



Kern County Sheriff's Office Community Relations Unit

COMPUTER SECURITY AWARENESS

November 30th is National Computer Security Day. This day, is a call to action to protect computers, personal information, and online accounts from cyber threats.

SECURITY TIPS TO AVOID BEING A VICTIM

✓ Create Strong Passwords

Reusing, sharing, or exposing your passwords makes it easier for hackers to access multiple accounts if one is compromised.

✓ Research an app BEFORE downloading it

Be mindful of the permissions apps request, such as asking for more access than necessary. This is a red flag and can expose you to inappropriate content and scams.

✓ Do NOT overshare online

Strangers can obtain personal details like your birthdate, address, routines, or locations through upload times, shared location data, or identifiable landmarks in photos. Delay online uploads or schedule them for later.

✓ Do NOT avoid software updates

Unsecured apps and outdated protections can't defend against new cyber threats, making your device more vulnerable to attacks. Enable auto-updates.

✓ Do NOT click on phishing emails, links, ads, or click bait

Phishing is a common form of cyber attack where scammers impersonate legitimate entities to solicit personal information. Clickbait is used to drive traffic to a website or page and, in the worst cases, spread malware.

✓ Only Use Public WiFi & Bluetooth SAFELY

Attackers may steal login credentials, redirect users to fake sites, access accounts, and track activity on public networks. Research public networks before use, and disconnect when done to avoid threats. Leaving Bluetooth on can also make your device vulnerable to attacks.

PROTECT YOURSELF

- ✗ Avoid using personal information in your password.
- ✗ Avoid entering passwords on shared Wi-Fi.
- ✗ Avoid logging into important accounts on public networks.
- ✗ Avoid downloading Apps without prior research and from risky or unknown sites.
- ✗ Avoid posting vacation updates, identifiable landmarks, or location tags until after you have left the area.
- ✗ Avoid sharing personal or important information on profile bio's.

ONLINE REPORTING



KCSO

<https://www.kernsheriff.org/Reporting>



KCSO APP

Download today!



FBI

<https://www.ic3.gov/>

SCAN FOR MORE INFO

What's The
Harm?



Additional
Resources

Knowledgeflow.org



CONOCIMIENTO SOBRE LA SEGURIDAD INFORMÁTICA

El 30 de noviembre es el Día Nacional de la Seguridad Informática. Este día es un llamado a la acción para protegerlas computadoras, la información personal y las cuentas en línea de las amenazas cibernéticas.

CONSEJOS DE SEGURIDAD PARA EVITAR SER UNA VÍCTIMA

✓ Crea contraseñas seguras

Reutilizar, compartir o exponer tus contraseñas facilita que los hackers accedan a varias cuentas si una es comprometida.

✓ No evites las actualizaciones de software

Las apps sin protección y las defensas desactualizadas no pueden protegerte contra las nuevas amenazas cibernéticas, haciendo que tu dispositivo sea más vulnerable a los ataques. Activa las actualizaciones automáticas.

✓ NO compartas demasiado en línea

Los desconocidos pueden obtener datos personales como tu fecha de nacimiento, dirección, rutinas o ubicaciones a través de los momentos en que realizas publicaciones, los datos de ubicación compartidos o los puntos de referencia identificables en las fotos. Retrasa las publicaciones en línea o prográmalas para más tarde.

✓ Investiga una app ANTES de descargarla

Ten cuidado con los permisos que solicitan las aplicaciones, como pedir más acceso del necesario. Esto es una señal de alerta y puede exponerte a contenido inapropiado y estafas.

✓ NO hagas clic en correos electrónicos de phishing, enlaces, anuncios o cebo de clics

El phishing es una forma común de ciberataque donde los estafadores se hacen pasar por entidades legítimas para solicitar información personal. El ciberanzuelo se usa para atraer tráfico a un sitio web o página y, en los peores casos, para difundir malware.

✓ Usa WiFi público y Bluetooth solo de manera segura

Los atacantes pueden robar credenciales de inicio de sesión, redirigir a los usuarios a sitios falsos, acceder a cuentas y rastrear la actividad en redes públicas. Investiga las redes públicas antes de usarlas y desconéctate cuando termines para evitar amenazas. Dejar el Bluetooth activado también puede hacer que tu dispositivo sea vulnerable a ataques.

CÓMO PROTEGERTE

- ✗ Evita el uso de información personal en tu contraseña.
- ✗ Evita ingresar contraseñas en WiFi compartida.
- ✗ Evita iniciar sesión en cuentas importantes durante el uso de redes públicas.
- ✗ Evita descargar aplicaciones sin investigar antes y de sitios riesgosos o desconocidos.
- ✗ Evita publicar actualizaciones de tus vacaciones, lugares reconocibles o etiquetas de ubicación hasta que hayas salido del área.
- ✗ Evita compartir información personal o importante en la biografía del perfil.

REPORTE EN LÍNEA



KCSO

<https://www.kernsheriff.org/Reporting>



APP de KCSO

¡Descarga hoy!



FBI

<https://www.ic3.gov/>

ESCANEA PARA MÁS INFORMACIÓN

¿Qué daño
hace?



Knowledgeflow.org

Recursos
adicionales