Edición 2024

CIBER-GUÍA 2024

Practicando la ciberseguridad sin pánico en este año

MAD CONSULTING

Saludos,

Al comienzo de cada año nos proponemos muchas metas. Comencemos este 2024 practicando la ciberseguridad sin pánico.

Esta guía es la ideal para comenzar en la protección de tu mundo digital. Diseñada pensando en ti, que estás dando los primeros pasos en el este mundo digital.

Algunas de las razones por las cuales esta guía es ideal para ti:

- Lenguaje ameno
- Enfoque en lo fundamental
- Aplica a tu vida diaria
- Paso a Paso
- Recursos adicionales

La ciberseguridad puede ser simple y efectiva, y esta guía es tu compañera perfecta para empezar este viaje de forma segura y confiada.

¡Adelante, descubre cómo proteger tu presencia en línea libre de pánico!
Tu guía,

Melissa

¿QUÉ ES CIBERSEGURIDAD?

La ciberseguridad se enfoca en proteger a los dispositivos e información de mal uso, robo y daño.

La mayoría de las veces no sabemos por dónde comenzar. Comienza preguntándote si estás al pendiente de estas tres áreas:

- ¿Mis dispositivos están cubiertos?
- ¿Mis cuentas están protegidas?
- ¿Estoy cuidando la información de los demás?

La seguridad en línea es crítica en esta era digital en la que vivimos. Ya todo lo que hacemos y donde interactuamos tiene una presencia en línea. Algunas razones que la importancia de mantenerse seguro en línea son:

1. Protección de la Información Personal, documentos, etc.
2. Prevención de robo de identidad
3. Protección contra ciber-amenazas
4. Asegurar las finanzas
5. Cuidado de reputación y marca
6. Cumplir con las leyes y regulaciones

En resumen, no es necesario que te conviertas en una persona experta en ciberseguridad, pero que al menos conozcas lo esencial para cubrir tus riesgos y crear hábitos que te ayuden a practica la ciberseguridad sin pánico.

La ciberseguridad es asunto de todos.

-Melissa A. Delgado

AMENAZAS

Frecuentemente veo cómo se habla de la ciberseguridad como algo a temer, algo que sólo es entendido por personas dedicadas a la tecnología. Sin embargo, eso está muy lejos de lo cierto.

La clave para que seamos personas ciberseguras está en ejercitar las mejores prácticas, mantenerse al día en los cambios y conocer las amenezas del diaro en donde interactuamos para protegernos adecuadamente.

Cada vez que interactuamos en línea exponemos nuestra información personal, la de los nuestros y más. Amenazas como lo son virus, malware, estafas, enlaces maliciosos nos acechan. A continuación te explico brevemente las más comunes.

- **VIRUS -** programas maliciosos diseñados para replicarse y dañar archivos o en tu dispositivo.
- **MALWARE -** abarca varias amenazas, desde spyware que rastrea tu actividad hasta adware que muestra anuncios no deseados.
- **PHISHING -** táctica engañosa en la que los estafadores se hacen pasar por personas o entidades confiables con el fin de tener tu información (hay variedad de términos para este tipo de amenaza basado en cómo se genera el contacto).
- **RANSOMEWARE -** cifra tus archivos y exige un rescate para su liberación.
- **CIBER-DEPREDADORES -** personas que cometen abuso sexual infantil, entre otras ofensas, que comienza o tiene lugar en Internet.

Esta guía está diseñada para que puedas conocer lo básico y puedas comenzar a accionar, pero si deseas información detallada sobre amenzas y más, te invito a obtener mi libro *Ciberseguridad...en arroz y habichuelas*, donde te muestro en lenguaje sencillo desde como desarrollar ciber-higiene hasta como crear tu coraza de protección.

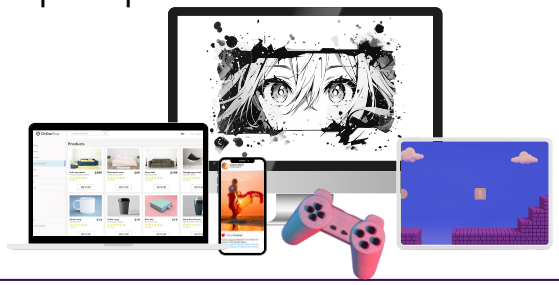
PROTEGE LO TUYO

Al mencionar el proteger nuestros dispositivos, nos llega a la mente celular, laptop y tablets. Pero para efectos de practicar la ciberseguridad responsablemente debes considerar que dispositivo es todo aquello que utilizas para interactuar en línea, almacenar datos, etc. Además de los dispositivos, también debemos proteger nuestras cuentas e información.

Comienza pasando inventario de los dispositivos y cuentas que utilizas a diario y desarrolla los siguientes hábitos:

- Separa tus cuentas personales de las de negocio
- Mantén tus dispositivos y cuentas actualizadas
- Actualiza tus configuraciones de seguridad y privacidad
- Activa la Autenticación Multi-Factor (MFA, por sus siglas en inglés)
- Usa contraseñas únicas y seguras (no las compartas)
- Desactiva la abilidad de rastreo
- Configura los controles parentales
- No utilices Wi-Fi público y si tienes que hacerlo activa tu VPN (Red Privada Virtual, por sus siglas en inglés)
- Interactúa sólo en websites confiables y seguros (https)
- Establece un plan de back-up (resguardo)
- Evita abrir enlaces de desconocidos
- No contestes llamadas, textos, emails de desconocidos
- Evita sobrecompartir información
- Mantén privadas las cuentas personales de redes sociales
- Controla el uso de tu información por websites y applicaciones
- Ten la ciber-conversación con tus menores desde temprana edad

En mi libro Ciberseguridad...en arroz y habichuelas, te ofrezco más detalles y una lista de dispositivos que puedes utilizar para pasar inventario.



CASOS REALES

Aprendamos de casos reales* que muestran consecuencias cuando no se practica la ciberseguridad adecuadamente. Esta es la base de todo, si sabemos cómo evitar caer en riesgo y tomar las medidas necesarias, entonces aumentamos nuestra protección en línea .

CASO #1

Mirta fue víctima de robo de identidad después de hacer clic en un enlace de phishing aparentemente inofensivo. Los ciber-criminales obtuvieron acceso a su información personal impactando su historial de crédito, creando deudas y más.

- **AMENAZA**: Phishing
- **CIBER-PRÁCTICA:** No abrir enlaces de desconocidos o sospechosos.

CASO #2

Pedro fue víctima de fraude financiero al hacer una compra en un website que no cumplía con los estándares de seguridad, dando paso a que los criminales obtuvieran toda su información bancaria.

- **AMENAZA**: Fraude
- **CIBER-PRÁCTICA:** Verifica el website antes de entrar información personal y sólo entra en aquellos confiables. Busca que comiencen con "https" entre otros.

CASO #3

Nana fue víctima malware al bajar una aplicación sin antes verificarla ni haber descargado la última actulización en su dispositivo, perdiendo así todas las fotos que tenía de sus abuelitos y familiares que son irrecobrables.

- **AMENAZA**: Malware
- **CIBER-PRÁCTICA**: Mantén actualizados a tus dispositivos y sólo descarga programas de compañias confiables.

CASO #4

Cukis4u tuvo un ataque de ransomware que paralizó sus operaciones durante días. Los ciber-criminales cifraron sus archivos y exigieron un rescate de alto valor. Impactando sus ventas y la reputación ante sus clientes, 6 meses después del ataque, Cukis4u cerró operaciones.

- **AMENAZA**: Ransomware
- **CIBER-PRÁCTICA:** Tener un plan y medidas adecuadas en la protección de dispositivos y sistemas en tu negocio, no importa su tamaño.

CASO #5

Sasha se encontró con una amiguita que había conocido en jugando en línea, para su sorpresa era un adulto malintencionado.

- **AMENAZA**: Ciber-depredación
- **CIBER-PRÁCTICA:** Tener la ciber-conversación con menores, activar controles parentales, cuentas de juegos en línea privadas y monitorear su actividad en línea.

*Todos los nombres han sido cambiados.

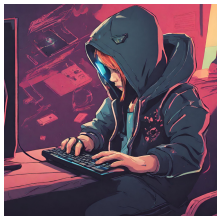
NUESTROS MENORES

Proteger a nuestros menores en línea es responsabilidad de todos (padres, cuidadores, educadores, comunidad). Al educar, tener una comunicación abierta y establecer límites claros, podemos ayudarlos a navegar el ciberespacio en una forma segura y responsable no importa su edad.

Desde ciber-acoso (cyberbullying) hasta la ciber-depredación (online predator), muchas son las razones por las cuales debemos tener la ciber-conversación con nuestros menores y establecer medidas de seguridad. A continuación te comparto medidas con las que puedes comenzar para desarrollar ese músculo de ciberseguridad para ti y los tuyos.

- Comienza ciber-conversación con tus menores desde temprana edad. Háblales sobre no compartir información personal (nombre, dirección, telefono, etc.), ten una comunicación abierta en los riesgos y toma de decisiones (buscar ayuda de adulto, bloquear cuentas, y más).
- Antes de darles un dispositivo, actualizalos y configura su nivel de seguridad y privacidad.
- Activa los controles parentales y filtros de contenido de acuerdo a su edad.
- Juegos en línea apropiados para su edad, configurado en modo privado, evitando chats o divulgación de información a desconocidos.
- Redes sociales seguras incluyendo sus cuentas siempre en modo privado.
- Conoce las plataformas donde interactúan en línea y supervisa periodicamente sus actividades.
- Establece límite de edad, tiempo, uso y tiempo de desconexión (unplugging time)

La clave es involucrarte activamente en la vida digital de los niños y ser un recurso de apoyo.


TEN UN PLAN

Ya seas un invividuo o negocio, el tener un plan es parte de tu ciberseguridad. El momento va llegar en el que seremos víctimas, la diferencia va a ser nuestra preparación para enfrentar los riesgos, manejar la situación y capacidad para sobrellevar las consecuencias.

Cada vez son más las estafas a personas de mayor edad, emprendedores y negocios pequeños. Principalmente porque el criminal sabe que no poseen las finanzas para contrarrestar un ataque, no importa su magnitud. Cuando hablamos de menores, el precio en algunos casos es muy alto a pagar. Es por eso que debes tener un plan de acción para evitar y sobrepasar un ciber-ataque. Aquí te muestro algunos a considerar e implementar:

- Ten un código secreto familiar para evitar fraude por mensajes o llamadas.
- Haz back-up (resguardo) de todos tus datos. No *pongas todos los huevos en una canasta*, el back-up no puede estar en la misma localización que tu datos.
- Separa presupuesto para cualquier remediación en caso de un ataque.
- Si tienes negocio, usa políticas de acceso a información sensitiva tanto de la compañía como la de tus clientes.
- Ten contactos de profesionales de tecnología que te puedan asistir de manera efectiva.
- Crea comunicados (a nivel personal o empresarial) que enviarás a tus allegados o clientes en caso de un ataque (robo de cuenta, uso de tu número de cel, bloqueo de redes sociales, etc.)

Tener un plan no es una comodidad sino una necesidad, estar preparado para estros casos ayudará grandemente en el nivel de impacto que experimentarás en el proceso.

EDÚCATE

La tecnología cambia constantemente y las amenazas evolucionan con ella, por eso es importante que te conviertas en una persona informada y al día de lo que sucede en el mundo digital.

Aquí algunas de los pasos que puedes comenzar a añadir a tu rutina para mantenerte informado y al día:

- Website confiables que ofrezcan noticias sobre ciberseguridad.
- Foros y comunidades en línea que compartan experiencias.
- Adiestramiento en tu trabajo sobre las mejores prácticas en línea y manejo de dispositivos.
- Canales, podcasts y videos educativos.
- Si te interesa incursionar en el mundo de la ciberseguridad, puedes encontrar programas de certificacion.
- Participar de eventos, conferencias y aprende de expertos.

La ciberseguridad requiere un compromiso constante con la educación y la conciencia. Mantente informado sobre las últimas amenazas y técnicas de protección y encuentra oportunidades para mejorar tus habilidades y conocimientos. La educación continua no sólo te hace más competente en la defensa de tu vida digital, sino que también te permite estar un paso adelante en un mundo en constante evolución. ¡Sigue aprendiendo y mantente seguro, estoy para ayudarte!

CONECTA CONMIGO

¡Felicidades por llegar hasta el final de nuestra guía! Espero que hayas encontrado información útil para comenzar a practicar la ciberseguridad sin pánico.

Gracias por la oportunidad de seguir conectando contigo y compartir más contenido inspirador. ¡Gracias por ser parte de esta increíble comunidad!

Si quieres seguir en contacto y obtener aún más recursos, consejos y actualizaciones exclusivas, ¡estoy aquí para ti! Conecta conmigo en mis redes sociales para seguir la conversación y formar parte de nuestra comunidad. Además, no te pierdas de lo último y contenido exclusivo visitando nuestra página.

@MADelgadoConsulting

@MADConsultingTV

Ciberseguridad y más

@MADelgado-Consulting

MADelgadoConsulting.com

Contactos

La ciberseguridad es asunto de todos.

-Melissa A. Delgado

MAD CONSULTING