وخذوا حِذركم

إعداد: إسماعيل المغربي

بِسْمِ اللَّـهِ الرَّحْمَـٰنِ الرَّحِيمِ

مقدمة

الحمد لله الذي جعل الجهاد للعز قرينا، القائل في كتابه: (وَخُذُوا حِذْرَكُمْ ۗ إِنَّ اللَّهَ أَعَدَّ لِلْكَافِرِينَ عَذَابًا مُّهِينًا)، و الصلاة و السلام على سيدنا محمد المجاهد الشهيد، وعلى آله وصحبه وسلم تسليما أما بعد:

مع عصر التحول الرقمي المتسارع، وهيمنة القوى الغربية الكافرة على كبرى شركات التكنولوجيا، و تسييرها في خدمة أجندتها العالمية والتي من أولها تضييق الخناق على الإسلام و المسلمين لنسف هذا الدين الحنيف ومن يناصره في كل بقعة من بقاع الأرض ، فمع تزايد اعتمادنا على التكنولوجيا في كل جانب من جوانب حياتنا اليومية، من التواصل إلى العمل والتعلم وحتى إدارة الشؤون المالية، تبرز الحاجة الملحة إلى فهم أفضل لكيفية حماية بياناتنا الشخصية من التهديدات المتزايدة للحد أو التقليل من هذا الخطر الذي نحمله معنا كل الوقت و ندخله بيوتنا بإرادتنا.

تتعرض الخصوصية الرقمية اليوم لاختراقات متكررة، سواء من خلال سرقة البيانات الشخصية، أو المراقبة الجماعية، أو الاحتيال الإلكتروني. هذه التهديدات لا تقتصر على الأفراد فحسب، بل تمتد إلى المؤسسات والحكومات، مما يجعل الأمن الرقمي مسألة ذات أبعاد اجتماعية واقتصادية وسياسية واسعة. ومن هنا، يهدف هذا البحث إلى توفير أدوات واستراتيجيات عملية تساعد الفرد المسلم على تعزيز حماية خصوصيته وأمنه الرقمي.

سيستعرض البحث المفاهيم الأساسية للأمن الرقمي، ويقدم نصائح عملية لتأمين الهواتف الذكية والحواسيب، بالإضافة إلى استكشاف أدوات متقدمة مثل شبكات التخفي والتشفير الشامل. كما سيتم تسليط الضوء على أهمية الوعي الأمني والممارسات اليومية التي يمكن أن تقلل من التعرض للهجمات الإلكترونية.

من خلال هذا البحث، نأمل أن نساهم في تعزيز الوعي بأهمية الخصوصية والأمان الرقمي، وأن نقدم للقارئ الأدوات والمعرفة اللازمة لمواجهة التحديات الرقمية في عالم اليوم والله خير حفظاً وهو أرحم الراحمين.

أهمية الخصوصية والأمان الرقمي:

* **حماية البيانات الشخصية:** تشمل البيانات الشخصية معلومات حساسة مثل الاسم والعنوان ورقم الهاتف وتاريخ الميلاد، بالإضافة إلى معلومات مالية مثل أرقام الحسابات البنكية وبطاقات الائتمان. هذه البيانات إذا ما تم تسريبها أو اختراقها، قد تستغل في عمليات احتيال وسرقة هوية ومراقبة للشخص الذي تم اختراقه، وهذا من أهم الطرق الابتزازية التي يتعرض لها كثير من المسلمين الآن لإجبارهم على تنفيذ أعمال تجسسية ضد بلدانهم أو ضد جماعة معينة بغية اختراقها من الداخل.

* **الحفاظ على حرية التعبير:** في بعض الأنظمة الديكتاتورية، قد تستخدم الحكومات أو الشركات أدوات التتبع والمراقبة الرقمية لتقييد حرية التعبير والتضييق على المعارضين. كما ثبت ذلك على بعض الدول العربية مثل الإمارات العربية المتحدة ومصر والسعودية وغيرهم حيث يعدون من أبرز المشترين لخدمات برامج التجسس مثل برنامج (pegasus) الإسرائيلي.

* **الأمن المالي:** الجرائم الإلكترونية مثل التصيد الاحتيالي وسرقة البيانات أصبحت شائعة، وقد تؤدي إلى خسائر مالية كبيرة للأفراد والشركات. لذا، فإن اتخاذ التدابير اللازمة للأمن الرقمي يساعد على حماية الأموال والمعلومات المالية من السرقة.

* **الأمن الوطني:** لا يقتصر خطر الاختراق والتجسس على الأفراد والشركات، بل يمتد ليشمل الدول والحكومات. فقد تعرض البنية التحتية الحيوية والمؤسسات

الحكومية لهجمات سيبرانية، مما قد يؤدي إلى تعطيل الخدمات الأساسية وتهديد الأمن الوطني.

مخاطر الاختراق و التتبع الإلكتروني:

* **سرقة البيانات:** يقوم المخترقون بسرقة البيانات الشخصية والمالية لبيعها في السوق السوداء أو استخدامها في أغراض إرهابية ترغم الشخص المختَرق على الإذعان لأوامر المُختَرق وتنفيذ ما يطلب منه سواء التجسس أو الإسقاط وغيرها من الأعمال.

* **الاحتيال:** يستخدم المخترقون البيانات المسروقة في عمليات احتيال مالي، مثل انتحال الشخصية وفتح حسابات بنكية وهمية وسرقة الأموال.

* **الابتزاز:** قد يقوم المخترقون بابتزاز الأفراد أو الشركات، مهددين بنشر بياناتهم الشخصية أو المالية إذا لم يتم دفع فدية.

الفصل الأول:

مفاهيم أساسية في الأمن الرقمي

*** مصطلحات رئيسية:**

* الاختراق (Hacking): يشير إلى محاولة الوصول إلى نظام أو شبكة معلومات بشكل غير مصرح به، بهدف سرقة البيانات أو تعطيل النظام أو التجسس على المستخدمين.

* التتبع الرقمي (Tracking): هو جمع معلومات عن أنشطة المستخدمين على الإنترنت، مثل المواقع التي يزورونها والصفحات التي يشاهدونها والبيانات التي يدخلونها.

* التشفير (Encryption): هو تحويل البيانات إلى صيغة غير قابلة للقراءة، بحيث لا يمكن لأي شخص غير مصرح به الاطلاع عليها.

* VPN (الشبكة الافتراضية الخاصة): هي خدمة تسمح للمستخدمين بالاتصال بالإنترنت بشكل آمن ومجهول، عن طريق توجيه حركة المرور عبر خادم مشفر.
* محرك البحث Tor: هو شبكة افتراضية مجهولة المصدر، تسمح للمستخدمين بتصفح الانترنت بشكل مجهول وتجاوز الرقابة.
* البصمة الرقمية (Digital Footprint): هي مجموعة البيانات التي يتركها المستخدمون على الإنترنت، مثل المواقع التي يزورونها والبيانات التي يشاركونها.

التهديدات الشائعة:

* البرمجيات الخبيثة (Malware): هي برامج ضارة يتم تصميمها لإلحاق الضرر بأنظمة الحاسوب، مثل الفيروسات والديدان وبرامج التجسس.
* التصيد الاحتيالي (Phishing): هو محاولة للحصول على معلومات شخصية أو مالية حساسة من المستخدمين، عن طريق إرسال رسائل بريد إلكتروني أو روابط وهمية.
* التتبع عبر الإعلانات والكوكيز: تستخدم الشركات تقنيات التتبع لجمع معلومات عن المستخدمين، بهدف عرض إعلانات مخصصة لهم.

* اختراق الحسابات: يقوم المخترقون بمحاولة الوصول إلى حسابات المستخدمين على الإنترنت، مثل حسابات البريد الإلكتروني ووسائل التواصل الاجتماعي.

* مبادئ الحماية الأساسية:
* **مبدأ "الأقل امتيازًا"** (Least Privilege): يعني إعطاء المستخدمين الحد الأدنى من الصلاحيات اللازمة لأداء مهامهم، وذلك للحد من تأثير أي اختراق أو هجوم.

* **أهمية التحديثات الأمنية:** تقوم الشركات بإصدار تحديثات أمنية لأنظمتها وبرامجها، لإصلاح الثغرات الأمنية وحماية المستخدمين من الهجمات. لذا، من الضروري تثبيت التحديثات الأمنية بانتظام.
هذا الفصل يقدم لمحة موجزة عن المفاهيم الأساسية في الأمن الرقمي والتهديدات الشائعة، ويمهد الطريق للفصول اللاحقة التي ستتناول بالتفصيل كيفية حماية الهاتف الذكي والحاسوب والخصوصية على الإنترنت، بالإضافة إلى الأدوات المتقدمة للحماية والوعي الأمني.

الفصل الثاني:
حماية الهاتف الذكي

1. تأمين نظام التشغيل:
* **تفعيل القفل البيومتري:** تعتبر بصمة الإصبع أو التعرف على الوجه من الوسائل الفعالة لحماية الهاتف من الوصول غير المصرح به. تأكد من تفعيل هذه الميزة وإعدادها بشكل صحيح.
* **تحديث النظام بانتظام:** تقوم الشركات المصنعة بإصدار تحديثات دورية لأنظمة التشغيل لإصلاح الثغرات الأمنية وتحسين الأداء. لذا، من الضروري تثبيت هذه التحديثات فور صدورها.

* **تجنب "Jailbreak" أو "Rooting":** يشير مصطلح "Jailbreak" إلى إزالة القيود المفروضة على نظام iOS، بينما يعني "Rooting" منح المستخدم صلاحيات Root في نظام Android. هذه العمليات قد تعرض الهاتف لمخاطر أمنية، لذا ينصح بتجنبها.

2. إدارة التطبيقات:

* **اختيار مصادر موثوقة:** قم بتحميل التطبيقات من المتاجر الرسمية فقط، مثل Google Play Store لنظام Android و App Store لنظام iOS. تجنب تحميل التطبيقات من مصادر غير معروفة، فقد تحتوي على برامج ضارة.
* مراجعة الصلاحيات: قبل تثبيت أي تطبيق، تحقق من الصلاحيات التي يطلبها. إذا كان التطبيق يطلب صلاحيات لا تبدو ضرورية لوظيفته، فقد يكون هناك شيء مريب.

* **استخدام تطبيقات بديلة:** هناك العديد من التطبيقات البديلة التي تركز على الخصوصية والأمان، مثل Signal بدلاً من WhatsApp و DuckDuckGo بدلاً من Google.

3. اتصالات آمنة:
* **استخدام VPN:** تقوم خدمة VPN بتشفير بياناتك وإخفاء عنوان IP الخاص بك، مما يجعل تصفح الإنترنت أكثر أمانًا وخصوصية.
* **تجنب شبكات الواي فاي العامة:** شبكات الواي فاي العامة غالبًا ما تكون غير آمنة، وقد تسمح للمخترقين بالتجسس على بياناتك. إذا كنت مضطرًا لاستخدامها، فقم بتفعيل VPN.

4. تشفير البيانات:
* **تفعيل تشفير الهاتف:** معظم الهواتف الذكية الحديثة توفر خيار تشفير الجهاز، مما يحمي بياناتك في حالة فقدان الهاتف أو سرقته.
* **استخدام تطبيقات التخزين المشفرة:** هناك تطبيقات متخصصة توفر تشفيرًا قويًا لملفاتك وصورك ومقاطع الفيديو الخاصة بك، مثل Cryptomator.

نصائح إضافية:
* **استخدام كلمات مرور قوية:** اختر كلمات مرور معقدة وطويلة، وقم بتغييرها بشكل دوري.

* **الحذر من الرسائل والروابط المشبوهة:** لا تفتح رسائل البريد الإلكتروني أو الرسائل النصية التي تبدو مشبوهة، ولا تنقر على الروابط غير المعروفة.

* **تحديث التطبيقات بانتظام:** تأكد من تحديث جميع التطبيقات المثبتة على هاتفك بانتظام، حيث أن التحديثات غالبًا ما تتضمن إصلاحات للثغرات الأمنية.

* **عمل نسخ احتياطية للبيانات:** قم بعمل نسخ احتياطية لبياناتك الهامة بشكل دوري، حتى تتمكن من استعادتها في حالة فقدان الهاتف أو تلفه.

باتباع هذه النصائح، يمكنك تعزيز أمان هاتفك الذكي وحماية بياناتك من المخاطر السيبرانية المتزايدة.

الفصل الثالث:

الحماية على الحاسوب

1. تأمين النظام:

* **جدار الحماية (Firewall):** يعمل جدار الحماية كحاجز بين جهازك والانترنت، حيث يقوم بمراقبة حركة المرور الواردة والصادرة، ويمنع الوصول غير المصرح به. تأكد من تفعيل جدار الحماية وتكوينه بشكل صحيح.

* **برامج مكافحة الفيروسات:** تقوم برامج مكافحة الفيروسات بفحص جهازك بحثًا عن البرامج الضارة والفيروسات، وإزالتها إذا تم العثور عليها. قم بتثبيت برنامج مكافحة فيروسات موثوق به، وتأكد من تحديثها بانتظام.

* **أنظمة تشغيل مخصصة للخصوصية:** هناك أنظمة تشغيل مخصصة للخصوصية، مثل Tails و Linux، توفر مستوى عالٍ من الأمان والحماية من التتبع. إذا كنت تهتم بالخصوصية بشكل كبير، يمكنك تجربة أحد هذه الأنظمة.

2. التصفح الآمن:
* **متصفحات تركز على الخصوصية:** هناك متصفحات تركز على الخصوصية، مثل Brave و Tor Browser، توفر ميزات متقدمة لحماية خصوصيتك أثناء التصفح، مثل منع التتبع وحظر الإعلانات.

* **إضافات مكافحة التتبع:** يمكنك تثبيت إضافات على متصفحك، مثل uBlock Origin و Privacy Badger، لمنع المواقع من تتبع أنشطتك عبر الإنترنت.

3. إدارة الحسابات:
* **كلمات مرور قوية:** اختر كلمات مرور معقدة وطويلة، وقم بتغييرها بشكل دوري. لا تستخدم نفس كلمة المرور لحسابات مختلفة.

* **مدير كلمات المرور:** يمكنك استخدام مدير كلمات مرور، مثل Bitwarden و KeePass، لتخزين كلمات مرورك بشكل آمن و توليد كلمات مرور قوية.

* **تفعيل المصادقة الثنائية (2FA):** توفر المصادقة الثنائية طبقة إضافية من الأمان لحساباتك، حيث تتطلب إدخال رمز تحقق بالإضافة إلى كلمة المرور. قم بتفعيل هذه الميزة في جميع حساباتك التي تدعمها.

نصائح إضافية:
* **تحديث البرامج بانتظام:** تأكد من تحديث جميع البرامج المثبتة على جهازك بانتظام، حيث أن التحديثات غالبًا ما تتضمن إصلاحات للثغرات الأمنية.

* **الحذر من رسائل البريد الإلكتروني والروابط المشبوهة:** لا تفتح رسائل البريد الإلكتروني أو الرسائل النصية التي تبدو مشبوهة، ولا تنقر على الروابط غير المعروفة.

* **عدم استخدام أجهزة USB مجهولة المصدر:** تجنب استخدام أجهزة USB مجهولة المصدر، فقد تحتوي على برامج ضارة.

* **عمل نسخ احتياطية للبيانات:** قم بعمل نسخ احتياطية لبياناتك الهامة بشكل دوري، حتى تتمكن من استعادتها في حالة فقدان البيانات أو تلف الجهاز.

باتباع هذه النصائح، يمكنك تعزيز أمان جهازك وحماية بياناتك من المخاطر السيبرانية المتزايدة.

الفصل الرابع:
الخصوصية على الإنترنت

1. محركات البحث والبيانات:
* **استخدام محركات بحث بديلة:** تعتبر Google محرك البحث الأكثر استخدامًا في العالم، ولكنه يقوم أيضًا بجمع كميات هائلة من البيانات عن المستخدمين. يمكنك استخدام محركات بحث بديلة تركز على الخصوصية، مثل DuckDuckGo و Startpage، التي لا تقوم بتتبع أنشطتك ولا تخزن بياناتك الشخصية.

* **إدارة ملفات الكوكيز:** تستخدم المواقع ملفات الكوكيز لتتبع أنشطتك وتخصيص الإعلانات لك. يمكنك إدارة ملفات الكوكيز في متصفحك، وحذفها بانتظام لمنع المواقع من تتبعك.

* **حذف البصمة الرقمية:** تشير البصمة الرقمية إلى مجموعة البيانات التي تتركها على الإنترنت، مثل عنوان IP الخاص بك ونوع المتصفح الذي تستخدمه والمواقع التي تزورها. يمكنك استخدام أدوات لحذف البصمة الرقمية، مثل Tor Browser، لإخفاء هويتك على الإنترنت.

2. التواصل الاجتماعي:

* **تقليل مشاركة المعلومات الشخصية:** تجنب مشاركة معلوماتك الشخصية الحساسة على وسائل التواصل الاجتماعي، مثل رقم هاتفك وعنوانك وتاريخ ميلادك.

* **ضبط إعدادات الخصوصية:** قم بمراجعة إعدادات الخصوصية على منصات التواصل الاجتماعي التي تستخدمها، وتأكد من أنها مضبوطة بشكل يحمي خصوصيتك.

* **الحذر من التطبيقات:** كن حذرًا من التطبيقات التي تسمح لها بالوصول إلى حساباتك على وسائل التواصل الاجتماعي، وتأكد من أنها جديرة بالثقة.

3. البريد الإلكتروني:
* **استخدام خدمات بريد إلكتروني مشفرة:** هناك خدمات بريد إلكتروني مشفرة، مثل ProtonMail و Tutanota، توفر مستوى عالٍ من الخصوصية والأمان لرسائلك.
* **تجنب فتح مرفقات أو روابط مشبوهة:** لا تفتح مرفقات البريد الإلكتروني أو الروابط التي تبدو مشبوهة، فقد تحتوي على برامج ضارة.

* **الحذر من رسائل التصيد الاحتيالي:** كن حذرًا من رسائل البريد الإلكتروني التي تطلب معلومات شخصية أو مالية، فقد تكون محاولات تصيد احتيالي.

نصائح إضافية:
* **استخدام VPN:** يمكن لخدمة VPN أن تساعدك على حماية خصوصيتك على الإنترنت عن طريق إخفاء عنوان IP الخاص بك وتشفير بياناتك.

* **تجنب المواقع غير الآمنة:** لا تدخل إلى المواقع التي لا تستخدم بروتوكول HTTPS، حيث أن هذه المواقع قد تكون غير آمنة وتعرض بياناتك للخطر.

* **قراءة سياسات الخصوصية:** قبل استخدام أي موقع أو خدمة عبر الإنترنت، اقرأ سياسة الخصوصية الخاصة بها لمعرفة كيفية جمع بياناتك واستخدامها.

باتباع هذه النصائح، يمكنك حماية خصوصيتك على الإنترنت وتقليل المخاطر السيبرانية التي قد تواجهها.

الفصل الخامس:

أدوات متقدمة للحماية

1. شبكات التخفي:
* **كيفية استخدام Tor:** تعتبر شبكة Tor من أقوى الأدوات المتاحة للتصفح المجهول وإخفاء هويتك على الإنترنت. تعمل Tor عن طريق توجيه حركة المرور الخاصة بك عبر سلسلة من الخوادم المتطوعة، مما يجعل من الصعب تتبعك أو تحديد موقعك.

* **حدود وفوائد Tor:** على الرغم من قوتها، إلا أن Tor لها بعض الحدود، مثل بطء التصفح في بعض الأحيان. ومع ذلك، فإن فوائدها في حماية الخصوصية والتجاوز الرقابة تفوق هذه العيوب.

2. التشفير الشامل:

* **تشفير المحادثات:** توفر بعض تطبيقات المراسلة، مثل Signal و Telegram (في الوضع السري)، تشفيرًا شاملاً للمحادثات، مما يضمن أن الرسائل لا يمكن قراءتها من قبل أي شخص آخر غير المرسل إليه والمستقبل.

* **تشفير الملفات:** يمكنك استخدام برامج تشفير الملفات، مثل VeraCrypt و AxCrypt، لتشفير ملفاتك الهامة وحمايتها من الوصول غير المصرح به.

3. الحماية من التتبع الجغرافي:
* **تعطيل خدمات الموقع:** العديد من التطبيقات والخدمات تطلب الوصول إلى موقعك الجغرافي. يمكنك تعطيل خدمات الموقع غير الضرورية لحماية خصوصيتك.

* **استخدام تطبيقات الخرائط البديلة:** هناك تطبيقات خرائط بديلة، مثل OsmAnd، لا تقوم بتتبع موقعك الجغرافي.

نصائح إضافية:
* **استخدام نظام تشغيل آمن:** يمكنك تثبيت نظام تشغيل آمن على جهازك، مثل Tails، الذي يوفر مستوى عالٍ من الخصوصية والأمان.

* **استخدام أجهزة تخزين مشفرة:** يمكنك استخدام أجهزة تخزين خارجية مشفرة لحماية بياناتك الهامة.

* **التعلم المستمر:** ابحث عن المزيد من الأدوات والتقنيات المتقدمة لحماية خصوصيتك وأمانك على الإنترنت، حيث أن هذا المجال يتطور باستمرار.
باتباع هذه النصائح واستخدام الأدوات المتقدمة، يمكنك تعزيز مستوى الأمان والخصوصية بشكل كبير وحماية بياناتك من المخاطر السيبرانية المتزايدة.

الفصل السادس:

الوعي الأمني والممارسات اليومية

1. التعرف على الهجمات:

* **علامات التصيد الاحتيالي:** يعتبر التصيد الاحتيالي من أكثر الهجمات شيوعًا، حيث يقوم المخترقون بإرسال رسائل بريد إلكتروني أو رسائل نصية تبدو وكأنها من مصادر موثوقة، مثل البنوك أو الشركات، بهدف الحصول على معلومات شخصية أو مالية. يجب الانتباه إلى علامات التصيد الاحتيالي، مثل الأخطاء الإملائية والنحوية والروابط المشبوهة.

* **تجنب التصيد الاجتماعي:** يعتمد التصيد الاجتماعي على استغلال ثقة المستخدمين وخداعهم للكشف عن معلومات حساسة. يجب الحذر من الأشخاص الذين يتصلون بك عبر الإنترنت ويطلبون معلومات شخصية أو مالية، حتى لو كانوا يدعون أنهم من جهات موثوقة.

2. عادات آمنة:

* **نسخ احتياطي منتظم للبيانات:** قم بعمل نسخ احتياطية لبياناتك الهامة بشكل دوري، حتى تتمكن من استعادتها في حالة فقدان البيانات أو تلف الجهاز.

3. التثقيف المستمر:

* **متابعة أخبار الثغرات الأمنية:** تابع أخبار الثغرات الأمنية واقرأ عن الهجمات السيبرانية الشائعة، حتى تكون على دراية بأحدث التهديدات وكيفية التعامل معها.

'

* **مصادر موثوقة لتعلم الأمان الرقمي:** هناك العديد من المصادر الموثوقة التي يمكنك من خلالها تعلم المزيد عن الأمان الرقمي، مثل المواقع الإلكترونية والمدونات والكتب والدورات التدريبية.

خاتمة

في الختام، نؤكد على أن حماية الخصوصية والأمن الرقمي هي مسؤولية مشتركة بين الأفراد والمؤسسات. يجب علينا جميعًا أن نكون على دراية بالمخاطر السيبرانية وأن نتخذ الإجراءات اللازمة لحماية أنفسنا و بياناتنا. نرجوا من الله أن يكون هذا البحث قد ساهم في زيادة الوعي بأهمية هذا الموضوع وتزويد القارئ بالأدوات والمعرفة اللازمة لحماية خصوصيته وأمنه الرقمي. و الله خير حفظا وهو أرحم الراحمين.