Chapter 2: Threats

- Introduction to Threats
- Physical Threats
- Social Engineering Attacks
- Insider Threats
- Network-Based Threats
- Malware, Spyware and Keyloggers
- Phishing, Email and Web-Based Threats
- Zero-Day Exploits

15

15

Introduction to Threats

- A threat is any event or action that could potentially cause harm to an **information system** or **network**.
- Threats can be **intentional** or **unintentional**, and they can be **physical** or **logical**.
- It is important to identify and **mitigate** threats in order to protect information systems and networks from harm.

مقدمةفي التهديدات

- التهديدهو أي حدث أو إجراء من المحتمل أن يتسببفي ضرر**نظام معلومات**أو**شبكة**.
- يمكنأن تكون التهديدات**متعمد**أو **غير مقصود**،ويمكن أن يكونوا كذلك**بدني** أو**منطقي**.
- منالمهم تحديد و**يخفف من** التهديدات منأجل حماية أنظمة وشبكات المعلومات منالأذى.

16

Physical Threats

- Physical threats are those that can cause damage to information systems or networks through **physical** means.
- Some examples of physical threats include:
  - Unauthorized access
  - Theft
  - Vandalism
  - Natural disasters
  - Power outages

التهديداتالجسدية

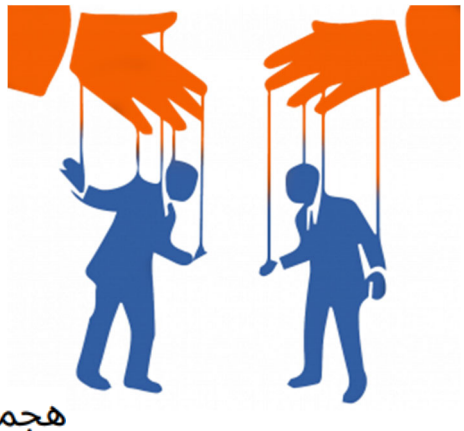
- التهديداتالمادية هي تلك التي يمكن أن تسببأضراراً لأنظمة المعلومات أو الشبكات من خلالها**بدني**وسائل.
- تتضمنبعض أمثلة التهديدات الجسدية ما يلي:
  - دخولغير مرخص
  - سرقة
  - التخريب
  - الكوارثالطبيعية
  - انقطاعالتيار الكهربائي

17

17

Social Engineering Attacks

- Social engineering attacks are those that **exploit** human **psychology** to trick people into revealing **sensitive** information or taking actions that harm information systems or networks.
- Some examples of social engineering attacks include:
  - Phishing
  - Impersonation
  - Tailgating



هجماتالهندسة الاجتماعية

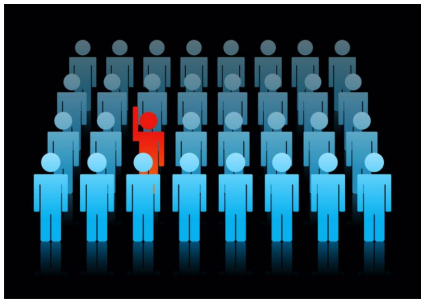
- هجماتالهندسة الاجتماعية هي تلك **يستغل** بشر**علم النفس**لخداع الناس لكي يكشفوا **حساس**المعلومات أو اتخاذ إجراءات من شأنهاالإضرار بنظم المعلومات أو الشبكات.
- تتضمنبعض الأمثلة على هجمات الهندسة الاجتماعيةما يلي:
  - التصيد
  - التمثيل
  - ذيل

18

18

Insider Threats

- Insider threats are those that are posed by **individuals** who have **authorized access** to information systems or networks.
- Insider threats can be **intentional** or **unintentional**, and they can be motivated by a variety of factors, such as **financial** gain, **revenge**, or **ideology**.



التهديداتالداخلية

- التهديداتمن الداخل هي تلك التي يطرحها **فرادى**الذين لديهم**الوصول المصرح به** لنظمالمعلومات أو الشبكات.
- يمكنأن تكون التهديدات الداخلية**متعمد**أو **غير مقصود**، ويمكن تحفيزهم من خلال مجموعة متنوعةمن العوامل ، مثل**مالي** يكسب،**انتقام**، أو**أيديولوجية**.

19

Network-Based Threats

- Network-based threats are those that exploit vulnerabilities in **communication** channels to attack information systems or networks.
- Some examples of network-based threats include:
  - **Man-in-the-middle** attacks
  - Denial of service (**DoS**) attacks
  - Distributed denial of service (**DDoS**) attacks

التهديداتالقائمة على الشبكة

- التهديداتالمستندة إلى الشبكة هي تلك التي تستغلنقاط الضعف في **تواصل**قنوات لمهاجمة أنظمة أو شبكاتالمعلومات.
- تتضمنبعض الأمثلة على التهديدات المستندة إلىالشبكة ما يلي:
  - **رجلفي الوسط**الهجمات
  - الحرمانمن الخدمة (**DoS**) الهجمات
  - رفضالخدمة الموزعة (**DDoS**) الهجمات

20

Malware

- Malware is **software** that is designed to **harm** information systems or networks.
- Malware can be delivered in a variety of ways, such as through email **attachments**, **downloads**, or **social engineering** attacks.
- Examples of malware include:
  - Viruses
  - Worms
  - Trojans
  - Ransomware

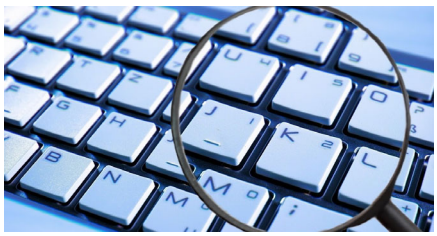
البرمجياتالخبيثة

- البرمجياتالخبيثة**برمجة**هذا مصمم ل **ضرر** نظمالمعلومات أو الشبكات.
- يمكنتسليم البرامج الضارة بعدة طرق ، مثل البريدالإلكتروني**المرفقات**و **التحميلات**، أو **هندسةاجتماعية**الهجمات.
- تتضمنأمثلة البرامج الضارة ما يلي:
  - الفيروسات
  - الديدان
  - حصانطروادة
  - برامجالفدية

21

Spyware and Keyloggers

- Spyware is software that is designed to **collect information** about a user **without** their knowledge or consent.
- Keyloggers are a type of spyware that **records** every keystroke that a user makes.
- Spyware and keyloggers can be used to steal **sensitive** information, such as **passwords**, credit card numbers, and **social security** numbers.



برامجالتجسس و Keyloggers

- برامجالتجسس هي برامج مصممة ل **جمع المعلومات**عن مستخدم **بدون**معرفتهم أو موافقتهم.
- كيلوغرزهي نوع من برامج التجسس **السجلات**كل ضغطة مفتاح يقوم بها المستخدم.
- يمكناستخدام برامج التجسس و keyloggers للسرقة**حساس**المعلومات ، مثل **كلمات السر**وأرقام بطاقات الائتمان و **الضمانالاجتماعي**أعداد.

Phishing and Email Threats

- Phishing is a type of social engineering attack in which attackers send **emails** that appear to be from **legitimate** sources in order to trick recipients into revealing sensitive information, such as **passwords** or credit card numbers.
- Email threats are any type of malicious content that is delivered through email, such as **malware**, phishing attacks, or **spam**.

تهديداتالتصيد الاحتيالي والبريد الإلكتروني

- التصيدهو نوع من هجمات الهندسة الاجتماعيةيقوم المهاجمون بإرساله**رسائل البريدالإلكتروني**التي يبدو أنها من**شرعي** لخداعالمستلمين للكشف عن معلومات حساسة ،مثل**كلمات السر** أو أرقام بطاقات الائتمان.
- تهديداتالبريد الإلكتروني هي أي نوع من أنواع المحتوى الضار الذييتم تسليمه عبر البريد الإلكتروني ، مثل**البرمجيات الخبيثة**أو هجمات التصيد الاحتيالي أو **رسائل إلكترونية مزعجة**.

23

Web-Based Threats

- Web-based threats are those that exploit vulnerabilities in **websites** and **web applications** to gain access to information systems and networks.
- Examples of web-based threats include:
  - **Drive-by downloads**
  - Cross-site scripting (XSS)
  - SQL injection

التهديداتالمستندة إلى الويب

- التهديداتالمستندة إلى الويب هي تلك التيتستغل نقاط الضعف في**المواقع**و **تطبيقاتالويب**للوصول إلى أنظمة وشبكاتالمعلومات.
- تتضمنأمثلة التهديدات المستندة إلى الويب ما يلي:
  - **منخلال التنزيلات**
  - البرمجةالنصية عبر المواقع (XSS)
  - حقنSQL

24

24

Zero-Day Exploits

ثغرات يوم الصفر هي ثغرات لا يعرفها بائع البرنامج ولا يتوفر لها تصحيح.

- Zero-day exploits are vulnerabilities that are **unknown** to the software **vendor** and for which there is no patch available.
- Zero-day exploits are often used in **targeted attacks**, such as those carried out by **nation-states**.

- ثغراتيوم الصفر هي نقاط ضعف موجودة**مجهول**للبرنامج **بائع**والتي لا يتوفرلها تصحيح.
- غالبأما تستُخدم ثغرات يوم الصفر في **الهجماتالمستهدفة**، مثل تلك التي نفذتها**الدول القومية**.

25

25

Botnets

- A botnet is a **network** of computers that have been **infected** with malware and are controlled by a single attacker.
- Botnets can be used to carry out a variety of malicious **activities**, such as **denial of service** attacks, spam campaigns, and data theft.

بوت نت

- الروبوتاتهي **أشبكة**من أجهزة الكمبيوتر التيتم**مصاب**ببرامج ضارة ويتحكم فيها مهاجمواحد.
- يمكناستخدام شبكات الروبوت لتنفيذ مجموعة متنوعةمن البرامج الضارة**أنشطة**، مثل **الحرمان من الخدمة**الهجمات وحملات البريد العشوائي وسرقةالبيانات.

26

26

Mitigation and Defense Strategies

- There are a number of mitigation strategies that can be used to protect against threats.
- Some of the most common mitigation strategies include:
  - Regular software updates
  - Strong authentication
  - User education
  - Backups

استراتيجيات التخفيف والدفاع

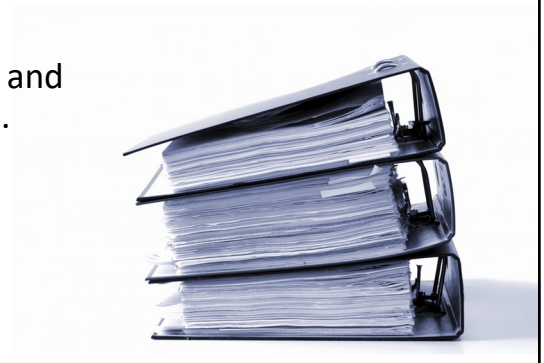
- هناك عدد من استراتيجيات التخفيف التي يمكن استخدامها للحماية من التهديدات.
- تتضمن بعض استراتيجيات التخفيف الأكثر شيوعاً ما يلي:
  - تحديثات البرامج العادية
  - مصادقة قوية
  - تعليم المستخدم
  - النسخ الاحتياطية

27

27

Case Studies

- Case studies can be a valuable tool for understanding the risks posed by threats and the **effectiveness** of mitigation strategies.
- Some of the most notable case studies include:
  - The Stuxnet attack
  - The WannaCry ransomware attack
  - The SolarWinds hack



دراسات الحالة

- يمكن أن تكون دراسات الحالة أداة قيمة لفهم المخاطر التي تشكلها التهديدات و**فعالية** من استراتيجيات التخفيف.
- تشمل بعض أبرز دراسات الحالة ما يلي:
  - هجوم Stuxnet
  - هجوم WannaCry ransomware
  - اختراق SolarWinds

28

28

Conclusion

التهديدات هي تحد مستمر ومتطور.

- Threats are a **constant** and **evolving** challenge.
- It is important to be aware of the different types of threats, to implement **mitigation** strategies, and to stay **up-to-date** on the latest security threats and vulnerabilities.

من المهم أن تكون على دراية بأنواع التهديدات المختلفة ، وتنفيذ استراتيجيات التخفيف ، والبقاء على اطلاع بأحدث التهديدات الأمنية ونقاط الضعف.

29

29