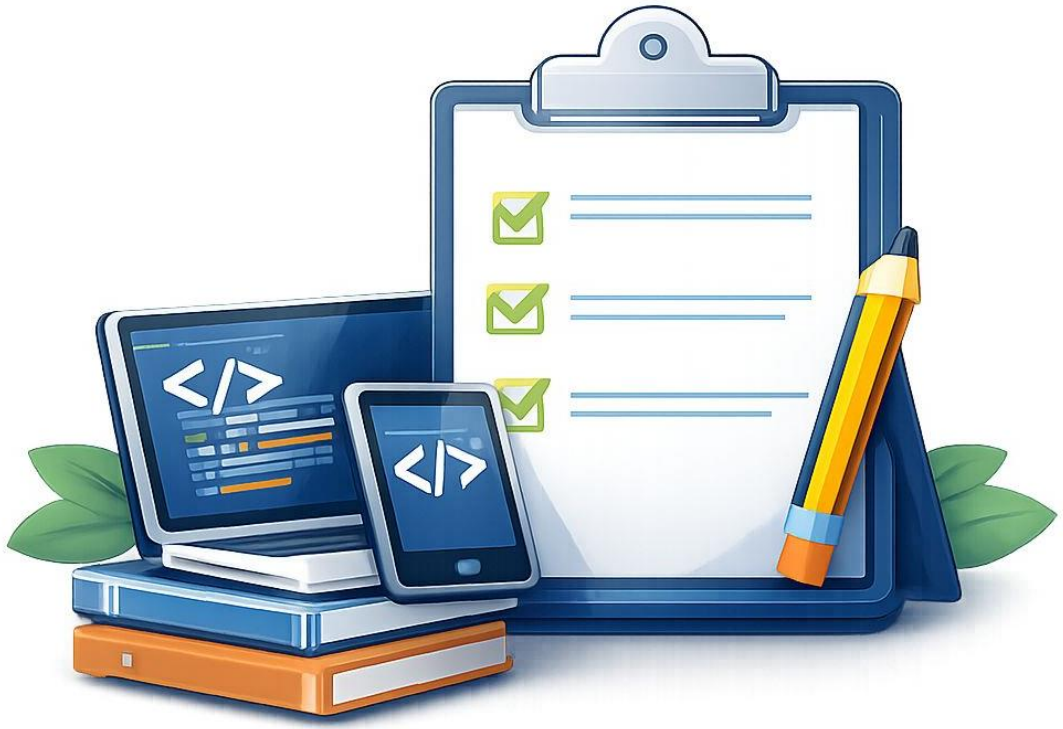
الأمن الرقمي والتصفح الآمن

اسم المدرب: **شيماء عباس شرف علي**

مسؤولة وحدة التعليم الالكتروني
اللقب العلمي : مدرس مساعد
مكان العمل : جامعة النهرين _ مركز الحاسبة الالكترونية
البريد الإلكتروني : shaimaa@nahrainuniv.edu.iq

أهداف الدورة التدريبية

- التعرف على مفهوم الأمن الرقمي
- فهم التهديدات الرقمية الشائعة
- تطبيق مبادئ التصفح الآمن
- حماية البيانات والمعلومات الشخصية
- تعزيز السلوك الرقمي المسؤول



الفئة المستهدفة

- منتسبو تشكيلات الوزارات والمؤسسات الحكومية
- الموظفون في القطاع الخاص
- العاملون في المجالات الإدارية والتقنية

مكان انعقاد الدورة التدريبية

- جامعة النهرين
  قاعات مركز الحاسبة الالكترونية

مدة الدورة التدريبية

- أسبوعان – 10 محاضرات
- ساعتان لكل محاضرة
- اليوم الأخير مخصص للاختبار النهائي

طرائق التدريب المعتمدة

- المناقشة والحوار
- الاستقراء
- التعلم التعاوني
- طريقة لعب الادوار

القي نظرة على الفيديو القصير التالي

الجدول الزمني للدورة التدريبية

اليوم	الجلسة الأولى (55 دقيقة)	استراحة (10 دقائق)	الجلسة الثانية (55 دقيقة)
اليوم الأول	• مدخل إلى الأمن الرقمي • مفهوم الأمن الرقمي • أهمية الأمن الرقمي	استراحة	• المخاطر الرقمية • أمثلة واقعية • مناقشة تفاعلية
اليوم الثاني	• التهديدات الرقمية • أنواع التهديدات	استراحة	• أمثلة على التهديدات الرقمية • حالات عملية
اليوم الثالث	• التصيد الاحتيالي • مفهوم التصيد	استراحة	• طرق التصيد الاحتيالي • مؤشرات الرسائل المشبوهة
اليوم الرابع	• البرمجيات الخبيثة • أنواع البرمجيات	استراحة	• طرق الانتشار والإصابة • أمثلة عملية
اليوم الخامس	• كلمات المرور • معايير كلمة المرور القوية	استراحة	• الأخطاء الشائعة في كلمات المرور • تطبيقات عملية
اليوم السادس	• التصفح الآمن • المواقع الآمنة	استراحة	• السلوك الآمن أثناء التصفح • أمثلة توضيحية
اليوم السابع	• حماية البيانات الشخصية • الخصوصية الرقمية	استراحة	• المعلومات الحساسة • طرق الحماية
اليوم الثامن	• أمن البريد الإلكتروني • مخاطر البريد الإلكتروني	استراحة	• الاستخدام الآمن للبريد الإلكتروني • أمثلة ورسائل حقيقية
اليوم التاسع	• أمن وسائل التواصل الاجتماعي • الخصوصية	استراحة	• السلوك الرقمي الآمن • إعدادات الحماية
اليوم العاشر	• مراجعة شاملة	استراحة	• الاختبار النهائي

اليوم الأول
مدخل إلى الأمن الرقمي

اليوم الأول
مدخل إلى الأمن الرقمي

- **محاور المحاضرة:**
- مفهوم الأمن الرقمي
- أهمية الأمن الرقمي
- مخاطر الإهمال الرقمي

الأمن الرقمي هو مجموعة من الإجراءات والممارسات التي تهدف إلى حماية الأجهزة والحسابات والبيانات من الوصول غير المصرح به أو الاستخدام غير المشروع، ويُعد عنصرًا أساسيًا في بيئات العمل الحديثة.

اليوم الأول
مدخل إلى الأمن الرقمي

- **عناصر الأمن الرقمي الأساسية:**
- **حماية الأجهزة**
تأمين أنظمة التشغيل، تحديث البرامج، واستخدام برامج الحماية من البرمجيات الخبيثة.
- **حماية الحسابات**
إنشاء كلمات مرور قوية، تفعيل المصادقة الثنائية، وعدم مشاركة بيانات الدخول.
- **حماية البيانات**
تشفير البيانات الحساسة، النسخ الاحتياطي الدوري، وتجنب تخزين المعلومات المهمة في أماكن غير آمنة.
- **الوعي الرقمي للمستخدم**
التحقق من الروابط والرسائل، تجنب المواقع المشبوهة، ومعرفة أساليب الاحتيال الإلكتروني.

مهمة اليوم الأول

- عرّف الأمن الرقمي بكلماتك
- اذكر سببًا واحدًا لأهميته

ترفع الإجابة من خلال الصف الالكتروني

اليوم الثاني
التهديدات الرقمية

اليوم الثاني
التهديدات الرقمية

- **محاور المحاضرة:**
- مفهوم التهديد الرقمي
- أنواع التهديدات الرقمية
- أمثلة واقعية

التهديدات الرقمية هي محاولات تستهدف اختراق الأنظمة أو سرقة المعلومات، وتتنوع بين تهديدات تقنية وأخرى تعتمد على خداع المستخدم.

اليوم الثاني
التهديدات الرقمية

- **التهديدات التقنية:**
- **البرمجيات الخبيثة (Malware):**
مثل الفيروسات، أحصنة طروادة، وبرامج التجسس البيانات.
- **هجمات الاختراق:**
محاولات الوصول غير المصرح به إلى الأنظمة أو الشبكات.
- **هجمات حجب الخدمة (DoS):**
تعطيل الخدمات الإلكترونية عن طريق إغراقها بطلبات وهمية.

اليوم الثاني
التهديدات الرقمية

- **التهديدات المعتمدة على الخداع:**
- **التصيد الاحتيالي (Phishing):**
رسائل أو مواقع مزيفة تهدف إلى سرقة كلمات المرور أو المعلومات الشخصية.
- **الهندسة الاجتماعية:**
استغلال ثقة المستخدم لإقناعه بالكشف عن بيانات حساسة.
- **الروابط والمرفقات الخبيثة:**
تؤدي إلى تنزيل برامج ضارة عند فتحها.

اليوم الثاني _ التهديدات الرقمية

- **أمثلة واقعية:**
- رسالة تدّعي أنها من جهة رسمية تطلب تحديث كلمة المرور.
- رابط وهمي لعرض مغرٍ يؤدي إلى موقع مزيف.
- ملف مرفق مجهول المصدر يحتوي على برمجيات ضارة.

مهمة اليوم الثاني

- اذكر نوعين من التهديدات الرقمية
ترفع الإجابة من خلال الصف الالكتروني

اليوم الثالث
التصيد الاحتيالي(Phishing)

اليوم الثالث
التصيد الاحتيالي(Phishing)

- **محاور المحاضرة:**
- مفهوم التصيد الاحتيالي
- أساليبه
- مؤشرات الرسائل الاحتيالية

التصيد الاحتيالي يعتمد على خداع المستخدم من خلال رسائل أو مواقع مزيفة بهدف سرقة البيانات مثل كلمات المرور أو المعلومات الشخصية.

اليوم الثالث
التصيد الاحتيالي(Phishing)

- **أساليب التصيد الاحتيالي**
- **البريد الإلكتروني الاحتيالي:**
  - رسائل تدّعي أنها من جهات رسمية أو بنوك.
  - تحتوي على روابط أو مرفقات خبيثة.
  - تطلب تحديث البيانات أو تأكيد كلمة المرور.

الرسائل النصية والمكالمات (Smishing / Vishing):

- رسائل SMSتدّعي وجود مشكلة بالحساب.
- مكالمات هاتفية تنتحل صفة جهة موثوقة.
- تهديد المستخدم بإيقاف الخدمة لإجباره على التفاعل.

اليوم الثالث
التصيد الاحتيالي(Phishing)

- **أساليب التصيد الاحتيالي**
- **مواقع الويب المزيفة:**
  - صفحات تشبه المواقع الأصلية تمامًا.
  - روابط مختصرة أو عناوين URL غير دقيقة.
  - جمع بيانات الدخول دون علم المستخدم.
- **وسائل التواصل الاجتماعي:**
  - حسابات وهمية تنتحل شخصيات أو مؤسسات.
  - روابط لعروض وهمية أو جوائز مغرية.
  - طلبات صداقة أو رسائل مشبوهة.

مهمة اليوم الثالث

- اذكر علامتين تدلان على رسالة تصيد احتيالي
ترفع الإجابة من خلال الصف الالكتروني

اليوم الرابع
البرمجيات الخبيثة

اليوم الرابع
البرمجيات الخبيثة

- **محاور المحاضرة:**
- مفهوم البرمجيات الخبيثة
- أنواعها
- طرق انتقالها

البرمجيات الخبيثة هي برامج مصممة لإلحاق الضرر بالأجهزة أو سرقة البيانات، وتنتقل غالبًا عبر ملفات أو روابط غير موثوقة.

اليوم الرابع
البرمجيات الخبيثة

- **أنواع البرمجيات الخبيثة**
- **●الفيروسات (Viruses:)**
- برامج تلتصق بالملفات أو البرامج.
- تنتشر عند تشغيل الملفات المصابة.
- تؤدي إلى تلف البيانات أو تعطيل النظام.

اليوم الرابع
البرمجيات الخبيثة

- **أنواع البرمجيات الخبيثة**
- **الديدان (:Worms)**
- تنتشر تلقائيًا عبر الشبكات.
- لا تحتاج إلى تدخل المستخدم.
- تسبب استهلاك الموارد وبطء الأنظمة.

اليوم الرابع
البرمجيات الخبيثة

- **أنواع البرمجيات الخبيثة**
- **أحصنة طروادة (Trojan Horses):**
- برامج تبدو شرعية لكنها خبيثة.
- تفتح بابًا خلفيًا للمهاجم.
- تُستخدم لسرقة البيانات أو التحكم بالجهاز.

اليوم الرابع
البرمجيات الخبيثة

- **أنواع البرمجيات الخبيثة**
- **برامج التجسس (Spyware):**
- تراقب نشاط المستخدم دون علمه.
- تجمع كلمات المرور والمعلومات الحساسة.
- تؤثر على الخصوصية والأمان.

اليوم الرابع
البرمجيات الخبيثة

- **أنواع البرمجيات الخبيثة**
- **●برامج الفدية (Ransomware):**
- تشفّر الملفات وتمنع الوصول إليها.
- تطلب فدية مالية لفك التشفير.
- من أخطر أنواع البرمجيات الخبيثة.

مهمة اليوم الرابع

- اذكر نوعًا واحدًا من البرمجيات الخبيثة

ترفع الإجابة من خلال الصف الالكتروني

اليوم الخامس
كلمات المرور الآمنة

اليوم الخامس
كلمات المرور الآمنة

- **محاور المحاضرة:**
- خصائص كلمة المرور القوية
- أخطاء شائعة في كلمات المرور

تُعد كلمات المرور خط الدفاع الأول عن الحسابات، واستخدام كلمات ضعيفة أو مكررة يزيد من احتمالية الاختراق.

اليوم الخامس
كلمات المرور الآمنة

- **خصائص كلمة المرور القوية**
- **🔐ما الذي يجعل كلمة المرور آمنة؟**
- لا تقل عن **12 حرفًا**.
- تحتوي على **حروف كبيرة وصغيرة**.
- تتضمن **أرقامًا ورموزًا خاصة**.
- لا تتضمن معلومات شخصية (الاسم، تاريخ الميلاد).
- مختلفة لكل حساب.

اليوم الخامس
كلمات المرور الآمنة

- **أخطاء شائعة في كلمات المرور**
- **❌تجنّب ما يلي:**
- استخدام كلمة مرور واحدة لجميع الحسابات.
- كلمات سهلة أو متوقعة (123456 – word).
- حفظ كلمات المرور في ملفات غير محمية.
- مشاركة كلمة المرور مع الآخرين.
- عدم تغيير كلمة المرور لفترات طويلة.

مهمة اليوم الخامس

- اذكر معيارين لكلمة مرور قوية

ترفع الإجابة من خلال الصف الالكتروني

Class code

jpvleqto

اليوم السادس
التصفح الآمن

اليوم السادس
التصفح الآمن

- **محاور المحاضرة:**
- المواقع الآمنة
- السلوكيات الآمنة أثناء التصفح

التصفح الآمن يعتمد على استخدام مواقع موثوقة وتجنب الروابط المشبوهة وتحديث المتصفح باستمرار.

اليوم السادس
التصفح الآمن

- **ممارسات التصفح الآمن**
- **🌐التحقق من أمان الموقع:**
- التأكد من وجود **HTTPS** وقفل الأمان في شريط العنوان.
- تجنب إدخال البيانات في مواقع غير موثوقة.
- الحذر من المواقع التي تطلب معلومات غير ضرورية

اليوم السادس
التصفح الآمن

- **ممارسات التصفح الآمن**
- **🌐🔗التعامل مع الروابط:**
- عدم الضغط على روابط مجهولة المصدر.
- تمرير المؤشر فوق الرابط للتحقق من العنوان الحقيقة
- الحذر من الروابط المختصرة والمضللة.

اليوم السادس
التصفح الآمن

- **ممارسات التصفح الآمن**
- **تحديثات المتصفح والإضافات:**
- تحديث المتصفح بشكل دوري لسد الثغرات الأمنية.
- تثبيت الإضافات من المتاجر الرسمية فقط.
- حذف الإضافات غير المستخدمة.

اليوم السادس
التصفح الآمن

- **ممارسات التصفح الآمن**
- **حماية الخصوصية أثناء التصفح:**
- تجنب استخدام الشبكات العامة لإدخال بيانات حساسة.
- تسجيل الخروج من الحسابات بعد الانتهاء.
- استخدام وضع التصفح الآمن أو الخاص عند الحاجة.

مهمة اليوم السادس

- اذكر سلوكًا واحدًا يعزز التصفح الآمن
ترفع الإجابة من خلال الصف الالكتروني

اليوم السابع
حماية البيانات الشخصية

اليوم السابع
حماية البيانات الشخصية

- **محاور المحاضرة:**
- مفهوم البيانات الشخصية
- طرق حمايتها

تشمل البيانات الشخصية المعلومات التي تخص الفرد، ويجب حمايتها من المشاركة غير الضرورية أو التخزين غير الآمن.

اليوم السابع
حماية البيانات الشخصية

- **أنواع البيانات الشخصية ومخاطرها**
- **🔐أمثلة على البيانات الشخصية:**
- الاسم الكامل، رقم الهاتف، العنوان.
- رقم الهوية، رقم البطاقة المصرفية.
- البريد الإلكتروني وكلمات المرور.
- الصور والمستندات الشخصية.
- بيانات الموقع الجغرافي وسجل التصفح.

اليوم السابع
حماية البيانات الشخصية

- ⚠ **مخاطر إهمال حماية البيانات:**
- **سرقة الهوية** واستخدام البيانات لأغراض غير قانونية.
- **الاحتيال المالي** وسحب الأموال دون علم صاحبها.
- **انتهاك الخصوصية** ونشر المعلومات الشخصية.
- استغلال البيانات في **الهندسة الاجتماعية والتصيد الاحتيالي**.

اليوم السابع
حماية البيانات الشخصية

- 🛡**ممارسات أساسية لحماية البيانات:**
- عدم مشاركة البيانات إلا عند الضرورة.
- استخدام كلمات مرور قوية وتفعيل المصادقة الثنائية.
- مراجعة إعدادات الخصوصية في التطبيقات والمواقع.
- تخزين البيانات الحساسة في أماكن آمنة ومشفّرة.

مهمة اليوم السابع

- اذكر مثالًا على بيانات شخصية
ترفع الإجابة من خلال الصف الالكتروني

اليوم الثامن
أمن البريد الإلكتروني

اليوم الثامن
أمن البريد الإلكتروني

- **محاور المحاضرة:**
- مخاطر البريد الإلكتروني
- الاستخدام الآمن

يُعد البريد الإلكتروني وسيلة شائعة للهجمات الرقمية، لذا يجب الحذر من الروابط والمرفقات غير المعروفة.

اليوم الثامن
أمن البريد الإلكتروني

- **مخاطر البريد الإلكتروني الشائعة**
- **⚠ أبرز التهديدات:**
- **رسائل التصيد الاحتيالي:**
رسائل مزيفة تنتحل صفة جهات رسمية لسرقة
- **المرفقات الخبيثة:**
ملفات تحتوي على فيروسات أو برامج تجسس.
- **الروابط المشبوهة:**
تؤدي إلى مواقع مزيفة أو تحميل برمجيات خبيثة.
- **انتحال العناوين البريدية:**
استخدام عنوان مشابه لعنوان موثوق لخداع المستخدم.

اليوم الثامن
أمن البريد الإلكتروني

- **إرشادات الاستخدام الآمن للبريد الإلكتروني**
- **🛡لحماية حسابك:**
- عدم فتح الرسائل من مرسلين غير معروفين.
- عدم الضغط على الروابط قبل التحقق من مصدرها.
- فحص المرفقات قبل فتحها.
- تفعيل **المصادقة الثنائية (2FA).**
- تحديث كلمة المرور بشكل دوري.

مهمة اليوم الثامن

- اذكر إجراءً واحدًا لحماية البريد الإلكتروني
ترفع الإجابة من خلال الصف الالكتروني

اليوم التاسع
أمن وسائل التواصل الاجتماعي

اليوم التاسع
أمن وسائل التواصل الاجتماعي

- **محاور المحاضرة:**
- الخصوصية
- السلوك الرقمي الآمن

الاستخدام غير الواعي لوسائل التواصل قد يؤدي إلى تسريب المعلومات، لذلك يجب ضبط إعدادات الخصوصية وعدم مشاركة البيانات الحساسة.

اليوم التاسع
أمن وسائل التواصل الاجتماعي

- **ممارسات آمنة على وسائل التواصل الاجتماعي**
- **🔐حماية الخصوصية:**
- ضبط إعدادات الخصوصية وجعل الحسابات خاصة عند الحاجة.
- تحديد من يمكنه رؤية المنشورات والمعلومات الشخصية.
- مراجعة الأذونات الممنوحة للتطبيقات المرتبطة بالحساب.

اليوم التاسع
أمن وسائل التواصل الاجتماعي

- **ممارسات آمنة على وسائل التواصل الاجتماعي**
- **إدارة الحسابات:**
- استخدام كلمة مرور قوية ومختلفة لكل منصة.
- تفعيل المصادقة الثنائية لحماية الحساب.
- مراقبة محاولات تسجيل الدخول غير المعتادة.

اليوم التاسع
أمن وسائل التواصل الاجتماعي

- **ممارسات آمنة على وسائل التواصل الاجتماعي**
- **الحذر من المحتوى والتفاعل:**
- عدم مشاركة معلومات حساسة أو صور خاصة.
- الحذر من الروابط والرسائل المشبوهة.
- عدم قبول طلبات صداقة من حسابات مجهولة.

اليوم التاسع
أمن وسائل التواصل الاجتماعي

- **ممارسات آمنة على وسائل التواصل الاجتماعي**
- **السلوك الرقمي المسؤول:**
- التفكير قبل النشر أو التعليق.
- احترام خصوصية الآخرين وعدم إعادة نشر محتوى دون إذن.
- الإبلاغ عن الحسابات أو المحتوى المشبوه.

مهمة اليوم التاسع

- اذكر خطرًا واحدًا من سوء استخدام وسائل التواصل
  ترفع الإجابة من خلال الصف الالكتروني

الخاتمة

دعونا نسأل أنفسنا الأسئلة التالية ونقيّم مدى الاستفادة من هذه الدورة:

- هل أصبح لدينا فهم واضح لمفهوم **الأمن الرقمي** وأهميته في حياتنا العملية والشخصية؟
- هل استطعنا التمييز بين **التهديدات الرقمية** وأساليب الاحتيال الإلكتروني المختلفة؟
- هل تعلّمنا كيفية **إنشاء كلمات مرور قوية** واستخدامها بشكل آمن؟
- هل أصبحنا أكثر وعيًا بممارسات **التصفح الآمن** والتعامل مع الروابط والمرفقات؟
- هل أدركنا أهمية **حماية البيانات الشخصية** وعدم مشاركتها دون ضرورة؟
- هل أصبح استخدامنا **للبريد الإلكتروني ووسائل التواصل الاجتماعي** أكثر أمانًا ومسؤولية؟
- هل نحن مستعدون لتطبيق ما تعلمناه ونقل ثقافة الأمن الرقمي إلى بيئة العمل والمجتمع؟

- إذا كانت الإجابة عن بعض هذه الأسئلة **بحاجة إلى تطوير**، فإن هذه الدورة تمثل خطوة أولى نحو بناء وعي رقمي مستدام، يتطلب ممارسة مستمرة والتزامًا بالسلوكيات الآمنة لحماية أنفسنا ومؤسساتنا من المخاطر الرقمية.

استبيانة تحليل مخرجات الدورة التدريبية

الاختبار النهائي Keywords

- Digital Security
- Phishing
- Malware
- Strong Passwords
- Safe Browsing
- Data Protection
- Social Media Security

المراجع

- **Google Safety Center**
  https://safety.google
- **National Cyber Security Centre (NCSC) – UK**
  https://www.ncsc.gov.uk
- **Cybersecurity & Infrastructure Security Agency (CISA)**
  https://www.cisa.gov/cybersecurity
- **Kaspersky Resource Center**
  https://www.kaspersky.com/resource-center
- **Stay Safe Online – Get Cyber Safe (Canada)**
  https://www.getcybersafe.gc.ca
- **Be Internet Awesome – Google**
  https://beinternetawesome.withgoogle.com
- **OWASP – Web Security Basics**
  https://owasp.org

شكرا لاصغائكم