Gestión de abusos

TABLA DE CONTENIDO

Mejores prácticas para usar software de acceso remoto

Esquemas ejecutados actualmente

Autoridades y gestión de abusos

Este artículo describe mejores prácticas sencillas a seguir al usar software de Acceso Remoto, destaca escenarios comunes de mal uso y explica cómo detectar y reportar actividades sospechosas. Seguir estas pautas asegura una experiencia de Escritorio Remoto más segura y confiable.

Mejores prácticas para usar software de acceso remoto

1. **Verifique la autenticidad del sitio web**
   Asegúrese siempre de que los sitios web que visita sean auténticos. Tenga cuidado con las páginas de phishing y las descargas maliciosas que pueden comprometer sus datos.

2. **Sea escéptico ante ofertas de acceso remoto**
   Los funcionarios legítimos nunca solicitarán acceso remoto a su dispositivo sin que usted lo pida. Siempre desconfíe de tales solicitudes.

3. **Proteja sus códigos de acceso**
   Nunca comparta los códigos de acceso a sus dispositivos con nadie. Esto es crucial para mantener su seguridad.

4. **Ignore intentos de llamadas en frío**
   No responda a intentos de llamadas no solicitadas. Los estafadores a menudo usan esta táctica para obtener acceso no autorizado.

5. **Restrinja el acceso solo a partes de confianza**
   Solo conceda acceso remoto a personas de confianza. Tenga especial cuidado con individuos

que afirman ser de empresas legítimas.

6. **Solicite verificación de identidad**
   Siempre pida credenciales de identidad a cualquiera que solicite acceso a su dispositivo. Verifique su legitimidad antes de proceder.

7. **Cuidado con las llamadas no solicitadas**

   No interactúe ni proporcione información a personas que llamen desde orígenes desconocidos. Los estafadores pueden intentar extraer información confidencial de esta manera.

8. **Proteja la información confidencial**
   Nunca revele información confidencial, incluidas credenciales bancarias, a desconocidos o partes no verificadas.

9. **Reconozca las prácticas legítimas de las empresas** Las empresas legítimas nunca lo llamarán en frío para resolver un problema. Siempre inicie el contacto usted mismo si necesita asistencia.

10. **Reporte la actividad de estafadores**
    Si encuentra estafadores, registre todos los detalles y reporte el incidente a las autoridades locales de inmediato.

Siguiendo estas mejores prácticas, puede ayudar a protegerse de posibles amenazas de seguridad y garantizar una experiencia de escritorio remoto más segura.

Esquemas ejecutados actualmente

1. Robo de dinero a través de sesiones móviles en India:
   - Los estafadores extraen datos durante sesiones móviles para robar dinero. Para más detalles, consulte la Advertencia del RBI.

2. Falsos técnicos de Microsoft:
   - Los estafadores se hacen pasar por técnicos de Microsoft, alegando que necesitan limpiar su dispositivo de software malicioso. Recuerde, Microsoft nunca lo llamará en frío por tales problemas.

3. Suplantación de empresas legítimas:

- Los estafadores a menudo intentan ganarse su confianza fingiendo representar a empresas legítimas. Siempre sea escéptico ante el contacto no solicitado.

4. Falsos reclamos de soporte de AnyDesk:
    - Los estafadores pueden hacerse pasar por soporte de AnyDesk, alegando resolver errores en Windows, incluso si está usando un dispositivo macOS.

> 🚨 **IMPORTANTE**
>
> AnyDesk solo responderá a tickets de soporte que usted inicie. Además, proporcionamos soporte exclusivamente para problemas relacionados con el software AnyDesk y no damos soporte a software o productos de terceros.

Autoridades y gestión de abusos

En AnyDesk, tomamos el abuso en serio y cooperamos estrechamente con las autoridades policiales para combatir actividades fraudulentas. Los usuarios que se encuentren violando nuestros términos de uso serán bloqueados tras su identificación.

Trabajando juntos, podemos ayudar a asegurar un entorno más seguro y protegido para todos los usuarios.

Artículos relacionados:

- Reportar Estafa Microsoft
- Reportar Estafa Google

La capacidad de acceder y controlar un dispositivo desde una ubicación diferente usando AnyDesk, facilitando el soporte remoto y el trabajo.

La capacidad de acceder y controlar un dispositivo desde una ubicación diferente usando AnyDesk, facilitando el soporte remoto y el trabajo.