الوحدة الأولى : الأمن السيبراني ورقة عمل الدرس الأول: مقدمة في الأمن السيبراني

اسم الطالبة :..... الصف :.....

ضعي المصطلح العلمي المناسب في الفراغات للعبارات الموجوده مستعينه بالكلمات التالية :

الجرائم الإلكترونية - مفهوم الأمن السيبراني - أهمية الأمن السيبراني - مثلث الحماية (CIA)

١	إن الهدف الأساسي للأمان الإلكتروني هو التركيز على توفير حماية متوازنة للمعلومات والبيانات من حيث سريتها وتكاملها وتوافرها، وهذا يعرف باسم	.....
٢	تزداد في زيادة أهمية البيانات والمعلومات المتوفرة على الشبكة وضرورة توافر البيانات للمستخدمين دون انقطاع بالإضافة إلى عدد المستخدمين الذين يحتاجون للوصول إلى تلك البيانات والمعلومات بشكل مستمر	.....
٣	حماية أجهزة الحاسب والشبكات والبرامج والبيانات من الوصول غير المصرح به والذي قد يهدف إلى الحصول على المعلومات الحساسة أو تغييرها أو إتلافها أو ابتزاز المستخدمين للحصول على الأموال، بل وأحيانًا تعطيل عمليات المؤسسة عمومًا	.....
٤	هي استخدام الحاسب كأداة لتحقيق غايات غير قانونية مثل الاحتيال أو التوزيع غير القانوني للمواد المحمية بحقوق الطبع والنشر أو سرقة الهويات أو انتهاك الخصوصية	.....

اختاري المفهوم المناسب فيما يلي من مكونات مثلث الحماية :

.....

هي إتاحة البيانات والمعلومات للأشخاص المعنيين بها فقط والمسموح لهم بالاطلاع عليها، ولتحقيق ذلك يتم استخدام أساليب مختلفة مثل اسم المستخدم وكلمة المرور، وقوائم الأشخاص ذوي الصالحيات.

.....

يشير إلى الحفاظ على دقة وصحة المعلومات، والتأكد من عدم إمكانية تعديلها إلا من قبل الأشخاص المخولين بذلك، ومن أساليب الحفاظ على تكامل البيانات والمعلومات: تحديد الأذونات والصلاحيات (Permissions) والتشفير Encryption، وغيرها.

.....

ضمان الوصول للمعلومات في الوقت المناسب وبطريقة موثوقة لاستخدامها، من أمثلة الإجراءات المتخذة لضمان توافر البيانات والمعلومات، الحفاظ على سلامة الأجهزة المستضيفة للبيانات، والنسخ الاحتياطي، وتحديثات النظام، وتحسين كفاءة الشبكة لتسهيل وصول المستخدمين ما أمكن

نشاط ٣

صلي مايلي من أنواع الجرائم الإلكترونية بالمفهوم الصحيح له بالجدول التالي :

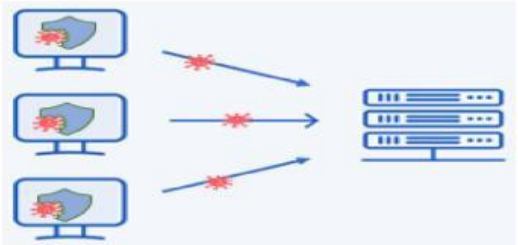
١- المضايقات عبر الأنترنت	يحدث هذا الاحتيال عندما يتقمص المجرم الإلكتروني دور جهة موثوقة يتعامل معها الضحية، بغرض الحصول على معلومات شخصية عن مستخدم معين مثل كلمات المرور المصرفية وعنوان البيت أو الرقم الشخصي. تتم هذه العملية عادةً من خلال مواقع الاحتيال التي تُقلد المواقع الرسمية.
٢- التسلل الإلكتروني	بعد سرقة البيانات الشخصية، يقوم المحتالون بانتحال شخصية الضحية واستخدام بياناته لإجراء معاملات مالية، أو أعمال غير قانونية.
٣- الاحتيال الإلكتروني	تشمل التهديدات عبر البريد الإلكتروني أو الرسائل الفورية أو المشاركات المسيئة في وسائل التواصل الاجتماعي مثل فيسبوك وتويتر.
٤- سرقة الهوية	عادة ما يصيب المتسللون الإلكترونيون أجهزة الحاسب الخاصة بضحاياهم ببرامج ضارة يمكنها تسجيل نشاط الحاسب لمراقبة نشاطاتهم عبر الإنترنت، فمثلًا يقوم برنامج **مسجل المفاتيح** (keylogger) بتتبع وتسجيل أزرار لوحة المفاتيح المضغوطة بطريقة سرية بحيث يصعب على الشخص معرفة أنه تتم مراقبته وجمع بياناته الخاصة.
٥- انتهاك الخصوصية	يحدث انتهاك الخصوصية عند محاولة شخص ما التطفل على الحياة الشخصية لشخص آخر، وقد يتضمن ذلك اختراق الحاسب الشخصي الخاص به أو قراءة رسائل البريد الإلكتروني أو مراقبة الأنشطة الشخصية الخاصة به عبر الإنترنت.

نشاط ٤

اختاري المسميات الصحيحة في الفراغات التالية لأنواع الهجمات الإلكترونية :

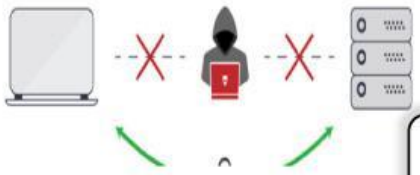
هو نوع من أنواع الهجمات السيبرانية حيث يقوم جهاز حاسب واحد أو شبكة بإغراق موقع أو خادم مستهدف بحركة المرور

.....



هو إصدار أكثر تقدمًا من هجوم حجب الخدمات حيث يتم استخدام العديد من أجهزة الحاسب أو الشبكات لإغراق موقع ويب أو خادم مستهدف بحركة المرور

.....



يتطفل فيه المهاجم بين اتصال المستخدم والتطبيق، ويجلس في منتصفه متظاهرًا بأنه الطرف الآخر. يمكنه قراءة أو تعديل أو إدخال رسائل جديدة في تدفق الاتصال. يمكن استخدام هجوم الوسيط لسرقة معلومات حساسة أو تنفيذ أنشطة ضارة أخرى

.....

من الأمثلة على هجمات الوسيط الالكتروني

1

.....

.....

يمكن للمهاجم إعداد نقطة وصول واي فاي خادعة تظهر على أنها نقطة وصول شرعية، مما يسمح له باعتراض وقراءة حركة مرور الشبكة غير المشفرة المرسلة من قبل الضحايا المطمئنين الذين يتصلون بنقطة الوصول الخادعة

2

.....

.....

في هذا الهجوم، يعترض المهاجم استعلامات نظام اسم النطاق DNS ويغيرها، ويعيد توجيه الضحايا إلى موقع ويب ضار بدلا من موقع الويب المشروع المقصود.

3

.....

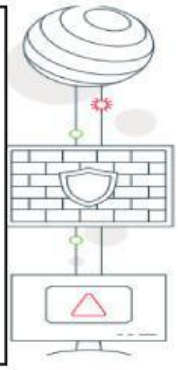
.....

في هذا النوع من الهجوم يعترض المهاجم رسائل البريد الالكتروني وتغيير المحتوى أو إضافة مرفقات أو روابط ضارة لسرقة معلومات حساسة أو لنشر برامج ضارة.

نشاط ٥

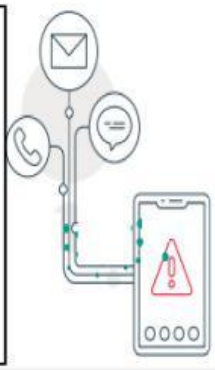
عددي أهم التدابير التي يجب اتخاذها للوقاية من الجرائم الإلكترونية..

يُعدُّ أحد أكثر حلول الأمن السيبراني للتقليل من خطر برمجيات الاختراق الخاصة وخاصة تلك التي تعتمد على ابتزاز المستخدم

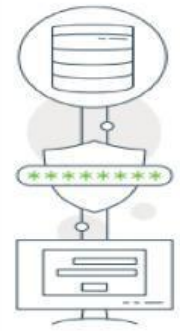


يُعدُّ الحل الأكثر نجاحا في محاربة الهجمات نظرًا لأنه يمنع البرمجيات الضارة والفيروسات الخبيثة الأخرى من الدخول إلى جهازك وتعريض بياناتك للخطر

يتحكم في حركة مرور البيانات الواردة والصادرة من خلال تحليل حزم البيانات وتحديد ما إذا كان ينبغي السماح بمرورها أم لا

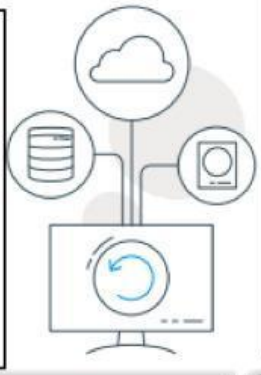


ينبغي الانتباه إلى كافة أشكال التواصل الرقمي سواء عبر البريد الإلكتروني أو منصات التواصل الاجتماعية وحتى المكالمات الهاتفية والرسائل النصية فمثلا تجنب فتح الرسائل الإلكترونية المرسلة من جهات مجهولة، والتأكد من الروابط التشعبية بدقة قبل الضغط عليها، وتوخي الحذر من مشاركة أي معلومات شخصية عبر هذه المنصات



يجب أن تكون كلمة المرور القوية على درجة كافية من التعقيد، وتتغير بشكل دوري. وفي هذا الوقت الذي تتعدد حسابات المستخدمين على منصات وتطبيقات عديدة، ظهرت الحاجة إلى استخدام أدوات إدارة كلمات المرور Password Managers والتي تحتفظ بكلمات المرور بصورة مشفرة في قواعد بيانات آمنة، بحيث يتم استرجاعها عند طلب المستخدم والتحقق من هويته

تقدم عملية التحقق الثاني أو المتعدد خيارات أمان إضافية، حيث تتطلب عملية المصادقة التقليدية إدخال اسم المستخدم وكلمة المرور فقط،



يعد إجراءه للبيانات بشكل دوري خطوة مهمة في مجال الحفاظ على أمان الإنترنت الشخصي، فبشكل أساسي عليك الاحتفاظ بثلاث نسخ من بياناتك على نوعين مختلفين من وسائط تخزين البيانات، كنسختين على (القرص الصلب المحلي والخارجي)، ونسخة أخرى على موقع خارجي أو باستخدام التخزين السحابي.

يُنصح بتجنب استخدام شبكة واي فاي العامة دون استخدام شبكة افتراضية خاصة - Virtual private network VPN فباستخدام هذه الشبكة، يتم تشفير حركة نقل البيانات بين الجهاز وخادم VPN مما يصعب على القراصنة الوصول إلى بياناتك على الإنترنت، كما يوصى باستخدام الشبكة الخلوية عند عدم وجود شبكة VPN وذلك للحصول على مستوى أعلى من الأمان

معلمة المادة : سلطانه الشمري