المحور الثالث: الأمن المعلوماتي

النشاط الأول: تحليل عناوين المواقع (URLs) والتعرف على المواقع الآمنة

1. الفرق بين الموقعين في الصورتين من حيث تفاصيل عنوان URL:

الفرق بين الموقعين هو أن أحدها يستخدم هو بروتوكول نقل النص الفائق من نوع **HTTP**، والأخر يستخدم **HTTPS**.

2. الموقع الذي يعتبر أمن: هو الموقع الذي يستخدم بروتوكول نقل النص الفائق من نوع **HTTPS**

لأن:

- بروتوكول **HTTP** هو بروتوكول نقل النص الفائق لكنه غير مشفر، مما يعرض البيانات للسرقة.
- وبروتوكول **HTTPS** المضاف إليه "S" تعني "Secure" يستخدم شهادة **TLS/SSL** لتشفير البيانات وحمايتها أثناء النقل.

3. المخاطر المحتملة عند إدخال معلوماتك في موقع يستخدم بروتوكول نقل النص الفائق HTTP:

المواقع غير المشفرة يمكن أن تكون عرضة لهجمات **التنصت (Man-in-the-Middle Attacks)** ، حيث يمكن للقراصنة اعتراض بيانات المستخدم.

النشاط الثاني: فحص شهادات الأمان في المتصفحات

1. الفرق بين الموقعين في الصورتين:

بالرغم من أن الموقعين في الصورتين تستخدم بروتوكول **HTTPS** ، إلا أن موقع منصة التعليم عن بعد للمركز الجامعي ميلة تظهر رمز القفل مع علامة تعجب وعند الضغط على الرمز تظهر لنا كما في الصورة على أن شهادة أمن الموقع **غير موثوقة.** على عكس موقع وزارة التعليم العالي والبحث العلمي التي تظهر أن الموقع موثوق بشهادة **TLS/SSL** لتشفير البيانات وحمايتها أثناء النقل.

- **كيف يمكنك معرفة أن شهادة الأمن الرقمية صالحة:**
  - افتح أي موقع آمن (مثل المواقع في الصورة موقع وزارة التعليم العالي والبحث العلمي الجزائرية أو منصة التعليم عن بعد للمركز الجامعي ميلة...)
  - اضغط على رمز القفل بجانب عنوان الموقع في شريط المتصفح.
  - استعرض معلومات الشهادة، مثل الجهة التي أصدرتها ومدى صلاحيتها.

وعليه، تكون الشهادة صالحة حين تكون صادرة عن هيئة معترف بها ومفعلة في رابط الموقع الإلكتروني (رمز القفل فقط دون علامة تعجب أو خط).

2. يعني ظهور رسالة "الشهادة غير موثوقة" عند زيارة موقع معين:

- إذا كانت الشهادة غير موثوقة، فقد يكون الموقع مزيفًا أو تعرض لاختراق أو أن الموقع فقد شهادة **TLS/SSL** لتشفير البيانات وحمايتها أثناء النقل نتيجة انتهاء الآجال وعدم تجديد الاشتراك أو تعليق الاشتراك لأسباب أخرى، أو أن الموقع يحتاج إلى إعادة ضبط الإعدادات.

3. إذا رأيت تحذيرًا يشير إلى "اتصالك غير آمن":

- عند ظهور تحذير "اتصال غير آمن"، من الأفضل عدم إدخال بيانات حساسة مثل كلمات المرور أو معلومات الدفع.

النشاط الثالث: تحليل البريد الإلكتروني الاحتيالي والتصيد الإلكتروني (Phishing)

1. **البريد الإلكتروني الأصلي للمؤسسة الهندية:** هو رقم **2** (patel_dv@ongc.co.in) لأن اسم المؤسسة في الايميل متطابق مع اسمها المؤسسة "ongc". في حين الإيميل رقم 01 تم تغير مكان حرف "g" بتقديمة من اسم المؤسسة ليصبح "ognc" كما يلي (patel_dv@ognc.co.in) لخداع المستخدمين.
2. **نوع التهديد الأمني الذي واجهته المؤسستين:** التهديد الأمني الذي تعرضت له المؤسستين يتمثل **التصيّد الاحتيالي (Phishing)** وتحديدًا **انتحال البريد الإلكتروني** – (Email Spoofing / Business Email Compromise BEC) بحيث:

- المحتالون قاموا بتزوير البريد الإلكتروني الرسمي للشركة الهندية بإجراء تعديل طفيف عليه (تغيير حرف واحد)
- استخدموا هذا البريد المزيف للتواصل مع شركة أرامكو وإقناعها بتحويل الأموال إلى حساب بنكي لا علاقة له بالشركة الأصلية.
- هذا النوع من الهجمات يُعرف أيضًا بـ "**انتحال الهوية الرقمية لمؤسسة**" بهدف **الاحتيال المالي**. وهو من أشكال **الهندسة الاجتماعية على الشركات** التي تعتمد على استغلال الثقة والعلاقات التجارية القائمة.

3. يستخدم المحتالون عبر البريد الإلكتروني لغة مستعجلة مثل "حسابك سيتعرض للإغلاق خلال 24 ساعة":

- الرسائل الاحتيالية تستخدم أساليب تخويف لجعل المستخدم يتصرف بسرعة دون تدقيق.

4. إذا تلقيت بريدًا مشبوهًا عليك بـ:

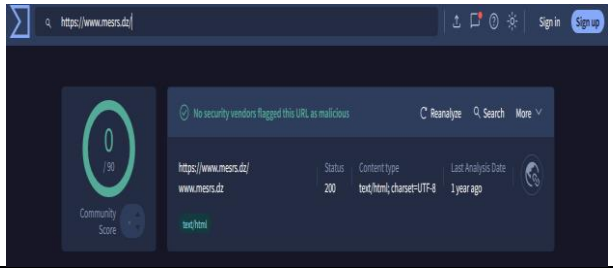
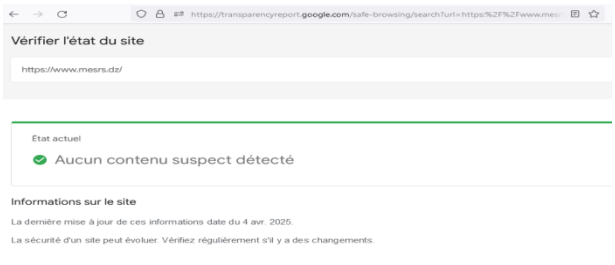
- إذا كنت تشك في رسالة، لا تنقر على أي رابط، وقم بالإبلاغ عنها.

النشاط الرابع: استخدام أدوات فحص المواقع الإلكترونية

استخدم موقعًا مثل **VirusTotal** أو **Google Safe Browsing** لفحص المواقع التالية مثلًا:

https://www.mesrs.dz/	/https://elearning.centre-univ-mila.dz/a2025
https://www.centre-univ-mila.dz/	/https://www.cbr.ru/eng
/https://www.meta.com	

1. **أدخل عناوين URL وشاهد النتيجة – وثق النتيجة في شكل صور:**

VirusTotal	Google Safe Browsing
https://www.virustotal.com/gui/home/url	**https://transparencyreport.google.com/safe-browsing/search**
https://www.mesrs.dz/	
	
بنفس الطريقة مع باقي المواقع...	

2. **تساعد هذه الأدوات في تحديد المواقع الضارة:**

- تقوم هذه الأدوات بمقارنة الموقع بقاعدة بيانات للمواقع المشبوهة.

3. **الخطوات التي يجب اتخاذها إذا كنت تشك في موقع معين:**

- بعد إجراء فحص للموقع، وإذا تم تصنيف الموقع على أنه ضار، لا تقم بزيارته أو إدخال أي بيانات عليه. وقم بالإبلاغ عنها من خلال مواقع مخصصة لهذا الغرض مثل: موقع غوغل (Google) للإبلاغ عن صفحة تصيد، متوفرة على الرابط التالي:

https://safebrowsing.google.com/safebrowsing/report_phish/?hl=ar

المحور الثالث: الأمن المعلوماتي

دراسة حالة 01

1. **نوع الهجوم الذي تعرضت له شركة "ألفا":** التهديد الأمني الذي تعرضت له شركة "ألفا" يتمثل في **هجوم سيبراني من عدة أنوع ومراحل:**

- يبدأ بهجوم **التصيد الاحتيالي (Phishing)** حيث تم استخدام رسالة بريد إلكتروني خادعة لخداع الموظف وحمله على النقر على رابط ضار.
- بمجرد إصابة جهاز الموظف، تم استخدام برمجية خبيثة للوصول إلى شبكة الشركة، مما يشير إلى وجود هجوم **برمجية خبيثة (Malware)**
- في النهاية، تمكن المهاجمون من سرقة قاعدة بيانات العملاء، مما يعتبر **خرقًا للبيانات (Data Breach)**

2. **نقاط الضعف التي استغلها المهاجمون في هذا الهجوم:**

- **العامل البشري:** يمثل الموظف الذي وقع ضحية التصيد الاحتيالي نقطة ضعف رئيسية. عدم تدريبه على التعرف على رسائل التصيد الاحتيالي جعله عرضة للخداع.
- **نقص الوعي الأمني:** قد يشير إلى عدم وجود سياسات وإجراءات أمنية كافية في الشركة، أو عدم تطبيقها بشكل فعال.
- **عدم كفاية الحماية التقنية:** يشير إلى أنظمة أمن الشركة (مثل جدران الحماية، وأنظمة كشف الاختراق) لم تكن قادرة على منع البرمجية الخبيثة من الانتشار أو اكتشاف الهجوم في وقت مبكر.

3. **الأضرار المحتملة التي قد تلحق بشركة "ألفا" نتيجة هذا الهجوم:**

- **فقدان الثقة:** قد يفقد العملاء ثقتهم في الشركة نتيجة تسرب بياناتهم السرية، مما يؤدي إلى خسارة العملاء والإضرار بالسمعة.
- **الأضرار المالية:** قد تتكبد الشركة خسائر مالية نتيجة دفع غرامات أو تعويضات للعملاء المتضررين، بالإضافة إلى تكاليف التحقيق في الحادث وإصلاح الأنظمة المتضررة.
- **المسائلة القانونية:** قد تواجه الشركة دعاوى قضائية من العملاء المتضررين أو الجهات التنظيمية نتيجة عدم حماية البيانات بشكل كافٍ.
- **تعطيل العمليات:** قد يؤدي الهجوم إلى تعطيل عمليات الشركة لفترة من الوقت، مما يؤثر على الإنتاجية والإيرادات.

4. الإجراءات التي يمكن لشركة "ألفا" اتخاذها لمنع وقوع مثل هذا الهجوم في المستقبل:

- **تدريب الموظفين:** توعية الموظفين بمخاطر التصيد الاحتيالي والهجمات الإلكترونية الأخرى، وتدريبهم على أفضل الممارسات الأمنية.
- **تنفيذ سياسات أمنية قوية:** وضع سياسات وإجراءات أمنية واضحة وشاملة، وتطبيقها بشكل فعال في جميع أنحاء الشركة.
- **تعزيز الحماية التقنية:** استخدام جدران الحماية وأنظمة كشف ومنع الاختراق وبرامج مكافحة الفيروسات المحدثة، وتطبيق المصادقة متعددة العوامل، وتشفير البيانات الحساسة.
- **إجراء تقييمات أمنية دورية:** تقييم نقاط الضعف في الأنظمة والإجراءات الأمنية بشكل دوري، واتخاذ الإجراءات اللازمة لمعالجتها.
- **وضع خطة للاستجابة للحوادث:** وضع خطة مفصلة للاستجابة للحوادث الأمنية، بما في ذلك إجراءات احتواء الهجوم، واستعادة الأنظمة، وإبلاغ الأطراف المعنية.

دراسة حالة 02

1. نوع التهديد الأمني الذي واجهته منصة "عدل 3" بسبب محاولات التسجيل غير الشرعي:

التهديد الأمني يتمثل في **هجوم سيبراني من نوع انتحال الهوية (Identity Spoofing) وهجوم الحرمان من الخدمة (DDoS Attack)**، حيث حاول أفراد غير مستحقين التسجيل، مما أدى إلى تعطيل الوصول للمنصة بسبب الضغط غير المبرر عليها.

2. التدابير التي يمكن اتخاذها لحماية منصة "عدل 3" من هذه الاختراقات: يمكن اتخاذ عدة تدابير، منها:

- **تفعيل التحقق الثنائي (2 FA) – المصادقة متعددة العوامل:** لضمان أن المستخدمين الحقيقيين فقط هم من يسجلون.
- **استخدام تقنيات كشف الموقع الجغرافي (Geo-Blocking)** لمنع تسجيل الحسابات من خارج الجزائر.
- **تعزيز أنظمة الحماية من هجمات الحرمان من الخدمة (DDoS Protection)**
- **مراقبة وتحليل حركة المرور على المنصة لكشف أي نشاط غير طبيعي.**

3. يمكن أن يؤثر هذا التهديد الأمني على المواطنين الجزائريين الذين يحاولون التسجيل بشكل قانوني من خلال: التأثيرات تشمل:

- **تعطيل أو تأخير عملية التسجيل** بسبب الضغط العالي على الخوادم.
- **إمكانية فقدان الفرصة للتسجيل في الأجال المحددة** بسبب امتلاء النظام بمعلومات غير صحيحة.
- **تزايد الشكوك حول مصداقية المنصة** مما يؤدي إلى فقدان الثقة في الحكومة الإلكترونية.

4. الفرق بين الأمن المعلوماتي والأمن السيبراني في هذا السياق؟

- **الأمن المعلوماتي** يهتم بحماية البيانات داخل النظام، مثل تشفير بيانات المستخدمين وضمان سرية معلوماتهم.
- **الأمن السيبراني** يركز على حماية البنية التحتية للمنصة من الهجمات الخارجية، مثل منع الهجمات الإلكترونية وصد محاولات الاختراق.

5. الدروس المستفادة من هذه الحالة لتطوير منصات حكومية أكثر أمانًا في المستقبل؟

- ضرورة **دمج معايير أمن المعلومات (ISO 27001)** في تطوير المنصات الرقمية.
- **إجراء اختبارات أمنية دورية** لمحاكاة الهجمات المحتملة والتأكد من جاهزية النظام.
- **توعية المستخدمين بطرق التسجيل الآمنة** وأهمية الحفاظ على بياناتهم الشخصية.
- **التعاون مع مزودي خدمات الإنترنت (ISP)** للكشف المبكر عن الهجمات والتصدي لها... الخ