
بسم الله الرحمن الرحيم

وزارة التعليم
Ministry of Education

NCEPD

الأمن السيبراني

الهدف العام

التعرف على أساسيات الأمن السيبراني

واستراتيجياته.

الأهداف التفصيلية

أنواع الهجمات

عناصر أمن المعلومات

التصيد الإلكتروني

مفهوم الأمن السيبراني

البرمجيات الخبيثة

إحصائيات وأرقام في الأمن السيبراني

كلمات السر

مجالات ومخاطر الإنترنت

الأهداف التفصيلية

اختراقات عالمية

اختراقات محلية

العيون الخمسة

بعض أساليب الحماية من الاختراقات

قصة سفر الملفات

التشفير

إحصائيات وأرقام في الأمن السيبراني

جهود المملكة العربية السعودية في الأمن السيبراني

خطة البرنامج التدريبي

اليوم التدريبي	العنوان	الموضوع/الموضوعات	الهدف	الزمن
الأول	مقدمة في أساسيات الأمن السيبراني	مصطلحات وتعريفات الفرق بين امن المعلومات والأمن السيبراني أهداف الأمن السيبراني نظرة تاريخية عن أبرز الهجمات طرق الاختراق	التعرف على أشهر مصطلحات الأمن السيبراني. التفريق بن أمن المعلومات والأمن السيبراني التعرف على اهداف الأمن السيبراني الاطلاع على تاريخ الأمن السيبراني التعرف على بعض طرق الاختراق	٤ ساعات
الثاني	الجرائم المعلوماتية	الجرائم المعلوماتية أساليب الحماية من الهجوم السيبراني	التعرف على الجرائم المعلوماتية تطبيق بعض أساليب الحماية من الهجوم السيبراني	٤ ساعات
الثالث	البرامج الخبيثة	الفيروسات الديدان احصنة طروادة خبراء ومجرمي الأمن السيبراني	التعرف على أشهر البرمجيات الخبيثة وطرق عملها. التعرف على خبراء ومجرمي الأمن السيبراني ودور كل منهم.	٤ ساعات

خطة البرنامج التدريبي

اليوم التدريبي	الجلسة التدريبية	العنوان	الموضوع/الموضوعات	الهدف/ المحور	الزمن
الأول	الأولى	مقدمة في أساسيات الأمن السيبراني	مصطلحات وتعريفات الفرق بين امن المعلومات والأمن السيبراني أهداف الأمن السيبراني	التعرف على أشهر مصطلحات الأمن السيبراني. التفريق بن أمن المعلومات والأمن السيبراني التعرف على اهداف الأمن السيبراني	٩٠ دقيقة
		استراحة			٢٠ دقيقة
	الثانية	مقدمة في أساسيات الأمن السيبراني	نظرة تاريخية عن أبرز الهجمات	الاطلاع على تاريخ الأمن السيبراني	٦٠ دقيقة
		استراحة			١٠ دقائق
	الثالثة	مقدمة في أساسيات الأمن السيبراني	طرق الاختراق	التعرف على بعض طرق الاختراق	٦٠ دقيقة

الجلسة التدريبية الأولى

٢٠ حقيقة ربما لا تعرفها عن الأمن السيبراني

١. ١ من كل ٣٦ جهاز معرض للاختراق بسبب تطبيقات غير موثوقة. المصدر: (Symantec)

٢. يتم برمجة ٣٠٠,٠٠٠ برمجية خبيثة يومياً. المصدر: (McAfee)

٣. كل ٣٩ ثانية، تحدث هجمة إلكترونية. المصدر: (security magazine)

٤. يتم سرقة ٧٥ سجل كل ثانية. المصدر: المصدر: (Breach Level Index)

٥. ٦٨% من الهاكرز يمكن هزيمتهم بالتشفير وطرق التحقق الثنائية. المصدر: (Thycotic)

٢٠ حقيقة ربما لا تعرفها عن الأمن السيبراني

٦. ٩٢% من البرمجيات الخبيثة تصلك عبر البريد الإلكتروني. المصدر: CSO (Online)

٧. ١٢٤$ مليار دولار هو الإنفاق العالمي في الأمن السيبراني حالياً. المصدر: (Cybersecurityventures)

٨. فقط ٥% من بيانات الشركات هي فعلاً محمية. المصدر: (Varonis)

٩. تتجه ٨٣% من الشركات هذا العام الى التخزين السحابي. المصدر: (Forbes)

١٠. في المتوسط، تحدث ٢,٢٤٤ هجمة إلكترونية يومياً. المصدر: University of (Maryland)

٢٠ حقيقة ربما لا تعرفها عن الأمن السيبراني

١١. في عام ٢٠١٦، تم سرقة بيانات ٣,٥ مليار حساب من شركة Yahoo في أكبر عملية اختراق على الإطلاق. المصدر: (NY Times)

١٢. في ٢٠١٧، برمجية وناكري Wannacry الشهيرة اصابت أكثر من ٤٠٠,٠٠٠ جهاز في أكثر من ١٥٠ دولة حول العالم وبخسائر وصلت لـ ٤ مليار دولار. المصدر: Technology (Inquirer)

١٣. كلف هجوم Wannacry على مؤسسة الرعاية الصحية ببريطانيا (NHS) أكثر من ١٠٠ مليون دولار. المصدر: (Datto)

١٤. يبلغ متوسط هجوم الفدية على الشركات ١٣٣,٠٠٠$. المصدر: (SafeAtLast)

١٥. ٩٠% من برمجيات التحكم عن بعد التي يزرعها الهاكر في جهاز الضحية، يستخدمها في تعدين العملات الرقمية. المصدر: (CSO Online)

٢٠ حقيقة ربما لا تعرفها عن الأمن السيبراني

١٦. ستتوفر ٣,٦ مليون وظيفة في الأمن السيبراني بحلول عام ٢٠٢٣. المصدر: (Cybersecurityventures)

١٧. في ٢٠٢١، كلفت الجرائم الإلكترونية الشركات حول العالم مجموع ٦٠٠$ مليار دولار. المصدر: (McAfee)

١٨. في ٢٠٢١، ١٥% من الشركات في المملكة المتحدة فقدت السيطرة على شبكاتها لصالح الهاكر. المصدر: (Cyber Security Breaches Survey)

١٩. من بين ٥٢% من الخروقات التي تمت، ٢٨% منها كانت عبر برمجية خبيثة، و٣٢%-٣٤% تمت عبر الهندسة الإجتماعية والتلاعب الفكري بالضحية. المصدر: (Verizon)

٢٠. بحلول نهاية عام ٢٠٢٢، سيزيد العدد التقديري لكلمات المرور المستخدمة من قبل البشر والآلات في جميع أنحاء العالم إلى ٣٠٠ مليار. المصدر: (Cybersecurity Media)

(..تحذيقة..)

قبل أن نبدأ....

فضلا ادخل على الرابط التالي:

https://haveibeenpwned.com/

مصطلحات وتعريفات

السيبرانية

- مأخوذة من كلمة (سيبر) Cyber،وتعني صفة لأي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي.
- فالسيبرانية، تعني : (فضاء الانترنت)

تعريب مصطلح cyber security

المصطلح الأول: الأمن الحاسوبي.
المصطلح الثاني: الأمن الرقمي
المصطلح الثالث : الأمن السَّبْراني
المصطلح الرابع : الأمن المعلوماتي

الامن السيبراني

جهد مستمر لحماية أنظمة الشبكة المتصلة بالإنترنت لحماية جميع البيانات من الاستخدام غير المصرح به أو الذي يسبب الضرر

أمن المعلومات على أجهزة وشبكات الحاسب الآلي، والعمليات والآليات التي يتم من خلالها حماية معدات الحاسب الآلي والمعلومات والخدمات من أي تدخل غير مقصود أو غير مصرّح به أو تغيير أو اختلاف قد يحدث

حيث يتم استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به ومنع سوء الاستغلال واستعادة المعلومات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها

الأمن السيبراني

هو المجال الجديد الخامس للحروب الحديثة بعد البر والبحر والجو والفضاء الحقيقي.

الأمن السيبراني

هـــو المجـــال الجديـــد الخامـــس للحروب الحديثـــة بعد البر والبحر والجـــو والفضاء الحقيقي

وهو يمثل جميع شـــبكات الحاســـب الالي الموجودة حول العالم

ويشـــمل ذلك الاجهزة الالكترونية المرتبطة من خلال شـــبكة الالياف البصرية

والشـــبكات اللاســـلكية الفضاء السيبراني

ليس الإنترنت فقط وانما شبكات اخرى كثيرة متصلة

يتضح من هذا

الفضاء السيبراني مجال عملياتي يعتبر الميدان الخامس للحروب الحديثة بعد ميدان الحرب البرية والجوية والبحرية والفضائية

البنى التحتية لأنظمة الاتصالات وتقنية المعلومات جزء أساسي من الفضاء السيبراني

الفضاء السيبراني لايقتصر على شبكة الإنترنت فقط
وانما شبكات عالمية وخاصة أخرى مثل : gps / Acars / Swift / Gsm / pstn

الفضاء السيبراني

مجال عالمي داخل البيئة المعلوماتية، يتكون من شبكة مستقلة من البنى التحتية لأنظمة المعلومات.

استخدام الفضاء السيبراني للدفاع أو الهجوم على المعلومات وشبكات الحاسب الآلي وحرمان العدو من تنفيذ نفس المقدرات

الجرائم السيبرانية

هي السلوك غير المشروع أو المنافي للأخلاق أو غير المسموح به المرتبط بالشبكات المعلوماتية العالمية

الحرب السيبرانية (الرقمية)

هو سلاح استراتيجي بيد الحكومات والأفراد، لا سيما أن الحرب السيبرانية أصبحت جزءًا لا يتجزأ من الأساليب الحديثة للحروب والهجمات بين الدول.

الأمن السيبراني

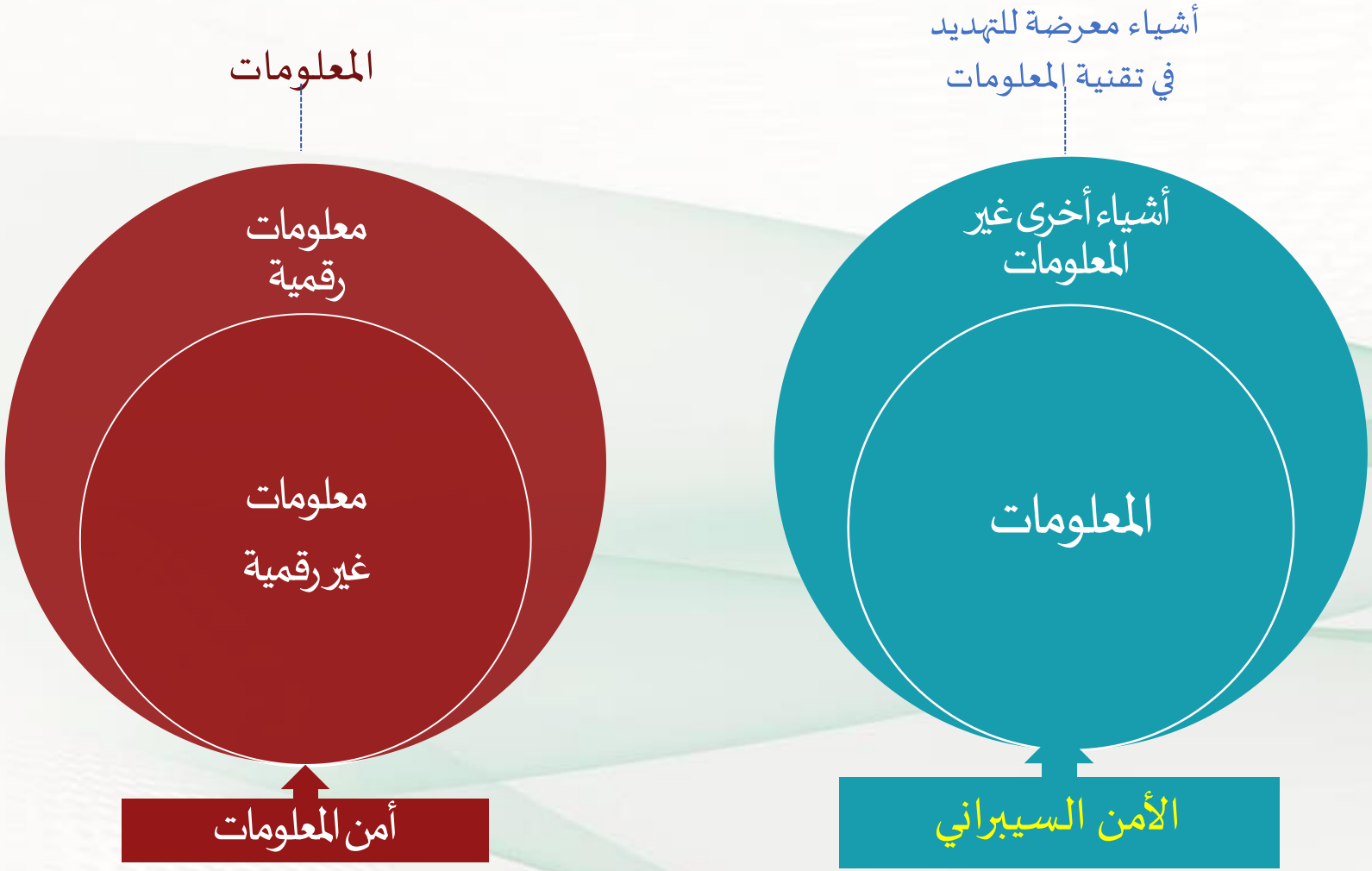
الفرق بين أمن المعلومات والأمن السيبراني

أمن المعلومات يهدف إلى:

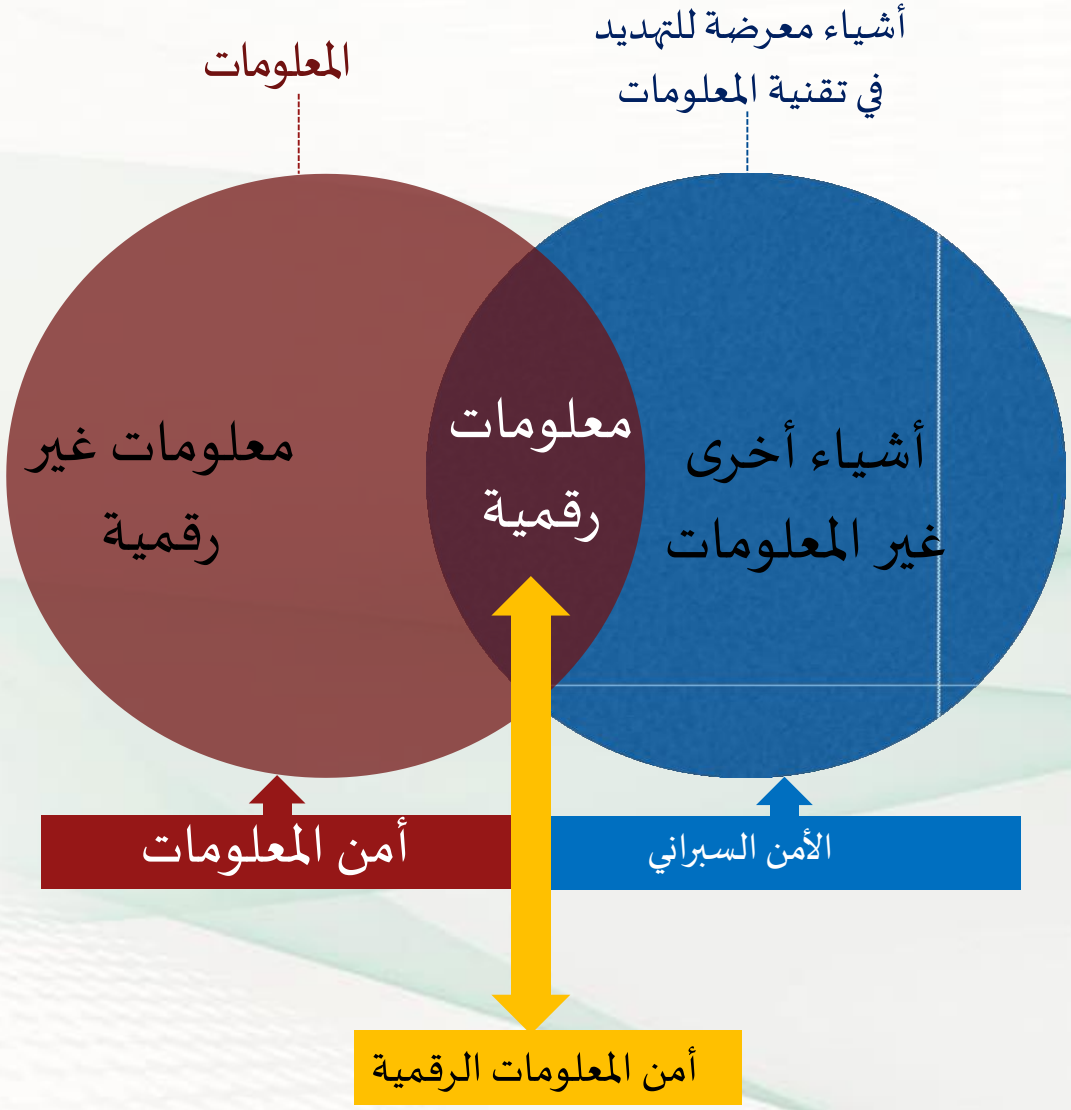
حماية الأنظمة الحاسوبية من الوصول غير الشرعي لها، أو العبث بالمعلومات أثناء التخزين أو المعالجة أو النقل:

- يهدف إلى الحماية ضد تعطيل خدمة المستخدمين الشرعيين
- يعنى بالوسائل الضرورية لاكتشاف وتوثيق وصد كل هذه التهديدات
- أمن المعلومات يشمل كل ما من شأنه حماية (المعلومة) التي قد تكون في نظام حاسوبي أو قد لا تكون كذلك
- أمن المعلومات المظلة الكبرى التي تغطي كل الأفرع الأخرى المرتبطة بحماية البيانات والمعلومات وتأمينها
- أمن المعلومات يهتم بمجالات ضخمة، كالتشفير، والتخزين، والتأمين الفيزيائي، والمعايير الأمنية، وإدارة أمن المعلومات والمخاطر..

أمن المعلومات والأمن السيبراني



أمن المعلومات والأمن السيبراني



الفرق بين أمن المعلومات والأمن السيبراني

الأمن السيبراني يأخذ في عين الاعتبار أيضا حماية مواقع تخزين البيانات والتقنيات المستخدمة لتأمينها.

الأمن السيبراني يتعلق بتأمين الأشياء المعرضة للخطر من خلال تكنولوجيا المعلومات والاتصالات"	" أمن المعلومات هو كل شيء عن حماية المعلومات ، التي تركز بشكل عام على سرية وسلامة وتوافر المعلومات"

فأمن المعلومات والأمن السيبراني هما مصطلحان متشابهان، لكنهما ليسا متطابقَين

أمن المعلومات بالتعريف هو أعم وأوسع من الأمن السيبراني

لعل التخصيص هنا بالتركيز على مجال الأمن السيبراني، بوصفه مجالًا من مجالات العلم، هو أمر مفيد جدًّا؛

فعلم الحاسب وعلم التشفير - مثلًا- اشتُقَّا أول ما اشتُقَّا من علم الرياضيات التطبيقية لأهميتهما، ثم ما لبثت هذه المجالات العلمية أن حلقت في فضاء العلم الرحب؛ لتتمدد، وتتوسع، وتخرج خارج الأطر العلمية لمجالها الأب. وهو الأمر ذاته لمجال الأمن السيبراني

أمن المعلومات والأمن السيبراني

الأمن السيبراني

القدرة على الدفاع أو حماية الفضاء السيبراني (الالكتروني) من الهجمات السيبرانية.

أمن المعلومات

حماية نظم المعلومات والمعلومات من الوصول أو الاستخدام غير المصرح به أو التسريب أو التخريب أو التعديل أو التدمير وضمان توفير السرية والنزاهة والتوافر.

أهداف الأمن السيبراني

أهداف الأمن السيبراني

- ضمان توافر استمرارية عمل نظم المعلومات
- تعزيز حماية وسرية وخصوصية البيانات الشخصية
- اتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين على حدٍ سواء من المخاطر المحتملة في مجالات استخدام الإنترنت المختلفة
- حماية الأنظمة التشغيلية من أي محاولات للولوج بشكل غير مسموح به لأهداف غير سليمة
- التأسيس لصناعة وطنية في مجال الأمن السيبراني تحقق للمملكة الريادة في هذا المجال
- تعزيز حماية أنظمة تقنية المعلومات

يتبع أهداف الأمن السيبراني

- تعزيز حماية أنظمة تقنية المعلومات
- أن تكون المرجع الوطني للمملكة في شؤون تخصصها
- حماية مصالح المملكة الحيوية وأمنها الوطني، والبنى التحتية الحساسة فيها
- تعزيز حماية أنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات
- مراعاة الأهمية الحيوية المتزايدة لتخصصها
- تعزيز حماية الشبكات

لماذا نحتاج الامن السيبراني؟

أهمية الأمن السيبراني

91٪ يقوم ممن يمتلكون أجهزة ذكية حول العالم بإتمام مُعاملات مالية أو عمليات شراء وتسوق عبر الإنترنت

%87 يستخدم من البشر المُتصلون بالإنترنت شبكات التواصل

25% يحتفظ من المُستخدمين بكلمات المرور الخاصة بحساباتهم الشخصية وحساباتهم البنكية على هواتفهم الذكية أو حاسباتهم

%65 تزايد نسبة من يحتفظون بصورهم الشخصية على هواتفهم الذكية أو أجهزتهم اللوحية

%72 نسبة من الاختراقات الإلكترونية ناجمة من الاخطاء البشرية

أهمية الأمن السيبراني

خسائر اقتصادية

متوسط تكلفة خرق البيانات في عام ٢٠٢١
يتجاوز ١٥٠ مليون دولار

في عام ٢٠٢١ تمكن المخترقون من سرقة نصف مليار من السجلات الشخصية

٧٦ مليار دولار من الأنشطة غير المشروعة تعتمد على بيتكوين

أهمية الأمن السيبراني

- وظائف الأمن السيبراني في جميع أنحاء العالم وصلت إلى ٣,٥ مليون عام ٢٠٢٢
- المتوقع أن يتم إنفاق ٦ تريليونات دولار تقريبًا على مستوى العالم على الأمن السيبراني بحلول عام ٢٠٢٣
- ٣٠٠ مليار دولار سوق الأمن السيبراني
- في عام ٢٠٢٢ هناك ما يقرب من ٢٠٠ مليار جهاز متصل
- أكثر من ٧٧ ٪ من المؤسسات ليس لديها خطة للاستجابة لحوادث الأمن السيبراني
- تستغرق معظم الشركات حوالي ٦ أشهر للكشف عن خرق البيانات ، حتى الشركات الكبرى
- تبلغ ميزانية الأمن السيبراني في الولايات المتحدة ١٤,٩٨ مليار دولار

إحصائية

عدد المستخدمين في ا لمملكة العربية السعودية