

جرواب خبير مايكروسوفت

- الاسم / حسان سيد محمد بعد الغني
- الوظيفة / معلم شرعي بالأزهر الشريف
- رائد تحول رقمي
- مرشد سياحي فرنسي
- خبير مايكروسفت
- سفير في منصة T4 التعليمية
- سفير في منصة Olympia التعليمية
- سفير في منصة ويكايت التعليمية
- عضو في منصة اريد العلمية



الأمن السيبراني: حماية البيانات والعالم الرقمي

في عالمنا الرقمي سريع التطور، أصبح الأمن السيبراني ضرورة ملحة لحماية البيانات الشخصية والأعمال التجارية من التهديدات الإلكترونية المتزايدة. سنستكشف أهمية الأمن السيبراني وعناصره الأساسية، مع التركيز على كيفية الحفاظ على سلامة العالم الرقمي.



by Hassan Sayed Mohamed



أهمية الأمن السيبراني في عصر التكنولوجيا

الحماية من الهجمات

منع الهجمات الإلكترونية مثل القرصنة والفيروسات التي يمكن أن تؤثر على الأجهزة والبيانات.

ضمان سرية البيانات

الحفاظ على سرية المعلومات الشخصية والعملية والمنع من الوصول غير المصرح به إليها.

تعزيز الثقة

منح المستخدمين ثقة أكبر في استخدام الأجهزة والخدمات الرقمية، وتحسين سمعة الشركات.

عناصر الأمن السيبراني الأساسية



الجدار الناري

يعمل كحاجز بين شبكة الكمبيوتر والعالم الخارجي لمنع الوصول غير المصرح به.

مكافحة الفيروسات

يكتشف ويحذف البرامج الضارة التي يمكن أن تسبب ضررًا للأجهزة والبيانات.

التشفير

يحول البيانات إلى شكل غير قابل للقراءة لمنع الوصول غير المصرح به إليها.

التحقق من الهوية

يقوم بتأكيد هوية المستخدمين قبل السماح لهم بالوصول إلى أنظمة أو بيانات معينة.

الحماية من التهديدات الإلكترونية



استخدام برامج الأمان

تثبيت وتحديث برامج مكافحة الفيروسات والجدران النارية بانتظام.



التحقق من الهوية

استخدام كلمات مرور قوية وتغييرها بشكل دوري، وتفعيل المصادقة ثنائية العوامل.



التوعية

التعرف على أنواع التهديدات الإلكترونية الشائعة وكيفية تجنبها.

أنواع التهديدات السيبرانية الشائعة

1

الفيروسات

برامج ضارة مصممة لتدمير أو تعطيل الأجهزة والبيانات.

2

الهجمات التصيدية

رسائل البريد الإلكتروني أو المواقع الإلكترونية المزيفة التي تحاول سرقة بياناتك الشخصية.

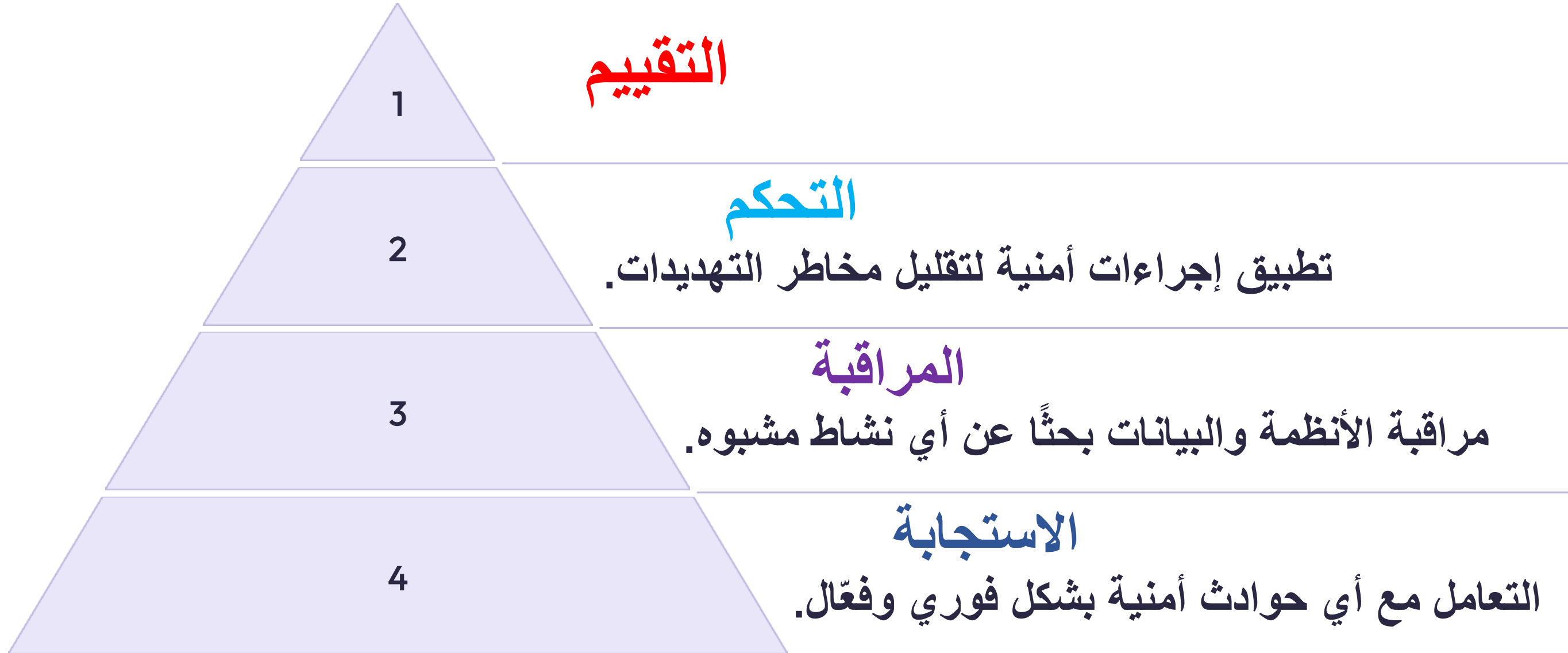
3

البرمجيات الخبيثة

برامج ضارة تُثبت على جهازك دون علمك وتعمل على جمع بياناتك.



إدارة المخاطر السيبرانية



الامتثال والتنظيمات في الأمن السيبراني

1

GDPR

القانون العام لحماية البيانات.

2

HIPAA

قانون الأمن والخصوصية لمعلومات الصحة.

3

PCI DSS

معيار أمان بيانات بطاقات الدفع.

「Ired ace
Speite lnrg.」



أفضل الممارسات للحماية من الهجمات السيبرانية

1

التحديثات

تحديث أنظمة التشغيل وبرامج الأمان بانتظام.

2

كلمات المرور

استخدام كلمات مرور قوية وتغييرها بشكل دوري.

3

التوعية

التعرف على أنواع الهجمات الإلكترونية وكيفية تجنبها.

دور الموارد البشرية في تعزيز الأمن السيبراني

- 1 التوعية بالمخاطر الإلكترونية.
- 2 تدريب الموظفين على أفضل الممارسات.
- 3 إنشاء ثقافة أمنية قوية.



التوجهات المستقبلية في مجال الأمن السيبراني

