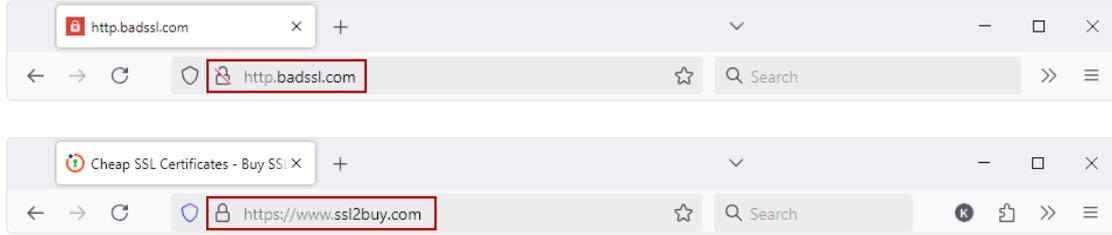


المحور الثالث: الأمن المعلوماتي

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

تم زيارة موقعين إلكترونيين مختلفين على متصفح فيرفُكس (Mozilla Firefox)، لاحظ تفاصيل عنوان URL لكل موقع في الصور أدناه:

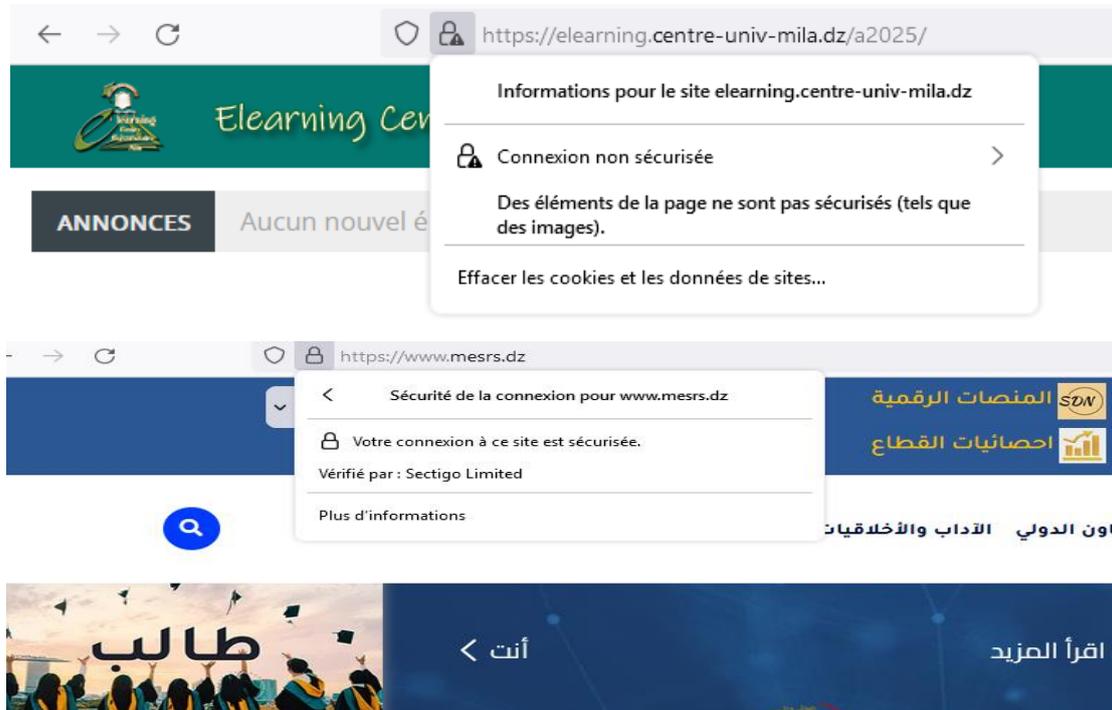


المطلوب:

- ما الفرق بين الموقعين في الصورتين من حيث تفاصيل عنوان URL؟
- أي الموقعين يعتبر أمن؟ ولماذا؟
- ما المخاطر المحتملة عند إدخال معلوماتك في موقع يستخدم بروتوكول نقل النص الفائق HTTP؟

النشاط الثاني: فحص شهادات الأمان في المتصفحات

تم في 04 أبريل 2025 على الساعة 21:17 فتح موقع كل من منصة التعليم عن بعد للمركز الجامعي عبد الحفيظ بوالصوف، ميلة (الجزائر) (Elearning)، وموقع وزارة التعليم العالي والبحث العلمي الجزائرية على متصفح فيرفُكس (Mozilla Firefox)، وتم بعدها الضغط على رمز القفل بجانب عنوان الموقع في شريط المتصفح. ليتم استعراض معلومات شهادة الأمان، وكانت النتائج كما توضحه الصور أدناه:



- ما الفرق بين الموقعين في الصورتين ؟ وكيف يمكنك معرفة أن شهادة الأمن الرقمية صالحة؟
- ماذا يعني ظهور رسالة "الشهادة غير موثوقة" عند زيارة موقع معين؟
- كيف تتصرف إذا رأيت تحذيراً يشير إلى "اتصالك غير آمن"؟

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

كشفت صحيفة "ذا إنديان إكسبرس" الهندية عن خسارة شركة نפט وغاز طبيعي في الهند لنحو 197 مليار روبية (في حدود 30 مليون دولار)، في واحدة من أكبر جرائم الاحتيال عبر الإنترنت في مومباي. وأشارت إلى أن تلك الخسارة ناجمة عن قيام المحتالين بتزوير البريد الإلكتروني للشركة الهندية، مع إدخال تعديلات طفيفة للغاية عليه، واستخدامه لإقناع شركة أرامكو السعودية بتحويل الأموال على حساب المحتالين بدلاً من حساب الشركة الهندية. وأضافت أن المحتالين استندوا في عملية الاحتيال إلى أن الشركة السعودية التي ستقوم بتحويل الأموال لن تلاحظ التغيير الطفيف في عنوان البريد الإلكتروني للشركة الهندية. وذكرت "الصحيفة" أن عنوان البريد الإلكتروني الأصلي للشركة الهندية هو

وذكرت "الصحيفة" أن الشركة الهندية طلب منها إرسال 36 ألف طن متري من الـ"نافتا" وهو خليط هايدروكربوني سائل قابل للاشتعال، وذلك إلى شركة أرامكو في السعودية. وأشارت إلى أن الشركة الهندية لاحظت أنها لم تتلقَّ المقابل المالي من "أرامكو" نظير إرسالها جزءاً من الطلب على حسابها في "بنك الهند" كما هو معتاد، وذلك في سبتمبر الماضي، وعندما استفسرت الشركة الهندية عن سبب التأخير أُخبرت بأن ذلك يعود إلى العطلات العامة وإجازات البنوك في المملكة، فقامت بإرسال الدفعة الثانية من السائل المطلوب في 22 سبتمبر. وأضافت أن الشركة الهندية لاحظت وجود مشكلة عندما لم تحصل على المال رغم إرسال الدفعة الثانية، خاصة بعدما تلقت رسالة من "أرامكو" تشير إلى أنها أرسلت المال إلى حساب جديد للشركة الهندية في "بنك بانكوك"، على الرغم من أن الشركة الهندية لم تطلب مطلقاً تحويل المال على هذا الحساب.

وذكرت "الصحيفة" أن الشركة الهندية قامت في 10 أكتوبر 2015 بالتقدم ببلاغ رسمي لشرطة جرائم الإنترنت للتحقيق في القضية، ووجدت الشرطة أن شخصاً ما على علم بالتواصل البريدي بين الشركة الهندية وأرامكو، قام بعمل بريد إلكتروني مشابه للبريد الإلكتروني الرسمي للشركة الهندية، ولم تلاحظ أرامكو الاختلاف بين الحسابين فقامت بإرسال المال للحساب المزيف.



- إليك عناوين البريد الإلكتروني التالية، علمًا أن أحدها عنوان البريد الإلكتروني الأصلي للمؤسسة الهندية:

1- patel_dv@ognc.co.in

2- patel_dv@ongc.co.in

- حسب رأيك، أي منها ليس البريد الإلكتروني الأصلي للمؤسسة الهندية؟ ولماذا؟
- ما هو نوع التهديد الأمني الذي واجهته المؤسستين؟
- لماذا يستخدم المحتالون عبر البريد الإلكتروني لغة مستعجلة مثل "حسابك سيتعرض للإغلاق خلال 24 ساعة"؟
- ماذا تفعل إذا تلقيت بريدًا مشبوهًا؟

النشاط الرابع: استخدام أدوات فحص المواقع الإلكترونية

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

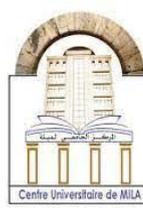
/https://elearning.centre-univ-mila.dz/a2025	https://www.mesrs.dz/
/https://www.cbr.ru/eng	https://www.centre-univ-mila.dz/
/https://www.meta.com	

المطلوب:

- أدخل عناوين URL وشاهد النتيجة - وثق النتيجة في شكل صور؟ بحيث يمكن استخدام المواقع من خلال الرابط التالية:

Google Safe Browsing	VirusTotal
https://transparencyreport.google.com/safe-browsing/search	https://www.virustotal.com/gui/home/url

- كيف تساعد هذه الأدوات في تحديد المواقع الضارة؟
- ما الخطوات التي يجب اتخاذها إذا كنت تشك في موقع معين؟



المحور الثالث: الأمن المعلوماتي

دراسة حالة 01

تعرضت شركة "ألفا" لهجوم إلكتروني أدى إلى تسرب بيانات العملاء السرية. تبين أن الهجوم بدأ برسالة بريد إلكتروني تصيدية استهدفت أحد موظفي الشركة، حيث قام الموظف بالنقر على رابط ضار في الرسالة، مما أدى إلى تثبيت برمجية خبيثة على جهاز الكمبيوتر الخاص به. استخدم المهاجمون هذه البرمجية للوصول إلى شبكة الشركة وسرقة قاعدة بيانات العملاء.

المطلوب:

1. ما نوع الهجوم الذي تعرضت له شركة "ألفا"؟
2. ما هي نقاط الضعف التي استغلها المهاجمون في هذا الهجوم؟
3. ما هي الأضرار المحتملة التي قد تلحق بشركة "ألفا" نتيجة هذا الهجوم؟
4. ما هي الإجراءات التي يمكن لشركة "ألفا" اتخاذها لمنع وقوع مثل هذا الهجوم في المستقبل؟

دراسة حالة 02

أطلقت الحكومة الجزائرية منصة رقمية لتسجيل طالبي السكن ضمن برنامج "عدل 3"، بهدف تسهيل عملية التسجيل وتقليل التزاحم الإداري. إلا أن المنصة واجهت تحديات أمنية خطيرة، من بينها محاولات تسجيل غير شرعية من خارج الجزائر، لا سيما من بعض الأفراد في المملكة المغربية، مما أدى إلى تعقيد عملية التسجيل وتأخير وصول المواطنين المستحقين.

المطلوب:

1. ما هو نوع التهديد الأمني الذي واجهته منصة "عدل 3" بسبب محاولات التسجيل غير الشرعي؟
2. ما هي التدابير التي يمكن اتخاذها لحماية منصة "عدل 3" من هذه الاختراقات؟
3. كيف يمكن أن يؤثر هذا التهديد الأمني على المواطنين الجزائريين الذين يحاولون التسجيل بشكل قانوني؟
4. ما الفرق بين الأمن المعلوماتي والأمن السيبراني في هذا السياق؟
5. ما هي الدروس المستفادة من هذه الحالة لتطوير منصات حكومية أكثر أمانًا في المستقبل؟