واقع تطبيق ممارسات النظافة الرقمية في جامعات محافظة بني سويف: دراسة ميدانية

The reality of implementing digital hygiene practices in universities in Beni Suef Governorate: a field study

إعداد

فاطمة علي إبراهيم أحمد
مدرس مساعد قسم علوم المعلومات

أ.د. رحاب يوسف
أستاذ ورئيس قسم علوم المعلومات

د/ وليد محمود السيد
قسم نظم المعلومات-كلية الحاسبات والذكاء الاصطناعي-جامعة بني سويف

كلية الآداب جامعة بني سويف

تاريخ الإرسال	تاريخ القبول	تاريخ النشر
٢٠٢٢/١٠/٣	٢٠٢٢/١١/٢٩	٢٠٢٣/٤/١

المستخلص

تناولت الدراسة موضوع ممارسات النظافة الرقمية في جامعات محافظة بني سويف. وهدفت إلى معرفة الفروق بين كلًا من جامعة بني سويف، وجامعة النهضة، والجامعة التكنولوجية الحديثة في تطبيق ممارسات النظافة الرقمية وذلك من خلال قياس اتجاهات أعضاء هيئة التدريس ومعاونيهم بكل جامعة من هذه الجامعات تجاه تطبيق تلك الممارسات، وقد اعتمدت الدراسة على المنهج الوصفي التحليلي والدراسة المقارنة لتحقيق هدف الدراسة باستخدام الاستبانة كأداة من أدوات جمع البيانات تتلاءم مع طبيعة الموضوع وقد تم توزيعها على عينة من مجتمع الدراسة. وقد خرجت الدراسة بعدة نتائج أهمها أن جامعة بني سويف أفضل من جامعة النهضة من حيث نسب تعرضها للاختراق والحوادث السيبرانية، أن الجامعة التكنولوجية بحاجة للمزيد من التطوير للنهوض بذاتها، وعليه قد أوصت الدراسة بضرورة مواكبة التغيرات والتطورات التكنولوجية من قبل جامعة النهضة لتحقيق التقدم في مجال الأمن والحماية.

Abstract

The study dealt with the issue of digital hygiene practices in the universities of Beni Suef Governorate. It aimed to know the differences between Beni Suef University, Al-Nahda University, and the Modern University of Technology in applying digital hygiene practices by measuring the attitudes of faculty members and their assistants in each of these universities towards the application of these practices. The study relied on the descriptive analytical approach and comparative study to achieve the goal of the study, the questionnaire was used as a data collection tool that is compatible with the nature of the topic and has been distributed to a sample of the study population. The study came out with several results, the most important of which is that Beni Suef University is better than Al-Nahda University in terms of rates of exposure to hacking and cyber incidents, that the University of Technology needs more development to advance itself, and accordingly the study recommended the need to keep pace with changes and technological

developments by Al-Nahda University to achieve progress in the field of security and protection.

أولًا : المقدمة المنهجية:

إن موضوع النظافة الرقمية موضوع ذو أهمية كبيرة للغاية نظرًا لما تحققه ممارسات النظافة الرقمية من حفظ الأمان والحماية للأفراد والمؤسسات على اختلاف أنواعها فمن منا اليوم لا يستخدم التكنولوجيا ووسائلها ومن منا اليوم لا يقوم بتصفح الإنترنت عشرات المرات خلال يومه ومن ثم كان لابد وأن يكون هناك سبلًا للحماية من الهجمات والاختر اقات وحلًا للقراصنة والهواة وهنا يأتي دور الأمن السيبر اني والنظافة الرقمية حيث يقومان بحماية المستخدم أثناء تعاملاته مع الأجهزة والشبكات كذلك يعملان على تأمين بيانته الحساسة وحمايتها من المتطفلين ويتبين من خلال هذا البحث النتائج التي تم التوصل إليها إثر إجراء الدراسة الميدانية على عينة مجتمع الدراسة.

مشكلة الد راسة:

من الموضوعات التي تفرض نفسها على الساحة العلمية في عصر هذا موضوع الأمن السيبر اني والنظافة الرقمية، ورغم ذلك إلا أننا نسمع كل يوم عن حوادث الاختراق والهجمات الإلكترونية، سواء أكان ذلك لأفراد أو مؤسسات بعينها فعلى سبيل المثال لا الحصر في عام ٢٠١٨ شهدت ٦٢٪ من المؤسسات هجمات تصيد وهندسة اجتماعية، وأن ٥٪ فقط من مجلدات هذه الشركات محمية بشكل جيد، وفي النصف الأول من عام ٢٠١٩ كانت نسبة الانتهاكات المرتكبة بدو افع مادية ٧١٪، وأن ٢٥٪منها كانت بهدف التجسس. (varonis.2020). ومن هنا جاءت مشكلة الدراسة للرد على التساؤل التالي ماهي الإجراءات التي تقوم بها جامعات محافظة بني سويف لتحقيق الحماية من الهجمات والأمان لها وللعاملين بها؟

أهد اف الد راسة:

هدفت هذه الدراسة إلى التعرف على مدى وعي أعضاء هيئة التدريس ومعاونيهم بجامعات محافظة بني سويف بموضوع النظافة الرقمية، وممارسات تطبيقها التي يتبعونها.

تساؤلات الد راسة:

أجابه الدراسة عن التساؤل التالي: ما مدى وعي أعضاء هيئة التدريس ومعاونيهم بجامعات محافظة بني سويف بموضوع النظافة الرقمية وممارسات تطبيقها؟

حدود الدراسة:

الحدود الموضوعية: تناولت الدراسة ممارسات النظافة الرقمية المتبعة من قبل أعضاء هيئة التدريس ومعاونيهم بجامعات محافظة بني سويف.

الحدود المكانية: جامعات محافظة بني سويف

الحدود النوعية: تم تطبيق الدراسة على أعضاء هيئة التدريس والهيئة المعاونة من العاملين بجامعات محافظة بني سويف.

منهج الدراسة وأدواتها:

اعتمدت الدراسة على المنهج الوصفي التحليلي والدراسة المقارنة لتحقيق الهدف من الدراسة وذلك باستخدام أداة جمع البيانات الاستبانة.

مجتمع الدراسة وعينته: يضم مجتمع الدراسة جامعات محافظة بني سويف وهم (جامعة بني سويف، جامعة النهضة، الجامعة التكنولوجية الحديثة، الجامعة الأهلية) وقد اقتصرت الدراسة على الجامعات الأولى الثلاث نظرًا لأن الجامعة الأهلية تحت الإنشاء وسوف تبدأ الدراسة بها في الفترة ٢٠٢٢-٢٠٢٣م.

وقد اقتصرت عينة الدراسة من أعضاء هيئة التدريس بالجامعات الثلاث على أخذ نسبة عشوائية مقدرة ب ١٠٪ من جامعة بني سويف وبلغت ٣٠٠ مشاركًا حيث أن عدد أعضاء هيئة التدريس ومعاونيهم بجامعة بني سويف يبلغ ٣٠٠٠, وعند توزيع استمارات الاستبانة قامت الباحثة بتوزيع ٥٠٠ استبانة لمراعاة ما سيكون فاقدًا للمحاولة بالاحتفاظ بالنسبة المئوية قدر الإمكان ولكن لم يصلح من الاستبانات للتحليل سوى ٢٢٥ استبانة فقط، وبالنسبة لجامعة النهضة فيبلغ عدد المُعينين بها تقريبًا ١٩٠ عضو تم توزيع ١٠٠ إستبانة عليهم ولكن ما كان صالحًا للتحليل ٣٢ استبانة فقط، وبالنسبة للجامعة التكنولوجية فبلغ عدد المُعينين بها ١٠ أعضاء تم توزيع ١٠ استبانات عليهم و ما كان صالحًا منهم للتحليل ٨ استبانات.

مصطلحات الدراسة:

١- الأمن السيبراني: عبارة عن مجموع الوسائل التقنية والإدارية التي يتم استخدامها لمنع الوصول غير المصرح به وسوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات الشخصية ولحماية المواطنين، والمستهلكين في الفضاء السيبراني (غسان، ٢٠١٩).

٢- النظافة الرقمية Digital hygiene: مصطلح يستخدم لوصف نظافة أو عدم نظافة الوسيط الرقمي أو البنية الرقمية. ويمكن استخدامه لوصف رموز سطح المكتب، أو بنية الملف، أو عمليات المجلدات، أو ملفات "Photo shop" أو محرك الأقراص الثابتة أو صفحة شخصية على الـ" Facebook (cyborganthropology.2012).

الدراسات السابقة:

لقد وجد الباحثون في هذا الموضوع صعوبة الوصول لدراسات عربية سابقة تتعلق بهذه النقطة ولكن يمكن عرض مجموعة من الدراسات ذات الصلة بالموضوع باللغة الأجنبية بشكل عام فيما يلي:

Ossip, Silja-Madli.(2017). Cyber threats and cybercrime – a disruption of human security?

إهتمت هذه الدراسة بالعلاقة بين الفرد والأمن السيبراني من خلال بحث أكثر دقة حول موضوع الفضاء الإلكتروني والتهديدات التي يشكلها لمستخدمي الإنترنت، كما قامت الباحثة بعمل إستبيان لإستطلاع رأي عينة من المشاركين عبر الإنترنت لمعرفة مدى وعيهم بالتهديدات السيبرانية، وأن نتائج هذه الإستبانة سيتم تحليلها وفق مفهوم الأمن البشري لاستكشاف مستوى الاضطراب الناشئ عن التهديدات المختلفة.

Buczak, Anna L. & Guven, Erhan (2016). A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection.

إهتمت هذه الدراسة المسحية بدراسة استقصائية للمؤلفات المركزة حول التعلم الآلي (ML) وأساليب استخراج البيانات (DM) للتحليلات السيبرانية لدعم الكشف عن التسلل. حيث يتم توفير أوصاف البرنامج التعليمي القصير لكل طريقة ML/ DM. وبناءً على عدد الاستشهادات أو أهمية طريقة ناشئة، تم تحديد وقراءة وتلخيص الأوراق التي تمثل كل طريقة. نظرًا لأن البيانات مهمة جدًا في نهج ML/DM، يتم وصف بعض مجموعات البيانات الإلكترونية المعروفة المستخدمة في ML/ DM. يتم تناول تعقيد خوارزميات ML/DM، وتقديم مناقشة التحديات المتعلقة باستخدام ML/DM للأمن السيبراني، وتقديم بعض التوصيات حول وقت استخدام طريقة معينة.

Vural, Y., Aydos, M., & Tekerek, M. (2016) Protection of national cyber security: Awareness & education.

تناولت هذه الدراسة الهجمات السيبرانية وكيفية حدوثها وأن هذه الهجمات هى أكبر التهديدات التي تواجه الأمن، وقد كانت تحدث في السنوات السابقة دون تمييز في الأهداف، ولكنها أصبحت في السنوات الأخيرة منظمة ومعتمدة وموجهة نحو نظم المعلومات الوطنية. وقد هدفت الدراسة إلى: تحديد أنظمة المعلومات الوطنية الاستراتيجية، وصف أمن المعلومات الشخصية والمؤسسية التي تعتبر مراحل مهمة في توفير الأمن لنظم المعلومات الوطنية، مناقشة الاختبارات الأمنية اللازمة وأهمية التعليم والوعي إجراء تقييمات لأمن المعلومات الوطني. وأوصت الدراسة بالآتي: يجب تأسيس أمن المعلومات على مستوى الأفراد والمؤسسات من أجل تجنب تهديدات أمن المعلومات التي تحاول عرقلة أو حتى تدمير أمن المعلومات الوطني، وتتسبب في أضرار ملموسة وغير ملموسة على الأفراد والمؤسسات. من أجل تقليل تأثير مثل هذه التهديدات السيبرانية إلى الحد الأدنى على المستوى الوطني فهناك احتياطات ضرورية للمؤسسات والأمن الشخصي. يعد تأسيس المؤسسة وأمن المعلومات الشخصية التي تشكل مراحل تأسيس أمن المعلومات الوطني على أعلى مستوى ووضع سياسة للأمن القومي من بين الأشياء الأولى التي يجب القيام بها.

Chak, Stephanie K.. (2014). MANAGING CYBERSECURITY AS A BUSINESS RISK FOR SMALL AND MEDIUM ENTERPRISES.

أظهرت دراسات أمن المعلومات أن مجرد نشر المعلومات للجمهور كان ثاني أكبر سبب لخروقات البيانات بينما إتخذت هذه الدراسة إتجاه آخر في معالجة الموضوع حيث وضحت فكرة أن الوعي بأمن المعلومات يمكن أن يلعب دورا هاما في الحد من الخسائر الناجمة عن تلك الخروقات ، بالإضافة إلى توفر الهوية التنظيمية، كما تفترض الأدبيات الموجودة التي تمت مراجعتها في هذه الدراسة أيضًا أن المستخدم النهائي في كثير من الأحيان هو نقطة الفشل الأمني ، وأن الوعي بالكمبيوتر أو أمن المعلومات يعتبر واحدًا من أبسط الطرق للدفاع عن هجوم المنظمة. ومن المنطقي أنه مع استمرار كون المستخدم النهائي يهتم بدخول الأجهزة المحمولة الضارة، البريد الإلكتروني ، وغيرها من التعليمات البرمجية الضارة في المنظمات ، أن يتم استكشاف تحقيق في العلاقة بين السلوك الأمني والوعي الاستخباراتي مفتوح المصدر. تم تنفيذ هذا الاستكشاف من خلال البحث الكمي باستخدام استطلاع الوعي الأمني لمعهد SANS.

هذا وقد اتفقت الدراسة الحالية مع الدراسات السابقة في تناولها لموضوع ممارسات النظافة الرقمية بشكل خاص والأمن السيبراني بشكل عام واختلفت عنها في عينة التطبيق، والمؤشرات المستخدمة في الاستبانة لقياس مدى وعي أفراد العينة بها.

ثانيا الإطار النظري للدراسة:

ممارسات النظافة الرقمية:

لممارسات النظافة الرقمية أهمية كبيرة للغاية بالنسبة للأفراد والجامعات والمؤسسات بوجه_عام حيث تساعد على حمايتهم وحماية الأجهزة التي يستخدمونها كما تعمل على توفير بيئة آمنه لهم أثناء اتصالهم وتعاملهم مع شبكة الإنترنت خاصة بعدما أصبحنا في عالم رقمي كل من به يسعى إلى التحول الرقمي وإحلال التكنولوجيا في كل العمليات التي يقومون بها.

المقصود بالنظافة الرقمية:

" الممارسات والخطوات التي يتخذها مستخدمو أجهزة الكمبيوتر والأجهزة الأخرى للحفاظ على صحة النظام وتحسين الأمان عبر الإنترنت، وعادةً ما تكون هذه الممارسات جزءًا من روتين لضمان سلامة الهوية والتفاصيل الأخرى التي يمكن سرقتها أو إتلافها" (Brook، ٢٠١٨).

ممارسات النظافة الرقمية:

يوجد مجموعة من الإجراءات والممارسات التي قد تبدو روتينية والتي ينبغي إتباعها بانتظام لتحسين عملية أمن النظام بشكل كبير، والوقوف ضد التهديدات سواء أكانت داخلية أو خارجية، وهذه الممارسات والإجراءات يمكن إدراجها فيما يلي:

١- توثيق كافة المعدات والبرامج والتطبيقات الحالية عبر الإنترنت، وهذه المعدات والبرامج تشتمل بداخلها على ثلاثة أجزاء (Brook، ٢٠١٨):

أ- الأجهزة: بما فيها أجهزة الكمبيوتر، والأجهزة المتصلة (كالطابعات وأجهزة الفاكس)، والأجهزة المحمولة (مثل الهواتف الذكية والأجهزة اللوحية) (Brook، ٢٠١٨).

ب- البرامج: ويقصد بها جميع البرامج ، التي يستخدمها الجميع على شبكة معينة ، والتي يتم تثبيتها مباشرة على أجهزة الكمبيوتر (Brook، ٢٠١٨).

ج- التطبيقات: ويقصد بها تطبيقات الويب (مثل Google Drive, Dropbox) ، وتطبيقات الهواتف والأجهزة اللوحية وأي برنامج آخر لم يتم تثبيته مباشرة على الأجهزة (Brook، ٢٠١٨).

٢- تحليل قائمة المعدات والبرامج، وذلك لمعرفة نقاط الضعف، ومسح المعدات الغير مستخدمة والتخلص منها بالطريقة السليمة (Brook، ٢٠١٨)، وإن لم تكن البرامج قيد الاستخدام المنتظم ينبغي إلغاء تثبيتها بطريقة صحيحة، وتغيير كل كلمات مرور المستخدم،

كما يجب اختيار برامج وتطبيقات معينة لتكون الاختيار المخصص لوظائف معينة لجميع المستخدمين. على سبيل المثال، إذا تم استخدام كل من Google Drive و Dropbox لتخزين الملفات، فيجب اعتبار أحدهما أساسيًا والآخر يستخدم كنسخة احتياطية أو محذوف (Brook، ٢٠١٨).

١- ينبغي أن تمتلك المؤسسة برامج لمكافحة الفيروسات محددة لاستخدامها في فحص الأنظمة بانتظام (mckinsey.com، ٢٠١٩).

٢- إجراء تدقيق تكنولوجيا الأمن السيبر اني. والتأكد من أنه يتحقق من عوامل تصفية البريد العشو ائي والحماية من البرامج الضارة وما إلى ذلك (mckinsey.com، ٢٠١٩).

٣- تغيير كلمات المرور بانتظام كل ٣٠ يومًا أو التحقق من وجود تحديثات مرة واحدة على الأقل في الأسبوع. سيؤدي القيام بذلك إلى ضمان استمرار النظافة الرقمية لشبكتك الكاملة من الأجهزة والبرامج، وبالتالي الحماية من الأنشطة الضارة (Brook، ٢٠١٨).

٤- العمل على تحديث الأجهزة والبرامج باستمرار لمنع حدوث المشكلات (Brook، ٢٠١٨) كذلك تحديث البرامج والتطبيقات فالغالبية العظمى من الهجمات السيبر انية تستغل نقاط ضعف البرامج والأجهزة المعروفة فقد كشف تقرير تحقيقات خرق البيانات الصادر سنة ٢٠١٥ أن ٧٠٪ من الهجمات الإلكترونية الناجحة استغلت نقاط الضعف المعروفة مع التصحيحات المتاحة. هذا يعني أنه كان بإمكان العديد من الضحايا منع خرق البيانات إذا ما قاموا بتحديث أنظمة التشغيل والتطبيقات الخاصة بهم (spiceworks.com، ٢٠٢٠). أيضًا تحديث الكاميرات الأمنية وأجهزة الصوت والفيديو وما إلى ذلك (Jadav,Dhaval&Wilson,Chuck، ٢٠١٨).

٥- أن يكون هناك محترف واحد على الأقل في مجال تكنولوجيا المعلومات من بين الموظفين، والالتزام بمعايير NIST أو ممارسات معايير UL 2900. (mckinsey.com, 2019)

٦- إضافة تأمين يغطي ممارسات العمل ضد مخاطر الإنترنت من الطرف الأول والطرف الثالث (mckinsey.com، ٢٠١٩).

٧- الاستعانة بخبرة أمنية خارجية للتحقق من الممارسات الأمنية الداخلية. مع عدم وضع ثقة كافية في أي موظف بمفرده لدرجة أن هذا الموظف يعرف كل شيء فمن الممكن حدوث خطأ. ينبغي الحفاظ على بعض الفصل في الواجبات لحماية المنظمة (mckinsey.com، ٢٠١٩).

٨- إدارة عمليات التثبيت الجديدة: ينبغي إجراء كل تثبيت جديد بشكل صحيح وتوثيقه للاحتفاظ بجرد محدث لجميع الأجهزة والبرامج (Brook، ٢٠١٨).

٩- معالجة الأخطاء، والعيوب لتحسين الاستقرار العام لنظام التشغيل أو التطبيق، وإصلاح الثغرة الأمنية إلى جانب التحديثات الأخرى مثل إصدارات النقاط (أو إصلاحات كاملة) لنظام التشغيل، فتُعد هذه الأمور من إجراءات الصيانة الوقائية الأساسية اللازمة للحفاظ على الآلات محدثة ومستقرة وآمنة من البرامج الضارة والتهديدات الأخرى (spiceworks.com، ٢٠٢٠)

١٠- تصحيح أجهزة الحاسب المحمولة والخوادم مبكرًا وبشكل متكرر فالبرامج غير المصححة، خاصة إذا كان أحد التطبيقات المستخدمة على نطاق واسع مثل Adobe Flash أو Internet Explorer، يمكن أن يكون نقطة جذب للبرامج الضارة والفيروسات. مثال على ذلك: فيروس Conficker على نظام التشغيل Windows الذي تم اكتشافه في أواخر عام ٢٠٠٨، والذي يستفيد من الإصدارات غير المصححة من Microsoft Windows (spiceworks.com, 2020).

١١- إحضار "متسلل أخلاقي" أو خبير في أمن الكمبيوتر لتقييم نقاط الضعف المحتملة (أي اختبار الاختراق الداخلي والخارجي) (Jadav,Dhaval&Wilson,Chuck، ٢٠١٨)

١٢- ينبغي القيام بتدريب مفصل للموظفين للتوعية بالنظافة الرقمية وينبغي ان يشتمل هذا التدريب على موضوعات سلامة البيانات، والاستخدام السليم للبريد الإلكتروني وخلافه (Jadav,Dhaval&Wilson,Chuck، ٢٠١٨).

١٣- الحصول على تحديثات رقمية" شهرية أو سنوية لتذكير الموظفين ببروتوكولات الأمن السيبراني. يجب أن تكون جلسات التدريب التوعوية المستمرة هذه مطلوبة لجميع الموظفين وتتضمن تدريبًا في الموقع أو مقاطع فيديو للأمن السيبراني أو محاكاة للتصيد الاحتيالي أو ندوات عبر الإنترنت (Jadav,Dhaval&Wilson,Chuck، ٢٠١٨).

١٤- البحث عن مصدر لأي إخطارات تهديد على سبيل المثال: إذا تم اختراق DocuSign أو Google Docs، فيجب أن تكون على دراية بمصدر هذا الخرق (mckinsey.com، ٢٠١٩).

١٥- و ضع خطة للاستجابة للحوادث إذا كان هناك خرق أو تعرض لبرامج الفدية، فمن الضروري أن تتواجد خطة ومعرفة الخطوات التالية للحد من تعطل العمل ، و ايضًا العمل على تقييد الوصول المادي للشبكات (Jadav,Dhaval&Wilson,Chuck، ٢٠١٨).

١٦- التعرف على شبكات الشركاء المتصلة بالشبكة الخاصة بك، والتأكد باستمرار من وجود ضوابط الأمان التعويضية وتجزئة الشبكة في حالة تعرض شبكة الشريك للخطر (SEAL، ٢٠٢٠).

هذا وبعد ما تم عرضه من ممارسات النظافة الرقمية ترى الدراسة أنه في حالة تطبيقها سيؤدي هذا إلى القضاء على الهجمات أو بمعنى أدق القضاء على نسبة كبيره منها، ولعل ما يؤكد صدق هذه الرؤية الدراسة التي قام بها جيمس لويس James Lewis والتي هي بعنوان رفع مستوى الأمن السيبراني: "Raising the Bar for Cybersecurity." أن نسبة الانتهاكات الناجحة لشبكات الشركات والتي بلغت من ٨٠-٩٠٪ لم تتطلب فقط سوى تقنيات القرصنة الأساسية وقدرة المخترق على الصبر، وأن هذه الانتهاكات قد انخفضت بنسبة ٨٥٪ حال تطبيق بعض ممارسات النظافة الرقمية، وأن في بعض الحالات بلغت النسبة (صفر) وأن الإجراءات التي تم اتباعها لتقليل هذه الانتهاكات كانت كالتالي (Lewis,James A, 2013):

١- تقييد البرامج المصرح لها فقط للتشغيل على جهاز كمبيوتر أو شبكة؛ التصحيح في الوقت الفعلي للبرامج مثلPdf، وMicrosoft Office ومتصفحات الويب (Lewis,James A، ٢٠١٣).

- معالجة نقاط الضعف في نظام التشغيل مثل نظام التشغيل Microsoft Windows وLinux ونظام التشغيل Apple.
- تصحيح أخطا نظام التشغيل (Lewis,James A، ٢٠١٣).
- تقليل عدد الأشخاص على الشبكة الذين يتمتعون بامتيازات المسؤول، حيث إن طرق الاختراق تتم بإجراءات بسيطة جدًا (Lewis,James A، ٢٠١٣).

أيضًا مما يدلل على صدق هذه الرؤية ما ذكره Stephanie K Chak في دراسته نقلًا عن Vince Cerf أن أكثر من نسبة ٨٠ ٪ من الهجمات يمكن التعامل معها من خلال إجراءات النظافة الرقمية الأساسية، مثل: التصحيحات وكلمات المرور ومكافحة البرامج الضارة والجدران النارية، حتى عند وضع هذه الأدوات في مكانها الصحيح إذا تم تتم الصيانة الدورية، تصبح هذه الأدوات عديمة الفائدة (Chak، ٢٠١٥).

ثالثًا الإطار التطبيقي:

الخصائص الديموغرافية لعينة الدراسة: تناولت الدراسة خصائص عينة الدراسة من المنتمين لجامعات محافظة بني سويف من حيث (الجامعة، العمر، النوع، الدرجة العلمية).

وقدتم توزيع الاستبانة عليهم لمعرفة مدى وعيهم بمصطلح النظافة الرقمية وبعض المصطلحات الأخرى ذات الصلة وكذلك لمعرفة الممارسات التي يتبعونها من ضمن ممارسات النظافة الرقمية. وفيما يلي سنتناول توزيع أعداد المشاركين وفق الجامعة التابعون لها، وكذلك وفق جنسهم ودرجاتهم العلمية وأعمارهم ثم بعد ذلك الدخول في المؤشرات التي يمكن من خلالها الإيفاء بالغرض من الدراسة.

جدول (١) توزيع عدد المشاركين في الرد على الاستبانة وفق الجامعة

الجامعة	عدد المشاركين
جامعة بني سويف	٢٢٥
الجامعة التكنولوجية	٨
جامعة النهضة	٣٢

يوضح الجدول توزيع عدد المشاركين وفق كل جامعة ونلاحظ من خلاله أن العدد الأكبر جاء تبعًا لجامعة بني سويف تلاه بعد ذلك جامعة النهضة ثم التكنولوجية وهذا لأن الباحثة قامت بتوزيع ما يقرب من (٥٠٠) استبانة على جامعة بني سويف، ولكن لم يحظى بالقبول الصالح للاستخدام سوى ٢٢٥ استبانة فقط حيث أن هناك من الاستبانات ما جاء ناقصًا في الردود وقد بلغت نسبتهم (٦٥) استبانة، وفاقد (٢١٠) استبانة حيث أن بعض افراد العينة قد اعتذر عن ملء الاستبانة والبعض الآخر لم يقم بإرجاعه. وبالنسبة لجامعة النهضة فقد تم توزيع مئة استبانة، ولكن لم يقم بالرد سوى (٣٢ فقط). أما الجامعة التكنولوجية فقد تم توزيع (١٠) استبانات لأن المُعينين بالجامعة من الهيئة المعاونة يبلُغ عددهم (١٠) أفراد. أما بالنسبة للأعداد في جامعة بني سويف فيبلُغ (٣٠٠٠) عضو هيئة تدريس وهيئة معاونة، وجامعة النهضة يبلُغ عدد المُعينين بها ما يقرُب من (١٩٠) عضو.

جدول (٢) توزيع أفراد العينة حسب النوع

		التكرار	%
النوع	ذكر	144	54.3

	أنثى	121	45.7
	الإجمالي	265	100.0

يوضح هذا الجدول توزيع أفراد العينة بالجامعات الثلاث حسب الجنس ويتضح أن نسبة الذكور هي الأعلى مقارنًة بالإناث حيث جاء عدد الذكور المشاركين مئة وأربعة وأربعون ذكر ما يعادل نسبة مئوية ٥٤,٣ % في حين أن الإناث بلغت نسبتهم المئوية٤٥,٧ %، والأمر في ذلك يعود إلى أنه قد تم اختيار العينة عشوائيًا الأمر الذي جعل نسبة الذكور أكبر من الإناث. كما قد يكون السبب في ذلك راجعًا إلى حب الذكور لهذه الموضوعات عن الإناث.

جدول (٣) توزيع أفراد العينة حسب الجامعة

		التكرار	%	الإجمالي
الجامعة	جامعة بني سويف	225	84.9	84.9
	جامعة النهضة	32	12.1	97.0
	الجامعة التكنولوجية	8	3.0	100.0
	الإجمالي	265	100.0	-

الجدول هذا يوضح نسب أفراد العينة موزعه وفق الجامعات ويتضح أن أعلى نسبة مشاركين من جامعة بني سويف يليه جامعة النهضة ثم الجامعة التكنولوجية وهذا التفاوت والاختلاف قد نتج عن اختلاف نسب أفراد مجتمع الدراسة بكل جامعة حيث أن جامعة بني سويف عدد الأفراد بها من أعضاء هيئة التدريس والهيئة المعاونة (٣٠٠٠) ومن ثم قد تم أخذ عينة عشوائية بنسبة ١٠٪ من مجتمع الدراسة ولكن لم تتلقى الباحثة استبانات صالحة للتحليل سوى (٢٢٥) استمارة والبالغ نسبتهم ٨٤٪ ، وبالنسبة لجامعة النهضة فقد بلغت نسبة المشاركين منها ١٢,١٪ بما يعادل (٣٢ مفردة)، وهذا لأن عدد المُعينين بجامعة النهضة أقل كثيرًا من جامعة بني سويف حيث يقرُب عددهم من الـ (٢٠٠ فردًا)، أما بالنسبة للجامعة التكنولوجية فهذه كانت الأقل عددًا ونسبة مئوية حيث أن عدد المُعينين بها (١٠ أفراد) ما بين مُعيدين ومدرسين مساعدين وتم توزيع الاستبانة عليهم ولكن لم يُجب سوى (٨ أفراد فقط) ولذلك جاءت نسبتهم أقل نسبة حيثُ بلغت (٣,٠٪) من إجمالي حجم العينة.

جدول (٤) توزيع أفراد العينة حسب العمر

	التكرار	%	الإجمالي

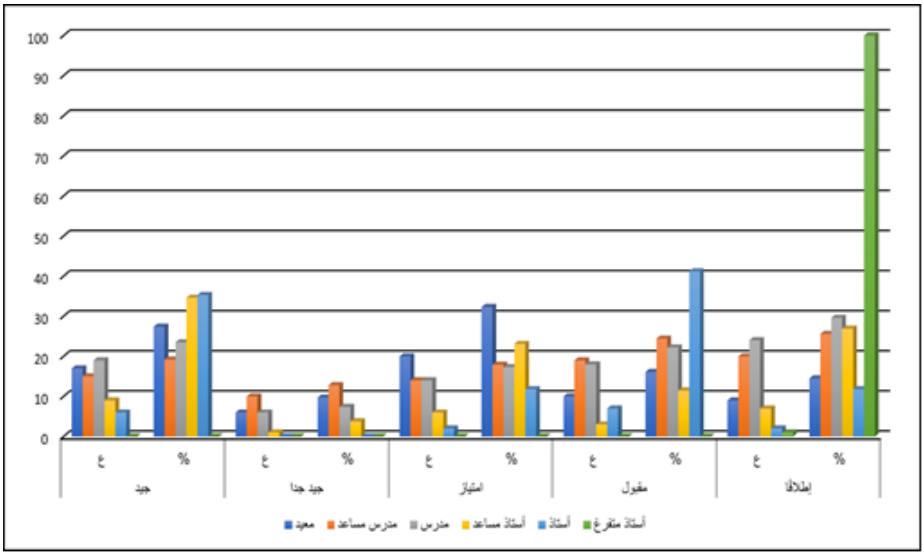
العمر	31-40	88	33.2	33.2
	21- 30	125	47.2	80.4
	41-50	44	16.6	97.0
	51فأكثر	8	3.0	100.0
	الإجمالي	265	100.0	-

يتضح من خلال الجدول السابق بيان بنسب المشاركين وفق أعمارهم والذي يوضح أن أعلى نسبة مشاركة قد جاءت من فئة الشباب الأعمار من (٢١-٣٠) حيث بلغ عددهم (١٢٥) بنسبة ٤٧٪ تلاهم في ذلك أصحاب الفئة العمرية من(٣١-٤٠) حيث بلغ عددهم (٨٨) بنسبة ٣٣,٢٪ تلاهم بعد ذلك الفئتين الأكبر سنًا من ٤١-٥٠ حيث بلغ عددهم (٤٤) بنسبة ١٦,٦٪ و ذوو الأعمار من ٥١ فأكثر وقد بلغوا (٨ مشاركين فقط) بنسبة ٣,٠٪ فهذه النسب توضح أنه كلما ذاد العمر كلما قلت نسب المشاركة الأمر الذي يُدلل على أن الشباب هم أكثر وعيًا بمصطلح النظافة الرقمية حيثُ أنه مصطلح جديد يرتبط بالتكنولوجيا أي أن أصحاب الأعمار الأقل هم أكثر استخداما للتكنولوجيا وبالتالي هم أكثر دراية بمصطلحاتها ويُمكننا أيضًا إثبات صحة هذه النتيجة أو نفيها فيما بعد مع تحليل النتائج الأخرى.

جدول (٥) الفروق بين أعضاء هيئة التدريس والهيئة المعاونة من حيث مدى الوعي بمصطلح النظافة الرقمية.

س	م	جيد		جيد جدا		امتياز		مقبول		إطلاقًا		الإجمالي	
		ع	%	ع	%	ع	%	ع	%	ع	%	ع	%
ما مدى وعيك بمصطلح النظافة الرقمية	معيد	١٧	٢٧,٤	٦	٩,٧	٢٠	٣٢,٣	١٠	١٦,١	٩	١٤,٥	٦٢	١٠٠
	مدرس	١٥	١٩,٢	١٠	١٢,٨	١٤	١٧,٩	١٩	٢٤,٤	٢٠	٢٥,٦	٧٨	١٠٠
	مدرس	١٩	٢٣,٥	٦	٧,٤	١٤	١٧,٣	١٨	٢٢,٢	٢٤	٢٩,٦	٨١	١٠٠
	أستاذ	٩	٣٤,٦	١	٣,٨	٦	٢٣,١	٣	١١,٥	٧	٢٦,٩	٢٦	١٠٠
	أستاذ	٦	٣٥,٣	٠	٠	٢	١١,٨	٧	٤١,٢	٢	١١,٨	١٧	١٠٠
	أستاذ	٠	٠	٠	٠	٠	٠	٠	٠	١	١٠٠	١	١٠٠

شكل رقم(١) الفروق بين أعضاء هيئة التدريس والهيئة المعاونة من حيث مدى الوعي بمصطلح النظافة الرقمية.



يوضح الجدول والشكل لسابقين مدى وعي أعضاء هيئة التدريس ومعاونهم بمصطلح النظافة الرقمية ويتبين من خلاله أن المعيدين هم أكثر وعيًا من الدرجة الممتازة عن غيرهم حيث بلغ عدد من يرى أنه على وعي بالمصطلح لحد الامتياز عشرون فردًا بنسبة ٣٢٪ تلاهم في ذلك الأساتذة المساعدين وبلغ عددهم ستة أفراد بنسبة ٢٣٪ تلاهم المدرسين المساعدين بنسبة ١٧,٩٪ والمدرسون بنسبة ١٧,٣٪. وكما كانت النسبة عالية في الأساتذة المساعدين من حيث التمكُن من معرفة المصطلح كانت عالية بينهم من حيث المعرفة الجيدة بالمصطلح فبلغت نسبة من أفادو ب (جيد) ٣٤,٦٪ بينما ارتفعت نسبة الأساتذة من حيث المعرفة بالمصطلح حيث بلغت نسبتهم ٣٥,٣٪. إذا فالواضح من هذا الجدول أن المعيدين والأساتذة المساعدين هم الأكثر وعيًا بالمصطلح هذه النتيجة سيتم تأكيدها أو نفيها من خلال النسب الموضحة في الجدول التالي والذي يعكس مفهوم مصطلح النظافة الرقمية والنسبة الصحيحة من العينة في اختياره. كما أن السبب في ارتفاع نسب المعيدين والأساتذة هي أن الأساتذة لديهم خبرات واسعة بالمصطلحات ومعانيها وذلك وفق طبيعة عملهم في بحوث الترقيات، وإشرافهم على الرسائل الجامعية ومناقشتها وبالتالي فهم ينقلون حصاد هذه الخبرة للمعيدين الذين يقومون بالإشراف عليهم.

جدول (٦) مفهوم النظافة الرقمية من وجهة نظر أعضاء هيئة التدريس والهيئة المعاونة

س	المتغيرات	الممارسات التي ينبغي على مديري أنظمة تكنولوجيا المعلومات ومستخدميها اتباعها من أجل تنظيم البيانات وحمايتها من السرقة وتعزيز الأمن السيبراني.		طرق مواجهة الهجمات التي تتم عبر الإنترنت لاختراق الشبكات.		مجموعة من الوظائف المتبعة لتحقيق أمان المستخدم عند التعامل مع الشبكة		لا أعلم		الإجمالي	
		ع	%	ع	%	ع	%	ع	%	ع	%
أيًا من العبارات التالية يشير إلى مفهوم النظافة الرقمية.	معيد	٣٠	٤٨,٤	١٠	١٦,١	٨	١٢,٩	١٤	٢٢,٦	٦٢	١٠٠
	مدرس مساعد	٣٦	٤٦,٢	١١	١٤,١	٢٢	٢٨,٢	٩	١١,٥	٧٨	١٠٠
	مدرس	٤١	٥٠,٦	١٢	١٤,٨	١٤	١٧,٣	١٤	١٧,٣	٨١	١٠٠
	أستاذ مساعد	١٨	٦٩,٢	٦	٢٣,١	٠	٠	٢	٧,٧	٢٦	١٠٠
	أستاذ	١١	٦٤,٧	٠	٠	٦	٣٥,٣	٠	٠	١٧	١٠٠
	أستاذ متفرغ	١	١٠٠	٠	٠	٠	٠	٠	٠	١	١٠٠

يتناول الجدول السابق ثلاثة من المفاهيم التي منها أثنين قريبين من مفهوم النظافة الرقمية والثالث هو الأدق والمعبر، حيث تعني النظافة الرقمية مجموعة الوظائف والممارسات المتبعة من قبل المستخدم لتحقيق الأمان له عند تعامله مع الأجهزة والشبكة، ومن خلال هذا المفهوم يتضح أن الأساتذة هم الأكثر وعيًا بالمفهوم الصحيح لمصطلح النظافة الرقمية حيث بلغت نسبتهم٣٥,٣٪ من إجمالي حجم العينة يليهم في ذلك المدرسين المساعدين والذين بلغت نسبتهم٢٨,٢٪. والسبب في ذلك لصغر سن المعيدين والمدرسين ومواكبتهم للتطورات التكنولوجية بما فيها مجال الأمن السيبراني والموضوعات المتعلقة به، كما أننا أصبحنا نحيا حياة رقمية ومن ثم أغلب الاتجاهات الحالية في البحوث العلمية تتجه نحو التكنولوجيا بتقنياتها ومصطلحاتها الجديدة هذا الأمر بالنسبة للمدرسين المساعدين أما بالنسبة للأساتذة فالأمر قريب من ذلك فهم من يشرفون على الرسائل الأكاديمية وهم من يعملون بلجان البحوث والترقيات وبالتالي هذا الأمر يجعلهم يتطرقون لكل ما هو جديد، ومن ثم نقل خبراتهم لمن هم أصغر منهم من طلابهم من المدرسين المساعدين والمعيدين، ونلاحظ أيضًا أن نسبة ٦٩٪ من الأساتذة المساعدين لم يعبروا عن مفهوم النظافة الرقمية بشكل صحيح وبالتالي هذا

يتنافى مع النتيجة الموجودة في الجدول السابق وقد يكون السبب في ذلك اختلاط الأمر عليهم في المفاهيم نظرًا لتقاربها من مفهوم النظافة الرقمية.

جدول (٧) المقصود بالأمن السيبراني من وجهة نظر أعضاء هيئة التدريس والهيئة المعاونة

س	المتغيرات	مجموعة العمليات المتبعة لتحقيق إحباط سرقة الأجهزة والمساس بمكوناتها المادية.		الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام.		حماية المعلومات من المخاطر التي تهددها		لا أعلم		الإجمالي	
		ع	%	ع	%	ع	%	ع	%	ع	%
ماذا يقصد بالأمن السيبراني.	معيد	٣	٤,٨	٣٤	٥٤,٨	١٠	١٦,١	١٥	٢٤,٢	٦٢	١٠٠
	مدرس مساعد	١١	١٤,١	٣٩	٥٠	١٥	١٩,٢	١٣	١٦,٧	٧٨	١٠٠
	مدرس	١٣	١٦	٣٤	٤٢	١١	١٣,٦	٢٣	٢٨,٤	٨١	١٠٠
	أستاذ مساعد	٤	١٥,٤	١٣	٥٠	٧	٢٦,٩	٢	٧,٧	٢٦	١٠٠
	أستاذ	٣	١٧,٦	٧	٤١,٢	٦	٣٥,٣	١	٥,٩	١٧	١٠٠
	أستاذ متفرغ	٠	٠	١	١٠٠	٠	٠	٠	٠	١	١٠٠

يتبين من الجدول السابق رقم (٧) أن مفهوم الأمن السيبراني والمُتمثل في "مجموع من الوسائل التقنية والإدارية التي يتم استخدامها لمنع الاستخدام غير المصرح به على شبكات الكمبيوتر، وسوء الاستغلال واستعادة المعلومات الالكترونية التي تحتويها بهدف ضمان واستمرار عمل نظم المعلومات وتأمين حماية وسرية وخصوصية البيانات سواءً الخاصة بالأفراد او الجهات في الفضاء السيبراني". وهو يوضح مدى الوعي بين أعضاء هيئة التدريس والهيئة المعاونة بمصطلح الأمن السيبراني والذي يبرز أن هناك نسب عالية من عينة الدراسة على وعي به حيث بالنظر إلى الأساتذة المتفرغين سنجد أنهم الأكثر وعيًا بمفهومه فقد بلغت نسبتهم ١٠٠٪، تلاهم في ذلك المعيدين وقد بلغت نسبته ٥٤,٨٪ ثم المدرسين المساعدين أما الأساتذة المساعدين فجاءت نسبتهم متماثلة حيث بلغ كلاً منهم نسبة ٥٠٪ تبعهم في ذلك المدرسين حيث بلغت نسبتهم ٤٢٪ ثم الأساتذة ونسبتهم ٤١,٢٪. وهذه النسب تُدلل على أن هناك وعي بمصطلح الأمن السيبراني أكثر من الوعي بمصطلح النظافة الرقمية، ربما لأن مصطلح الأمن السيبراني هو الأكثر شيوعًا والأقدم مقارنةً بمصطلح النظافة الرقمية. أما بالنسبة لاختلاف النسب بين أفراد العينة وارتفاعها في الأساتذة المتفرغين فربما يكون الأمر عائد لخبرتهم وعملهم في مجال الأمن السيبراني أو لوجودهم في القطاعات الإدارية وشغلهم

للمناصب العالية والتي تُحتم عليهم الإلمام بكافة الطرق والإجراءات الأمنية للمحافظة على البيانات الحساسة التي توجد تحت أيديهم. وبالنسبة للدرجات العلمية الأقل فربما قد انتقلت لهم خبرات من هم أعلى منهم أو لربما لتتبعهم كل ما هو جديد في مجال التكنولوجيا حيث أصبح الأمن السيبراني هو حديث الساعة خاصة بعد توجه الدولة إلى عمليات التحول الرقمي.

جدول (٨) مفهوم الهجمات الإلكترونية من وجهة نظر أعضاء هيئة التدريس والهيئة المعاونة.

س	المتغيرات	تلك الهجمات التي يتم من خلالها انتحال شخصية كيان موثوق به بغرض الإيقاع بالضحية إلكترونيًا.		هجوم يتم شنه من أحد أجهزة الكمبيوتر او مجموعة من الأجهزة		هجوم يتم من خلاله إحداث خلل في تطبيقات الويب		لا أعلم		الإجمالي	
		ع	%	ع	%	ع	%	ع	%	ع	%
أيًا من العبارات التالية يشير إلى الهجمات الإلكترونية.	معيد	١٩	٣٠,٦	٣٠	٤٨,٦	١٣	٢١	٠	٠	٦٢	١٠٠
	مدرس مساعد	٢٦	٣٣,٣	٣٩	٥٠	١٣	١٦,٧	٠	٠	٧٨	١٠٠
	مدرس	٣٦	٤٤,٤	٣٦	٤٤,٤	٩	١١,١	٠	٠	٨١	١٠٠
	أستاذ مساعد	١١	٤٢,٣	١١	٤٢,٣	٤	١٥,٤	٠	٠	٢٦	١٠٠
	أستاذ	٥	٢٩,٤	١١	٦٤,٧	١	٥,٩	٠	٠	١٧	١٠٠
	أستاذ متفرغ	٠	٠	١	١٠٠	٠	٠	٠	٠	١	١٠٠

يتبين من الجدول السابق أن الأساتذة المتفرغين هم الأكثر وعيًا بمفهوم الهجمات الإلكترونية والذي يعني "هجوم يتم شنه من أحد أجهزة الكمبيوتر او مجموعة من الاجهزة على جهاز كمبيوتر اخر او عدة أجهزة كمبيوتر او شبكات. ثم الأساتذة والذين تبلغ نسبتهم ٦٤,٧٪ يليهم المدرسين المساعدين بنسبة ٥٠٪ ثم المعيدين بنسبة ٤٨,٦٪، ويرجع التفاوت في هذ النسب إلى و اقع خبرة الأساتذة، والأساتذة المتفرغين ودرايتهم الواسعة بمفهوم هذه المصطلحات حيثُ أنهم هم القائمون بالإشراف على الرسائل العلمية، وهم أنفسهم المحكمون في لجان البحوث والترقيات ومن ثم هما أكثر خبرة ودراية من الأعمار والدرجات العلمية التي تصغرهم.

جدول (٩) المقصود باختراق البيانات من وجهة نظر أعضاء هيئة التدريس والهيئة المعاونة.

س	المتغيرات	التطفل على أجهزة الآخرين من خلال استغلال الثغرات		سرقة معلومات حساسة أو تسريبها		لا أعلم		الإجمالي	
		ع	%	ع	%	ع	%	ع	%
ماذا يقصد باختراق البيانات.	معيد	٢٥	٤٠,٣	١٧	٢٧,٤	٢٠	٣٢,٣	٦٢	١٠٠
	مدرس مساعد	٢٨	٣٥,٩	٢٩	٣٧,٢	٢١	٢٦,٩	٧٨	١٠٠
	مدرس	٣٢	٣٩,٥	٣٣	٤٠,٧	١٦	١٩,٨	٨١	١٠٠
	أستاذ مساعد	١٢	٤٦,٢	١٠	٣٨,٥	٤	١٥,٤	٢٦	١٠٠
	أستاذ	٩	٥٢,٩	٥	٢٩,٤	٣	١٧,٦	١٧	١٠٠
	أستاذ متفرغ	٠	٠	١	١٠٠	٠	٠	١	١٠٠

يوضح الجدول السابق رقم (٩) الفروق بين أعضاء هيئة التدريس ومعاونيهم تجاه المقصود باختراق البيانات والذي يقصد به : " التطفل على أجهزة الآخرين من خلال استغلال الثغرات الأمنية" سنجد الفروق كالتالي أن الأساتذة هم أكثر وعيًا بالمصطلح فقد بلغت نسبتهم ٥٢,٩٪، ثم الأساتذة المساعدين والذين بلغت نسبتهم٤٦,٢٪، والسبب في ذلك يعود إلى درايتهم الواسعة بهذه المصطلحات وخبرتهم التي حتمتها عملية البحث العلمي ورحلته الطويلة، كذلك عمليات البحث والتنقيب التي يقومون بها إثر عملهم في مجال بحوث الترقي إلى جانب رصيدهم المعرفي الناتج عن الإشراف ومناقشة الرسائل الأكاديمية.

المحور الثاني: الاستخدام والسلوكيات، يهدف هذا المحور إلى معرفة الاختلافات في سلوكيات أفراد العينة من حيث التعامل مع كلمات المرورواستخدامها...

جدول (١٠) الفروق الفردية بين الذكوروالإناث من حيث التعامل مع كلمات المرور.

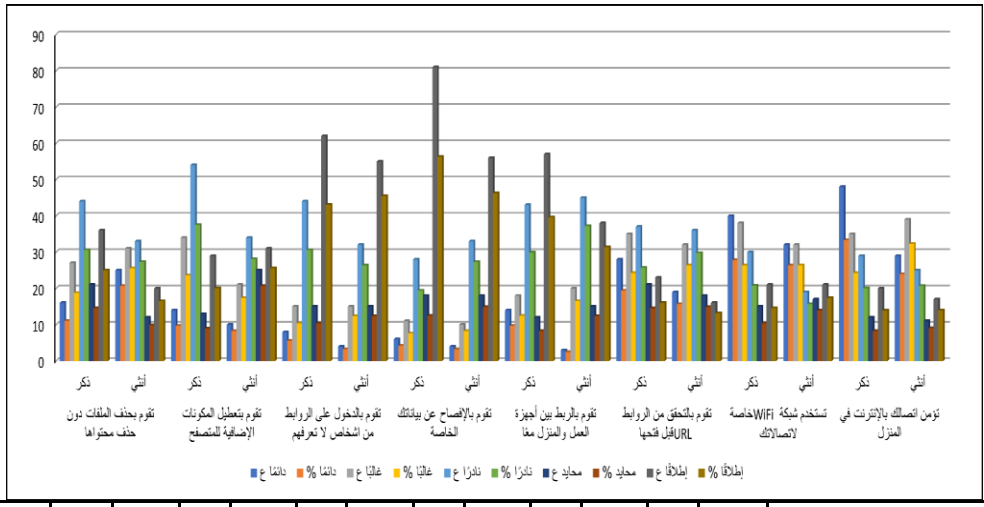
س	النوع	دائمًا		غالبًا		نادرًا		محايد		إطلاقًا		الإجمالي	
		ع	%	ع	%	ع	%	ع	%	ع	%	ع	%
مشاركة كلمات المرور	ذكر	٨	٥,٦	١٥	١٠,٤	٤٠	٢٧,٨	٨	٥,٦	٧٣	٥٠,٧	١٤٤	١٠٠
	أنثي	٦	٥	١٤	١١,٦	٣٨	٣١,٤	٦	٥	٥٧	٤٧,١	١٢١	١٠٠
اختيار كلمات المرور	ذكر	٦	٤,٢	٢٧	١٨,٨	٣٥	٢٤,٣	١٦	١١,١	٦٠	٤١,٧	١٤٤	١٠٠
	أنثي	٩	٧,٤	٢٢	١٨,٢	٤١	٣٣,٩	١٣	١٠,٧	٣٦	٢٩,٨	١٢١	١٠٠
حفظ كلمات المرور	ذكر	٧	٤,٩	١٤	٩,٧	٢٦	١٨,١	٨	٥,٦	٨٩	٦١,٨	١٤٤	١٠٠
	أنثي	١٤	١١,٦	١٠	٨,٣	٢١	١٧,٤	١١	٩,١	٦٥	٥٣,٧	١٢١	١٠٠
اختيار كلمات المرور من القاموس	ذكر	٥	٣,٥	٢٠	١٣,٩	٢٨	١٩,٤	١٨	١٢,٥	٧٣	٥٠,٧	١٤٤	١٠٠
	أنثي	٧	٥,٨	٦	٥	٣٢	٢٦,٤	١٥	١٢,٤	٦١	٥٠,٤	١٢١	١٠٠

يوضح الجدول السابق الاختلاف بين الذكور والإناث في التعامل مع كلمات المرور، فبالنظر إلى مشاركة كلمات المرور سنجد أن النسبة الأكبر من الذكور لا تقوم بمشاركتها حيث بلغ عدد الذكور الذين لا يقومون بمشاركة كلمات المرور على الإطلاق٧٣ ذكرًا بنسبة ٥٠,٧٪ من إجمالي عدد الذكور (١٤٤)، ونسبة ٢٧,٨٪ من النادر من الذكور يقومون بمشاركة كلمة المرور وقلة قليلة منهم بلغت ٥,٦٪ هم من يشاركون كلمات المرور دائمًا. أما بالنسبة للإناث فنسبة من لا يشاركن كلمات المرور مطلقًا بلغت٤٧,١٪ ومن النادر مشاركتها بلغت ٣١,٤٪ ومن تشاركن دائمًا بلغن ٥٪. ومن حيث اختيار كلمات مرور يسهل تخمينها اتضح أن الإناث هم أعلى معدل من الذكور من حيث دائما ما يختارون كلمات مرور سهلة فبلغت نسبتهن ٧,٤٪ مقارنًة بنسبة الذكور التي بلغت ٤,٢٪، كما جاءت نسب الإناث أقل من نسب الذكور في عدم اختيار كلمات مرور سهلة حيث بلغت نسبتهن ٢٩٪.٩ مقارنة بنسبة الذكور التي بلغت ٤١,٧٪.

وكما اختلفت النسب في النقطتين السابقتين اختلفت أيضًا في طريقة حفظ كلمة المرور حيث النسبة الأعلى من الإناث يقمن بحفظ كلمات المرور الخاصة بهن أسفل لوحة المفاتيح، وبالتالي فما الداعي من حفظها إذاً؟! بلغت نسبة الإناث في ذلك ١١,٦٪ مقارنة بالذكور ٤,٩٪ وهذه النتيجة متسقة مع سابقيها وتؤكد صحة النتيجتين السابقتين. أما بالنسبة للطريقة التي يتم بها اختيار كلمات المرور فسنلاحظ أن الذكور كانوا أكثر دقة من الإناث من حيث اختيار كلمات مرور من القاموس أو عدمه فقد بلغت نسبة قلة منهم يختارون من القاموس حيث تمثلت نسبتهم في ٣,٥٪ مقارنة بالإناث اللاتي بلغن نسبتهن ٥,٨٪. ومن خلال هذه النسب يمكن القول: أن الذكور هم أكر دقة وتحفظًا من الإناث في التعامل مع كلمات المرور، رغم أن هذا يُنافي الثقافة العربية والتي من المفترض أن تكون الإناث فيها أكثر دقة وملاحظة وتحفظًا. الأمر الثاني أن بهذا الشكل ستُصبح الإناث أكثر عُرضة للهجمات وبالتالي هذا سيؤثر عليهن وعلى عمل المؤسسة التي ينتمين إليها.

جدول (١١) يوضح الفروق بين الذكور والإناث من حيث السلوكيات لبعض الاستخدام

س	النوع	دائمًا		غالبًا		نادرًا		محايد		إطلاقًا		الإجمالي	
		ع	%	ع	%	ع	%	ع	%	ع	%	ع	%
تقوم بحذف الملفات دون حذف محتواها	ذكر	16	11.1	27	18.8	44	30.6	21	14.6	36	25	١٤٤	١٠٠
	أنثي	25	20.7	31	25.6	33	27.3	12	9.9	20	16.5	١٢١	١٠٠
تقوم بتعطيل المكونات الإضافية للمتصفح	ذكر	14	9.7	34	23.6	54	37.5	13	9	29	20.1	١٤٤	١٠٠
	أنثي	10	8.3	21	17.4	34	28.1	25	20.7	31	25.6	١٢١	١٠٠
تقوم بالدخول على	ذكر	8	5.6	15	10.4	44	30.6	15	10.4	62	43.1	١٤٤	١٠٠



الروابط من اشخاص لا تعرفهم	أنثي	4	3.3	15	12.4	32	26.4	15	12.4	55	45.5	١٢١	١٠٠
تقوم بالإفصاح عن بياناتك الخاصة	ذكر	6	4.2	11	7.6	28	19.4	18	12.5	81	56.3	١٤٤	١٠٠
	أنثي	4	3.3	10	8.3	33	27.3	18	14.9	56	46.3	١٢١	١٠٠
تقوم بالربط بين أجهزة العمل والمنزل معًا	ذكر	14	9.7	18	12.5	43	29.9	12	8.3	57	39.6	144	100
	أنثي	3	2.5	20	16.5	45	37.2	15	12.4	38	31.4	121	100
تقوم بالتحقق من الروابط URL قبل فتحها	ذكر	28	19.4	35	24.3	37	25.7	21	14.6	23	16	144	100
	أنثي	19	15.7	32	26.4	36	29.8	18	14.9	16	13.2	121	100
تستخدم شبكة WiFi خاصة لاتصالاتك	ذكر	40	27.8	38	26.4	30	20.8	15	10.4	21	14.6	144	100
	أنثي	32	26.4	32	26.4	19	15.7	17	14	21	17.4	121	100
تؤمن اتصالك بالإنترنت في المنزل	ذكر	48	33.3	35	24.3	29	20.1	12	8.3	20	13.9	144	100
	أنثي	29	24	39	32.3	25	20.7	11	9.1	17	14	121	100

شكل (٢) يوضح الفروق بين الذكور والإناث من حيث السلوكيات لبعض الاستخدام

يتناول الجدول السابق رقم (١١) والشكل رقم (٢) الاختلافات الموجودة بين سلوكيات الذكور والإناث من حيث بعض الاستخدامات كما سيتضح: بالنسبة لحذف الملفات التي تحتوي على بيانات نجد أن نسبة ٣٠,٦٪ من الذكور نادرًا ما تقوم بحذف الملف دون حذف البيانات الموجودة بداخله وأن نسبة ١١,١٪ منهم من يقومون بحذف الملف بالكامل دون حذف المحتوى. في حين تقل النسبة في الإناث من حيث الندرة في حذف الملفات دون حذف المحتوى والتي بلغت ٢٧,٣٪ في حين كانت النسبة لمن قُمن بحذف الملفات دون حذفها محتواها من حيث الديمومة في فعل ذلك 20.7%.

بالنسبة لتعطيل المكونات الإضافية للمتصفح سنلاحظ أن ٩,٧٪ من الذكور دائمًا ما يقومون بتعطيل المكونات الإضافية للمتصفح حال عدم استخدامها وأن ٢٣,٦٪ منهم غالبًا ما يقومون بتعطيلها في حين تنخفض النسب عند الإناث حيث إن نسبة ٨,٣٪ من الإناث يقُمن بتعطيل المكونات الإضافية حال عدم الاستخدام وأن ١٧,٤٪ منهُن يقُمن غالبًا بتعطيلها أي أن الذكور أفضل من الإناث.

بالنسبة للدخول على الروابط المجهولة سنجد أن الذكور أعلى في معدل الدخول عن الإناث فقد بلغت نسبة الذكور الذين دائمًا ما يدخلون على الروابط المجهولة ٥,٦٪ مقارنة بالإناث البالغ نسبتهن ٣,٣٪ بينما ازدادت نسبة الإناث اللاتي غالبًا ما يدخُلن إلى المواقع المجهولة حيث بلغت ١٢,٤٪ مقارنةً بالذكور الذين بلغت نسبتهم ١٠,٤٪، ولكن بالنظر إلى النسبتين الأخيرتين من حيث الندرة والإطلاق سنجد أن الذكور أقل من الإناث في معدل الدخول إلى الروابط المجهولة. بالنسبة للإفصاح عن البيانات الخاصة سنلاحظ أن الإناث أقل نسبة من الذكور في الإفصاح دائمًا عن بيانتهن حيث بلغت النسبة ٣,٣٪ من الإناث يقُمن بذلك مقارنًة بالذكور البالغ نسبتهم ٤,٢٪، وان نسبة 27.3 % من الإناث نادرًا ما يفعلن ذلك في ين كانت نسبة الذكور١٩,٤٪. ربما يكون السبب في ذلك طبيعة الإناث التحفظية وذلك وفق عادات وثقافة المجتمع.

بالنسبة للربط بين أجهزة العمل والمنزل معًا يتضح أن الذكور أعلى نسبة من الإناث حيث بلغت نسبتهم من حيث الربط دائمًا٩,٧٪ في حين كانت نسبة الإناث ٢,٥٪. التحقق من الروابط، نسبة١٩,٤٪ من الذكور دائمًا ما يتحققون من الروابط قبل فتحها، بينما انخفضت النسبة إلى١٥,٧٪ من الإناث. استخدام شبكة Wifi خاصة للاتصالات الذكور أيضًا أعلى معدل في ذلك من الإناث حيث بلغ نسبة من يلجأون من الذكور دائمًا إلى استخدام شبكة خاصة ٢٧,٨٪ مقارنة بالإناث البالغ نسبتهن٢٦,٤٪. وأخيرًا تأمين الاتصال بالإنترنت في المنزل، ارتفع معدل الذكور عن الإناث في ذلك أيضًا حيث بلغت نسبت الذكور الذين يقومون بتأمين اتصالهم في المنزل ٣٣,٣٪ مقارنةً بالإناث٢٤٪. فهذه النسب تؤكد وتُبرهن على صدق النتائج المستخلصة في الجدول السابق وكون إن الإناث يتفوقون على الذكور في نقطة أو إثنين فهذا لا ينفي مطلقًا النتيجة السابقة وهي أن الذكور أفضل من الإناث من حيث سلوكيات الاستخدام الموضح بالجدولين أعلاه رقم (١٠،١١).

ثالثًا محور الكفاءة الذاتية لاستخدام الكمبيوتر: يقيس مدى كفاءة أعضاء هيئة التدريس بالجامعات الثلاث نحو استخدام أجهزة الكمبيوتر.

جدول (١٢) يوضح الفروق بين جامعة بني سويف والنهضة والتكنولوجية في التعامل مع الأجهزة والمعدات.

س	الجامعة	نعم		لا		الإجمالي	
		ع	%	ع	%	ع	%
هل لديك القدرة على التعامل مع الأجهزة والمعدات التقنية؟	جامعة بني سويف	١٨٦	٨٢,٧	٣٩	١٧,٣	٢٢٥	١٠٠
	جامعة النهضة	٢٧	٨٤,٤	٥	١٥,٦	٣٢	١٠٠
	الجامعة التكنولوجية	٧	٨٧,٥	١	١٢,٥	٨	١٠٠

يتضح من الجدول السابق أن الجامعة التكنولوجية الحديثة هي الأعلى مُعدلًا من حيث القدرة على التعامل مع الأجهزة والمعدات التقنية حيث بلغت نسبتها ٨٧,٥٪ يليها في ذلك جامعة النهضة وتمثلت النسبة بها ٨٤,٤٪ ثم جامعة بني سويف حيث بلغت نسبتها ٨٤,٧٪. والسبب في ذلك يعود إلى أن الجامعة التكنولوجية المُعينين بها أغلبهم من كليتي هندسة وحاسبات، وأن المشاركين من جامعة النهضة كانوا من كليات طب وعلاج طبيعي وصيدلة وحاسبات وهذه الكليات أكثر تعاملاتها مع الأجهزة والمعدات، وبالنظر إلى جامعة بني سويف سنلاحظ أن أغلب المشاركين بها كانوا من كليات نظرية ولذلك يُمكن القول أن ما جعل نظيراتها يتفوقوا عليها هو طبيعة تخصصات المشاركين في الرد على الاستبيان.

جدول (١٣) يوضح الفروق بين جامعة بني سويف والنهضة والتكنولوجية من حيث عمل التحديثات وصيانة الأجهزة

س	الجامعة	دائمًا		غالبًا		نادرًا		محايد		إطلاقًا		الإجمالي	
		ع	%	ع	%	ع	%	ع	%	ع	%	ع	%
هل تستطيع عمل التحديثات اللازمة لجهازك	جامعة بني سويف	20	8.9	29	12.9	85	37.8	31	13.8	60	26.7	٢٢٥	١٠٠
	جامعة النهضة	1	3.1	6	18.8	8	25.0	13	40.6	٤	١٢,٥	٣٢	١٠٠
	الجامعة التكنولوجية	٠	٠	1	12.5	2	25.0	2	25.0	3	37.5	٨	١٠٠
هل يمكنك القيام بأعمال	جامعة بني سويف	64	28.4	52	23.1	70	31.1	22	9.8	17	7.6	٢٢٥	١٠٠
	جامعة	5	15.6	٤	١٢,٥	٧	٢١,٩	١٤	٤٣,٨	٢	٦,٣	٣٢	١٠٠

الصيانة الأساسية لأجهزتك؟	النهضة												
	الجامعة التكنولوجية	١	١٢,٥	٣	٣٧,٥	١	١٢,٥	١	١٢,٥	٢	٢٥	٨	١٠٠

يتضح من خلال الجدول السابق أن جامعة النهضة أعلى معدلًا من حيث القدرة على عمل تحديثات الأجهزة فبلغت نسبتها ١٨,٨٪ يليها في ذلك جامعة بني سويف١٢,٩٪ الجامعة التكنولوجية ١٢,٥٪. بينما تفوقت جامعة بني سويف على كلا من النهضة والتكنولوجية في صيانة الأجهزة حيث بلغت جامعة بني سويف نسبة ٢٨,٨٪ يليها النهضة بنسبة ١٥,٦٪ ثم التكنولوجية بنسبة ١٢,٥٪. وهذا عكس النتائج الواردة في الجدول السابق، و أنه يوضح أن كل جامعة منهم تفوقت عن الأخرى في نقطة معينة ومن ثم يمكن القول بأن لا جامعة أفضل من الأخرى في هذا السياق إلى أن يثبُت العكس.

رابعًا محور الموثوقية:

جدول (١٤) الفروق بين أعضاء هيئة التدريس والهيئة المعاونة من حيث الموثوقية في تنزيل الملفات، استخدام المو اقع، رسائل البريد الإلكتروني، تقييد الوصول.

س	م	دائمًا		غالبًا		نادرًا		محايد		إطلاقًا		الإجمالي	
		ع	%	ع	%	ع	%	ع	%	ع	%	ع	%
تقوم بتنزيل الملفات الغير موثوقة باستخدام الإنترنت	معيد	1	1.6	13	21.0	19	30.6	4	6.5	25	40.3	٦٢	١٠٠
	مدرس مساعد	6	7.7	9	11.5	27	34.6	5	6.4	31	39.7	٧٨	١٠٠
	مدرس	6	7.4	11	13.6	39	48.1	4	4.9	21	25.9	٨١	١٠٠
	أستاذ مساعد	٣	١١,٥	١٠	٣٨,٥	٩	٣٤,٦	١	٣,٨	٣	١١,٥	٢٦	١٠٠
	أستاذ	٤	٢٣,٥	٤	٢٣,٥	٥	٢٩,٤	١	٥,٩	٣	١٧,٦	١٧	١٠٠
	أستاذ متفرغ	٠	٠	٠	٠	١	١٠٠	٠	٠	٠	٠	١	١٠٠
تستخدم الإنترنت في الدخول إلى مو اقع الويب المجهولة	معيد	٥	٨,١	٥	٨,١	١٩	٣٠,٦	٤	٦,٥	٢٩	٤٦,٨	٦٢	١٠٠
	مدرس مساعد	٦	٧,٧	٦	٧,٧	٢٨	٣٥,٩	٦	٧,٧	٣٢	٤١	٧٨	١٠٠
	مدرس	٥	٦,٢	١٠	١٢,٣	٣٢	٣٩,٥	١٠	١٢,٣	٢٤	٢٩,٦	٨١	١٠٠
	أستاذ مساعد	٤	١٥,٤	٣	١١,٥	١١	٤٢,٣	٤	١٥,٤	٤	١٥,٤	٢٦	١٠٠
	أستاذ	٣	١٧,٦	٥	٢٩,٤	٦	٣٥,٣	٠	٠	٣	١٧,٦	١٧	١٠٠
	أستاذ	٠	٠	٠	٠	٠	٠	١	١٠٠	٠	٠	١	١٠٠

	متفرغ											
التعامل مع رسائل البريد الإلكتروني ذات الروابط المجهولة	معيد	٣	٤,٨	٤	٦,٥	٢٢	٣٥,٥	٢	٣,٢	٣٢	٥٠	٦٢	١٠٠
	مدرس مساعد	6	7.7	7	9.0	17	21.8	10	12.8	38	48.7	٧٨	١٠٠
	مدرس	6	7.4	5	6.2	32	39.5	9	11.1	29	35.8	٨١	١٠٠
	أستاذ مساعد	2	7.7	٥	١٩,٢	٧	٢٦,٩	٤	١٥,٤	٨	٣٠,٨	٢٦	١٠٠
	أستاذ	٣	١٧,٦	٤	٢٣,٥	٤	٢٣,٥	١	٥,٩	٥	٢٩,٤	١٧	١٠٠
	أستاذ متفرغ	٠	٠	٠	٠	٠	٠	١	١٠٠	٠	٠	١	١٠٠
تقوم بتقييد الوصول عن بعد بمعنى التأكد من أن الاتصال مشفر بشكل صحيح	معيد	٩	١٤,٥	21	33.9	16	25.8	5	8.1	11	17.7	٦٢	١٠٠
	مدرس مساعد	12	15.4	١٨	٢٣,١	٢٦	٣٣,٣	١٥	١٩,٢	٧	٩	٧٨	١٠٠
	مدرس	١٠	١٢,٣	١٤	١٧,٣	٣٣	٤٠,٧	١٢	١٤,٨	١٢	١٤,٨	٨١	١٠٠
	أستاذ مساعد	٥	١٩,٢	١١	٤٢,٣	٩	٣٤,٦	٠	٠	١	٣,٨	٢٦	١٠٠
	أستاذ	٥	٢٩,٤	٧	٤١,٢	٤	٢٣,٥	٠	٠	١	٥,٩	١٧	١٠٠
	أستاذ متفرغ	٠	٠	٠	٠	١	١٠٠	٠	٠	٠	٠	١	١٠٠

يتناول الجدول السابق الاختلافات بين أعضاء هيئة التدريس ومعاونيهم من حيث عدم تنزيل الملفات غير الموثوقة من الإنترنت نجد أن النسبة الأعلى في عدم تنزل ملفات مجهولة كانت نسبة المعيدين وتمثلت في ٤٠,٣ تلاها المدرسين المساعدين وبلغت نسبتهم 39.7 % م المدرسين البالغ نسبتهم ٢٩,٩٪ ثم الأساتذة بنسبة ١٧,٦٪ وأخيرًا الأساتذة المساعدين بنسبة ١١,٥٪. وهذا يُدلل على مدى وعي الشباب بخطورة تنزيل الملفات غير الموثوقة كما يُبرهن على مغامرة الأساتذة المساعدين، الأساتذة المتفرغين حيث بلغت نسبة الأساتذة المتفرغين في عدم تنزيل مثل هذه الملفات (٠).

مو اقع الويب المجهولة: نجد من خلال الجدول أن النسبة الأكبر لعدم الدخول للمو اقع المجهولة عبر الويب قد جاءت متمثلة في المعيدين حيث بلغت نسبتهم ٤٦,٨٪ تلاهم المدرسين المساعدين بنسبة ٤١٪ والمدرسين جاءت نسبتهم مقدرة بـ ٢٩,٦ % والأساتذة المساعدين بنسبة ١٥,٤٪ والأساتذة بنسبة ١٧,٦٪ والأساتذة المتفرغين ٠٪. رسائل البريد الإلكتروني :٥٠٪ من المعيدين لا يقومون بالضغط على الرو ابط المجهولة في رسائل البريد الإلكتروني،٤٨,٧٪ من المدرسين المساعدين لا يفعلون ذلك، و أيضًا المدرسين بنسبة ٣٥,٨٪ ونسبة ٣٠,٨٪ في حين كانت

نسبة الأساتذة ٢٩,٤٪ والأساتذة المتفرغين٠٪ مما يؤكد أن المعيدين أكر حرصًا من غيرهم على تجنب مثل هذه الرسائل يليهم المدرسين المساعدين. من حيث تشفير الاتصال بشكل صحيح سنلاحظ ٢٩,٩٪ من الأساتذة يقومون بتشفير الاتصال مقارنة بنسبة مئوية ٠٪ من الأساتذة المتفرغين لم يقوموا بذلك.

وعليه من خلال هذه النسب يتبين أن المعيدين هم أكثر فئة على دراية بممارسات النظافة الرقمية يليهم المدرسين الساعدين الأمر، وإن كان هذا الأمر يُظهر أنه على مُتنافي مع النتائج الموجودة في جداول المفاهيم إلا أن هناك فارق فيما بين الدراية بالمفاهيم والمصطلحات والدراية باستخدام التكنولوجيا وتقنياتها وممارستها ومن ثم يُمكن القول بأنهم قد أخطأوا في التعبير عن المفهوم، ولكنهم على وعي كبير بالممارسات التي من شأنها تحقيق النظافة الرقمية وتأمين أنفسهم عند التعامل مع الأجهزة والشبكة.

جدول (١٥) مقارنة بين أعضاء هيئة التدريس والهيئة المعاونة من حيث التخلص من المعلومات الحساسة

س	م	عن طريق حذف محتوى الملف ثم حذف الملف بالكامل.		عن طريق حذفها من خلال الأمر Shift Delate		عن طريق حذفها بسلة المهملات.		بيانات مفقودة		الإجمالي	
		ع	%	ع	%	ع	%	ع	%	ع	%
كيف تقوم بالتخلص من المعلومات الحساسة أو الشخصية؟	معيد	13	21.0	20	32.3	28	45.2	1	1.6	٦٢	١٠٠
	مدرس مساعد	19	24.4	26	33.3	33	42.3	.	.	٧٨	١٠٠
	مدرس	19	23.5	32	39.5	30	37.0	.	.	٨١	١٠٠
	أستاذ مساعد	2	7.7	18	69.2	6	23.1	.	.	٢٦	١٠٠
	أستاذ	2	11.8	11	64.7	4	23.5	.	.	١٧	١٠٠
	أستاذ متفرغ	.	.	.	.	١	١٠٠	.	.	١	١٠٠

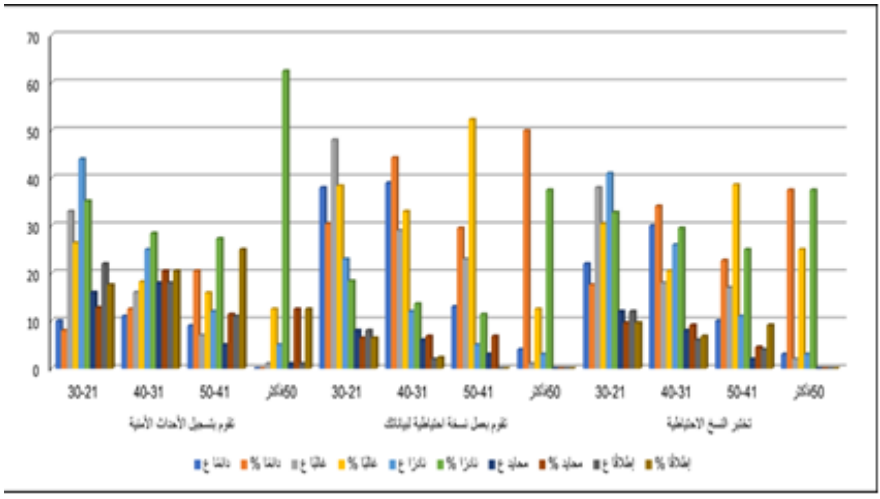
يوضح الجدول السابق رقم (١٥) الفروق بين أعضاء هيئة التدريس ومعاونهم من حيث التخلص من المعلومات الحساسة ويتبين من خلاله أن الشائع بين المعيدين والمدرسين المساعدين والأساتذة المتفرغين للتخلص منها هو حذفها مباشرةً عن طريق سلة المهملات حيث بلغت نسبة الأساتذة المتفرغين١٠٠٪، تلاهم المعيدين في ذلك ٤٥,٢٪، والمدرسين المساعدين٤٢,٣٪. وربما يكون المبرر لذلك هو سهولة عملية الحذف بهذه الطريقة حيث أن الأمر لا يتعدى خطوة واحدة بالفأرة. وكان الشائع بين المدرسين والأساتذة المساعدين هو

حذفها من خلال الأمرShift Delate وجاءت النسبة الأعلى في ذلك من قبل الأساتذة المساعدين والبالغ نسبتهم٦٩,٢٪والأساتذة ٦٤,٧٪ والمدرسين بنسبة ٣٩,٥٪، أما حذف محتوى الملف ثم حذفه بالكامل فقد كان المعدل الأعلى في ذلك من قبل المدرسين المساعدين الذين بلغو٢٤,٤٪ تبعهم المدرسين بنسبة ٢٣,٥٪ ربما لم تلقى هذه الطريقة إجماع كبير عليها لاحتياجها العديد من الخطوات.

جدول (١٦) الاختلافات العمرية بين أفراد العينة من حيث القيام ببعض الممارسات الأمنية

س	العمر	دائمًا		غالبًا		نادرًا		محايد		إطلاقًا		الإجمالي	
		ع	%	ع	%	ع	%	ع	%	ع	%	ع	%
تقوم بتسجيل الأحداث الأمنية	٢١-٣٠	١٠	٨	٣٣	٢٦,٤	٤٤	٣٥,٢	١٦	١٢,٨	٢٢	١٧,٦	١٢٥	١٠٠
	٣١-٤٠	١١	١٢,٥	١٦	١٨,٢	٢٥	٢٨,٤	١٨	٢٠,٥	١٨	٢٠,٥	٨٨	١٠٠
	٤١-٥٠	٩	٢٠,٥	٧	١٥,٩	١٢	٢٧,٣	٥	١١,٤	١١	٢٥	٤٤	١٠٠
	٥٠فأكثر	٠	٠	١	١٢,٥	٥	٦٢,٥	١	١٢,٥	١	١٢,٥	٨	١٠٠
تقوم بعمل نسخة احتياطية لبياناتك	٢١-٣٠	٣٨	٣٠,٤	٤٨	٣٨,٤	٢٣	١٨,٤	٨	٦,٤	٨	٦,٤	١٢٥	١٠٠
	٣١-٤٠	39	44.3	٢٩	٣٣	١٢	١٣,٦	٦	٦,٨	٢	٢,٣	٨٨	١٠٠
	٤١-٥٠	١٣	٢٩,٥	٢٣	٥٢,٣	٥	١١,٤	٣	٦,٨	٠	٠	٤٤	١٠٠
	٥٠فأكثر	٤	٥٠	١	١٢,٥	٣	٣٧,٥	٠	٠	٠	٠	٨	١٠٠
تختبر النسخ الاحتياطية	٢١-٣٠	22	17.6	38	30.4	41	32.8	12	9.6	12	9.6	١٢٥	١٠٠
	٣١-٤٠	30	34.1	18	20.5	26	29.5	٨	٩,١	٦	٦,٨	٨٨	١٠٠
	٤١-٥٠	١٠	٢٢,٧	١٧	٣٨,٦	١١	٢٥	٢	٤,٥	٤	٩,١	٤٤	١٠٠
	٥٠فأكثر	٣	٣٧,٥	٢	٢٥	3	37.5	٠	٠	٠	٠	٨	١٠٠

شكل (٣) الاختلافات العمرية بين أفراد العينة من حيث القيام ببعض الممارسات الأمنية



يتناول الجدول والشكل السابقين مجموعة من الممارسات اللازمة لتحقيق الأمان ويقيس الفروق العمرية في القيام بذلك من عينة الدراسة حيث يتضح أن نسبة من هم أعمارهم صغيره من _٢١-٣٠_ ٢٦,٤٪ يقومون على الأغلب بتسجيل الأحداث الأمنية وبالتالي هم أعلى معدل ممن أعمارهم ٣١-٤٠ الذين بلغت نسبتهم ١٨,٢٪ وفي هذه الفئات العمرية تقع الدرجات العلمية من معيد لـ مدرس وبالتالي المعيدين نسبتهم أعلى من المدرسين المساعدين والمدرسين وبالمثل سنجد أن من أعمارهم من ٤١-٥٠ بلغت نسبتهم ١٥,٩٪ مقارنة بالفئة الأكبر من ٥١ فأكثر وبالتالي أيضًا الأساتذة المساعدين والأساتذة سيكونون أكثر معدلًا في تسجيل الأحداث الأمنية من الأساتذة المتفرغين وعليه يمكن القول أنه كلما صغر العمر كلما زاد الاهتمام بتتبع الأحداث الأمنية وتسجيلها. وبالنظر إلى نسخ البيانات سنؤكد على النتيجة السابقة حيث كانت نسبة القيام بذلك من قبل الأعمار (٢١-٣٠) ٣٨,٤٪، مقارنةً بأصحاب الأعمار (٣١-٤٠) البالغ نسبتهم ٣٣٪ إذا فالمعيدين والمدرسين المساعدين أفضل من المدرسين، وبالنظر إلى الأعمار (٤١-٥٠) جاءت نسبتهم مرتفعة عن ذوات الأعمار (٥١فأكثر) وذلك بنسبة ٥٢,٣٪: ١٢,٥٪ وتسير المعدلات نفس الاتجاه السابق بالنسبة لاختبار النسخ الاحتياطية وعليه يمكن القول بأن أصحاب الأعمار في عمر (٢١-٣٠) أفضل من أصحاب الأعمار في عمر ٣١-٤٠ وكذلك الأمر أصحاب الأعمار (٤١-٥٠) أفضل من ذوات الأعمار (٥١فأكثر). وذلك من حيث القيام ببعض الممارسات الأمنية.

جدول (١٦) كيفية الحفاظ على أنظمة التشغيل

س	العمر	من خلال حفظ جميع البرامج الخاصة بك مصححة ومحدثة بما فيها أنظمة التشغيل. تقنية حماية الذاكرة		من خلال حفظ جميع البرامج الخاصة بك مصححة ومحدثة بما فيها أنظمة التشغيل		تقنية حماية الذاكرة.		حفظ جميع البرامج الخاصة بك مصححة ومحدثة بما فيها أنظمة التشغيل تقنية ترقية سماحيات المستخدم		بيانات مفقودة		الإجمالي	
		ع	%	ع	%	ع	%	ع	%	ع	%	ع	%
ما الكيفية التي تتمكن من خلالها المحافظة على أنظمة التشغيل	٢١-٣٠	٢٤	١٩,٢	٦٣	٥٠,٤	٢٥	٢٠	١٣	١٠,٤	٠	٠	١٢٥	١٠٠
	٣١-٤٠	١٠	١١,٤	٦٠	٦٨,٢	١١	١٢,٥	٦	٦,٨	١	١,١	٨٨	١٠٠
	٤١-٥٠	٤	٩,١	٣١	٧٠,٥	٦	١٣,٦	٣	٦,٨	٠	٠	٤٤	١٠٠
	٥١ فأكثر	١	١٢,٥	٧	٨٧,٥	٠	٠	٠	٠	٠	٠	٨	١٠٠

يتناول الجدول السابق رقم (١٦) الكيفية التي يمكن من خلالها الحفاظ على أنظمة التشغيل مصححة وسليمة ويتضح من الجدول أن الغالبية تعتمد على حفظ البرامج مصححة ومحدثة بما فيها أنظمة التشغيل وكانت أعلى نسبة وفق الفئة العمرية تعتمد هذه الطريقة هي الأفراد في عمر(٥١ فأكثر) حيث بلغت نسبتهم ٨٧,٥٪ والأفراد ذوو الأعمار(من ٤١-٥٠) بلغو ٧٠,٥٪ وذو الأعمار (٣١-٤٠) بلغت نسبتهم ٦٨,٢٪ وذلك مقارنةً بأصحاب الفئة العمرية من (٢١-٣٠) الذين بلغت نسبتهم ٥٠,٤٪.١٩,٢٪ من أصحاب الفئة العمرية (٢١-٣٠) يستخدمون تقنية حماية الذاكرة (لكي تعمل البرامج يجب أن يتوفر لها الموارد التي يمكن من خلالها التعامل معها بشكل أسرع ، هذا الأمر يأتي بما يسمى RAM (ذاكرة الوصول العشو ائي) وهي التي تقوم بهذا العمل الرام هي نوع من التخزين المؤقت (أي شيء يجري فيها يتم مسحه عند إيقاف التشغيل) وهي تسمح أن يتم كتابة وقراءة البيانات بسرعة كبيرة) (أمان أنظمة التشغيل | كيف يبقيك كل نظام تشغيل آمناً، ٢٠١٧) إلى جانب حفظ البرامج و أنظمة التشغيل مصححة ومحدثة تبعهم أصحاب الأعمار من (٥١فأكثر) بنسبة ١٢,٥٪ ثم أصحاب الأعمار من(٣١-٤٠) بنسبة ١١,٤٪. واضح جدًا أن النسبة الأعلى هنا جاءت في أصحاب الفئة الأقل عمرًا وربما يعود السبب في ذلك إلى مميزات تقنية الذاكرة حيث تعمل هذه التقنية على حماية الذاكرة من أية برامج ضارة وبالتالي حماية نظام التشغيل نفسه. ونلاحظ أيضًا من خلال الجدول إن ١٣,٦٪من أصحاب الأعمار(٤١-٥٠) بنسبة ٢٠٪ يعتمدون على تقنية حماية الذاكرة بمفردها وهذا لميزتها السابقة. ولكن تضاءلت النسب عند استخدام تقنية ترقية سماحيات المستخدم حيث بلغت ١٠,٤٪ في الأفراد ذوو الأعمار(٢١-٣٠) وتماثلت النسبة في الأفراد من الأعمار(٣١-٥٠) بنسبة ٦,٨٪. وتستخدم هذه السماحيات تساعد في حماية وتأمين جهاز الحاسب، ولكن هذه السماحيات تسمح بعدد معين من المستخدمين فقط هم من يمكنهم تعديل أشياء معينة مثل تفضيلات النظام.. ويمكن لذلك الإقبال عليها قليل حيث في حال تعدي المستخدم الأمور المحددة له يمكن التغيير والعبث في نظام التشغيل وهذا الأمر غير مضمون.

جدول (١٧) أنظمة التشغيل الأكثر استخدامًا حسب الفروق العمرية بين أفراد العينة

س	العمر	Microsoft Windows		Linux		Microsoft Windows Linux		Microsoft Windows Mac OS X		UNIX		UNIX, Microsoft Windows		الإجمالي	
		ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%
ما هو نظام	٢١-	٧٠	٥٦	١٤	١١,٢	١٠	٨	١٧	١٣,٦	٨	٦,٤	٦	٤,٨	١٢٥	١٠٠
	٣١-	٥٩	٦٧	٥	٥,٧	١٠	١١,٤	٢	٢,٣	٧	٨	٥	٥,٧	٨٨	١٠٠

التشغيل المستخدم على	٤١-	٢٩	٦٥,٩	٣	٦,٨	٣	٦,٨	٥	١١,٤	٢	٤,٥	٢	٤,٥	٤٤	١٠٠
	٥١ فأكثر	٥	٦٢,٥	١	١٢,٥	٠	٠	٢	٢٥	٠	٠	٠	٠	٨	١٠٠

يوضح الجدول السابق رقم (١٧) أن أنظمة التشغيل مايكروسوفت ويندوز هي الأعلى مُعدلًا من حيث الاستخدام من قبل الفئات العمرية المختلفة لعينة الدراسة، يليها في ذلك أنظمة التشغيل لينوكس. ولعل السبب في ذلك يعود إلى الميزات العالية التي تتمتع بها أنظمة التشغيل مايكروسوفت ويندوز حيث تتميز بتو افقها مع غالبية الأجهزة، إلى جانب سهولة الاستخدام، تحقيق الحماية والأمان هي الأعلى كفاءة مقارنةً بغيرها، هي الأكثر شيوعًا و انتشارا وشهرة بين نظيراتها. كذلك الأمر بالنسبة لأنظمة التشغيل لينوكس فما جعلها تأتي في المرتبة الثانية لاستخدامها من قبل فئات العينة هو مميزاتها حيث يتمتع نظام تشغيل لينوكس بدقة الأداء وجود النظام على الشبكة مجانًا، أنها لا تتطلب أية برامج لمكافحة الفيروسات، نلاحظ من خلال الجدول أيضًا أن نسبته ١١,٤٪ من أفراد العينة المتمثل أعمارهم في ٤١-٥٠ يستخدمون نظامي تشغيل معًا وهما النظامين السابقين ولعل السبب في ذلك هو الجمع بين مز ايا كلًا منهما.

ولكن هذا الأمر في غاية الخطورة حيث إن عمل النظامين معًا (مايكروسوفت ويندوزولينوكس) على نفس الجهاز من الممكن أن يؤدي إلى: فقدان البيانات حيث إن عملية تثبيت نظام التشغيل لينوكس إلى جانب الويندوز تؤدي إلى فقدان العديد من البيانات. قد يتسبب ذلك في بطء الجهاز فمن الممكن ألا تتلاءم القدرات الفنية للجهاز مع تثبيت نظامين معًا.

البعض الآخر من أفراد العينة فضل استخدام نظامي التشغيل "Mac Microsoft Windows OS X" من المعروف أن نظام Mac OS X متاح لأجهزة Apple، ولكن يُمكن استخدامه مع أنظمة Microsoft Windows دون حدوث أي ضرر بل بالعكس تقديم المميزات التالية: كلا النظامين يقدّمان معالجة تطبيق واضحة ونقيّة، فبالإمكان استخدام النظامين دون الحاجة لإنشاء حساب مستخدم من Microsoft أوApple . (samma3a، ٢٠١٩) خيارات تسجيل الدخول المتنوعة متاحة على الواجهتين، وبالتالي يتضمن إجراءات تتعدى السلوك التقليدي لعمليات تسجيل الدخول لسطح المكتب.

سنلاحظ من خلال الجدول السابق أيضًا أن نسبة قليلة فقط هي من اعتمدت على نظام تشغيل " Unix"والسبب في ذلك يعود إلى: أن النظام مصمم بشكل رئيسي للمبرمجين حيث يعتمد على سطر الأوامر، وبالتالي الأمر صعب بالنسبة للمستخدم المبتدئ. الأوامر المشفرة،

تتطلب غالبية الأوامر المستخدمة في نظام التشغيل (UNIX) استخدام أحرف معينة، وهذا الأمر صعب جدا على المستخدمين العاديين. (e3arabi، نظام التشغيل يونيكس – Unix، ٢٠٢٠). يوجد فئة قليلة اعتمدت في عملها على نظامي التشغيل UNIX, Microsoft Windows وربما يعود السبب في ذلك للاستفادة من مزايا نظام التشغيل يونيكس وتفادي عيوبه.

جدول (١٨) يوضح اتجاهات الأفراد حسب أعمارهم نحو طريقة معينة لحماية بريدهم الشخصي من الانتحال

س	العمر	Dmarck		Spf		لا أعرف		بيانات مفقودة		الإجمالي	
		ع	%	ع	%	ع	%	ع	%	ع	%
كيف يتم منع انتحال البريد الإلكتروني	٢١-٣٠	٧٩	٦٣,٢	٢٩	٢٣,٢	١٦	١٢,٨	١	٨	١٢٥	١٠٠
	٣١-٤٠	٦٤	٧٢,٧	١٤	١٥,٩	١٠	١١,٤	٠	٠	٨٨	١٠٠
	٤١-٥٠	٢٩	٦٥,٩	٩	٢٠,٥	٦	١٣,٦	٠	٠	٤٤	١٠٠
نلانلا	٥١ فأكثر	٧	٨٧,٥	٠	٠	١	١٢,٥	٠	٠	٨	١٠٠

نلاحظ من خلال الجدول السابق أن نسب استخدام طريقة Dmarck لمصادقة البريد الإلكتروني أعلى كثيرًا من نسب استخدامات نظام التعرف على هوية المستخدم Spf وذلك على اختلاف الفئات العمرية المختلفة فمن الواضح انها المفضلة من قبل أفراد العينة على اختلاف أعمارهم وبالتالي على اختلاف درجاتهم العلمية أيضًا والسبب في ذلك: أن Dmarck تعمل على منع المها جمين من انتحال الاسم وتزوير "من "برسالة إلكترونية. وتبدو رسالة الانتحال بأنها واردة من المؤسسة أو النطاق اللذين تعرضا لانتحال هويتهما. توفر إمكانية طلب التقارير من خوادم البريد الإلكتروني التي تتلقى رسائل من المؤسسة. تتضمن هذه التقارير معلومات للمساعدة في تحديد مشاكل المصادقة المحتملة والنشاط الضار للرسائل المُرسَلة من قبل مستخدمها وربما كانت النسبة في استخدام نظام Spf أقل لأنه يحدد الخوادم والنطاقات المصرح لها بإرسال رسائل إلكترونية نيابةً عن المؤسسة أي أن استخدامه يكون أكثر من قبل المؤسسات لأنه يخدم الجانب المؤسسي أكثر.

جدول (١٩) كيفية حماية الأجهزة من البرامج الضارة وفيرس الفدية وفق الفئات العمرية المختلفة لعينة الدراسة

س	العمر	من خلال برامج الحماية		من خلال منع الوصول غير المخول لها		من خلال برامج الحماية من خلال منع الوصول غير المخول لها		لا أعلم		بيانات مفقودة		الإجمالي	
		ع	%	ع	%	ع	%	ع	%	ع	%	ع	%
كيف تحمي أجهزتك من البرامج الضارة وفيرس الفدية	٢١-٣٠	٨٤	٦٧,٢	٢٠	١٦	٢١	١٦,٨	٠	٠	٠	٠	١٢٥	١٠٠
	٣١-٤٠	٥٠	٥٦,٨	٢٣	٢٦,١	١٣	١٤,٨	١	١,١	١	١,١	٨٨	١٠٠
	٤١-٥٠	٣٢	٧٢,٧	٧	١٥,٩	٢	٤,٥	١	٢,٣	٢	٤,٥	٤٤	١٠٠
	٥١ فأكثر	٧	٨٧,٥	١	١٢,٥	٠	٠	٠	٠	٠	٠	٨	١٠٠

يتضح من خلال الجدول السابق أن النسبة الأكبر من أفراد العينة على اختلاف فئاتهم العمرية تعتمد على برامج الحماية للحفاظ على الأجهزة من البرامج الضارة وفيروسات الفدية حيث بلغت نسبة الأفراد في الأعمار من ٥١ سنة فأكثر٨٧,٥٪ تلاهم الأفراد في عمر ٤١-٥٠ بنسبة ٧٢,٧٪ وكانت الفئة العمرية من ٢١-٣٠ هي الأعلى معدلًا بين الفئات الأخرى من حيث الاستخدام حيث بلغت نسبتها ٦٧,٢٪ تلاها الأفراد في ٣١-٤٠ حيث بلغت نسبتهم في الإعتماد على برامج الحماية ٥٦,٨٪عمر و أقل فئة وسط الفئات جاءت في الأعمار من ٥١ فأكثر. ويرجع السبب في الإقبال على استخدام برامج الحماية لـ: قدرتها على حماية الأجهزة من أي برمجيات خبيثة من الممكن أن تتسلل إليها، توفير جدار حماية آمن للأجهزة من أي تهديدات عند تصفح شبكة الإنترنت والدخول إلى المو اقع التي من المحتمل ان يكون بها الكثير من الفيروسات. إلى جانب هذه الطريقة بعضهم اعتمد على طريقة منع الوصول غير المصرح أي لغير الأفراد المأذون لهم بذلك، وهناك من اعتمد على الطريقتين معًا لتحقيق حماية أفضل.

جدول (٢٠) يوضح الفروق بين فئات العينة حسب اختلاف أعمارهم من حيث تخزين النسخ الاحتياطية وحفظها

س	العمر	Google Drive, الفلاشات ميموري (Flash Memory).		Google Drive بطاقات التخزينية الذاكرة النسخ برامج الاحتياطية الفلاشات ميموري		Google الفلاشات Drive, الأقراص أو الثابتة الصلبة التخزينية الذاكرة بطاقات ,المحمولة		الأقراص المدمجة الفلاشات ميموري (Flash Memory)		الأقراص الصلبة الثابتة أو المحمولة الفلاشات ميموري (Flash Memory).		Google Drive, Storage Cloud		الأقراص الصلبة الثابتة أو المحمولة الفلاشات ميموري (Flash Memory).		Google Drive, الأقراص الصلبة الثابتة أو المحمولة الأقراص المدمجة الفلاشات ميموري (Flash Memory		Storage Cloud برامج النسخ الاحتياطية الفلاشات ميموري		Google Drive, Storage Cloud, الفلاشات ميموري (Flash Memory)		الإجمالي	
		%	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	ع
كيف	30–21	46.4	58	7.2	9	23.9	21	5.6	7	3.4	3	6.8	3	2.3	1	29.5	13	38.6	34	5.6	7	2.3	2	5.6	7	3.4	4	6.4	8	100	125
تقوم	40–31	25	2	–	–	–	–	–	–	–	–	–	–	12.5	1	50	4	–	–	15.9	7	4.5	2	–	–	9.1	4	–	–	100	8
بتخزين	50–41	38.6	34	3.4	3	23.9	21	5.6	7	3.4	3	6.8	3	5.7	5	10.2	9	4.5	4	5.6	7	2.3	2	6.8	3	2.3	2	5.7	5	100	88
النسخ	51 فأكثر	29.5	13	2.3	1	6.8	3	5.6	7	13.6	6	4.5	2	15.9	7	–	–	7.2	9	5.6	7	3.4	3	2.3	2	9.1	4	11.4	5	100	44

يتبين من خلال الجدول السابق الاختلافات العمرية في حفظ وتخزين النسخ الاحتياطية ويتضح أن أكثر وسيلتين عليهم إجماع لحفظ النسخ وتخزينها هُما جوجل درايف والفلاشات ميموري معًا مع ملاحظة تكرار استخدام الفلاشات ميموري ما يزيد عن خمسة مرات مع الطرق الأخرى ولعل السبب في ذلك راجع إلى مميزات كلا النوعين حي يتميز التخزين على جوجل درايف بالآتي: إمكانية حفظ وتخزين أي ملفات على شبكة الإنترنت سهولة الوصول إليها في أي وقت ومن أي مكان، تقديم مساحة تخزين كبيرة تصل إلى ١٥ جيجا على شبكة الإنترنت ويمكن زيادتها ولكن في حالة الزيادة يتطلب مقابل إمكانية مشاركة الملفات.

بالنسبة للفلاشات ميموري فهي تتميز بـ: سهولة الاستخدام والاسترجاع. لا تتطلب اتصال بالإنترنت للحصول على المعلومات المخزنة عليها، لا تشغل حيز مكاني كبير، انخفاض تكلفتها إلى جانب سهولة حملها ونقلها، يمكن استخدامها كناقل للتطبيقات المحمولة، سعة التخزين.

كما يتبين من خلال الجدول انخفاض نسب استخدام كلًا من:

Storage Cloud وذلك يرجع إلى: أن عملية نقل البيانات للتخزين السحابي تكون بكمية محددة وبالطبع عند زيادة هذه الكمية ستزيد التكلفة، لا يمكن الوصول للبيانات المخزنة في حالة عدم وجود إنترنت، مسألة وجود البيانات المخزنة على الإنترنت يسمح بإمكانية اختر اقها أو تهكيرها، تتطلب برنامج خاص بالخدمة ينبغي تحميلة على الجهاز لتحميل اللغات.

بالنسبة للأقراص فيُعاب عليها في: البطء في السرعة بخلاف الأنواع الأخرى، هناك ضرر كبير آخر موجود في محرك الأقراص الصلبة وهو عامل الهيكل الهائل، في ضوء وجود أجزاء ميكانيكية، لا يمكن جعل القرص الصلب أكثر بساطة بشكل معين، استهلاك القوة، الضوضاء، إلى جانب الأعطال الميكانيكية. (e3arabi، ٥)

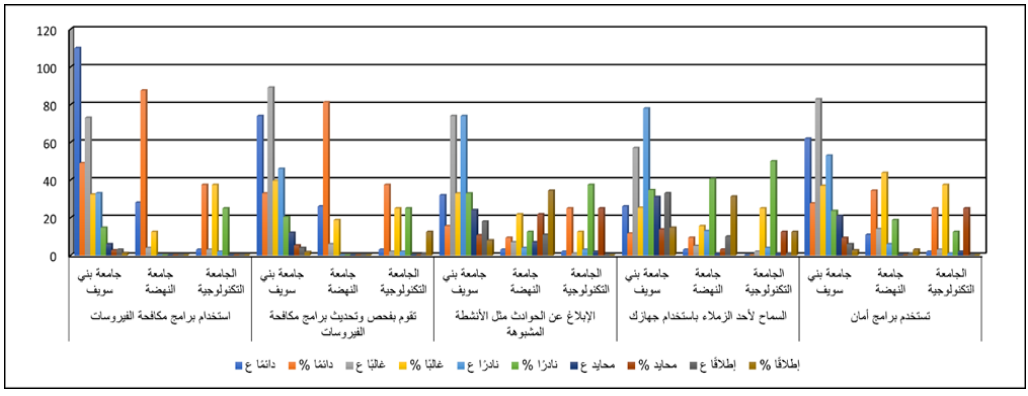
الطريقة الثالثة التي لم تلقى قبول واسع هي برامج النسخ الاحتياطي والسبب في ذلك يعود إلى: ظهور رسائل تعذر الحفظ، أيضًا رسائل الخطأ لا توجد مساحة كافية على الحاسب وهكذا الرسائل الأخرى من هذا المثيل. (mobiletrans، ٢٠٢٢).

سادسًا محور الأمان وإدارة المخاطر

جدول (٢١) الفروق بين الجامعات الثلاث في التأمين والتعامل مع الحوادث

س	الجامعة	دائمًا		غالبًا		نادرًا		محايد		إطلاقًا		الإجمالي	
		ع	%	ع	%	ع	%	ع	%	ع	%	ع	%
استخدام برامج مكافحة الفيروسات	جامعة بني	١١٠	٤٨,٩	٧٣	٣٢,٤	٣٣	١٤,٧	٦	٢,٧	٣	١,٣	٢٢٥	١٠٠
	جامعة	٢٨	٨٧,٥	٤	١٢,٥	٠	٠	٠	٠	٠	٠	٣٢	١٠٠
	الجامعة	٣	٣٧,٥	٣	٣٧,٥	٢	٢٥	٠	٠	٠	٠	٨	١٠٠
تقوم بفحص وتحديث برامج مكافحة للفيروسات	جامعة بني	٧٤	٣٢,٩	٨٩	٣٩,٦	٤٦	٢٠,٤	١٢	٥,٣	٤	١,٨	٢٢٥	١٠٠
	جامعة	٢٦	٨١,٣	٦	١٨,٨	٠	٠	٠	٠	٠	٠	٣٢	١٠٠
	الجامعة	٣	٣٧,٥	٢	٢٥	٢	٢٥	٠	٠	١	١٢,٥	٨	١٠٠
الإبلاغ عن الحوادث مثل الأنشطة المشبوهة	جامعة بني	٣٢	١٥,٦	٧٤	٣٢,٩	٧٤	٣٢,٩	٢٤	١٠,٧	١٨	٨	٢٢٥	١٠٠
	جامعة	٣	٩,٤	٧	٢١,٩	٤	١٢,٥	٧	٢١,٩	١١	٣٤,٤	٣٢	١٠٠
	الجامعة	٢	٢٥	١	١٢,٥	٣	٣٧,٥	٢	٢٥	٠	٠	٨	١٠٠
السماح لأحد الزملاء باستخدام جهازك	جامعة بني	٢٦	١١,٦	٥٧	٢٥,٣	٧٨	٣٤,٧	٣١	١٣,٨	٣٣	١٤,٧	٢٢٥	١٠٠
	جامعة	٣	٩,٤	٥	١٥,٦	١٣	٤٠,٦	١	٣,١	١٠	٣١,٣	٣٢	١٠٠
	الجامعة	٠	٠	٢	٢٥	٤	٥٠	١	١٢,٥	١	١٢,٥	٨	١٠٠
تستخدم برامج أمان	جامعة بني	٦٢	٢٧,٦	٨٣	٣٦,٩	٥٣	٢٣,٦	٢١	٩,٣	٦	٢,٧	٢٢٥	١٠٠
	جامعة	١١	٣٤,٤	١٤	٤٣,٨	٦	١٨,٨	٠	٠	١	٣,١	٣٢	١٠٠
	الجامعة	٢	٢٥	٣	٣٧,٥	١	١٢,٥	٢	٢٥	٠	٠	٨	١٠٠

شكل (٤) الفروق بين الجامعات الثلاث في التأمين والتعامل مع الحوادث



يوضح الجدول رقم (٢٢) والشكل السابق الاختلافات الموجودة بين جامعة بني سويف والنهضة والتكنولوجية من حيث بعض إجراءات الأمان فبالنظر إلى استخدام برامج مكافحة الفيروسات سنجد أن جامعة النهضة هي أعلى معدل من جامعتي بني سويف والتكنولوجيا حيث كانت النسب ٨٧,٥٪ :٤٨,٩٪،٣٧,٥٪. وكذلك جاءت النسبة الأعلى من حيث تحديث برامج مكافحة الفيروسات من نصيب جامعة النهضة. أما من حيث الإبلاغ عن الحوادث الأمنية: فكانت الجامعة التكنولوجية أعلى معدلًا للقيام بذلك تبعتها جامعة بني سويف ثم النهضة بالنسب ٢٥٪: ١٥,٦٪،٩,٤٪. وبالنسبة للسماح للزملاء باستخدام الجهاز سنجد أيضًا أن جامعة النهضة أفضل من الجامعتين الأخيرتين حيث نسبة من لا يسمحون بذلك على الإطلاق منها بلغت ٣١,٣٪ يليها بني سويف بنسبة ١٤,٧٪ ثم التكنولوجية بنسبة ١٢,٥٪. ومن ناحية استخدام برامج الأمان سنلاحظ أن النهضة أفضلهم في ذلك فهي بلغت أعلى نسبة ٣٤,٤٪ مقارنةً ببني سويف٢٧,٦٪، والتكنولوجية٢٥٪. وعليه يمكن القول بأن جامعة النهضة أفضل من جامعة بني سويف والتكنولوجية في هذه المؤشرات، وربما يكون السبب في ذلك بسبب حجم إمكاناتها المالية وميزانيتها التي تختلف عن الجامعتين الحكومتين ما يُمكنها من ذلك. وسيتم تأكيد هذه النتيجة أو نفيها من خلال تحليل الجداول الأخرى.

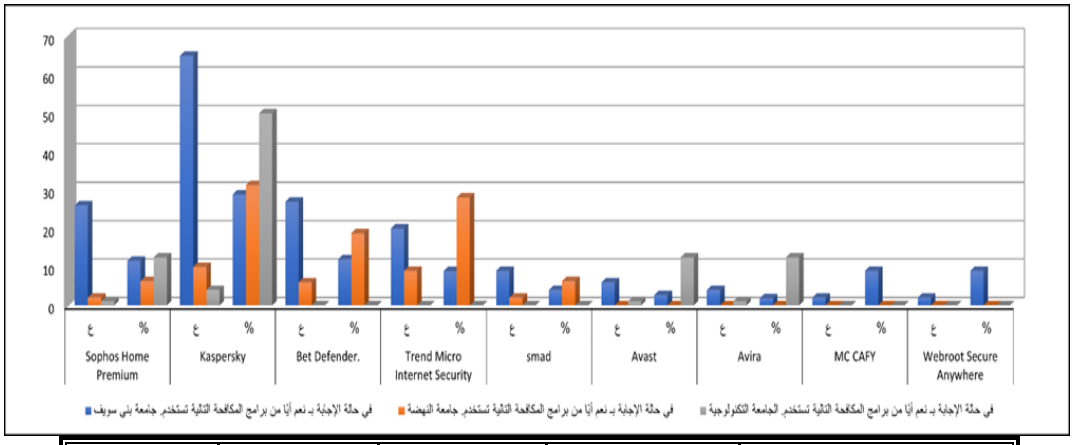
جدول (٢٣) يوضح كيفية التعامل مع الرسائل مجهولة المصدر من قبل الجامعات الثلاث وضع الدراسة.

س	الجامعة	تقوم بحذفها		تقوم بفتحها		تقوم بتجاهلها		الإجمالي	
		ع	%	ع	%	ع	%	ع	%
ماذا تفعل حينما تجد رسالة مجهولة المصدر مرسلة إليك	جامعة بني سويف	٩٥	٤٢,٢	٢٥	١١,١	١٠٥	٤٦,٧	٢٢٥	١٠٠
	جامعة النهضة	١١	٣٤,٤	٢	٦,٣	١٩	٥٩,٤	٣٢	١٠٠
	الجامعة التكنولوجية	١	١٢,٥	٣	٣٧,٥	٤	٥٠	٨	١٠٠

يتناول الجدول السابق الاختلافات بين الجامعات الثلاث موضع الدراسة من حيث التعامل مع الرسائل مجهولة المصدر ويتضح أن جامعة بني سويف هي الأفضل في التعامل مع الرسائل المجهولة حيث بلغت نسبة من يقومون بحذفها من جامعة بني سويف ٤٢,٢٪، تبعها جامعة النهضة بنسبة ٣٤,٤٪ وأخيرًا التكنولوجية بنسبة ١٢,٥٪. مع ملاحظة أن الجامعة الأخيرة هي الأكثر تعرضًا للخطر عند فتحها للرسائل المجهولة حيث بلغت نسبتها في ذلك ٣٧,٥٪. وذلك لأن الأفضل في التعامل مع الرسائل المرسلة من قبل أشخاص غير معروفين هو حذفها فإذا تم

تجاهلها سيتم تكدس صندوق الرسائل وفي حال فتحها حدث ولا حرج فربما كانت برامج ضارة فربما كانت فيرس فدية وما إلى أخرة إذّا فالأفضل حذفها.

جدول (٢٤) يوضح نسب استخدام برامج مكافحة الفيروسات في الجامعات موضع الدراسة.



س	الجامعة	نعم		لا		الإجمالي	
		ع	%	ع	%	ع	%
هل تستخدم برامج مكافحة الفيروسات؟	جامعة بني سويف	١٦٣	٧٢,٤	٦٢	٢٧,٦	٢٢٥	١٠٠
	جامعة النهضة	٢٩	٩٠,٦	٣	٩,٤	٣٢	١٠٠
	الجامعة التكنولوجية	٦	٧٥	٢	٢٥	٨	١٠٠

يتبين من خلال الجدول السابق أن نسبة الأفراد المُعرضين للهاكروالبرامج الضارة بجامعتي بني سويف والتكنولوجيا أكبر من نسبة هؤلاء الموجودين بجامعة النهضة حيث أن نسبة ٢٧,٦٪ من أفراد العينة بجامعة بني سويف لا يقومون باستخدام برامج مكافحة الفيروسات وأن الأفراد بنسبة ٢٥٪ أيضًا من الجامعة التكنولوجية معرضين لذلك لنفس السبب بينما نسبة قليلة من جامعة النهضة هي

التي من الممكن حدوث هجوم عليها حيث بلغت ٩,٤٪.

جدول (٢٥) يوضح أكثر أنواع برامج مكافحة الفيروسات استخدامًا من قبل الجامعات موضع الدراسة

س	الجامعة	Sophos Home Premium		Kaspersky		Bet Defender.		Trend Micro Internet Security		smad		Avast		Avira		MC CAFV		Webroot Secure Anywhere		قيم متفوقة		الإجمالي	
		ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%
في حالة الإجابة بنعم أيًا من برامج المكافحة التالية تستخدم.	جامعة بني سويف	26	11.6	65	28.9	27	12	20	8.9	9	4	6	2.7	4	1.8	2	9	2	9	64	28.4	225	100
	جامعة النهضة	2	6.3	10	31.3	6	18.8	9	28.1	2	6.3	-	-	-	-	-	-	-	-	3	9.4	32	100
	الجامعة التكنولوجية	1	12.5	4	50	-	-	-	-	-	-	1	12.5	1	12.5	-	-	-	-	1	12.5	8	100

شكل (٥) يوضح أكثر أنواع برامج مكافحة الفيروسات استخدامًا من قبل الجامعات موضع الدراسة

يتضح من خلال الجدول السابق والشكل السابق أن أكثر برنامج مكافحة فيروسات مستخدم من قبل أفراد الجامعات الثلاثة هو برنامج Kaspersky.وكانت أعلى نسب استخدامه على الترتيب الثاني الجامعة التكنولوجية ثم النهضة ثم بني سويف بالنسب المقدرة على النحو ٥٠٪،٣١,٣٪،٢٨,٩٪. والسبب في ذلك يعود إلى: أنه يقدم الحماية ضد جميع أنواع البرامج الضارة بما فيها الفيروسات وبرامج التجسس وفيرس الفدية، يقدم حماية إضافية لنظام ماكنتوش وللهاتف النقال، إضافة إلى الحماية ضد الجرائم الإلكترونية مثل التصيد الاحتيالي، يقدم ميزات إضافية مثل مدير كلمات المرور وأدوات الرقابة الأبوية. (safetydetectives، ٢٠٢٢) إلى جانب ذلك شهرته الواسعة بين برامج مكافحة الفيروسات الأخرى.

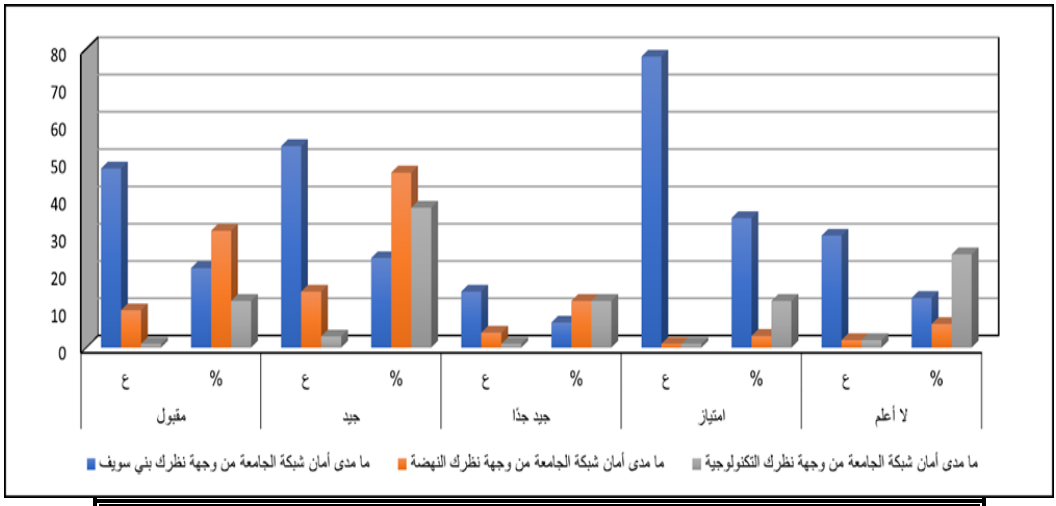
جدول (٢٦) يوضح درجة الأمان بجامعات محافظة بني سويف

س	الجامعة	مقبول		جيد		جيد جدًا		امتياز		لا أعلم		الإجمالي	
		ع	%	ع	%	ع	%	ع	%	ع	%	ع	%
ما مدى أمان شبكة الجامعة من وجهة نظرك	بني سويف	٤٨	٢١,٣	٥٤	٢٤	١٥	٦,٧	٧٨	٣٤,٧	٣٠	١٣,٣	٢٢٥	١٠٠
	النهضة	١٠	٣١,٣	١٥	٤٦,٩	٤	١٢,٥	١	٣,١	٢	٦,٣	٣٢	١٠٠
	التكنولوجية	١	١٢,٥	٣	٣٧,٥	١	١٢,٥	١	١٢,٥	٢	٢٥	٨	١٠٠

شكل (٦) يوضح درجة الأمان بجامعات محافظة بني سويف

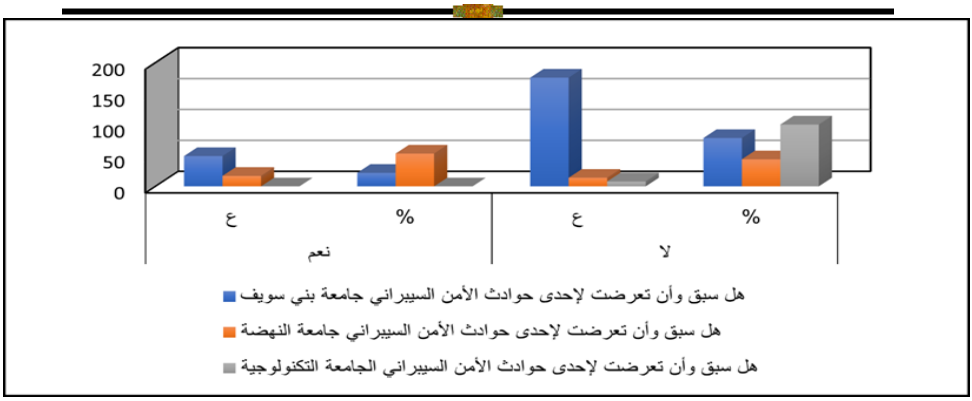
يتضح من خلال الجدول السابق والشكل السابق أن جامعة بني سويف هي الأكثر أمانًا حيث بلغت نسبتها٣٤,٧٪ يليها الجامعة التكنولوجية ١٢,٤٪ ثم جامعة النهضة٦,٣٪ وهذه النسب جاءت وفق وجهات نظر العاملين بكل جامعة من أعضاء هيئة التدريس ومعاونيهم. ولكن ليس من المنطقي أن تكون الجامعة التكنولوجية أعلى مُعدلًا من جامعة النهضة خاصةً وبأن هذه الأولى لا تستخدم أيًا من أجهزة الحماية أو أيًا من المعدات التقنية المتعلقة بالأمن السيبراني وهذا الأمر ما وجدته الباحثة أثناء دراستها الميدانية التي أجرتها على الجامعات الثلاث.

جدول (٢٧) جدول يوضح نسب التعرض لحوادث الأمن السيبراني من عدمها بالجامعات الثلاث



س	الجامعة	نعم		لا		قيم مفقودة		الإجمالي	
		ع	%	ع	%	ع	%	ع	%
هل سبق وأن تعرضت لإحدى حوادث الأمن السيبراني	جامعة بني سويف	٤٩	٢١,٨	١٧٦	٧٨,٢	٠	٠	٢٢٥	١٠٠
	جامعة النهضة	١٧	٥٣,١	١٤	٤٣,٨	١	٣,١	٣٢	١٠٠
	الجامعة التكنولوجية	٠	٠	٨	١٠٠	٠	٠	٨	١٠٠

شكل (٨) جدول يوضح نسب التعرض لحوادث الأمن السيبراني من عدمها بالجامعات الثلاث



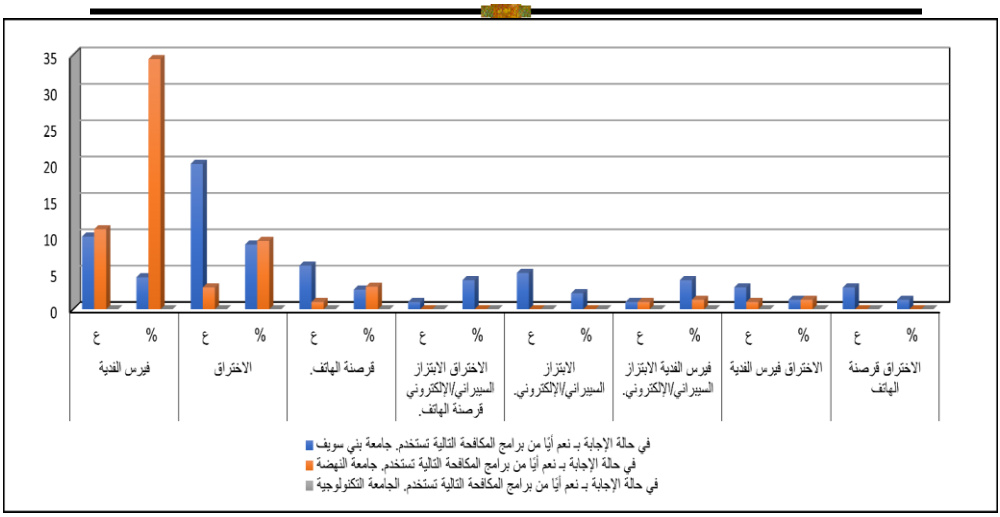
يتبين من خلال الجدول والشكل السابقين أن نسبة من تعرض لهجوم أو اختراق أو فيرس فدية أو خلافة من حوادث الأمن السيبراني بالجامعة التكنولوجية صفر%، يليهم جامعة بني بنسبة ٢١,٨٪ بينما كانت النسبة الأكبر في التعرض لحوادث الأمن السيبراني تابعة لجامعة النهضة حيث بلغت ٥٣,١٪.

السبب في ذلك وجود الثغرات الأمنية التي يستغلها المخترق للتسلل للأجهزة والأنظمة، عدم استخدام برنامج أمان قوي قادر على حماية البيانات الحساسة، عدم الالتزام بممارسات النظافة الرقمية، الدخول إلى المو اقع المجهولة وفتح رسائل البريد الإلكتروني من أشخاص مجهولين، تثبيت التطبيقات غير المعروفة وما إلى ذلك من العمليات التي من شأنها الإيقاع بالأفراد والمؤسسات والنيل منهم.

جدول (٢٨) يوضح أكثر أنواع حوادث الأمن السيبراني بالجامعات موضع الدراسة.

س	الجامعة	فيرس الفدية		الاختراق		قرصنة الهاتف.		الاختراق الابتزاز السيبراني/الإلكتروني. قرصنة الهاتف.		الابتزاز السيبراني/الإلكتروني.		فيرس الفدية الابتزاز السيبراني/الإلكتروني.		الاختراق فيرس الفدية		الاختراق قرصنة الهاتف		قيم مفقودة		الإجمالي	
		ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%	ع	%
في حالة الإجابة بـ نعم أيًا من برامج المكافحة التالية تستخدم.	جامعة بني سويف	10	4.4	20	8.9	6	2.7	1	4	5	2.2	1	1	4	1.3	3	1.3	176	78,2	225	100
	جامعة النهضة	11	34.4	3	9.4	1	3.1	–	–	–	–	1	1.3	1	1.3	–	–	15	46,9	32	100
	الجامعة التكنولوجية	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	8	100	8	100

شكل (٩) يوضح أكثر أنواع حوادث الأمن السيبراني بالجامعات موضع الدراسة.



يوضح الجدول رقم (٢٨) والشكل السابق أكثر أنواع الحوادث حدوثًا بالجامعات موضع الدراسة وهما فيرس الفدية، والاختراق والملاحظ أن النصيب الأكبر من فيرس الفدية كان بجامعة النهضة حيث بلغت نسبتها ٣٤,٤٪ مقارنة بجامعة بني سويف التي بلغت نسبتها ٤,٤٪ وهو شيء لا يذكر إلى جانب هذه النسبة الضخمة. وأن الجامعة التكنولوجية قد جاءت نسبتها مقدرة بـ(٠) وهذا أمر طبيعي بالنسبة لها فليس لديهم ما يجعلهم فريسة أمام المخترقين والهواة. وكما كانت النهضة أعلى معدلًا من حيث الإصابة بفيرس الفدية فهي الأعلى أيضًا من حيث الاختراق حيث بلغت نسبتها ٩,٤٪ مقارنة ببني سويف ٨,٩٪. وهذه النسب إن دلت على شيء فهي تدل على قوة الأمان بجامعة بني سويف والقدرة العالية لتحقيق الحماية بخلاف جامعة النهضة، وأن هذه النتيجة تنفي النتيجة السابقة الموجودة في جدول (٢٥) الخاص بإدارة الأمان والمخاطر وهى أن جامعة النهضة أفضل من جامعة بني سويف في اتخاذ إجراءات الأمان وهذا بدليل نسب تعرضها لفيرس الفدية والاختراق.

جدول (٢٩) يوضح نسب استخدام ادوات كشف الهجمات وخطط التعامل مع الحوادث من قبل الجامعات موضع الدراسة.

س	الجامعة	نعم		لا		الإجمالي	
		ع	%	ع	%	ع	%
هل لديك أدوات تعتمد عليها للكشف عن الهجمات	جامعة بني سويف	٣٠	١٣,٣	١٩٥	٨٦,٧	٢٢٥	١٠٠
	جامعة النهضة	٢٣	٧١,٩	٩	٢٨,١	٣٢	١٠٠
	الجامعة التكنولوجية	٠	٠	٨	١٠٠	٨	١٠٠
هل هناك خطة للتعامل مع الحوادث عند وقوعها	جامعة بني سويف	٣٧	١٦,٤	١٨٨	٨٣,٦	٢٢٥	١٠٠
	جامعة النهضة	٢٢	٦٨,٨	١٠	٣١,٣	٣٢	١٠٠

الجامعة التكنولوجية	٤	٥٠	٤	٥٠	٨	١٠٠	

يتبين من الجدول السابق ان ١٣,٣٪ من جامعة بني سويف يعتمدون على أدوات لكشف الهجمات، وأن ٨٦,٧٪ منهم لا يقومون بذلك ولعل السبب في ذلك يعود إلى عاملين إما أنهم ليسوا بحاجة لها ولديهم البديل، أو أنهم ليسوا على دراية بها. كما أفادت الجامعة التكنولوجية بأنها لا تستخدم أيًا من تلك الأدوات، وهذا أمر ليس بغريب فهي بحاجة إلى الكثير من التطوير. أما جامعة النهضة فكانت أعلى نسبة لاستخدام هذه الأدوات والأقل في عدم استخدامها وربما يكون ذلك بسبب وعيها بمثل هذه الأدوات والكيفية التي تُستخدم بها. كما يتضح من خلال الجدول أن الجامعات الثلاث لديهم خطط للتعامل مع الحوادث السيبرانية عند وقوعها وأكدت على ذلك جامعة النهضة بنسبة ٦٨,٨٪، وبني سويف بنسبة ١٦,٤٪، والتكنولوجية بنسبة ٥٠٪. وهذه النتيجة يمكن إثبات صحتها من عدم صحتها من خلال الجدول اللاحق.

جدول (٣٠) يوضح أكثر أدوات كشف الهجمات استخداما من قبل الجامعات الثلاث

الجامعة	في حالة الإجابة بنعم أيًا من الأدوات التالية تستخدم						قيم مفقودة		الإجمالي	
	Darklayer GUARD		VectorN Detection		X-Ploit Resilience					
	ع	%	ع	%	ع	%	ع	%	ع	%
بني سويف	١٢	٥,٣	١١	٤,٩	١٦	٧,١	186	82.7	٢٢٥	١٠٠
النهضة	٣	٩,٤	٤	١٢,٥	١٦	٥٠,٠	9	28.1	٣٢	١٠٠
التكنولوجية	٠	٠	٠	٠	٠	٠	٨	١٠٠	٨	١٠٠

يتضح من الجدول السابق أن أكثر آداه معتمده من قبل جامعتي بني سويف والنهضة هي آداه X-Ploit Resilience وذلك للميزات التي تقدمها حيث أنها: بمثابة نقطة نهاية للتهديدات، آداه مفيدة لتحقيق البرامج القديمة وتقوم تلقائيًا بتصحيح وتحدي معظم البرامج نظرًا لأن المتسللين غالبًا ما يستفيدون من نقاط الضعف الأمنية للبرامج القديمة لهجمات الاستغلال فإن هذه الميزة تعد إضافة أمان ممتازة. (kisahsekolah، ٢٠٢٢).

محور التهديدات: يقيس توجهات الأفراد نحو بعض الممارسات السلبية.

جدول (٣١) يوضح الممارسات السلبية بين الذكور والإناث.

س	النوع	دائمًا		غالبًا		نادرًا		محايد		إطلاقًا		الإجمالي	
		ع	%	ع	%	ع	%	ع	%	ع	%	ع	%
تقوم بالدخول إلى شبكة Wi-Fi	ذكر	٣٦	٢٥	٤٢	٢٩,٢	٣٩	٢٧,١	٦	٤,٢	٢١	١٤,٦	١٤٤	١٠٠
	أنثي	٣١	٢٥,٦	٢٧	٢٢,٣	٤٤	٣٦,٤	٨	٦,٦	١١	٩,١	١٢١	١٠٠

غير مؤمنة كتلك التي توجد في المطاعم والأماكن العامة												
تقوم بتحميل البرامج دون التأكد من موثوقيتها	ذكر	٣٤	٢٣,٦	٣٥	٢٤,٣	٤٤	٣٠,٦	١٠	٦,٩	٢١	١٤,٦	١٤٤	١٠٠
	أنثي	٢٦	٢١,٥	٢٨	٢٣,١	٣٥	٢٨,٩	١٣	١٠,٧	١٩	١٥,٧	١٢١	١٠٠
تقوم بإدخال أي وسيط لجهاز الحاسب أو جهازك الشخصي مثلUSB	ذكر	٤٥	٣١,٣	٥١	٣٥,٤	٣٤	٢٣,٦	٥	٣,٥	٩	٦,٣	١٤٤	١٠٠
	أنثي	٤٦	٣٨	٣٣	٢٧,٣	٢٤	١٩,٨	١١	٩,١	٧	٥,٨	١٢١	١٠٠

يبين الجدول السابق الإختلافات الفردية بين الذكور والإناث من حيث القيام ببعض الممارسات السلبية التي من شأنها يمكن تعرضهم للتهديدات والابتزاز، والملاحظ من خلال الجدول اختلاف نسب كلًا منهم وفق لكل ممارسة يقومون بها حيث عند النظر إلى الدخول إلى شبكات الWi-fi العامة سنجد أن نسبة الذكور الذين لا يدخلون مطلقًا على شبكات الWi-fi العامة تمثل ١٤,٦٪ وهى نسبة قليلة مقارنةً بحجم العينة ولكنها أفضل من نسبة الإناث الذين يفعلن ذلك حيث بلغت نسبتهن ٩,١٪ وبالتالي يكون الإناث هنا أكثر عرضة للتهديدات من الذكور، بالنسبة لتحميل البرامج دون موثوقيتها بلغت نسبة الذكور الذين لا يقومون بذلك مطلقًا١٤,٦٪ والإناث ١٥,٧٪ أي أن الإناث هنا أفضل من الذكور. وبالنسبة لإدخال الوسائط المجهولة للأجهزة مثل USB والفلاشات. فسنلاحظ ارتفاع معدل الذكور عن الإناث فنسبة الذكور٦,٣٪ والإناث ٥,٨٪ إذا فهنا تفوق عنصر الذكور على الإناث. وبتأمل الجدول السابق والنظر إلى السلبيات التي دائمًا ما يقوم بها كلًا من الذكور والإناث سنجد أن نسبة ٧٩,٩٪ من الذكور مُعرضين للانتهاكات والهاكر، وأن نسبة ٨٥,١٪ من الإناث معرضين لنفس التهديدات. وعليه سنجد أن نسبة الإناث المُعرضن للخطر أكبر من الذكور وهو ما يؤكد النتيجة التي تم الوصول إليها في الجدولين (١٢،١٣).

النتائج والتوصيات:

أ- أكثر حادثتي أمن سيبراني تعرضا لها مجتمع الدراسة كانتا فيرس الفدية والاختراق.

ب- أن نسب الاختراقات وفيروسات الفدية في جامعة النهضة أعلى مُعدلا من جامعة بني سويف.

ج- الجامعة التكنولوجية بحاجة إلى الكثير من التطوير.

د- أن الذكور أقل عرضة من الإناث في التعرض للانتهاكات مستقبلًا.

ومن ثم أوصت الدراسة بالآتي:

أ- العمل على تكثيف الإجراءات الأمنية وتطبيق ممارسات النظافة الرقمية بالشكل الأمثل.

ب- أن تقوم الجامعة التكنولوجية بالمزيد من التطويرات التي تجعلها تنهض مثل نظيراتها من الجامعات.

ج- أن يكون هناك الكثير من الدورات والندوات التعريفية بمخاطر الهجمات والاعتداءات التي تتم عبر الإنترنت وما هي سبل الحماية منها وكيفية تطبيقها.

قائمة المراجع:

١. غسان (٢٠١٩). الأمن السيبراني وإدارة مخاطره في مجال الأعمال.متاح من خلال : https://cutt.ly/p1bJTgi

٢. e3arabi. (2020) نظام التشغيل يونيكس Unix. Retrieved from e3arabi: https://cutt.ly/p1bJYLG

3 - e3arabi سبتمبر ٢٠٢١ .(مزايا وعيوب القرص الصلب Advantages and disadvantages of Hard Disk. Retrieved from e3arabi: https://cutt.ly/p1bJYLG

٤ - mobiletrans (2022) .أفضل ١٠ حلول لمشكلات النسخ الاحتياطي والاستعادة في iTunes. Retrieved from mobiletrans: https://mobiletrans.wondershare.com/ar/restore/itunes-backup-restore-problems-and-solutions.html

5-safetydetectives (2022) . مراجعة مكافح الفيروسات Kaspersky في ٢٠٢٢: هل هو برنامج تجسس روسي فعلًا؟ Retrieved from safetydetectives: https://ar.safetydetectives.com/best-antivirus/kaspersky/ .

samma3a(2019) .ايهما افضل نظام ماك ام ويندوز !؟ اليك المقارنة الشاملة Retrieved from samma3a: https://www.samma3a.com/tech/ar/macos-vs-windows/ .

6. Brook, C. (2018, ديسمبر ٥). What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More. Retrieved from digitalguardian: https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more

7. Chak, S. (2015). MANAGING CYBERSECURITY AS A BUSINESS RISK FOR. Baltimore, Maryland.

8. Lewis,James A. (2013, February 12). Raising the Bar for Cybersecurity. Retrieved from Center for Strategic and International Studies.(CSIS): https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf

9. spiceworks.com. (2020). Why you should patch and update your PCs and server computers. Retrieved from spiceworks.com: https://www.spiceworks.com/it-articles/patch-and-update-pc-and-server-computers/

10. Wilson,Chuck&Jadav,Dhaval. (2018, ٢٢ يونية). Cybersecurity Hygiene: 17 Steps Your Business Should Be Taking Now. Retrieved from industryweek: https://www.industryweek.com/technology-and-iiot/cybersecurity/article/22024980/cybersecurity-hygiene-17-steps-your-business-should-be-taking-now