محاضرات مبادئ الحاسوب

COMPUTER FUNDAMENTALS

قسم الجغرافية

المرحلة الأولى – الدراسة الصباحية

العام الدراسي 2025–2026

المحاضرة الثالثة

المدرس رعد ذياب خلف

أمن الحاسوب

مفهوم أمن الحاسوب

أمن الحاسوب هو مجموعة الإجراءات والتقنيات والسلوكيات التي تهدف إلى حماية الأجهزة والبرامج والبيانات والحسابات من الوصول غير المصرح به والتلف والسرقة والتعطيل .لا يقتصر الأمن على تثبيت برنامج حماية، بل يشمل تحديث الأنظمة واختيار كلمات مرور قوية والتعامل الواعي مع الملفات والروابط.

أهمية أمن الحاسوب

تحتوي الحواسيب على بحوث الطلبة ودرجاتهم ووثائقهم وصورهم وملفات المؤسسات .وقد يؤدي فقدان هذه البيانات أو تسريبها إلى تعطيل الدراسة أو العمل، وإلى خسائر مادية أو أضرار تتعلق بالخصوصية والسمعة.

الأهداف الأساسية للأمن

السرية :منع غير المخولين من الاطلاع على المعلومات .السلامة أو التكامل :المحافظة على صحة البيانات ومنع تعديلها دون إذن .الإتاحة :ضمان إمكانية الوصول إلى النظام والبيانات عند الحاجة . وتعرف هذه الأهداف بثلاثية.CIA

الفرق بين التهديد والثغرة والخطر

التهديد هو حدث أو جهة قد تسبب ضرراً، مثل رسالة احتيالية .الثغرة نقطة ضعف يمكن استغلالها، مثل نظام غير محدث .الخطر هو احتمال وقوع الضرر وحجم أثره .أما الضابط الأمني فهو الإجراء الذي يقلل احتمال الخطر أو أثره.

مثال دراسي

إذا احتفظ طالب ببحث التخرج على جهاز واحد دون نسخة احتياطية، فإن تعطل القرص قد يؤدي إلى فقدان البحث .وجود نسخة احتياطية مستقلة يقلل أثر هذا الخطر.

التهديدات التي تواجه الحاسوب

مصادر التهديد

قد تنشأ التهديدات من الإنترنت أو الأجهزة الخارجية أو التطبيقات غير الموثوقة أو أخطاء المستخدم أو الأعطال المادية .ولا يتطلب كل حادث أمني وجود مهاجم؛ فقد يتسبب حذف ملف مهم بالخطأ في فقدان بيانات.

البرمجيات الخبيثةMalware

هي برامج أو شيفرات صممت لإحداث ضرر أو التجسس أو سرقة البيانات أو تعطيل النظام .تشمل الفيروسات والديدان وأحصنة طروادة وبرامج التجسس وبرامج الفدية.

الفيروسات والديدان

يرتبط الفيروس غالباً بملف أو برنامج وينتشر عند تشغيله في ظروف معينة .أما الدودة فتستطيع في بعض الحالات الانتشار عبر الشبكات دون الحاجة إلى إرفاق نفسها بملف مستخدم.

حصان طروادة

برنامج يبدو نافعاً أو عادياً لكنه يخفي سلوكاً ضاراً، مثل تثبيت مكونات غير مرغوبة أو إتاحة وصول غير مصرح به .قد يصل ضمن برنامج مزيف أو مرفق غير موثوق.

برامج الفديةRansomware

قد تشفر ملفات المستخدم أو تمنع الوصول إليها ثم تطلب مقابلاً مالياً .دفع المبلغ لا يضمن استعادة الملفات؛ لذلك تعد النسخ الاحتياطية المنفصلة والتحديثات والوعي بالروابط وسائل وقاية مهمة.

برامج التجسس

تجمع معلومات عن نشاط المستخدم أو بياناته دون موافقة صحيحة .وقد تؤدي إلى كشف كلمات المرور أو المعلومات الشخصية.

أمثلة على الأعراض

تباطؤ غير معتاد أو ظهور نوافذ غريبة أو تغيّر إعدادات المتصفح أو اختفاء ملفات قد يكون مؤشراً على مشكلة، لكنه لا يكفي وحده لإثبات الإصابة.

الهندسة الاجتماعية والتصيد الإلكتروني

الهندسة الاجتماعية

هي محاولة التأثير في الأشخاص نفسياً لدفعهم إلى كشف معلومات أو تنفيذ إجراءات ضارة .يستغل المحتال الخوف أو الاستعجال أو الفضول أو الثقة بالجهات المعروفة.

التصيد الإلكترونيPhishing

رسائل أو صفحات مزيفة تحاول سرقة كلمات المرور أو رموز التحقق أو بيانات الدفع .قد تصل عبر البريد الإلكتروني أو الرسائل النصية أو تطبيقات التواصل.

علامات الرسائل المشبوهة

طلب عاجل لتحديث الحساب، تهديد بإغلاقه، روابط ذات عناوين غريبة، أخطاء في اسم الجهة، مرفقات غير متوقعة، أو طلب إرسال رمز التحقق .قد تكون الرسائل الاحتيالية مكتوبة بلغة سليمة، فلا يعتمد الحكم على الأخطاء اللغوية وحدها.

طريقة التعامل الصحيحة

لا تفتح الرابط مباشرة؛ ادخل إلى الموقع أو التطبيق الرسمي بنفسك .تحقق من عنوان المرسل دون الاعتماد عليه وحده .لا ترسل كلمات المرور أو رموز التحقق، وأبلغ الجهة المعنية إذا كانت الرسالة تخص الجامعة أو المؤسسة.

انتحال الهوية والمكالمات

قد يدعي شخص أنه موظف دعم فني ويطلب تثبيت برنامج للتحكم عن بعد أو مشاركة الشاشة .لا تمنح الوصول إلا بعد التحقق المستقل من هويته وحاجتك الفعلية للمساعدة.

تطبيق للطالب

إذا وصلت رسالة تدعي أنها من الجامعة وتطلب تسجيل الدخول إلى رابط غير مألوف للاطلاع على الدرجات، فيجب فتح بوابة الجامعة الرسمية بدلاً من الرابط المرسل.

كلمات المرور والمصادقة

أهمية كلمة المرور

كلمة المرور هي أحد وسائل حماية الحسابات، لكنها قد تُسرق أو تُخمّن أو تُعاد الاستفادة منها إذا استخدمت في عدة مواقع.

اختيار كلمة مرور قوية

يفضل استخدام عبارة مرور طويلة وفريدة لكل حساب، مؤلفة من عدة كلمات غير متوقعة أو من سلسلة عشوائية يولدها مدير كلمات مرور .طول كلمة المرور وتفردها أهم من الاكتفاء بتبديل بعض الحروف برموز شائعة.

مدير كلمات المرور

يساعد على إنشاء كلمات مرور قوية ومختلفة وتخزينها بصورة منظمة .ينبغي حماية المدير بكلمة رئيسية قوية وتفعيل المصادقة الإضافية إن كانت متاحة.

المصادقة متعددة العواملMFA

تضيف وسيلة تحقق ثانية إلى كلمة المرور، مثل تطبيق مصادقة أو مفتاح أمان .وتعد مفاتيح المرور Passkeys خياراً حديثاً يقلل الاعتماد على كلمات المرور ويقاوم كثيراً من أساليب التصيد.

قواعد مهمة

لا تشارك كلمة المرور أو رمز التحقق مع أحد، ولا تحفظهما في ملف مكشوف .تجنب إعادة استخدام كلمة المرور، وغيّرها فور وجود دليل على انكشافها.

حماية الأجهزة المشتركة

لا تترك الحساب مفتوحاً على حاسوب المختبر، وسجل الخروج بعد الانتهاء، ولا تسمح للمتصفح بحفظ بيانات الدخول على الأجهزة العامة.

تمرين

اطلب من الطلبة وصف خصائص عبارة مرور قوية دون كتابة كلمات المرور الحقيقية الخاصة بهم.

تحديثات النظام والبرامج والحماية

لماذا نحدث البرامج؟

تعالج التحديثات أخطاءً وثغرات أمنية وقد تحسن الاستقرار والأداء .إن تأجيل التحديثات المهمة يزيد مدة تعرض الجهاز للمشكلات المعروفة.

مصادر البرامج الآمنة

ثبت التطبيقات من المواقع الرسمية أو المتاجر الموثوقة، وتحقق من اسم الناشر والصلاحيات المطلوبة .تجنب النسخ المقرصنة وملفات التفعيل المجهولة لأنها قد تحمل برمجيات ضارة.

برامج مكافحة البرمجيات الخبيثة

تفحص الملفات والسلوكيات المشبوهة وتساعد على منع بعض التهديدات أو عزلها .لكنها ليست ضماناً كاملاً، ويجب أن تعمل مع تحديث النظام والحذر من الروابط والملفات.

الجدار الناريFirewall

يراقب الاتصالات الشبكية وفق قواعد محددة ويساعد على تقليل الاتصالات غير المرغوبة .لا يحل محل الحماية من التصيد أو إدارة كلمات المرور.

صلاحيات التطبيقات

يجب منح البرامج أقل قدر لازم من الصلاحيات .تطبيق بسيط لا يحتاج عادة إلى الوصول الدائم للكاميرا أو الميكروفون أو جميع الملفات ما لم تكن وظيفته تتطلب ذلك.

علامات تستدعي الفحص

ظهور برنامج لم تثبته أو طلبات صلاحيات غير مبررة أو تحذيرات أمنية متكررة .ينبغي التحقق بهدوء وتجنب تنزيل أدوات إصلاح مجهولة.

إجراء عملي

فعّل التحديث التلقائي من المصدر الرسمي، وراجع قائمة التطبيقات المثبتة دورياً، واحذف ما لم تعد تحتاج إليه.

أمن الإنترنت والشبكات

المتصفح الآمن

يجب تحديث المتصفح، والتحقق من اسم الموقع قبل إدخال البيانات، وتجنب الإضافات غير الموثوقة .وجود HTTPS يعني تشفير الاتصال عادة، لكنه لا يثبت أن الموقع نفسه صادق أو آمن.

شبكات Wi-Fi العامة

قد تكون الشبكات العامة غير موثوقة أو تنتحل اسم شبكة معروفة .تجنب التعامل مع المعلومات الحساسة على شبكة مشبوهة، واستخدم اتصالاً موثوقاً كلما أمكن.

حماية الشبكة المنزلية

استخدم تشفير WPA2-AES أو WPA3 عند توفره، وكلمة مرور قوية للشبكة، وغيّر بيانات إدارة الموجّه الافتراضية، وثبّت تحديثاته الأمنية.

مشاركة الملفات

شارك الملفات مع الأشخاص المعنيين فقط، وحدد صلاحية العرض أو التعديل حسب الحاجة، وألغِ الروابط العامة عندما تنتهي الحاجة إليها.

التنزيل الآمن

افحص مصدر الملف ونوعه، واحذر من الملفات التنفيذية التي تصل باسم مستند أو صورة .لا تفعّل وحدات الماكرو في المستندات المجهولة.

استخدام الخدمات السحابية

تتيح الخدمات السحابية حفظ الملفات ومزامنتها، لكن أمانها يتطلب حماية الحساب ومراجعة صلاحيات المشاركة وفهم الفرق بين المزامنة والنسخ الاحتياطي.

مثال

عند إرسال بحث جماعي، يمنح الطالب زملاءه صلاحية التعليق أو التعديل فقط إذا احتاجوا إليها، ولا ينشر رابط الملف لجميع مستخدمي الإنترنت.

النسخ الاحتياطي وحماية البيانات

النسخ الاحتياطيBackup

هو إنشاء نسخة إضافية من البيانات لاستعادتها عند الحذف أو التلف أو فقدان الجهاز أو التعرض لهجوم .لا تكفي نسخة وحيدة موجودة على القرص نفسه.

قاعدة3-2-1

توصية عملية شائعة :الاحتفاظ بثلاث نسخ من البيانات، على وسيطين مختلفين، مع نسخة واحدة على الأقل خارج الموقع أو منفصلة عن الجهاز .يمكن تكييف القاعدة وفق حجم البيانات والإمكانات.

الفرق بين النسخ والمزامنة

المزامنة تنقل التغييرات بين الأجهزة، وقد تنقل الحذف أو التلف أيضاً .أما النسخ الاحتياطي المصمم جيداً فيتيح الرجوع إلى نسخة سابقة عند الحاجة.

تشفير البيانات

يحوّل البيانات إلى صيغة لا يمكن قراءتها بسهولة دون المفتاح المناسب .يفيد تشفير الجهاز أو الملفات الحساسة عند فقدان الحاسوب أو وسائط التخزين.

استعادة الملفات

يجب تجربة استعادة ملف غير حساس من النسخة الاحتياطية بين حين وآخر للتأكد من سلامتها . النسخة التي لا يمكن استعادتها لا تحقق الهدف المطلوب.

حماية البيانات الشخصية

لا تجمع أو تشارك بيانات الآخرين إلا لغرض مشروع ومحدد .أخفِ المعلومات الحساسة عند نشر الصور أو مشاركة المستندات.

تطبيق جغرافي

يمكن حفظ بيانات المسح الميداني وخرائط المشروع في مجلد منظم، مع نسخة احتياطية منفصلة ونسخة محفوظة في مساحة سحابية موثوقة.

أمن الأجهزة والوسائط المحمولة

الأمن المادي

يشمل حماية الحاسوب من السرقة والتلف والحرارة والسوائل وانقطاع الكهرباء .يجب وضعه في مكان مناسب وتجنب تركه دون مراقبة في الأماكن العامة.

قفل الشاشة

فعّل قفل الشاشة التلقائي واستخدم رمزاً أو وسيلة تحقق مناسبة .القفل يمنع كثيراً من حالات الوصول العابر لكنه لا يغني عن تشفير البيانات.

وحدات USB الخارجية

قد تحتوي وسائط التخزين على ملفات خبيثة أو بيانات حساسة .لا توصل وسائط مجهولة المصدر، وافحص الملفات قبل فتحها، ولا تشغل البرامج غير الموثوقة منها.

الهواتف والأجهزة اللوحية

تحتاج إلى تحديثات وقفل آمن ومراجعة صلاحيات التطبيقات والنسخ الاحتياطي، لأنها تخزن حسابات وصوراً ومراسلات ومعلومات موقع.

التخلص من الأجهزة

قبل بيع الجهاز أو نقله، احتفظ بنسخة من بياناتك ثم استخدم إجراءات مسح آمنة مناسبة لنوع التخزين، وأزل الحسابات المرتبطة به.

انقطاع الكهرباء

يساعد جهاز UPS على منح وقت قصير لحفظ العمل والإغلاق المنظم عند انقطاع الطاقة، لكنه لا يعد بديلاً عن النسخ الاحتياطي.

مثال عملي

بعد انتهاء المختبر، يحفظ الطالب ملفاته في مكانه المخصص، ويخرج من الحساب، ويزيل وحدة التخزين الخاصة به، ويتأكد من عدم ترك مستندات شخصية.

التعامل مع الحوادث الأمنية

ما الحادث الأمني؟

هو واقعة تؤثر أو قد تؤثر في سرية البيانات أو سلامتها أو إتاحتها، مثل اختراق حساب أو ضياع جهاز أو إصابة ببرنامج فدية.

الخطوة الأولى :الملاحظة

سجل ما حدث والوقت التقريبي والرسائل الظاهرة، ولا تتجاهل تنبيهات الحماية .تجنب حذف الأدلة أو تشغيل برامج إصلاح مجهولة.

عند الاشتباه بإصابة

أوقف استخدام الملفات المشبوهة، وافصل الجهاز عن الشبكة عند وجود مؤشرات قوية على انتشار الضرر أو تسريب البيانات، واطلب مساعدة مسؤول التقنية المختص.

عند اختراق حساب

استخدم جهازاً موثوقاً لتغيير كلمة المرور، وألغِ الجلسات غير المعروفة، وفعّل المصادقة متعددة العوامل، وراجع وسائل الاسترداد والنشاط الأخير.

عند فقدان جهاز

أبلغ الجهة المسؤولة إذا كان الجهاز تابعاً للمؤسسة، واستخدم وسائل القفل أو المسح عن بعد إذا كانت مفعلة ومناسبة، وغيّر بيانات الدخول المعرضة للخطر.

الإبلاغ والتعلم

الإبلاغ المبكر يقلل الضرر ويساعد على منع تكرار الحادث .بعد المعالجة، راجع سبب المشكلة وأعد ضبط الإجراءات الوقائية.

تنبيه

في بيئة الجامعة ينبغي الالتزام بتعليمات قسم تقنية المعلومات وعدم إجراء محاولات فحص أو اختراق على أجهزة الآخرين دون تصريح.

مراجعة شاملة وتطبيقات للطلبة

قواعد يومية مختصرة

حدّث النظام والتطبيقات؛ استخدم كلمات مرور فريدة ومصادقة إضافية؛ تحقق من الروابط؛ تجنب البرامج المجهولة؛ اقفل الجهاز؛ واحتفظ بنسخ احتياطية قابلة للاستعادة.

حالة دراسية أولى

استلم طالب رسالة تدعي أن حسابه الجامعي سيتوقف خلال ساعة وتطلب إدخال كلمة المرور . السلوك الصحيح هو عدم فتح الرابط، والدخول إلى البوابة الرسمية بصورة مستقلة، وإبلاغ الدعم المختص عند الحاجة.

حالة دراسية ثانية

احتفظت مجموعة بحثية بخرائطها على ذاكرة USB واحدة ثم تلفت .الدرس المستفاد هو تنظيم الملفات وإعداد نسخ احتياطية مستقلة واختبار استعادتها.

حالة دراسية ثالثة

ثبّت مستخدم برنامجاً مجانياً من موقع غير معروف وطلب البرنامج صلاحية الوصول إلى كل الملفات .ينبغي التحقق من المصدر والناشر وسبب الصلاحيات قبل الموافقة.

أسئلة للمناقشة

1.عرّف أمن الحاسوب واذكر أهدافه الثلاثة .2 .ما الفرق بين الفيروس والدودة وبرنامج الفدية؟ 3.كيف تتعرف على رسالة تصيد؟ .4 لماذا لا تكفي كلمة المرور وحدها؟ .5 ما الفرق بين المزامنة والنسخ الاحتياطي؟ .6 ما خطوات التصرف عند اختراق حساب؟

نشاط تطبيقي

يقسم الطلبة إلى مجموعات، وتُعطى كل مجموعة حالة تتعلق برسالة احتيالية أو جهاز مفقود أو ملف تالف .تحدد المجموعة التهديد والثغرة والإجراء الوقائي وطريقة الاستجابة.

خلاصة

أمن الحاسوب مسؤولية مشتركة بين التقنية والمستخدم .وتتحقق الحماية الفعالة عندما تجتمع المعرفة والسلوك السليم والتحديثات والنسخ الاحتياطي والاستجابة المبكرة للحوادث.