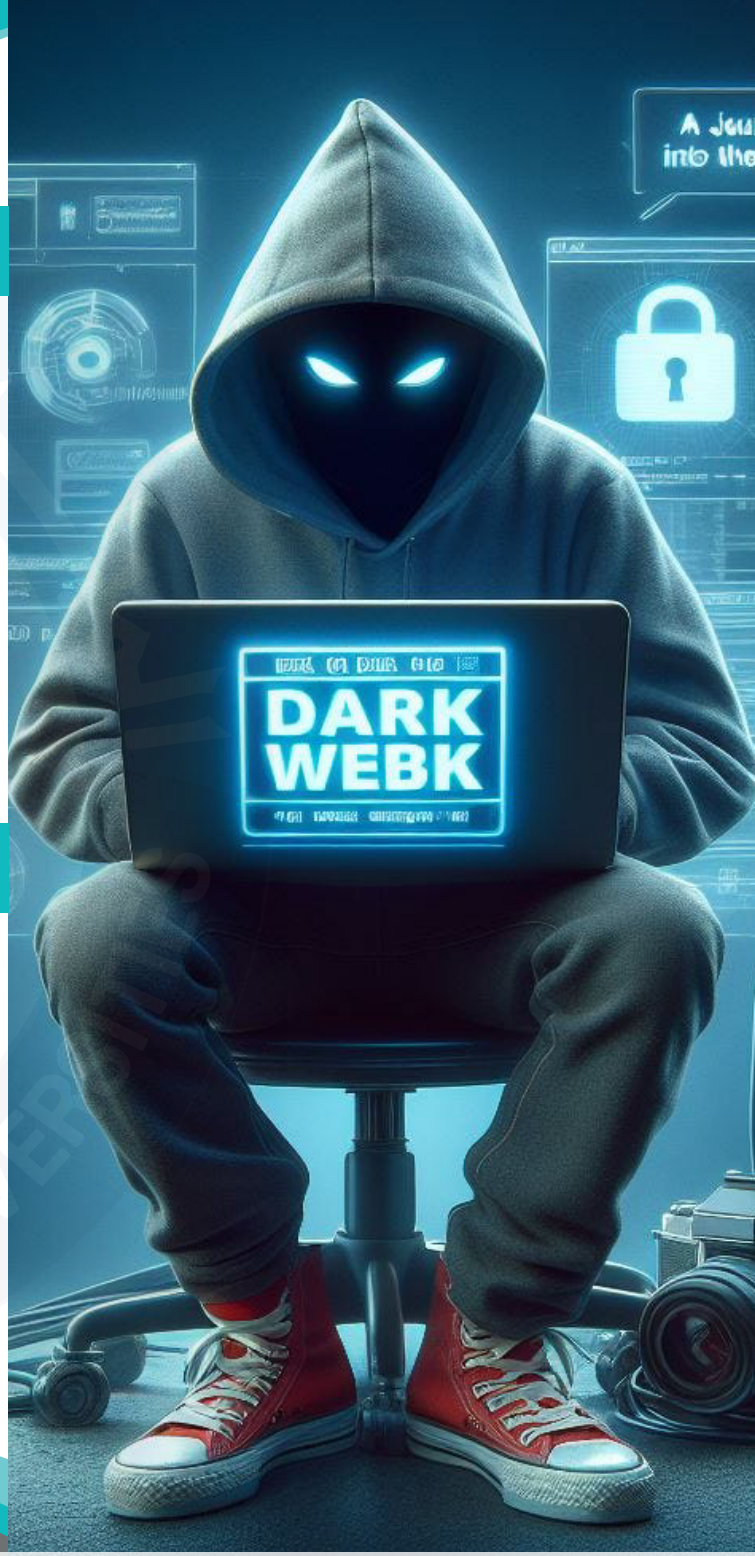
الويب المظلم (Dark Web)

هو جزء مخفي من مواقع الويب التي لا يمكن الوصول إليه من خلال محركات البحث التقليدية مثل جوجل. يتطلب الوصول إليه استخدام برامج خاصة والتي تخفي هوية المستخدم وتجعل من الصعب تتبع نشاطه.

ظهر الويب المظلم في الأصل كأداة للحفاظ على خصوصية المستخدمين وتصفح الويب بشكل آمن مثل الحكومات والصحفيين. ومع مرور الوقت، أصبح ملاذًا للأنشطة غير القانونية والمستخدمين الذين يبحثون عن الخصوصية المطلقة لإخفاء أنشطتهم المشبوهة خاصة أنه يصعب تتبع مقدمي الخدمة أو ناشري المحتوى على الويب المظلم.

مخاطر وتهديدات الويب المظلم

العديد من الأنشطة على الويب المظلم غير قانونية، ويمكن أن يؤدي التورط في مثل هذه الأنشطة إلى مشاكل قانونية سواء محلية أو دولية. بالإضافة إلى ذلك، هناك مخاطر أمنية تتعلق بالتعرض للهجمات الإلكترونية أو الاختراقات السيبرانية قد يتعرض لها مستخدمي الويب المظلم. ومن بين التهديدات الرئيسية للويب المظلم ما يلي:



أنواع الأنشطة على الويب المظلم

- **تجارة المخدرات والأسلحة:**
توجد أسواق كاملة مخصصة لبيع وشراء المخدرات والأسلحة بشكل غير قانوني.

- **التزوير والاحتيال المالي:**
يشمل ذلك بيع بيانات بطاقات الائتمان المسروقة وتزوير الوثائق الرسمية.

- **البرامج الضارة وبرامج الفدية:**
يمكن أن يصاب مستخدمي الويب المظلم ببرامج ضارة تؤدي إلى سرقة بياناتهم أو تشفيرها على أجهزتهم مقابل فدية مالية. هذه البرامج تشكل تهديدًا كبيرًا على أمن الأجهزة والمعلومات الشخصية.

- **التصيد الاحتيالي:**
تشمل محاولات لخداع المستخدمين للكشف عن معلومات شخصية مثل كلمات المرور والحسابات البنكية. غالبًا ما يتم تنفيذ هذه الهجمات عبر رسائل البريد الإلكتروني أو مواقع الويب المزيفة وتزداد هذه المحاولات على الويب المظلم.

- **سرقة الهوية:**
تتضمن سرقة المعلومات الشخصية واستخدامها لانتحال الهوية والذي يؤدي بدوره إلى عواقب وخيمة تشمل استخدام الهوية المسروقة في أنشطة إجرامية.

- **التورط في الأنشطة الإجرامية:**
يمُكن للمستخدمين التعرض للاعتقال أو الملاحقة القانونية إذا تورطوا في أنشطة إجرامية على الويب المظلم.

- **الأسواق السوداء:**
تشمل هذه الأسواق بيع كل شيء من الأدوية غير المرخصة إلى الأجهزة الإلكترونية المسروقة.

- **الخدمات غير القانونية مثل استئجار قراصنة:**
للقيام بأنشطة غير قانونية مثل اختراق الحسابات أو المواقع.

- **المعلومات المسربة والوثائق السرية:**
نشر وثائق حساسة أو بيانات مسروقة من الشركات أو الحكومات.

دراسات حالة وأمثلة واقعية

- **قضية سوق طريق الحرير (Silk Road):**

في عام ٢٠١١، أسس روس أولبريخت سوقًا على الويب المظلم يُدعى "طريق الحرير"، حيث يمكن للمستخدمين شراء وبيع سلع وخدمات غير قانونية. سرعان ما أصبح السوق شهيرًا، وجذب انتباه السلطات الأمريكية. بعد تحقيقات طويلة، تم القبض على أولبريخت في عام ٢٠١٣ وإغلاق الموقع. حُكم على أولبريخت بالسجن مدى الحياة، مما يبرز المخاطر القانونية الكبيرة المرتبطة بالأنشطة المشبوهة على الويب المظلم.

- **حادث طفل شبرا الخيمة:**

في مايو ٢٠٢٤، تم العثور على جثة طفل في منطقة شبرا الخيمة وتبين من التحقيقات أن الجريمة تم التخطيط لها وتنفيذها من خلال الويب المظلم. وتمت الجريمة بهدف بيع فيديو الجريمة على الويب المظلم مقابل مبلغ مالي كبير.

كيفية البقاء آمنًا على الإنترنت

- **تجنب الدخول الى الويب المظلم:**

لا تحاول الدخول الى الويب المظلم بدافع الفضول فقد يصاب جهازك ببرامج الضارة أو برامج الفدية بمجرد تحميل أحد الملفات أو الدخول على الروابط المشبوهة.

- **تجنب الوقوع في فخ التصيد الاحتيالي:**

يجب على المستخدمين التعرف على رسائل البريد الإلكتروني المشبوهة والروابط الضارة التي قد تؤدي إلى التصيد الاحتيالي. يجب دائمًا التحقق من عنوان البريد الإلكتروني والرابط قبل النقر عليه.

- **الحذر من مشاركة المعلومات الشخصية:**

تجنب مشاركة المعلومات الشخصية على الإنترنت والابتعاد عن المواقع التي تطلب بيانات شخصية دون سبب واضح. استخدم كلمات مرور قوية لكل حساب لحماية الهوية الرقمية.

يعد الويب المظلم جزءًا معقدًا ومتعدد الأوجه من الإنترنت له مخاطر كبيرة تتعلق بالأمان ومن المهم أن يكون المستخدمون على دراية بالتهديدات المحتملة وأن يتخذوا الاحتياطات اللازمة للحفاظ على سلامتهم وأمانهم أثناء التصفح. بالإضافة إلى ذلك، يجب أن يتم النظر في القضايا القانونية والأخلاقية بعناية لضمان استخدام التكنولوجيا بشكل مسؤول وآمن. يجب على الأفراد والمؤسسات العمل معًا لتعزيز الوعي والتثقيف حول استخدام الإنترنت بشكل آمن ومسؤول.