Ciberseguridad Web

Definición

La ciberseguridad web es la práctica de proteger sistemas, redes y datos de ataques cibernéticos en el contexto del internet. En otras palabras, se trata de las medidas que tomamos para garantizar la seguridad de nuestra información y dispositivos mientras navegamos, interactuamos y realizamos actividades en línea.

Amenazas Cibernéticas Comunes

Malware: Software malicioso que puede dañar dispositivos o robar información.

Phishing: Engaños en línea diseñados para robar información personal o financiera.

Ataques de ransomware: Secuestro de datos con la exigencia de un pago para su liberación.

Ataques de denegación de servicio (DDoS): Inundación de tráfico a un sitio web para hacerlo inaccesible.

Vulnerabilidades de software: Errores en el software que pueden ser explotados por piratas informáticos.

Tipos de permisos en el desarrollo

Permiso basado en roles

Permiso basado en atributos

Permiso basado en recursos

Permisos discrecionales

Permisos basados en listas de control de acceso (ACL)

Permisos heredados

Permisos obligatorios

Buenas Prácticas de Ciberseguridad

Crear contraseñas seguras y únicas para cada cuenta.

Activar la autenticación de dos factores (2FA).

Mantener el software actualizado.

Tener cuidado con los correos electrónicos y sitios web sospechosos.

No compartir información personal en línea.

Utilizar una red Wi-Fi segura.

Herramientas de Ciberseguridad

Software antivirus y anti-malware.

Firewalls.

VPN (Redes privadas virtuales).

Administradores de contraseñas.

Recursos adicionales

curso de ciberseguridad:

https://www.youtube.com/watch?v=w7T8CGHLOLE

https://www.youtube.com/@SEGURIDADCERO/playlists