العدد ١٨ آب ٢٠٢٥
No. 18 – Ang 2025
المجلة العراقية للبحوث الانسانية والاجتماعية والعلمية
Iraqi Journal of Humanitarian, Social and Scientific Research
Print ISSN 2710-0952 Electronic ISSN2790-1254

توظيف انشطة العلاقات العامة لحماية الافراد من الاختراق السيبراني

(دراسة تحليلية)

Utilizing Public Relations Activities to Protect Individuals from Cyber Attacks

(Analytical Study)

الاسم الاول: م.م محمد رعد عبد

Mohammed Raad Abd

الايميل : mohammed.r.abed@aliaqia.edu.iq

رقم الهاتف: ٠٧٥١٣٧٣٨٤٥٢ -٠٧٧٦٧٢٠٦٠٣٣

الاسم الثاني: م.م احمد خيري احمد

Ahmed khairi Ahmed

الايميل : ahmed.k.ahmed@aliaqia.edu.iq

رقم الهاتف: ٠٧٨٥٥٢٢٢٠٠٦

جامعة العراقية/ كلية الاعلام – قسم العلاقات العامة

Al-Iraqiya University / College of Media - Public Relations Department

Keywords: Utilizing, Public Relations, Activities, to Protect Individualsm from Cyber Attacks

مستخلص البحث:

تناول البحث تحليل مضامين صفحة مركز الامن السيبراني المختصة عن قضايا الاختراق السيبراني البنية التحتية للمعلومات والبيانات الشخصية والمؤسسية، لذلك قام الباحثان في دراسة صفحة مركز الامن السيبراني عبر موقع الفيس بوك للمنشورات من تاريخ ٢٠٢٤/١٢/٢٠ لغاية ٢٠٢٥ /٣/٢٠ وتم الحصول في هذه المدة الى (١٣٣) منشور لصفحة الموقع من نشاطات التي اعتمدتها العلاقات العامة، وانت مشكلة وتم تصميم استمارة التحليل المضمون وفق متطلبات البحث الى (فئات ماذا قيل؟) و(فئات كيف قيل؟) وحدد مشكلة البحث بتساؤل رئيسي (ما المضامين والاشكال التي استخدمتها العلاقات العامة لمواجهة الاختراق السيبراني) وقد تفرع عنه الى مجموعة من تساؤلات الفرعية، حتى حصلا الى مجموعة من نتائج منها أن الأنشطة التدريبية والتوعوية تلعب دورًا هامًا في تعزيز الأمن السيبراني، حيث جاءت الدورات التدريبية المستمرة في المرتبة الأولى، تليها المحاضرات التوعوية وورش العمل. هذه الأنشطة تساهم في تعزيز الوعي والمهارات اللازمة للافراد للتعامل مع التهديدات السيبرانية.

كلمات المفتاحية: توظيف ، انشطة العلاقات العامة، حماية الافراد، اختراق، السيبراني

Abstract:

This study analyzed the content of the cybersecurity center's page on Facebook, focusing on issues related to cyber attacks, information infrastructure, and personal and institutional data. The researchers examined the page's posts from December 20, 2024, to March 20, 2025, and collected 133 posts that reflected the activities of the public relations department.The study aimed to answer the main research question: "What content and forms were employed by public relations to address cyber attacks?" The researchers designed a content analysis form according to the research requirements, categorizing the data into "what was said?" and "how was it said?" categories.The study's findings indicated that training and awareness activities play a crucial role in enhancing cybersecurity. Specifically, the results showed that:Continuous training courses ranked first, Awareness lectures and workshops followed.

مقدمة:

شكلت التهديدات السيبرانية خطراً كبيراً على الافراد للتعامل مع البيانات والمعلومات الالكترونية أو الرقمية سواء على مستوى الشخصي أو المؤسسات، وهذا التحدي اصبح ملازم للنشاط وعمل الافراد في حفظ المعلومات أو نقلها، لذلك ركز البحث في دراسة المضامين التي تستخدمها العلاقات العامة عبر صفحة مركز الامن السيبراني عند نشر المفاهيم الاعلامية التي تزيد من وعي الافراد وتوجيههم نحو حفظ المعلومات ومتابعة الشركات الاجنبية لمعالجة الثغرات من الهجوم السيبراني، ومع هذا التهديد الالكتروني اصبح من الضروري التعامل مع المحتويات الرقمية بشكل آمن من استخدام البرامج الفحص الالكتروني، وتم تقسيم البحث الى ثلاثة مباحث الاول ضم الاطار المنهجي للبحث التمثل بالمشكلة البحثية واهمية البحث العلمية والعملية والاجتماعية، واهداف البحث والاداة المستخدمة وغيرها من الخطوات الاخرى.

فيما تناول المبحث الثاني الجانب النظري للبحث عن العلاقات العامة والامن السيبراني، استهل بالمفهوم وتعريف العلاقات العامة وانشتطها للتعامل مع الاختراق السيبراني، وكذلك عن مفهوم الاختراق السيبراني وابعاد المستخدمة له.

وشمل المبحث الثالث جداول نتائج والتكرارات والنسب المئوية وتفسرها والحصول على النتائج التي توصل اليها البحث ثم الخروج بالاستنتاجات والتوصيات البحث.

المبحث الاول: الاطار المنهجي للبحث

أولا: مشكلة البحث:

في ظل تزايد استخدام المواقع الالكترونية من جميع فئات المجتمع، فان ذلك لا يخلو من تحديات تواكب التطور التكنولوجي، اصبحت التهديدات الالكترونية ملاحقة الافراد والمؤسسات والشركات العالمية للاتصال من الاختراق المعلومات، بوضع التهديدات في اختراق الحسابات عبر روابط الوهمية وانتحال الشخصيات المعروفة لكسب المعلومات والابتزاز الالكتروني، ولاشك بان الاختراق السيبراني يمثل تهديداً

لمواقع الشخصية والمؤسسات فقط بل تعدى الامر الى زعزة استقرار المجتمع عبر تبني القضايا الجيوسياسية والقضايا المتعلقة بالمصالح الاشخاص والمجتمع، لذلك التفتت وزارة الداخلية الى انشاء مركز متخصص لمواجهة الاختراق المعلومات وسمية بالمركز الامن السيبراني الذي يتبنى القضايا الاختراق وكيفية التعامل مع الصفحات الالكترونية المزيفة والتصدي لها، وتكمن مشكلة البحث حول الاختراق السيبراني بالتساؤل الرئيسي (ما المضامين والاشكال التي استخدمتها العلاقات العامة لمواجهة الاختراق السيبراني؟) ويفرع منه عدة تساؤلات:

١- ما المضامين التي تناولها منشورات مركز الامن السيبراني في الاختراق المعلومات؟

٢- ما وسائل الابراز المستخدمة لدى صفحة مركز الامن السيبراني؟

٣- ما استراتيجيات العلاقات العامة المستخدمة في مركز الامن السيبراني؟

٤- ما اهداف العلاقات العامة المستخدمة في مركز الامن السيبراني؟

٥- ما انشطة العلاقات العامة المستخدمة في مركز الامن السيبراني؟

٦- ما الفنون الصحفية المستخدمة في عرض الاختراق المعلومات؟

٧- ما الجمهور المستهدف من الاختراق المعلومات؟

ثانياً: اهمية البحث:

بسب التطورات الحاصلة في التكنولوجية المعلومات وافق ذلك الاختراق السيبراني لامن المعلومات الشخصية للافراد والمؤسسات الدولة المتمثلة بالوزارات والمنظمات والشركات بسبب تعاملهم المباشر وتزويد المعلومات والخدمات اللازمة لهم.

١- الاهمية العلمية: الأهمية العلمية لهذا الموضوع تكمن في فهم كيفية مشاركة الأفراد في دائرة الاستهداف السيبراني، سواء كانوا مستفيدين من خدمات الدولة أم لا. يتطلب الكشف عن هوية المستهدفين فهمًا عميقًا للنوايا الدافعة وراء الاستهداف، مثل إرسال الروابط الجهولة أو البرامج الضارة لاختراق المعلومات وكذلك الكشف عن أساليب هوية المستهدفين، وايضاً تطوير استراتيجيات حماية المعلومات من الاختراق.

٢- الاهمية التطبيقية: أهمية البحث تتطلب من الشركات الإلكترونية والحكومات اتخاذ إجراءات فعّالة لمتابعة محركات البحث العالمية والصفحات الرسمية، والتعامل بفعالية مع المعلومات المرسلة وفحص البيانات عبر برامج الكشف عن محاولات اختراق المعلومات.

٣- الاهمية الاجتماعية: التصدي للاختراق السيبراني تكمن في حماية الأفراد والمجتمعات من المخاطر الناجمة عن التهديدات السيبرانية، يتطلب ذلك معرفة مستوى خطر الاختراق السيبراني وكيفية الحفاظ على أمن المعلومات، واستخدام، أرقام سرية قوية لحماية البيانات حتى يتم إدارة المعلومات بشكل آمن ومنظم عند استخدام برامج حماية فعالة للتصدي للفيروسات الإلكترونية وتمكين التعامل مع الرسائل الوهمية التي تنتحل صفات وأسماء مستعارة.

ثالثاً: أهداف البحث:

١- التعرف على المضامين التي تناولها منشورات مركز الامن السيبراني في الاختراق المعلومات.

٢- معرفة وسائل الابراز المستخدمة لدى صفحة مركز الامن السيبراني.

٣- تحديد استراتيجيات العلاقات العامة المستخدمة في مركز الامن السيبراني.

٤- توضيح اهداف العلاقات العامة المستخدمة في مركز الامن السيبراني.

٥- معرفة انشطة العلاقات العامة المستخدمة في مركز الامن السيبراني.

٦- معرفة الفنون الصحفية المستخدمة في عرض الاختراق المعلومات.

٧- تحديد الجمهور المستهدف من الاختراق المعلومات.

رابعاً: مجالات البحث:

وتشمل مجالات البحث الى:

١- **المجال المكاني:** اعتمد البحث على صفحة مركز الامن السيبراني لوزارة الداخلية العراقية عبر موقع الفيس بوك.

٢- **المجال الزماني:** تم تحديد المدة الزمنية للبحث في ثلاثة شهور من(٢٠٢٤/١٢/٢٠ الى ٢٠٢٥/٣/٢٠) كون هذه المدة اعتمد فيها المركز الامن السيبراني على زيادة وررش عمل ومحاضرات والندوات واهتمام العلاقات العامة بعرض الانشطة عبر صفحة الفيس بوك لمركز الامن السيبراني .

٣- **المجال الموضوعي للبحث:** تمثل في منشورات مركز الامن السيبراني وتوظيف العلاقات العامة من المضامين ونشرها عبر موقع المركز وكيفية الكشف عن الصفحات الاسماء الوهمية، وكذلك متابعة الشركات الالكترونية للتعامل مع الثغرات الامنية الالكترونية.

خامساً: مجتمع البحث:

استهدف البحث عدة مضامين صفحة الفيس بوك لمركز الامن السيبراني، وتم تحليل (١٣٣) منشور لمدة ثلاثة اشهر عن طريق استخدام اسلوب الحصر الشامل للمدة من (٢٠٢٤/١٢/٢٠ الى ٢٠٢٥/٣/٢٠).

سادساً: نوع البحث ومنهجه:

يعد البحث من البحوث الوصفية التحليلية الذي يستخدم في دراسة تحليل المضامين الاعلامية، لكشف انشطة العلاقات العامة لوصف الظاهرة أو موضوعات يتعلق بحفظ وأمن المعلومات من الاختراق السيبراني، كما ان البحوث التحليلية تكشف مواطن القوة والضعف في المنشورات الاعلامية عبر مواقع التواصل الاجتماعي بما يقدمه من صور وفيديوهات، تظهر الاساليب المتبعة لحفظ البيانات واضافة العناصر التي تمكن المستخدمين أو المتابعين لصفحة مركز الامن السيبراني عبر فيس بوك من التعامل مع المخترق السيبراني، لذلك وجد البحث في استخدام المنهج التحليلي لمعرفة الاجراءات والطرق المتبعة في الصفحة اعلاه التابعة لوزارة الداخلية.

سابعاً: اجراءات البحث وأدوات جمع البيانات:

بعد دراسة موقع مركز الامن السيبراني الفيس بوك، لاحظا الباحثان عن استخدام انشطة العلاقات العامة بشكل مستمر ويوحي لمعرفة دورها في الوقاية من الاختراق للمعلومات الشخصية والمركزية ومواقع المؤسسات الخدمية وغيرها، لوحظ بوجود اهتمام بتوعية افراد المؤسسات عند التعامل مع تلك التهديدات السيبرانية.

وعلى ضوء ذلك تم تحديد اداة استمارة تحليل المضمون وتم تصميمها وفقا لمتطلبات البحث، واعتمد الباحثان في ذلك الموضوع على تحليل (وحدة الموضوع أو الفكرة) كونها الملائمة لموضوع البحث لمنشورات صفحة مركز الامن السيبراني عبر موقع الفيس بوك، وتم عرض استمارة تحليل المضمون على مجموعة من المحكمين(*)، وبعد ذلك تم تحديد فئات التحليل على النحو التالي:

الجانب الاول: يتناول مضامين (فئات ماذا قيل؟) والتي تضمنت فئات الرئيسية والبالغ عددها(٤)، والفئات الفرعية بلغ عددها (٣٥) فئة.

والجانب الثاني: يتناول الشكل الذي تم عرض المضمون عبر موقع الفيس بوك لصفحة مركز الامن السيبراني (فئات كيف قيل؟) الذي يتضمن (٥٢) فئة.

ثامناً: اختبار الصدق والثبات:

صدق التحليل: وهي ملائمة طريقة البحث أو أسلوب القياس باستخلاص النتائج المطلوبة بغية تحقيق الموضوعية في تحليل المحتوى وينبغي أن يكون معولاً على نتائجه، أي أن تكون نتائجه صادقة(مؤيد خلف، ٢٠٠٨، ص٢٦٠).
ولتحقيق الصدق في عملية التحليل، عرض ما استخرج من الفئات الرئيسية وتم صياغتها بشكل مختصر وواضح قبل البدء بعملية التحليل والتفسير اللاحقة، وقد عرضت استمارة الفئات على عدد من الخبراء عندما قدمت الفئات إلى (٥) محكمين في مجال الإعلام لتقويمها وتصويبها واتفقوا على صلاحيتها في قياس توظيف أنشطة العلاقات العامة لحماية الأفراد من الاختراق المعلوماتي، وفي ضوء آرائهم عدلت بعض الفئات ولم تستبعد أي فئة لأنَّها حظيت بموافقتهم بنسبة (٨٠%) فأكثر، لذا اعتمدت هذه النسبة معياراً لصلاحية الفئات. كما في جدول (١) يُوضح نسبة اتفاق المحكمين على فئات استمارة التحليل والتي بلغت نسبتها (٩٢.٨٨%) وهي نسبة مقبولة جداً من الناحية العلمية(بيرق حسين، ٢٠١٨، ص١٥٥).

$$\text{الصدق الظاهري} = \frac{\text{مجموع الفئات الصالحة}}{\text{العدد الكلي للفئات}}$$

(*) اسماء المحكمين

١) أ.د صباح أنور محمد / قسم العلاقات العامة / كلية الاعلام / الجامعة العراقية.
٢) أ. راضي رشيد / قسم الاذاعة والتلفزيون / كلية الاعلام / الجامعة العراقية.
٣) أ. م.د حردان هادي / قسم العلاقات العامة / كلية الاعلام / الجامعة العراقية.
٤) أ.م.د صباح عواد محمد / قسم الصحافة / كلية الاعلام / الجامعة العراقية.
٥) د. علاء حسين / قسم العلاقات العامة / كلية الاعلام / جامعة الفراهيدي..

٢٧٤

= ــــــــــــــــــــــــــــ

٢٩٥

الصدق الظاهري=٩٢.٨٨%

وهذه النسبة تشير إلى ان معظم الفئات المطروحة في الاستمارة قابلة لتحقيق الهدف الذي وضعت لأجله.

جدول (١) يوضح الصدق الظاهري للخبراء لاستمارة تحليل المضمون

ت	اسماء الخبراء	الاختصاص الدقيق	الفئات الصالحة	الفئات المعدلة	الفئات المرفوضة	العدد الكلي للفئات	النسبة المئوية
١	ا.د صباح أنور	العلاقات العامة	٥٥	٤	-	٥٩	%٩٣.٢٢
٢	ا. راضي رشيد	إذاعة وتلفزيون	٥٦	٣	-	٥٩	%٩٤.٩٢
٣	ا.م.د. حردان هادي	العلاقات العامة	٥٤	٥	-	٥٩	%٩١.٥٣
٤	ا.م.د علاء حسين	العلاقات العامة	٥٥	٤	-	٥٩	%٩٣.٢٢
٥	ا.م.د صباح عواد محمد	الصحافة	٥٤	٥	-	٥٩	%٩١.٥٣
المجموع			٢٧٤	٢١	-	٢٩٥	٨٢٣.٥

ثبات التحليل: استخدم الباحث طريقة الاتساق عبر الزمان: بمعنى أن يحصل الباحثون المحللون على النتائج نفسها إذا طبقوا الفئات ذاتها على المضمون نفسه لفترات متباعدة أو مختلفة.

إذ قام بإعادة التحليل بعد مضي شهرين على عملية التحليل الأولى، وقد خرج الباحث بالنتائج نفسها باستثناء اختلافات طفيفة. وعند تطبيق معادلة (هولستي) لقياس الثبات حصل الباحث على درجة ثبات (0.966) وهي درجة مقبولة لقياس الثبات. وفي أدناه نص المعادلة(وهيب مجيد، ٢٠١٠، ص٧٢):

$$R=\frac{2(C1-2)}{C1+C2}=\frac{2\times 2-59}{59+59}=\frac{114}{118}=0.966$$

إذ أن R يمثل معامل الثبات

C1+C2 = عدد الإجابات المتفق عليها بين المحلل الأول والمحلل الثاني.

C1 = عدد الإجابات التي انفرد بها المحلل الأول.

C2 = عدد الإجابات التي انفرد بها المحلل الثاني.

تاسعاً: مصطلحات البحث:

توظيف: وتعني استخدام المختلفة لتعزيز مهارات أو قدرات معينة لدى الافراد في بيئة العمل أو في السياقات التعليمية أو التطويرية لتحسين المهارات المهنية، وتعزيز القدرات لتشجيع للمشاركة والتفاعل.

انشطة العلاقات العامة: هي عملية اتصالية وتفاعلية بين المنظمة أو الفرد أو الجمهور أو الشركات والعملاء لنشر المعلومات حول مخاطر والتهديدات، وتعليم الافراد كيفية حماية انفسهم، ونشر المعلومات حول افضل الممارسات الامنية في تعزيز الوعي السيبراني.

حماية الافراد: هي مجموعة من الاجراءات اللازمة لتمكين الافراد من امن واستخدام اجهزة الحاسوب والهواتف الشخصية من استخدام الكلمات المرور واستحداث البرامج لمكافحة الفيروسات و الثغرات الامنية.

الاختراق السيبراني: هو عملية غير مسرح بها للوصول الى أنظمة الكمبيوتر أو الشبكات أو البيانات بهدف سرقة أو استغلال المعلومات عن طريق القرصنة وارسال البرامج الخبيثة أو الهجمات الالكترونية.

المبحث الثاني : العلاقات العامة والامن السيبراني

أولاً: مفهوم العلاقات العامة: أن مفهوم العلاقات العامة كأداة تمارس في المنظمات أو المؤسسات ، الا أنها ليست نشاطا إدارياً فقط كأي ادارة أخرى داخل هيكل المؤسسة وأنما هي نشاط جوهر الاتصال ، فالعلاقات العامة تمثل نظاماً مفتوحاً تتفاعل مع بيئتها وتؤثر فيها وتتأثر بها ، فطبيعة عمل منظمات والمؤسسات قائم على مبدأ المشاركة والنزوع نحو العمل الطوعي وعدم الربحية يجعلها في الحاجة ماسة التواصل والاتصال المستمر بأفراد المجتمع لكي يضمن اقامة علاقات التفاهم والثقة المتبادلة مع الجماهير . وتحتاج العلاقات العامة الى العمل الطوعي خاصةً اذا كان هدفه في خدمة المجتمع وتحديدا في مواجهة الظواهر السلبية التي تحدث في مجتمع معين ،لانها تقود الى الاستقرار أو تقليل بعض اختراق الالكتروني التي تستهدف الافراد ، لذلك على العلاقات العامة أن تتواصل مع جميع الاطراف لكي تحقق الاهداف على مستوى الفرد أو على مستوى المجتمع (عبد الرزاق الدليمي، ٢٠١٥، ص٤).

عرفها ريكس هارلو ((هي الوظيفة الادارية متميزة تساعد في تكوين وإدامة خطوط أتصال ثنائية في تحقيق التفاهم والتعاون بين المنظمة وجماهيرها وتشمل هذه الوظيفة أدارة المشكلات والقضايا وتساعد الادارة على استمرار في الاطلاع على اتجاهات الرأي العام والاستجابة له وتحدد وتؤكد مسؤولية الادارة في خدمة الصالح العامة .كما وتساعد الادارة مجارات التغيير ،وكما تستخدم كنظام إنذار مبكر للمساعدة في التنبؤ والتعرف على اتجاهات الجديدة ،مستخدمة في ذلك البحث والاتصالات كأدوات أساسية)) (محمد ابراهيم، ٢٠١٧، ص٢٤) .

ثانياً: انشطة العلاقات العامة: توظيف أنشطة تعني استخدام الأنشطة المختلفة لتعزيز مهارات أو قدرات معينة لدى الأفراد، سواء في بيئة العمل أو في السياقات التعليمية أو التطويرية. يمكن أن تشمل هذه الأنشطة(خالد عبد الحق، دعاء عبد العال٢٠٢٥، ص٣٣):

١. التدريب المهني: أنشطة مصممة لتحسين المهارات المهنية.

٢. ورش العمل: جلسات تفاعلية تهدف إلى تعلم مهارات أو مفاهيم جديدة.

٣. التطوير الشخصي: أنشطة تهدف إلى تحسين الذات وتعزيز القدرات الشخصية.

٤. التعلم النشط: أنشطة تعليمية تشجع على المشاركة والتفاعل.

وان توظيف الأنشطة يمكن أن يساعد في تحقيق أهداف محددة، مثل تحسين الأداء، تعزيز المهارات، أو بناء الفريق، العلاقات العامة تلعب دورًا هامًا في حماية الأفراد من خلال(خالد عبد الحق، دعاء عبد العال، مرجع سابق، ص٤٣):

١. توعية الجمهور: نشر المعلومات حول المخاطر والتهديدات.

٢. تثقيف الأفراد: تعليم الناس كيفية حماية أنفسهم.

٣. بناء الثقة: تعزيز الثقة بين الأفراد والمؤسسات.

٤. استجابة للطوارئ: تقديم المعلومات والدعم أثناء الأزمات.

٥. تعزيز الوعي السيبراني: نشر المعلومات حول أفضل الممارسات الأمنية

ثالثاً: الاختراق السيبراني: ان مخاطر الانترنيت اثار أمن البنية التحتية السيبراني بشكل عام بتعرض أمن أجهزة الكمبيوتر الخاصة بالافراد عن طريق فتح رسائل البريد الالكتروني أو عند عدم تفعيل برامج مكافحة الفيروسات[1] ، هو عملية غير مصرح بها للوصول إلى أنظمة الكمبيوتر أو الشبكات أو البيانات بهدف سرقة أو إتلاف أو استغلال المعلومات. يشمل الاختراق السيبراني مجموعة واسعة من الأنشطة، بما في ذلك(**Resources Magagment Association USA, 2012, p3**) :

١. القرصنة: الوصول غير المصرح به إلى الأنظمة أو الشبكات.

٢. البرمجيات الخبيثة: استخدام البرمجيات الضارة لإتلاف أو سرقة البيانات.

٣. الهجمات الإلكترونية: الهجمات الموجهة ضد الأنظمة أو الشبكات بهدف تعطيلها أو استغلالها.

الأمن السيبراني: هو مجموعة من الإجراءات والتدابير التي تهدف إلى حماية الأنظمة والشبكات والبيانات من الهجمات والتهديدات السيبرانية، مثل القرصنة والبرمجيات الخبيثة والفيروسات، يهدف الأمن السيبراني إلى(مصدر من الانترنيت):

١. حماية البيانات: منع الوصول غير المصرح به إلى البيانات.

٢. حماية الأنظمة: حماية الأنظمة والشبكات من الهجمات.

٣. ضمان الاستمرارية: ضمان استمرارية العمل وتقليل الأثر في حالة الهجمات.

رابعاً: ابعاد الأمن السيبراني: يشمل عدة مجالات، مثل: أمان الشبكات، أمان التطبيقات، أمان البيانات، إدارة التهديدات، الاستجابة للحوادث، يعد الأمن السيبراني ضروريًا لحماية الأفراد والمنظمات من التهديدات السيبرانية المتزايدة، والأمن السيبراني يمتلك عدة أبعاد مهمة، تشمل(عادل عبد الصادق، ٢٠٢٠، ص٢٨-٣٠):

١. الأمان الوقائي: حماية الأنظمة والبيانات من الهجمات والتهديدات.

٢. الكشف والاستجابة: اكتشاف التهديدات والاستجابة لها بسرعة.

٣. الاستعادة بعد الهجوم: استعادة الأنظمة والبيانات بعد هجوم سيبراني.

٤. التعاون والمشاركة: التعاون بين المنظمات والمؤسسات لتبادل المعلومات حول التهديدات.

٥. التدريب والتوعية: تعليم الأفراد حول أفضل الممارسات الأمنية.

٦. الامتثال للمعايير: اتباع المعايير واللوائح الأمنية.

المبحث الثالث: عرض وتحليل نتائج البحث

يقدم البحث في هذا الفصل الجانب العملي وما تم من تحليل المضامين لصفحة مركز الامن السيبراني في تناول المواضيع التي تهتم في كشف عن الحالات الاختراق وطرق تحصين البيانات المركزية سواء كانت لوزارات ومؤسسات والمعلومات الشخصية عن طريق استخدام جهاز الحاسوب أو استخدام الهاتف الشخصي، وما نبحث عنه هو كيفية توظيف انشطة العلاقات العامة عبر صفحة مركز الامن السيبراني لزيادة وعي الجماهير في الحصول على المعلومات أو المشاركة الرسائل أو ما يخص في التعامل الجهات المجهولة عبر مواقع التواصل الاجتماعي.

انشئت صفحة مركز الامن السيبراني التابعة لوزارة الداخلية العراقية في ٩ نوفمبر ٢٠٢٣، واختصت في الكشف عن حالات الاختراق السيبراني ومتابعة الشركات الالكترونية في معالجة الثغرات، وكذلك نشر النشاطات التي يقدمها المركز من زيادة وعي منتسبي الداخلية بشكل خاص وتعامل الافراد بشكل عام.

المحور الاول: فئات ماذا قيل؟

كشف البحث تحليلاً لمضامين منشورات لدى صفحة مركز الامن السيبراني عبر موقع الفيس بوك بواقع (١٣٣) منشوراً من تاريخ (٢٠٢٤/١٢/٢٠) لغاية (٢٠٢٥/٣/٢٠) وتمثلت فئات الرئيسية حيث بلغت (اربعة فئات) والفئات الفرعية بلغت (٣٥) فئة ، بواقع (٢١٢) تكرار.

جدول (٢) يبين الفئات الرئيسية لمضامين منشورات العلاقات العامة في صفحة مركز الامن السيبراني

ت	الفئة الرئيسية	التكرار	النسبة المئوية	المرتبة
١	ابراز مفهوم جريمة الاختراق المعلومات	٧٤	%٣٤.٩	الاولى
٢	التوعية بجرائم الاختراق المعلومات	٧٢	%٣٣.٩	الثانية
٣	مستوى الخطر للاختراق المعلومات	٤٥	%٢١.٢	الثالثة
٤	اساليب المستخدمة للاختراق المعلومات	٢١	%٩.٩	الرابعة
المجمـــــــــــــــــوع		**٢١٢**	**%١٠٠**	

يشير الجدول (٢) ان ابراز مفهوم جريمة الاختراق المعلومات: حصل على المرتبة الأولى بتكرار(٧٤) وبنسبة مئوية بلغت (٣٤.٩%)، هذا يشير إلى أن تعريف وتوضيح مفهوم جريمة الاختراق المعلوماتي أمر مهم، أما التوعية بجرائم الاختراق المعلومات: حصل على المرتبة الثانية بتكرار(٧٢) وبنسبة مئوية بلغت (٣٣.٩%)، هذا يعتقدون أن التوعية بجرائم الاختراق المعلوماتي أمر ضروري، في حين ان مستوى الخطر للاختراق المعلومات: حصل على المرتبة الثالثة على(٤٥) تكرار وبنسبة مئوية بلغت(٢١.٢%)، اما اساليب المستخدمة للاختراق المعلومات: حصل على المرتبة الرابعة على(٢١) تكرار وبنسبة مئوية

بلغت(٩.٩%)، هذا يشير إلى أن فهم الأساليب المستخدمة للاختراق المعلوماتي أمر أقل أهمية مقارنة بالمواضيع الأخرى.

أن وتوضيح مفهوم جريمة الاختراق المعلوماتي والتوعية بها أمران مهمان للغاية يأتي فهم مستوى الخطر المرتبط بالاختراق المعلوماتي في المرتبة الثالثة، مما يشير أن هذا الأمر مهم ولكن ليس بنفس الأهمية التي يوليها للتعريف والتوعية يبدو أن فهم الأساليب المستخدمة للاختراق المعلوماتي يعتبر أقل أهمية .

١- ابراز مفهوم جريمة الاختراق المعلومات:

جدول رقم (٣) يبين الفئات الفرعية للفئة الرئيسية (ابراز مفهوم جريمة الاختراق المعلومات)

ت	الفئة الفرعية	التكرار	النسبة المئوية	المرتبة
١	الوقاية من الاختراق السيبراني	٣٥	%٤٧.٢	الاولى
٢	تأمين الحسابات الشخصية	٢٠	%٢٧.٢	الثانية
٣	عدم التعامل مع الروابط التي تنتحل صفحات مواقع مستعارة	١٠	%١٣.٥	الثالثة
٤	بيان التعامل مع الروابط الالكترونية المجهولة	٧	%٩.٤	الرابعة
٥	عدم التعامل مع الروابط الالكترونية التي تنتحل اسماء مستعارة	٢	%٢.٧	الخامسة
المجموع		**٧٤**	**%١٠٠**	

يشير الجدول (٣) ان لوقاية من الاختراق السيبراني: حصل المرتبة الأولى على(٣٥) تكرار و بنسبة مئوية بلغت (٤٧.٢%)[٢]، هذا يشير أن الوقاية من الاختراق السيبراني أمرًا بالغ الأهمية، وتاتي تأمين الحسابات الشخصية: حصل المرتبة الثانية على (٢٠) تكرار بنسبة مئوية بلغت(٢٧.٢%)[٣] ، هذا يشير أن تأمين الحسابات الشخصية أمر مهم للغاية، في حين ان عدم التعامل مع الروابط التي تنتحل صفحات مواقع مستعارة: حصل المرتبة الثالثة على(١٠) تكرار بنسبة مئوية بلغت (١٣.٥%)، هذا يشير إلى أن تجنب التعامل مع الروابط التي تنتحل صفحات مواقع مستعارة أمر مهم اما عن بيان التعامل مع الروابط الالكترونية المجهولة: حصل المرتبة الرابعة على (٧) تكرار وبنسبة مئوية بلغت(٩.٤%)هذا يشير إلى أن فهم كيفية التعامل مع الروابط الالكترونية المجهولة أمر مهم، في حين عدم التعامل مع الروابط الالكترونية التي تنتحل اسماء مستعارة: حصل المرتبة الخامسة على (٢) تكرار وبنسبة مئوية بلغت (٢.٧%) هذا يشير أن تجنب التعامل مع الروابط الالكترونية التي تنتحل اسماء مستعارة أمر أقل أهمية فيما يخص مركز الامن.

ان الوقاية من الاختراق السيبراني وتأمين الحسابات الشخصية أمران مهمان للغاية يأتي تجنب التعامل مع الروابط التي تنتحل صفحات مواقع مستعارة في المرتبة الثالثة، وأن هذا الأمر مهم.وكذلك أن فهم كيفية التعامل مع الروابط الالكترونية المجهولة وتجنب التعامل مع الروابط الالكترونية التي تنتحل اسماء مستعارة أمران أقل أهمية.

---

[٢] نشر في صفحة مركز الامن السيبراني يوم ٥/ مارس / ٢٠٢٥ محاضرة.

[٣] نشر في صفحة مركز الامن السيبراني بتاريخ ٨ / فبراير / ٢٠٢٥ رصد تقرير الى تسريب الحسابات.

٢- التوعية بجرائم الاختراق المعلومات

جدول رقم (٤) يبين الفئات الفرعية للفئة الرئيسية (التوعية بجرائم الاختراق المعلومات)

ت	الفئة الفرعية	التكرار	النسبة المئوية	المرتبة
١	الكشف عن ثغرات الالكترونية للاختراق المعلومات	٤٥	%٦٢.٥	الاولى
٢	الزام الافراد بالفحص الروابط قبل فتحها	١٤	%١٩.٤	الثانية
٣	متابعة الشركات الانترنيت للتصدي عن الفيروسات	٧	%٩.٧	الثالثة
٤	عرض دليل عن الصفحات المخترقة	٣	%٤.١	الرابعة
٥	التأكد من عنوان الالكتروني للموقع مكتوب بشكل صحيح	٣	%٤.١	الرابعة
٦	الكشف عن الصفحات الضحية	٠	%٠	-
المجموع		٧٢	%١٠٠	

يبين الجدول (٤) ان الكشف عن ثغرات الالكترونية للاختراق المعلومات: حصل على المرتبة الأولى (٤٥) تكرار بنسبة مئوية بلغت (٦٢.٥%) [٤] هذا يشير إلى أن الكشف عن ثغرات الاختراق المعلوماتي أمرًا بالغ الأهمية، في حين الزام الافراد بالفحص الروابط قبل فتحها: حصل على المرتبة الثانية على(١٤) تكرار وبنسبة مئوية بلغت(١٩.٤%) [٥]هذا يشير أن إلزام الأفراد بفحص الروابط قبل فتحها أمر مهم، اما ان متابعة الشركات الانترنيت للتصدي عن الفيروسات: حصل على المرتبة الثالثة (٧) تكرار بنسبة بلغت(٩.٧%)هذا يشير إلى أن متابعة الشركات للتصدي للفيروسات أمر مهم، عرض دليل عن الصفحات المخترقة: حصل على المرتبة الرابعة على(٣) تكرارات وبنسبة(٤.١%)هذا يشير أن عرض دليل عن الصفحات المخترقة أمر أقل أهمية، وكذلك التأكد من عنوان الالكتروني للموقع مكتوب بشكل صحيح: حصل على المرتبة الرابعة أيضًا (٣) تكرار وبنسبة مئوية بلغت(٤.١%). هذا يشير إلى أن التأكد من عنوان الموقع الإلكتروني أمر أقل أهمية.

٣- اساليب المستخدمة في الاختراق المعلومات: **جدول رقم**

(٥) يبين الفئات الفرعية للفئة الرئيسية (اساليب المستخدمة في الاختراق المعلومات)

ت	الفئة الفرعية	التكرار	النسبة المئوية	المرتبة
١	الكشف عن ملفات الغير الرسمية	٩	%٤٢.٨	الاولى
٢	عرض المواقع المخترقة	٧	%٣٣.٣	الثانية
٣	الكشف عن انتحال الصفحات المشهورة والمعروفة	٥	%٢٣.٨	الثالثة
المجموع		**٢١**	**%١٠٠**	

[٤] **نشر في صفحة مركز الامن السيبراني بتاريخ ١٢/ يناير/ ٢٠٢٥ اصدرت شركة cisco لمعالجة ثغرة الالكترونية.**

[٥] **نشر في صفحة مركز الامن السيبراني بتاريخ ٢٦/ديسمبر/ ٢٠٢٤ موضوع عن استراتيجية الحماية المتعددة الطبقات.**

يوضح جدول رقم (٥) ان الكشف عن ملفات الغير الرسمية: حصل على المرتبة الأولى (٩) تكرار و بنسبة مئوية (٤٢.٨%)[٦]، هذا يشير إلى أن الكشف عن ملفات الغير الرسمية أمر مهم، اما عن عرض المواقع المخترقة: حصل على المرتبة الثانية (٧) تكرار و بنسبة (٣٣.٣%)[٧]، هذا يشير إلى أن عرض المواقع المخترقة أمر مهم، اما الاخير الكشف عن انتحال الصفحات المشهورة والمعروفة: حصل على المرتبة الثالثة(٥) تكرار وبنسبة(٢٣.٨%) هذا يشير إلى أن الكشف عن انتحال الصفحات المشهورة أمر مهم.

يبدو أن الكشف عن ملفات الغير الرسمية وعرض المواقع المخترقة والكشف عن انتحال الصفحات المشهورة والمعروفة أمور مهمة، يأتي الكشف عن ملفات الغير الرسمية في المرتبة الأولى، مما يشير إلى أن هذا الأمر أكثر أهمية.

٤- مستوى الخطر للاختراق السيبراني: **جدول رقم**

(٦) يبين الفئة الفرعية للفئة الرئيسية (مستوى الخطر للاختراق السيبراني)

ت	الفئة الفرعية	التكرار	النسبة المئوية	المرتبة
١	اختراق الحسابات الشخصية	٣٠	%٦٦.٦	الاولى
٢	اختراق البيانات المركزية للمؤسسات	١٢	%٢٦.٦	الثانية
٣	استخدام صفحات وهمية لتهديد أمن واستقرار المجتمع	٣	%٦.٦	الثالثة
المجموع		٤٥	%١٠٠	

يبن الجدول رقم (٦) ان اختراق الحسابات الشخصية: حصل على المرتبة الأولى بتكرار(٣٠) وبنسبة مئوية بلغت(٦٦.٦%) هذا يشير إلى أن اختراق الحسابات الشخصية يمثل النسبة الأكبر من التهديدات، مما قد يدل على ضعف في أمان الحسابات الشخصية أو سهولة اختراقها، اما عن اختراق البيانات المركزية للمؤسسات: جاء في المرتبة الثانية بتكرار (١٢) وبنسبة مئوية بلغت(٢٦.٦%)هذا يشير إلى أن اختراق البيانات المركزية للمؤسسات يمثل تهديدًا كبيرًا، ولكنه أقل من اختراق الحسابات الشخصية، والاخير تم استخدام صفحات وهمية لتهديد أمن واستقرار المجتمع: حصل على المرتبة الثالثة بتكرار(٣) وبنسبة بلغت(٦.٦%)[٨]هذا يشير إلى أن استخدام الصفحات الوهمية يمثل تهديدًا أقل مقارنة بالاختراقات الأخرى، ولكنه لا يزال يشكل خطرًا على الأمن والاستقرار بشكل عام، يمكن استنتاج أن اختراق الحسابات الشخصية هو التهديد الأكثر شيوعًا، يليه اختراق البيانات المركزية للمؤسسات، ثم استخدام الصفحات الوهمية. هذه النتائج قد تعكس نقاط الضعف في الأمن السيبراني التي تحتاج إلى معالجة لتحسين الأمان والحماية.

ثانياً: انشطة العلاقات العامة المستخدمة في صفحة مركز الامن السيبراني:

جدول رقم (٧) يبين الفئات الفرعية للفئة الرئيسية (انشطة العلاقات العامة المستخدمة في صفحة مركز الامن السيبراني)

ت	الفئة	التكرار	النسبة المئوية	المرتبة
١	الدورات التدريبية المستمرة للافراد للتعامل مع المخترق السيبراني	٥٧	%٤٢.٨	الاولى
٢	اقامة المحاضرات التوعوية للافراد في وزارة الداخلية	٢٩	%٢١.٨	الثانية

[٦] نشر في صفحة مركز الامن السيبراني ١٩ / فبراير / ٢٠٢٥ تقارير عن ملفات الاختراق السيبراني.

[٧] نشر في صفحة مركز الامن السيبراني بتاريخ ٢٥/ يناير / ٢٠٢٥ اختراق الموقع الوتساب.

[٨] نشر في صفحة مركز الامن السيبراني بتاريخ ٦/ فبراير/ ٢٠٢٥ عن الخطاب الكراهية والطائفية.

٣	تنفيذ ورشات عمل مع الجهات ومؤسسات الدولة	٢٢	%١٦.٥	الثالثة
٤	اقامة المسابقات والمنافسات للتعامل مع الاختراق السيبراني	١٣	%٩.٧	الرابعة
٥	اقامة الندوات التوعوية للاجهزة الحكومية الاخرى	١٢	%٩.١	الخامسة
	المجموع	١٣٣	%١٠٠	

يبين الجدول (٧) ان الدورات التدريبية المستمرة: حصلت على المرتبة الأولى بتكرار(٥٧) وبنسبة مئوية(٤٢.٨%)، مما يشير إلى أهمية التدريب المستمر في هذا المجال، اما عن المحاضرات التوعوية: جاءت في المرتبة الثانية بتكرار(٢٩) وبنسبة مئوية(٢١.٨%)، مما يدل على أهمية التوعية والتعليم في مجال الأمن السيبراني، في حين ان ورش العمل: حصلت على المرتبة الثالثة بتكرار(٢٢) وبنسبة مئوية (١٦.٥%)، مما يشير إلى أهمية التعاون والتنسيق بين الجهات الحكومية، اما عن المسابقات والمنافسات: جاءت في المرتبة الرابعة بتكرار (١٣) وبنسبة مئوية(٩.٧%)، مما يدل على أهمية تحفيز الأفراد على تعلم مهارات الأمن السيبراني، وفي الاخير ان الندوات التوعوية: حصلت على المرتبة الخامسة بتكرار (١٢) وبنسبة مئوية (٩.١%)، مما يشير إلى أهمية نشر الوعي والمعرفة في مجال الأمن السيبراني.

هذه النتائج تعكس الأولويات والاحتياجات في مجال الأمن السيبراني، وتشير إلى أهمية التدريب والتوعية في هذا المجال. الاستنتاج هو أن الأنشطة التدريبية والتوعوية تلعب دورًا هامًا في تعزيز الأمن السيبراني، حيث جاءت الدورات التدريبية المستمرة في المرتبة الأولى، تليها المحاضرات التوعوية وورش العمل. هذه الأنشطة تساهم في تعزيز الوعي والمهارات اللازمة للتعامل مع التهديدات السيبرانية، وتشير إلى أهمية الاستثمار في التدريب والتوعية لتحسين الأمن السيبراني.

ثالثا: أهداف العلاقات العامة المستخدمة في صفحة مركز الامن السيبراني:

جدول رقم (٨) يبين الفئات الفرعية للفئة الرئيسية (أهداف العلاقات العامة المستخدمة في صفحة مركز الامن السيبراني)

ت	الفئة	التكرار	النسبة المئوية	المرتبة
١	تأمين الحسابات الشخصية وعدم فتح الروابط المجهولة	٥٣	%٣٩.٨	الاولى
٢	استخدام برامج الفحص الروابط المزيفة	٣٩	%٢٩.٣	الثانية
٣	تجنب مشاركة البيانات الشخصية الالكترونية	٢٨	%٢١.١	الثالثة
٤	تغير كلمة المرور للموقع الالكتروني	١٣	%٩.٧	الرابعة
المجموع		١٣٣	%١٠٠	

يبين الجدول (٨) ان تأمين الحسابات الشخصية وعدم فتح الروابط المجهولة: حصل على المرتبة الأولى بتكرار(٥٣) وبنسبة مئوية بلغت(٣٩.٨%) هذا يشير إلى أن تأمين الحسابات الشخصية وتجنب الروابط المجهولة يعتبران من أهم الإجراءات التي يتخذها الأفراد لحماية أنفسهم من التهديدات السيبرانية، اما عن استخدام برامج الفحص الروابط المزيفة: جاء في المرتبة الثانية بتكرار (٣٩) وبنسبة مئوية (٢٩.٣%)هذا يشير إلى أن استخدام برامج الفحص تعتبر خطوة مهمة في حماية الأفراد من الروابط المزيفة والتهديدات السيبرانية، وكانت تجنب مشاركة البيانات الشخصية الإلكترونية: حصل على المرتبة الثالثة بتكرار(٢٨) وبنسبة مئوية(٢١.١%) هذا يشير إلى أن تجنب مشاركة البيانات الشخصية يعتبر إجراءً مهمًا، ولكنه أقل شيوعًا مقارنة بالتأمين وفحص الروابط، وفي الاخير تغير كلمة المرور للموقع الإلكتروني: جاء في المرتبة الرابعة بتكرار (١٣) وبنسبة مئوية(٩.٧%) هذا يشير إلى أن تغيير كلمة المرور يعتبر إجراءً أقل شيوعًا،

وربما يحتاج إلى مزيد من الاهتمام من قبل الأفراد، بشكل عام، يمكن استنتاج أن الأفراد مركز الامن السيبراني يركزون على تأمين حساباتهم الشخصية وتجنب الروابط المجهولة، يليهم استخدام برامج الفحص، ثم تجنب مشاركة البيانات الشخصية، وأخيرًا تغيير كلمة المرور، هذه النتائج قد تعكس الوعي بأهمية الأمن السيبراني والاحتياجات التدريبية المحتملة.

رابعاً: استراتيجيات المستخدمة للعلاقات العامة في صفحة مركز الامن السيبراني:

جدول رقم (٩) يبين الفئات الفرعية للفئة الرئيسية (استراتيجيات المستخدمة للعلاقات العامة في صفحة مركز الامن السيبراني)

ت	الفئة	التكرار	النسبة المئوية	المرتبة
١	استراتيجية المسؤولية الاجتماعية	٣٩	%٢٩.٣	الاولى
٢	استراتيجية بناء المعاني	٣٥	%٢٦.٣	الثانية
٣	استراتيجية الحوار	٣٣	%٢٤.٨	الثالثة
٤	استراتيجية الاعلام	٢٦	%١٩.٥	الرابعة
المجموع		١٣٣	%١٠٠	

يبين جدول رقم (٩) ان استراتيجية المسؤولية الاجتماعية: حصلت على المرتبة الأولى بتكرار (٣٩) وبنسبة مئوية(٢٩.٣%) هذا يشير إلى أن هذه الاستراتيجية تحظى بأهمية كبيرة وقد تكون الأكثر استخدامًا أو تأثيرًا في السياق المعني، اما عن استراتيجية بناء المعاني: جاءت في المرتبة الثانية بتكرار (٣٥) و بنسبة مئوية (٢٦.٣%) هذا يشير إلى أن بناء المعاني يمثل جزءًا كبيرًا من الاستراتيجيات المستخدمة، وقد يكون له تأثير كبير في تحقيق الأهداف، في حين استراتيجية الحوار: حصلت على المرتبة الثالثة بتكرار (٣٣) وبنسبة (٢٤.٨%)هذا يشير إلى أن الحوار يمثل جزءًا مهمًا من الاستراتيجيات، وقد يكون له دور كبير في تحقيق النتائج المرجوة، واستراتيجية الإعلام: جاءت في المرتبة الرابعة بتكرار (٢٦) وبنسبة مئوية(١٩.٥%)هذا يشير إلى أن الإعلام يمثل جزءًا مهمًا، ولكنه أقل من الاستراتيجيات الأخرى في هذه الدراسة.

بشكل عام، يمكن استنتاج أن استراتيجية المسؤولية الاجتماعية هي الأكثر شيوعًا أو تأثيرًا، تليها استراتيجية بناء المعاني، ثم استراتيجية الحوار، وأخيرًا استراتيجية الإعلام. هذه النتائج قد تعكس الأولويات أو التوجهات في السياق المعني.

المحور الثاني: فئات الشكل (كيف قيل)؟

تضمنت فئات الشكل بتحليل مضمون منشورات مركز الامن السيبراني المختص في الاختراق المعلومات عبر موقع الفيس بوك للمدة (٢٠٢٤/١٢/٢٠) لغاية (٣٠/ ٢٠٢٥/٣) وبلغ عدد المنشورات خلال هذه الفترة (١٣٣) محيطة بمجموعة من الفئات رئيسية بلغ عددها (٦) وهي (التقنيات والبرامج والمواقع الالكترونية المستهدفة للاختراق السيبراني، الفنون الصحفية، مصادر الصفحة، وسائل الابراز، الجمهور المستهدف) وفئات الفرعية بلغ عددها(٢٥) فئة، وفيما يلي عرض الفئات بالتفصيل.

أولا: فئة التقنيات والبرامج والمواقع الالكترونية المستهدفة للاختراق السيبراني:

جدول رقم (١٠) يبين الفئات الفرعية للفئة الرئيسية الاولى في فئات الشكل وهي(التقنيات والبرامج والمواقع الالكترونية المستهدفة للاختراق السيبراني)

ت	الفئة	التكرار	النسبة المئوية	المرتبة

١	توجيه الشركات العالمية للتعامل مع معالجات الثغرات الالكترونية	٤٣	%٣٢.٣	الاولى
٢	اجهزة الهواتف الشخصية	٣٤	%٢٥.٥	الثانية
٣	اجهزة الحاسوب	٢٨	%٢١.١	الثالثة
٤	ارسال برمجيات ضارة الى اجهزة الكمبيوتر	١٨	%١٣.٥	الرابعة
٥	المواقع التواصل الاجتماعي مثل الفيس بوك	٧	%٥.٢	الخامسة
٦	البرامج المستخدمة مثل وتساب وغيرها	٢	%١.٥	السادسة
٧	الرسائل البريد SMS	١	%٠.٧٥	السابعة
المجموع		١٣٣	%١٠٠	

يبين الجدول (١٠) ان توجيه الشركات العالمية للتعامل مع معالجات الثغرات الالكترونية حصل على المرتبة الأولى بتكرار (٤٣) وبنسبة مئوية بلغت (٣٢.٣%)، مما يشير إلى أهمية دور الشركات العالمية في معالجة الثغرات الالكترونية، أجهزة الهواتف الشخصية جاءت في المرتبة الثانية بتكرار(٣٤) وبنسبة مئوية(٢٥.٥%)، مما يشير إلى أهمية أمان الهواتف الشخصية في مواجهة التهديدات السيبرانية، أجهزة الحاسوب حصلت على المرتبة الثالثة بتكرار (٢٨) وبنسبة مئوية (٢١.١%)، مما يشير إلى أهمية أمان الحواسيب في حماية البيانات والمعلومات، في حين ان إرسال برمجيات ضارة إلى أجهزة الكمبيوتر جاء في المرتبة الرابعة بتكرار(١٨) وبنسبة مئوية (١٣.٥%)، مما يشير إلى خطورة البرمجيات الضارة على أجهزة الكمبيوتر، اما عن المواقع التواصل الاجتماعي مثل الفيس بوك حصلت على المرتبة الخامسة (٧ تكرارات) وبنسبة مئوية(٥.٢%)، مما يشير إلى أهمية أمان المواقع الاجتماعية، تليها البرامج المستخدمة مثل واتساب وغيرها جاءت في المرتبة السادسة (٢ تكرار) وبنسبة مئوية(١.٥%)، مما يشير إلى أهمية أمان البرامج المستخدمة، وحصلت الرسائل البريدية على المرتبة السابعة (١ تكرار) وبنسبة مئوية (٠.٧٥%)، مما يشير إلى خطورة الرسائل البريدية في نقل التهديدات السيبرانية، هذه النتائج قد تعكس أهمية التوعية بأمان المعلومات والتهديدات السيبرانية المختلفة، أن التوعية بأمان المعلومات والتهديدات السيبرانية تعتبر ضرورية في مواجهة التحديات السيبرانية المتزايدة. النتائج تشير إلى أهمية دور الشركات العالمية في معالجة الثغرات الإلكترونية، وأمان الهواتف الشخصية والحواسيب، والبرمجيات الضارة، ومواقع التواصل الاجتماعي، والبرامج المستخدمة، والرسائل البريدية. من خلال التركيز على هذه المجالات، يمكن تعزيز الأمن السيبراني وحماية البيانات والمعلومات من التهديدات السيبرانية.

ثانيا: الفنون الصحفية المستخدمة في منشورات الصفحة المركز الامن السيبراني:

جدول رقم(١١) يبين الفئات الفرعية للفئة الرئيسية (الفنون الصحفية المستخدمة في منشورات الصفحة المركز الامن السيبراني)

ت	الفئة	التكرار	النسبة المئوية	المرتبة
١	الخبر	٧٠	%٥٢.٦	الاولى
٢	التقرير	٦٣	%٤٧.٤	الثانية
٣	التحقيق	٠	%٠	-
٤	المقال	٠	%٠	-
المجموع		١٣٣	%١٠٠	

يوضح الجدول رقم (١١) ان الخبر حصل على المرتبة الأولى (٧٠ تكرار) وبنسبة مئوية (٥٢.٦%)، مما يشير إلى أهمية الأخبار في هذا السياق، ان التقرير جاء في المرتبة الثانية بتكرار (٦٣) وبنسبة مئوية (٤٧.٤%)، مما يشير إلى أهمية التقارير في تقديم المعلومات، النتائج تشير إلى أن الأخبار والتقارير يشكلان الجزء الأكبر من المحتوى، بينما لم تظهر أي نتائج للتحقيق والمقال، هذه النتائج قد تعكس تفضيل تقديم الأخبار والتقارير في هذا السياق.

ثالثا: مصادر الصفحة لمركز الامن السيبراني:

جدول رقم (١٢) يبين الفئة الفرعية للفئة الرئيسية (مصادر الصفحة لمركز الامن السيبراني)

ت	الفئة	التكرار	النسبة المئوية	المرتبة
١	توجيهات الوزير الداخلية	٤٥	%٣٣.٨	الاولى
٢	الشركات الالكترونية	٤١	%٣٠.٨	الثانية
٣	مساهمة المصادر المحلية	٤٠	%٣٠.١	الثالثة
٤	التعاون مع الوزارات الحكومية الاخرى	٧	%٥.٢	الرابعة
المجموع		١٣٣	%١٠٠	

النتائج الجدول (١٢) تشير إلى أن توجيهات الوزير الداخلية حصلت على المرتبة الأولى بتكرار(٤٥) وبنسبة مئوية(٣٣.٨%)، تليها الشركات الالكترونية بتكرار(٤١) وبنسبة مئوية بلغت(٣٠.٨%)، ثم مساهمة المصادر المحلية بتكرار(٤٠) وبنسبة مئوية(٣٠.١%). بينما حصل التعاون مع الوزارات الحكومية الأخرى على المرتبة الرابعة (٧ تكرارات) وبنسبة مئوية (٥.٢%)هو أن توجيهات وزير الداخلية والشركات الإلكترونية والمصادر المحلية تلعب دورًا هامًا في تعزيز الأمن السيبراني، وتشير النتائج إلى أهمية التعاون بين مختلف الجهات لمواجهة التهديدات السيبرانية يمكن أن تساهم هذه الجهود في تعزيز الأمن السيبراني وحماية البيانات والمعلومات من التهديدات السيبرانية.

رابعاً: وسائل الابراز الصفحة لمركز الامن السيبراني:

جدول رقم (١٣) يبين الفئات الفرعية للفئة الرئيسية (وسائل الابراز الصفحة لمركز الامن السيبراني)

ت	الفئة	التكرار	النسبة المئوية	المرتبة
١	اقتران النص مع الصورة	٦٧	%٥٠.٣	الاولى
٢	النص	٥٠	%٣٧.٦	الثانية
٣	الرابط الالكتروني	١٢	%٩	الثالثة
٤	فيديو	٣	%٢.٣	الرابعة
٥	اقتران النص مع الفيديو	١	%٠.٨٠	الخامسة
٦	الصورة	٠	٠	-
المجموع		١٣٣	%١٠٠	

يوضح الجدول رقم (١٣) اقتران النص مع الصورة: حصل على المرتبة الأولى بتكرار(٦٧) وبنسبة مئوية (٥٠.٣%)، مما يشير إلى فعالية استخدام الوسائط المتعددة في إيصال المعلومات، في حين ان النص: جاء في المرتبة الثانية بتكرار(٥٠) وبنسبة مئوية (٣٧.٦%)، مما يدل على أهمية النصوص في تقديم المعلومات، اما الرابط الإلكتروني: حصل على المرتبة الثالثة بتكرار(١٢) وبنسبة مئوية (٩%)، مما يشير إلى استخدام الروابط الإلكترونية في توفير المزيد من المعلومات ، وحصل الفيديو: جاء في المرتبة الرابعة

(٣ تكرارات) وبنسبة مئوية(٢.٣%)، مما يشير إلى استخدام الفيديو في بعض الأحيان، وفي المرتبة الاخيرة اقتران النص مع الفيديو: حصل على المرتبة الخامسة بنسبة (١ تكرار) وبنسبة مئوية(٠.٨٠%)، مما يشير إلى قلة استخدام هذا النوع من المحتوى، ويمكن استنتاج هو أن استخدام الوسائط المتعددة، خاصة اقتران النص مع الصورة، يعتبر فعالًا في مجال الأمن السيبراني، حيث يمثل النسبة الأكبر من المحتوى المستخدم. هذا يشير إلى أهمية استخدام أساليب تواصل متعددة لتعزيز الفهم والتواصل في هذا المجال.

خامساً: الجمهور المستهدف في صفحة لمركز الامن السيبراني:

جدول رقم (١٤) يبين الفئات الفرعية للفئة الرئيسية (الجمهور المستهدف في صفحة لمركز الامن السيبراني)

ت	الفئة	التكرار	النسبة المئوية	المرتبة
١	الجمهور العام	٦٠	%٤٥.١	الاولى
٢	الجمهور الخاص	٤٣	%٣٢.٣	الثانية
٣	الجمهور الحكومات	٢٦	%١٩.٥	الثالثة
٤	المنظمات	٤	%٣	الرابعة
المجموع		١٣٣	%١٠٠	

يبين جدول رقم (١٤) ان الجمهور العام: حصل على المرتبة الأولى بتكرار(٦٠) وبنسبة مئوية (٤٥.١%)، مما يشير إلى أهمية توعية الجمهور العام بأمن المعلومات، في حين الجمهور الخاص: جاء في المرتبة الثانية بتكرار (٤٣) وبنسبة مئوية (٣٢.٣%)، مما يدل على أهمية حماية البيانات الشخصية للجمهور الخاص، اما عن الجمهور الحكومي: حصل على المرتبة الثالثة بتكرار(٢٦) وبنسبة مئوية (١٩.٥%)، مما يشير إلى أهمية أمن المعلومات في القطاع الحكومي، واخيرا المنظمات: جاء في المرتبة الرابعة (٤ تكرارات) وبنسبة مئوية (٣%)، مما يشير إلى أهمية أمن المعلومات في المنظمات، وهذا يشير هو أن الجمهور العام والخاص يعتبران الفئات الأكثر أهمية في مجال الأمن السيبراني، حيث حصلتا على النسبتين الأعلى في التكرار، مما يستدعي ضرورة التركيز على توعية وتثقيف هذه الفئات بأمن المعلومات لتعزيز الأمن السيبراني.

الاستنتاجات:

١- ان الوقاية من الاختراق السيبراني وتأمين الحسابات الشخصية أمران مهمان للغاية يأتي تجنب التعامل مع الروابط التي تنتحل صفحات مواقع مستعارة في المرتبة الثالثة، وأن هذا الأمر مهم.وكذلك أن فهم كيفية التعامل مع الروابط الالكترونية المجهولة وتجنب التعامل مع الروابط الالكترونية التي تنتحل اسماء مستعارة أمران أقل أهمية.

٢- يبدو أن الكشف عن ملفات الغير الرسمية وعرض المواقع المخترقة والكشف عن انتحال الصفحات المشهورة والمعروفة أمور مهمة، يأتي الكشف عن ملفات الغير الرسمية في المرتبة الأولى، مما يشير إلى أن هذا الأمر أكثر أهمية.

٣- أن اختراق الحسابات الشخصية هو التهديد الأكثر شيوعًا، يليه اختراق البيانات المركزية للمؤسسات، ثم استخدام الصفحات الوهمية. هذه النتائج قد تعكس نقاط الضعف في الأمن السيبراني التي تحتاج إلى معالجة لتحسين الأمان والحماية.

٤- أن الأنشطة التدريبية والتوعوية تلعب دوراً هاماً في تعزيز الأمن السيبراني، حيث جاءت الدورات التدريبية المستمرة في المرتبة الأولى، تليها المحاضرات التوعوية وورش العمل. هذه الأنشطة تساهم في تعزيز الوعي والمهارات اللازمة للتعامل مع التهديدات السيبرانية، وتشير إلى أهمية الاستثمار في التدريب والتوعية لتحسين الأمن السيبراني.

٥- أن الأفراد مركز الامن السيبراني يركزون على تأمين حساباتهم الشخصية وتجنب الروابط المجهولة، يليهم استخدام برامج الفحص، ثم تجنب مشاركة البيانات الشخصية، وأخيرًا تغيير كلمة المرور، هذه النتائج قد تعكس الوعي بأهمية الأمن السيبراني والاحتياجات التدريبية المحتملة.

٦- أن التوعية بأمان المعلومات والتهديدات السيبرانية تعتبر ضرورية في مواجهة التحديات السيبرانية المتزايدة. النتائج تشير إلى أهمية دور الشركات العالمية في معالجة الثغرات الإلكترونية، وأمان الهواتف الشخصية والحواسيب، والبرمجيات الضارة، ومواقع التواصل الاجتماعي، والبرامج المستخدمة، والرسائل البريدية من خلال التركيز على هذه المجالات، يمكن تعزيز الأمن السيبراني وحماية البيانات والمعلومات من التهديدات السيبرانية.

٧- أن الجمهور العام والخاص يعتبران الفئات الأكثر أهمية في مجال الأمن السيبراني، حيث حصلتا على النسبتين الأعلى في التكرار، مما يستدعي ضرورة التركيز على توعية وتثقيف هذه الفئات بأمن المعلومات لتعزيز الأمن السيبراني.

التوصيات:

١- زيادة في انشاء الدورات التدريبية والتوعوية التي تساهم في تعزيز الوعي وكسب المهارات اللازمة للتعامل مع التهديدات السيبرانية مع الافراد والمؤسسات لحفظ المعلومات.

٢- ضرورة الكشف عن الجهات التي تخترق الحسابات الشخصية والمؤسسية أو الصفحات المخترقة لخلق حالة من تأكيد على وجود الهجمات السيبرانية الاضرار الناتجة عنها مثل الابتزاز الالكتروني.

٣- ضرورة وضع مجموعة من الاجراءات لتأمين الحسابات الشخصية قبل التصفح في الصفحات الوهمية مثل وضع البرامج الوقائية أو البرامج التي تكشف عن وجود تهديد سيبراني يكون بمثابة جهاز مبكر قبل الاختراق.

المراجع:

وهيب مجيد الكبيسي، القياس النفسي بين النظرية والتطبيق، بيروت: مؤسسة مصر مرتضى للكتاب العراقي، ٢٠١٠.

خالد عبد الحق، دعاء عبد العال، العلاقات العامة الرقمية، عمان: دار اليازوري العلمية ، ٢٠٢٥. عادل عبد الصادق، الاقتصاد الرقمي، القاهرة: المركز العربي للابحاث الفضاء الالكتروني، ٢٠٢٠.

عبد الرزاق الدليمي ، العلاقات العامة وإدارة الازمات، ط٢، عمان: دار اليازوري العلمية ، ٢٠١٥.

فارس محمد العمارات، ابراهيم محمد الحماصة، الامن السيبراني المفهوم وتحديات العصر، عمان: دار الخليج، ٢٠٢٢.

محمد أبراهيم الزيدي، العلاقات العامة والإعلام الرقمي ،عمان: دار غيداء للنشر والتوزيع، ٢٠١٧.

مؤيد خلف حسين الدليمي، اتجاهات الصحافة المصرية نحو السياسة الأمريكية في العراق، اطروحة دكتوراه غير منشورة، كلية الإعلام، جامعة بغداد، ٢٠٠٨.
مصدر من الانترنيت، تاريخ الدخول ١٥/٥/ ٢٠٢٥ https://bakkah.com/ar/knowledge-cente
1-Resources Magagment Association USA, Cyber Crime, Hershey PA: IGI Global Information, 2012.

***:References**

1-Wahib Majid Al-Kubaisi, Psychometrics Between Theory and Practice Beirut: Mu'assasat Misr Murtada lil-Kitab al-Iraqi, 2010.
2-Khalid Abdul Haq, Doaa Abdul Aal, Digital Public Relations, Amman: Dar Al-Yazouri Al-Ilmiyah, 2025. Adel Abdul Sadek, Digital Economy, Cairo: Arab Center for Research and Electronic Space, 2020.
3-Abdul Razaq Al-Dulaimi, Public Relations and Crisis Management, 2nd edition, Amman: Dar Al-Yazouri Al-Ilmiyah, 2015.
4- Faris Muhammad Al-Amarat, Ibrahim Muhammad Al-Hamasa, Cyber Security: Concept and Challenges of the Era, Amman: Dar Al-Khaleej, 2022.
5- Muhammad Ibrahim Al-Zidi, Public Relations and Digital Media, Amman: Dar Ghaidaa for Publishing and Distribution, 2017.
6- Muayyad Khalaf Hussein Al-Dulaimi, Trends of Egyptian Press Towards American Policy in Iraq, Unpublished PhD thesis, College of Media, University of Baghdad, 2008.

ملحق:

١- نشر في صفحة مركز الامن السيبراني بتاريخ ٢٦/ديسمبر/ ٢٠٢٤ موضوع عن استراتيجية الحماية المتعددة الطبقات.
٢- نشر في صفحة مركز الامن السيبراني بتاريخ ١٢/ يناير/ ٢٠٢٥ اصدرت شركة cisco لمعالجة ثغرة الالكترونية.
٣- نشر في صفحة مركز الامن السيبراني بتاريخ ٢٥/ يناير / ٢٠٢٥ اختراق الموقع الوتساب.
٤- نشر في صفحة مركز الامن السيبراني بتاريخ ٦/ فبراير/ ٢٠٢٥ عن الخطاب الكراهية والطائفية.
٥- نشر في صفحة مركز الامن السيبراني بتاريخ ٨ / فبراير / ٢٠٢٥ رصد تقرير الى تسريب الحسابات.
٦- نشر في صفحة مركز الامن السيبراني ١٩ / فبراير / ٢٠٢٥ تقارير عن ملفات الاختراق السيبراني.
٧- نشر في صفحة مركز الامن السيبراني يوم ٥/ مارس / ٢٠٢٥ محاضرة.