

# دليل الأمان الرقمي

حماية عالمك الرقمي بأمان وفعالية

إعداد:

عبد القادر حسين

ahussain@codeexpert.com.tr



# جدول المحتويات

المقدمة	01
مفاهيم تأسيسية عن الأمان الرقمي	02
الوعي في العالم الرقمي	03
لماذا يجب الحفاظ على الأمان الرقمي	04
أنظمة الأمان والخدمات والبرامج	05
التشفير	06
النسخ الاحتياطي	07
كلمات المرور وتأمين متصفحات الويب	08
الحماية	09
تأمين الهاتف المحمول	10
حماية معلومات الشركة وبيانات العملاء	11



# مقدمة



مع التطور السريع للتكنولوجيا وانتشار استخدام الإنترنت في مختلف جوانب الحياة اليومية، أصبح الأمان الرقمي ضرورة ملحة لحماية البيانات الشخصية والمؤسسات من التهديدات الإلكترونية. يشير الأمان الرقمي إلى مجموعة من الممارسات والإجراءات والتقنيات التي تهدف إلى تأمين الأنظمة الرقمية والمعلومات من الوصول غير المصرح به، والاختراق، أو التلاعب.

يتضمن الأمان الرقمي عدة جوانب، منها حماية الأجهزة الشخصية، تأمين الشبكات، استخدام كلمات مرور قوية، وتحديث البرامج بانتظام. كما يشمل أيضاً التوعية بالمخاطر مثل التصيد الاحتيالي، البرمجيات الخبيثة، والهجمات السيبرانية.

في عصر يعتمد فيه الأفراد والشركات بشكل متزايد على التقنيات الرقمية لإدارة أعمالهم وخصوصياتهم، يمثل الأمان الرقمي خط الدفاع الأول ضد التهديدات التي قد تؤدي إلى خسائر مالية أو انتهاكات للخصوصية. لذلك، يُعد الاستثمار في تعزيز الوعي الرقمي وتبني أدوات الحماية من الأولويات لضمان بيئة رقمية آمنة ومستقرة.

# مفاهيم تأسيسية عن الأمان الرقمي



## الخصوصية الرقمية (Digital Privacy) 02

تشير إلى حق الأفراد في التحكم بالمعلومات الشخصية الخاصة بهم على الإنترنت، وكيفية جمعها واستخدامها ومشاركتها.

## إدارة الهوية (Identity Management) 04

هي الطرق والتقنيات التي تُستخدم للتحقق من هوية المستخدمين وإدارة وصولهم إلى الأنظمة الرقمية. يتم ذلك عادة باستخدام كلمات المرور، أو المصادقة متعددة العوامل.

## البيانات الحساسة (Sensitive Data) 01

هي المعلومات التي يجب حمايتها من الوصول غير المصرح به، وتشمل البيانات الشخصية (مثل الاسم، العنوان، وأرقام الهوية) والبيانات المالية (مثل أرقام البطاقات المصرفية) وبيانات العمل السرية.

## التشغیر (Encryption) 03

عملية تحويل البيانات إلى صيغة غير مفهومة للأطراف غير المصرح لها، باستخدام خوارزميات وبرمجيات تشغیر، مما يجعل البيانات محمية حتى لو تم الوصول إليها.

# مفاهيم تأسيسية عن الأمان الرقمي



## البرمجيات الخبيثة (Malware) 06

تشمل فيروسات الحاسوب، برامج الفدية، وبرامج التجسس. تهدف إلى التسبب في أضرار للنظام أو سرقة البيانات.

## الجدران النارية (Firewalls) 05

أدوات حماية تُستخدم لمنع الدخول غير المصرح به إلى الشبكات أو الأجهزة عن طريق مراقبة حركة المرور الواردة والصادرة.

## المصادقة متعددة العوامل (MFA) 08

آلية أمان تضيف طبقة إضافية من الحماية تتطلب من المستخدمين إثبات هويتهم من خلال تقديم أكثر من وسيلة تحقق (مثل كلمة مرور ورمز يتم إرساله للهاتف).

## التصيد الاحتيالي (Phishing) 07

أحد أشكال الاحتيال الإلكتروني الذي يتم فيه خداع المستخدمين لتقديم معلومات حساسة، مثل كلمات المرور أو بيانات البطاقة البنكية، عبر رسائل مزيفة أو موقع تبدو حقيقة.

# مفاهيم تأسيسية عن الأمان الرقمي



## التحديثات الأمنية (Security Patches) 09

هي تحديثات تصدرها الشركات المصنعة للبرمجيات لإصلاح ثغرات أمنية تم اكتشافها، مما يجعل النظام أقل عرضة للاختراق.

## النسخ الاحتياطي (Backup) 10

نسخ البيانات والاحتفاظ بها في مكان آمن لضمان استعادتها في حال حدوث أخطاء أو هجمات إلكترونية.



# الوعي في العالم الرقمي



يُعد الوعي في العالم الرقمي أساساً مهماً لحماية الأفراد والمؤسسات من التحديات والمخاطر التي تصاحب استخدام التكنولوجيا والإنترنت. يتمثل هذا الوعي في إدراك المخاطر التي قد تنتج عن مشاركة البيانات الشخصية، وكيفية التعامل مع التهديدات الرقمية مثل **التصيد الاحتيالي**، **البرمجيات الخبيثة**، و**انتهاكات الخصوصية**.

تعزيز الوعي الرقمي يشمل **تعليم الأفراد كيفية التعرف على المحتوى المشبوه**، استخدام **تقنيات الأمان** مثل **التشفير** و**كلمات المرور القوية**، و**التعامل بمسؤولية مع المحتوى الرقمي**. كما يتضمن فهم حقوقهم وواجباتهم في الفضاء الرقمي، و**ضمان التعامل الآمن مع الأجهزة والشبكات المستخدمة**.

إن تعزيز هذا الوعي يساهم في **تمكين الأفراد من اتخاذ قرارات واعية** أثناء استخدامهم للإنترنت، **ويقلل من احتمالية تعرضهم للاختراق أو الوقوع ضحية للجرائم الإلكترونية**. مما **يعزز الأمن الشخصي والمجتمعي في البيئة الرقمية**.



# لماذا يجب الحفاظ على الأمان الرقمي؟

الحفاظ على الأمان الرقمي ضرورة أساسية في ظل التحديات والمخاطر المتزايدة في العالم الرقمي. هناك جانبان رئيسيان يجب مراعاتها في هذا السياق:

**1. الأمان:** يشير الأمان إلى ضمان خلو الأجهزة والخدمات التي نستخدمها من البرمجيات الخبيثة أو التي تراقب بياناتنا وترسلها إلى جهات خارجية دون علمنا. من أمثلة ذلك:

03

## البرمجيات الخارة

التي قد تخرب أجهزتك أو تعطلها بشكل كبير.

02

## التصيد الاحتيالي

محاولات لخداعك للحصول على معلومات حساسة أو اختراق حساباتك الشخصية.

01

## التجسس وسرقة البيانات

مثل البرمجيات التي تسرق أرقام بطاقاتك الآئتمانية أو كلمات المرور.

استخدام أجهزة أو خدمات غير آمنة يمكن أن يعرضك لاختراق بياناتك وملفاتك وسرقة معلوماتك وأموالك، مما قد يؤدي إلى أضرار لا يمكن تصوّرها.

# لماذا يجب الحفاظ على الأمان الرقمي؟



**2. الخصوصية:** تعني الخصوصية الرقمية الحفاظ على سرية نشاطاتك على الإنترنت ومنع الآخرين من الوصول إلى معلوماتك الشخصية. تشمل الخصوصية درجة السرية التي تتمتع بها أثناء التصفح أو إجراء المعاملات عبر الإنترنت. تضمن الخصوصية أن معلوماتك مثل: ([نشاطك](#), [بياناتك الشخصية](#), [وسلوكياتك الرقمية](#)), تبقى في مأمن من التتبع أو الاستغلال.



## ما العلاقة بين الأمان والخصوصية؟

س

- الأمان هو الأساس الذي يبني عليه الحفاظ على الخصوصية.
- بدون أمان، تصبح بياناتك ونشاطاتك عرضة للخترق والاستغلال من قبل الآخرين.

## لماذا الأمان هو الأساس؟

س

- إذا لم تحافظ على الأمان الرقمي، فإنك تعرض نفسك للعديد من المخاطر، منها:
- سرقة معلوماتك الحساسة مثل بياناتك المالية أو حساباتك الشخصية.
  - استغلال معلوماتك بشكل غير مشروع أو مسيء.
  - إتلاف أو تعطيل الأجهزة والملفات الخاصة بك.

الحفاظ على الأمان الرقمي ليس مجرد حماية للأجهزة، بل هو حماية لهوبيتك وخصوصيتك وأصولك في العالم الرقمي.



# **أنظمة الأمان والخدمات والبرامج**

تشكل أنظمة الأمان والخدمات والبرامج جزءاً أساسياً من حماية الأجهزة، الشبكات، والبيانات في العالم الرقمي. صُممَت هذه الأدوات والتقنيات للتتصدي للتهديدات المختلفة مثل البرمجيات الخبيثة، التصيد الاحتيالي، والوصول غير المصرح به.



# أنظمة الأمان والخدمات والبرامج



1. **أنظمة الأمان:** أنظمة الأمان هي الأدوات التقنية التي تُستخدم لتوفير الحماية للأجهزة والبيانات. من أبرز هذه الأنظمة:

## جدار الحماية (Firewalls) 01

تعمل ك حاجز بين شبكتك الخاصة والشبكات العامة، حيث تُراقب حركة البيانات وتمنع أي محاولات غير مرخصة للدخول. أمثلة: SonicWall, Cisco ASA.

## أنظمة كشف التسلل (IDS) وأنظمة منع التسلل (IPS) 02

تساعد في تحديد النشاط غير الطبيعي في الشبكة ومنع الهجمات في الوقت الفعلي. أمثلة: Snort, Suricata.

## مضادات الفيروسات والبرامج الضارة 03

تُستخدم لتحديد وإزالة البرمجيات الضارة التي قد تصيب الأجهزة. أمثلة: Norton, Kaspersky, Malwarebytes.



# أنظمة الأمان والخدمات والبرامج



**2. الخدمات:** الخدمات الأمنية تعتمد على مجموعة من الحلول السحابية أو المدارة لضمان حماية البيانات وتقديم مراقبة دائمة. أمثلة على ذلك:

03

## خدمات إدارة الهوية والوصول (IAM):

تدير حقوق الوصول للمستخدمين.

أمثلة: Azure AD, Okta

02

## خدمات التحقق الثنائي (2FA):

تضيف طبقة إضافية من الأمان  
لتسجيل الدخول. أمثلة: Google  
Authenticator, Authy

01

## خدمات تأمين البريد الإلكتروني:

تتيح تشفير البريد الإلكتروني وحمايته  
من التصيد الاحتيالي والهجمات.

أمثلة: Microsoft Defender for Office 365,  
ProtonMail

# أنظمة الأمان والخدمات والبرامج



3. البرامج: هناك برامج متنوعة تلبي احتياجات الحماية الرقمية على مستويات مختلفة:

## أدوات فحص أمان الشبكات

مثل: Nmap. لتحليل الشبكة واكتشاف الثغرات.

## برامج النسخ الاحتياطي الآمنة

مثل: Carbonite.Acronis لضمان استعادة البيانات في حالات الطوارئ.

## برامج التشفير

مثل: VeraCrypt. لتشفيير الأقراص والمجلدات، أو Signal لتشفيير المحادثات.

## إدارة كلمات المرور

مثل: Dashlane, LastPass، Bitwarden. تُستخدم لتخزين كلمات المرور بشكل آمن وإنشاء كلمات مرور قوية.

# أنظمة الأمان والخدمات والبرامج



**4. الأنظمة المتكاملة:** العديد من الشركات تستخدم أنظمة متكاملة مثل:

## إدارة معلومات الأمان والأحداث (SIEM):

تجمع بين التحليل والذكاء الاصطناعي لرصد التهديدات، مثل: IBM QRadar، Splunk.

## الأمن السحابي (Cloud Security)

. AWS Security Hub, Microsoft Azure Security Center: تشمل حلولًا مثل: لحماية البيانات في البيانات السحابية.

# التشغیر ودوره في حماية البيانات



## التشغیر:

هو عملية تحويل البيانات الأصلية (النص الصريح) إلى صيغة غير قابلة للقراءة (النص المشفر) باستخدام خوارزميات رياضية و密钥. لا يمكن قراءة البيانات المشفرة إلا بواسطة الأطراف التي تمتلك المفتاح الصحيح لفك التشفير.

## الاستخدامات الأساسية للتشفير:

### .1. حماية البيانات أثناء النقل:

- عندما تُرسل بيانات عبر الشبكات (مثل الإنترنت)، تكون عرضة للاعتراض. التشفير يضمن أن البيانات المُعرضة تكون غير مفهومة بدون المفتاح.

### أمثلة:

- تشغیر الاتصالات باستخدام بروتوكول HTTPS (المستخدم في HTTPS) لتأمين موقع الويب
- تشغیر البريد الإلكتروني عبر PGP (Pretty Good Privacy) لتأمين الرسائل.

# التشغیر ودوره في حماية البيانات



## الخدمات الأساسية للتشغیر:

### .2 حماية البيانات المخزنة:

- تُستخدم تقنيات التشغیر لحماية الملفات المخزنة على الأقراص الصلبة أو السحابة من الوصول غير المصرح به.

#### أمثلة:

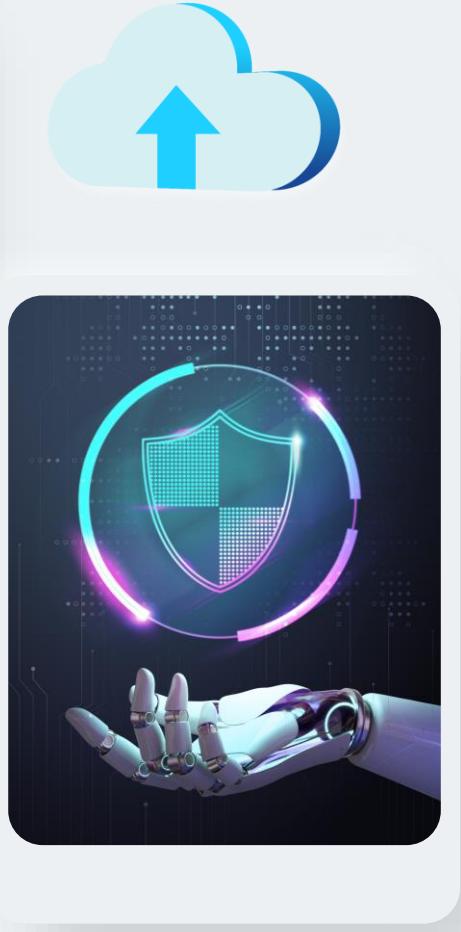
- تشغیر الأقراص الكاملة باستخدام برامج مثل FileVault أو BitLocker
- حماية قواعد البيانات باستخدام AES (Advanced Encryption Standard)

### .3 المصادقة والتحقق من الهوية:

- يساهم التشغیر في إنشاء توقيعات رقمية تُستخدم للتحقق من أن البيانات لم تتعرض للتلاعب أثناء النقل..

#### أمثلة:

- توقيع المستندات باستخدام PKI (Public Key Infrastructure)
- التحقق من هويات المستخدمين عبر الشهادات الرقمية.



# التشغیر ودوره في حماية البيانات



## الخدمات الأساسية للتشغیر:

### .4 الاتصالات الآمنة:

- تستخدم أنظمة التشغیر لتأمين المکالمات والمراسلات.

أمثلة:

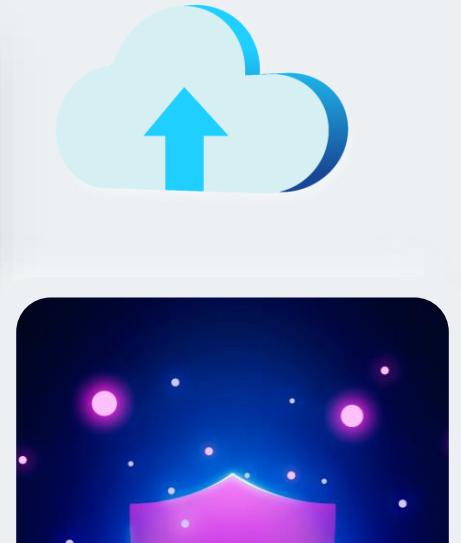
- تطبيقات التراسل الفوري مثل WhatsApp و Signal تعتمد على التشغیر من طرف إلى طرف (End-to-End Encryption).

### .5 حماية كلمات المرور:

- يتم تشغیر كلمات المرور في قواعد البيانات لمنع اختراقها حتى في حالة تسريب قاعدة البيانات.

أمثلة:

- استخدام التجزئة المشفرة عبر خوارزميات مثل SHA-256 أو bcrypt.



# كيف يساهم التشفير في حماية بياناتك؟



## تقليل تأثير الهجمات السيبرانية:

إذا تمكّن مهاجم من اختراق النظام وسرقة البيانات، فإن التشفير يمنعه من الاستفادة منها دون المفتاح الصحيح.

02

## منع التجسس والاعتراض:

التفير يجعل البيانات غير قابلة للقراءة، حتى لو تمكّن شخص غير مصرح له من الوصول إليها أثناء النقل أو التخزين.

01

## ضمان النزاهة:

عند استخدام تقنيات التشفير مع التوقيعات الرقمية، يمكن التأكد من أن البيانات لم يتم تعديلها أثناء النقل.

04

## تعزيز الخصوصية:

التفير يحمي الاتصالات الشخصية والبيانات الحساسة من الكشف غير المصرح به.

03

## التوافق مع اللوائح:

تُطلب تقنيات التشفير في العديد من المعايير واللوائح التنظيمية مثل GDPR لحماية البيانات الحساسة.

05

التفير هو أحد الأعمدة الأساسية للأمان الرقمي. باستخدام التشفير، يمكن حماية المعلومات الحساسة مثل بيانات العملاء، الرسائل، الملفات، والمعاملات المالية من التعرض للاختراق أو التلاعب. ولتعزيز الأمان، يجب تطبيق التشفير بشكل متكمّل مع الأنظمة والخدمات الأخرى.

# النسخ الاحتياطي: درع الأمان لبياناتك



## أهمية النسخ الاحتياطي:

**النسخ الاحتياطي** هو عملية أساسية تهدف إلى تأمين البيانات والملفات لضمان عدم فقدانها في حالات الطوارئ مثل الأعطال المفاجئة، الفيروسات، أو حتى سرقة الأجهزة. تُعتبر هذه الممارسة من أهم الخطوات للحفاظ على ذكرياتك، مستنداتك، وبياناتك الحساسة.

## لماذا النسخ الاحتياطي مهم؟

### حالات التوقف المفاجئ للأجهزة:

01

قد يتوقف الجهاز عن العمل فجأة بسبب عطل تقني أو حادث، مما يؤدي إلى فقدان كل البيانات المخزنة.



# النسخ الاحتياطي: درع الأمان لبياناتك



لماذا النسخ الاحتياطي مهم؟

02

الإصابة بالفيروسات أو البرمجيات الخبيثة:

قد تسبب البرمجيات الخبيثة تشفير ملفاتك أو حذفها. النسخ الاحتياطي يتيح استرجاع هذه الملفات.

03

سرقة الجهاز:

فقدان الجهاز يعني فقدان البيانات، إلا إذا كانت هناك نسخة احتياطية آمنة.

04

الأخطاء البشرية:

يمكن أن يتم حذف الملفات المهمة أو تعديلها بشكل خاطئ، مما يجعل النسخ الاحتياطي ضرورياً لاستعادة النسخ الأصلية.



# أنواع النسخ الاحتياطي



السلبيات	الإيجابيات	الاستخدام	أنواع النسخ الاحتياطي
<ul style="list-style-type: none"><li>1. تطلب إجراء النسخ يدوياً بشكل دوري.</li><li>2. قد يكون عرضة للفقدان أو التلف المادي.</li></ul>	<ul style="list-style-type: none"><li>1. غير مقيد بحجم معين، مما يتيح نسخ ملفات كبيرة أو حتى نظام التشغيل بأكمله.</li><li>2. لا يعتمد على شركات خارجية، مما يمنحك سيطرة كاملة على ملفاتك.</li></ul>	<p>يتم فيه تخزين الملفات على وسائل خارجية مثل الأقراص الصلبة المحمولة أو وحدات USB.</p>	التخزين المحلي (Local Storage)
<ul style="list-style-type: none"><li>1. محدودية المساحة المجانية.</li><li>2. الاعتماد على شركات خارجية قد تعرض الملفات للانقطاع أو انتهاءك الخصوصية.</li></ul>	<ul style="list-style-type: none"><li>1. المزامنة التلقائية مع مختلف الأجهزة.</li><li>2. سهولة المشاركة مع الآخرين.</li></ul>	<p>يتم فيه تخزين الملفات على خوادم عبر الإنترنت مثل Google Drive أو Dropbox</p>	التخزين السحابي (Cloud Storage)

# كيفية إجراء النسخ الاحتياطي بطرق مختلفة



## النسخ الاحتياطي عبر التخزين المحلي:

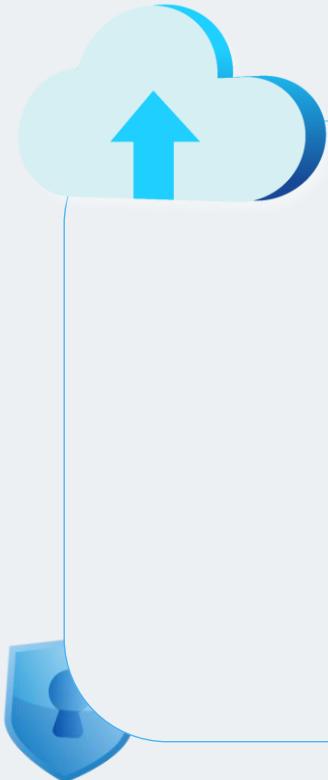
- ❖ استخدم أقراص صلبة خارجية أو وحدات تخزين USB لعمل نسخ احتياطية للملفات.
- ❖ استخدم برنامج مثل [Duplicati](#), الذي يدعم التشفير والجدولة لأتمتة العملية.
- ❖ خزن النسخة الاحتياطية في مكان منفصل عن الجهاز الأساسي.

## النسخ الاحتياطي عبر التخزين السحابي:

- ❖ اشتراك في خدمة تخزين مثل [Dropbox](#) أو [Google Drive](#).
- ❖ قم بتنصيب التطبيق الخاص بالخدمة على جهازك لتفعيل مزامنة الملفات تلقائياً.
- ❖ تأكد من تخزين الملفات المهمة داخل مجلد المزامنة الخاص بالخدمة لتحديثها تلقائياً.
- ❖ على الهواتف، يمكن تفعيل النسخ التلقائي للصور والمستندات عبر الإعدادات الخاصة بالخدمة.



# نصائح لزيادة فعالية النسخ الاحتياطي



- ❖ قم بجدولة النسخ الاحتياطي دوريًا لتجنب نسيان إجراء العملية.
- ❖ احتفظ بنسخة احتياطية في مواقعين مختلفين: واحدة سحابية وأخرى محلية.
- ❖ تحقق بانتظام من أن النسخ الاحتياطية تحتوي على الملفات المحدثة والمهمة.
- ❖ استخدم التشفير لحماية البيانات الاحتياطية، خاصةً عند استخدام التخزين السحابي.

النسخ الاحتياطي ليس مجرد إجراء تقني، بل هو استثمار في أمان بياناتك ومستقبلها. سواء اخترت التخزين المحلي أو السحابي، أو مزيجاً من الاثنين، فإن الالتزام بإجراء النسخ الاحتياطي بشكل منتظم سيجنبك الكثير من الخسائر والندم.

# كلمات المرور وتأمين متصفحات الويب



## أولاً: كلمات المرور

### أهمية كلمات المرور القوية

**حماية البيانات الشخصية:** تمنع الوصول غير المصرح به إلى الحسابات والمعلومات الحساسة.

**تقليل مخاطر الاختراق:** تجعل من الصعب على المخترقين فك شفراتها أو الوصول إلى معلوماتك.

### معايير إنشاء كلمة مرور قوية

**الطول:** يجب أن تكون كلمة المرور من 12 حرفاً أو أكثر.

**التنوع:** تحتوي على مزيج من الأحرف الكبيرة والصغيرة، الأرقام، والرموز.

**النفرد:** يجب أن تكون كلمة المرور مختلفة لكل حساب وغير مستخدمة في مكان آخر.

# كلمات المرور وتأمين متصفحات الويب



## أولاً: كلمات المرور

### نصائح لإدارة كلمات المرور

- استخدام برامج إدارة كلمات المرور: مثل Bitwarden أو LastPass لحفظ كلمات المرور وتأمينها.
- التحديث الدوري: تغيير كلمات المرور بشكل منتظم لزيادة الأمان.
- تجنب الكتابة على الورق: استخدم وسائل رقمية آمنة لتخزين كلمات المرور، وتجنب الاحتفاظ ورقياً.

# كلمات المرور وتأمين متصفحات الويب



## ثانياً: تأمين متصفحات الويب

### أهمية تأمين المتصفح

حماية الأنشطة على الإنترنت: تقليل مخاطر التجسس وسرقة البيانات أثناء التصفح.

منع البرامج الضارة: يساعد على منع تنزيل البرامج الضارة أو التعرض لمحاولات الاختراق.

### خطوات تأمين متصفح الويب

التحديث المنتظم: حافظ دائمًا على تحديث المتصفح للحصول على أحدث تصحيحات الأمان.

استخدام إضافات الحماية: مثل AdBlock Plus لتجنب الإعلانات الضارة و HTTPS Everywhere لضمان الاتصال الآمن.

تفعيل التصفح الآمن: قم بتشغيل ميزات الحماية مثل التصفح الآمن والمراقبة من الفيروسات.



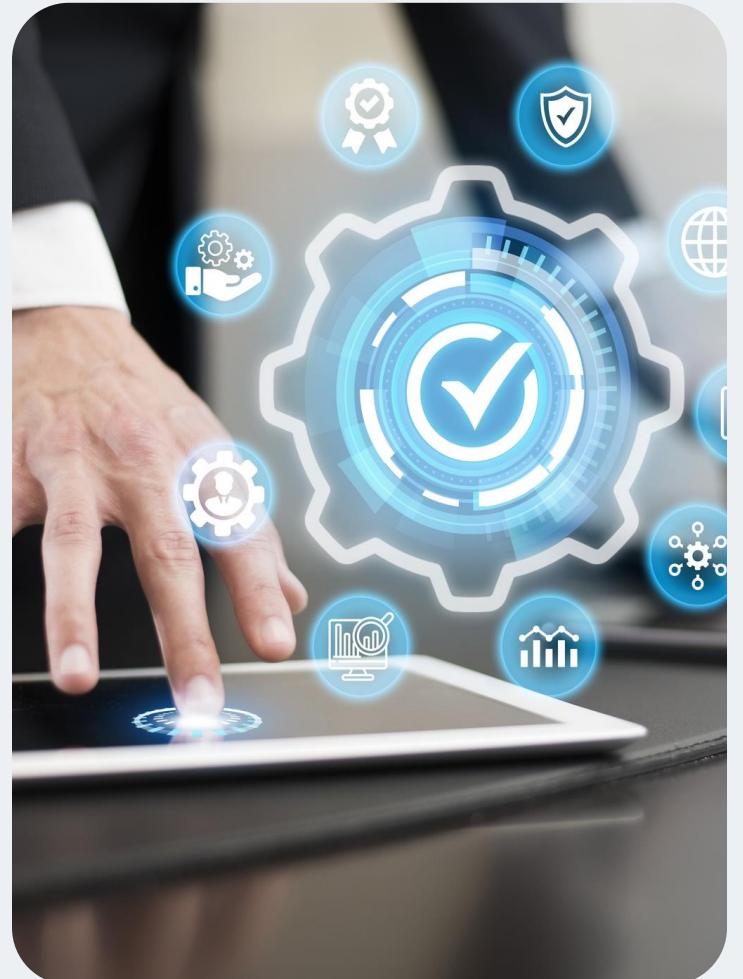
# كلمات المرور وتأمين متصفحات الويب



## ثانياً: تأمين متصفحات الويب

### سلوكيات تصفح آمنة

- تجنب الشبكات العامة:** تجنب إدخال بيانات حساسة أثناء استخدام شبكات Wi-Fi العامة غير الآمنة.
- التحقق من المواقع:** تأكد من أن المواقع تستخدم بروتوكول HTTPS قبل إدخال معلوماتك الشخصية.
- مسح بيانات التصفح بانتظام:** امسح ملفات الكوكيز وسجل التصفح بانتظام لتقليل تتبع نشاطك على الإنترنت.



تعدّ مواقع الإنترن特 بوابة أساسية لأنشطتنا الرقمية، لكنها أيضاً تمثل خطراً كبيراً على خصوصيتنا إذا لم نكن حذرين. يومياً، تتعرض بيانات المستخدمين لمحاولات تجسس أو استغلال من خلال تقنيات متقدمة وممارسات خفية تقوم بها بعض الجهات. لذا، يجب أن يكون تعاملنا مع مواقع الإنترن特 واعياً ومدروساً.

## . 1. الانتباه إلى نتائج البحث:

### مخاطر الكلمة المفتاحية:

عند إدخال كلمات بحث في محركات مثل Google، تصل مواقع الويب إلى الكلمة المفتاحية التي استخدمتها. قد تبدو هذه الممارسة عادية، لكن في حال ارتباطها بعنوان IP الخاص بك، يمكن استخدامها لتكوين صورة دقيقة عن نشاطاتك وhogiتك.

### الممارسات الآمنة:

- ✓ استخدم إضافات تمنع الموقع من معرفة "الصفحة المُحيطة" (Referral Page).
- ✓ لا تنقر على روابط نتائج البحث التي تبدو غير مألوفة أو تحمل أسماء نطاقات غريبة.



## سجلات البحث على مواقع الإنترنٌت:

### تسجيل النشاطات:

موقع التواصل مثل فيسبوك وتويتر تسجل عمليات البحث التي تقوم بها، مما يكشف اهتماماتك وحتى الأشخاص الذين تبحث عنهم.

### التأثير على الخصوصية:

هذه السجلات قد تستخدمها المواقع لتحسين إعلاناتها أو قد تكون عرضة للاختراق من قبل جهات خبيثة.

### الحلول:

- ✓ قم بحذف السجلات بانتظام من إعدادات الحساب.
- ✓ تعطيل تسجيل النشاط على منصات مثل جوجل من خلال صفحة "نشاطي" (My Activity).

## .3 إدارة رسائل البريد الإلكتروني:

### البريد الإلكتروني كبصمة شخصية:

يعتبر البريد الإلكتروني نقطة تجمع لكل أنشطتك الرقمية، حيث يحتفظ برسائل تحتوي على تفاصيل حساسة مثل استعادة كلمات المرور، العروض الترويجية، وحتى معلومات عن الحسابات المرتبطة به.

### التدابير الوقائية:

- ✓ تعطيل الإشعارات غير الضرورية من إعدادات الموقع.
- ✓ حذف الرسائل الحساسة بانتظام لمنع تراكمها.





## التسجيل في المواقع وإعطاء المعلومات:

### ما تكشفه عند التسجيل:

- ✓ عنوان IP الخاص بك.
- ✓ معاومات جهازك مثل الاسم والموقع.
- ✓ بصمة المتصفح (Browser Fingerprint) التي تتيح للموقع التعرف عليك بدقة.

### التقنيات الوقائية:

- ✓ استخدام أدوات تغيير بصمة المتصفح.
- ✓ الاعتماد على أسماء أو بيانات بديلة إذا كان التسجيل في موقع غير موثوق.

## الحذر من تطبيقات الطرف الثالث:

### تعريفها:

تطبيقات الطرف الثالث هي خدمات خارجية ترتبط بحساباتك على موقع التواصل أو الخدمات الأخرى لتوفير ميزات إضافية.

### المخاطر المحتملة:

قد تكون هذه التطبيقات وسيلة لاختراق حساباتك إذا حصلت على صلاحيات كبيرة أو إذا تعرضت هي نفسها لل اختراق.

### طرق الحماية:

- ✓ راجع بانتظام التطبيقات التي تمتلك صلاحيات على حساباتك.
- ✓ قم بإلغاء أي تطبيق لم تعد بحاجة إليه أو لا تثق بمصدره.
- ✓ لا توافق على منح الصلاحيات إلا للتطبيقات الرسمية والموثوقة.



# الحماية



"التعامل بحذر مع مواقع الإنترنت هو درعك الأول لحماية خصوصيتك وأمانك الرقمي. تأكد من أنك على دراية بالمارسات التي قد تهدد بياناتك واتخذ الخطوات الضرورية للتقليل من المخاطر. قضاء دقائق بسيطة لضبط إعدادات الأمان قد يوفر عليك الكثير من الجهد والمشاكل لاحقاً."



# تأمين الهاتف المحمول

في عالمنا الرقمي الحالي، يُعتبر تأمين الهاتف المحمولة من أهم الأولويات، حيث إن هذه الأجهزة ليست فقط أدوات تواصل، بل أصبحت مستودعاً لبياناتنا الشخصية وأسرارنا. ومع ذلك، فإن الهاتف المحمولة غالباً ما تكون نقطة ضعف رئيسية في منظومة الأمان الرقمي للمستخدم.



# تأمين الهاتف المحمول



لماذا تأمين الهواتف المحمولة مهم؟

أهمية العوطف في الحياة اليومية:

01

يقضي الأفراد ساعات طويلة على أجهزتهم المحمولة، مما يجعلها عرضة للاختراق.

طبيعة الهاتف غير المؤمنة افتراضياً:

02

بعكس الحواسيب، تأتي معظم الهواتف بأنظمة تشغيل وتطبيقات مغلقة المصدر، يصعب استبدالها أو التحكم بها دون المساس بضمان الشركة المصنعة.

تعقب الموقع والبيانات:

03

مزودو الشبكات والتطبيقات يستطيعون تحديد موقعك ومراقبة أنشطتك عبر الكاميرا، الميكروفون، وخدمات الموقع.



# أسسیات تأمين الهاتف المحمول



## استخدام قفل الشاشة

سواء كان نقشًا أو كلمة مرور، لمنع الوصول غير المصرح به.

01

## تعطيل الإشعارات على شاشة القفل

حماية لخصوصيتك من التغافل العرضي.

02

## إعداد التشفير الكامل

لضمان أمان البيانات حتى في حالة سرقة الجهاز.

03

# إدارة التطبيقات



01

03

**استخدام إصدارات الويب للتطبيقات**  
لتقليل الصلاحيات الممنوحة للتطبيقات التي  
تعمل على هاتفك.

01

02

## إدارة الأذونات

لا تمنح التطبيقات صلاحيات لا تحتاجها، مثل  
الوصول إلى الميكروفون أو الكاميرا إذا لم  
يكن ذلك ضرورياً.

01

01

**تنزيل التطبيقات من مصادر موثوقة**  
مثل متجر Google Play أو بدائل آمنة مثل:  
F-Droid أو Aurora Store.



# التحديثات وبرامج الأمان



تحديث النظام والتطبيقات باستمرار

للحصول على أحدث التصحيحات الأمنية.

تثبيت برامج مكافحة الفيروسات

لحماية الجهاز من البرمجيات الضارة.

تصفح الإنترنت بأمان

استخدم متصفحات آمنة مثل Firefox أو Brave للحصول على حماية إضافية أثناء تصفح الإنترنت.

# تأمين الهاتف المحمول



"رغم أن تأمين الهاتف المحمول بشكل كامل أمر شبه مستحيل بسبب طبيعة الأجهزة والأنظمة الحالية، إلا أن اتباع هذه الإجراءات يساعد على حماية بياناتك وتقليل المخاطر. تذكر دائمًا أن التأمين يبدأ من سلوكك الرقمي الوعي والحرص على خصوصيتك."



## حماية معلومات الشركة وبيانات العملاء

في العصر الرقمي الحديث، تُعتبر حماية معلومات الشركة وبيانات العملاء أحد أهم الأولويات لأي منظمة. ذلك لأن أي خرق أمني يمكن أن يؤدي إلى خسائر مالية كبيرة، تلف للسمعة، وتعريض بيانات حساسة للخطر. لضمان الأمان والخصوصية، يجب

اتباع الخطوات التالية:



# حماية معلومات الشركة وبيانات العملاء

1. **تصنيف البيانات:** تحديد وتصنيف البيانات الحساسة بناءً على أهميتها.
2. **التحكم في الوصول:** تطبيق مبدأ الحد الأدنى من الامتيازات واستخدام إدارة الهوية والصلاحيات.
3. **تشفير البيانات:** حماية البيانات أثناء النقل والتخزين بتقنيات التشفير الحديثة.
4. **النسخ الاحتياطي:** إجراء نسخ احتياطي مشفر ومنتظم للبيانات.
5. **تحديث الأنظمة:** ضمان تحديث الأنظمة والتطبيقات باستمرار.
6. **حماية الشبكات:** استخدام جدران الحماية، VPN، وأنظمة كشف التسلل.
7. **تدريب الموظفين:** توعية الموظفين بعمليات الأمان مثل تجنب التصيد الاحتيالي.

# حماية معلومات الشركة وبيانات العملاء



8. **حماية العملاء:** تخزين البيانات الشخصية بشكل آمن والالتزام بمعايير الخصوصية.

9. **مراقبة الأنظمة:** الكشف المبكر عن الأنشطة المشبوهة وتحليل سلوك المستخدم.

10. **الاستجابة للحوادث:** إعداد خطة واضحة للتعامل مع الحوادث الأمنية.



في ظل التحديات المتزايدة التي تواجهه أمن المعلومات، أصبحت حماية بيانات الشركة والعملاء ضرورة استراتيجية لا يمكن تجاهلها. من خلال اتباع أفضل الممارسات وتطبيق التقنيات الحديثة، يمكن للشركات تعزيز مستوى الحماية وتقليل المخاطر المرتبطة بالهجمات السيبرانية. إن الاستثمار في الأمان السيبراني ليس مجرد خيار، بل هو مسؤولية تضمن استدامة الأعمال والحفاظ على الثقة مع العملاء. بذلك، تصبح حماية المعلومات عنصراً أساسياً لتحقيق النجاح والنمو في عالم يتسم بالتطور الرقمي المستمر.

شكراً لكم!