وزارة الاعمار والاسكان والبلديات العامة

الفصل الاول لسنة ٢٠٢٦

النشرة الالكترونية

العدد
١٠٠

- تقنيات تغير شكل مستقبل الحواسيب والتقنيات المحمولة
- فتح الحسابات المغلقة والمحظورة في ويندوز ١١
- استرجاع الملفات المصابة بفيروس من القرص الصلب او الفلاش USB او من بطاقة SD
- code Review اداة ذكاء اصطناعي جديدة من انثروبيك للتدقيق البرمجي
- الامن السيبراني
- التزييف العميق بغزو الانترنت
- التواصل الاجتماعي وتركيز الاطفال
- مستقبل نظم المعلومات الجغرافية والذكاء الاصطناعي

مركز نظم المعلومات

موقع الوزارة

WWW.Moch.gov.iq

Cois@moch.gov.iq

فريق النشرة

المشرف العام

المهندس

عمر محمد صالح

مدير مركز نظم للمعلومات

فريق المصادقة

عمار عبد الامير عبد السادة

عائدة عمران

محمد عبد اللطيف

لينا محمد عبد الوهاب

فريق التصميم

رشا جعفر

عائدة امير علوان

محمد عبد العزيز حيدر

محمد اسعد عبد الزهرة

ميسم هادي حسن

فتح الحسابات المغلقة والمحظورة في وندوز 11

تسجيل الدخول باستخدام حساب آخر في Windows 11
إذا كان لديك حسابات مستخدمين متعددة في نظام Windows 11 الخاص بك ، فإن تسجيل الدخول بحساب آخر يساعدك على استعادة الوصول. تتجاوز هذه الطريقة الحساب المقفل وتسمح لك باستكشاف المشكلة وإصلاحها بشكل فعال.
الخطوة الأولى. انقر فوق ارتباط خيارات "تسجيل الدخول" الموجود أسفل حقل كلمة المرور في شاشة تسجيل الدخول إلى Windows.
الخطوة 2. حدد خيار "مستخدم آخر". اضغط على Ctrl + Alt + Del في نفس الوقت ، ثم انقر على "تبديل المستخدم".
الخطوة 3. أدخل بيانات اعتماد الحساب البديل (اسم المستخدم وكلمة المرور) بامتيازات إدارية.
الخطوة 4. انقر على "السهم" أو اضغط على Enter لتسجيل الدخول بالحساب البديل. بمجرد تسجيل الدخول بنجاح ، يجب عليك استكشاف أخطاء الحساب المغلق وإصلاحه

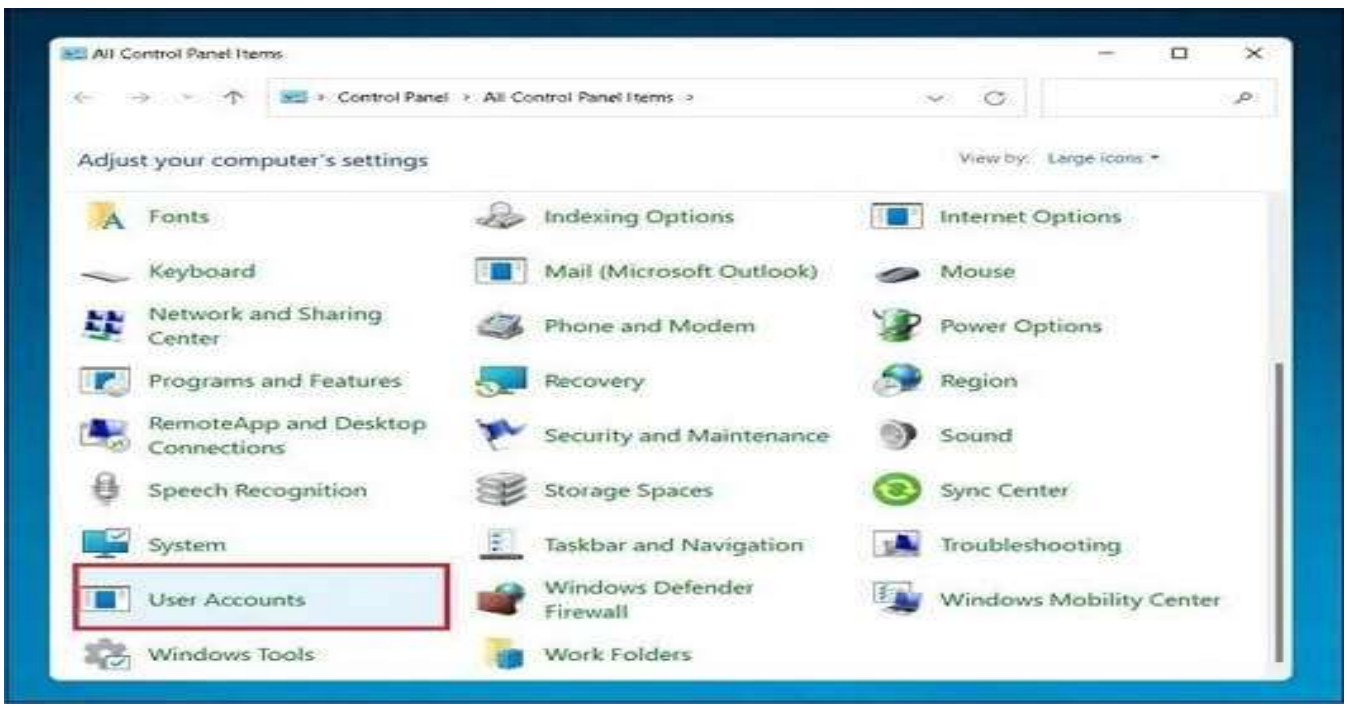
الخطوة 5. ادخل إلى "لوحة التحكم" وتابع "حسابات المستخدمين

الخطوة 6. اختر خيار "إدارة الحسابات".

الخطوة 7. حدد موقع الحساب المغلق وأعد تعيين كلمة المرور الخاصة به.

خطوة 8. تسجيل الخروج من حسابك الحالي ، والوصول إلى حسابك المقفل باستخدام كلمة المرور الجديدة.

تتيح لك هذه الطريقة تسجيل الدخول بحساب آخر واستعادة الوصول إلى Windows 11 الخاص بك.



او عن طريق إعادة تعيين كلمة مرور حساب Windows 11 الخاص بك

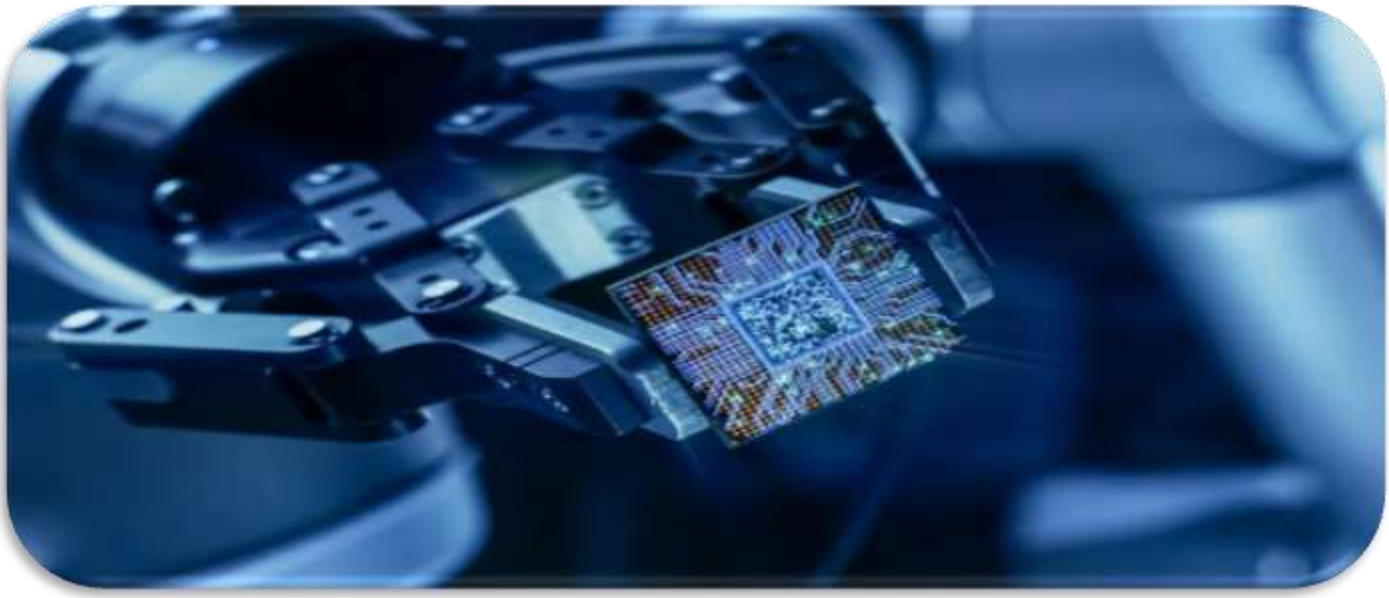
اذا قمت بتسجيل الدخول إلى Windows11 باستخدام حساب Microsoft ، فيمكنك إعادة تعيين كلمة المرور الخاصة بك عبر الإنترنت من خلال عملية استرداد حساب Microsoft.

الخطوة 1: على جهاز آخر ، قم بزيارة صفحة استرداد حساب مايكروسوف.

الخطوة 2: انقر فوق خيار "لقد نسيت كلمة المرور الخاصة بي" وانتقل إلى الشاشة التالية.

الخطوة3: أدخل عنوان البريد الإلكتروني المرتبط بحسابك المقفل وأكمل عملية التحقق الأمني.

3 تقنيات تغير شكل مستقبل الحواسيب والتقنيات المحمولة



شهدت السنوات الأخيرة ظهور تقنيات مبتكرة في قطاع الحواسيب والأجهزة المحمولة تؤثر في طريقة استخدامنا للتقنية يوميًا. ورغم أن الذكاء الاصطناعي استحوذ على الاهتمام مؤخرًا، فإن الشركات التقنية تواصل العمل على ابتكارات أخرى قد تغيّر شكل الأجهزة في المستقبل. هذه التقنيات ما تزال في مراحل التطوير وتُعد مفاهيم مستقبلية، لكن نجاحها قد يقود إلى نقلة كبيرة تجعل الأجهزة أقرب إلى ما نشاهده في الخيال العلمي.

من أبرز هذه الاتجاهات تطور منصات الحواسيب المحمولة، حيث لم يعد الأداء القوي مرتبطًا بالحجم الكبير كما كان في الماضي. فقد أصبحت الأجهزة الصغيرة قادرة على تقديم أداء قوي ينافس الحواسيب المكتبية. ويظهر ذلك في منصات الألعاب المحمولة الحديثة والحواسيب المتنقلة التي تجمع بين الحجم الصغير والأداء العالي، مما يجعلها مناسبة للاستخدام أثناء التنقل دون التضحية بالقوة.

كما تمثل الحواسيب المحمولة التي تعمل بمعمارية ARM مثالًا واضحًا على هذا التوجه، إذ تقدم أداءً قويًا مع استهلاك أقل للطاقة وحرارة أقل. وقد أثبتت هذه الأجهزة قدرتها على تنفيذ المهام الثقيلة مثل البرمجة وتحرير الفيديو، مما دفع العديد من الشركات إلى تطوير معالجات ومنصات مشابهة لمنافسة الحواسيب التقليدية.

إلى جانب ذلك، يجري تطوير بطاريات سيليكات الكربون التي توفر سعات طاقة أكبر وسرعات شحن أعلى مقارنة بالبطاريات التقليدية. هذه التقنية قد تساعد في حل مشكلة استهلاك الطاقة في الحواسيب والأجهزة المحمولة، إذ يمكنها تقديم بطاريات بسعة كبيرة في أحجام صغيرة، مما يسمح بتشغيل الأجهزة لفترات أطول دون زيادة الحجم.

ومن التقنيات المستقبلية الأخرى الشاشات القابلة للتمدد، التي قد تمثل المرحلة التالية بعد الشاشات القابلة للطي. تسمح هذه التقنية بزيادة حجم الشاشة عند الحاجة دون زيادة حجم الجهاز نفسه، مما يوفر تجربة استخدام أكثر مرونة. وقد عرضت بعض الشركات نماذج أولية لحواسيب بشاشات قابلة للتوسع يمكنها زيادة حجم الشاشة بشكل ملحوظ بضغطة زر.

ورغم أن هذه الابتكارات ما تزال في مراحلها الأولى، فإنها تشير إلى مستقبل قد يشهد تطورًا كبيرًا في تصميم الحواسيب والأجهزة المحمولة، حيث تجمع الأجهزة بين الأداء القوي والحجم الصغير والمرونة في الاستخدام.

محمد عبد العزيز حيدر
مركز نظم المعلومات

كيفية حماية المواقع الالكترونية وتطبيقات الويب من الاختراق

الإستضافة (Hosting)

1. التأكد من اختيار شركة استضافة مواقع موثوقة :

من أهم عوامل تحقيق أمن المواقع هو اختيار شركة استضافة مواقع موثوقة ورصينة اذ يجب أن يكون لشركة الاستضافة سمعة في مجال الإستضافة ولها عامل كبير ومهم فى حماية وامن الموقع الالكتروني.

مثال : Hostinger, GoDaddy

SSL

2. شهادات امان المواقع : SSL

لا تهُمل ابداً إستخدام شهادات أمن المواقع فهى تُمكنك من تشفير بيانات موقعك على المتصفح مما يزيد من أمن المواقع, تكون باضافة بروتوكول https لبداية رابط وعنوان موقعك. يتم الحصول على هذه الشهادة من شركة الإستضافة.

Monitoring

3. الملاحظة والمتابعة اليومية لموقعك :

من ضمن طرق امن المواقع وحمايتها من الاختراق القيام بالمتابعة اليومية للموقع وملاحظة اي تغيرات تطرأ عليه, فمجرد ظهور اي تعديلات او ظهور نوافذ منبثقة على سبيل المثال يجب الانتباه فوراً.

Strong Password

4. اختيار كلمة مرور قوية وصعبة التخمين :

لا تستهين باختيار كلمة المرور بعناية , سواء كلمة المرور الخاصة ببيانات الاستضافة أو كلمة مرور لوحة تحكم موقعك, حاول اختيار كلمة مرور تشمل حروف وارقام صعب تخمينها, ولا تجعل بيانات حسابك الخاص على موقعك متداول بين اشخاص كثيرة من فريق العمل حتى لا يكون عرضه للاختراق.

Website Backup

5 - أخذ نسخ احتياطية باستمرار وبشكل دوري :

يعتبر اخذ نسخ احتياطية للموقع بشكل دوري ضمن أهم طرق لأمن المواقع, حيث يمكنك من خلال اخذ النسخ الإحتياطية استعادة نسخة موقعك مرة اخرى في حالة حدوث اي اختراق الكتروني أو حتى في حالة حدوث فقد بيانات مثل تعطل الاستضافة او نقلها لشركة استضافة أخرى فهذه الطريقة تُجنبك فقد بيانات موقعك او اختراقه .

Updates

6. القيام بعمل اي تحديثات جديدة بشكل دوري :

تقوم شركات البرمجيات بإصدار التحديثات لمعالجة اي ثغرات او اخطاء برمجية واردة بالنسخ الاقدم , ويجب عدم إهمال هذه التحديثات وقم بها باستمرار لتجنب اي ثغرات تخص أمن المواقع ومنعاً لاختراق موقعك او مدونتك.

رشا جعفر
مركز نظم المعلومات

مستقبل نظم المعلومات الجغرافية والذكاء الاصطناعي

مستقبل نظم المعلومات الجغرافية (GIS)يتجه نحو دمج الذكاء الاصطناعي، الحوسبة السحابية، وإنترنت الأشياء (IoT) لتحليل البيانات المكانية في الوقت الفعلي .سيشهد المستقبل اعتمادًا أوسع على الطائرات المسيرة، تحليل البيانات الضخمة، والواقع المعزز (AR) لدعم اتخاذ القرارات الذكية في المدن الذكية، الإدارة البيئية، واللوجستيات .

\

أبرز اتجاهات مستقبل نظم المعلومات الجغرافية:

- الذكاء الاصطناعي والتعلم الآلي : دمج الذكاء الاصطناعي لأتمتة المهام الروتينية، وتحليل صور الأقمار الصناعية، وتحسين النمذجة المناخية.
- إنترنت الأشياء والوقت الفعلي :استخدام حساسات متصلة بإنترنت الأشياء (IoT)لتحليل البيانات البيئية وحركة المرور فورياً.
- الحوسبة السحابية والبيانات الضخمة:

توفير تطبيقات GIS سحابية تتيح الوصول للبيانات والتحليلات من أي مكان،مما يسهل العمل الميداني والتعاون.

- التقنيات المكانية المتقدمة
- توسع استخدام الطائرات المسيّرة (Drones) والليدار (LiDAR) لجمع بيانات دقيقة، والواقع المعزز (AR) لتصور البنية التحتية.
- المدن الذكية والنمذجة ثلاثية الأبعاد :اعتماد شامل لـ GIS في التخطيط الحضري وإدارة المرافق والخدمات .

عايدة امير علوان/مدير
مركز نظم المعلومات

التزييف العميق يغزو الإنترنت: الاحتيال يزداد 20 ضعفاً في 3 سنوات

أفاد تحليل نشره خبراء في الذكاء الاصطناعي أن عمليات الاحتيال بتقنية التزييف العميق، التي تستخدم الذكاء الاصطناعي، قد أصبحت على نطاق "صناعي".

وذكر التحليل أن الأدوات التي تتيح ابتكار عمليات احتيال مخصصة، وحتى شخصية، مثل استخدام مقاطع فيديو مزيفة، لم تعد مقتصرة على فئة محدودة،بل أصبحت رخيصة الثمن وسهلة الاستخدام على نطاق واسع، بحسب قاعدة بيانات حوادث الذكاء الاصطناعي.

ووثق التحليل أكثر من اثنتي عشرة حالة حديثة من "انتحال الشخصية لتحقيق الربح"، وأطباء مُزيفين بتقنية التزييف العميق يروجون لكريمات للبشرة، بحسب تقرير لصحيفة "ذا غارديان البريطانية، اطلعت عليه "العربية .Business".

تُعد هذه الأمثلة جزءًا من اتجاهٍ يستخدم فيه المحتالون أدوات الذكاء الاصطناعي المتاحة على نطاق واسع لتنفيذ عمليات احتيال متزايدة الاستهداف. وقال سايمون ميليوس، الباحث في معهد ماساتشوستس للتكنولوجيا والذي يعمل على مشروع مرتبط بقاعدة بيانات حوادث الذكاء الاصطناعي: "لقد وصلت القدرات فجأة إلى مستوى يسمح لأي شخص تقريبًا بإنتاج محتوى مزيف".

رشا جعفر
مركز نظم المعلومات

استرجاع الملفات المصابة بفيروس من القرص الصلب او الفلاش USB أو من بطاقة SD

,استخدام CMD لاسترجاع الملفات المصابة بالفيروس من على وحدة تخزين عند فقدان ملفاتك أو تعذر الوصول إليها نتيجة هجوم فيروس، يصبح الحل الأفضل أمامك هو أن تحاول استخدام واجهة الأوامر CMD لاسترجاع الملفات المصابة بالفيروس، وتعد واجهة CMD حل ممتاز لكونها أداة مجانية وسهلة الاستخدام، والآن لنرى كيف تعمل (سأستخدم ويندوز 7 لشرح هذه العملية والتي تصلح مع أي نظام تشغيل ويندوز):,

1. قم بتوصيل قرصك الصلب أو بطاقة الذاكرة أو الفلاش USB الخاص بك مع الكومبيوتر.

2.توجه إلى قائمة ابدأ الخاصة بك (زر شعار الويندوز) وقم بكتابة CMD في مربع البحث ثم اضغط على زر Enter وسترى بعدها ملف يدعى cmd.exe تحت قائمة البرامج.

3.اضغط على cmd.exe، وسينقلك هذا إلى نافذة واجهة الأوامر التي ستمكنك من كتابة الأمر الذي سيعيد لك ملفاتك المصابة بالفيروس.

قم بكتابة الأمر " chkdsk E: /f" واستبدل حرف E برمز القرص المصاب الخاص بك.

اكتب Yثم اضغط على .Enter

اكتب E ثم اضغط Enter استبدل حرف E برمز القرص المصاب.

اكتب الأمر التالي: attrib -h -r -s /s /d *.* ثم اضغط .Enter

سيبدأ بعدها الويندوز في عملية إصلاح الملفات المصابة على القرص الصلب أو بطاقة الذاكرة أو الفلاش USB ويستغرق هذا الأمر عادة من دقيقة إلى دقيقتين لإنهاء عملية الإصلاح، لذا يمكنك الانتظار قليلا، وبعد انتهاء عملية الإصلاح، توجه إلى مكان الملفات المصابة لتتأكد إذا كانت قد عادت أم لا.

ميسم هادي حسن
مركز نظم المعلومات

احذروا رسائل الاحتيال باسم “ "META على فيسبوك

في الآونة الأخيرة انتشرت رسائل مزيفة تُرسل إلى أصحاب الصفحات على فيسبوك، تحمل اسم "Meta " أو "تقرير الصفحة"، وتزعم أنّ صفحتك قد ارتكبت مخالفات مثل انتهاك حقوق الطبع أو استخدام صور بالذكاء الاصطناعي.

هذه الرسائل غالبًا ما تحتوي على رابط خارجي غريب (ليس تابعًا لـ facebook.com أو meta.com) وتطالبك بالضغط عليه لتصحيح الوضع أو تقديم إشعار مضاد.

⚠ الحقيقة: هذه مجرد محاولة احتيال (Phishing) تهدف إلى سرقة بيانات حسابك (البريد الإلكتروني وكلمة المرور)، ومن ثم السيطرة على صفحتك أو حسابك الشخصي.

✨ كيف تميّز الرسالة المزيفة؟

استخدام لغة التخويف والتهديد بغلق الصفحة.

وجود رابط خارجي غير رسمي.

أخطاء لغوية وصياغة غير مهنية.

طلب إدخال بياناتك في موقع غير تابع لفيسبوك.

✔ ماذا تفعل إذا وصلتك رسالة مشابهة؟

1. لا تضغط على أي رابط خارجي.
2. لا تدخل بياناتك إطلاقًا خارج موقع فيسبوك الرسمي
3. فعّل المصادقة الثنائية (2FA) لحماية حسابك.
4. أبلغ عن الرسالة كـ"احتيال".

🔒 وفي الاخير :

فيسبوك أو Meta لا يرسلان روابط خارجية لإدارة الانتهاكات. كل التنبيهات الرسمية ستجدها فقط داخل إعدادات حسابك أو مركز الدعم على فيسبوك.

رشا جعفر
مركز نظم المعلومات

Code Review أداة ذكاء اصطناعي جديدة من أنثروبيك للتدقيق البرمجي

أعلنت شركة Anthropic عن إضافة أداة جديدة إلى مساعدها البرمجي Claude Code باسم Code Review، وتهدف هذه الأداة إلى مساعدة المطورين في اكتشاف الأخطاء البرمجية ومعالجتها قبل دمج التعديلات في المشاريع البرمجية. تقوم الأداة بتحليل التغييرات في الشفرة تلقائيًا عند فتح طلب دمج Pull Request، حيث يستخدم النظام مجموعة من الوكلاء الأذكياء لفحص الأكواد بالتوازي. بعد ذلك يتم التحقق من الأخطاء المكتشفة لتقليل الإنذارات الخاطئة، ثم ترتيبها حسب مستوى الخطورة، ويعرض النظام النتائج في تعليق شامل داخل طلب الدمج مع ملاحظات مباشرة على الأسطر التي تحتوي على أخطاء.

يعتمد النظام على آلية مراجعة متعددة الوكلاء تتكيف مع حجم وتعقيد التعديلات البرمجية؛ إذ يتم تخصيص عدد أكبر من الوكلاء لتحليل التغييرات الكبيرة والمعقدة، بينما تكتفي التحديثات الصغيرة بمراجعة أخف. وتشير اختبارات الشركة إلى أن مراجعة طلب دمج متوسط الحجم تستغرق عادةً حوالي 20 دقيقة. وجاء تطوير هذه الميزة بعد ملاحظة ارتفاع حجم الشفرات البرمجية التي ينتجها المهندسون بنسبة تقارب 200% خلال العام الماضي نتيجة الاعتماد المتزايد على أدوات الذكاء الاصطناعي في البرمجة.

وتستخدم الشركة الأداة حاليًا في معظم طلبات الدمج داخلها، وقد سجلت تحسنًا ملحوظًا في جودة المراجعة التقنية. وبعد نجاح الاختبارات الداخلية بدأت Anthropic طرح الميزة بشكل تجريبي لمشتركي خطط Claude for Teams و.Claude Enterprise وتعتمد الأداة على نظام تسعير قائم على استهلاك الرموز البرمجية Tokens، حيث تتراوح تكلفة مراجعة الشفرة عادة بين 15 و25 دولارًا لكل طلب دمج حسب حجم التعديلات وتعقيدها. وتأتي هذه الخطوة في ظل المنافسة المتزايدة مع شركات مثل OpenAI و Google في تطوير أدوات الذكاء الاصطناعي الموجهة للمطورين.

محمد عبد العزيز حيدر
مركز نظم المعلومات

المهارات المطلوبة لمهندس الإيعازات:

المهارة	الوصف
التفكير التحليلي	فهم ما يريده المستخدم بدقة
إتقان اللغة	استخدام لغة واضحة ومناسبة للنموذج
التجريب والتحسين	اختبار أكثر من صيغة وتحليل النتائج
فهم النموذج المستخدم	معرفة حدود وإمكانات النموذج مثل GPT-4، Claude، Gemini
التدرّج في التوجيه	البدء البسيط ثم التطوير بناءً على المخرجات

تحديات الذكاء الاصطناعي:

1 - غموض النتائج: الذكاء الاصطناعي قد يقدم مخرجات غير متوقعة إن كان الإيعاز غير دقيق.

2 - التحيّز: بعض النماذج قد تحمل تحيزاً بناءً على بيانات التدريب.

3 - عدم الاتساق: يمكن أن تختلف المخرجات لنفس الإيعاز في كل مرة.

4 - عدد اللغات والثقافات: تحتاج الإيعازات إلى تخصيص حسب اللغة والسياق المحلي.

مستقبل هندسة الإيعازات

- من المتوقع أن تصبح هندسة الإيعازات مهارة أساسية في سوق العمل الرقمي بحلول عام 2030.
- ظهور أدوات تدعم توليد الإيعازات تلقائياً بناءً على أهداف المستخدم.
- دمج هندسة الإيعازات في المناهج التعليمية والتدريبية لتخصصات الإدارة، الإعلام، والتعليم.

التوصيات

1 إنشاء وحدات تدريبية للعاملين في المؤسسات حول هندسة الإيعازات.
2 دمج الهندسة في المناهج الجامعية المرتبطة بالتقنية والإدارة.
3 التجريب الدوري لتحسين صياغة الإيعازات في فرق العمل.
4 توظيف هندسة الإيعازات ضمن أنظمة تخطيط الموارد المؤسسية (.ERP)
5 اعتماد أدوات تحليل جودة الإيعاز والمخرجات لتحقيق كفاءة أعلى.

ومن خلال رصد التطبيقات العملية، ثبت أن تحسين هندسة الإيعازات يمكن أن يؤدي إلى:

- زيادة كفاءة الإنتاجية بنسبة قد تتجاوز 25–40٪ في بعض القطاعات.
- تقليص الوقت الضائع في التجريب العشوائي أو إعادة الصياغة.
- تعزيز جودة النتائج وتحقيق أهداف المستخدم بدقة أعلى.
- تمكين الموظفين والمستخدمين غير التقنيين من التعامل بسلاسة مع أدوات الذكاء الاصطناعي دون الحاجة إلى برمجة.

في المقابل، تبرز تحديات جوهرية مثل التحيّز الخوارزمي، الحاجة إلى التدريب المستمر، وتعدد اللغات والسياقات الثقافية، مما يفرض على المؤسسات التعليمية، والتقنية، والإدارية إعادة النظر في برامجها التدريبية، ومناهجها الجامعية، وأنظمتها التقنية لتشمل هذا المفهوم المحوري.

وفي الخلاصة النهائية إن هندسة الإيعازات ليست مجرد مهارة مستقبلية، بل هي ضرورة حاضرة؛ وستمثّل العمود الفقري لجميع التفاعلات الذكية بين الإنسان والآلة وكلما ازداد ذكاء النماذج الاصطناعية، زادت الحاجة إلى ذكاء البشر في توجيهها.

ايات اركان محمد
وسل صالح مهدي
مركز نظم المعلومات

دراسة:وسائل التواصل الاجتماعي و تركيز الأطفال

دراسة دولية تابعت أكثر من 8,000 طفل أمريكي بين 9 و10 سنوات على مدى 4 سنوات، خرجت بالآتي:

- **الأطفال الذين زاد استخدامهم لوسائل التواصل الاجتماعي من نصف ساعة إلى ساعتين ونصف يوميًا كانوا أكثر عرضة لتراجع التركيز وظهور أعراض تشتت الانتباه ADHD).)**
- **هذا التأثير لم يُلاحظ بنفس الدرجة مع مشاهدة التلفزيون أو ألعاب الفيديو.**
- **الإشعارات والرسائل المتكررة تشتت ذهن الأطفال حتى دون استخدام المنصات بشكل مباشر.**
- **زيادة أعراض التشتت ارتبطت مباشرة بارتفاع استهلاك الشبكات الاجتماعية، دون تأثير واضح على فرط الحركة.**
- **الباحثون دعوا لمراجعة عادات الأطفال الرقمية وتحديد حدود واضحة للاستخدام اليومي حفاظًا على الصحة الذهنية للأجيال القادمة.**

رشا جعفر
مركز نظم المعلومات

الإمارات تطلق أول صراف آلي ذكي للذهب في العالم

أعلنت Emirates Gold، بالتعاون مع Public Gold الماليزية، عن تدشين أول صراف آلي ذكي للذهب بالإمارات.

- أُطلق أول جهاز في برج الماس بدبي، مع خطة لنشر 35-40 جهاز إضافي في أنحاء الدولة خلال 2026.
- الأجهزة تتيح شراء أكثر من 70 تصميم من سبائك الذهب والفضة على مدار الساعة، مع دعم الدفع الإلكتروني وبطاقات الائتمان وسحب السبائك فعليًا.
- الصرافات الذكية تدمج الدفع الرقمي، وتوزيع السبائك، وأنظمة أمان متقدمة في منصة واحدة.

تخطط الشركة لإضافة ميزات مستقبلية مثل التحويل بالعملات الرقمية والاستلام عبر الإنترنت.

رشا جعفر
مركز نظم المعلومات

اقام المركز الوطني لادارة البيانات المكانية ومستشارية الامن القومي المؤتمر الدولي الخامس لتقنيات الجيومكانية والمدن الذكية من (7-9/شباط/ 2026) وتم حضور مدير قسم المعلومات الجغرافية (GIS) في مركز نظم المعلومات السيد محمد عبد اللطيف وتقديم ورقة بحث حول انجازات الوزارة في بوابة العراق الجغرافية (نظام متابعة وادارة المشاريع فنياً ومكانياً) .

ورشة عمل (السياسة الوطنية لامن ومشاركة المعلومات وحماية الاتصالات)

نظم مركز التدريب والتطوير بالتعاون مع شركة آشور العامة للمقاولات الانشائية ورشة عمل بعنوان (السياسة الوطنية لامن ومشاركة المعلومات وحماية الاتصالات)

- أقيمت الورشة على قاعة الشركة اعلاه اليوم الثلاثاء الموافق ١٧/ ٣/ ٢٠٢٦ وبمشاركة عدد من الموظفين من الوزارة والتشكيلات التابعة لها.
- تم خلال الورشة مناقشة عدد من المحاور تضمنت ::

التعريف بوثيقة السياسة الوطنية لامن ومشاركة المعلومات وحماية الاتصالات.

الاطار القانوني للوثيقة.

المسؤوليات والادوار.

التوصيات والخلاصة.

- تهدف الورشة إلى ::

التوعية والارشاد للعاملين.

ضرورة تطبيق الوثيقة وسياساتها.

تأمين المعلومات ونظم المعلومات وحمايتها من الاخطار.

- محاضر الورشة :: ر. مبرمجين اقدم/ عباس صاحب عاجب

ورشة عمل (مبادئ استخدام الذكاء الاصطناعي)

نظم مركز التدريب والتطوير بالتعاون مع شركة آشور العامة للمقاولات الانشائية ورشة عمل بعنوان (مبادئ استخدام الذكاء الاصطناعي) .

- أقيمت الورشة على قاعة الشركة اعلاه اليوم الاربعاء الموافق ٢٥/ ٢/ ٢٠٢٦ وبمشاركة عدد من الموظفين من الوزارة والتشكيلات التابعة لها.
- تم خلال الورشة مناقشة عدد من المحاور تضمنت ::

تعريف الذكاء الاصطناعي.

مراحل تطور الذكاء الاصطناعي.

كيف يعمل الذكاء الاصطناعي.

ايجابيات وسلبيات الذكاء الاصطناعي.

- الهدف من الورشة هو توعية المجتمع بضرورة استخدام الذكاء الاصطناعي في العصر الرقمي الحديث بالاضافة الى شرح اهم تطبيقات الذكاء الاصطناعي بشكل مبسط.
- محاضر الورشة :: ملاحظ / محمود نبيل ناجي

دورة تدريبية (تصميم المواقع الالكترونية)

نظم مركز التدريب والتطوير التابع لوزارة الإعمار والإسكان والبلديات والاشغال العامة دورة تدريبية بعنوان (تصميم المواقع الالكترونية)

- اقيمت الدورة على قاعة مبنى المركز للفترة من ٨_ ١٢ / ٢ / ٢٠٢٦ بمشاركة عدد من الموظفين من الوزارة والتشكيلات التابعة لها.
- اهم محاور الدورة التي تضمنت اهمها ::
  - مقدمة في تطوير الويب.
  - أساسيات HTML
  - نماذج الادخال ((Forms
  - أساسيات CSS
  - تنسيق واجهات احترافية.
  - مشاريع تطبيقية.
- تهدف الدورة الى ::

✳تمكين المتدرب من فهم اساسيات تطوير مواقع الويب وكيفية عملها بشكل صحيح ومنظم.

✳ اكتساب المتدرب القدرة على انشاء صفحات ويب باستخدام (HTML)باسلوب احترافي.

✳تعليم المتدرب تنسيق وتصميم صفحات الويب باستخدام CSS

✳فهم كيفية بناء تخطيطات الصفحات والتحكم في توزيع العناصر.

✳تمكين المتدرب من تصميم مواقع متجاوبة تعمل على مختلف احجام الشاشات.

✳ تعزيز مهارات كتابة كود نظيف ومنظم وقابل للتطوير.

✳تمكين المتدرب من نشر موقعه الالكتروني على الانترنت.

- محاضر الدورة :: مهندس اقدم / حسن عبد الهادي

دورة تدريبية الالتزام بالسياسة الوطنية لأمن ومشاركة المعلومات وحماية الاتصالات)

نظم مركز التدريب والتطوير بالتعاون مع دائرة بحوث البناء ورشة عمل بعنوان (الالتزام بالسياسة الوطنية لأمن ومشاركة المعلومات وحماية الاتصالات)

- أقيمت الورشة على القاعة الدائرة اعلاه اليوم الاربعاء الموافق ١١ / ٢/ ٢٠٢٦ بمشاركة عدد من الموظفين من الوزارة والتشكيلات التابعة لها.
- تم خلال الورشة مناقشة عدد من المحاور تضمنت ::
  - حماية الاموال المعلوماتية للدولة.
  - تعزيز الثقافة الرقمية.
  - تبادل البيانات والمعلومات بأمان من الجهات الحكومية.
  - سرية البيانات.
  - تصنيف البيانات والحد من القرصنة السيبرانية
  - تعزيز الاقتصاد الرقمي وحماية الخصوصية.
- تهدف الورشة الى ::
  - حماية البيانات.
  - تنظيم مشاركة البيانات.
  - الالتزام بالقوانين لحماية المعلومات.
  - تعزيز الكفاءة الرقمية ورفع مستوى الآمان السيبراني.
  - التوعية وادارة الحوادث السيبرانية واحتوائها.
- محاضر الورشة : ر. مبرمجين اقدم اول / عمار عادل عبد الرزاق

دورة تدريبية (برنامج الريفيت الانشائي Revit)

نظم مركز التدريب والتطوير التابع لوزارة الإعمار والإسكان والبلديات والاشغال العامة دورة تدريبية بعنوان (برنامج الريفيت الانشائي Revit)

- ❖ اقيمت الدورة على قاعة مبنى المركز للفترة من ١ _ ٥ / ٢ / ٢٠٢٦ بمشاركة عدد من الموظفين من الوزارة والتشكيلات التابعة لها.
- ❖ المحاور الرئيسية التي تضمنت منهاج الدورة ::
  - مقدمة شاملة عن تقنية الـ Bimوبرنامج Revit.
  - شرح واجهة المستخدم والتحكم في Project Browserو Properties.
  - ضبط بيئة المشروع وانشاء المحاور Gridوالمناسيب Levels.
  - استعراض قائمة Structureوالتعرف على الايعازات.
  - نمذجة الجدران الانشائية Structural Wallوايعازات الاعمدة وانواعها.
  - تطبيق عملي وربط الاعمدة بالجدران والاسس.
  - نمذجة الاساسيات Foundationوتطبيق عملي، والعمل على اوامر التعديل Modify Tools.
  - نمذجة الجسور Beamsونظم الجسور Beam Systems.
  - نمذجة الارضيات والاسقف الانشائية واقامة الابعاد والنصوص واخراج اللوحات.
- ❖ تهدف الدورة الى ::
  - اتقان اساسيات نمذجة معلومات البناء (.Bim)
  - بناء الهيكل الرقمي الانشائي المتكامل وانشاء نموذج انشائي D model.3
  - احتراف مهارات التعديل والضبط الهندسي من خلال استخدام ادوات Modify.
  - التمهيد لعمليات التصميم الانشائي والتحليل.
- ❖ محاضر الدورة :: مهندس اقدم/ كرار خليفة بدر

دورة تدريبية (الامن السيبراني)

نظم مركز التدريب والتطوير التابع لوزارة الإعمار والإسكان والبلديات والاشغال العامة دورة تدريبية بعنوان (الامن السيبراني)

- اقيمت الدورة على قاعة مبنى المركز للفترة من ٢٥_ ٢٩ / ١ / ٢٠٢٦ بمشاركة عدد من الموظفين من الوزارة والتشكيلات التابعة لها.
- اهم المحاور التي تضمنت اهمها ::
  - مقدمة تعريفية حول بيئة العالم الرقمي.
  - المخاطر التي تواجه العالم الرقمي.
  - الهجمات السيبرانية التي تواجه البيئة الرقمية للمؤسسات.
  - آليات واساليب الدفاع ضد الهجمات السيبرانية.
  - تنظيم بيئة رقمية مؤسسية مؤمنة.
- تهدف الدورة إلى ::
  - زيادة الوعي في التنظيم والاستخدام الآمن للانظمة والاجهزة.
  - تحويل كوادر تكنلوجيا المعلومات الى فرق استجابة أمنية.
  - الوصول الى بيئة رقمية مؤسسية مؤمنة وقادرة على التعامل مع الهجمات السيبرانية.
- محاضر الدورة :: م.ر. مهندسين/ سامر كاظم جواد

دورة تدريبية (برنامج قواعد البيانات Access)

نظم مركز التدريب والتطوير التابع لوزارة الاعمار والاسكان والبلديات العامة دورة تدريبية بعنوان (برنامج قواعد البيانات Access)

- أقيمت الدورة على قاعة مبنى المركز للفترة من ١٨ - ٢٢ / ١ / ٢٠٢٦ بمشاركة عدد من موظفي الوزارة والتشكيلات التابعة لها.
- اهم المحاور الرئيسية التي تضمنها منهاج الدورة ::

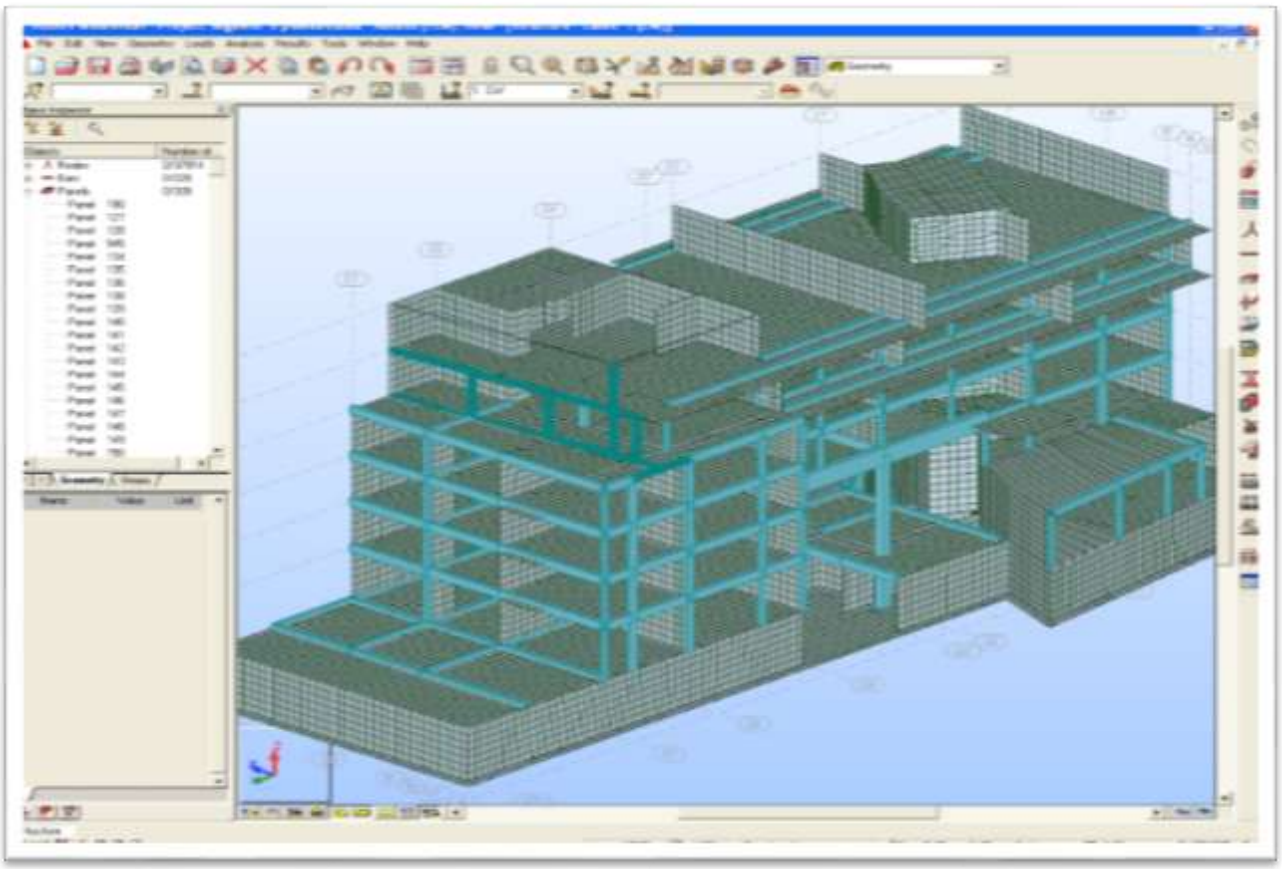
التعرف على قواعد البيانات وانواعها .

- انشاء الجداول والحقول .
- انشاء القوائم المنسدلة وتحديد نمط وقواعد ادخال البيانات .
- استيراد البيانات من ملفات الاكسل.
- اجراء عملية البحث والتصفية والحسابات.
- انشاء الاستمارات التي تسهل عملية ادخال البيانات.

- الهدف من الدورة هو تمكين المشاركين من التعامل مع قواعد البيانات وانشاء الجداول والاستمارات وتحديد المستخدمين بادخال البيانات من خلال القوائم المنسدلة وقواعد وانماط ادخال البيانات .
- محاضر الدورة :: ر . مهندسين / نصر سعد عليوي

دورة تدريبية (البرنامج الانشائي Robot)

نظم مركز التدريب والتطوير دورة تدريبية الكترونية على تطبيق ZOOM بعنوان (البرنامج الانشائي Robot) للفترة من 8 - 12 / 2/ 2026 القى فيها المحاضرات حازم عبد إبراهيم / رئيس مهندسين اقدم .



دورة تدريبية (AUTO CAD)

نظـم مركـز التـدريب والتطـوير دورة تدريبيــة الكترونيــة علــى تطبيــق ZOOM بعنـوان (AUTO CAD) للفتـرة مـن 18 - 22 / 1/ 2026 القـى فيها المحاضرات حازم عبد إبراهيم / رئيس مهندسين اقدم .

في حال وجود
استفسار او مشكلة

يرجى مراسلة مركز نظم المعلومات
عبر البريد الالكتروني
cois@moch.gov.iq
او مراجعة مركز نظم المعلومات في مقر الوزارة
الكائن في بغداد ساحة المتحف

موقع الوزارة
www.moch.gov.iq
cois@moch.gov.iq