تصنيع ونشر البيانات والتصريحات والمعلومات المضللة لأغراض إثارة الفوضى والاحتيال المالي وإفساد الانتخابات والأزمات الدبلوماسية. (Ajder; Patrini; et all, 2019) و (Wilkerson, 2021) و (Wang ; Kim ,2022).

ولم يعد استغلال تقنية التزييف العميق Deepfakes قاصراً على عدد قليل من المحترفين بعد طرح تطبيقات عديدة مثل Deep Face Lab و FaceApp و FaceSwap التي مكنت غير المحترفين من انتاج محتويات مزيفة تبدو واقعية وتمريرها عبر مواقع التواصل الاجتماعي.

وتلعب مواقع التواصل الاجتماعي عدة أدوار مساعدة لتقنية التزييف العميق فغالبا ما تكون أقصر الطرق للحصول على الصور أو الفيديوهات والبيانات الشخصية للضحية والتي يتم استخدامها كمادة خام لصناعة فيديو مزيف بهذه التقنية، كما أن تلك المواقع لا تمتلك ألية لكشف الديب فيك لاستئصال محتوياته أو منعها أو حذفها وبذلك تحتضن تلك المحتويات المزيفة وتعد الوسيلة الرئيسية في وصول تلك المحتويات لملايين المستخدمين وخداعهم.

وبالتالي تتغير طبيعة وأهمية الاستخدام الآمن لمواقع التواصل الاجتماعي كإجراء استباقي واحترازي ووقائي في ظل وجود تهديدات تقنية التزييف العميق، و عدم توافر طريقة موثوقة في كشف هذا التزييف، حتي لا يصبح المستخدم ضحية او يتم التلاعب به من خلال هذه التقنية الخطيرة.

ومن هنا وجد الباحثان أهمية خاصة في دراسة:

إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وعلاقته باستخدامهم الآمن لتلك المواقع

الدراسات السابقة

بعد الاطلاع علي العديد من الدراسات السابقة فقد تم تقسيمها الي محورين أساسيين:

المحور الاول: الدراسات الخاصة بتقنية التزييف العميق " الديب فيك "

المحور الثاني: الدراسات الخاصة بالاستخدام الآمن لمواقع التواصل الاجتماعي

وقد تم ترتيب الدراسة من الاقدم الي الاحدث لتناول كيفية التطور الذي شهدته تقنية التزييف العميق عبر سنوات قصيرة.

اولا: الدراسات الخاصة بتقنية التزييف العميق (Deep fakes) :

دراسة **(**Ajder; Patrini; et all, 2019**)** والتي حصرت عدد مقاطع الديب فيك على مستوى العالم والتي بلغت 14678 مقطع ويمثل هذا العدد زيادة سنوية بنسبة 100% تقريباً عن العام السابق للدراسة والذي بلغ فيه عدد المقاطع (7964) الذي تم التقاطه في ديسمبر 2018، وأشارت نتائج الدراسة أن نسبة 96% من اجمالي المقاطع المزيفة كانت للمحتوى الإباحي، واستهدفت مقاطع الديب فيك الإباحية الإناث بنسبة 100%، بينما استهدفت مقاطع الديب فيك غير الإباحية الذكور في الترتيب الأول بنسبة 61%، ثم الإناث بنسبة 39%، كما اوضحت نتائج الدراسة أن فنانات موسيقى البوب الكوري كانت أكثر الفئات استهدافاً على مستوى العالم بفيديوهات الديب فيك الإباحية بنسبة 25% من اجمالي الفيديوهات الإباحية المزيفة.

وسلطت دراسة **(Maras ; Alexandrou , 2019)** الضوء على مصداقية الصور ومقاطع الفيديو كدليل جنائي للمحكمة بعد ظهور تقنية التزيف العميق، وأكدت الدراسة أن الإدانات الجنائية استنادا إلى الصور ومقاطع الفيديو ستكون معرضة للخطر إذا لم يأخذ وكلاء العدالة الجنائية والمهنيون القانونيون بعين الاعتبار إمكانية تعرض الصور ومقاطع الفيديو للتلاعب بتقنيات الذكاء الإصطناعي التزييف العميق، وأشارت استنتاجات الدراسة إلى عدم دقة تقارير خبراء الطب الشرعي للوسائط الرقمية بالمحكمة الفيدرالية الأمريكية لتوثيق الأدلة في وجود التزييف العميق، لعدم وجود تقنية حاسمة لكشف التزييف لدى خبراء القانون.

في حين قدمت دراسة(Tolosana; Rodriguez, et al., 2020) تحليل كيفي وكمي من خلال مسح للدراسات التجريبية التي حاولت التوصل لتقنيات لكشف التلاعب بالوجه ومن بينها أساليب الديب فييك لإبطال تهديداته المتزايدة، وقامت الدراسة بتقييم لقدرات قواعد البيانات والتطبيقات المستخدمة في التزييف العميق والتي قسمتها إلى الجيل الأول الذي يتسم بإنخفاض الجودة في تركيب الوجه، وظهور عناصر مرئية من الفيديو الأصلي أثناء عرض الفيديو المزيف، وتأثيرات غريبة ومصطنعة بين اطارات الفيديو، وظهور حدود للوجه المزيف، وتباين الألوان بين بشرة الوجه الحقيقي والمزيف، بينما تم تطوير الجيل الثاني من التزييف العميق من خلال التعلم العميق وتقنيات الذكاء الإصطناعي لتزداد واقعية الفيديو المزيف لتصبح عملية اكتشافه غاية في الصعوبة من خلال التغلب على العيوب التقنية التي

ظهرت في الجيل الأول بالإضافة إلى محاكاة الإضاءة النهارية والليلية، ومراعاة التصوير الداخلي والخارجي من حيث الواقعية، وواقعية مسافة الشخصيات بالنسبة للكاميرا، وامكانية التنويع في مستوى ارتفاع الكاميرا، وتوصلت الدراسة إلى عدة استنتاجات أهمها أنه أصبح من السهل انتاج فيديو بتقنية الديب فييك بواقعية كبيرة وذلك الأمر يمثل تهديد واسع النطاق في مجالات عدة، و أن هناك العديد من الدراسات قدمت طرق لاكتشاف فيديوهات الدييب فيك ولكنها لايمكن الاعتماد عليها بشكل قاطع نظراً لتوافر معدل خطأ بالإضافة إلى قدرة التزييف العميق على التطور من خلال التعلم العميق، وأخيراً أوصت الدراسة بضرورة البحث عن تقنية جديدة للكشف الحاسم عن فيديوهات التزييف العميق وإيقاف تهديداته المتزايدة.

أما دراسة**(Vaccari ; Chadwick , 2020) فتناولت** تقييم لتأثيرات التزييف العميق على تصورات الأفراد للحقيقة والتزييف عبر وسائل التواصل الاجتماعي،واستخدمت الدراسة المنهج التجريبي من خلال تعريض المبحوثين لمقطعين فيديو للرئيس الأمريكي السابق أوباما بتقنية الديب فيك وقياس مستوى اليقين لديهم، ثم تعريضهم لمقطع فيديو يتقاسم فيه الممثل الكوميدي جوردان بيل الشاشة مع أوباما ليكشف أن مقاطع الفيديو التي تعرض لها المبحوثين مفبركة ثم قياس مستوى الثقة في أخبار وسائل التواصل الإجتماعي بشكل عام بعد التجربة، وتوصلت الدراسة إلى أن عدم اليقين الذي تثيره تقنية التزييف العميق تقلل من ثقة الجمهور في أخبار وسائل التواصل الاجتماعي سواء حقيقية أو مزيفة.

واعتبرت دراسة **(Saifuddin, 2021)** من أولى الدراسات التي تستكشف السلوك غير المقصود في مشاركة مقاطع التزييف العميق وبالتالي توسيع أثاره السلبية وتهديداته نتيجة انخفاض مستوى الوعي، وذلك بالتطبيق على عينة من مستخدمي مواقع التواصل الإجتماعي في الولايات المتحدة وسينغافورة، وتوصلت الدراسة إلى وجود علاقة ارتباطية عكسية بين مستوى القدرة المعرفية و مستوى مشاركة التزييف العميق غير المقصود في كلا البلدين، مما يؤكد أن الأفراد ذوي القدرة المعرفية العالية هم أقل عرضة لمشاركة التزييف العميق عن غير قصد.

وسعت دراسة**(Köbis; Doležalová; at al., 2021)** لاختبار ما اطلقت عليه الخداع المزدوج للتزييف العميق **(Fooled twice)** من خلال المنهج التجريبي على عينة من مستخدمي الإنترنت بالمملكة المتحدة بلغ قوامها 210 مفرده، لاختبار ثقة المبحوثين في قدرتهم الخاصة في اكتشاف مقاطع التزييف العميق (الثقة المزيفة)، حيث تم تعريضهم إلى 16 مقطع فيديو (8 مقاطع صحيحة – 8 مقاطع مزيفة)، وأكدت نتائج الدراسة أن الأشخاص لايمكنهم اكتشاف التزييف العميق بشكل موثوق به، ولكنهم يبالغون في تقدير قدراتهم على التعرف على هذه المقاطع وامكانياتهم في كشف التزييف، مما يعرضهم للخداع مرتين الأولى خداع في ثقتهم والثانية خداع في محتويات الديب فييك، حيث أثبتت وجود علاقة إرتباطية عكسية بين مستوى الثقة المزيفة وبين مستوى الدقة في كشف المبحوثين لمقاطع الفيديو المزيفة بتقنية التزييف العميق عند مستوى دلالة 0.01.

واستهدفت دراسة **(Diakopoulos ; Johnson , 2021)** التعرف على كيفية تأثير التزييف العميق على الانتخابات الرئاسية الأمريكية عام 2020 وقامت الدراسة بتحليل ثمانية سيناريوهات افتراضية لاستخدامات التزيف العميق في تلك الانتخابات تتضمن قدرات التزييف العميق السلبية (الخداع – تشويه السمعه – الترهيب - الاسناد الخاطئ – اضعاف الثقة)، وأكدت الدراسة قدرة التزييف العميق في إبطال نزاهة الانتخابات لعدم توافر تقنية حاسمة لكشف فيديوهات التزييف العميق، كما طورت أربع استراتيجيات لمواجهة تهديدات وأضرار التزييف العميق،تتمثل في الوعي ومحو الأمية الإعلامية، والدفاع عن الذات، والتحقق، ومحاصرة التزييف العميق.

وأكدت دراسة **(Gabriel , 2021)** أن سهولة استخدام ووصول المستخدم العادي للأدوات والبرامج والتطبيقات الخاصة التزييف العميق مثل DeepFaceLabو FaceApp كان عاملاً أساسياً في تعميم تقنية التزييف العميق في جميع أنحاء الصين وأنتشار أثارها السلبية، وتوصلت الدراسة الي أن المحتوى الإباحي يشكل الغالبية العظمى من عمليات التزييف العميق على منصات الوسائط الرقمية الصينية.

اما دراسة**(Jiang ; Li; et al.,: 2021)** فأبرزت التطور المستمر لاساليب جديدة تعتمد على الذكاء الاصطناعي والتعلم العميق لإنتاج التزييف العميق، جعل العديد من الدراسات تكثف جهودها لاقتراح طرق مختلفة لكشف التزييف العميق لمحاصرة المخاطر والتهديدات الناجمة عنه، ولتزويد الطب الشرعي للوسائط الرقمية بتقنيات يمكن الاعتماد عليها وتعميمها في كشف التزييف العميق، وعلى الرغم من تحقيق نتائج واعدة في اكتشاف التزييف العميق من خلال deep neural networks، إلا أن أداؤها سيتدهور بشكل كبير عند مواجهة التزييف العميق الذي تم إنشاؤه باستخدام طرق مختلفة ليظل التحدي قائم، ولذا أقترحت الدراسة طريقة جديدة بالاعتماد FakeFilter عن طريق تجزئة الفيديو إلى إطارات ووضعها تحت نظام مجهري لكشف التزييف، وأظهرت نتائج التجربة دقة أعلى من الطرق السابقة التي اعتمدت في اسلوب الكشف عن التزييف العميق على deep neural networks، وأوصت الدراسة بتدعيم التجربة بقواعد بيانات لاختبار امكانية تعميمها كدليل للطب الشرعي للوسائط الرقمية.

وحددت دراسة **(Wilkerson , 2021)** اسلوبين لاستخدام التزييف العميق في السياسة والتاثير على الانتخابات، يتمثل الأسلوب الأول في السخرية والذي يعتبرها القانون الأمريكي مشروعة كحرية تعبير رغم رصد تأثيراتها السلبية، والأسلوب الثاني هو التضليل المتعمد بنشر مقاطع فيديو تبدو واقعية لتمرير معلومات مغلوطة أو تشويه سمعه شخص، وأكدت الدراسة قدرة الأسلوبين على التأثير السلبي على نزاهة الانتخابات والعملية الديمقراطية، وأوصت الدراسة ببذل جهد أكبر وأسرع من جانب المشرعون القانونيون لتحجيم تهديدات الديب فيك في المجال السياسي.

وأثبتت دراسة **(الخولي، 2021)** أن الجاني مرتكب عملية التزييف العميق يسأل عن خطئه بتعمد تركيب الصور والوجوه على النظم الخوارزمية المولدة للفيديوهات المزيفة أو

التسجيلات الصوتية ومن ثم يجب قيام المسئولية المدنية وفقًا للقانون المصري وما تنص عليه المادة 163 من القانون المدني و المادة 25 و26 و 188 من قانون جرائم تقنية المعلومات، وأوضحت نتائج الدراسة أن للمسئولية المدنية في التزييف العميق ثلاثة عناصر لا تقوم بدونها أو بدون واحدة منها، أولها الخطأ في التزييف العميق سواء خطأ منشئ المحتوى و ناشر المحتوى أو خطأ المتواصلين مع ناشر المحتوى والذى عزف المشرع المصري عن بيانه، والعنصر الثاني هو الضرر الناتج عن التزييف العميق، ويتمثل العنصر الثالث في السببية وهى قائمة على السبب الفعال المحدث للضرر المتمثل في سلوك المدعي عليه بمحض إرادته لتركيب الصور لإنتاج فيديو مستحدث غير حقيقي، وأكدت الدراسة على أهمية الالتزام الوقائي والاحترازي من جانب مستخدمي مواقع التواصل الاجتماعي من استخدام الصور الشخصية المخزنة والغير مؤمنة حتى لا يتم عرضها بطريقة تنتهك حقوقهم وتسئ إلى سمعتهم أو تجعلهم عرضه للإبتزاز، كذلك أشارت الدراسة إلى خطأ منصات التواصل الاجتماعي في عدم امتلاكها أدوات تقنيه للكشف عن فيديوهات التزييف العميق والتي توسع من تهديدات التزييف العميق بإتاحه نشره بسهولة، واقترحت الدراسة وضع نصوص قانونية تحمل المستخدمين لمواقع التواصل الاجتماعي المسئولية المدنية في حالة نشر محتوى غير حقيقى أو مشاركته.

وناقشت دراسة **(ملح، 2021)** العلاقة بين تقنية التزييف العميق و تهديد مصداقية الاعلام الالكتروني من خلال اجراء مسح لعدد من التزييف بالمواقع الالكترونية وتوصلت الدراسة الي تنامي أعمال التزييف العميق في الأخبار والصور والفيديو بالإعلام الإلكتروني وأثبتت الدراسة باستخدام المنهج الوصفي تأثير تقنية التزييف العميق السلبي على مصداقية الإعلام الإلكتروني.

واشارت دراسة **(الشربيني، 2021)** الي أن استخدام التزييف العميق يؤدي إلى تفاقم الآثار النفسية من خلال تقويض الثقة الاجتماعية والاضرار بالسلامة النفسية للأفراد، وإثارة ردود فعل دفاعية إزاء حالة عدم اليقين في العالم، كما توصلت الدراسة إلى أن تقنيات الذكاء الاصطناعي الحالية غير كافية لحماية السلامة النفسية لمستخدمي الإنترنت من التزييف العميق، وأوصت الدراسة باستخدام التقنيات الإنسانية من خلال التفكير النقدي ورفع مستوى وعي الأفراد بالمشاكل الاجتماعية والنفسية الناتجة عن التزييف العميق وطرق الحماية والتصدي لها.

ورصدت دراسة **(Gregory , 2022)** الجهود التي قامت بها مؤسسة witness لحقوق الإنسان في تقدير حجم تهديدات التزييف العميق وآليات المواجهة على مستوى العالم، حيث عقدت المؤسسة اجتماعات في الفترة من 2018: 2020 لخبراء تقنيين وتجريبيين في الولايات المتحدة وأوروبا والبرازيل وأفريقيا وجنوب الصحراء وجنوب شرق آسيا وركزت على الاستعداد الحالي لمواجهة التزييف العميق كحق من حقوق الإنسان، وأشار الخبراء إلى ضرورة وضع تقنية التزييف العميق في سياق أوسع لمحو الأمية الإعلامية واكساب الجمهور مهارات التفكير النقدي لعدم توافر تقنية حاسمة لكشف التزييف العميق.

وقدمت دراسة**(Kolagati Priyadharshini ; et al., 2022)** ; نموذج مقترح لاكتشاف مقاطع الفيديو بتقنية التزييف العميق بالاعتماد على deep convolutional neural network model عن طريق على اكتشاف معالم الوجه، بحيث يتم استخراج البيانات المتعلقة بسمات الوجه المختلفة من مقاطع الفيديو ويتم تمرير هذه البيانات إلى مدرك متعدد الطبقات لمعرفة الاختلافات في مقاطع الفيديو الحقيقية ومقاطع الفيديو المزيفة في الوقت نفسه، واستخدمت الدراسة الشبكة العصبية التلافيفية CNN لاستخراج الخصائص وتخزينها والتدريب على مقاطع الفيديو لامكانية التصنيف مابين الحقيقي والزائف ومن ثم دمج هذين النموذجين لبناء كاشف للتزييف العميق متعدد المدخلات، تم تطبيق الدراسة التجريبية على318 مقطع فيديو، من بينها 199 مقطع فيديو مزيف و119 مقطع فيديو حقيقي، ويوفر النموذج المقترح نتائج تصنيف للفيديو جيدة حيث بلغت الدقة ٪84 ودرجة AuC 0.87.

واختبرت دراسة **(Wang ; Kim ,2022)** للتعرف على الاستجابات العاطفية والسلوكية لمستخدمي الانترنت بعد التعرض لمقاطع فيديو التزيف العميق الخاصة بفنانات البوب الكوري نظراً لاستهداف هذه الفئة، وقامت الدراسة بتطبيق اسلوب المسح لقياس المشاعر السلبية (الغضب – الشعور بالذنب) على عينة طبقية من مستخدمي الانترنت بكوريا الجنوبية قوامها 300 مفردة بعد التأكد من تعرضهم لفيديوهات إباحية خاصة بفنانات البوب الكوري، وكشفت النتائج أن مستوى مشاعر الغضب والشعور بالذنب لمستخدمي الانترنت له تأثير عميق على تحفيز سلوك الإبلاغ المباشر عبر الانترنت عن ضحايا العنف ضد المرأة وتقديم الدعم العاطفي لضحايا الديب فيك ورفع مستوى الوعي لدى الأخرين بحقيقة التزييف.

ثانيا: **الدراسات الخاصة بالاستخدام الآمن لمواقع التواصل الاجتماعي**

اهتمت الدراسات المختلفة بالكشف عن الاستخدام الآمن في التعامل مع الانترنت ومواقع التواصل الاجتماعي باعتباره المرشد الرئيسي للحفاظ علي حماية البيانات الخاصة بالافراد من التعدي واساءة الاستخدام واعتبره ابرز العوامل الذاتية للفرد في حماية خصوصيته ومن هذه الدراسة دراسة **(Patchin; Hinduja , 2010)** التي سعت لتحليل صفحات ملف تعريف للمراهقين علي موقع My Space لعينة عشوائية من هذه الملفات وبعد مرور عام من التحليل تمت اعادة التحليل مرة اخري لمعرفة مدي تغير المحتوي للصفحات الشخصية و ما اذا كانت هناك اي تغييرات ملحوظة في طريقة استخدام المراهقين لهذه المواقع خاصة وان الاباء اعربوا في الدراسة الاولي عن قلقهم من كمية ونوعية المعلومات الشخصية والخاصة التي يكشفها ابنائهم علي صفحاتهم الشخصية، وتوصلت الدراسة الي ان الغالبية العظمي من المراهقين اتخذوا خيارات مسؤوله اتجاه الاستخدام الآمن لمعلوماتهم التي يشاركوها عبر الانترنت بالرغم من وجود بعض الاستثناءات، وقد ارجعت الدراسة السبب في نمط الاستخدام الي جهود المنظمات التعليمية والمدنية لتعزيز فكرة امان الاستخدام وتزويد المراهقين بالمعرفة للبقاء بعيدا عن الاذي عند التفاعل مع الفضاء السيبراني، كما كان لاتخاذ اجراءات من قبل الاباء والمعلمين دور في تشجيعهم للاستخدام النمن والمسؤول للوسائل التكنولوجية.

دراسة (**فقيه،2016**) والتي اهتمت بتسليط الضوء علي اهمية حماية البيانات الشخصية عبر مواقع التواصل الاجتماعي في ظل تنامي وتزايد ظاهرة انتهاك الخصوصيات الشخصية للمشتركين في مواقع التواصل الاجتماعي واوصت بحتمية تلقي مستخدمي مواقع التواصل الاجتماعي لدورات تثقيفية حول حماية خصوصيتهم المعلوماتية وبيان اهمية تلك البيانات وعدم الافراط في افشاءها واحاطتهم بما يمكن ان يحدث لهم من اضرار من جراء هذا الاستخدام.

بينما بحثت دراسة (**Shin; Lwin, 2017**) في كيفية ارتباط الوساطة النشطة التي يستخدمها الاباء والاقران ومعلمي المدارس في تقعيل الاستخدام الآمن لتجنب المخاطر عبر الانترنت والتي تم تطبيقها علي عينة بلغت 746 طالبا تتراوح اعمارهم بين 12:15 عاما وتوصلت الي ان المناقشات المتعلقة بالاستخدام الآمن ومخاطر الانترنت من مدرسي المدارس يمكن ان تقلل من تعرض المراهقين لمخاطر محتملة وتحد من انتهاك خصوصيتهم، بينما كان الاباء اقل احتمالية في تقديم مقترحات بشأن الاستخدام الآمن للانترنت حيث ارتبطت الوساطة الابوية بمتغير التواصل الاجتماعي بين الاباء وابنائهم، وانحصر دور الاقران في تقديم المساعدات لاقرانهم عند الحاجة، ولذا اوصت الدراسة بان توفر المدارس مزيدا من التعلم الممن عبر الانترنت لتثقيف الطلاب حول ضرورة الاستخدام الآمن

في حين هدفت دراسة (**سمان، 2017**) للتعرف علي الطرق المناسبة لاستخدام الفتاة للفيسبوك والوقاية من الوقوع ضحية للابتزاز، وقد أكدت نتائج الدراسة ان ابرز اسباب وقوع الفتاة للابتزاز يتعلق بارسال صورها ونشرها علي الفيسبوك دون تحصين الجهاز المستخدم وارجعت النتائج السبب في ذلك ان 93%من مفردات العينة من طلاب قسم علوم الاعلام بجامعة قاصدي مرباح ورقلة يرجعون ذلك الي انخفاض خبرة ووعي الفتيات في استخدام التكنولوجيا الحديثة دون السعي لاكتشاف مخاطرها.

اما دراسة (**عبد المجيد، 2018**) فتري ان تقنيات التواصل الالكتروني الحديث بتطورها السريع وتنوع اشكالها وانواعها اضافة الي سهولة استخدامها قد جعلت هذه الميزات منها اداة في متناول كثير من فئات المجتمع وان استخدام هذه المواقع لم يسبقه التأهيل اللازم لاستخدام التكنولوجيا بالشكل الصحيح وعدم الاهتمام بخطورة امن المعلومات التي تؤدي لكثير من مشاكل الاختراق والابتزاز الالكتروني و ان 58.8% من المراهقين عينة الدراسة لايمانعون في اخبار اصدقائهم بكلمة السر الخاصة بهم ولايستخدمون برامج حماية ولا يقومون بتحديث تلك البرامج نتيجة لعدم معرفتهم بخطورة الاستخدام غير الممن لوسائل التواصل الاجتماعي.

وركزت دراسة (**مسعد، 2018**) علي اهمية تنمية مهارات الاستخدام الآمن للكمبيوتر والانترنت لدي تلاميذ المرحلة الاعدادية عن طريق قياس فاعلية برنامج قائم علي التعليم المدمج في تنمية هذه المهارة، وتم اجراء التجربة علي مجموعتين ضابطة وتجريبية لعينة قوامها 16 تلميذ وتوصلت لتفوق تلاميذ المجموعة التجريبية علي الضابطة في مجال الاداء المهاري للاستخدام الآمن للانترنت

وعن دور الاسرة لتحقيق الاستخدام الآمن لوسائل التواصل الاجتماعي فتوصلت دراسة **(مشعل،2021)** ان هناك علاقة ارتباطية موجبة بين الدور الاسري لتحقيق الاستخدام الآمن لوسائل التواصل الاجتماعي وبين استراتيجيات مواجهة التنمر الالكتروني، فكلما زاد الدور الاسري في وقاية المراهقين وتقويم سلوكهم مع وسائل التواصل الاجتماعي يصبح الاستخدام اكثر آمنا ويقلل من التعدي الرقمي والاثار السلبية للتنمر ويتحقق الامن السيبراني.

وقدمت دراسة **(نصر،2022)** دليل للوالدين في كيفية حماية الاطفال والمراهقين من اخطار مواقع التواصل الاجتماعي وتعزيز استخدمهم الآمن لهذه المواقع بعد ان اظهرت النتائج وجود علاقة ارتباطية موجبة دالة إحصائيا بين دورالأ سرة لتحقيق الاستخدام الآمن لمواقع التواصل الاجتماعي للمراهقين من وجهة نظرهم وتعزيز الامن الفكري والاخلاقي، كما وجدت علاقة رتباطية موجبة دالة إحصائيا بين دور الاسرة لتحقيق الاستخدام الىمن لمواقع التواصل الاجتماعي وا ستراتيجيات مواجهة التنمر الالكتروني. و لذا اوصت الدرسة بضرورة إعداد برامج إرشادية لتوعية بالاستخدام الآمن لمواقع التواصل الاجتماعي يقوم بإعدادها أخصائي إدارة مؤسسات الأسرة والطفولة من خلال وحدة الاستشارات الاسرية.

الاستفادة من الدراسات السابقة

- أكدت نتائج الدراسات السابقة على عدم وجود طريقة موثوقة في كشف تقنية التزييف العميق " الديب فيك" حتى الأن رغم إجراء العديد من البحوث التجريبية لهذا الغرض مما يزيد من خطورتها.
- تنوع التخصصات العلمية في دراسة تقنية التزييف العميق فمنها الإعلامية و التكنولوجية والنفسية والاجتماعية والقانونية والحقوقية والسياسية وذلك يشير إلى تهديداتها المتعددة والمتشعبة.
- أهمية رفع الوعي بتقنية التزييف العميق لمواجهة تأثيراتها السلبية خاصة في ظل غياب طريقة موثوقة في كشف تلك التقنية.
- المحتوى الإباحي يشكل الغالبية العظمى من عمليات التزييف العميق لتقنية الديب فيك على منصات الوسائط الرقمية وهو مؤشر خطير للاستخدام السيئ لتلك التقنية في تصفية وتشوية الأفراد بشكل متعمد.
- أكدت الدراسات على تنوع تهديدات تقنية الديب فيك على مستوى الفرد والمجتمعات.
- اما المحور الخاص بالاستخدام الآمن فاهتمت غالبية الدراسات بفئة الاطفال والمراهقين والشباب من المستخدمين لمواقع التواصل الاجتماعي باعتبارهم من اكثر الفئات تهديدا وتعرضا لمخاطر الاستخدام غير الآمن
- أظهرت النتائج المسؤليات المشتركة للمدرسة والاسرة ومؤسسات المجتمع المدني في رفع وعي المستخدمين بالاستخدام الآمن واتخاذه وسيلة لحماية بياناتهم من التعرض لتهديدات ومخاطر الكترونية

- استفاد الباحثان من عرض الدراسات السابقة في بناء خلفية معرفية عن موضوع الدراسة وتحديد المشكلة البحثية، وتحديد المنهج المستخدم، واختيار العينة المناسبة وأدوات جمع البيانات وأدي التنوع بالدراسات الي اتاحة الفرصة بمقارنة ومناقشة نتائج الدراسة مع الدراسات السابقة.

مشكلة الدراسة

تستطيع تقنية التزييف العميق "الديب فييك" في العصر الحالي أن تلعب دوراً كبيراً في إثارة الفوضى من خلال قدرتها على تدمير حياة البشر والمجتمعات، وذلك من خلال ما تقدمه من مقاطع فيديو اصطناعية تبدو واقعية، ويكون من الصعب التمييز بين ما هو حقيقي؟! وما هو مزيف؟! خاصة بالنسبة للمستخدم العادي، حيث يتم تخليق تلك المقاطع بالإعتماد على الذكاء الاصطناعي أوتطبيقات التعلم الآلي، التي تعتمد على الصور ومقاطع الفيديو المتاحة لشخص ما وأدمجها وأستبدلها مما يؤدي في النهاية إلى إنشاء مقطع فيديو مزيف يبدو أصلياً يظهر فيه هذا الشخص وتصدر منه أقوال ومعلومات وتصريحات وأفعال لم يقوم بها في الحقيقة

وتعتبر مواقع التواصل الاجتماعي البيئة الخصبة لتمرير مقاطع الديب فييك نظراً لضخامة أعداد مستخدميها وسهولة مشاركة المحتوى المرئي وانتشاره السريع، لكي تحقق تلك المقاطع أهدافها الخبيثة في خداع المستخدمين بتشويه سمعه أحد الأشخاص أو تصفيه شخصية عامة أو إلصاق محتوى جنسي لأحد الأشخاص أو التأثير على نزاهة الانتخابات أو تمرير معلومات مغلوطة على لسان أحد الشخصيات ذات المصداقية وغيرها من الأهداف التي قد تصل إلى شن حروب.

وقد ساهم في انتشار استخدامها أن أدوات إنشاء التزييف العميق مثل FaceApp و FaceSwap متاحة على نطاق واسع ـ،حيث مكنت هذه الأدوات المستخدم العادي من استغلال تقنية الديب فييك بعد أن كانت قاصره على عدد قليل من المحترفين، الأمر الذي يوسع نطاق التهديدات.

ونظراً لحداثة تقنية الديب فييك وتعدد تهديداتها على مستوى الفرد والمجتمع، بالإضافة إلى عدم وجود طريقة موثوقة لإكتشاف مقاطع الديب فييك،أو توفر إطار نظري محدد يمكن الاعتماد عليه في كشف تلك المقاطع المزيفة، فيرى الباحثان أن توفر الإدراك لدى مستخدمي مواقع التواصل الإجتماعي بتهديدات التزييف العميق "الديب فييك" قد يدفعهم إلى الاستخدام الآمن لمواقع التواصل الإجتماعي كإجراء وقائي واستباقي للحماية من مخاطر تلك التقنية.

وتتمثل مشكلة الدراسة في الإجابة على التساؤل التالي:

ما العلاقة بين إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق "الديب فيك" و استخدامهم الأمن لتلك المواقع؟

أهمية الدراسة

تنبع أهمية الدراسة من:

1. أهمية دراسة تقنية التزييف العميق (الديب فيك) والتي تناقش موضوعا حيويا ينعكس آثاره علي مستخدمي مواقع التواصل الاجتماعي اذ تعد من أهم وأخطر تقنيات الذكاء الإصطناعي الحديثة.
2. اتساع تهديدات ومخاطر تقنية التزييف العميق القائمة والمحتملة على مستوى الفرد والمجتمع والعالم وأهمية التحقق من إدراك مستخدمي مواقع التواصل الإجتماعي لها.
3. أهمية دراسة الاستخدام الآمن لمواقع التواصل الاجتماعي بعد ظهور تقنية التزييف العميق حيث اصبحت هناك حاجة ملحة خاصة في ظل عدم توافر طريقة موثوقة في كشف هذا التزييف، والذي يجعل الاستخدام الأمن اجراء استباقي واحترازي ووقائي حتي لا يصبح المستخدم ضحية او يتم التلاعب به من خلال هذه التقنية.
4. تعدد واتاحة أدوات وتطبيقات التزييف العميق للمستخدم العادي وسهولة تنفيذ مقاطع فيديو مزيفة يصعب اكتشافها، يزيد من أهمية إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وأهمية استخدامهم الأمن لتلك الوسائل حتى لا تصبح مهمة المزيف أكثر سهولة.
5. أهمية دراسة مواقع التواصل الاجتماعي والتي تعتبر من مستحدثات العصر دائمة التغير والنمو وواسعة الانتشار بين الفئات العمرية المختلفة، والتي تعتبر البيئة الخصبة لتمرير التزييف العميق واتساع تهديداته.
6. قد تساعد نتائج الدراسة الحالية في تقديم معلومات ونتائج تساعد المختصين والدراسات اللاحقة في اعداد البرامج التوعوية لتهديدات ومخاطر تقنية التزييف العميق، واعداد برامج توعوية للاستخدام الأمن لمواقع التواصل الاجتماعي للحماية من تهديدات التزييف العميق.

7- قلة الدراسات الأجنبية وندرة الدراسات العربية التي تناولت تقنية التزييف العميق نظرا لحداثتها.

أهداف الدراسة

تهدف الدراسة بصفة رئيسية إلى دراسة العلاقة بين إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق و استخدامهم الأمن لتلك المواقع، وينبثق من هذا الهدف الأهداف الفرعية التالية:

1. قياس مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق.
2. التعرف على مستوى الاستخدام الأمن لمستخدمي مواقع التواصل الإجتماعي.
3. تحديد مستوى ثقة مستخدمي مواقع التواصل الاجتماعي في قدرتهم على كشف التزييف العميق (الثقة المزيفة).

4. الكشف عن الفروق في مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وفقاً للمتغيرات الديمجرافية (النوع – العمر – المستوى العلمي).
5. الكشف عن الفروق في مستوى الاستخدام الأمن لمستخدمي مواقع التواصل الاجتماعي وفقاً للمتغيرات الديمجرافية (النوع – العمر – المستوى العلمي).
6. التعرف على مستوى استخدام مواقع التواصل الاجتماعي لدى المبحوثين.

تساؤلات الدراسة

1. ما مستوى استخدام المبحوثين لمواقع التواصل الاجتماعي؟
2. ما مستوى ثقة المبحوثين في قدراتهم على كشف التزييف العميق (الثقة الزائفة)؟
3. ما مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق؟
4. ما مستوى الاستخدام الأمن لدى مستخدمي مواقع التواصل الاجتماعي؟
5. ما المتغيرات الديمجرافية (النوع – العمر – المستوى العلمي) لدى المبحوثين من مستخدمي مواقع التواصل الاجتماعي؟
6. ما العلاقة بين مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق و مستوى استخدامهم الأمن لتلك المواقع؟

فروض الدراسة

1.توجد علاقة إرتباطية طردية ذات دلالة إحصائية بين مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وبين مستوى استخدامهم الأمن لتلك المواقع.

2.توجد علاقة إرتباطية عكسية ذات دلالة إحصائية بين مستوى ثقة مستخدمي مواقع التواصل الاجتماعي في قدرتهم على كشف التزييف العميق (الثقة المزيفة) وبين مستوى استخدامهم الأمن لتلك المواقع.

3.توجد فروق ذات دلالة إحصائية في مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وفقاً للمتغيرات الديمجرافية (النطاق الجغرافي– النوع – العمر – المستوى العلمي).

4.توجد فروق ذات دلالة إحصائية في مستوى الاستخدام الأمن لمستخدمي مواقع التواصل الاجتماعي وفقاً للمتغيرات الديمجرافية (النطاق الجغرافي- النوع – العمر – المستوى العلمي).

5.توجد علاقة إرتباطية طردية ذات دلالة إحصائية بين مستوى استخدام مواقع التواصل الإجتماعي وبين مستوى إدراك المستخدمين لتهديدات التزييف العميق.

الإطار المعرفي

كانت حملات المعلومات المزيفة والقيل والقال والتشهير موجودة على مدار معظم تاريخ البشرية، حتى عمليات التلاعب في الصور عن طريق تبديل الوجه موجودة منذ أكثر من 20عاماً (**Blanz ; Scherbaum;; et al., 2004**)، ومع ذلك فإن التطورات الأخيرة في تقنيات الذكاء الاصطناعي (AI) و خوارزميات التعلم العميق أدت إلى تحسين قدرة المستخدمين على إنشاء المحتوى الرقمي وتحويله ومعالجته وظهور مقاطع الديب فييك، و هي مقاطع فيديو لاستبدال الوجوه تبدو واقعية.

تقنية deepfake أو التزييف العميق بدأت عام 2017 وهي عبارة عن مقاطع فيديو يتم التلاعب بها رقمياً لجعلها تبدو وكأن شخص "يقول أويفعل شيًئا لم يفعله بشكل واقعي." لقد انتشرت التكنولوجيا الجديدة بشكل فيروسي على الإنترنت حيث تضاعفت عدد عمليات التزييف العميق على الإنترنت بين عامي 2018 و2019 وخاصة المواد الإباحية والمحاكاة الساخرة (**Wilkerson, 2021**).

تم تسميت deepfake بهذا المصطلح نظراً لأنه يجمع بين الواقع والزييف والذي تعرف تطبيقاته بالفبركة العميقة، التي تعتبر أبرز نتاجات الذكاء الاصطناعي التي مكنت من القيام بتزييف مقاطع صوتيه وصوريه متحركة لشخصيات عامة أو غير معروفة سواء كان المستهدف منها أشخاص أو مجتمعات (**الشمري: 2021**).

تمت صياغة مصطلح deepfake لأول مرة بواسطة مستخدم Redditالذي أنشأ منتدى بإسم deepfakes في الثاني من نوفمبر 2017، وقام بإنشاء مقطع فيديو إباحي مزيف باستخدام وجه نجمة هوليوود Gal Gadot،وخصص هذا المستخدم الذي لم يكشف عن هويته ذلك المنتدى لتبديل الوجوه صناعياً للمشاهير في مقاطع فيديو إباحية بالاعتماد على برامج التعلم العميق ؛ ولذا تم إزالة الحساب من Reddit في السابع من فبراير 2018، ومنذ ذلك التاريخ أصبحت تقنية الديب فييك تنتشر بشكل سريع خاصة مع ظهور منتديات وأدوات وخدمات جديدة للتزييف العميق و تجربة المزيد من المبدعين نماذج من التعلم العميق الجديدة (**Gabriele ,2021**)

في الوقت نفسه، قامت شركات التكنولوجيا مثل Snapو Appleو ByteDance بدمج وظائف deepfake في منصاتها بغرض توفير جانب من الترفيه والتسليه لمستخدميها.

وانتقل استخدام تقنية Deepfake إلى وسائل الإعلام والإعلانات وصناعة الأفلام على نطاق واسع، حيث أصبحت المؤثرات الخاصة والدبلجة وإعادة إنتاج الماضي أمر بسيط، فعلى سبيل المثال مكنت تقنية الديب فييك الممثل Robert De Niro من لعب شخصية أصغر منه في فيلم The Irish Man، كما تم إنشاء نسخة رقمية من الممثل الراحلCushig Peter في فيلم A Star Wars Story عام 2018.

كما استطاعت بعض المواقع ان تتيح لمستخدميها التلاعب بالصور والمقاطع مثل موقع Raface الذي يتيح للمستخدمين فرص تبادل الوجوه في الفيديوهات وملفات GIF، وموقع

MYHeritage الذي يحرك صور الاقارب المتوفيين، وموقع Zaog التطبيق الصيني الذي يسمح للمستخدمين بوضع وجوههم علي شخصيات شهيرة

وقد كشفت تقنية الديب فيك عن وجهها القبيح والتي تتيح لأي شخص يمتلك مجموعة من الصور والفيديوهات سواء عن طريق البحث في جوجل او مواقع التواصل الاجتماعي بإدخال البيانات لاستبدال الوجوه وانتاج مقاطع فيديو مزيفه بشكل لاتشوبه شائبة تقريًبا، حيث لاتحتاج التقنية إلى أي إشراف بشري بعد عملية التعلم الآلي الأولية ولكن تواصل الخوارزمية تحسين العملية بشكل مستقل ولا تستطيع العين المجرده كشف التلاعب.

.يمكن لأي شخص إنشاء مقاطع فيديو إباحية يقوم ببطولتها مشاهير أوسياسيون أو أصدقاء أو أعداء من بين المشاهير الذين كانوا ضحايا مقاطع فيديو.

نماذج واقعية لإثارة تقنية التزييف العميق " الديب فيك " للفوضى

شهدت دولة الهند في أبريل عام 2018 انتشار مقطع فيديو على تطبيق WhatsApp تظهر خلاله مجموعة من الأطفال يلعبون لعبة الكريكيت في الشارع.، فجأة يظهر رجلان على دراجة بخارية وأمسكوا بأحد الأطفال الصغار،ثم أسرعوا بعيًدا، تسبب مقطع فيديو "الاختطاف" هذا في ارتباك وذعر واسع النطاق وحالة فوضى شديدة بالهند، وكانت تلك اللقطات بتقنية الديب فيك عن طريق تعديل لجزء من فيديو لحملة تثقيفية عامة في باكستان،صممت لزيادة الوعي بعمليات اختطاف الأطفال**(BBC News, 2018)** .

في نفس الشهر، نشرت BuzzFeed مقطع فيديو يتحدث به الرئيس الأمريكي الأسبق باراك

أوباما مباشرة إلى الكاميرا، وفي أول 35 ثانية يظهر أوباما فقط، وبعد بضع تصريحات معتدلة،ألقى أوباما قنبلة حيث وصف الرئيس ترامب بالمغفل، وبعدها تظهر الشاشة منقسمة بها أوباما على اليسار ويظهر الممثل الكوميدي والمخرج جودان بيل على اليمين مع تتطابق تعابير وجه أوباما وبيل و حركة شفاهما تمامًا باستخدام الذكاء الاصطناعي من خلال تقنية الديب فيك ؛ لدق ناقوس الخطر والتحذير من واقعية فيديوهات الديب فيك وخطورة استخداماته المحتملة، حقق فيديو أوباما المزيف والذي نشر تحت عنوان (لن تصدق ما يقوله أوباما في هذا الفيديو) 5ملايين مشاهدة وأكثر من 83000 مشاركة على Facebook، وأكثر من 5ملايين مشاهدة على YouTube و 4.75 مليون مشاهدة و ما يقرب من 52000 تغريدة على Twitter **(Facebook, 2018; Twitter, 2018; YouTube, 2018)**.

في أواخر عام 2018 كانت هناك تكهنات مكثفة حول صحة الرئيس الجابوني علي بونجو، الذي كان غائبًا عن الحياة العامة لعدة أشهر. في محاولة لإنهاء التكهنات، أصدرت الحكومة مقطع فيديو لبونجو يلقي خطابًا تقليديًا بمناسبة العام الجديد. ومع ذلك، فإن ظهور بونجو غير المعتاد في الفيديو دفع الكثيرين على وسائل التواصل الاجتماعي،بما في ذلك السياسي الغابوني برونو موبامبا، إلى إعلان أن الفيديو كان مزيف عميًقا، ممايؤكد شكوكهم في أن الحكومة كانت تتستر على صحة بونجو أو تخفي وفاته، وبعد أسبوع من إطلاق الفيديو وسط

تصاعد الاضطرابات شن أفراد من الجيش الجابون محاولة انقلاب فاشلة ضد الحكومة.

ظهرت فضيحة سياسية في يونيو 2019 تتعلق بفيديو شذوذ جنسي يظهر فيه وزير الشؤون الاقتصادية الماليزي Azmin Ali يمارس اللواط، دافع الوزير وأنصاره ومن بينهم رئيس الوزراء الماليزي بأن الفيديو كان بتقنية الديب فييك بقصد تخريب حياته السياسية، ومع ذلك لم يتمكن الخبراء الدوليون من العثور على أي مؤشرات على التلاعب بالفيديو.

كانت القضية الأكثر تداولاً عبر منصات التواصل الاجتماعي للفتاة المصرية بمحافظة الغربية والتي لم تتجاوز 17 عام تدعى بسنت خالد ضحية الديب فييك والابتزاز الالكتروني والتي قامت بالانتحار 25 ديسمبر 2021 بعد نشر محتوى اباحي مزيف لها عبر مواقع التواصل الاجتماعي، انتشر بقريتها وبين زملائها وعاشت لحظات قاسية بين تعنيف وشك واتهام وفضيحة لها وأسرتها، ونتيجة تلك الحادثة أصدرت دار الإفتاء المصرية بياناً عبر صفحتها الرسمية بموقع التواصل الاجتماعي فيسبوك أوضحت خلاله أنه لا يجوز شرعاً استخدام تقنية الديب فييك المعروفة بالتزييف العميق لتلفيق مقاطع مرئية أو مسموعة للأشخاص.

تهديدات تقنية التزييف العميق "الديب فييك"

تستمد من النماذج الواقعية لاستخدامات الديب فييك السابقة وتوقعات الخبراء لمخاطره المحتملة التهديدات الأتية:

1. تهديدات الخصوصية الفردية

تستخدم تقنية الديب فييك لإيذاء الأفراد بقصد الاستغلال أو افساد حياتهم وتتعدد أشكال تهديد خصوصية الأفراد عن طريق الديب فييك كالتالي:

- **الانتقام الاباحي**

هو جريمة تقتضي مشاركة محتوى إباحي صريح بشكل عام على الإنترنت دون موافقة الشخص الظاهر بالمحتوى بهدف الانتقام.

كانت عملية الانتقام الإباحي قبل ظهور الديب فييك تتم غالبا بعد قرصنة حسابات مواقع التواصل الاجتماعي والسطو على مواد شخصية إباحية، أو قرصنة هواتف ذكية وحسابات التخزين السحابي، وبعد ظهور تقنية الديب فييك أصبحت تعتمد على الصور والفيديوهات التي ينشرها الضحية ويستطيع الشخص العادي الوصول اليها واستخدمها في انتاج فيديو اباحي مزيف يبدو واقعياً بهدف الانتقام.

- **الابتزاز المالي**

عملية تهديد وترهيب للضحية بنشر صور أو مواد فيلمية أو تسريب معلومات سرية تخص الضحية، مقابل دفع مبالغ مالية لصالح المبتزين.

- **الابتزاز الجنسي**

وهو التهديد بفضح صورة أو فيديوهات عارية أو جنسية فاضحة من أجل حمل الشخص على القيام بشيء مثل إرسال المزيد من الصور العارية أو الجنسية الصريحة، أو القيام بأعمال جنسية".

- دعاوي الاختطاف الاحتيالية
- التنمر
- انتحال الشخصية

2. تهديد الأمن القومي والديمقراطية

وصف الخبراء تقنية الديب فييك بأنها "أداة جديدة قوية لأولئك الذين قد يرغبون في استخدام المعلومات المضللة للتأثير على الانتخابات."

مما يشير إلى أن التزييف العميق هو سلاح سياسي يجب وضعه في الاعتبار، حيث يتخوف بعض السياسيين من استخدام التقنية خلال الانتخابات على نحو قد يُؤثر سلبًا في سير العملية الانتخابية.

وفي هذا الإطار، كان الديب فييك هو محور نقاش جلسة استماع لجنة الاستخبارات بمجلس النواب الأمريكي حول المخاطر الأمنية على الأمن القومي والانتخابي في الولايات المتحدة، محذرةً من سلبياتها على انتخابات 2020. فقد بات ممكنًا تصميم فيديوهات إباحية مفبركة لأي منافس أو أخرى سياسية ذات أثارٍ كارثية، ما دفع عضو مجلس النواب الأمريكي "ماركو روبيو" (Marco Rubio) لاعتبار أن تلك التقنية تُعادل خطورة الأسلحة النووية، قائلًا إن تهديد الولايات المتحدة الأمريكية كان يتطلب حاملات طائرات وأسلحة نووية وصواريخ بعيدة المدى. أما اليوم، يتطلب ذلك التهديد استعدادات أخرى لمواجهة قدرته على الدخول إلى أنظمة الولايات المتحدة الإلكترونية وأنظمتها البنكية أو إنتاج فيديوهاتٍ مزيفة تبدو واقعية جدًا قادرة على تدمير النظام الانتخابي واضعاف البلاد داخليًا **(Diakopoulos ; Johnson ,2021)**

3. تهديد الاحتيال والابتزاز المالي للشركات

رصد ما لا يقل عن ثلاث حالات خداع الشركات لتحويل ملايين الدولارات إلى حساباتٍ مصرفيةٍ خاطئةٍ، عن طريق الاحتيال بتقليد صوت شخص ما.

فقد تتسبب تسجيلاتٌ صوتيةٌ مبركةٌ لبعض المديرين التنفيذيين في ذيوع العمليات الاحتيالية لاسيما في الأعمال التجارية من خلال التصيد الاحتيالي. وعلى سبيل المثال، تعرض الرئيس التنفيذي لإحدى شركات الطاقة البريطانية لسرقة 243 ألف دولار باستخدام مقطعٍ صوتيٍ مصنوعٍ لرئيس شركته الأم يَطلب منه إجراء تحويلٍ ماليٍ طارئٍ. وقد كان التزييف مقنعًا إلى حدّ تصديقه، فحدث التحويل المالي في نهاية المطاف. ولم يشك الرئيس التنفيذي في الأمر إلا بعد أن طَلب منه رئيسه الحقيقي إجراء تحويلٍ ماليٍ آخر

فَكُشف الأمر، ولكن لم يعد من الممكن استعادة المال المسروق بعد تحويله إلى حسابٍ أخرٍ. ومن الممكن استخدام الديب فييك في ابتزاز رؤساء الشركات عن طريق تهديدهم بنشر مقاطع فيديو قد تضر بسمعتهم ما لم يدفعوا أموالًا مقابل عدم النشر.

4. اختلاق الأزمات الدبلوماسية

طرح بعض الخبراء سيناريو مفاده انتشار فيديو يقوم فيه زعيمٌ عالميٌ بمناقشة خطط تنفيذ الاغتيالات في دولةٍ معاديةٍ على سبيل المثال. فلا يمكن إغفال التداعيات السياسية السلبية لذلك الفيديو حتى حال اكتشاف تزويره؛ إذ يتوقع الخبراء استخدام الديب فييك لإحداث البلبلة ونشر المعلومات المضللة وبخاصة على الصعيد الدولي.

5. تهديد مصداقية الفيديو

إذا لم يتم خداع المشاهدين من خلال تقنية الديب فييك، فقد يصبحون غير متأكدين من حقيقية أي محتوى يتعرضون له، في ظل عدم وجود طريقة موثوقة لكشف التلاعب بالفيديو عن طريق تقنية الديب فييك.

نوع الدراسة ومنهجها:

تنتمي الدراسة الي البحوث الوصفية التي تهدف الي وصف موضوع او مشكلة الدراسة وتقرير خصائصها وتحديدها تحديدا كيفيا وكميا وهي بحوث تهتم بتحديد الواقع وجمع الحقائق عنه وتحليل بعض جوانبه بما يساهم في العمل علي تطويره.

واعتمدا الباحثان علي منهج المسح بالعينة من اجل استخلاص النتائج من مستخدمي مواقع التواصل الاجتماعي وذلك لدراسة مدى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وعلاقته باستخدامهم الآمن لتلك المواقع

مصطلحات الدراسة:

تتحدد مصطلحات الدراسة الاجرائية فيما يلي:

تقنية التزييف العميق "الديب فيك ":

احدي تقنيات الذكاء الاصطناعي تعمل علي تزييف الوسائط المتعددة بشكل يبدو واقعي باستخدام برمجيات الكترونية.

الثقة المزيفة:

ويقصد بها الثقة التي يعطيها الافراد لانفسهم حول قدرتهم لكشف تزييف الصور والفيديوهات المعتمدة علي تقنية الديب فيك

الاستخدام الآمن:

ويقصد بها الاجراءات التي يقوم بها مستخدمي مواقع التواصل الاجتماعي لحماية وتأمين بياناتهم الشخصية وخصوصيتهم من الانتهاك والحد من الوصول لاستخدام صورهم وفيديوهاتهم الخاصة وتداولها دون اذن مسبق منهم وبما يضمن عدم تعرضهم لتهديدات ومخاطر الكترونية.

مجتمع الدراسة:

تم تحديد مجتمع الدراسة من مستخدمي مواقع التواصل الاجتماعي بمحافظات جمهورية مصر العربية

عينة الدراسة

قاما الباحثان بالتطبيق علي عينة من مستخدمي مواقع التواصل الاجتماعي بلغ قوامها (600 مفردة) تم سحبها بأسلوب العينةالعشوائية الطبقية، لزيادة فرصة تمثيل خصائص المجتمع في العينة وقد تقسيم مجتمع الدراسة الي طبقات وفقا لمتغير مكان الاقامة او المحافظة التي يقيم فيها المبحوث وقد تم الاعتماد علي اسلوب التوزيع المتساوي وفقا للنطاق الجغرافي 150 مفردة لكل محافظة من المحافظات الأربعة محل الدراسة بعد استبعاد الاستمارات الغير مكتملة وتمثلت المحافظات في كلا من،(القاهرة: تمثيلا للعاصمة)، (بورسعيد: تمثيلاً لوجه بحري واقليم القناة)، (الدقهلية: تمثيلاً لريف مصر)، (أسيوط: تمثيلاً لصعيد مصر)،وقد تم الاعتماد علي اسلوب التوزيع المتساوي بأن تكون احجام العينات المسحوبة من الطبقات متساوية خاصة وان اسلوب التوزيع المتناسب يحتاج الي وجود احصائيات دقيقة عن مستخدمي مواقع التواصل الاجتماعي في كل محافظة وهو ما لم يتوفر بشكل دقيق، وجاء توزيع العينة كالاتي:

توزيع عينة الدراسة من مستخدمي مواقع التواصل الاجتماعي وفقاً للمتغيرات الديمجرافية:

جدول (1) توزيع عينة الدراسة وفقاً للمتغيرات الديمجرافية

المتغيرات الديمجرافية	الفئات	ك	%
النطاق الجغرافي	القاهرة	150	25
	بورسعيد	150	25
	الدقهلية	150	25
	أسيوط	150	25
النوع	أنثى	329	54.8
	ذكر	271	45.2
العمر	20 فأقل	116	19.3
	21: 30	152	25.3
	31: 40	187	31.2
	41: 50	92	15.3
	أكثر من 50	53	8.8
المستوى التعليمي	طلاب المدارس	104	17.3
	طلاب الجامعات	141	23.5
	دبلوم	38	6.3
	بكالوريوس	296	49.3
	ماجستير	14	2.3
	دكتوراه	7	1.2
	يقرأ ويكتب	0	0
اجمالى العينة		600	100

أدوات جمع البيانات

قام الباحثان بإعداد أدوات جمع البيانات في ضوء أهداف الدراسة و تضمنت استمارة الاستبيان الالكتروني واعتمدت الدراسة علي توزيع الاستمارة وتعبئها رقميا علي مستخدمي مواقع التواصل الاجتماعي عبرالصفحات والجروبات والمواقع المختلفة لكل محافظة في عينة الدراسة وطبقت الاستمارة في الفترة من 15يوليو الي 15 اغسطس 2022م وقد تم وضع **تعريف لتقنية التزييف العميق للمبحوثين** في اعلي الاستمارة، و اشتملت ثلاثة محاور رئيسية:

المحور الأول: البيانات الشخصية وبيانات الاستخدام لمواقع التواصل الاجتماعي.

المحور الثاني: إدراك تهديدات الديب فيك.

المحور الثالث: الاستخدام الأمن لمواقع التواصل الاجتماعي.

المحور الأول: البيانات الشخصية وبيانات الاستخدام لمواقع التواصل الاجتماعي.

- النطاق الجغرافي: تم التقسيم إلى (القاهرة – بورسعيد – اسيوط- الدقهلية)
- النوع: تم التقسيم إلى (ذكر، أنثى) بترميز (1، 2) على التوالي.
- العمر: تم التقسيم إلى فئات عمرية ((20 فأقل)،(21: 30)،(31: 40)، (41: 50)، (أكثر من 50)) بترميز (1، 2، 3، 4، 5) على التوالي.
- المستوى العلمي: (يقرأ ويكتب – طلاب المدارس – طلاب الجامعات – دبلوم – بكالوريوس – ماجستير – دكتوراه) بترميز (1، 2، 3، 4، 5، 6، 7) على التوالي.
- ترتيب مواقع التواصل الاجتماعي المفضلة لدى المبحوثين(فيسبوك، تويتر، سنابشات، انستجرام، واتساب، يوتيوب، تيكتوك) بترميز (1 = 7 نقاط)، 2 = 6 نقاط، 3 = 5 نقاط، 4 = 4 نقاط، 5 = 3 نقاط، 6 = نقطتين، 7 = نقطة واحدة).
- مستوي استخدام المبحوثين لمواقع التواصل الاجتماعي (نادراً، أحياناً،دائماً) بترميز (1، 2، 3) على التوالي.
- معدل استخدام المبحوثين لمواقع التواصل الاجتماعي يومياً وتم تقسيمها إلى (لا استخدمه بشكل يومي، أقل من ساعة يومياً، من ساعة لأقل من ساعتين يومياً، من ساعتين لأقل من 3 ساعات يومياً، من 3ساعات لأقل من 4 ساعات يومياً، من 3ساعات لأقل من 4 ساعات يومياً، 4 ساعات فأكثر) بترميز (1، 2، 3، 4، 5، 6، 7) على التوالي.

المحور الثاني: تهديدات التزييف العميق (الديب فيك).

- مصادر معرفة المبحوثين بمصطلح الديب فيك (التزييف العميق) وتم تقسيمها إلى (صفحات وسائل التواصل الاجتماعي - مواقع صحفية - برامج التليفزيون - الصحف الورقية - المعارف والأصدقاء- الكتب -التعريف الموجود اعلى استمارة الاستبيان) بترميز (1، 2، 3، 4، 5، 6، 7) على التوالي.

- مستوى ثقة المبحوثين في قدرتهم على كشف الديب فيك في حالة التعرض لأي فيديو مزيف (الثقة المزيفة) - والتي تم اعتبارها ثقة مزيفة وخادعة بناءاً على نتائج الدراسات السابقة والتي أكدت عدم وجود طريقة موثوق بها بشكل قاطع في كشف الديب فيك وعدم قدرة المستخدم العادي في كشف التزييف - وتم تقسيمها إلى (لا أثق مطلقاً في قدرتي على كشف الديب فيك، أثق إلى حد ما في قدرتي على كشف الديب فيك، أثق تماماً في قدرتي على كشف الديب فيك) بترميز (1، 2، 3) على التوالي.

- **مقياس إدراك المبحوثين لتهديدات التزييف العميق (الديب فيك)**

تضمن المقياس (18) عبارة، وتتحدد الإجابة على العبارات من خلال ثلاثة اختيارات تمثلت في (نعم – أحياناً – لا)، وتم تصحيح الاستجابات من خلال مفتاح تصحيح ثلاثي (3، 2، 1) للعبارات الإيجابية و (1، 2، 3) للعبارات السلبية، وقد تم تقسيم مستوى إدراك مستخدمي مواقع التواصل لتهديدات الديب فيك إلى ثلاثة مستويات من خلال تحديد الدرجة القصوى للمقياس بضرب عدد العبارات في أعلى استجابة (18 × 3 = 54)، وتحديد أدنى درجة للمقياس من خلال ضرب عدد العبارات في أقل استجابة (18 × 1 = 18) ومن ثم يتم حساب المدى عن طريق طرح أدنى درجة من الدرجة القصوى (54 – 18 = 36) ثم يتم قسمة الناتج على عدد المجموعات (36 ÷ 3 = 12) ويتم تحديد المستوى كالتالي:
المستوى المنخفض (أقل من 30)، المستوى المتوسط (من 30 إلى 42)، المستوى المرتفع (43 فأكثر)

المحور الثالث: الاستخدام الأمن لمواقع التواصل الاجتماعي.

- **مقياس الاستخدام الأمن لمواقع التواصل الاجتماعي**

تضمن المقياس (15) عبارة، وتتحدد الإجابة على العبارات من خلال ثلاثة اختيارات تمثلت في (نعم – أحياناً – لا)، وتم تصحيح الاستجابات من خلال مفتاح تصحيح ثلاثي (3 - 2 - 1) للعبارات الإيجابية و (1 – 2 - 3) للعبارات السلبية، وقد تم تقسيم الاستخدام الأمن لمواقع التواصل الاجتماعي إلى ثلاثة مستويات من خلال تحديد الدرجة القصوى للمقياس بضرب عدد العبارات في أعلى استجابة (15 × 3 = 45)، وتحديد أدنى درجة للمقياس من خلال ضرب عدد العبارات في أقل استجابة (15 × 1 = 15) ومن ثم يتم حساب المدى عن طريق طرح أدنى درجة من الدرجة القصوى (45 – 15 = 30) ثم يتم قسمة الناتج على

عدد المجموعات (30 ÷ 3 = 10) ويتم تحديد المستوى كالتالي: المستوى المنخفض (أقل من 25)، المستوى المتوسط (من 25 إلى 35)، المستوى المرتفع (36 فأكثر).

حدود الدراسة:

حدود موضوعية: وتتمثل في الكشف عن إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق (الديب فييك) وعلاقته باستخدامهم الآمن لتلك المواقع

حدود زمانية: وتتمثل في فترة تطبيق الاستمارة الالكترونية في الفترة من 15 يوليو الي 15 اغسطس

حدود مكانية: اقتصر التطبيق علي محافظة القاهرة وبورسعيد والدقهلية واسيوط

الصدق والثبات:

أولاً: صدق الاستبيان

تم حساب صدق الاستبيان بطريقتين:

1.صدق المحكمين (الصدق الظاهري وصدق المحتوى)

للتحقق من الصدق الظاهري لمحتوى إستمارة الإستبيان تم عرضها على 5 أساتذة في مجال الإعلام لتحكيم الإستبيان من حيث: مناسبة عبارات الإستبيان للجانب المراد قياسه، وتحديد مدى صحة صياغة العبارات، إبداء الملاحظات للتعديل، وجاء متوسط نسب إتفاق السادة المحكمين على عبارات الإستبيان (92.4%).

2.صدق الإتساق الداخلي (الصدق البنائي)

- **مقياس تهديدات التزييف العميق (الديب فييك):**

- تم اختبار صدق مقياس تهديدات التزييف العميق (الديب فييك) باستخدام الاتساق الداخلي عن طريق حساب معامل الارتباط بيرسون بين كل عبارة من عبارات المقياس وبين الدرجة الكلية للمقياس وكانت النتائج كالتالي:

جدول (1) صدق الاتساق الداخلي لمقياس تهديدات الديب فييك

رقم العبارة	معامل ارتباط بيرسون	مستوى الدلالة	رقم العبارة	معامل ارتباط بيرسون	مستوى الدلالة
ع 1	.934**	0.01	ع 10	.898**	0.01
ع 2	.891**	0.01	ع 11	.881**	0.01
ع 3	.908**	0.01	ع 12	.883**	0.01
ع 4	.881**	0.01	ع 13	.767**	0.01
ع 5	.927**	0.01	ع 14	.869**	0.01
ع 6	.806**	0.01	ع 15	.749**	0.01
ع 7	.919**	0.01	ع 16	.892**	0.01
ع 8	.785**	0.01	ع 17	.929**	0.01
ع9	.901**	0.01	ع 18	.863**	0.01

ويوضح الجدول السابق: أن تراوحت معاملات الإرتباط بين (**934.:.**749) وجميعها دالة احصائياً عند مستوى دلالة 0.01، مما يؤكد على صدق وتجانس عبارات المقياس.

- **مقياس الاستخدام الأمن لمواقع التواصل الاجتماعي:**

- تم اختبار صدق مقياس الاستخدام الأمن لمواقع التواصل الاجتماعي باستخدام الاتساق الداخلي عن طريق حساب معامل الارتباط بيرسون بين كل عبارة من عبارات المقايس وبين الدرجة الكلية للمقياس وكانت النتائج كالتالي:

جدول (2) صدق الاتساق الداخلي لمقياس الاستخدام الأمن لمواقع التواصل الاجتماعي

رقم العبارة	معامل ارتباط بيرسون	مستوى الدلالة	رقم العبارة	معامل ارتباط بيرسون	مستوى الدلالة
ع 1	.660**	0.01	ع9	.757**	0.01
ع 2	.725**	0.01	ع 10	.628**	0.01
ع 3	.745**	0.01	ع 11	.786**	0.01
ع 4	.760**	0.01	ع 12	.773**	0.01
ع 5	.726**	0.01	ع 13	.799**	0.01
ع 6	.912**	0.01	ع 14	.713**	0.01
ع 7	.601**	0.01	ع 15	.817**	0.01
ع 8	.630**	0.01			

ويوضح الجدول السابق: أن تراوحت معاملات الإرتباط بين (**912.:.**601) وجميعها دالة احصائياً عند مستوى دلالة 0.01، مما يؤكد على صدق وتجانس عبارات المقياس.

ثانياً: ثبات الاستبيان

تم اختبار ثبات الاستبيان عن طريق حساب معامل ثبات ألفا كرونباخ وجاءت النتائج كالتالي:

جدول (3) حساب معامل ثبات ألفا كرونباخ لمحاور الاستبيان

محاور الاستبيان	معامل ثبات ألفا كرونباخ
مقياس تهديدات التزييف العميق (الديب فيك)	.918
مقياس الاستخدام الأمن لمواقع التواصل الاجتماعي	.805
الاستبيان بالكامل	.847

ويوضح الجدول السابق: أن جاء معامل ثبات ألفا كرونباخ لمقياس تهديدات الديب فيك.918، كما جاء معامل ثبات ألفا كرونباخ لمقياس الاستخدام الأمن لمواقع التواصل الاجتماعي.805، في حين معامل ثبات ألفا كرونباخ.847، مما يشير إلى أن الاستبيان يتمتع بمعامل ثبات مقبول مما يعني امكانيه استخدامه في البحث الحالي والوثوق في النتائج التي يسفر عنها.

نتائج الدراسة:

1- ترتيب مواقع التواصل الاجتماعي المفضلة من وجهة نظر المبحوثين:

جدول (5)ترتيب مواقع التواصل الاجتماعي المفضلة من وجهة نظر المبحوثين (ن = 600)

الترتيب / مواقع التواصل	الأول	الثاني	الثالث	الرابع	الخامس	السادس	السابع	مجموع الأوزان	الوزن النسبي
فيسبوك	289	92	84	36	54	29	16	3375	20.0
واتساب	123	156	103	77	53	41	47	2908	17.2
تيك توك	63	179	58	57	102	92	49	2572	15.2
انستجرام	51	53	95	134	181	61	25	2376	14.1
يوتيوب	25	42	118	116	79	127	93	2065	12.2
تويتر	30	11	112	94	73	72	208	1883	11.1
سنابشات	19	67	30	86	58	178	162	1721	10.2
؛	16900								

يتضح من الجدول السابق: تفضيل جمهور مستخدمي مواقع التواصل الاجتماعي لموقع (فيسبوك) حيث جاء في مقدمة التفضيلات بوزن مئوي 20%، يليه في الترتيب تطبيق (واتساب) بوزن مئوي 17.2%، وفي الترتيب الثالث (تيك توك) بوزن مئوي 15.2%، وفي الترتيب الرابع (انستجرام) بوزن مئوي 14.1%، ثم في الترتيب الخامس (يوتيوب) بوزن مئوي 12.2%، وجاء في الترتيب السادس (تويتر) بوزن مئوي 11.1%، بينما جاء في الترتيب السابع والأخير (سنابشات) بوزن مئوي 10.2%.

واتفقت هذه النتيجة مع دراسة كلامن **(لطفي،2019)** حيث جاء موقع فيس بوك في مقدمة مواقع التواصل الاجتماعي المفضلة بنسبة 47.08% يليه واتساب في المرتبة الثانية، ودراسة **(اللبان ؛ الشريف، 2016)** حيث جاء موقع فيس بوك في صدارة المواقع التي يستخدمها المبحوثون بنسبة 92.8 % حيث ارجع هذا التفوق للأدوات التفاعلية التي لا تتاح للكثير من المواقع الاخري.

ويمكن تفسير هذه النتيجة بأن تلك المواقع تتمتع بثقة المستخدمين في تبادل المعلومات والبيانات أثناء التواصل مع الأخرين وهذا ما أكدته دراسة **(عبد الكريم، 2018)** حيث بينت الدراسة أن نسب (62.8% - 50%) من المستخدمين يثقون بدرجة كبيرة في موقعي (واتساب – فيسبوك) على التوالي وان اختلفت في الترتيب مع الدراسة الحالية

2- مستوى استخدام المبحوثين لمواقع التواصل الاجتماعي:

جدول (6) مستوى استخدام المبحوثين لمواقع التواصل الاجتماعي

مستوى استخدام	ك	%
دائماً	458	76.3
أحياناً	119	19.8
نادراً	23	3.8
الاجمالي	600	100

يتضح من الجدول السابق: ارتفاع مستوى استخدام المبحوثين لمواقع التواصل الاجتماعي حيث جاء (دائماً) في الترتيب الأول بنسبة 76.3%، يليه في الترتيب الثاني (أحياناً) بنسبة 19.8%، وفي الترتيب الثالث والأخير (نادراً) بنسبة 3.8%.

ويمكن تفسير ارتفاع مستوي الاستخدام لمواقع التواصل الاجتماعي من جانب المبحوثين الي الانتشار الواسع لاستخدامات الهواتف الذكية و ما تمتلكه تلك المواقع من قدرات وخصائص تخطت كونها وسيلة للتواصل والتعارف مع الاخرين بل اصبحت جزء اساسي من الطقوس الحياتية للافراد وامتدت لتشمل مجالات العمل والتعلم و الحصول على الأخبار والترفيه ونشر الثقافة والبيع والشراء كما انها اصبحت الوسيلة الاسرع لتحقيق الشهرة والبروز مثل المؤثرين على مواقع التواصل.

وتتفق هذه النتيجة مع ماتوصلت اليه دراسة **(عصام، 2013)** والتي أكدت ان اغلبية المبحوثين يستخدموا مواقع التواصل الاجتماعي بشكل دائم بنسبة 73%

3- معدل استخدام المبحوثين لمواقع التواصل الاجتماعي:

جدول (7)معدل استخدام المبحوثين لمواقع التواصل الاجتماعي

معدل الاستخدام	ك	%
من ساعة لأقل من ساعتين يومياً	153	23.7
من 3ساعات لأقل من 4 ساعات يومياً	185	29.2
من ساعتين لأقل من 3 ساعات يومياً	141	20.5
4 ساعات فأكثر	76	12.7
أقل من ساعة يومياً	53	8.8
لا استخدمه بشكل يومي	31	5.2
الاجمالي	600	100

وبينت نتائج الجدول معدلات الاستخدام اليومي حيث جاءت نسبة 29.2% من المبحوثين يستخدمون مواقع التواصل الاجتماعي (من 3ساعات لأقل من 4 ساعات يومياً)، وبلغت نسبة من يستخدون تلك المواقع (من ساعة لأقل من ساعتين يومياً) 23.7% في الترتيب الثاني، ثم في الترتيب الثالث (من ساعتين لأقل من 3 ساعات يومياً) بنسبة 20.5%، وفي الترتيب الرابع (4 ساعات فأكثر) بنسبة 12.7%، في حين أظهرت نتائج الدراسة أن نسبة 8.8% من المبحوثين يستخدمون مواقع التواصل الاجتماعي (أقل من ساعة يومياً) وفي الترتيب الخامس والأخير(لايستخدمه بشكل يومي).

ومن ثم يتضح ان 5.2% فقط من عينة الدراسة الذين لا يستخدمون مواقع التواصل الاجتماعي بشكل يومي، وأن 94.6% يستخدمون مواقع التواصل الاجتماعي بشكل يومي بمعدلات زمنية مختلفة، وهو ما يؤكد جاذبية تلك المواقع لمستخدميها والتي تحولت إلى عادات يومية لا يمكن الاستغناء عنها كما انها تستخدم لاشباع حاجات مختلفة ومتباينة لديهم.

واتفقت هذه النتيجة مع دراسة **(أمين، 2016)** والتي أكدت أن 96% من المبحوثين يستخدمون مواقع التواصل الاجتماعي بشكل يومي.كما اتفقت مع دراسة **(نصر،2022)** في

المدة التي يقضيها الجمهور المصري في استخدام الانترنت والتي تمثلت في استخدمهم لاكثر من 3 ساعات يوميا في الترتيب الاول.

4- مصادر معرفة المبحوثين بتقنية التزييف العميق:

جدول (8)مصادر معرفة المبحوثين بتقنية التزييف العميق

مصادر التعرف على تقنية الديب فييك	ك	%
صفحات وسائل التواصل الاجتماعي	280	46.7
التعريف الموجود اعلى هذه الاستمارة	134	22.3
مواقع صحفية	99	16.5
برامج التليفزيون	34	5.7
المعارف والأصدقاء	24	4.0
الصحف الورقية	18	3.0
الكتب	11	1.8
الاجمالي	600	100

يوضح الجدول السابق مصادر معرفة المبحوثين بتقنية الديب فييالتزييف العميق ك والتي جاءت في مقدمتها (صفحات وسائل التواصل الاجتماعي) في الترتيب الأول بنسبة 46.7%، وجاء في الترتيب الثاني (التعريف الموجود اعلى استمارة الاستبيان) بنسبة 22.3%، اما الترتيب الثالث فأرجعه المبحوثون الي (المواقع الصحفية) بنسبة 16.5%، وفي الترتيب الرابع (برامج التليفزيون) بنسبة 5.7%، يليه في الترتيب الخامس (المعارف والأصدقاء) بنسبة 4%، ثم (الصحف الورقية) بنسبة 3% والتي مثلت الترتيب السادس، بينما جاء في الترتيب السابع والأخير (الكتب) بنسبة 1.8%.

ومما سبق يمكن الاشارة الي أن نسبة 78.7% من المبحوثين كان لديهم معرفة مسبقة بمصطلح (التزييف العميق)، في حين أن 22.3% فقط لم يكن لديهم معرفة مسبقة بمصطلح التزييف العميق قبل التعرض للتعريف الذي ارفقه الباحثان بإستمارة الاستبيان.

ويمكن تفسير هذه النتيجة بالانتشار الواسع لنشر موضوع التزييف العميق عقب بعض الحوادث التي شهدها المجتمع المصري وعلى رأسها قضية بسنت خالد ضحية الديب فييك والتي تصدرت هاشتاج بسنت خالد المعروفة بـ«فتاة الغربية ضحية الابتزاز» بعدما أقدمت على الانتحار بعد قيام متهمين من شباب قريتها بفبركة صور مسيئة لها الأمر الذي أطلق نداء من الخبراء والمتخصصين في كيفية حماية الأسر من الجرائم الإلكترونية، وبعد تداول الموضوع اعلاميا، بالاضافة لانتشار فيديوهات بتقنية الديب فييك لشخصيات عالمية مثل مارك زوكربيرج مؤسس فيسبوك وأوباما الرئيس الأسبق للولايات المتحدة و الممثل توم كروز، مما جعل مصطلح الديب فييك (التزييف العميق) متداول على وسائل الإعلام وخاصة مواقع التواصل الاجتماعي منذ عام 2019.

5- ثقة المبحوثين في قدرتهم على كشف التزييف العميق في حالة التعرض لأي فيديو مزييف (الثقة المزيفة):

جدول (9)مستوى ثقة المبحوثين في قدرتهم على كشف الديب فييالتزييف العميق في حالة التعرض لأي فيديو مزييف (الثقة المزيفة)

مستوى الثقة المزيفة	ك	%
اثق تماما في قدرتي على كشف التزييف العميق	308	51.3
أثق إلى حد ما في قدرتي على كشف التزيف العميق	201	33.5
لا اثق مطلقا في قدرتي على كشف التزييف العميق	91	15.2
الاجمالي	600	100

يتضح من الجدول السابق: أن جاء مستوى (الثقة المزيفة) ثقة المبحوثين في قدرتهم على التزييف العميق في حالة التعرض لأي فيديو مزييف في الترتيب الأول (أثق تماماً في قدرتي على كشف الديب فييك) بنسبة 51.3%، ثم في الترتيب الثاني (أثق إلى حد ما في قدرتي على كشف الديب فييك) بنسبة 33.5%، وفي الترتيب الثالث والأخير (لا أثق مطلقاً في قدرتي على كشف الديب فييك) بنسبة 15.2%.

واتفقت هذه النتائج مع دراسة **(Köbis ; Doležalová, 2021)** والتي أثبتت أن المبحوثين يبالغون في معتقداتهم حول قدراتهم على كشف التزييف العميق (الثقة المزيفة)، كما أثبتت وجود علاقة إرتباطية عكسية بين مستوى الثقة المزيفة وبين مستوى الدقة في كشف المبحوثين لمقاطع الفيديو المزيفة بتقنية التزييف العميق عند مستوى دلالة 0.01.

6- مقياس إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق:

جدول (10) مقياس إدراك تهديدات التزييف العميق

مستوى إدراك تهديدات التزييف العميق	ك	%
منخفض	329	54.8
متوسط	167	27.8
مرتفع	104	17.3
الاجمالي	600	100

يشير الجدول السابق: الي انخفاض مستوي ادراك المبحوثين لتهديدات الديب فيك حيث جاء مستوي الادراك (منخفض) بنسبة 54.8%،وفي الترتيب الثاني جاء (متوسط) بنسبة 27.8%، وفي الترتيب الثالث والأخيرجاء المستوي (مرتفع) بنسبة 17.3%.

تؤكد نتائج الجدول على الإدراك المنخفض لتهديدات التزييف العميق والذي يمكن إسناده إلى عوامل عده منها حداثة تقنية الديب فييك كاحد روافد الذكاء الاصطناعي، وغياب حملات التوعية تجاه تلك التقنية الخطيرة

جدول (11) التكرارات والنسب المئوية لاستجابات أفراد العينة على عبارات مقياس إدراك تهديدات التزييف العميق (ن = 600)

م	العبارة	نعم		أحياناً		لا	
		ك	%	ك	%	ك	%
البعد الأول: تهديدات التزييف العميق على مستوى الفرد							
1	تستخدم تقنية الديب فيك غالباً بقصد إفساد حياة الأفراد	93	15.5	200	33.3	307	51.2
2	يستطيع الشخص العادي من خلال تطبيقات الديب فيك انتاج فيديو اباحي مزيف يبدو واقعياً بهدف الانتقام من شخص ما	89	14.8	198	33.0	313	52.2
3	تتيح تقنية الديب فيك فرصة للمجرمين لإبتزاز الفرد مادياً	125	20.8	182	30.3	293	48.8
4	قد يساوم مستخدم تقنية الديب فيك احد الأشخاص للقيام بأعمال جنسية تحت التهديد	87	14.5	201	33.5	312	52.0
5	تساعد تقنية الديب فيك في السخرية من فرد ما وايذائه على المستوى المعنوي	203	33.8	173	28.8	224	37.3
6	تؤدي تقنية الديب فيك إلى انتحال شخصية أحد الأفراد بواقعية لا استطيع اكتشافها	136	22.7	166	27.7	298	49.7
7	تهديدات الديب فيك محدودة النطاق لان استغلال تقنية الديب فيك قاصره على عدد قليل من المحترفين وليس المستخدم العادي	341	56.8	169	28.2	90	15.0
8	تستطيع الأفراد حالياً التمييز بين الفيديو الحقيقي والمزيف من خلال ملاحظة بعض العيوب مثل حركة العينين مما يقلل من تهديد الديب فيك	294	49.0	171	28.5	135	22.5
9	يؤدي الاستخدام السيئ لتقنية الديب فيك لانتحار بعض الضحايا	171	28.5	93	15.5	336	56.0
10	لدى تقنية الديب فيك القدرة على تشويه السمعه من خلال جعل الفرد يقول أو يفعل أشياء لم يقوم بها في الواقع	100	16.7	169	28.2	331	55.2
11	لا تتوفر لدى المتخصصين والخبراء طريقة موثوقة لكشف التزييف بتقنية الديب فيك حتى الأن	63	10.5	166	27.7	371	61.8
البعد الثاني: تهديدات التزييف العميق على مستوى المجتمع							
12	تساهم مقاطع الديب فيك في إثارة الفوضى وحدوث الإضطرابات والارتباك وحالات الزعر والخوف داخل المجتمعات بتمرير محتويات مزيفة	91	15.2	198	33.0	311	51.8
13	تؤثر تقنية الديب فيك على نزاهة العملية الانتخابية والعملية الديمقراطية	127	21.2	167	27.8	306	51.0
14	تهدد تقنية الديب فيك الأمن القومي للدول من خلال قدرتها على نشر معلومات وتصريحات مزيفة تبدو واقعية	90	15.0	195	32.5	315	52.5
15	تستطيع تقنية الديب فيك تشويه الرموز المجتمعية والسياسية من خلال فيديوهات مفبركة	132	22.0	159	26.5	309	51.5
16	استخدمت تقنية الديب فيك في العمليات الاحتيالية على الشركات التجارية بتقليد صوت شخص ما بغرض تحويل أموال	79	13.2	207	34.5	314	52.3
17	قد تؤدي تقنية الديب فيك لاختلاق الأزمات الدبلوماسية بين الدول	89	14.8	174	29.0	337	56.2
18	نتيجة وجود تقنية الديب فيك أصبح أي فيديو منشور بمواقع التواصل الاجتماعي غير موثوق به	74	12.3	215	35.8	311	51.8

يتضح من الجدول السابق من خلال استجابات أفراد العينة على **البعد الأول** (تهديدات التزييف العميق على مستوى الفرد) من مقياس إدراك تهديدات التزييف العميق : أن(15.5%) فقط من المبحوثين يرون أن تقنية الديب فيك تستخدم غالباً بقصد إفساد حياة الأفراد، كما يرى (14.8%) من المبحوثين أن الشخص العادي غير المحترف يستطيع من خلال تطبيقات الديب فيك انتاج فيديو اباحي مزيف يبدو واقعياً بهدف الانتقام من شخص ما، وأظهرت النتائج أن (20.8%) من المبحوثين مدركون قدرة تقنية الديب فيك في إتاحه فرصة للمجرمين لإبتزاز الفرد مادياً، وتشير النتائج أن (14.5%) فقط من المبحوثين مدركون لاحتمال وقوع مساومة من مستخدمي تقنية الديب فيك للقيام بأعمال جنسية تحت التهديد، كما أكد (33.8%) من المبحوثين أن تقنية الديب فيك تساعد في السخرية من الأفراد وايذائهم على المستوى المعنوي. وأظهرت النتائج أيضاً أن (22.7%) فقط من المبحوثين مدركون قدرة تقنية الديب فيك على انتحال شخصية أحد الأفراد بواقعية لا يمكن اكتشافها، في حين أن (56.8%) من المبحوثين أكدوا أن تهديدات الديب فيك محدودة النطاق بداعي أن استغلال تقنية الديب فيك قاصره على عدد قليل من المحترفين وليس المستخدم العادي، كما يرى أيضاً (49%) من المبحوثين إمكانية التمييز بين الفيديو الحقيقي والمزيف من خلال ملاحظة بعض العيوب مثل حركة العينين مما يقلل من تهديد الديب فيك من وجهة نظرهم،، كما أظهرت النتائج أن (28.5%) فقط من المبحوثين مدركون الأثار النفسية التي تصل لانتحار بعض الضحايا نتيجه الاستخدام السيئ لتقنية الديب فيك، كما أظهرت النتائج أن (16.7%) فقط من المبحوثين أكدوا أن تقنية الديب فيك قادرة على تشويه السمعه من خلال جعل الفرد يقول أو يفعل أشياء لم يقوم بها في الواقع،، كما تشير النتائج أن (10.5%) فقط من المبحوثين مدركون عدم توافر طريقة موثوقة لكشف التزييف بتقنية الديب فيك لدى المتخصصين والخبراء حتى الأن.

كما يتضح من الجدول السابق من خلال استجابات أفراد العينة على **البعد الثاني** (تهديدات الديب فيك على مستوى المجتمع) من مقياس إدراك تهديدات الديب فيك : أن (15.2%) فقط من المبحوثين يرون أن مقاطع الديب فيك تساهم في إثارة الفوضى وحدوث الإضطرابات والارتباك وحالات الزعر والخوف داخل المجتمعات بتمرير محتويات مزيفة، كما يرى (21.2%) من المبحوثين أن تقنية الديب فيك تؤثر على نزاهة العملية الانتخابية والعملية الديمقراطية، وأظهرت النتائج أن (15%) من المبحوثين فقط مدركون قدرة تقنية الديب فيك على تهديد الأمن القومي للدول من خلال نشر معلومات وتصريحات مزيفة تبدو واقعية، كما تشير النتائج أن (22%) من المبحوثين أكدوا أن تقنية الديب فيك تسطيع تشويه الرموز المجتمعية والسياسية من خلال فيديوهات مفبركة، كما أكد (13.2%) من المبحوثين أن تقنية الديب فيك تم استخدمها سابقاً في عمليات احتيالية على الشركات التجارية بتقليد صوت شخص ما بغرض تحويل أموال. وأظهرت النتائج أيضاً أن (14.8%) فقط من المبحوثين مدركون قدرة تقنية الديب فيك على اختلاق الأزمات الدبلوماسية بين الدول، في حين أن (12.3%) من المبحوثين أقروا أن وجود تقنية الديب فيك ادى لإنعدام الثقة في أي فيديو منشور بمواقع التواصل الاجتماعي.

7- مقياس الاستخدام الأمن لمواقع التواصل الاجتماعي:

جدول (12) مقياس الاستخدام الأمن لمواقع التواصل الاجتماعي

مستوى الاستخدام الأمن لمواقع التواصل الاجتماعي	ك	%
منخفض	293	48.8
متوسط	192	32.0
مرتفع	115	19.2
الاجمالي	600	100

يتضح من الجدول السابق: أن جاء مستوى الاستخدام الأمن لمواقع التواصل الاجتماعي لدى المبحوثين (منخفض) في الترتيب الأول بنسبة 48.8%، ثم في الترتيب الثاني (متوسط) بنسبة 32%، وفي الترتيب الثالث والأخير (مرتفع) بنسبة 19.2%.

وتثبت نتائج الجدول إنخفاض مستوى الاستخدام الأمن لمواقع التواصل الاجتماعي لدى المبحوثين، رغم تأكيد بعض الدراسات على ارتفاع مستوى الوعي بأمن وخصوصية المعلومات الرقمية والأمن السيبراني مثل دراسة **(العجلاني،2020)** ودراسة **(صائغ،2018)** ودراسة **(عبد الهادي، 2021)** والذي يمكن تفسيره بأن ترجمة الوعي لممارسة فعلية يحتاج إلى إدراك حقيقي للمخاطر والتهديدات وإدراك حقيقة أن أي فرد ليس بعيد عن دائرة الخطورة.

جدول (13) التكرارات والنسب المئوية لاستجابات أفراد العينة على عبارات مقياس الاستخدام الأمن لمواقع التواصل الاجتماعي (ن = 600)

م	العبارة	نعم		أحياناً		لا	
		ك	%	ك	%	ك	%
1	احرص على تركيب كلمات السر بشكل معقد لدى حساباتي بمواقع التواصل الاجتماعي أي ان تتكون من حروف ورموز وأرقام بشكل مختلط	159	26.5	180	30.0	261	43.5
2	استعمل كلمات سر مختلفة في كل موقع من مواقع التواصل الاجتماعي	87	14.5	199	33.2	314	52.3
3	اقوم بالخروج من الحساب بعد الإنتهاء من استخدام شبكات التواصل االجتماعي	113	18.8	207	34.5	280	46.7
4	احرص على حماية الهاتف الذكي بواسطة رمز سري لمنع استعماله من طرف الاغراب	433	72.2	59	34.0	108	18.0
5	اتجنب وضع المعلومات الشخصية والعائلية على مواقع التواصل االجتماعي	169	28.2	167	27.8	264	44.0
6	اتجنب الدخول على الروابط والصفحات والمحتويات من المصادر غير المعلومة	150	25.0	181	30.2	269	44.8
7	اقوم بإلغاء ربط الحسابات الشخصية بمحركات البحث إذا سمحت مواقع التواصل بذلك	12	2.0	177	29.5	403	67.1
8	اتجنب نشر الصور والفيديوهات الشخصية والعائلية على مواقع التواصل الاجتماعي وخاصة في حالة النظر مباشرة للكاميرا	164	27.3	179	29.8	257	42.8

9	اراجع بنود التراخيص المطلوبة من التطبيقات قبل تثبيتها على الأجهزة الذكية لأن بعضها يستخدم المعلومات الشخصية وذلك بموافقه من المستخدم نفسه	17	2.8	201	33.5	382	63.7
10	اتجنب قبول دعوات الصداقة على مواقع التواصل الاجتماعي إلا من الأشخاص الذين أعرفهم شخصياً	180	30.0	179	29.8	241	40.2
11	أتأكد باستمرار من إعدادات السرية الخاصة بالمعلومات الشخصية على مواقع التواصل االجتماعي	116	19.3	194	32.3	290	48.3
12	احرص على الإلمام بقوانين الملكية الفكرية المتعلقة بحماية المحتوى الخاص بي على مواقع التواصل الاجتماعي	23	3.8	150	25.0	427	71.2
13	اتجاهل الرسائل التي تطلب مني بياناتي الشخصية على مواقع التواصل الاجتماعي	383	63.8	176	29.3	41	6.8
14	اعرف أن المحتوى الذي أحذفه من مواقع التواصل الاجتماعي يظل ضمن النسخ الاحتياطية لفترة محدودة سواء صور او فيديوهات او غيرها	78	13.0	224	37.3	298	49.7
15	اقوم بتفعيل قفل الحساب لغير الأصدقاء (وضع lock) على مواقع التواصل الاجتماعي التي تتيح تلك الخاصية	99	16.5	221	36.8	280	46.7

يتضح من الجدول السابق من خلال استجابات أفراد العينة على مقياس الاستخدام الأمن لمواقع التواصل الاجتماعي: أن(26.5%) فقط من المبحوثين يحرصون على تركيب كلمات السر بشكل معقد لدى حساباتهم بمواقع التواصل الاجتماعي أي ان تتكون من حروف ورموز وأرقام بشكل مختلط، كما أكد (14.5%) فقط من المبحوثين أنهم يستخدمون كلمات سر مختلفة في كل موقع من مواقع التواصل الاجتماعي، وأظهرت النتائج أن (18.8%) من المبحوثين يحرصون على تسجيل الخروج من الحساب بعد الإنتهاء من استخدام شبكات التواصل االجتماعي، بينما تشير النتائج أن (72.2%) من المبحوثين أكدوا تفعيل حماية الهاتف الذكي بواسطة رمز سري لمنع استعماله من طرف الاغراب، كما تشير النتائج أن (28.2%) من المبحوثين يتجنبوا وضع المعلومات الشخصية والعائلية على مواقع التواصل الاجتماعي تماماً، كما يتجنب (27.3%) من المبحوثين نشر الصور والفيديوهات الشخصية والعائلية على مواقع التواصل الاجتماعي وخاصة في حالة النظر مباشرة للكاميرا، كما يتجنب أيضاً (25%) من المبحوثين الدخول على الروابط والصفحات والمحتويات من المصادر غير المعلومة، في حين أن (2%) فقط من المبحوثين أكدوا قيامهم بإلغاء ربط الحسابات الشخصية بمحركات البحث في مواقع التواصل التي تسمح بذلك، كما أظهرت النتائج أن (2.8%) فقط من المبحوثين يراجعون بنود التراخيص المطلوبة من التطبيقات قبل تثبيتها على الأجهزة الذكية لأن بعضها يستخدم المعلومات الشخصية وذلك بموافقه من المستخدم نفسه، كما أظهرت النتائج أيضاً أن (3.8%) فقط من المبحوثين أكدوا حرصهم على الإلمام بقوانين الملكية الفكرية المتعلقة بحماية المحتوى الخاص بهم على مواقع التواصل الاجتماعي، كما تشير النتائج أن (30%) من المبحوثين يمتنعون تماماً عن قبول دعوات الصداقة على مواقع التواصل الاجتماعي إلا من الأشخاص الذين يعرفونهم بشكل شخصي، كما تشير النتائج أن (19.3%) من المبحوثين تتأكد باستمرار من إعدادات السرية

الخاصة بالمعلومات الشخصية على مواقع التواصل الاجتماعي، بينما تشير النتائج أن (63.8%) من المبحوثين يتجاهلون الرسائل التي تطلب بياناتهم الشخصية على مواقع التواصل الاجتماعي تماماً، وأظهرت النتائج أيضاً أن (13%) فقط من المبحوثين يعرفون أن المحتويات المحذوفة من مواقع التواصل الاجتماعي تظل ضمن النسخ الاحتياطية لفترة محدودة سواء صور او فيديوهات او غيرها، كما أكد (16.5%) فقط من المبحوثين على قيامهم بتفعيل قفل الحساب لغير الأصدقاء (وضع lock) على مواقع التواصل الاجتماعي التي تتيح تلك الخاصية.

من نتائج الجدوليين السابقين يتضح اننا في حاجة ملحة لاستخدام حملات توعوية توضح ضرورة الاستخدام الآمن لمواقع التواصل الاجتماعي لاسيما بعد ظهور تلك النتائج التي توضح انخفاض مستوي الاستخدام الامن لدي نسبة تتقارب من نصف عينة المبحوثين.

نتائج الفروض:

1- توجد علاقة إرتباطية طردية ذات دلالة إحصائية بين مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وبين مستوى استخدامهم الأمن لتلك المواقع.

وللتحقق من صحة هذا الفرض تم حساب معامل ارتباط بيرسون لقياس العلاقة بين مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات الديب فيك وبين مستوى استخدامهم الأمن لتلك المواقع، وذلك كما يلي:

جدول (14) نتائج اختبار بيرسون لقياس العلاقة بين مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وبين مستوى استخدامهم الأمن لتلك المواقع

المتغيرات	مستوى الاستخدام الأمن	
	معامل الارتباط	الدلالة
مستوى إدراك تهديدات التزييف العميق	.799**	0.01

يتبين من الجدول السابق: وجود علاقة ارتباطية طردية قوية ذات دلالة إحصائية بين مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وبين مستوى استخدامهم الأمن لتلك المواقع حيث بلغة قيمة ر(.799**) وهي قيمة دالة إحصائياً عند مستوي دلالة (0.01).

وبذلك يتم قبول **صحة الفرض الأول** حيث وجود علاقة ارتباطية طردية ذات دلالة إحصائية بين مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وبين مستوى استخدامهم الأمن لتلك المواقع.

وتتفق هذه النتيجة مع ما توصلت اليه دراسة **(عبد المحسن:2010)** من ان وسائل التواصل الاجتماعي افرزت اشكال جديدة من الجرائم والتهديد والتشهير بالاخرين نتيجة تخلي مستخدمي مواقع التواصل الاجتماعي عن الحذر اللازم وسهولة الحصول علي بياناتهم الشخصية،كما أكدت دراسة **(Prandi; Furini, 2020)** ان سلوكيات المستخدمين الرَّقمية للتطبيقات دونَّ دراية بمعايير الحماية الرَّقمية لبياناتهم البيومترية؛ حيث يقوم

المستخدمون بتثبيت التطبيقات في أغلب الاوقات دون قراءة شروط وأحكام الاستخدام؛ والنتيجة هي أن خصوصياتهم في خطر متزايد

ومما سبق يمكن ان نستنتج ان كلما ادرك الفرد خطورة وامكانية تعرضه لتهديدات ومخاطر كلما اتخذ اجراءات حماية تمكنه من استخدام امان لمواقع التواصل الاجتماعي كاجراء وقائي لحماية نفسه من هذه التهديدات.

2. توجد علاقة إرتباطية عكسية ذات دلالة إحصائية بين مستوى ثقة مستخدمي مواقع التواصل الاجتماعي في قدرتهم على كشف التزييف العميق (الثقة المزيفة) وبين مستوى استخدامهم الأمن لتلك المواقع.

وللتحقق من صحة هذا الفرض تم حساب معامل ارتباط بيرسون لقياس العلاقة بين مستوى ثقة مستخدمي مواقع التواصل الاجتماعي في قدرتهم على كشف التزييف العميق (الثقة المزيفة) وبين مستوى استخدامهم الأمن لتلك المواقع، وذلك كما يلي:

جدول (15) نتائج اختبار بيرسون لقياس العلاقة بين مستوى ثقة مستخدمي مواقع التواصل الاجتماعي في قدرتهم على كشف التزييف العميق (الثقة المزيفة) وبين مستوى استخدامهم الأمن لتلك المواقع

المتغيرات	مستوى الاستخدام الأمن	
	معامل الارتباط	الدلالة
مستوى الثقة المزيفة	-.725**	0.01

يتبين من الجدول السابق: وجود علاقة ارتباطية عكسية قوية ذات دلالة إحصائية بين مستوى ثقة مستخدمي مواقع التواصل الاجتماعي في قدرتهم على كشف التزييف العميق (الثقة المزيفة) وبين مستوى استخدامهم الأمن لتلك المواقع حيث بلغة قيمة ر(-.725**) وهي قيمة دالة إحصائياً عند مستوي دلالة (0.01).

وبذلك يتم قبول **صحة الفرض الثاني** حيث وجود علاقة ارتباطية عكسية ذات دلالة إحصائية بين مستوى ثقة مستخدمي مواقع التواصل الاجتماعي في قدرتهم على كشف التزييف العميق (الثقة المزيفة) وبين مستوى استخدامهم الأمن لتلك المواقع.

اي ان الافراد كلما ارتفعت لديهم ثقتهم في قدراتهم علي كشف التزييف العميق اذا ما شاهدوا احدي هذه الصور والفيديوهات المفبركة كلما قل اهتمامهم بالاستخدام الامن وتأمين حساباتهم الشخصية ونشر صورهم الشخصية وملفاتهم دون تأمين كافي.

3. الفرض الثالث: توجد فروق ذات دلالة إحصائية في مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وفقاً للمتغيرات الديمجرافية (النطاق الجغرافي – النوع – العمر – المستوى التعليمي).

- أولاً / وفقاً للنطاق الجغرافي

تم تطبيق اختبار تحليل التباين الأحادي (ANOVA) لدلالة في مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وفقاً للنطاق الجغرافي

جدول (16) نتائج اختبار تحليل التباين الأحادي (ANOVA) لدلالة الفروق في مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وفقاً للنطاق الجغرافي

مصدر التباين	مجموعات المربعات	درجة الحرية	متوسط المربعات	قيمة ف	الدلالة
بين المجموعات	29.552	3	9.851	18.400	0.05
داخل المجموعات	319.073	596	.535		
المجموع	348.625	599			

تشير نتائج تطبيق اختبار تحليل التباين الأحادي (ANOVA) إلي وجود فروق دالة احصائياً في مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وفقاً للنطاق الجغرافي ((القاهرة: العاصمة)، (بورسعيد: تمثيلاً لوجه بحري واقليم القناة)، (الدقهلية: تمثيلاً لريف مصر)، (أسيوط: تمثيلاً لصعيد مصر))، حيث بلغت قيمة ف 18.400 وهي قيمة دالة احصائياً عند مستوي دلالة (0.05)، ولمعرفة اتجاه الفروق تم تطبيق اختبار Scheffe وكانت الفروق لصالح محافظتي (القاهرة) و (بورسعيد).

ويمكن تفسير هذه النتيجة الي ميل العواصم والمدن بمتابعة المستجدات العلمية والتكنولوجية وانتشار المعرفة التكنولوجية والاطلاع علي كل تطور في مجال التقنيات الالكترونية بشكل يتفوق علي الريف بطبيعتة المحافظة.

- ثانياً / وفقاً للنوع

تم تطبيق اختبار "ت" لقياس الفروق في مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وفقاً للنوع، وذلك كما يلي:

جدول (17) نتائج اختبار (ت) لدلالة الفروق في مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وفقاً للنوع

النوع / المتغير	ذكور			إناث			قيمة (ت)	درجة الحرية	مستوى الدلالة
	العدد	المتوسط	الانحراف المعياري	العدد	المتوسط	الانحراف المعياري			
مستوى إدراك تهديدات الديب فيك	271	1.4908	.68239	329	1.7356	.80773	3.959	598	0.01

تشير نتائج تطبيق اختبار "ت": إلي وجود فروق دالة إحصائياً في مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وفقاً للنوع، حيث بلغت قيمة "ت"(3.959)، وهي قيمة دالة إحصائياً عند مستوي دلالة (0.01)، كما تشير النتائج لاتجاه الفروق لصالح الإناث.

وقد يرجع السبب في هذه النتيجة الي ان الاناث من اكثر الفئات تعرضا لتهديات التزييف العميق ولاسيما الابتزاز الالكتروني وقد سجلت الفترة السابقة لاجراء البحث عدة قضايا كانت ضحيتها اناث وفتيات قاموا بالانتحار هروبا من نظرة المجتمع وتصديقه لهذه الفيديوهات المفبركة والتي لم يستطع الافراد العاديين كشفها.

- **ثالثاً / وفقاً للعمر**

تم تطبيق اختبار "ت" لقياس الفروق في مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وفقاً للعمر، وذلك كما يلي:

جدول (18) نتائج اختبار تحليل التباين الأحادي (ANOVA) لدلالة الفروق في مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وفقاً للعمر

مصدر التباين	مجموعات المربعات	درجة الحرية	متوسط المربعات	قيمة ف	الدلالة
بين المجموعات	.959	4	.240	.410	غير دالة
داخل المجموعات	347.666	595	.584		
المجموع	348.625	599			

تشير نتائج تطبيق اختبار تحليل التباين الأحادي (ANOVA) إلي عدم وجود فروق دالة احصائياً في مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وفقاً للعمر ((31: 40) سنة، (21: 30) سنة، (20 فأقل) سنة، (41: 50) سنة، (أكثر من 50))، حيث بلغت قيمة ف.410 وهي قيمة غير دالة احصائياً عند مستوي دلالة (0.05).

ويمكن ارجاع السبب في عدم وجود فروق في ادراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وفقا للعمر الي نظرحداثة التقنية والتي تتطلب مزيد من الجهود الاعلامية لالقاء الضوء علي مخاطرها لكل فئات المجتمع.

- **رابعاً / وفقاً للمستوى التعليمي**

تم تطبيق اختبار تحليل التباين الأحادي (ANOVA) لدلالة في مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وفقاً للمستوى التعليمي

جدول (19) نتائج اختبار تحليل التباين الأحادي (ANOVA) لدلالة الفروق في مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وفقاً للمستوى التعليمي

مصدر التباين	مجموعات المربعات	درجة الحرية	متوسط المربعات	قيمة ف	الدلالة
بين المجموعات	37.054	5	7.411	14.128	0.05
داخل المجموعات	311.571	594	.525		
المجموع	348.625	599			

تشير نتائج تطبيق اختبار تحليل التباين الأحادي (ANOVA) إلي وجود فروق دالة احصائياً في مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وفقاً للمستوى التعليمي ((طلاب المدارس – طلاب الجامعات – دبلوم – بكالوريوس – ماجستير – دكتوراه))، حيث بلغت قيمة ف 14.128 وهي قيمة دالة احصائياً عند مستوي دلالة (0.05)، ولمعرفة اتجاه الفروق تم تطبيق اختبار Scheffe وكانت الفروق لصالح (الماجستير) و (الدكتوراه).

وقد يمكن تفسير هذه النتيجة في اطار المام حملة الماجيستير والدكتوراه بمستجدات التطور التكنولوجي وفقا لطبيعة دراستهم التي غالبا ما تواكب مستحدثات العصر.

وبذلك يتم قبول **صحة الفرض الثالث جزئياً** كالتالي توجد فروق ذات دلالة إحصائية في مستوى إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق وفقاً للمتغيرات الديمجرافية (النطاق الجغرافي – النوع – المستوى التعليمي).

4. الفرض الرابع: توجد فروق ذات دلالة إحصائية في مستوى الاستخدام الأمن لمستخدمي مواقع التواصل الاجتماعي وفقاً للمتغيرات الديمجرافية (النطاق الجغرافي- النوع – العمر.– المستوى التعليمي).

- **أولاً / وفقاً للنطاق الجغرافي**

تم تطبيق اختبار تحليل التباين الأحادي (ANOVA) لدلالة في مستوى الاستخدام الأمن لمستخدمي مواقع التواصل الاجتماعي وفقاً للنطاق الجغرافي

جدول (20) نتائج اختبار تحليل التباين الأحادي (ANOVA) لدلالة الفروق في مستوى الاستخدام الأمن لمستخدمي مواقع التواصل الاجتماعي وفقاً للنطاق الجغرافي

مصدر التباين	مجموعات المربعات	درجة الحرية	متوسط المربعات	قيمة ف	الدلالة
بين المجموعات	43.527	3	14.509	27.745	0.05
داخل المجموعات	311.667	596	.523		
المجموع	355.193	599			

تشير نتائج تطبيق اختبار تحليل التباين الأحادي (ANOVA) إلي وجود فروق دالة احصائياً في مستوى الاستخدام الأمن لمستخدمي مواقع التواصل الاجتماعي وفقاً للنطاق الجغرافي ((القاهرة: العاصمة)، (بورسعيد: تمثيلاً لوجه بحري واقليم القناة)، (الدقهلية: تمثيلاً لريف مصر)، (أسيوط: تمثيلاً لصعيد مصر))، حيث بلغت قيمة ف 27.745 وهي قيمة دالة احصائياً عند مستوي دلالة (0.05)، ولمعرفة اتجاه الفروق تم تطبيق اختبار Scheffe وكانت الفروق لصالح محافظتي (القاهرة) و (بورسعيد).

- **ثانياً / وفقاً للنوع**

تم تطبيق اختبار "ت" لقياس الفروق في مستوى الاستخدام الأمن لمستخدمي مواقع التواصل الاجتماعي وفقاً للنوع، وذلك كما يلي:

جدول (21) نتائج اختبار (ت) لدلالة الفروق في مستوى الاستخدام الأمن لمستخدمي مواقع التواصل الاجتماعي وفقاً للنوع

النوع / المتغير	ذكور			إناث			قيمة (ت)	درجة الحرية	مستوى الدلالة
	العدد	المتوسط	الانحراف المعياري	العدد	المتوسط	الانحراف المعياري			
مستوي الاستخدام الامن	271	1.5018	.68245	329	1.8693	.79897	5.984	598	0.01

تشير نتائج تطبيق اختبار "ت": إلي وجود فروق دالة إحصائياً في مستوى الاستخدام الأمن لمستخدمي مواقع التواصل الاجتماعي وفقاً للنوع، حيث بلغت قيمة "ت"(5.984)، وهي قيمة دالة إحصائياً عند مستوي دلالة (0.01)، كما تشير النتائج لاتجاه الفروق لصالح الإناث.

ويمكن تفسيره في ان الاناث اكثر وعيا بالاستخدام الآمن واعتباره اجراء وقائي يحد من مخاوفها وقلقها من انتهاك بياناتها الخاصة واستخدامها في اغراض غير مرغوبة تعرضها للايذاء من قبل الاخرين.

وتتفق هذه النتيجة مع ماتوصلت اليه دراسة(Pearce;Vitak,2016) والتي أكدت علي ان النساء اكثر حرصا في التحكم في حساباتها علي مواقع التواصل الاجتماعي لتفادي الوقوع فيما يتعارض مع ثقافة المجتمع، ودراسة (Alsaggaf,2016) والتي توضح ان مستخدمات الفيس بوك يبدين قلقا من اختراق حساباتهم فمنهن من لا ينشر صور ومنهن من يتحكم في اعدادت الأمان كسلوك وقائي.

- **ثالثاً / وفقاً للعمر**

تم تطبيق اختبار "ت" لقياس الفروق في مستوى الاستخدام الأمن لمستخدمي مواقع التواصل الاجتماعي وفقاً للعمر، وذلك كما يلي:

جدول (22) نتائج اختبار تحليل التباين الأحادي (ANOVA) لدلالة الفروق في مستوى الاستخدام الأمن لمستخدمي مواقع التواصل الاجتماعي وفقاً للعمر

مصدر التباين	مجموعات المربعات	درجة الحرية	متوسط المربعات	قيمة ف	الدلالة
بين المجموعات	.771	4	.193	.324	غير دالة
داخل المجموعات	354.422	595	.596		
المجموع	355.193	599			

تشير نتائج تطبيق اختبار تحليل التباين الأحادي (ANOVA) إلي عدم وجود فروق دالة احصائياً في مستوى الاستخدام الأمن لمستخدمي مواقع التواصل الاجتماعي وفقاً للعمر ((31: 40) سنة، (21: 30) سنة، (20 فأقل) سنة، (41: 50) سنة، (أكثر من 50))، حيث بلغت قيمة ف.324 وهي قيمة غير دالة احصائياً عند مستوي دلالة (0.05).

- **رابعاً / وفقاً للمستوى التعليمي**

تم تطبيق اختبار تحليل التباين الأحادي (ANOVA) لدلالة في مستوى الاستخدام الأمن لمستخدمي مواقع التواصل الاجتماعي وفقاً للمستوى التعليمي

جدول (23) نتائج اختبار تحليل التباين الأحادي (ANOVA) لدلالة الفروق في مستوى الاستخدام الأمن لمستخدمي مواقع التواصل الاجتماعي وفقاً للمستوى التعليمي

مصدر التباين	مجموعات المربعات	درجة الحرية	متوسط المربعات	قيمة ف	الدلالة
بين المجموعات	18.010	5	3.602	6.346	0.05
داخل المجموعات	337.183	594	.568		
المجموع	355.193	599			

تشير نتائج تطبيق اختبار تحليل التباين الأحادي (ANOVA) إلي وجود فروق دالة احصائياً في مستوى الاستخدام الأمن لمستخدمي مواقع التواصل الاجتماعي وفقاً للمستوى التعليمي ((طلاب المدارس – طلاب الجامعات – دبلوم – بكالوريوس – ماجستير – دكتوراه))، حيث بلغت قيمة ف 6.346 وهي قيمة دالة احصائياً عند مستوي دلالة (0.05)، ولمعرفة اتجاه الفروق تم تطبيق اختبار Scheffe وكانت الفروق لصالح (الماجستير).

وبذلك يتم قبول **صحة الفرض الرابع جزئياً** كالتالي توجد فروق ذات دلالة إحصائية في مستوى الاستخدام الأمن لمستخدمي مواقع التواصل الاجتماعي وفقاً للمتغيرات الديمجرافية (النطاق الجغرافي – النوع – المستوى التعليمي).

5. الفرض الخامس: توجد علاقة إرتباطية ذات دلالة إحصائية بين مستوى استخدام مواقع التواصل الإجتماعي وبين مستوى إدراك المستخدمين لتهديدات الديب فييك.

وللتحقق من صحة هذا الفرض تم حساب معامل ارتباط بيرسون لقياس العلاقة بين مستوى استخدام مواقع التواصل الإجتماعي وبين مستوى إدراك المستخدمين لتهديدات الديب فييك، وذلك كما يلي:

جدول (24) نتائج اختبار بيرسون لقياس العلاقة بين مستوى استخدام مواقع التواصل الإجتماعي وبين مستوى إدراك المستخدمين لتهديدات التزييف العميق

المتغيرات	مستوى إدراك تهديدات الديب فييك	
	معامل الارتباط	الدلالة
مستوى استخدام مواقع التواصل الاجتماعي	.076	غير دالة

يتبين من الجدول السابق: عدم وجود علاقة ارتباطية ذات دلالة إحصائية بين مستوى استخدام مواقع التواصل الإجتماعي وبين مستوى إدراك المستخدمين لتهديدات الديب فييك حيث بلغة قيمة ر (076.) وهي قيمة غير دالة إحصائياً عند مستوي دلالة (0.05).

وبذلك يتم **رفض صحة الفرض الخامس** حيث ثبت عدم وجود علاقة ارتباطية ذات دلالة إحصائية بين مستوى استخدام مواقع التواصل الإجتماعي وبين مستوى إدراك المستخدمين لتهديدات الديب فييك.

ملخص النتائج:

1- يتضح من الدراسة تفضيل جمهور مستخدمي مواقع التواصل الاجتماعي لموقع (فيسبوك) حيث جاء في مقدمة اختيارتهم يليه تطبيق الواتساب، وجاء استخدام تلك المواقع بشكل دائم في المرتبة الاولي وبمعدل من (3 ساعات الي 4 ساعات يوميا) كما اشارت النتائج الي تقدم صفحات مواقع التواصل الاجتماعي كمصادر لمعرفة المبحوثين بتقنية التزييف العميق وتراجع الصحف الورقية والكتب في المراتب الاخيرة كمصادر للمعرفة عن التقنية.

2- اشارت النتائج الي ارتفاع مستوي الثقة المزيفة لدي المبحوثين في قدرتهم علي كشف التزييف العميق في حالة تعرضهم لفيديو مزيف حيث انعكس ذلك علي اجاباتهم (أثق تماماً في قدرتي على كشف الديب فييك) والذي جاء في مقدمة الاختيارات وبنسبة تخطت نصف مفردات العينة، كما كشفت النتائج عن انخفاض مستوي ادراك المبحوثين لتهديدات الديب فيك حيث جاء مستوي الادراك (منخفض)،وهو ما عكسته عبارات المقياس علي البعد الخاص بتهديدات الديب فيك علي مستوي الفرد حيث أكدوا أن (تهديدات الديب فييك محدودة النطاق بداعي أن استغلال تقنية الديب فييك قاصره على عدد قليل من المحترفين وليس المستخدم العادي)،و (إمكانية التمييز بين الفيديو الحقيقي والمزيف من خلال ملاحظة بعض العيوب مثل حركة العينين) اما فيما يتعلق بالبعد الخاص بتهديدات التزييف العميق علي مستوي المجتمع، فاشارت النتائج الي (أن تقنية الديب فييك تسطيع

تشويه الرموز المجتمعية والسياسية من خلال فيديوهات مفبركة)، و (أن تقنية الديب فييك تؤثر على نزاهة العملية الانتخابية والعملية الديمقراطية).

3- اما فيما يتعلق بمستوى الاستخدام الأمن لمواقع التواصل الاجتماعي لدى المبحوثين فجاء (منخفض)، حيث انخفضت نسبة المبحوثين الذين يحرصون على تركيب كلمات السر بشكل معقد لدى حساباتهم بمواقع التواصل الاجتماعي أي ان تتكون من حروف ورموز وأرقام بشكل مختلط، ومن يستخدمون كلمات سر مختلفة في كل موقع من مواقع التواصل الاجتماعي، ومن يحرص على تسجيل الخروج من الحساب بعد الإنتهاء من استخدام شبكات التواصل الاجتماعي، ومن يتجنب وضع المعلومات الشخصية والعائلية على مواقع التواصل الاجتماعي تماماً.

التوصيات:

1- الاهتمام برفع الوعي بماهية تقنية التزيف العميق من خلال المؤسسات الاعلامية ومؤسسات المجتمع المدني والمؤسسات التربوية والتعليمية والتركيز علي مفهوم صعوبة كشف زيفها بفضل البرمجيات الحديثة التي طورت منها اذ يعتبر الوعي هو خط الدفاع الاول لمواجهة هذه التهديدات والمخاطر التي يمكن ان يتعرض لها مستخدمي مواقع التواصل الاجتماعي.

2- الاهتمام بتفعيل برامج التربية الاعلامية ووضع برامج ارشادية لكيفية الاستخدام الامن لمواقع التواصل الاجتماعي والتي من شأنها الحفاظ علي بيانات وخصوصية المستخدم

3- توجيه الرأي العام من خلال الحملات الاعلامية بضرورة التشكيك كاجراء وقائي في ما يتم عرضه عبر وسائل التواصل الاجتماعي حتي التأكد من صحته حتي لايقع الافراد ضحايا لعدم تحري المجتمع من دقةالصور و الفيديوهات التي تعرض عليه.

4- الاهتمام باتخاذ الاجراءات القانونية والتوجه للجهات الامنية لملاحقة الخارجين من مستخدمي مواقع التواصل الاجتماعي

5-وضع شركات التواصل الاجتماعي امام مسؤلياتهم المجتمعية بضرورة تمويل مشروعات بحثية للتوصل لتقنية لكشف الديب فيك.

6- المطالبة بتوفير برمجيات خاصة بمواقع التواصل الاجتماعي من شأنها الكشف عن زيف الوسائط المتعددة بتقنية الديب فيك لمنع نشرها وتمريرها عبر صفحاتها المختلفة

المراجع:

اولا: المراجع العربية:

1. الخطيب، دعاء ؛ الطاهات، خلف (2018).ادراك الجمهور الاردني لمفهوم الخصوصية علي مواقع التواصل الاجتماعي، رسالة ماجيستير غير منشورة، جامعة اليرموك، كلية الاعلام.
2. الخولي، أحمد (2021). المسئولية المدنية الناتجة عن الاستخدام غير المشروع لتطبيقات الذكاء الاصطناعي: الديب فيك نموذجا. مجلة البحوث الفقهية والقانونية، ع36, ج2.
3. الشربيني، عمرو (2021). تأثير تطور تقنيات الذكاء الاصطناعي على العمل الشرطي لمواجهة الحروب النفسية.مجلة البحوث القانونية والاقتصادية، عدد خاص بالمؤتمر الدولي السنوي العشرون، 976 – 1035
4. الشمري، علاء (2021). الإعلام المرئي في ظل تحديات الذكاء الاصطناعي: دراسة استطلاعية. مجلة الآداب، ع137، 717 - 742.
5. أمين، رضا (2016). تأثير مواقع التواصل الاجتماعي على العلاقات الاجتماعية: دراسة ميدانية في ضوء نظريتى الحتمية التكنولوجية والقيمية. المجلة العلمية لبحوث العلاقات العامة والإعلان ع6.
6. عبد الكريم، فوزي (2018). أثر مواقع التواصل الاجتماعي وعلاقتها باتجاهات الجمهور: دراسة ميدانية. مجلة العلوم والدراسات الإنسانية ع58.
7. سمان، جويدة.(2017).الابتزاز الالكتروني للفتاة عبر مواقع التواصل الاجتماعي: الفيسبوك نموذجا: دراسة مسحية لعينة من طالبات قسم الاعلام والاتصال جامعة قاصدي مرباح،رسالة ماجيستير غير منشورة، الجزائر: جامعة قاصدي مرباح ورقلة ورقلة – كلية العلوم الانسانية والاجتماعية.
8. عبد المجيد، نبيه (2018). الامن الالكتروني ضرورة ملحة لأمن المجتمعات، مقترح الاسرة الامنة الخاصة بتوعية المجتمع العربي الخليجي في أمن المعلومات لكل من الطلاب والوالدين، المجلة العربية الدولية للمعلوماتية، مج 6،ع (11).
9. عبد الهادي، آية (2021). إدراك مستخدمي مواقع التواصل الاجتماعي لأهمية الأمن السيبراني ودوره في الأمن المعلوماتي: دراسة ميدانية.المؤتمر العلمي الدولي السادس والعشرين: الإعلام الرقمي والإعلام التقليدي: مسارات للتكامل والمنافسة، القاهرة: جامعة القاهرة - كلية الإعلام،مج2.
10. فقيه، جيهان.(2017). حماية البيانات الشخصية في الاعلام الرقمي. مجلة العلوم الانسانية، جامعة العربي بن مهيدي _ ام البواقي، ع(7)
11. لطفى، فاتن (2019). إدراك الشباب لإيجابيات وسلبيات مواقع التواصل الاجتماعي وعلاقته باستخدامهم تلك المواقع. مجلة بحوث في العلوم والفنون النوعية، ع11
12. محمد، نرمين (2022.(استخدام المراهقين لشبكات التواصل الاجتماعي وعلاقته بإدراكهم لانتهاكات خصوصيتهم: دراسة ميدانية.مجلة البحوث والدراسات الإعلامية، المعهد الدولي العالي للإعلام بالشروق، ع (20)
13. مسعد، رضا.(2018). التعليم المدمج: مدخل تكنولوجي لتنمية مهارات الاستخدام الآمن للانترنت والوعي بأخلاقيات التكنولوجية المعاصرة، مجلة تربويات الرياضيات: الجمعية المصرية لتربويات الرياضيات، مج 21، ع(3).
14. مشعل، رباب (2021). دور الأسرة لتحقيق الاستخدام الآمن لوسائل التواصل الاجتماعي للمراهقين

وعلاقته بتعزيز الأمن الفكري والأخلاقي واستراتيجيات مواجهة التنمر الإلكتروني.مجلة البحوث في مجالات التربية النوعية، جامعة المنيا، كلية التربية النوعية، ع34.

15.ملح، حبيب (2021). تقنية التزييف العميق وأثرها في تهديد مصداقية الإعلام الإلكتروني: دراسة وصفية. مجلة جامعة تكريت للعلوم الإنسانية،ج4،ع (28).

ثانيا: المراجع الاجنبية

1. **Ajder, H ; Patrini, G ; At all(2019). The state of deepfakes:landscape,threats‹and impact.Amsterdam:Deeptrace. Available:http://regmedia.co.uk/2019/10/08/deepfake_report.pdf.**
2. **BBC News. (2018, June 11). India WhatsApp "child kidnap" rumours claim two more victims. https://www.bbc.co.uk/news/ world-asia-india-44435127**
3. **Blanz, V ; Scherbaum, K ; At all (2004). Exchanging faces in images. Comput. Graph. Forum 23.**
4. **Diakopoulos, Nicholas; Johnson, Deborah (2021) Anticipating and addressing the ethical implications of deepfakes in the contextof elections. new media & society Vol. 23(7).**
5. **Facebook. (2018, April 17). You won't believe what Obama says in this video! https://www.facebook.com/watch/?v=10157675 129905329**
6. **Gregory, Sam (2022) Deepfakes, misinformation and disinformation and authenticity infrastructure responses: Impacts on frontline witnessing, distant witnessing,and civic journalism. Journalism Vol. 23(3).**
7. **Jiang, Jianguo ; Li, Boquan; At all (2021) FakeFilter: A cross-distribution Deepfake detection system with domain adaptation. Journal of Computer Security Vol 29.**
8. **Kolagati, Santosh ; Priyadharshini, Thenuga; At all (2022) Exposing deepfakes using a deep multilayer perceptron – convolutional neural network model. International Journal of Information Management Data Insights vol 2.**
9. **Maras, Marie Helen; Alexandrou, Alex (2019) Determining authenticity of video evidence in the age of artificial intelligence and in the wake of Deepfake videos. The International Journal of Evidence & Proof Vol. 23(3).**
10. **Patchin, Justin W ; Hinduja , Sameer (2010) Trends in online social networking: adolescent use of MySpace over time, new media & society vol.12(2)**

11. **Saifuddin, Ahmed (2021). Who inadvertently shares deepfakes? Analyzing the role of political interest, cognitive ability, and social network size. Telematics and**

Informatics Vol 57

12. **Seta, Gabriele de (2021) Huanlian, or changing faces: Deepfakes on Chinese digital media platforms. Convergence The International Journal of Research into New Media Technologies Vol. 27(4).**

13. **Shin, Wonsun ; Lwin, , May O (2017). How does "talking about the Internet with others" affect teenagers' experience of online risks? The role of active mediation by parents, peers, and school teacher. new media & society, Vol. 19(7).**

14. **Tolosana, Ruben; Rodriguez, Vera ; At all (2020) Deepfakes and beyond: A Survey of face manipulation and fake detection. Information Fusion vol 64**

15. **Twitter. (2018, April 17). You won't believe what Obama says in this video! https://twitter.com/BuzzFeed/status/9862579917 99222272**

16. **YouTube. (2018, April 17). You won't believe what Obama says in this video! https://www.youtube.com/watch?v=cQ54GD m1eL0**

17. **Vaccari, Cristian; Chadwick, Andrew (2020) Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News. Social Media + Society. Vol. 6(1).**

18. **Wang S. ; Kim S., (2022) Users' emotional and behavioral responses todeepfake videos of K-pop idols , Computers in Human Behavior. Available:https://doi.org/10.1016/j.chb.2022.107305.**

19. **Wilkerson, Lindsey (2021) The Rising Concerns of "Deepfake" Technology and Its Influence on Democracy and the First Amendment. Missouri Law Review Vol. 86(1).**