cisco SECURE Partner

PROTÉJASE CONTRA EL CIBERDELITO

CLAVES PARA PREVENIR ATAQUES

1

Mantenga la información personal privada

En las manos equivocadas, su información personal (es decir, fecha de nacimiento, apellido de soltera, identificación del pasaporte, etc.) puede provocar el robo de identidad y causar estragos en sus finanzas, crédito y bienestar mental.

2

Tenga cuidado para evitar ciberdelincuentes

Los ciberdelincuentes se han vuelto más sofisticados y vienen en todas formas y tamaños. Tenga cuidado con el phishing de correo electrónico, el smishing de texto y otras técnicas de ingeniería social que los malos actores están integrando en nuestra vida cotidiana. Tómese un momento para revisar quién está en el otro extremo de su comunicación antes de

En caso de duda:

- Verifique las direcciones de correo electrónico
- Tenga cuidado con los enlaces o archivos adjuntos incrustados
- Nunca proporcione información personal por correo electrónico o por teléfono
- Ir directamente al sitio web de la empresa para hacer un seguimiento de un mensaje en lugar de responder a través de un enlace interno
- Manténgase alerta y tenga cuidado cuando se le pida que haga

Los ciberdelincuentes a menudo usan:

- Mala gramática
- Una sensación de urgencia, miedo, curiosidad o codicia
- Ciertos comportamientos para obtener información personal, incluida su contraseña
- Ofertas que son demasiado buenas para ser verdad
- "Estimado señor/señora" y otros saludos genéricos

3

Actualice el Software regularmente

Los ciberdelincuentes buscan constantemente oportunidades en software sin parches. Mantenga su software actualizado: es una de las herramientas de seguridad más efectivas que tiene. Mejor aún, habilite las actualizaciones automáticas, para que nunca tenga que pensar en ello.

4

Cree contraseñas seguras usando paráfrasis

Todos tenemos docenas de contraseñas. Cualquier ciberdelincuente que adivine solo una puede acceder rápidamente a mucha información personal, desde tus datos bancarios a tu domicilio. Las estadísticas muestran que más de 280.000 contraseñas son robadas cada día.

Recomendaciones para contraseñas seguras:

- Las contraseñas más largas siempre son mejores. Apunta a por lo menos 14 caracteres
- Elije frases inusuales que sean fáciles para que recuerdes que incluyen números y símbolos
- Nunca use la misma contraseña para múltiples cuentas
- Para mejores resultados, use un administrador de contraseñas para crear y almacenar

5

Utilice la verificación de dos pasos siempre que sea posible

Verificación en dos pasos, también conocida como autenticación multifactor (MFA) o autenticación de dos factores, fortalece la seguridad al exigir formas adicionales de verificar su identidad más allá de su ID de usuario y clave. Estas capas añadidas ayudan a proteger contra el phishing, ingeniería de redes sociales y ataques de fuerza bruta de contraseñas.

TIP Pruebe Duo, la solución segura de autenticación de dos factores de Cisco.

boyra
comunica tus sueños

TELEFONOS: 57 6019156130, 57 350 6137478
DIAGONAL 61c Bis # 24-44 BOGOTA
WWW.BOYRA.COM

cisco SECURE Partner

PROTÉJASE CONTRA EL CIBERDELITO

CLAVES PARA PREVENIR ATAQUES

6 Tenga cuidado con el WIFI gratuito

Los ciberdelincuentes pueden piratear Wi-Fi gratuito o público para descubrir los sitios web que está visitando y capturar la información, incluida la información personal, que envía a través de la red.

Si debe usar Wi-Fi gratuito, evite los sitios web que usan y conservan sus datos personales:

- Banca en línea
- Cuentas escolares
- Medios de comunicación social

7 No deje su huella cibernética en dispositivos compartidos o públicos

Al usar una computadora pública o cualquier dispositivo que no sea el suyo, otro usuario puede acceder a sus datos y cuentas. Antes de cerrar la sesión, asegúrese de:

- Deshabilite cualquier opción para "guardar contraseñas"
- Salga de sus cuentas cuando termine
- Eliminar cookies, caché e historial de navegación

8 Administre su configuración de privacidad

Asegure su huella cibernética administrando la privacidad y la seguridad configuración en sus dispositivos, servicios en línea y aplicaciones. De esa manera, solo está compartiendo la información que se requiere, y nada más.

9 Audite regularmente las aplicaciones instaladas

Ya que la configuración de privacidad puede cambiar con las actualizaciones.

Algunas aplicaciones móviles pueden tener acceso a más información de la que cree. Antes de descargar una nueva aplicación, preste mucha atención a los permisos que requiere.

¿De verdad quieres que esa aplicación capture datos de tu:

- Rollo de la cámara
- Micrófono
- Pulsaciones de teclas.

10 Aseguremos el mañana, juntos

Comparta su conocimiento para ayudar a otros a ser más Cisco Ciberseguro.

- Necesitamos algunos de sus datos personales para que pueda usar nuestras soluciones y para brindarle soporte de garantía, soporte técnico y otros servicios.
- Algunos datos personales pueden ayudarnos a brindarle mejores consultas, análisis y conocimientos de expertos para que obtenga el máximo valor de nuestros productos y servicios.
- Podemos ayudarlo a tomar mejores decisiones de compra, renovar productos y hacer negocios.
- Si se reciben datos personales en relación con la información de los sistemas utilizados para mejorar nuestras soluciones, esta se tratará de acuerdo con la ley de datos personales aplicable, y sus contratos y acuerdos con nosotros. Para más información visite: Cisco Trust Portal

Déjenos ayudarlo a protegerse: contacto@boyra.com

boyra comunica tus sueños

TELEFONOS: 57 6019156130, 57 350 6137478
DIAGONAL 61c Bis # 24-44 BOGOTA
WWW.BOYRA.COM