مجلة المكتبات والمعلومات العربية

- برمجيات إدارة كلمات المرور المجانية
- معامل تأثير الدوريات العربية
- ملتقيات المبدعين بالمكتبة المركزية لكلية الهندسة جامعة الأسكندرية
- الطيف المعلوماتي المعرفي
- استخدام شبكات التواصل الاجتماعي العلمية بالجامعات المصرية
- مواقع القرآن الكريم على الإنترنت

دار المريخ للنشر

السنة السابعة والثلاثون - العدد الثالث

يوليو 2017م / شوال 1438هـ

بسم الله الرحمن الرحيم

مجلة المكتبات والمعلومات العربية

السنة السابعة والثلاثون - العدد الثالث
يوليو 2017م / شوال 1438هـ

مجلة المكتبات والمعلومات العربية

تصدر هذه المجلة فصلياً عن دار المريخ، لندن - بريطانيا

دار المريخ للنشر

السنة السابعة والثلاثون | العدد الثالث | يوليو 2017م | شوال 1438هـ

في هـذا العـدد

دراسـات:

☆ برمجيات إدارة كلمات المرور المجانية : دراسة تحليلية مقارنة
د . فايزة دسوقي أحمد 5 - 50

☆ معامل تأثير الدوريات العربية : دراسة ببليومترية
د . إسماعيل رجب عثمان 51 - 86

☆ ملتقيات المبدعين بالمكتبة المركزية لكلية الهندسة جامعة الإسكندرية : دراسة تقييمية للوضع الراهن واستشراف آفاق المستقبل
د . أمنية خير توفيق 87 - 128

☆ الطيف المعلوماتي المعرفي : دراسة استكشافية تحليلية ورؤية جديدة
د . رضا محمد النجار 129-160

☆ استخدام شبكات التواصل الاجتماعي العلمية بالجامعات المصرية : دراسة تحليلية
د . زينب حسن أبو الخير 161-184

☆ مواقع القرآن الكريم على الإنترنت : دراسة تحليلية للمحتوى والنمط المعلوماتي
عائشة محمد عبدالحميد 185-230

المراسلات والاشتراكات والإعلانات:

لجميع الدول العربية والعالم يتفق بشأنها مع

دار المريخ للنشر

☆ المملكة العربية السعودية
الرياض - ص .ب : 10720
الرمز البريدي 11443
فاكس : 4657939 (009661)
E: mars@marspub1.com

☆ جمهورية مصر العربية
الجيزة - 4 ش الفرات - المهندسين
ت : 33376579 - 37609971
فاكس : 37609457 (00202)
E: marspub2002@yahoo.com

الاشتراك السنوي:

☆ 200 ريالاً سعودياً بالمملكة .
☆ 60 دولاراً أمريكياً لكافة الدول العربية .
☆ 200 جنيه داخل جمهورية مصر العربية .
☆ 60 دولاراً أمريكياً للدول الأخرى .

المقالات المنشورة بهذه المجلة تعبر عن رأي أصحابها وتخضع للتحكيم الأكاديمي

مجلة المكتبات والمعلومات العربية

مجلة علمية محكمة

رئيس التحرير: الأستاذ الدكتور/ محمد فتحى عبد الهادى

أستاذ المكتبات والمعلومات - كلية الآداب - جامعة القاهرة

مدير التحرير: عبد الله الماجد

سكرتير التحرير: أسامة سلامة أحمد

المستشارون

الأستاذ الدكتور/ ربحي مصطفى عليان
أستاذ علم المكتبات والمعلومات
وعميد كلية العلوم التربوية
جامعة الزرقاء الخاصة (الأردن)

الأستاذ الدكتور/ سعد سعيد الزهري
أستاذ علم المعلومات المساعد
بجامعة الملك سعود (السعودية)

الأستاذ الدكتور/ سعد بن عبد الله الضبيعان
أستاذ المكتبات والمعلومات
قسم المكتبات والمعلومات بكلية الآداب
جامعة الملك سعود (السعودية)

الأستاذ الدكتور/ شريف كامل شاهين
أستاذ المكتبات والمعلومات
كلية الآداب - جامعة القاهرة (مصر)

الأستاذة الدكتورة/ مبروكة عمر محيريق
أستاذ المكتبات والمعلومات
الأكاديمية الليبية - طرابلس (ليبيا)

الأستاذ الدكتور/ هشام بن عبدالله العباس
أستاذ علم المكتبات والمعلومات
جامعة الملك عبد العزيز (السعودية)

الأستاذ الدكتور/ وحيد قدورة
أستاذ المكتبات والمعلومات
المعهد الأعلى للتوثيق (تونس)

الأستاذ الدكتور/ ياسر يوسف عبد المعطي
أستاذ المكتبات والمعلومات
قسم علوم المكتبات والمعلومات
كلية التربية الأساسية (الكويت)

الأستاذ الدكتور/ يحيى محمود بن جنيد
الأمين العام لمركز الملك فيصل
للبحوث والدراسات الإسلامية (السعودية)

قواعد النشر

1 – مجلة المكتبات والمعلومات العربية ، تصدر أربع مرات في العام ، صدر عددها الأول في يناير 1981م ، تتولى نشرها دار المريخ للنشر بالرياض وتصدر عن مكتبها بلندن (مؤقتا) .

2 – تقدم البحوث والمقالات والترجمات مطبوعة على الآلة الكاتبة على مسافتين على وجه واحد .

3 – تخضع الدراسات المقدمة للنشر في المجلة للتحكيم العلمي .

4 – يرفق الباحث ملخصاً لبحثه في حدود 100 كلمة (مائة كلمة) تصدر البحث .

5 – ترسم الأشكال والرسوم البيانية بالحبر الصيني على ورق «كلك» حتى تكون صالحة للطباعة أما الصور الفوتوغرفية فيراعى أن تكون مطبوعة على ورق لماع ، وإذا كانت ملونة فلابد من تقديم الشريحة الأصلية .

6 – يراعى وضع خطوط متعرجة تحت العناوين الجانبية ، وكذلك الألفاظ والعبارات التي يراد طبعها ببنط ثقيل ، كما توضع خطوط عادية أسفل عناوين الكتب والدوريات .

7 – يراعى كتابة علامات الترقيم بعناية (النقطة ، علامة الاستفهام ، علامة التعجب . . . الخ) في كتابة البحث وبصفة عامة يتبع الأسلوب العلمي في الكتابة .

8 – يفضل كتابة المصادر والحواشي في نهاية البحث ، وتأخذ أرقاماً مسلسلة وفقاً للقواعد الحديثة للوصف الببليوجرافي .

9 – أصول البحوث والمقالات التي تصل المجلة لاترد ولاتسترجع سواء نشرت أو لم تنشر بالمجلة .

10 – يخضع تنسيق البحوث والمقالات وترتيبها داخل العدد لاعتبارات فنية لاعلاقة لها بمكانة الكاتب .

11 – لاتقبل المجلة نشر البحوث أو المقالات أو الترجمات التي سبق نشرها ، كما لايجوز إعادة النشر في مجلات علمية أخرى بعد إقرار نشرها في هذه المجلة إلا بعد الحصول على إذن كتابي من هيئة تحرير المجلة .

12 – تقبل البحوث المكتوبة باللغتين العربية والإنجليزية على أن تكون الأبحاث باللغة الإنجليزية ، عن تجارب وإسهامات عربية في مجال المكتبات والمعلومات .

13 – تأمل هيئة التحرير من السادة الأساتذة الباحثين والكُتاب الذين يرغبون في نشر بحوثهم ومقالاتهم في الأعداد القادمة من المجلة أن يلتزموا بالإرشادات هذه ، لأن هذا يساعد هيئة تحرير المجلة على أداء عملها كما يساهم في خدمة أهداف المجلة ، وسنعتذر عن قبول أية مقالة أو بحث لايلتزم مؤلفها بتلك القواعد .

14 – تمنح إدارة المجلة لمؤلف كل بحث أو مقالة نسخة مجانية من المجلد الذي نشر به البحث أو المقال .

15 – توجه جميع المراسلات الخاصة بالمجلة إلى : دار المريخ للنشر على عنوانها التالي :

ص.ب: 10720 – الرياض: 11443 – المملكة العربية السعودية

للبحث في جميع أعداد المجلة السابقة منذ صدورها في يناير عام 1981 يمكن زيارة موقع :

www.cybrarians.info

دراسات

برمجيات إدارة كلمات المرور المجانية:

دراسة تحليلية مقارنة

د. فايزة دسوقي أحمد

أستاذ علم المعلومات المساعد (المشارك)

قسم علوم المعلومات– كلية الآداب– جامعة بني سويف

قسم المعلومات ومصادر التعلم – كلية الآداب والعلوم الإنسانية – جامعة طيبة

ملخص :

تهدف الدراسة إلى تعريف ماهية برمجيات إدارة كلمات المرور المجانية، وفوائدها والمشكلات التي تواجهها، ولتحقيق هذا الهدف تم دراسة 15 برمجية. واستخدمت الباحثة المنهج المسحي الميداني والمنهج المقارن، وتمثلت أدوات الدراسة في قائمة المراجعة، والملاحظة. ومن أهم النتائج التي توصلت لها الدراسة: أن البرمجيات عينة الدراسة تعمل على 3 منصات، هي: الحواسيب، والهواتف الذكية والأجهزة اللوحية، والإنترنت. وتدعم 6 نظم تشغيل، هي: **Windows, Linux, Android, iOS, MAC OS X, Windows Phone**. *كما تدعم 6 متصفحات هي:* **Chrome, Internet Explorer, Firefox, Safari, Opera, Yandex**. *وتعمل غالبيتها بنظام المصدر المغلق، وتدعم 6 برمجيات منها فقط اللغة العربية. وتتنوع خدماتها، حيث بلغ عددها 12 خدمة تتمثل في: حفظ كلمات المرور، وتوليد كلمات المرور، والتسجيل اليدوي لكلمات المرور، والتقاط كلمات المرور من المتصفح، وتنظيم كلمات المرور، واستيراد كلمات المرور، وتصدير كلمات المرور، ومشاركة كلمات المرور، والنسخ الاحتياطي لكلمات المرور، وحفظ المعلومات، وحسابات بعد الموت والطوارئ، والمزامنة. وبلغ عدد الإجراءات الأمنية التي تتبعها 9 إجراءات، تتمثل في: التوثق بكلمة مرور رئيسة قوية، والتوثق بخاصية حيوية، وتقييم قوة كلمة المرور، وعدم استعادة كلمة المرور الرئيسة، وعدم نقل كلمة المرور الرئيسة عبر الإنترنت، وعدم الاحتفاظ بكلمة المرور الرئيسة على جهاز المستخدم، وعدم الاحتفاظ بكلمة المرور الرئيسة على خادم البرمجية، والخروج بشكل آلي عند إغلاق المتصفح أو الحاسوب أو الهواتف الذكية*

والأجهزة اللوحية، واستخدام نظام تشفير آمن. وتتوافر 7 طرق للدعم الفني بها، تتمثل في: أسئلة وإجابة جاهزة، ودليل مستخدم، وفيديو، ونموذج، ومحادثة مباشرة، وبريد إلكتروني، ومنتدى/ مدونة. ووفقًا للدراسة التحليلية للبرمجيات عينة الدراسة فإن أفضل ثلاث برمجيات وفقًا للخصائص التي توفرها للمستخدمين هي على التوالي: Enpass, LogMeOnce, LastPass. كما اختتمت الدراسة بمجموعة من التوصيات تتعلق بالاختيار الأمثل لبرمجيات إدارة كلمات المرور، والسمات الواجب توافرها في كلمة المرور الرئيسة، واستخدام وسائل داعمة لتحقيق المزيد من الحماية لكلمات المرور.

0/ تمهيد:

تم تطوير أول كلمة مرور للحاسوب في عام 1961 في معهد ماساتشوستس للتكنولوجيا، لاستخدامها مع نظام Compatible Time-Sharing System (CTSS)، وقد تم تصميم هذا النظام لاستيعاب العديد من المستخدمين في وقت واحد وعلى نفس المعالج الأساسي، مما تطلب توافر نقطة دخول شخصية (كلمة مرور فردية) إلى النظام لكل باحث، يدخل منها إلى النظام عبر الطرفيات. وقد كانت كلمات المرور الأولى هذه بسيطة سهلة التخزين ؛ لعدم وجود قرصنة متطورة وقتها، وعدم وجود برمجيات لكسر كلمات المرور، ولهذا فقد تم حفظ جميع كلمات المرور في النظام. ولكن في 1962 قام باحث الدكتوراه Allan Scherr والذي كان مشتركًا آن ذاك في نظام (CTSS)، بنسخ جميع كلمات المرور المخزنة في الحاسوب حتى يستطيع الدخول من خلالها بحسابات مختلفة، لأن المدة المخصصة له كانت أربع ساعات فقط في الأسبوع، ولم تكن كافية له، فلجأ إلى تلك الحيلة. وتعد هذه أول عملية قرصنة لكلمات المرور، ولم تتوقف قرصنة كلمات المرور من حينها. ورغم التقدم في أنظمة الحاسوب، والاهتمام بعمليات تأمين كلمات المرور إلا أنها وحتى يومنا هذا ما زالت عرضة للخطر. ويرجع ذلك إلى حد كبير إلى أن كلمات المرور التي يستخدمها الأشخاص بسيطة للغاية (يميل المستخدم إلى جعل كلمة المرور قصيرة وسهلة التذكر)، بالإضافة إلى أن العديد من الأنظمة تسمح للمستخدم بتخمين كلمة المرور عدة مرات، وإتاحة خيار "نسيت كلمة المرور" وهي الخاصية التي يمكن من خلالها إعادة تعيين كلمة المرور (Hiscott, 2013).

وقد أوضحت الدراسات التي أجريت في مجال أمن المعلومات، أن الملايين من المتسوقين عبر الإنترنت وعملاء البنوك على الإنترنت يتعرضون لخطر الاحتيال وسرقة الهوية والابتزاز لأنهم فشلوا في حماية حساباتهم بكلمات مرور آمنة. فحوالي (75%) من الأشخاص لا

ينشئون كلمات مرور قوية، مما يعرضهم لخطر الوقوع ضحية للقراصنة الذين يقتنصون بيانات بطاقات الائتمان أو البيانات المصرفية أو المعلومات الشخصية أو الصور الفوتوغرافية، إلخ. وحوالي ثلثي الأشخاص يستخدمون كلمات مرور ضعيفة للغاية، على سبيل المثال أسماء أطفالهم، 123456, Iloveyou, password، الخ. وأن الاحتيال الذي يتم عبر اختراق الحسابات باستخدام كلمات المرور يصل إلى ملايين الدولارات سنويًا، وأن متوسط الحسابات التي يتعامل معها المستخدم قد تصل إلى 19 حسابًا. وأن عدد كبير من المستخدمين لديهم حسابات على مواقع الإنترنت لا يمكنهم الدخول إليها لأنهم نسوا كلمة المرور (Drury, 2012).

ورغم مخاطر استخدام كلمات المرور إلا أنه من المؤكد أن المستخدم سيستمر في استخدامها لفترة من الزمن لن تكون بالقصيرة، وحتى مع بدء استخدام الخصائص الحيوية في التعرف على هوية المستخدم، والتي ويُقصد بها السمات الجسدية للشخص physical characteristic مثل بصمات الأصابع وشبكية العين (McRobbie, 2003)، سيستمر استخدام كلمات المرور، نظرًا لما يكتنف السمات الحيوية من بعض المشكلات، وألفة المستخدم بكلمات المرور، والاعتياد على استخدامها.

1/ المقدمة المنهجية :

1/1 التعريفات الإجرائية:

المصطلح الأساس في هذه الدراسة هو :

برمجيات إدارة كلمات المرور Passwords Management Software

تُعرف برمجيات إدارة كلمات المرور بأنها تطبيقات برمجية تساعد المستخدمين على إنشاء كلمات المرور وجمعها وتخزينها وتنظيمها داخل قاعدة بيانات مُشفرة (Trumps, 2016) ويتم الوصول إلى قاعدة البيانات باستخدام كلمة مرور رئيسة MasterPassword. وتحتوي قاعدة البيانات على اسم المستخدم وكلمة المرور لكل موقع يريد المستخدم الاحتفاظ به في البرمجية.

ومن المصطلحات الإنجليزية التي يتم استخدامها للدلالة على هذه البرمجيات

Passwords management software، وpassword-managing software، و Password managers.

2/1 موضوع الدراسة وأهميته:

تعد كلمات المرور من أكثر أساليب الحماية المستخدمة من قِبل المستخدمين لضمان أمن المعلومات، بالإضافة إلى أن تسجيل الدخول لغالبية المواقع على الإنترنت للاستفادة من

خدماتها تتطلب اسم مستخدم وكلمة مرور. ومن المؤكد أن كلمات المرور تتعرض للعديد من المخاطر مما يستدعي استخدام العديد من الطرق لحمايتها ومن بين هذه الطرق استخدام «برمجيات إدارة كلمات المرور» التي تساعد المستخدم كثيرًا في إدارة كلمات مروره والحفاظ عليها آمنة.

وتستمد الدراسة أهميتها من أهمية حماية كلمات المرور بوصفها خطوة أساسية للتمتع ببيئة إنترنت آمنة، خاصة في ظل تنوع الجرائم المعلوماتية الموجهة نحو انتهاك أمن المعلومات، ولأن كلمات المرور إذا تم الكشف عنها فسيتم الكشف عن كل ما تحويه حسابات المستخدم من معلومات، مثل الحسابات البنكية، والبريد الإلكتروني، والشبكات الاجتماعية، والتجارة الإلكترونية، ... الخ. بالإضافة إلى أنها دراسة منهجية علمية تساعد المستخدمين في عملية اختيار برمجيات كلمات المرور الأكثر ملاءمة لاحتياجاتهم، وتحقيقًا لأمن كلمات مرورهم، والأكثر ثقة، لأن بعض برمجيات إدارة كلمات المرور قد تكون برمجيات تجسسية تسطو على كلمات مرورهم، وربما يستخدمونها دون الانتباه لذلك.

وقد انصبت الدراسة على البرمجيات المجانية لأنها عادة ما تكون الأكثر استخدامًا من قِبل المستخدمين الذين يفضلون التطبيقات المجانية عن المدفوعة، للتأكد من كفاءة تلك البرمجيات وتوافر الأمن فيها.

3/1 أهداف الدراسة:

تهدف الدراسة إلى تعريف ماهية برمجيات إدارة كلمات المرور المجانية، وفوائدها والمشكلات التي تواجهها، وعرض نماذج من هذه البرمجيات للتعرف على الخدمات التي توفرها، ومدى توافر الأمن بها.

4/1 تساؤلات الدراسة:

تتمثل تساؤلات الدراسة في:

- ما المخاطر التي تتعرض لها كلمات المرور؟
- ماهية برمجيات إدارة كلمات المرور، وطريقة عملها؟
- ما فوائد برمجيات إدارة كلمات المرور؟
- ما مخاطر استخدام برمجيات إدارة كلمات المرور؟
- ما المنصات التي تعمل عليها برمجيات إدارة كلمات المرور المجانية؟

- ما نظم التشغيل التي تدعمها برمجيات إدارة كلمات المرور المجانية؟
- ما متصفحات الإنترنت التي تدعمها برمجيات إدارة كلمات المرور المجانية؟
- ما نوع المصدر في برمجيات إدارة كلمات المرور المجانية؟
- هل تدعم واجهات برمجيات إدارة كلمات المرور المجانية اللغة العربية؟
- ما الخدمات التي توفرها برمجيات إدارة كلمات المرور المجانية؟
- ما إجراءات الحماية التي توفرها برمجيات إدارة كلمات المرور المجانية؟
- ما طرق الدعم الفني التي توفرها برمجيات إدارة كلمات المرور المجانية؟
- ما أفضل برمجية مجانية لإدارة كلمات المرور يمكن استخدامها؟

5/1 عينة الدراسة:

قامت الباحثة بالبحث في الإنترنت عن برمجيات إدارة كلمات المرور المجانية، وقد تم حصر 15 برمجية مجانية (بغض النظر عما إذا كان يتوافر من البرمجية نسخة مدفوعة أم لا) ستمثل عينة الدراسة. ويبين الجدول رقم (1) عينة الدراسة من برمجيات إدارة كلمات المرور.

الجدول رقم (1) عينة الدراسة (*)

م	البرمجية	م	البرمجية
1	Access Manager	9	Norton Identity Safe
2	Dashlane	10	PassBox
3	Efficient Password Manager	11	Password Memory
4	Enpass	12	Password Safe
5	Intuitive Password	13	Passwordbox
6	Keepass	14	RoboForm
7	LastPass	15	Safe in Cloud
8	LogMeOnce		

(*) تم ترتيب البرمجيات ترتيبًا هجائيًا.

والجدير بالذكر أن الدراسة استبعدت البرمجيات المدمجة Built- In في المتصفحات والتي توفرها المتصفحات مجانًا لإدارة كلمات المرور للمواقع التي يدخل إليها المستخدم، وتعمل كجزء من المتصفح، نظراً للطبيعة المختلفة لها عن البرمجيات التي توفرها جهات متخصصة وهو ما تنصب عليه عينة الدراسة الحالية.

6/1 حدود الدراسة:

أجريت الدراسة الميدانية على برمجيات إدارة كلمات المرور المجانية عينة الدراسة، في شهري فبراير ومارس من عام 2016.

7/1 منهج البحث وأدواته:

استخدمت الباحثة المنهج المسحي الميداني، والمنهج المقارن للمقارنة بين الخصائص المختلفة للبرمجيات عينة الدراسة. وتمثلت أدوات الدراسة في قائمة المراجعة التي تكونت من (8) أسئلة تم إعدادها لجمع البيانات التي تحتاج إليها الدراسة، والمتعلقة بالتعرف إلى المنصات التي تعمل عليها برمجيات إدارة كلمات المرور، ونظم التشغيل ومتصفحات الإنترنت التي تدعمها برمجيات إدارة كلمات المرور، ونوع المصدر في برمجيات إدارة كلمات المرور، والخدمات وإجراءات الحماية وطرق الدعم الفني التي توفرها برمجيات إدارة كلمات المرور. بالإضافة إلى الملاحظة التي اعتمدت عليها الباحثة لتحديد خصائص البرمجيات عينة الدراسة.

8/1 الدراسات السابقة:

تبين من استعراض الباحثة لما تم من دراسات عربية وأجنبية في الأدلة والببليوجرافيات التي ترصد الإنتاج الفكري في مجال المكتبات والمعلومات، فيما يتعلق بدراسة برمجيات إدارة كلمات المرور، ما يلي:

- عدم وجود دراسة عربية (على حد علم الباحثة) تناولت الموضوع.
- وجود عدد من الدراسات الأجنبية تناولت الموضوع، وجاءت على النحو التالي:

قام Silver وآخرون بدراسة أمن برمجيات إدارة كلمات المرور، وسياستها المتعلقة بالتعبئة التلقائية لكلمات المرور على الإنترنت، وقد تنوعت المنصات التي تعمل عليها برمجيات الدراسة، حيث تمت دراسة برمجيات إدارة كلمات مرور مدمجة في المتصفحات، وعلى الأجهزة المحمولة، والبرمجيات التي توفرها الشركات المتخصصة، وقد اشتملت عينة الدراسة على Chrome, Firefox, Safari, 1Password, Keeper, Keepass, LastPass، وتوصلت الدراسة إلى وجود فروق مهمة في سياسات التعبئة بين البرمجيات التي تم دراستها، ومن أهم النتائج التي توصلت لها أن بعض سياسات التعبئة تلك قد تؤدي إلى عواقب كارثية إذا تمت مهاجمة الشبكة، حيث يمكن للمهاجم الحصول على كلمات مرور المستخدم دون علمه، ومن أهم التوصيات التي قدمتها الدراسة أن التعبئة التلقائية لكلمات المرور ينبغي أن تتم فقط للمواقع الآمنة (HTTPS) ولا تتم للمواقع غير الآمنة (HTTP) (Silver, … [et al.,], 2014).

كما سعت دراسة أخرى إلى تحليل الجوانب الأمنية في برمجيتين من برمجيات إدارة كلمات المرور هما LastPass و RoboForm، مع التركيز على آليات التشفير المستخدمة فيهما، وقد توصلت الدراسة إلى وجود العديد من أنواع المخاطر (مخاطر حرجة وعالية ومتوسطة) في البرمجتين، يمكن استغلالها من قِبل المهاجمين لكسر أمن هاتين البرمجيتين، وقد سعت الدراسة إلى تقديم بعض الاقتراحات التي تسهم في تحسين التصميم الأمني للبرمجتين (Zhao, Yue, & Sun, 2013).

وعرض McCarney وآخرون ورقة توضح الخطوات التي قاموا بها لتصميم واستخدام وتقييم برمجية لإدارة كلمات المرور تُسمى Tapas، وهي برمجية متوافقة مع المصادقة المستندة إلى كلمة المرور Password-Based Authentication، كما أنها لا تعتمد على استخدام كلمة مرور رئيسة، ولا تتطلب إدخال تغييرات من جانب الخادم على مواقع الويب، ولديها القدرة على حماية كلمات المرور المخزنة في حالة سرقة الجهاز الأساسي أو الثانوي (على سبيل المثال، الحاسوب أو الهاتف الذكي)، وقد حاولوا دراسة كفاءتها الأمنية وتعهدوا بمواصلة تطويرها حتى يمكن استخدامها بشكل آمن (McCarney ... [et al.], 2012). وفي عام 2013 قدم McCarney رسالته للماجستير حول نفس البرمجية Tapas، وعرض فيها لخصائص البرمجية، ودراسة تقييمية لها حيث تم تجريبها من قِبل 30 مستخدم ومقارنتها ببرمجية إدارة كلمات المرور المدمجة في متصفح Firefox، وقد أفاد المستخدمون أنهم يفضلون Tapas عن البرمجية المدمجة في Firefox، وتم إدخال التعديلات على البرمجية وفقًا للدراسة التقييمية، أعيدت بعدها الدراسة التقييمية على 10 مستخدمين آخرين، للتأكد من كفاءتها(McCarney, 2013).

كما أجريت دراسة استشكافية حول برمجيات كلمات المرور المعتمدة على المتصفحات، هدفت إلى استكشاف سهولة استخدام كلمات المرور الرسومية والإجراءات الأمنية المتوافرة بها، وأجريت الدراسة التطبيقية على برمجية تُدعى iPMAN، وقدمت طرقًا يمكن من خلالها مجابهة الهجوم على البرمجية (Bicakci... [et al.,], 2011). كما تناولت دراسة قام بها (Al-Sinani & Mitchell, 2011) تطوير برمجية PassCard حتى تستطيع البرمجية استخدام كلاً من مواقع HTTP و HTTPS، ويمكن تسجيل اسم المستخدم وكلمة المرور في البرمجية، واستخدامها للدخول إلى مواقع الويب، ولا تتطلب البرمجية أية تغييرات في الخوادم، وتصف الدراسة النسخة الجديدة من البرمجية، وكيفية عملها، وتحلل القضايا الأمنية بها، وكذلك تعرض سهولة استخدامها.

كما هدفت دراسة (Belenko & Sklyarov, 2012) إلى تحليل تطبيقات برمجيات إدارة كلمات المرور على الأجهزة المحمولة مثل Apple iOS و BlackBerry، وقد ركزت الدراسة على أمن البيانات، وتوصلت الدراسة إلى وجود العديد من المشكلات الأمنية في هذه البرمجيات.

وسعت دراسة ([Li, Zhiwei... [et al.,) إلى إجراء تحليل أمني لخمس برمجيات لإدارة كلمات المرور تعتمد على استخدام متصفحات الإنترنت، هي LastPass و RoboForm و Passwordbox و My1login و NeedMyPassword، وذلك لمعرفة المخاطر الأمنية التي يمكن أن تواجهها هذه البرمجيات، ومن أهم النتائج التي توصلت لها الدراسة وجود نقاط ضعف شديدة في جميع البرمجيات عينة الدراسة، حيث يمكن للمهاجمين سرقة البيانات من حساب المستخدم، وقد قدمت الدراسة مقترحات فنية لمواجهة هذه المشكلات.

كما حاول Zhao و Yue اكتشاف نقاط الضعف في برمجيات إدارة كلمات المرور المدمجة في متصفحات Internet Explorer، Firefox، Google Chrome، Safari، Opera، وتحليل الكيفية التي يمكن استغلال هذه النقاط بها للهجوم على كلمات مرور المستخدمين المحفوظة بتلك البرمجيات، وتصميم نظام لتخزين كلمات المرور معتمدة على السحب الإلكترونية، يتوافر فيه مستوى عال من الأمن والسرية والسلامة، والعديد من الخصائص، وقد تم تطبيق هذا النظام في متصفح Firefox لتقييم جوانب الأمن والأداء وسهولة الاستخدام، وبينت النتائج أن النظام المقترح يمكن استخدامه بكفاءة وسهولة، ويمكن أن يتكامل مع المتصفحات لجعل تجربة استخدام الإنترنت أكثر أمنًا وراحة (Zhao & Yue).

يتضح من العرض السابق للدراسات الأجنبية في موضوع برمجيات إدارة كلمات المرور:

- اهتمام الباحثين الأجانب بموضوع برمجيات إدارة كلمات المرور.
- انصب اهتمام الدراسات على القضايا الأمنية في برمجيات إدارة كلمات المرور.
- تناول برمجيات إدارة كلمات المرور المستخدمة على منصات العمل المختلفة.
- تصميم برمجيات لإدارة كلمات المرور، يتوافر فيها الأمن.

وبهذا يمكن القول بأنه لا توجد دراسة عربية -على حد علم الباحثة- تتعلق بموضوع برمجيات إدارة كلمات المرور، مما يستدعي ضرورة معالجة هذا الموضوع نظرًا لأهميته.

2/ المخاطر التي تتعرض لها كلمات المرور:

تتعدد المواقع التي يستخدمها الشخص على الإنترنت، وتشترط غالبية هذه المواقع التسجيل باستخدام اسم مستخدم وكلمة مرور للتأكد من هوية الشخص، ضمانًا لأمن المعلومات

وحفاظًا على خصوصية المستخدم ومعلوماته الحساسة. إلا أن الواقع أثبت أن كلمات المرور عرضة للكثير من أنواع الهجمات،فهناك خطورة من كشف كلمات المرور بعدة وسائل: مثل كسر cracking كلمات المرور الضعيفة، أو استخدام الهندسة الاجتماعية، أو البحث والتنصت.

(1) كسر كلمات المرور الضعيفة:

يمكن كسر كلمة المرور الضعيفة بعدة طرق منها:

(أ) الكسر باستخدام كلمات المعجم :

يقوم المهاجم في هذه الطريقة بمحاولة الدخول للنظام بكتابة كلمة مرور مكونة من أحد كلمات المعجم، وفي هذه الحالة ينبغي أن تكون كلمة المرور مكونة من أحد كلمات المعجم مثل: شمس، فلسطين، عبد الرحمن ...إلخ، وتتعدى تلك الطريقة كلمات المعجم التقليدي إلى محاولة كلمات مرور دارجة مثل 123، 2000... إلخ . وتتميز بأنها سريعة نوعًا ما، لأن عدد الكلمات ليس كثيرًا، وكذلك لوجود الحواسيب السريعة التي يمكن من خلالها محاولة استخدام أكثر من 10 مليون كلمة مرور في الثانية، لكن يعيبها أنها محدودة بكلمات المعجم.

(ب) الكسر باستخدام الطريقة الاستقصائية BruteForce

تُستخدم هذه الطريقة لمعرفة كلمات المرور التي لا تنتمي إلى المعجم أو ليست كلمة معروفة. وتتلخص في تجريب كل الاحتمالات حتى يتم الوصول إلى كلمة المرور، فعلى سبيل المثال لكسر كلمة مرور تتكون من ثلاثة حروف يتم تجريب كل الاحتمالات باستخدام اختبار الحروف والأرقام بالشكل التالي...aaa, aab, aac... aaA, aaB, aaC... aa0, aa1, aa2, aa3 ...aba, aca, ada (Cliff، 2001). وتتميز هذه الطريقة بأنها لا تدع احتمالاً إلا استخدمته. ولكن يعيبها أن تكسير كلمات المرور الطويلة قد يحتاج إلى أيام أو شهور أو سنوات، خاصة مع كلمات المرور المكونة من أكثر من ثماني خانات وتحوي خليطًا من الأرقام والحروف والرموز.

(ج) دمج الطريقتين السابقتين معًا :

في هذه الطريقة تستخدم كلمات القاموس مع تجربة جميع الاحتمالات على الكلمة مثل: CAT، CAT0، CAT1، CAT2، ... CAT9 (الغثبر والقحطاني، 2009).

(د) استخدام البرمجيات لكسر كلمات المرور :

يمكن كسر كلمات المرور يدويًا بالطرق السابقة، ولكن استخدام هذا الأسلوب يستغرق وقتًا طويلاً، لذا يلجأ المعتدون إلى استخدام البرمجيات. وتتنوع البرمجيات التي يمكن

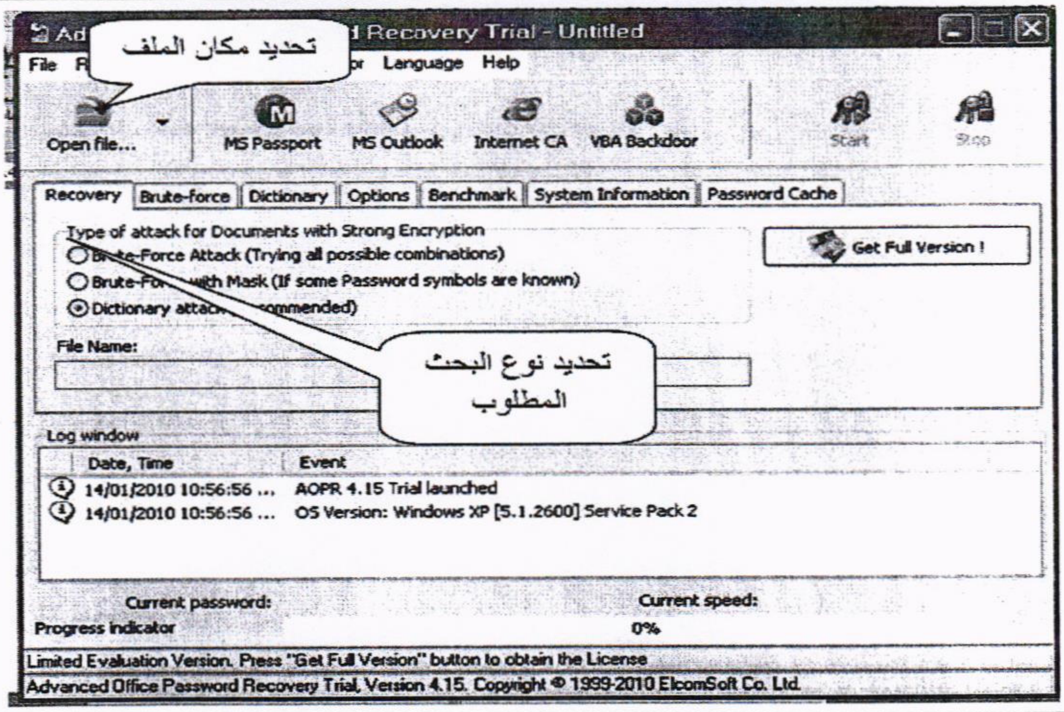
استخدامها لكسر كلمات المرور، فهناك برمجيات لفتح الملفات المضغوطة، وبرمجيات لفتح ملفات Microsoft Office، وأخرى لفتح ملفات PDF .... (Elcomsoft Co. Ltd., 2010)

وقد قامت الباحثة -في بحث سابق (أحمد، 2011)- بتجريب برمجية "Advanced Office Password Recovery" لكسر كلمة المرور في ملف Word لمعرفة مدى قدرة مثل تلك البرمجيات على القيام بذلك. **وقد اتبعت الخطوات التالية:**

- تنزيل برمجية "Advanced Office Password Recovery" وتنصيبها على الحاسوب الشخصي للباحثة من الموقع التالي:

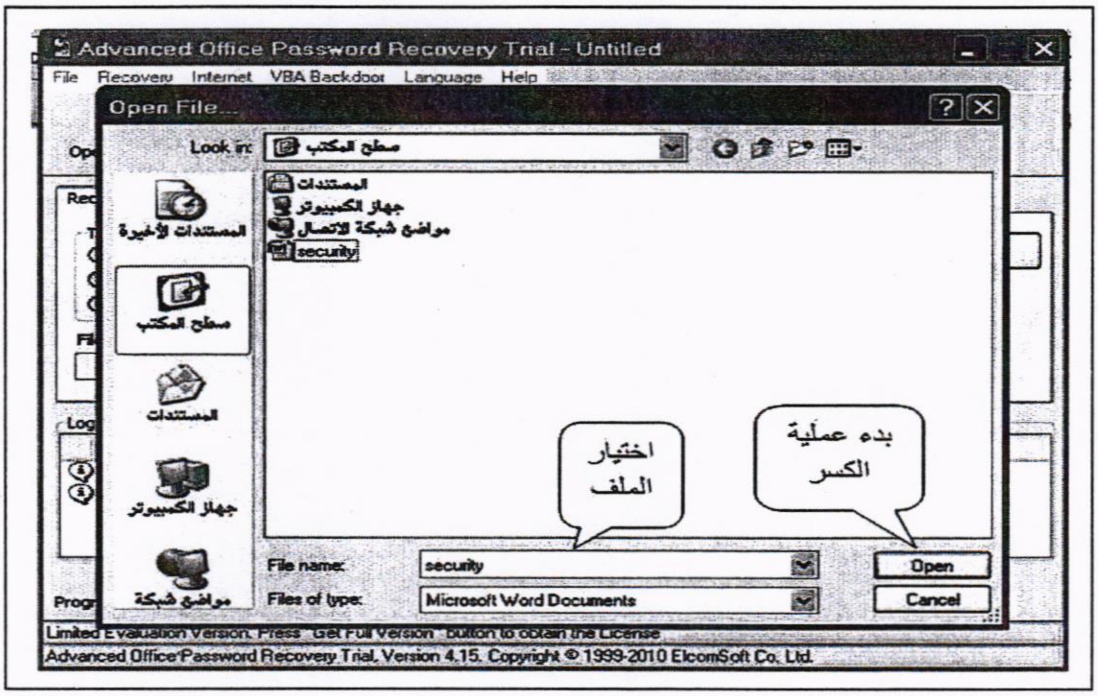
http://www.elcomsoft.com/aopr.html

- حماية ملف Word بعنوان "security" باستخدام كلمة مرور هي "nany".
- استخدام البرمجية لمحاولة كسر كلمة المرور. ويوضح الشكل رقم (1) واجهة البرمجية، وكيفية تحديد مكان الملف المطلوب لكسر كلمة المرور الخاصة به، وتحديد نوع البحث المطلوب باستخدام كلمات المعجم، أو باستخدام الطريقة الاستقصائية.



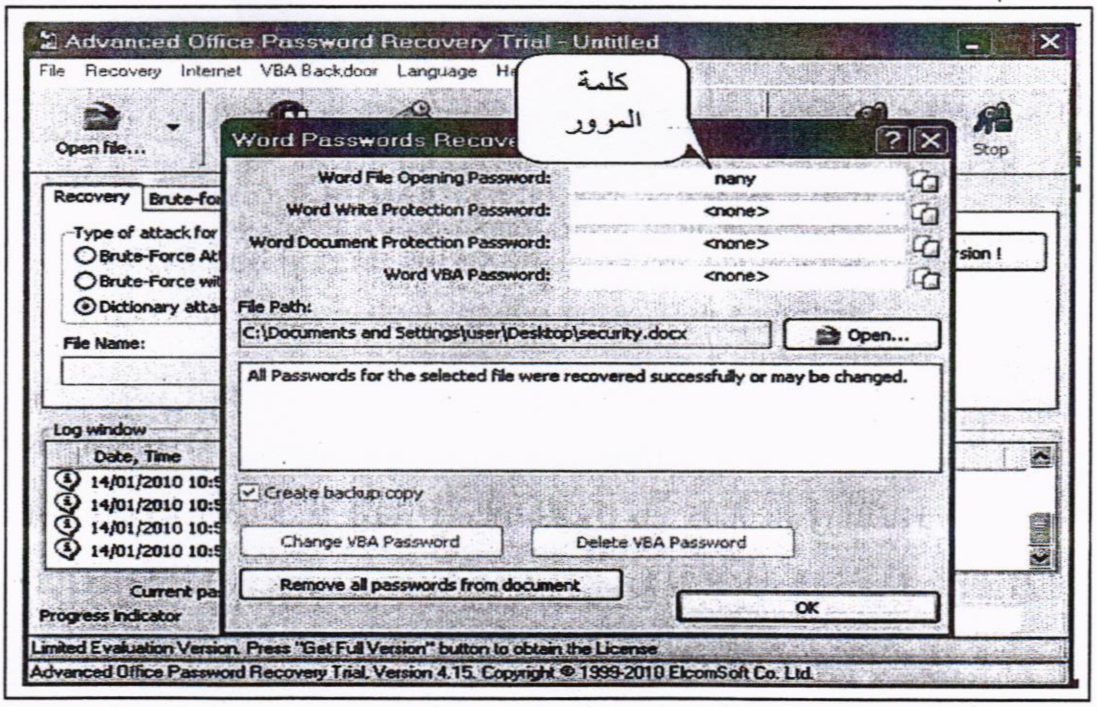
الشكل رقم (1) تحديد مكان الملف لاختياره، وتحديد نوع البحث المطلوب

ويوضح الشكل رقم (2) عملية اختيار الملف المطلوب، وبدء عملية الكسر.



الشكل رقم (2) اختيار الملف المطلوب، وبدء عملية الكسر

كما يبين الشكل رقم (3) اكتشاف البرمجية لكلمة المرور وقد تمت هذه العملية بسرعة كبيرة لم تتجاوز الثانية الواحدة.



الشكل رقم (3) اكتشاف كلمة المرور

والجدير بالذكر أن مثل هذه البرمجيات إذا لم يستطع تحديد كلمة المرور التي وضعها الشخص فإنه في بعض الأحيان قد يصل إلى كلمة مرور أخرى مختلفة عنها إلا أنها تصلح أيضًا لفتح الملف، وهذا ما قد توصل إليه "الغثبر والقحطاني" حيث استخدما برمجية Advanced ZIP Password Recovery (AZPR) لكسر كلمات المرور في الملفات المضغوطة، وكانا قد استخدما كلمة (sami) ككلمة مرور ورغم أن البرمجية لم تتوصل إلى كلمة (sami) إلا أنها اقترحت كلمة أخرى لفتح الملف وهي (ii) وبالفعل نجحا في فتح الملف بها، ويبين هذا كما ذكرا إمكانية وجود أكثر من كلمة مرور لفتح الملفات وعادة ما تكون أسهل وأضعف من كلمة المرور الأساسية (الغثبر والقحطاني، 2009).

(2) استخدام الهندسة الاجتماعية Social Engineering

من تعريفات الهندسة الاجتماعية أنها استخدام مهاجم خارجي لحيل نفسية ضد مستخدم حقيقي لنظام الحاسوب من أجل الحصول على المعلومات التي يحتاجها للوصول إلى النظام، أو الحصول على المعلومات المطلوبة (كلمات المرور على سبيل المثال) من شخص بدلاً من اقتحام النظام (Granger، 2001).

*** أشكال الهجمات باستخدام الهندسة الاجتماعية**

قد يحدث الهجوم باستخدام الهندسة الاجتماعية على صعيدين الأول حسي والثاني نفسي.

(أ) الصعيد الحسي: ومن أشكال هذا الهجوم:

- **مكان العمل**: يدخل المهاجم مكان العمل متظاهرًا بأنه أحد الموظفين، أو المتعاقدين مع جهة العمل، أو عمال نظافة أو صيانة. وإذا تمكن المهاجم من الدخول فإنه يحاول الحصول على كلمات المرور المكتوبة على أوراق ملصقة بشاشة الحاسوب أو لوحة المفاتيح.
- **الهاتف**: يتصل المهاجم بالضحية ويدَّعي حدوث مشكلة فنية ما ويستدرجه للحصول على بعض البيانات ومن بينها كلمات المرور.
- **النفايات**: يستطيع المهاجم في بعض الأحيان الحصول على كلمات المرور الملقاة في النفايات.
- **الإنترنت**: عادة ما يستخدم الشخص كلمة مرور واحدة لاستخدام البرمجيات والتطبيقات المختلفة، وعند اكتشاف كلمة المرور هذه يمكن للمهاجم فتح جميع البرمجيات والتطبيقات التي يستخدمها الضحية. ويمكن الحصول على كلمات المرور من خلال الإنترنت بعدة طرق منها: التظاهر بتقديم خدمات معينة مثل تنزيل البرمجيات مجانًا ويشترط على الشخص

التسجيل باستخدام اسم مستخدم وكلمة مرور، وعند الحصول عليهما يستخدمهما المهاجم في الوصول إلى ما يريد من معلومات تخص الضحية. كما يمكن أن يرسل المهاجم رسالة تبدو أنها من مديري الشبكة التي يستخدم الضحية واحدة أو أكثر من خدماتها، ويطلب من الضحية إعادة إرسال اسم المستخدم وكلمة المرور بسبب وجود تحديثات في الشبكة أو حدوث مشكلة فنية تستلزم ذلك (الغثبر والقحطاني، 2009).

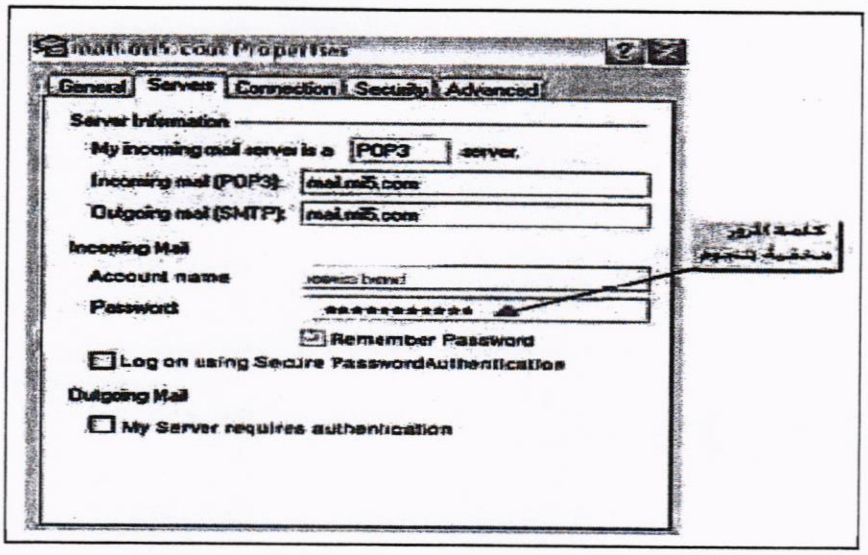
(ب) الصعيد النفسي:

يتعلق هذا الأسلوب بكيفية تهيئة بيئة نفسية مثالية ملائمة للهجوم. ويعتبر الإقناع من أهم الأساليب المستخدمة لذلك، والإقناع له أوجه كثيرة منها: انتحال شخصية شخص أخر (مثل المدير، أو موظف الدعم الفني، ...)، واستغلال العلاقات الودية الموجودة من قبل بين الضحية والمهاجم. وبغض النظر عن الطريقة المستخدمة، فإن الهدف الرئيس هو إقناع الشخص الذي يكشف عن المعلومات بأن المهاجم هو في الواقع شخص يمكن الثقة فيه ومنحه هذه المعلومات الحساسة. وعادة ما يسأل المهاجم أسئلة قليلة حتى يحافظ على مظهر العلاقة المريحة.

وهناك أيضًا أسلوب الهندسة الاجتماعية العكسية Reverse Social Engineering وهو أسلوب متقدم للحصول غير المشروع على المعلومات. ويتلخص هذا الأسلوب في أن المهاجم يصنع موقفًا يبدو فيه أنه يمتلك السلطة والقدرة على معالجة المشكلة التي نتجت عن هذا الموقف، مما يجعل الضحية يطلب منه المساعدة. وهناك ثلاث مراحل للهجوم باستخدام الهندسة الاجتماعية العكسية هي: التخريب، والإعلان، والمساعدة. وتتلخص هذه المراحل في أن المهاجم يقوم بتخريب ما في الشبكة مما يسبب مشكلة، ومن ثم يعلن المهاجم عن نفسه بأنه من فريق الدعم الفني وأنه الشخص المناسب لعلاج هذه المشكلة، وعندما يأتي لعلاجها يطلب معلومات معينة من الموظفين وبهذا يحصل على ما جاء من أجله. وعادة لا يكتشف أحد حقيقة هذا الشخص لأنه يحل المشكلة بالفعل (Granger، 2001).

(3) البحث والتنصت:

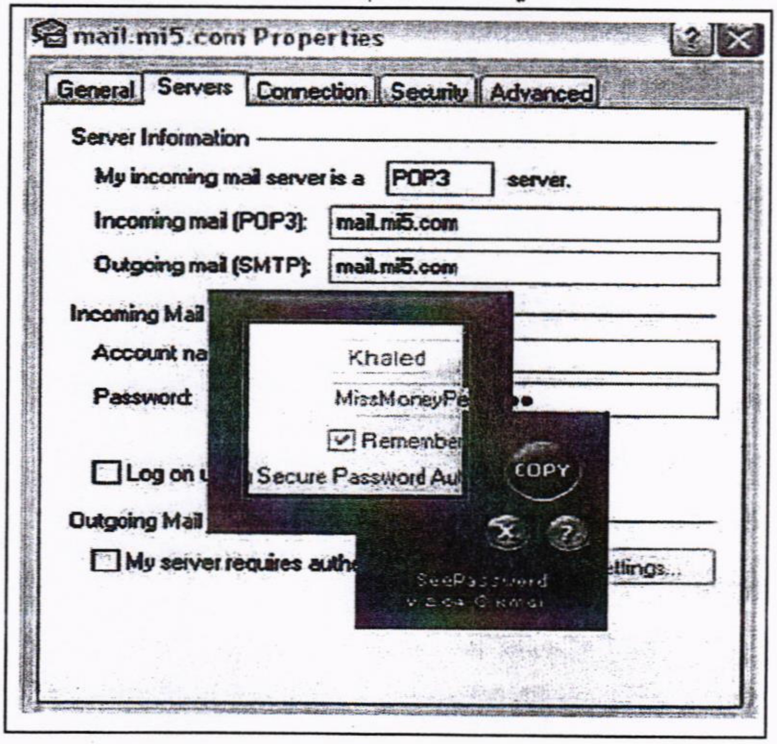
من الأساليب التقليدية المستخدمة في هذه الطريقة الوقوف خلف الضحية عند كتابته كلمة المرور، أو البحث عن كلمة مرور الضحية مكتوبة تحت لوحة المفاتيح. أما الأساليب الحديثة فهي تعتمد على استخدام التقنية، مثل تركيب برمجية تسجل جميع الأحرف والأرقام المدخلة عن طريق لوحة المفاتيح. وهناك طريقة أخرى تتمثل في إمكانية تركيب برمجية في حاسب الضحية، تسمح للمهاجم باكتشاف كلمات المرور المعتمة التي تظهر على شكل نجوم أو دوائر صغيرة (الغثبر والقحطاني، 2009). ويبين الشكل رقم (4) كلمة المرور مخفية:



الشكل رقم (4) كلمة المرور مخفية

(المصدر: الغثبر والقحطاني، 2009)

وباستخدام برمجية تسمى SeePassword وتمريرها على كلمة المرور المعتمة أمكن معرفة كلمة المرور بسهولة، كما هو مبين في الشكل رقم (5).



الشكل رقم (5) معرفة كلمة المرور المخفية

(المصدر: الغثبر والقحطاني، 2009)

يتضح مما سبق الخطورة التي تكتنف استخدام كلمات المرور، لذا ستتناول فيما يلي واحدة من الأساليب المستخدمة لحل المشكلات التي تجابه كلمات المرور، وهي برمجيات إدارة كلمات المرور.

3. برمجيات إدارة كلمات المرور:

يتناول هذا الجزء ماهية برمجيات إدارة كلمات المرور وطريقة عملها، وفوائدها والمخاطر التي تعترضها. والمنصات التي تعمل عليها برمجيات إدارة كلمات المرور عينة الدراسة، ونظم التشغيل ومتصفحات الإنترنت التي تدعمها، ونوع المصدر فيها، والخدمات وإجراءات الحماية وطرق الدعم الفني التي توفرها.

1/3 ماهية برمجيات إدارة كلمات المرور، وطريقة عملها:

تعمل برمجيات «إدارة كلمات المرور» كخزينة تخيلية، فبعد تثبيت البرمجية على جهاز الحاسوب أو الهاتف المحمول أو الجهاز اللوحي أو متصفح الإنترنت، يقوم المستخدم بتسجيل كلمات المرور الخاصة به في هذه البرمجية، والتي تقوم بدورها بتشفير هذه الكلمات وتخزينها ضمن قاعدة بيانات خاصة أو ضمن نظام سحابي على الشبكة. ويتم تأمين هذا التطبيق بواسطة كلمة مرور خاصة يقوم المستخدم بإنشائها، تُسمى كلمة المرور الرئيسة. وبهذه الطريقة عند رغبة المستخدم في الوصول إلى كلمة المرور لتطبيق أو لخدمة معينها يستخدمها، عليه الدخول إلى البرمجية عبر كلمة المرور الرئيسة ليصل إلى كلمة المرور الخاصة بالخدمة أو التطبيق الذي يريد.

وفي حالة برمجيات «إدارة كلمات المرور» التي بها خاصية التكامل مع متصفح الإنترنت، تقوم البرمجية تلقائيًا بتسجيل اسم المستخدم وكلمة المرور الخاصة به عند أول دخول للمستخدم إلى موقع معين. وعند رغبة المستخدم فيما بعد الدخول مرة أخرى إلى هذا الموقع، فإن البرمجية تستعيد اسم المستخدم وكلمة المرور المخزنة بها لهذا الموقع، وبالتالي يتم دخول المستخدم مباشرة، دون الحاجة إلى إدخال اسم المستخدم وكلمة المرور، كما تقوم البرمجية بتحديث كلمات المرور المخزنة إذا قام المستخدم بإدخال كلمة مرور جديدة (The SANS Institute, 2013).

2/3 فوائد برمجيات إدارة كلمات المرور:

توفر برمجيات إدارة كلمات المرور العديد من الفوائد، منها على سبيل المثال:

- عدم الحاجة إلى حفظ العديد من كلمات المرور.

- التكلفة المنخفضة، وأحيانًا مجانية.
- توليد كلمات مرور قوية ومعقدة وصعبة، وبالتالي يصعب كسرها.
- حفظ كلمات المرور بأمان في قاعدة بيانات مُشفرة على الحاسوب أو في سحابة إلكترونية.
- الوصول إلى كلمات المرور المحفوظة من أي مكان وفي أي وقت، بمجرد وجود اتصال بالإنترنت عبر المتصفحات المختلفة، باستخدام الحواسيب والهواتف الذكية والأجهزة اللوحية.
- تنزيل كلمات المرور الموجودة في قاعدة البيانات إلى الحاسوب.
- تخزين بيانات العناوين، وأرقام بطاقات الاعتماد، والإيصالات والملاحظات وغيرها من الوثائق التي تتطلب حفظها بأمان.
- تخزين كلمات المرور مُنظمة بحيث يسهل البحث فيها والاسترجاع منها.
- جعل التجارة الإلكترونية أكثر أمنًا وسهولة (Hunsberger، 2014).
- مزامنة البيانات عبر الأجهزة الحاسوبية واللوحية والهواتف الذكية (Notenboom، 2016).
- عدم الحاجة إلى إعادة إدخال اسم المستخدم وكلمات المرور، عند الدخول إلى مواقع الإنترنت (Community Pepperdine، 2016).

3/3 مخاطر استخدام برمجيات إدارة كلمات المرور:

تتعرض برمجيات إدارة كلمات المرور للعديد من المخاطر منها على سبيل المثال لا الحصر:

- استهدافها من خلال تصميم برمجيات تستطيع تسجيل ضربات لوحة المفاتيح لالتقاط كلمات المرور الرئيسة المستخدمة للدخول إليها (Westervelt، 2014).
- تعرضها لمحاولات الاصطياد الإلكتروني (Le VPN).
- تعرض قواعد البيانات المخزن بها كلمات المرور في خوادم موردي برمجيات إدارة كلمات المرور لهجمات القرصنة (Cluley، 2015).
- بعض هذه البرمجيات هي برمجيات تجسسية تسطو على كلمات المرور (security strong hold, 2016).
- الكشف عن كلمة المرور الرئيسة، يؤدي إلى الكشف عن جميع كلمات مرور المستخدم.
- قد يتم إغلاق البرمجية وإنهاء عملها.

4/3 المنصات التي تعمل عليها برمجيات إدارة كلمات المرور عينة الدراسة:

توجد ثلاث أنواع من المنصات تعمل عليها برمجيات إدارة كلمات المرور، على النحو التالي:

1. برمجيات إدارة كلمات المرور في الحاسوب الشخصي :

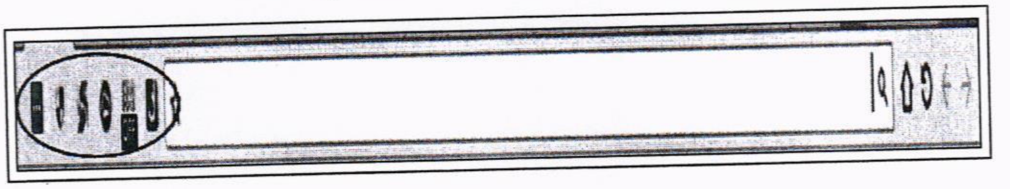
هي برمجيات يتم تحميلها على الحواسيب، وتقوم بتخزين جميع كلمات المرور في قاعدة بيانات واحدة لتسهيل عملية نقلها لأي جهاز آخر "أو في حال تهيئة الجهاز Format"، وتكون قاعدة البيانات مشفرة بشكل قوي بالإضافة إلى حمايتها بكلمة مرور رئيسة.

2. برمجيات إدارة كلمات المرور المعتمدة على الإنترنت :

تعمل هذه التطبيقات بشكل مشابه لبرمجيات إدارة كلمات المرور الخاصة بأجهزة سطح المكتب، ويكمن الفرق فقط في تخزين قاعدة البيانات على خادم Server الشركة المزودة للبرمجية، أو على سحب إلكترونية مشترك فيها المستخدم، لا الحاسوب الشخصي.

وتقوم برمجيات إدارة كلمات المرور المعتمدة على الإنترنت بتشفير قاعدة البيانات "التي تتضمن كلمات المرور"، والتي يستطيع المستخدم الوصول إليها عبر كلمة المرور الرئيسة. وتتم عمليات التشفير وفك التشفير على الحاسوب Local Host لأن الشركة لا تملك مفتاح التشفير (الرقميات، 2013).

ويتم تثبيت البرمجيات في متصفحات الإنترنت في هذا النوع من البرمجيات، ويوضح الشكل رقم (6) مكان إضافة برمجيات إدارة كلمات المرور في المتصفحات.



الشكل رقم (6) مكان إضافة برمجيات إدارة كلمات المرور في المتصفحات

3. برمجيات إدارة كلمات المرور في الهواتف الذكية والأجهزة اللوحية :

تعمل هذه البرمجيات على الهواتف الذكية والأجهزة اللوحية، وفيها يتم تخزين قاعدة البيانات التي تحتوي على كلمات المرور في الهواتف الذكية والأجهزة اللوحية، وتعمل بنفس أسلوب عمل البرمجيات على الحواسيب والإنترنت فيما يتعلق بالتشفير واستخدام كلمة رئيسة لفتح البرمجية.

ويوضح الجدول رقم (2) المنصات التي تعمل عليها برمجيات إدارة كلمات المرور عينة الدراسة.

الجدول رقم (2) المنصات التي تعمل عليها برمجيات إدارة كلمات المرور عينة الدراسة (*)

م	المنصات / البرمجيات	الحواسيب	الهواتف الذكية والأجهزة اللوحية	الإنترنت	المجموع
1	Access Manager	✓	×	×	1
2	Dashlane	✓	✓	✓	3
3	Efficient Password Manager	✓	✓	×	2
4	Enpass	✓	✓	✓	3
5	Intuitive Password	✓	✓	✓	3
6	Keepass	✓	×	×	1
7	LastPass	✓	✓	✓	3
8	LogMeOnce	✓	✓	✓	3
9	Norton Identity Safe	✓	✓	✓	3
10	PassBox	✓	✓	×	2
11	Password Memory	✓	×	×	1
12	Password Safe	✓	✓	×	2
13	Passwordbox	✓	×	✓	2
14	RoboForm	✓	✓	✓	3
15	Safe in Cloud	✓	✓	✓	3
المجموع		**15**	**11**	**9**	**35**
النسبة المئوية		**43**	**301**	**26**	**%100**
الترتيب النسبي		**1**	**2**	**3**	**-**

(*) إجابة السؤال رقم (1) بقائمة المراجعة.

يتضح من الجدول رقم (2) ما يلي:

- تعمل البرمجيات عينة الدراسة على 3 منصات هي: الحواسيب، والهواتف الذكية والأجهزة اللوحية، والإنترنت.
- تعمل8 برمجيات (بنسبة مئوية قدرها 53% من إجمالي عينة الدراسة) على كل من الحواسيب والهواتف الذكية والأجهزة اللوحية وعلى الإنترنت. وتتمثل هذه البرمجيات في Dashlane، Enpass، Intuitive Password، LastPass، LogMeOnce، Norton Identity Safe، RoboForm، SafeinCloud.
- تعمل 4 برمجيات (بنسبة مئوية قدرها 27% من إجمالي عينة الدراسة) على منصتين،

حيث تعمل برمجية Efficient Password Manager، وبرمجية Password Safe، وبرمجية PassBoxعلى الحواسيب، والهواتف الذكية والأجهزة اللوحية. أما برمجية Passwordbox فإنها تعمل على الحواسيب والإنترنت.

- تعمل 3 برمجيات (بنسبة مئوية قدرها 20% من إجمالي عينة الدراسة) على منصة واحدة هي الحواسيب، وتتمثل هذه البرمجيات في PasswordMemory، Keepass، Access Manager.
- أكثر منصة تعمل عليها البرمجيات عينة الدراسة هي الحواسيب حيث تعمل جميع البرمجيات عليها، تليها في المركز الثاني الهواتف الذكية والأجهزة اللوحية، وتوافرت في 11 برمجية من عينة الدراسة، أما الإنترنت فقد جاء في المركز الثالث الأخير، وتعمل عليه 9 برمجيات فقط من عينة الدراسة.

نستنتج مما سبق :

تنوع المنصات التي يمكن أن تعمل عليها البرمجيات عينة الدراسة، ويمكن للمستخدم اختيار ما يتناسب مع احتياجاته منها. وعلى المستخدم أن يعي الفوائد والمخاطر المصاحبة لكل من الأنواع الثلاثة عند الاختيار، فالفائدة الرئيسة من استخدام الحواسيب والهواتف كمنصات تعمل عليها برمجيات إدارة كلمات المرور، تتمثل في وجود قاعدة البيانات على حاسوب المستخدم أو هاتفه الذكي أو جهازه اللوحي، مما يقلل من إمكانية تعرض القاعدة للكشف العرضي غير المقصود (Create IT. Com)، إلا أنها عرضة للإصابة بالبرمجيات الخبيثة التي تصيب الملفات والتطبيقات الموجودة على الحاسوب والهواتف (Nordquist, 2016)، كما أنها لا تتيح إمكانية التقاط كلمات المرور عبر المتصفح، ويقتصر تسجيل كلمات المرور على الشكل اليدوي فقط، مما يحرم المستفيد من الدخول الآلي على مواقع الإنترنت التي له حساب عليها.

بينما تتمثل الفائدة الرئيسة من استخدام الإنترنت كمنصة تعمل عليها برمجيات إدارة كلمات المرور، في وجود قاعدة البيانات المخزن عليها كلمات المرور على الإنترنت، مما يعني إمكانية وصول المستخدم إليها أينما كان طالما يمكنه الاتصال بالإنترنت (CreateIT. Com)، بالإضافة إلى أن لديها القدرة على إدخال اسم المستخدم وكلمة المرور الخاصة بالمستخدم تلقائيًا إلى نماذج تسجيل الدخول على مواقع الإنترنت. إلا أن هناك مشكلة تظهر عند استخدام السحب الإلكترونية والخوادم في تخزين قاعدة البيانات تتلخص في أن السحب والخوادم ليست آمنة، حيث لا يتحكم فيها المستخدم، ولا يعرف أين تُخزن كلمات مروره (Depp, 2014).

5/3 نظم التشغيل التي تدعمها برمجيات إدارة كلمات المرور عينة الدراسة:

تتنوع نظم التشغيل التي يمكن استخدامها على الحواسيب والهواتف الذكية والأجهزة اللوحية. وقد أوضح الجدول رقم (3) نظم التشغيل التي تدعمها برمجيات إدارة كلمات المرور عينة الدراسة.

الجدول رقم (3) نظم التشغيل التي تدعمها برمجيات إدارة كلمات المرور عينة الدراسة (*)

م	نظم التشغيل / البرمجيات	Windows	Linux	Android	iOS	MAC OS X	Windows Phone	المجموع
1	Access Manager	✓	×	×	×	×	×	1
2	Dashlane	✓	✓	✓	✓	✓	✓	6
3	Efficient Password Manager	✓	×	✓	✓	✓	✓	5
4	Enpass	✓	✓	✓	✓	✓	✓	6
5	Intuitive Password	✓	×	✓	✓	×	×	3
6	Keepass	✓	✓	×	×	×	×	2
7	LastPass	✓	✓	✓	✓	✓	✓	6
8	LogMeOnce	✓	×	✓	×	✓	✓	4
9	Norton Identity Safe	✓	✓	✓	✓	×	×	4
10	PassBox	✓	×	×	×	×	×	1
11	Password Memory	✓	×	×	×	×	×	1
12	Password Safe	✓	×	✓	✓	✓	✓	5
13	Passwordbox	✓	✓	✓	✓	×	×	4
14	RoboForm	✓	✓	✓	✓	✓	✓	6
15	Safe in Cloud	✓	✓	✓	✓	✓	✓	6
	المجموع	15	8	11	10	8	8	60
	النسبة المئوية	25	14	18	17	13	13	%100
	الترتيب النسبي	1	4	2	3	4	4	-

(*) إجابة السؤال رقم (2) بقائمة المراجعة.

يتضح من الجدول رقم (3) ما يلي:

- تدعم البرمجيات عينة الدراسة 6 نظم تشغيل هي: Windows، Linux، Android، iOS، MAC OSX، WindowsPhone.
- جاءت 5 برمجيات (بنسبة مئوية قدرها 33% من إجمالي عينة الدراسة) في المركز الأول؛ حيث تدعم كل برمجية منهم 6 نظم تشغيل. وتتمثل هذه البرمجيات في: Dashlane، Enpass، LastPass، RoboForm، SafeinCloud.

وجاءت برمجيتان (بنسبة مئوية قدرها 13% من إجمالي عينة الدراسة) هما Efficient Password Manager، Password Safe في المركز الثاني ؛ حيث تدعم كل برمجية منهما 5 نظم تشغيل. وجاءت 3 برمجيات (بنسبة مئوية قدرها 20% من إجمالي عينة الدراسة) هي LogMeOnce، NortonIdentity Safe، Passwordbox في المركز الثالث ؛ حيث تدعم كل برمجية منهما 4 نظم تشغيل.

وجاءت برمجية Intuitive Password (بنسبة مئوية قدرها 7% من إجمالي عينة الدراسة) في المركز الرابع ؛ حيث تدعم 3 نظم تشغيل. تليها برمجية Keepass (بنسبة مئوية قدرها 7% من إجمالي عينة الدراسة) في المركز الخامس ؛ حيث تدعم نظامين تشغيل. أما المركز السادس الأخير فقد احتلته 3 برمجيات (بنسبة مئوية قدرها 20% من إجمالي عينة الدراسة)، وهي Access Manager، Pass Box، Password Memory ؛ حيث تدعم كل برمجية منها نظام تشغيل واحد.

- نظام التشغيل Windows هو أكثر نظم التشغيل دعمًا من البرمجيات عينة الدراسة ؛ حيث تدعمه جميعها. يليه في المركز الثاني نظام التشغيل Android وتدعمه 11 برمجية، ثم نظام التشغيل iOS في المركز الثالث وتدعمه 10 برمجيات، وجاءت نظم التشغيل Linux، MAC OSX، Windows Phone في المركز الرابع حيث تُدعم من قِبل 8 برمجيات من برمجيات عينة الدراسة.

نستنتج مما سبق أن برمجيات إدارة كلمات المرور عينة الدراسة، حرصت على أن تتوافق إصداراتها مع غالبية نظم التشغيل المستخدمة في الحواسيب والهواتف الذكية والأجهزة اللوحية، مما يعني عدم وجود مشكلة لدى المستخدم عند استخدامه لبرمجيات إدارة كلمات المرور على نظم التشغيل المختلفة، وما عليه إلا أن يتعرف على نظم التشغيل التي تتوافر على أجهزته، ليختار البرمجيات التي تدعمها.

6/3 متصفحات الإنترنت التي تدعمها برمجيات إدارة كلمات المرور عينة الدراسة:

يُعد دعم متصفحات الإنترنت من الأمور المهمة التي ينبغي أن تحرص عليها برمجيات إدارة كلمات المرور، حتى يسهل تسجيل كلمات المرور للمواقع التي يتم الدخول إليها بشكل آلي بغض النظر عن المتصفح الذي يستخدمه المستخدم. ويبين الجدول رقم (4) المتصفحات التي تدعهما البرمجيات عينة الدراسة.

الجدول رقم (4) متصفحات الإنترنت التي تدعمها برمجيات إدارة كلمات المرور عينة الدراسة (*)

م	المتصفحات / البرمجيات	Chrome	Internet Explorer	Firefox	Safari	Opera	Yandex	المجموع
1	Access Manager	×	×	×	×	×	×	0
2	Dashlane	✓	✓	✓	×	×	×	3
3	Efficient Password Manager	×	×	×	×	×	×	0
4	Enpass	✓	×	✓	✓	✓	✓	5
5	Intuitive Password	✓	×	✓	✓	✓	×	4
6	Keepass	×	×	×	×	×	×	0
7	LastPass	✓	✓	✓	✓	✓	×	5
8	LogMeOnce	✓	✓	✓	✓	✓	×	5
9	Norton Identity Safe	✓	✓	✓	✓	×	×	4
10	PassBox	×	×	×	×	×	×	0
11	Password Memory	×	×	×	×	×	×	0
12	Password Safe	×	×	×	×	×	×	0
13	Passwordbox	✓	✓	×	✓	✓	×	4
14	RoboForm	✓	×	✓	×	×	×	2
15	Safe in Cloud	✓	×	✓	✓	✓	✓	5
	المجموع	**9**	**5**	**8**	**7**	**6**	**2**	**37**
	النسبة المئوية	**24**	**14**	**22**	**19**	**16**	**5**	**%100**
	الترتيب النسبي	**1**	**5**	**2**	**3**	**4**	**6**	**-**

(*) إجابة السؤال رقم (3) بقائمة المراجعة.

يتضح من الجدول رقم (4) ما يلي:

- تدعم برمجيات إدارة كلمات المرور عينة الدراسة 6 متصفحات هي: Chrome، Internet Explorer، Firefox، Safari، Opera، Yandex.
- جاءت 4 برمجيات (تمثل نسبة مئوية قدرها 27% من إجمالي عينة الدراسة) في المركز الأول حيث تدعم كل برمجية منهم 5 متصفحات. وتتمثل هذه البرمجيات في: Enpass، LastPass، LogMeOnce، Safe in Cloud. وجاءت 3 برمجيات (تمثل نسبة قدرها 20% من إجمالي عينة الدراسة) في المركز الثاني حيث تدعم كل برمجية منهم 4 متصفحات. وتتمثل هذه البرمجيات في: Intuitive Password، Norton Identity Safe، Password box. وجاءت برمجية واحدة (Dashlane) في المركز الثالث (بنسبة مئوية قدرها 7% من إجمالي عينة الدراسة) حيث تدعم 3 متصفحات. تليها برمجية (Robo Form) في المركز

الرابع (بنسبة مئوية قدرها 7% من إجمالي عينة الدراسة) حيث تدعم متصفحين فقط. أما المركز الخامس الأخير فقد احتلته 6 برمجيات (Access Manager، Efficient Password Manager، Keepass، PassBox، Password Memory، Password Safe) بنسبة مئوية قدرها 60% من إجمالي عينة الدراسة، حيث لم تدعم أي متصفح، وترى الباحثة أن هذا أمر طبيعي جاء نتيجة أن هذه البرمجيات من برمجيات إدارة كلمات المرور في الحاسوب الشخصي والهواتف الذكية، ولا تعمل على متصفح الإنترنت كمنصة.

- أكثر متصفح تدعمه البرمجيات عينة الدراسة هو متصفح Chrome حيث تدعمه 9 برمجيات. يليه في المركز الثاني متصفح Firefox، حيث تدعمه 8 برمجيات. وفي المركز الثالث جاء متصفح Safari، حيث تدعمه 7 برمجيات. أما متصفح Opera فجاء في المركز الرابع، حيث تدعمه 6 برمجيات. يليه متصفح Internet Explorer في المركز الخامس، حيث تدعمه 5 برمجيات. أما المركز السادس الأخير فقد احتله متصفح Yandex، حيث تدعمه برمجيتان فقط من البرمجيات عينة الدراسة.

نستنتج مما سبق أن برمجيات إدارة كلمات المرور عينة الدراسة المتاحة عبر الإنترنت حرصت على دعم المتصفحات الأكثر استخدامًا من قِبل المستخدمين على الإنترنت.

3/ 7 نوع المصدر في برمجيات إدارة كلمات المرور عينة الدراسة:

هناك نوعان من المصادر التي تعمل بها برمجيات إدارة كلمات المرور، هما المصدر المغلق والمصدر المفتوح. ويبين الجدول رقم (5) نوع المصدر في برمجيات إدارة كلمات المرور عينة الدراسة.

الجدول رقم (5) نوع المصدر في برمجيات إدارة كلمات المرور عينة الدراسة (*)

م	الفئات / البرمجيات	مغلق المصدر	مفتوح المصدر	المجموع
1	Access Manager	✓	×	1
2	Dashlane	✓	×	1
3	Efficient Password Manager	✓	×	1
4	Enpass	✓	×	1
5	Intuitive Password	✓	×	1
6	Keepass	×	✓	1
7	LastPass	✓	×	1
8	LogMeOnce	✓	×	1
9	Norton Identity Safe	✓	×	1
10	PassBox	✓	×	1

تابع - الجدول رقم (5) نوع المصدر في برمجيات إدارة كلمات المرور عينة الدراسة (*)

م	الفئات / البرمجيات	مغلق المصدر	مفتوح المصدر	المجموع
11	Password Memory	✓	×	1
12	Password Safe	✓	×	1
13	Passwordbox	✓	×	1
14	RoboForm	✓	×	1
15	Safe in Cloud	✓	×	1
المجموع		14	1	15
النسبة المئوية		93	7	%100
الترتيب النسبي		1	2	-

(*) إجابة السؤال رقم (4) بقائمة المراجعة.

يتضح من الجدول رقم (5) أن الغالبية العظمى من البرمجيات عينة الدراسة (93% من إجمالي عينة الدراسة) تعمل بنظام المصدر المغلق، وأن برمجية واحدة Keepass (7% من إجمالي عينة الدراسة) تعمل بنظام المصدر المفتوح. ونستنتج من ذلك عدم اهتمام الجهات الراعية للمصادر المفتوحة بتصميم برمجيات إدارة كلمات المرور.

وترى الباحثة ضرورة الاهتمام بإتاحة برمجيات إدارة كلمات المرور مفتوحة المصدر، نظرًا لما توفره من مزايا للمستخدم في مقابل البرمجيات مغلقة المصدر العاملة في هذا المجال، ومن هذه المزايا على سبيل المثال:

- قدرة المستخدم على الوصول الكامل إلى شفرة المصدر.
- منع الثغرات الخلفية، ويمكن للمستخدم مراجعة شفرة المصدر وإدخال الإضافات التي يريد عليها.
- تحقق المستخدم من قوة أمن البرمجية، وقدرته -إذا أراد- على استخدام أي خوارزمية أخرى للتشفير.
- تشجيع المستخدمين على تصميم نسخ أخرى من البرمجية تتناسب مع الأنظمة المختلفة، أو إعداد ترجمات لها(Keepass، 2016).

8/3 دعم واجهات برمجيات إدارة كلمات المرور عينة الدراسة للغة العربية:

من معايير المفاضلة بين برمجيات إدارة كلمات المرور وجود واجهة Interface تدعم اللغة العربية. وقد بين الجدول رقم (6) عدد البرمجيات التي تدعم اللغة العربية.

الجدول رقم (6) دعم واجهات برمجيات إدارة كلمات المرور عينة الدراسة للغة العربية (*)

م	البرمجيات	تدعم اللغة العربية	لا تدعم اللغة العربية	المجموع
1	Access Manager	×	✓	1
2	Dashlane	×	✓	1
3	Efficient Password Manager	✓	×	1
4	Enpass	✓	×	1
5	Intuitive Password	×	✓	1
6	Keepass	×	✓	1
7	LastPass	✓	×	1
8	LogMeOnce	✓	×	1
9	Norton Identity Safe	✓	×	1
10	PassBox	×	✓	1
11	Password Memory	×	✓	1
12	Password Safe	×	✓	1
13	Passwordbox	×	✓	1
14	RoboForm	×	✓	1
15	Safe in Cloud	✓	×	1
	المجموع	**6**	**9**	**15**
	النسبة المئوية	**40**	**60**	**%100**
	الترتيب النسبي	**2**	**1**	**-**

(*) إجابة السؤال رقم (5) بقائمة المراجعة.

يتضح من الجدول رقم (6) ما يلي:

- بلغ عدد البرمجيات التي تدعم اللغة العربية 6 برمجيات فقط (بنسبة مئوية قدرها 40% من إجمالي عينة الدراسة)، وتتمثل هذه البرمجيات في : Efficient Password Manager، Enpass، LastPass، LogMeOnce، Norton Identity Saf ، Safe in Cloud.
- بلغ عدد البرمجيات التي لا تدعم اللغة العربية 9 برمجيات (بنسبة مئوية قدرها 60% من إجمالي عينة الدراسة)، وتتمثل هذه البرمجيات في:.Access Manager, Dashlane, Intuitive Password, Keepass, PassBox, Password Memory , Password Safe, Password box, Robo Form.

نستنتج مما سبق أن بعض المستخدمين العرب الذين لا يجيدون استخدام اللغة الإنجليزية، لن يتاح أمامهم سوى عدد قليل من برمجيات إدارة كلمات المرور للاختيار من بينها.

9/3 الخدمات التي توفرها برمجيات إدارة كلمات المرور عينة الدراسة:

إن الهدف الأساس من برمجيات إدارة كلمات المرور هو حفظ كلمات المرور، إلا أن هذه البرمجيات توسعت في تقديم خدمات مساندة مثل توليد كلمات المرور واستيرادها وتصديرها، وحفظ المعلومات المهمة وغير ذلك. ويوضح الجدول رقم (7) الخدمات التي توفرها برمجيات إدارة كلمات المرور عينة الدراسة.

الجدول رقم (7) الخدمات التي توفرها برمجيات إدارة كلمات المرور عينة الدراسة (*)

م	الخدمات / البرمجيات	حفظ كلمات المرور	توليد كلمات المرور	التسجيل اليدوي لكلمات المرور	التقاط كلمات المرور من المتصفح	تنظيم كلمات المرور	استيراد كلمات المرور	تصدير كلمات المرور	مشاركة كلمات المرور	النسخ الاحتياطي لكلمات المرور	حفظ معلومات	حسابات بعد الموت والطوارئ	المزامنة	المجموع
1	Access Manager	✓	✓	✓	×	✓	✓	×	✓	✓	✓	×	×	8
2	Dashlane	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	×	10
3	Efficient PasswordManager	✓	✓	✓	×	×	✓	✓	×	✓	×	×	×	6
4	Enpass	✓		✓	✓	✓	✓	✓	✓	✓	✓	×	✓	11
5	Intuitive Password	✓	✓	✓	✓	✓	✓	×	✓	×	✓	×	✓	9
6	Keepass	✓	✓	✓	×	✓	✓	✓	×	✓	×	×	×	7
7	LastPass	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	✓	✓	11
8	LogMeOnce	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	12
9	Norton Identity Safe	✓	×	✓	✓	×	✓	✓	×	✓	✓	×	✓	8
10	PassBox	✓	✓	✓	×	✓	✓	✓	×	✓	×	×	✓	8
11	Password Memory	✓	✓	✓	×	✓	×	×	×	✓	✓	×	×	6
12	Password Safe	✓	✓	✓	×	✓	✓	✓	×	✓	×	×	×	7
13	Passwordbox	✓	✓	✓	✓	×	×	✓	✓	×	✓	✓	×	8
14	RoboForm	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	×	✓	11
15	Safe in Cloud	✓	✓	×	✓	✓	✓	✓	×	✓	✓	×	✓	9
	المجموع	15	14	14	9	12	13	12	8	11	11	4	8	131
	النسبة المئوية	12	11	11	7	9	10	9	6	8	8	3	6	%100
	الترتيب النسبي	1	2	2	6	4	3	4	7	5	5	8	7	-

(*) إجابة السؤال رقم (6) بقائمة المراجعة.

يتبين من الجدول رقم (7) ما يلي:

- تنوع الخدمات التي تقدمها برمجيات إدارة كلمات المرور عينة الدراسة، حيث بلغ عددها 12 خدمة تتمثل في:

o **حفظ كلمات المرور**: هي الخدمة الأساس التي صُممت من أجلها برمجيات إدارة كلمات المرور.

o **توليد كلمات المرور**: خدمة تقوم البرمجية من خلالها باقتراح كلمات مرور قوية صعب الكسر، يمكن للمستخدمين استخدامها بدلاً من كلمات مرورهم الضعيفة التي يستخدمونها عند التسجيل في المواقع المختلفة.

o **التسجيل اليدوي لكلمات المرور**: يقوم المستخدم من خلال هذه الخدمة، بتسجيل اسم المستخدم وكلمة المرور للمواقع والخدمات التي يستخدمها من خلال إدخال تلك البيانات إلى برمجية إدارة كلمات المرور عبر لوحة المفاتيح.

o **التقاط كلمات المرور من المتصفح**: تقوم البرمجية من خلال هذه الخدمة بالتسجيل الآلي لاسم المستخدم وكلمة المرور التي يقوم المستخدم بإدخالها عند دخوله لمواقع الإنترنت.

o **تنظيم كلمات المرور**: خدمة يمكن للمستخدم من خلالها تنظيم كلمات المرور في مجلدات أو تحت مسميات معينة، حتى يسهل الاسترجاع منها.

o **استيراد كلمات المرور**: خدمة تتيح للمستخدم جلب كلمات المرور من برمجيات إدارة كلمات مرور أخرى، أو من ملفات عادة ما تكون في صيغة CSV و XML.

o **تصدير كلمات المرور**: خدمة تسمح للمستخدم بتصدير كلمات المرور المخزنة في قاعدة البيانات، وعادة ما يتم التصدير في ملفات في صيغ CSV، XML، HTML، TXT.

o **مشاركة كلمات المرور**: خدمة تسمح للمستخدم بمشاركة كلمات مروره مع آخرين.

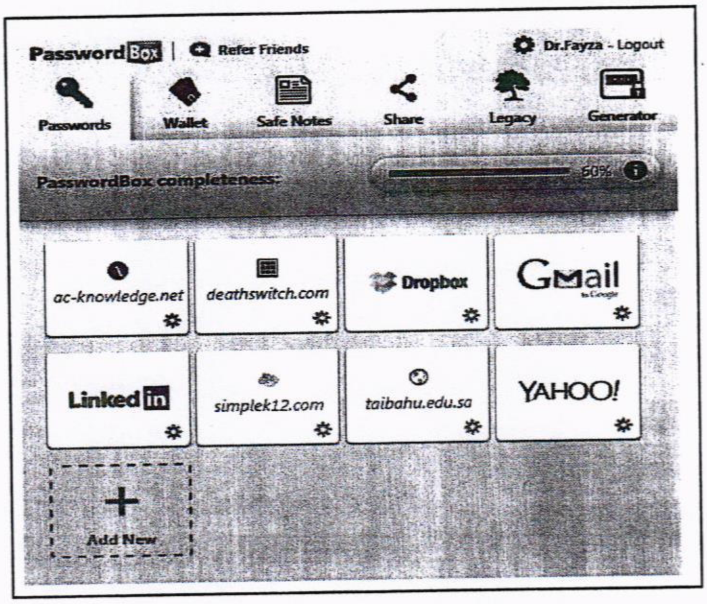
o **النسخ الاحتياطي لكلمات المرور**: خدمة تتيح للمستخدم إعداد نسخة احتياطية من قاعدة البيانات المخزن بها كلمات مروره، حتى يمكن استرداد تلك الكلمات في حالة حدوث تدمير لقاعدة البيانات الرئيسة. ويمكن أن يتم النسخ الاحتياطي لقاعدة البيانات على جهاز المستخدم، أو على سحب إلكترونية مثل Google Drive، One Drive، Dropbox، وغيرها.

o **حفظ المعلومات**: خدمة يمكن للمستخدم من خلالها تسجيل بيانات عن: العناوين، وبطاقات الائتمان، والهوية، والحسابات البنكية، وايصالات التجارة الإلكترونية، ورخصة القيادة، والضمان الاجتماعي، وعضوية اللجان والمنظمات، وجواز السفر، والتأمين، والصور والملفات، والملاحظات، وغيرها من المعلومات المهمة والحساسة التي يخشى المستفيد عليها من الفقد، ويرغب في حفظها بأمان.

o **حسابات بعد الموت والطوارئ:** خدمة تسمح للمستخدم بإتاحة كلمات المرور المخزنة في قاعدة البيانات لأشخاص يثق فيهم ويحددهم، في حالة حدوث طوارئ له أو وفاته. وعادة يحدد المستخدم مدة معينة إذا لم يدخل إلى البرمجية خلالها، فإن البرمجية تبدأ في إرسال رسائل تذكيرية له، وفي حالة استمرار عدم دخول المستخدم إلى البرمجية، فإن البرمجية تتيح كلمات المرور للأشخاص الذين حددهم المستخدم قبل وفاته أو حدوث الحالة الطارئة له.

o **المزامنة:** خدمة المزامنة بين الأجهزة، تعني إمكانية تحديث كلمات المرور في قاعدة البيانات بغض النظر عن الجهاز الذي تم منه الدخول إلى القاعدة. حيث يقوم المستخدم بعد إدخال كلمات المرور بعمل «مزامنة» وبالتالي تحدث قاعدة البيانات.

ويوضح الشكل رقم (7) الخدمات التي تقدمها برمجية Passwordbox، كنموذج للخدمات التي تقدمها البرمجيات عينة الدراسة.



الشكل رقم (7) الخدمات التي تقدمها برمجية Passwordbox

- برمجية LogMeOnce هي أكثر برمجيات عينة الدراسة إتاحة للخدمات حيث جاءت في المركز الأول وتتيح 12 خدمة. تليها 3 برمجيات هي RoboForm، LastPass، Enpass في المركز الثاني وتقدم كل منها 11 خدمة. وجاءت برمجية Dashlane في المركز الثالث، حيث تقدم 10 خدمات. وجاءت برمجية Intuitive Password، وبرمجية Safe in Cloud في المركز الرابع وأتاحت كل برمجية منها 9 خدمات. وفي المركز الخامس جاءت 4 برمجيات هي Passwordbox، Pass Box، Norton Identity Safe، Access Manager حيث تقدم كل منها 8 خدمات. وجاءت برمجية Keepass، وبرمجية Password Safe في المركز السادس

وتوفر كل برمجية منهما 7 خدمات. وفي المركز السابع الأخير جاءت برمجية Efficient Password Manager، وبرمجية Password Memory، حيث أتاحت كل برمجية منهما 6 خدمات.

- خدمة "حفظ كلمات المرور" هي الخدمة الأكثر إتاحة، حيت تقدمها جميع البرمجيات عينة الدراسة، تليها في المركز الثاني خدمة "توليد كلمات المرور" وخدمة "التسجيل اليدوي لكلمات المرور" حيث توافرت كل خدمة منهما في 14 برمجية، وجاءت خدمة "استيراد كلمات المرور" في المركز الثالث وتقدمها 13 برمجية. وجاءت خدمة "تنظيم كلمات المرور"، وخدمة "تصدير كلمات المرور" في المركز الرابع، وتوافرت كل خدمة منهما في 12 برمجية.

وجاءت في المركز الخامس خدمة "النسخ الاحتياطي لكلمات المرور"، وخدمة "حفظ معلومات"، حيث تتوافر كل خدمة منهما في 11 برمجية.

وفي المركز السادس جاءت خدمة "التقاط كلمات المرور من المتصفح"، وتوافرت في 9 برمجيات. وجاءت خدمة "مشاركة كلمات المرور" وخدمة "المزامنة" في المركز السابع، حيث تتوافر كل منها في 8 برمجيات. أما المركز الثامن الأخير فقد جاءت فيه خدمة "حسابات بعد الموت والطوارئ"، حيث لم تتوافر إلا في 4 برمجيات فقط من البرمجيات عينة الدراسة.

نستنتج مما سبق تنوع الخدمات التي توفرها البرمجيات عينة الدراسة، مما يعكس اهتمام برمجيات إدارة كلمات المرور ليس فقط بإتاحة الخدمة الأساسية منها وهي خدمة «حفظ كلمات المرور»، ولكن أيضًا إتاحة خدمات مساندة توفر للمستخدم المزيد من الصلاحيات للتحكم في كلمات مروره. تبين أيضًا أن البرمجيات المتاحة عبر متصفحات الإنترنت أكثر تقديمًا للخدمات من تلك المتاحة عبر الحواسيب والهواتف الذكية والأجهزة اللوحية فقط.

والجدير بالذكر أن الباحثة لاحظت أثناء الدراسة الميدانية أن بعض الخدمات لا توفرها البرمجيات المجانية، لأن لديها نسخة مدفوعة تتيح عبرها المزيد من الخدمات، فعلى سبيل المثال:

- لا تتاح خدمة «تصدير كلمات المرور»، وخدمة «المزامنة» في النسخة المجانية من برمجية Access Manager، إلا أنها متوافرة في النسخة المدفوعة.
- لا تتاح خدمة "النسخ الاحتياطي لكلمات المرور"، وخدمة "المزامنة" في النسخة المجانية من برمجية Dashlane، إلا أنها متوافرة في النسخة المدفوعة.
- لا تتاح خدمات "استيراد كلمات المرور"، و"مشاركة كلمات المرور"، و"حفظ معلومات"، و"المزامنة" في النسخة المجانية من برمجية Efficient Password Manager، إلا أنها متوافرة في النسخة المدفوعة.

10/3 إجراءات الحماية التي توفرها برمجيات إدارة كلمات المرور عينة الدراسة:

نظرًا لاحتواء قواعد بيانات برمجيات لإدارة كلمات المرور على كلمات مرور ومعلومات وملاحظات تستدعي الحماية ضد المخاطر الأمنية المختلفة، لذا تسعى البرمجيات لاتخاذ عدة إجراءات لتفادي تلك المخاطر، وقد أوضح الجدول رقم (8) الإجراءات التي اتخذتها البرمجيات عينة الدراسة لحماية كلمات مرور المستخدمين ومعلوماتهم وملاحظاتهم.

الجدول رقم (8) إجراءات الحماية التي توفرها برمجيات إدارة كلمات المرور عينة الدراسة (*)

م	إجراءات الحماية / البرمجيات	التوثق بكلمة مرور رئيسة قوية	التوثق بخاصية حيوية	تقييم قوة كلمة المرور	عدم استعادة كلمة المرور الرئيسة	عدم نقل كلمة المرور الرئيسة عبر الإنترنت	عدم الاحتفاظ بكلمة المرور الرئيسة على جهاز المستخدم	عدم الاحتفاظ بكلمة المرور الرئيسة على خادم البرمجية	الخروج بشكل آلي عند إغلاق الجهاز أو التصفح	نظام تشفير آمن	المجموع
1	Access Manager	×	×	×	✓	**	✓	**	✓	✓	4
2	Dashlane	✓	×	✓	✓	✓	✓	✓	✓	✓	8
3	Efficient Password Manager	×	×	×	✓	**	✓	**	✓	✓	4
4	Enpass	✓	✓	✓	✓	✓	✓	✓	✓	✓	9
5	Intuitive Password	×	×	✓	✓	✓	✓	✓	✓	✓	7
6	Keepass	✓	×	✓	✓	**	✓	**	✓	✓	6
7	LastPass	✓	×	✓	✓	✓	×	✓	✓	✓	7
8	LogMeOnce	✓	✓	✓	✓	✓	✓	✓	✓	✓	9
9	Norton Identity Safe	✓	×	×	×	✓	✓	✓	✓	✓	6
10	PassBox	×	×	×	×	×	✓	✓	✓	✓	4
11	Password Memory	×	×	×	✓	**	×	**	✓	✓	3
12	Password Safe	×	×	×	✓	**	×	**	×	✓	2
13	Passwordbox	✓	×	✓	✓	**	✓	**	×	✓	5
14	RoboForm	✓	×	✓	✓	✓	✓	✓	✓	✓	8
15	Safe in Cloud	✓	×	✓	✓	✓	✓	✓	✓	✓	8
	المجموع	9	2	9	13	8	12	9	13	15	90
	النسبة المئوية	10	2	10	15	9	13	10	15	16	%100
	الترتيب النسبي	4	6	4	2	5	3	4	2	1	-

(*) إجابة السؤال رقم (7) بقائمة المراجعة.

(**) لا ينطبق لأن البرمجية لا تتاح عبر الإنترنت.

يتبين من الجدول رقم (8) ما يلي:

- بلغ عدد الإجراءات الأمنية التي تتبعها البرمجيات عينة الدراسة 9 إجراءات، تتمثل في:
  - **التوثق بكلمة مرور رئيسة قوية**: يُقصد بها الاعتماد على كلمة مرور رئيسة للتوثق من المستخدم الحقيقي والتأكد من هويته، وهذا من الإجراءات الأمنية المهمة، لأن كلمات المرور الرئيسة الضعيفة، تجعل من السهل اختراق قاعدة البيانات المخزن عليها كلمات المرور.
  - **التوثق بخاصية حيوية**: يتم التوثق من المستخدم الحقيقي وتحديد هويته باستخدام خاصية حيوية، مثل الوجه أو بصمة الإصبع، وهذه الطريقة نسبة الأمن فيها عالية حيث من الصعب تخمين الخاصية الحيوية أو سرقتها، كما هو الحال عند التوثق من المستخدم باستخدام كلمات المرور.
  - **تقييم قوة كلمة المرور**: حتى يتم التأكد من أن كلمات المرور التي يستخدمها المستخدم للتسجيل في المواقع، هي كلمات قوية يصعب كسرها.
  - **عدم استعادة كلمة المرور الرئيسة**: تلجأ برمجيات إدارة كلمات المرور لهذه الطريقة حتى تضمن عدم استعادة كلمة المرور الرئيسة من شخص غير المستخدم الحقيقي، لذا على المستخدم عدم نسيان كلمة المرور الرئيسة لفتح البرمجية والوصول لقاعدة البيانات المخزنة بها كلمات مروره ومعلوماته.
  - **عدم نقل كلمة المرور الرئيسة عبر الإنترنت**، وعدم الاحتفاظ بكلمة المرور الرئيسة على جهاز المستخدم، وعدم الاحتفاظ بكلمة المرور الرئيسة على خادم البرمجية: هي وسائل يتم اتخاذها حتى لا يتم قرصنة الكلمة الرئيسة أثناء انتقالها أو تخزينها على الويب.
  - **الخروج بشكل آلي عند إغلاق المتصفح أو الحاسوب أو الهواتف الذكية والأجهزة اللوحية**: حتى لا تتاح الفرصة أمام شخص غير المستخدم الحقيقي للوصول إلى البرمجية في حالة فتحه لجهاز المستخدم أو المتصفح.
  - **استخدام نظام تشفير آمن**: وقد أوضحت الدراسة أن جميع برمجيات عينة الدراسة تعتمد على نظام AES: The Advanced Encryption Standard لتشفير كلمة المرور الرئيسة وكلمات المرور والمعلومات المخزنة في قاعدة البينات، وهذا النظام عبارة عن معيار تشفير مطور تبناه المركز القومي للمعايير والتكنولوجيا التابع لحكومة الولايات المتحدة الأمريكية. وهذا المعيار من أكثر طرق التشفير قبولاً على مستوى العالم، وهو يسمح بثلاثة

أطوال مختلفة لمفتاح التشفير هي 128، 192، 256 بت (Kak، 2016)، وطول المفتاح الأخير هو الذي اعتمدت عليه برمجيات إدارة كلمات المرور عينة الدراسة.

- جاءت برمجية Enpass، وبرمجية LogMeOnce في المركز الأول ؛ حيث تتوافر بها جميع إجراءات الحماية التسع. وفي المركز الثاني جاءت برمجيات Dashlane، RoboForm، Safe in Cloud ويتوافر بكل منها 8 إجراءات، وجاءت برمجية Intuitive Password، وبرمجية LastPass في المركز الثالث ويتوافر بكل منهما 7 إجراءات،وجاءت برمجية Keepass ، وبرمجية Norton Identity Safe في المركز الرابع ويتوافر بكل منهما 6 إجراءات، وجاءت Password box في المركز الخامس ويتوافر بها 5 إجراءات، وفي المركز السادس جاءت برمجيات Access Manager، Efficient Password Manager، PassBox وتوافر بكل منها 4 إجراءات، واحتلت برمجية Password Memory المركز السابع وتوافر بها 3 إجراءات، وجاءت في المركز الثامن الأخير برمجية Password Safe حيث توافر بها إجراءين فقط.
- "نظام التشفير الآمن" هو أكثر وسائل الحماية توافرًا في البرمجيات عينة الدراسة ؛ حيث توافر في جميع البرمجيات. يليه في المركز الثاني "عدم استعادة كلمة المرور الرئيسة" و"الخروج بشكل آلي عند إغلاق الجهاز أو المتصفح" ، حيث توافر كل إجراء منهما في 13 برمجية، وفي المركز الثالث جاء "عدم الاحتفاظ بكلمة المرور الرئيسة على جهاز المستخدم" وتوافر هذا الإجراء في 12 برمجية، وجاء في المركز الرابع "التوثق بكلمة مرور رئيسة قوية"، و "تقييم قوة كلمة المرور"، و "عدم الاحتفاظ بكلمة المرور الرئيسة على خادم البرمجية"، حيث توافر كل إجراء منها في 9 برمجيات، وجاء "عدم نقل كلمة المرور الرئيسة عبر الإنترنت" في المركز الخامس ؛ حيث توافر في 8 برمجيات، وكان إجراء الحماية المتمثل في "التوثق بخاصية حيوية" هو أقل الإجراءات توافرًا في البرمجيات عينة الدراسة، وجاء في المركز السادس الأخير ؛ حيث لم يتوافر هذا الإجراء إلا في برمجيتين فقط.

نستنتج مما سبق:

- نجاح جميع برمجيات إدارة كلمات المرور عينة الدراسة في توفير التشفير الآمن لكلمات المرور، إلا أن البعض فشل في تحقيق مبدأ أساس من وسائل الحماية، وهو استخدام كلمة مرور رئيسة قوية، فعند قيام الباحثة بتجريب كلمات المرور الرئيسة في البرمجيات عينة الدراسة، لا حظت أن 6 برمجيات منها -كما هو موضح في الجدول رقم (8)- قبلت كلمة مرور ضعيفة جدًا تم استخدام الأرقام التالية بها (12345)، ويعني هذا أن البرمجيات الست فشلت في أن تكون آمنة، حيث من المتفق عليه أن برمجيات إدارة كلمات المرور تكون

آمنة فقط، عندما تكـون كلمة المرور الرئيسـة بها قويـة، وتستخدم نظام تشفير قوي (Community Pepperdine, 2016).

- حرص جميع البرمجيات عينة الدراسة على عدم استعادة كلمة المرور الرئيسة عند نسيانها، باستثناء برمجية Norton Identity Safe التي تتيح استعادتها من خلال الإجابة عن سؤال أمن يسجله المستخدم عند إدخاله كلمة المرور الرئيسة للمرة الأولى في البرمجية، وبرمجية PassBox التي تسمح باستردادها عبر ارسال بريد إلكتروني للمستخدم به كلمة مرور جديدة بديلة عن تلك التي نسيها. وترى الباحثة أن هذا قد يحقق فائدة للمستخدم، حيث لن يضطر إلى فقد جميع كلمات مروره إذا نسي كلمة المرور الرئيسة.
- حرص جميع البرمجيات عينة الدراسة على الخروج بشكل آلي عند إغلاق المستخدم للجهاز أو المتصفح، باستثناء برمجية Password Safe، وبرمجية Password box ، حيث لا تغلق البرمجية نفسها عند إغلاق الجهاز أو المتصفح، وأعطت المستخدم خيار الإبقاء على البرمجية في الوضع المفتوح، أو الضغط على أيقونة الخروج. وترى الباحثة أن هذا الأسلوب قد يسهل استخدام البرمجية، حيث لا يتطلب الأمر تسجيل كلمة المرور الرئيسة كلما كانت هناك رغبة في الوصول على قاعدة البيانات بها، إلا أن هذا أمر خطير فإذا فتح أحد الأشخاص جهاز المستخدم أو متصفحه لتمكن من الدخول إلى قاعدة البيانات وهو ما يعني وصوله إلى كل كلمات مرور المستخدم والمعلومات المخزنة بها.
- حرص جميع البرمجيات عينة الدراسة على عدم الاحتفاظ بكلمة المرور الرئيسة على جهاز المستخدم، باستثناء برمجيات Password Safe ، Password Memory، LastPass، حيث تحتفظ بكلمة المرور الرئيسة وبمجرد ضغط المستخدم على أيقونة البرمجية لفتحها، يتم فتحها مباشرة. وكانت برمجية LastPass هي البرمجية الوحيدة من البرمجيات الثلاث التي أوضحت بشكل واضح للمستفيد بأن هذا أمر خطر، وذلك من خلال رسالة منبثقة ظهرت عندما اختارت الباحثة خيار "تذكرني" عند إدخال كلمة المرور الرئيسة.

11/3 طرق الدعم الفني التي توفرها برمجيات إدارة كلمات المرور عينة الدراسة:

يقصد بالدعم الفني مساعدة مستخدمي برمجيات كلمات إدارة المرور لفهم عمل هذه البرمجيات، وحل أية مشكلات تعترضهم أثناء استخدامها. ويبين الجدول رقم (9) طرق الدعم الفني التي توفرها برمجيات إدارة كلمات المرور عينة الدراسة.

الجدول رقم (9) طرق الدعم الفني التي توفرها برمجيات إدارة كلمات المرور عينة الدراسة (*)

م	طرق الدعم / البرمجيات	أسئلة وإجابة جاهزة	دليل مستخدم	فيديو	نموذج	محادثة مباشرة	بريد إلكتروني	منتدى/ مدونة	المجموع
1	Access Manager	✓	✓	×	✓	×	×	✓	4
2	Dashlane	✓	✓	×	✓	×	×	×	3
3	Efficient Password Manager	✓	✓	×	✓	×	✓	×	4
4	Enpass	✓	✓	×	✓	×	✓	✓	5
5	Intuitive Password	✓	✓	✓	✓	✓	✓	×	6
6	Keepass	✓	✓	×	×	×	×	✓	3
7	LastPass	✓	✓	×	✓	×	×	✓	4
8	LogMeOnce	✓	×	✓	✓	×	×	✓	4
9	Norton Identity Safe	✓	×	×	✓	×	×	×	2
10	PassBox	×	✓	×	×	×	×	×	1
11	Password Memory	×	✓	×	×	×	×	×	1
12	Password Safe	×	✓	×	✓	×	×	✓	3
13	Passwordbox	×	✓	×	✓	×	×	×	2
14	RoboForm	✓	✓	×	×	✓	×	✓	4
15	Safe in Cloud	✓	×	×	×	×	✓	×	2
	المجموع	**11**	**12**	**2**	**10**	**2**	**4**	**7**	**48**
	النسبة المئوية	**23**	**25**	**4**	**21**	**4**	**8**	**15**	**%100**
	الترتيب النسبي	**2**	**1**	**6**	**3**	**6**	**5**	**4**	**-**

(*) إجابة السؤال رقم (8) بقائمة المراجعة.

يتبين من الجدول رقم (9) ما يلي:

- تتوافر 7 طرق للدعم الفني في البرمجيات عينة الدراسة، تتمثل في: أسئلة وإجابة جاهزة، ودليل مستخدم، وفيديو، ونموذج، ومحادثة مباشرة، وبريد إلكتروني، ومنتدى/ مدونة.
- جاءت برمجية Intuitive Password في المركز الأول حيث وفرت 6 طرق للدعم الفني، وجاءت برمجية Enpass في المركز الثاني حيث وفرت 5 طرق. وجاءت 6 برمجيات في المركز الثالث، حيث أتاحت 4 طرق للدعم الفني، وتشتمل هذه البرمجيات على Access Manager، Efficient Password Manager، LastPas، LastPass، LogMeOnce، Robo Form. وجاءت 3 برمجيات في المركز الرابع حيث أتاحت 3 طرق للدعم الفني، وتشتمل هذه البرمجيات على Dashlane، Keepass، PasswordSafe. وجاءت 3 برمجيات في المركز الخامس حيث أتاحت طريقتين للدعم الفني، وتشتمل هذه البرمجيات علىNorton Identity Safe، Password box، Safe in Cloud. أما المركز السادس الأخير فقد احتلته

برمجيتين هما PassBox، Password Memory ؛ حيث وفرت كل برمجية منهما طريقة واحدة للدعم الفني.

- أكثر طرق الدعم الفني توافرًا في البرمجيات عينة الدراسة هو دليل المستخدم الذي توافر في 12 برمجية من البرمجيات عينة الدراسة، تليه في المركز الثاني الأسئلة والأجوبة الجاهزة ؛ وتوافرت في 11 برمجية. ثم جاء النموذج المخصص لتلقي الأسئلة في المركز الثالث، وتوافر في 10 برمجيات. وجاءت المدونات / المنتديات في المركز الرابع، حيث توافرت في 7 برمجيات. يليها إرسال بريد إلكتروني إلى مسؤولي الدعم الفني في المركز الخامس، وتتوافر هذه الطريقة في 4 برمجيات. أما المركز السادس الأخير فقد جاء فيه الفيديو كوسيلة للشرح، والمحادثة المباشرة التي يمكن من خلالها التواصل بشكل مباشر مع مسؤولي الدعم الفني، وتوافرت كل طريقة منهما في برمجيتين فقط.

نستنتج مما سبق أن هناك تفاوتًا بين البرمجيات عينة الدراسة في العمل على توافر الدعم الفني لمستخدمي البرمجيات. بالإضافة إلى تنوع طرق الدعم الفني مما يتيح للمستخدم معرفة كيفية استخدام هذا النوع من البرمجيات، والحصول على حلول للمشكلات التي تواجهه أثناء استخدامه لها.

12/3 أفضل برمجيات عينة الدراسة:

ولتحديد أفضل برمجيات عينة الدراسة التي يمكن استخدامها لإدارة كلمات المرور، قامت الباحثة من خلال استخدام الجداول أرقام(2)، (3)، (4)، (6)، (7)، (8)، (9) بترتيب البرمجيات، وفقًا للخصائص التي توفرها للمستخدمين، ويبين الجدول رقم (10) ترتيب البرمجيات عينة الدراسة.

الجدول رقم (10) أفضل برمجيات عينة الدراسة

م	العناصر / البرمجيات	المنصات	نظم التشغيل	المتصفحات	دعم اللغة العربية	الخدمات	إجراءات الحماية	طرق الدعم الفني	المجموع	الترتيب
1	Access Manager	1	1	0	0	8	4	4	18	12
2	Dashlane	3	6	3	0	10	8	3	33	5
3	Efficient Password Manager	2	5	0	1	6	4	4	22	10
4	Enpass	3	6	5	1	11	9	5	40	1
5	Intuitive Password	3	3	4	0	9	7	6	32	6
6	Keepass	1	2	0	0	7	6	3	19	11
7	LastPass	3	6	5	1	11	7	4	37	3

تابع - الجدول رقم (10) أفضل برمجيات عينة الدراسة

م	العناصر / البرمجيات	المنصات	نظم التشغيل	المتصفحات	دعم اللغة العربية	الخدمات	إجراءات الحماية	طرق الدعم الفني	المجموع	الترتيب
8	LogMeOnce	3	4	5	1	12	9	4	38	2
9	Norton Identity Safe	3	4	4	1	8	6	2	28	7
10	PassBox	2	1	0	0	8	4	1	16	13
11	Password Memory	1	1	0	0	6	3	1	12	14
12	Password Safe	2	5	0	0	7	2	3	19	11
13	Passwordbox	2	4	4	0	8	5	2	25	9
14	RoboForm	3	6	2	0	11	8	4	34	4
15	Safe in Cloud	3	6	5	1	9	8	2	34	4

يتضح من الجدول رقم (10) أن أفضل ثلاث برمجيات وفقًا للخصائص التي توفرها للمستخدمين هي على التوالي: LastPass، LogMeOnce، Enpass.

4. نتائج الدراسة:

من أهم النتائج التي توصلت لها الدراسة :

- تتعرض كلمات المرور للكثير من أنواع الهجمات، فهناك خطورة من كشف كلمات المرور بعدة وسائل: مثل كسر cracking كلمات المرور الضعيفة، أو استخدام الهندسة الاجتماعية، أو البحث والتنصت.
- من أهم الفوائد التي توفرها برمجيات إدارة كلمات المرور:
  - عدم الحاجة إلى حفظ العديد من كلمات المرور.
  - توليد كلمات مرور قوية ومعقدة وصعبة، وبالتالي يصعب كسرها.
  - حفظ كلمات المرور بأمان في قاعدة بيانات مُشفرة على الحاسوب أو في سحابة إلكترونية.
  - الوصول إلى كلمات المرور المحفوظة من أي مكان وفي أي وقت.
  - تخزين كلمات المرور مُنظمة بحيث يسهل البحث فيها والاسترجاع منها.
  - جعل التجارة الإلكترونية أكثر أمنًا وسهولة.
- تتعرض برمجيات إدارة كلمات المرور للعديد من المخاطر، منها:
  - استهدافها من خلال تصميم برمجيات تستطيع تسجيل ضربات لوحة المفاتيح لالتقاط كلمات المرور الرئيسة المستخدمة للدخول إليها.

- تعرضها لمحاولات الاصطياد الإلكتروني.
- تعرض قواعد البيانات المخزن بها كلمات المرور في خوادم موردي خدمات برمجيات إدارة كلمات المرور لهجمات القرصنة.
- الكشف عن كلمة المرور الرئيسة، يؤدي إلى الكشف عن جميع كلمات مرور المستخدم.

- تعمل البرمجيات عينة الدراسة على 3 منصات هي: الحواسيب، والهواتف الذكية والأجهزة اللوحية، والإنترنت. وأكثر منصة تعمل عليها البرمجيات عينة الدراسة هي الحواسيب حيث تعمل عليها جميع البرمجيات، تليها في المركز الثاني الهواتف الذكية والأجهزة اللوحية، وتوافرت في 11 برمجية من عينة الدراسة، أما الإنترنت فقد جاء في المركز الثالث الأخير، وتعمل عليه 9 برمجيات فقط من عينة الدراسة.
- تدعم البرمجيات عينة الدراسة 6 نظم تشغيل هي: Windows، Linux، Android، iOS، MACOSX، Windows Phone.ونظام التشغيل Windows هو أكثر نظم التشغيل دعمًا من البرمجيات عينة الدراسة ؛ حيث تدعمه جميعها. يليه في المركز الثاني نظام التشغيل Android وتدعمه 11 برمجية، ثم نظام التشغيل iOS في المركز الثالث وتدعمه 10 برمجيات، وجاءت نظم التشغيل Linux، MAC OS X، Windows Phone في المركز الرابع حيث تُدعم من قِبل 8 برمجيات من برمجيات عينة الدراسة.
- تدعم برمجيات إدارة كلمات المرور عينة الدراسة 6 متصفحات هي: Chrome، Internet Explorer، Firefox، Safari، Opera، Yandex. وأكثر متصفح تدعمه البرمجيات عينة الدراسة هو متصفح Chrome حيث تدعمه 9 برمجيات. يليه في المركز الثاني متصفح Firefox، حيث تدعمه 8 برمجيات. وفي المركز الثالث جاء متصفح Safari، حيث تدعمه 7 برمجيات. أما متصفح Opera فجاء في المركز الرابع، حيث تدعمه 6 برمجيات. يليه متصفح Internet Explorer في المركز الخامس، حيث تدعمه 5 برمجيات. أما المركز السادس الأخير فقد احتله متصفح Yandex، حيث تدعمه برمجيتان فقط من البرمجيات عينة الدراسة.
- تعمل الغالبية العظمى من البرمجيات عينة الدراسة (93% من إجمالي عينة الدراسة) بنظام المصدر المغلق، وتعمل برمجية واحدة Keepass (7% من إجمالي عينة الدراسة) بنظام المصدر المفتوح.
- بلغ عدد البرمجيات التي تدعم اللغة العربية 6 برمجيات فقط (بنسبة مئوية قدرها 40% من إجمالي عينة الدراسة)، وتتمثل هذه البرمجيات في: Efficient Password Manager، Enpass، LastPass، LogMeOnce،Norton Identity Saf ، Safe in Cloud.
- تنوع الخدمات التي تقدمها برمجيات إدارة كلمات المرور عينة الدراسة، حيث بلغ عددها 12

خدمة تتمثل في: حفظ كلمات المرور، وتوليد كلمات المرور، والتسجيل اليدوي لكلمات المرور، والتقاط كلمات المرور من المتصفح، وتنظيم كلمات المرور، واستيراد كلمات المرور، وتصدير كلمات المرور، ومشاركة كلمات المرور، والنسخ الاحتياطي لكلمات المرور، وحفظ المعلومات، وحسابات بعد الموت والطوارئ، والمزامنة.

- بلغ عدد الإجراءات الأمنية التي تتبعها البرمجيات عينة الدراسة 9 إجراءات، تتمثل في: التوثق بكلمة مرور رئيسة قوية، والتوثق بخاصية حيوية، وتقييم قوة كلمة المرور، وعدم استعادة كلمة المرور الرئيسة، وعدم نقل كلمة المرور الرئيسة عبر الإنترنت، وعدم الاحتفاظ بكلمة المرور الرئيسة على جهاز المستخدم، وعدم الاحتفاظ بكلمة المرور الرئيسة على خادم البرمجية، والخروج بشكل آلي عند إغلاق المتصفح أو الحاسوب أو الهواتف الذكية والأجهزة اللوحية، واستخدام نظام تشفير آمن.
- تتوافر 7 طرق للدعم الفني في البرمجيات عينة الدراسة، تتمثل في: أسئلة وإجابة جاهزة، ودليل مستخدم، وفيديو، ونموذج، ومحادثة مباشرة، وبريد إلكتروني، ومنتدى/ مدونة.
- أفضل ثلاث برمجيات في عينة الدراسة وفقًا للخصائص التي توفرها للمستخدمين هي على التوالي: LastPass، LogMeOnce، Enpass.

5. توصيات الدراسة:

من أهم التوصيات التي يمكن أن تقدمها الدراسة :

- اختيار برمجيات «إدارة كلمات المرور» التي تتوافر فيها الخصائص التالية:
  - من مصادر معروفة وموثوق بها، وعلى المستخدم أن يحذر من استخدام البرمجيات الصادرة حديثًا والتي لا يتوافر آراء كافية من المستخدمين حولها. فقد يقوم مجرمي الإنترنت بتصميم برمجيات يكون هدفها سرقة المعلومات الخاصة بالمستخدم.
  - يتم تحديثها باستمرار، وعلى المستخدم الحرص على الحصول على التحديثات الأخيرة فورًا.
  - سهلة الاستخدام، لتجنب الوقوع في الأخطاء.
  - تستخدم نظام تشفير معروف ومعتمد، وينبغي الحذر من استخدام البرمجيات التي تستخدم أنظمة تشفير غير معروفة.
  - تعمل على مختلف الأجهزة التي يستخدمها المستخدم، ويُفضل توافر نسخة منها للأجهزة المحمولة الذكية.
  - تتيح ميزة المزامنة بين الأجهزة المختلفة، وأن تتم المزامنة بشكل آمن (تشفير البيانات قبل إرسالها من جهاز لآخر).

- o لديها القدرة على توليد كلمات مرور عشوائية قوية.
- o تتيح خاصية تقييم مدى قوة كلمات المرور التي اختارها المستخدم (The SANS Institute, 2013).
- o تسمح بأن يكون مكان الاحتفاظ بكلمات المرور في جهاز المستخدم، لتجنب قرصنة قواعد البيانات الموجودة على خوادم مقدمي خدمات برمجيات إدارة كلمات المرور (Cluley, 2015).

- اختيار كلمة مرور رئيسة Master Password قوية لتسجيلها لفتح البرمجية، ومن الاقتراحات التي يمكن تقديمها في هذا الشأن:
  - o أن يكون ترتيب الحروف عشوائي.
  - o ألا تقل عن 8 عناصر.
  - o مزيج من الحروف الكبيرة والصغيرة والأرقام والرموز.
  - o يمكن تذكرها: يمكن أخذها من أغنية أو قصيدة أو اقتباس أو قول مأثور. على سبيل المثال، استخدام الاقتباس "Knowledge is power. Information is liberating." لتكوين كلمة المرور الخاصة بالمستخدم، وفقًا للقاعدة التالية:
    - ■ أخذ الحرف الأول من كل جملة: KIPIIL
    - ■ تحويل بعض الحروف إلى الحروف الصغيرة KiPiiL
    - ■ إضافة بعض الأرقام والرموز 9KiP#iiL%
    - ■ لزيادة قوة كلمة المرور يتم استبدال حرف واحد من حروف الـ I برقم 1 وبهذا تصبح الكلمة 9KiP#1iL% تتسم بالقوة وإمكانية تذكرها (Kovacs, 2015).
- عدم تخزين كلمات مرور المواقع الحساسة في برمجية إدارة كلمات المرور (Noah 2015).

كما توصي الباحثة باستخدام وسائل داعمة لتحقيق المزيد من الحماية لكلمات المرور، ومنها:

- الحرص على أمن كلمات المرور بشكل عام، وفقًا لما يلي:

- عدم كتابة كلمة المرور على الإطلاق.
- عدم استخدام كلمة مرور واحدة لكل النظم أو الخدمات أو البرمجيات، بل يجب إنشاء كلمات مرور مختلفة لكل منها.
- الاستفادة من كل الخدمات التي توفرها برمجيات إدارة كلمات المرور، وخاصة توليد كلمات المرور العشوائية صعبة الكسر.

- تغيير كلمة المرور بانتظام، وبصفة خاصة عند كسر كلمة المرور أو محاولة كسرها (Cliff, 2001).
- عدم إعطاء كلمة المرور عبر الهاتف مطلقًا.
- عدم إعطاء كلمة المرور لمديري النظم أو فنيي الصيانة لأن لديهم كلمات مرور تتيح لهم العمل في حساب المستخدم دون الحاجة إلى معرفة كلمة المرور التي يستخدمها (Guenther, 2001).
- مكافحة الهندسة الاجتماعية: ومن الأساليب التي يمكن استخدامها لذلك:
  - o التنويه بشكل كبير عن «الهندسة الاجتماعية» بوصفها من أخطر أنواع الهجوم للحصول على كلمات المرور والتي عادة ما لا يتم الانتباه إليها.
  - o عند شعور المستخدم أنه وقع ضحية الهندسة الاجتماعية عليه كتابة تقرير بالحادثة إلى مسئول الأمن فورًا، كما عليه أن يبلغ الآخرين الذين يعملون في أماكن مشابهة حتى يأخذوا حذرهم.
  - o جعل النفايات في مكان آمن ومراقب جيدًا، والتخلص منها بأسلوب آمن (Granger, 2002).
- عند الدخول إلى المواقع الحساسة، يتم استخدام لوحة المفاتيح التي قد توفرها هذه المواقع ويتم فتحها على شاشة الحاسوب (الشكل رقم 8)لإدخال كلمات المرور، وذلك بهدف تجنب خطر برمجيات وأجهزة رصد لوحة المفاتيح.

الشكل رقم (8) لوحة المفاتيح التي تتوافر على شاشة الحاسوب

- عدم الدخول إلى تطبيقات الويب الحساسة من أجهزة غير محمية.

-التأكد من وجود برمجية مضادة للبرمجيات الخبيثة على جهاز المستخدم، وتحديثها باستمرار.

-توخي الحذر بشأن رسائل البريد الإلكتروني الاحتيالية، حتى لو بدت أنها واردة من مصدر موثوق به. وعند تسلم رسالة بها رابط لموقع على الإنترنت، ينبغي التحقق من أن الرابط لموقع حقيقي، ومن الأفضل عدم النقر على الرابط المرسل في الرسالة، وبدلاً من ذلك يتم نسخ الرابط ولصقه في المتصفح للتأكد منه.

- عند التعامل مع المواقع والتطبيقات المهمة يتم استخدام عامل توثق إضافي بالإضافة إلى كلمة المرور، لأن هذا يتطلب إضافة معلومات أخرى من المستخدم عند تسجيل الدخول، مما يصعب عمليات قرصنة كلمة المرور(Tamir، 2013).

المراجع

أولاً: روابط مواقع عينة الدراسة التي تم الاعتماد عليها للإجابة عن أسئلة قائمة المراجعة:

1. http://keepass.info/index.html
2. http://password-memory.jsoftj.com/1887
3. http://safe-in-cloud.com/en/
4. http://www.accessmanager.co.uk/download-free-version/
5. http://www.efficientpasswordmanager.com/freeedition.htm
6. http://www.thewindowsclub.com/passbox-download
7. https://identitysafe.norton.com/
8. https://pwsafe.org/
9. https://www.Dashlane.com/
10. https://www.enpass.io/
11. https://www.intuitivepassword.com/en/Service/CompareEditions
12. https://www.lastpass.com/
13. https://www.logmeonce.com/
14. https://www.Passwordbox.com/
15. https://www.roboform.com/

ثانيًا: المراجع التي أعتمد عليها الجانب النظري:

16. أحمد، فايزة دسوقي (2011). أمن معلومات السجلات الطبيّة الإلكترونيّة: مدينة الملك فهد الطبيّة نموذجًا.- العربية 3000. س 11، ع 43.

17. الرقميات (2013). برامج إدارة كلمات المرور: عندما ننسى كلمات المرور الكثيرة ! .- متاح في:
http://www.alrakameiat.com/?path=news/read/4535

18. الغثبر، خالد بن سليمان والقحطاني، محمد عبد الله (2009). أمن المعلومات بلغة ميسرة.-متاح في: http://coeia.edu.sa/images/stories/books/Information-Security.pdf

19. The SANS Institute (2013). تطبيقات "إدارة كلمات المرور".- متاح في:
https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201310_aa.pdf

20. Al-Sinani, Haitham S & Mitchell, Chris J (2011). Extending the Scope of CardSpace.- Available at:https://repository.royalholloway.ac.uk/items/28202256-639a-866c-a096-873f06c67a10/3/

21. Belenko, Andrey& Sklyarov, Dmitry (2012). "Secure Password Managers" and "Military-Grade Encryption" on Smartphones: Oh, Really?.- Available at: https://www.elcomsoft.com/WP/BH-EU-2012-WP.pdf

22. Bicakci, Kemal… [et al.,] (2011). Exploration and Field Study of a Browser-based Password Manager using Icon-based Passwords.- Available at: http://people.scs.carleton.ca/~paulv/papers/ipman-preproceedings.pdf

23. Cliff, A. (2001). Password crackers - ensuring the security of your password.- Available at: http://www.symantec.com/connect/articles/password-crackers-ensuring-security-your-password

24. Cluley, Graham (2015). Don't let the LastPass hack destroy your faith in password managers.- Available at: https://heatsoftware.com/security-blog/10249/lastpass-hack/

25. CommunityPepperdine (2016). Password Managers.- Available at: http://community.pepperdine.edu/it/security/password/passmgrs.htm

26. Create IT. Com. A comparison of password managers.- Available at: http://www.createitg.com/a-comparison-of-password-managers/

27. Depp, Greg (2014). Password Managers — Worth it?.- Available at: http://thefamilyhelpdesk.com/2014/10/24/password-managers-worth-it/

28. Drury, Ian (2012). Millions of internet shopping and banking customers at risk of crimes including fraud and identity theft because passwords they use are not secure enough.- Available at:http://www.dailymail.co.uk/news/article-2794511/millions-internet-shopping-banking-customers-risk-crimes-including-fraud-identity-theft-passwords-use-not-secure-enough.html

29. ElcomsoftCo. Ltd. (2010). Password Recovery.- Available at: http://www.elcomsoft.com/

30. Granger, Sarah (2001). Social engineering fundamentals, part I: Hacker tactics.- Available at: http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics

31. Granger, Sarah (2002). Social Engineering Fundamentals, part II: Combat Strategies.-

Available at: http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-ii-combat-strategies

32. Guenther, Melissa (2001). Social Engineering.- Available at: http://www.iwar.org.uk/comsec/resources/security-awareness/social-engineering-generic.pdf
33. Hiscott, Rebecca (2013). The Evolution of the Password — And Why It's Still Far From Safe.- Available at: http://mashable.com/2013/12/30/history-of-the-password/#77e0a..z0sqc
34. Hunsberger, Brent (2014). Password managers: Time to secure yourself one.- Available at:http://www.oregonlive.com/finance/index.ssf/2014/03/password_managers_online_security.html
35. Kak, Avi. (2016). AES: The Advanced Encryption Standard.- Available at:https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture8.pdf
36. Keepass (2016). KeePass Features.- Available at: http://keepass.info/features.html#lnkexp
37. Kovacs, Nadia (2015). Password Managers: Are The Key To Secure Passwords?.- Available at:http://community.norton.com/en/blogs/norton-protection-blog/password-managers-are-key-secure-passwords
38. Le VPN. Phishing Attack Targeting Password Managers.- Available at: https://www.le-vpn.com/phishing-attack-targeting-password-managers/
39. Li, Zhiwei… [et al.,]. The Emperor's New Password Manager: Security Analysis of Web-based Password Managers.- Available at: http://devd.me/papers/pwdmgr-usenix14.pdf
40. McCarney, Daniel (2013). Password Managers: Comparative Evaluation, Design, Implementation and Empirical Analysis.- Available at: https://www.scs.carleton.ca/content/password-managers-comparative-evaluation-design-implementation-and-empirical-analysis
41. McCarney, Daniel, … [et al.,] (2012). Tapas: Design, Implementation, and Usability Evaluation of a Password Manager.- Available at: http://people.scs.carleton.ca/~paulv/papers/acsac2012-tapas.pdf
42. McRobbie, Michael (2003). "It Security". In: Encyclopedia of Distributed Learning.- Available at: http://sage-ereference.com/distributedlearning/Article_n92.html.-
43. Noah (2015). Password managers: Never memorize a password again.- Available at:http://www.hackblossom.org/password-managers-protect-your-digital-life-from-yourself/
44. Nordquist, Brett (2016). The Risks and Rewards of Password Managers.- Available at:https://www.storagecraft.com/blog/the-risks-and-rewards-of-password-managers/
45. Notenboom, Leo A. (2016). Are Password Managers Safe? .- Available at: https://askleo.com/are_password_managers_safe/
46. securitystronghold (2016). 123 Write All Stored Passwords Removal: Remove 123

Write All Stored Passwords Easily.- Available at: https://www.securitystronghold.com/gates/123-write-all-stored-passwords.html#Technical

47. Silver, David … [et al.,] (2014). Password Managers: Attacks and Defenses.- Available at: https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-silver.pdf

48. Tamir, Dana. (2013). 3 Ways to Steal Corporate Credentials.- Available at:https://securityintelligence.com/3-ways-steal-corporate-credentials/#.VG3h3cn7h8E

49. Trumps, Nicole (2016). Password Managers Simplify The Login Process.- Available at: http://www.eliteteamofla.com/Blog/Password-Managers-Simplify-the-Login-Process

50. Westervelt, Robert (2014). Password Stealer: Citadel Banking Malware Targets Popular Password Managers.- Available at:http://www.crn.com/news/security/300074862/password-stealer-citadel-banking-malware-targets-popular-password-managers.htm

51. Zhao, Rui & Yue, Chuan. Toward A Secure and Usable Cloud-based Password Manager for Web Browsers.- Available at: http://www.cs.uccs.edu/~cyue/papers/LISA12.pdf

52. Zhao, Rui; Yue, Chuan & Sun, Kun (2013). Vulnerability and Risk Analysis of Two Commercial Browser and Cloud Based Password Managers.- Available at: http://www.cs.uccs.edu/~cyue/papers/ASEScience13.pdf

قائمة المراجعة

(1) ما المنصات التي تعمل عليها برمجيات إدارة كلمات المرور؟

- الحواسيب.
- الهواتف الذكية والأجهزة اللوحية.
- الإنترنت.

(2) ما نظم التشغيل التي تدعمها برمجيات إدارة كلمات المرور؟

- Windows
- Linux
- Android
- iOS
- MAC OS X
- Windows Phone
- أخرى (يتم تحديدها).

(3) ما متصفحات الإنترنت التي تدعمها برمجيات إدارة كلمات المرور؟

- Chrome
- Internet Explorer
- Firefox
- Safari Safari
- Opera
- Yandex
- أخرى (يتم تحديدها).

(4) ما نوع المصدر في برمجيات إدارة كلمات المرور؟

- مغلقة المصدر.
- مفتوحة المصدر.

(5) هل تدعم واجهات برمجيات إدارة كلمات المرور اللغة العربية؟

- نعم.
- لا.

(6) ما الخدمات التي توفرها برمجيات إدارة كلمات المرور؟

- حفظ كلمات المرور.
- توليد كلمات المرور.
- التسجيل اليدوي لكلمات المرور.
- التقاط كلمات المرور من المتصفح.
- تنظيم كلمات المرور.
- استيراد كلمات المرور.
- تصدير كلمات المرور.
- مشاركة كلمات المرور.
- النسخ الاحتياطي لكلمات المرور.
- حفظ معلومات.
- حسابات بعد الموت والطوارئ.
- المزامنة.
- أخرى (يتم تحديدها).

(7) ما إجراءات الحماية التي توفرها برمجيات إدارة كلمات المرور؟

- التوثق بكلمة مرور رئيسة قوية.
- التوثق بخاصية حيوية.
- تقييم قوة كلمة المرور.
- عدم استعادة كلمة المرور الرئيسة.
- عدم نقل كلمة المرور الرئيسة عبر الإنترنت.
- عدم الاحتفاظ بكلمة المرور الرئيسة على جهاز المستخدم.
- عدم الاحتفاظ بكلمة المرور الرئيسة على خادم البرمجية.
- الخروج بشكل آلي عند إغلاق الجهاز أو المتصفح.
- نظام تشفير آمن.
- أخرى (يتم تحديدها).

(8) ما طرق الدعم الفني التي توفرها برمجيات إدارة كلمات المرور؟

- أسئلة وإجابة جاهزة.
- دليل مستخدم.
- فيديو.
- نموذج.
- محادثة مباشرة.
- بريد إلكتروني.
- منتدى/ مدونة.
- أخرى (يتم تحديدها).