الحماية من الفيروسات والبرمجيات الخبيثة وهجمات التصيّد

المواضيع

البرمجيات الخبيثة

- ما هي البرمجيات الخبيثة Malware؟
- ما الذي تفعله البرمجيات الخبيثة Malware؟
- كيف يمكنك الحماية من البرمجيات الخبيثة Malware؟

هجمات التصيّد Phishing

- ما هي هجمات التصيّد Phishing؟
- آليات هجمات التصيّد Phishing
  كيف يمكنك الوقاية من الـ Phishing؟

- **البرمجيات المضادة للفيروسات Anti-virus applications**

- **جدران الحماية Firewalls**

المواضيع

- البرمجيات المضادة للفيروسات Anti-virus applications
- جدران الحماية Firewalls

البرمجيات الخبيثة Malware

ما هي البرمجيات الخبيثة Malware؟

- يأتي مصطلح Malware من كلمتين: **mal**icious soft**ware**، أي البرمجيات الخبيثة.

- برنامج مصمم خصّيصًا **لتعطيل** أو **إتلاف** أو **الحصول على وصول غير مصرح به** إلى أنظمة الحاسوب.

- عادة ما تنشئ هذه البرمجيات مجموعة من قراصنة الحاسوب hackers.

ما هي البرمجيات الخبيثة Malware؟

- عادةً ما تكون الغاية منها الحصول على منافع مادية
- يمكن أن تستخدم لأغراض سياسية، لفحص مدى قوة أنظمة الحماية، أو حتى كسلاح بين الدول

ما الذي تفعله البرمجيات الخبيثة Malware؟

- **الفيروس Virus:** الفيروسات تلحق نفسها بملفات "نظيفة" وتصيب ملفات نظيفة أخرى. يمكن أن تنتشر بشكل لا يمكن السيطرة عليها، وإلحاق أضرار بالوظائف الأساسية للنظام وحذف أو إتلاف الملفات. تظهر عادةً كملف قابل للتنفيذ (.exe).

- **أحصنة طروادة Trojans**: يظهر هذا النوع من البرامج الضارة كبرنامج سليم أو تتنكر وراء برامج مشروعة بعد أن يتم العبث بها.

- تتصرف هذه البرامج بشكل خفي وتقوم بإنشاء "أبواب خلفية" Backdoors للسماح بدخول برامج ضارة أخرى.

ما الذي تفعله البرمجيات الخبيثة Malware؟

- **برامج التجسس Spyware**: هي برمجيات خبيثة صممت خصيصا للتجسس على المستخدمين.

- تختبئ برامج التجسس في الخلفية ويراقب ما تفعله عبر الإنترنت، بما في ذلك كلمات المرور وأرقام بطاقات الائتمان وعادات التصفح والمزيد.

- **الديدان Worms**: تصيب الديدان شبكات من الأجهزة بشكل كامل، سواء أكانت الشبكة محلية أو عبر الإنترنت، وذلك باستخدام واجهات الشبكة. يستخدم كل جهاز مصاب على التوالي لإصابة الآخرين.

ما الذي تفعله البرمجيات الخبيثة Malware؟

- **برامج الفدية Ransomware**: عادةً ما تقوم هذا النوع من البرامج بمنعك من استخدام جهاز الحاسوب الخاص بك وملفاتك، ويهدد بمسح كل شيء ما لم تدفع فدية (مبلغًا ماليًا).

- **البرامج الإعلانية Adware**: على الرغم من أن البرامج الإعلانية العدوانية ليست ضارة دائمًا بطبيعتها، فإنها يمكن أن تؤثر على أمانك الرقمي لمجرد عرض إعلانات لك.

- **شبكات "البوت" Botnets**: هي شبكات من أجهزة الحاسوب المصابة المصممة للعمل معًا تحت سيطرة أحد المهاجمين.

كيف يمكنك أن تحمي نفسك من البرمجيات الخبيثة؟

- عندما يتعلق الأمر بالبرامج الضارة، فإن **الوقاية خير من العلاج**.

- لحسن الحظ، هناك بعض السلوكيات السليمة والتي يمكن أن تتبعها بسهولة للتقليل من احتمالات تعرضك لأي من هذه البرامج السيئة.

كيف يمكنك أن تحمي نفسك من البرمجيات الخبيثة؟

- **لا تثق بمن لا تعرفه على الإنترنت**
  - تعتبر "الهندسة الاجتماعية"، التي يمكن أن تشمل رسائل البريد الإلكتروني الغريبة والتنبيهات المفاجئة والحسابات الزائفة والعروض التي تثير الفضول، الطريقة الأولى لتوصيل البرمجيات الخبيثة.
  - إذا كنت لا تعرف بالضبط عن شيء ما، فلا تضغط عليه.
- **تأكد من الملفات التي تقوم بتنزيلها**
  - من المواقع التي تتيح محتوى "مقرصن" وغير أصلي إلى واجهات المتاجر الرسمية ، غالبًا ما تتواجد البرامج الضارة في الجوار. لذا ، قبل التنزيل ، تحقق دائمًا من أن الموفر جدير بالثقة من خلال قراءة التعليقات والتعليقات بعناية.

كيف يمكنك أن تحمي نفسك من البرمجيات الخبيثة؟

- **فعّل البرمجيات التي تمنع الإعلانات Ad-Blockers**
- زادت في الآونة الأخيرة الإعلانات الخبيثة Malvertising، حين يستخدم المخترقون إعلانات لإصابة جهازك. لا يمكنك معرفة الإعلانات الضارة: لذلك، فمن الأكثر أمانًا حظرها جميعًا باستخدام "مانع إعلانات" موثوق.

- **كن حذرا عندما تتصفح على الإنترنت**

- تتواجد البرامج الضارة في العديد من الأماكن، ولكنها أكثر شيوعًا في مواقع الويب التي تتميز بضعف أمان الواجهة الخلفية، مثل مواقع الويب الصغيرة وغير الموثوقة. إذا التزمت بالمواقع الكبيرة ذات السمعة الجيدة، فإنك تقلل بشدة من خطر مواجهتك للبرامج الضارة.

هجمات التصيّد

Phishing

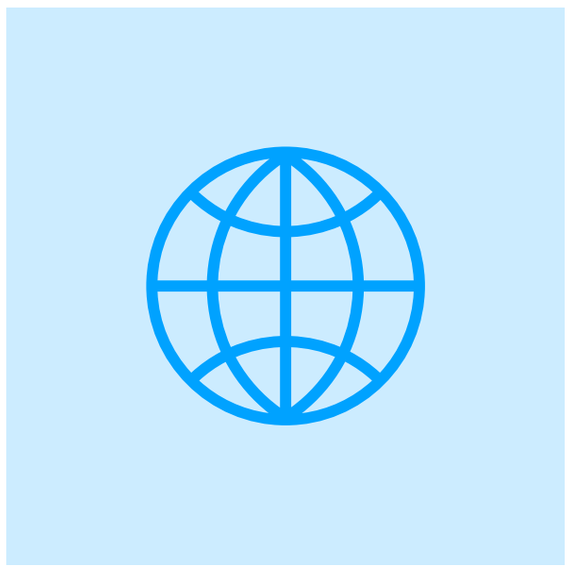
ما هي هجمات التصيّد؟

- جريمة إلكترونية يتم فيها إغراء أو خداع الصحية لتوفير بيانات حساسة:
- مثل معلومات التعريف الشخصية وتفاصيل الحسابات البنكية وبطاقات الائتمان وكلمات المرور.

- يظهر المهاجم بأنه مؤسسة شرعية وموثوقة.

- يتم التواصل مع الضحية عن طريق البريد الإلكتروني أو الهاتف أو الرسائل النصية.

أنواع شائعة من الخداع في هجمات التصيّد Phishing



آليات مستخدمة في هجمات التصيّد Phishing

الحماية من هجمات التصيّد Phishing

PHISHING

Social Engineering Red Flags

FROM

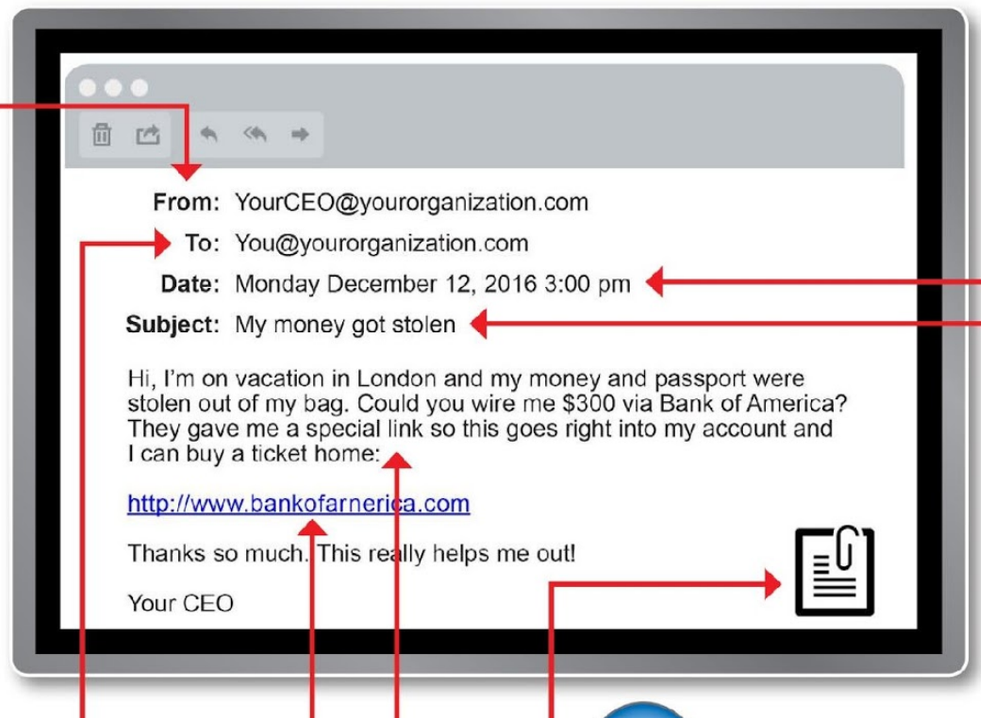
- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

TO

- I was cc'd on an email sent to one or more people, but **I don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."



DATE

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

SUBJECT

- Did I get an email with a subject line that is **irrelevant** or **does not match** the message content?
- Is the email message a reply to something **I never sent or requested**?

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

CONTENT

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence** or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

KnowBe4
Human error. Conquered.

البرمجيات المضادة للفيروسات

Anti-Virus

كيف تعمل البرمجيات المضادة للفيروسات Anti-Virus ؟

- **On-Access Scanning**
  - يعمل برنامج مكافحة الفيروسات في الخلفية ويتحقق من كل ملف تفتحه.
  - on-access scanning, background scanning, real-time protection.

- **Full System Scans**
  - تقوم معظم برامج مكافحة الفيروسات بإعداد عمليات فحص نظام كاملة مجدولة ، غالبًا مرة واحدة في الأسبوع.

- **Heuristics**
  - تسمح لبرنامج مكافحة الفيروسات بتحديد أنواع جديدة أو معدلة من البرامج الضارة، حتى بدون ملفات تعريف الفيروسات.

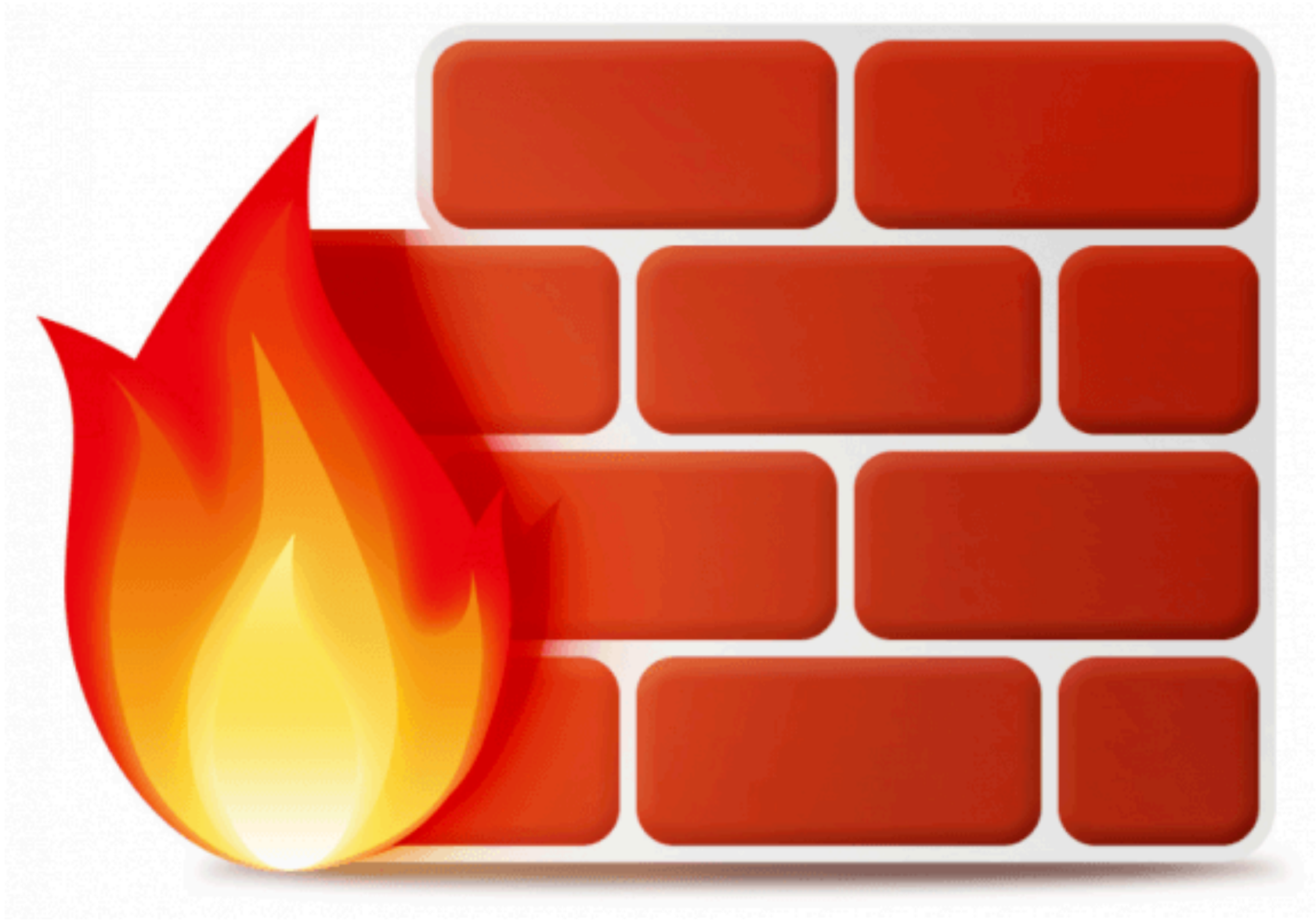
البرمجيات المضادة للفيروسات

Avast

https://www.avast.com/en-us/free-antivirus-download

Avira

https://www.avira.com/en/free-antivirus-windows



جدران النار
Firewalls