

Guía de Navegación Segura en la Red

La seguridad en la red es fundamental para proteger su información y garantizar una experiencia de navegación segura. Este documento le proporcionará información esencial sobre las amenazas en línea y recomendaciones para evitar riesgos.

Tipos de Amenazas en la Red:

Malware

El malware abarca cualquier software malicioso diseñado para dañar, interrumpir o acceder a sistemas sin autorización. Incluye virus, gusanos, troyanos y spyware.

Spyware

Este tipo de malware recopila información sobre el usuario sin su conocimiento, como hábitos de navegación y datos personales. Puede interferir con el funcionamiento del dispositivo y comprometer la privacidad.

Spam

Se refiere a mensajes electrónicos no solicitados que se envían en masa. Aunque comúnmente asociado al correo electrónico, el spam también se presenta en redes sociales, foros y aplicaciones de mensajería.

Phishing

El phishing intenta obtener información confidencial haciéndose pasar por entidades legítimas. Esto se realiza a través de correos electrónicos o mensajes que se dirigen a sitios web falsos.

Pharming

Un ataque que redirige el tráfico de un sitio legítimo a uno fraudulento, buscando robar datos sensibles como contraseñas y números de tarjetas de crédito.

Recomendaciones de Seguridad:

Control de Malware

- Mantenga un antivirus actualizado y realice análisis periódicos.
- Instale software anti-spyware y bloqueadores de ventanas emergentes.

- Aplique actualizaciones de seguridad regularmente en sistemas operativos y navegadores.

Gestión del Correo Electrónico

- No publique su dirección de correo en sitios no confiables.
- No revele información confidencial por correo.
- Evite hacer clic en enlaces de correos sospechosos; verifique la URL manualmente.

Prevención de Phishing

- No responda a correos sospechosos que soliciten información personal.
- Revise los certificados SSL de los sitios web que visita.

Contraseñas Seguras

- Cambie sus contraseñas con regularidad y utilice combinaciones fuertes (mínimo 10 caracteres, incluyendo números y símbolos).
- No comparta sus contraseñas a través de correos electrónicos no seguros.

Mecanismos de Seguridad en Emprendetres:

Autenticación y Control de Acceso

Emprendetres implementa sistemas robustos de autenticación para asegurar que solo usuarios autorizados accedan a la red y servicios.

Protección de Red

- ***Firewall:*** Proporciona la primera línea de defensa contra amenazas externas.
- ***Antivirus y Antispam:*** Protege los dispositivos y servidores contra malware y correos no deseados.

Filtrado de Contenidos

Se utilizan servidores para bloquear el acceso a sitios peligrosos, incluyendo aquellos con contenido inapropiado.

Monitoreo Continuo

Realizamos un seguimiento constante de la red para detectar actividades inusuales y responder rápidamente a incidentes de seguridad.

La seguridad en la red es una responsabilidad compartida. Siga estas recomendaciones y esté atento a las amenazas para garantizar una experiencia de navegación segura. La prevención y la educación son sus mejores aliados en el mundo digital.