MASTER YOUR CARD

EMPOWERING YOUR COMMUNITY

LA PREPARACIÓN CIBERNÉTICA ES FUNDAMENTAL PARA PROPIETARIOS DE NEGOCIOS

Un ataque cibernético afecta más que sus resultados; también puede afectar la reputación de su organización. En el mundo conectado de hoy, empresas de todos los tamaños pueden ser vulnerables a los ataques cibernéticos. Todas las organizaciones están conectadas en el mundo digital de hoy y la seguridad cibernética es tan fuerte como su eslabón más débil. De hecho, el 60% de los ataques cibernéticos se dirigen a pequeñas y medianas empresas (PYMES).

Una violación a la seguridad cibernética de su organización puede dañar a sus clientes, socios y empleados. Comprender estos riesgos y proteger a su organización es el primer paso para crear una organización con la preparación cibernética adecuada. Por eso es importante prepararse, protegerse y tener la preparación cibernética adecuada.

Autenticación

Las contraseñas son los guardianes de su información más importantes. Los atacantes cibernéticos son oportunistas y pueden descifrar fácilmente una contraseña débil.

CONSEJOS: Cada vez que cree una contraseña, debe tratar de hacer lo siguiente:

- Use caracteres en mayúscula y minúscula
- Use Números (0 a 9)
- Incluya caracteres no alfanuméricos
- No use información personal como fecha de nacimiento, nombres, etc.
- Nunca use la misma contraseña en varios sitios
- Cambie las contraseñas con regularidad (cada tres meses)
- No comparta contraseñas

El **63%** de las violaciones de datos se deben a contraseñas débiles o robadas.

90% de las contraseñas de los empleados puede ser violada en seis horas por los piratas informáticos.

Más del **20%** de los empleados comerciales han compartido su contraseña con asistentes o compañeros de trabajo.

El **81%** de las infracciones relacionadas con la piratería son el resultado de contraseñas robadas y / o débiles.

Phishing

Con esta táctica, intentarán que comparta información confidencial como contraseñas o que haga clic en un enlace o en un archivo adjunto. Esto puede poner software malicioso en su computadora, lo cual pone en riesgo su identidad u organización.

CONSEJOS: Verifique el remitente. Nunca comparta información confidencial. En caso de duda, no haga clic.

El **91%** de todos los ataques cibernéticos comienzan con un correo electrónico de phishing.

El **89%** de los ataques de phishing imitan los correos electrónicos corporativos.

88% de las organizaciones experimentaron ataques de phishing en 2019.

El **81%** de las empresas que cayeron en un ataque de phishing perdieron clientes.

84% de los ataques phishing están dirigidos a pequeñas empresas.

USB/Medios Removibles

Las memorias USB y otros tipos de medios removibles son una forma útil de compartir información, pero a menudo están infectados con software malintencionado que puede dañar sus sistemas, y no hay forma de saberlo hasta que es demasiado tarde. Así que sea USB inteligente.

CONSEJOS: Compre siempre unidades de memoria de fabricantes y vendedores confiables o considere desechar su USB y moverse a la "Nube" para el almacenamiento de archivos. Nunca conecte unidades de memoria desconocidas en su computadora y no use las mismas en las computadoras que usa en su casa y en el trabajo.

El **27%** de las infecciones de malware en pequeñas y medianas empresas

se originaron por USB infectadas.

El **87%** de los empleados perdieron un dispositivo de memoria USB y no se lo dijeron a su empleador.

El **48%** de las memorias USB que se encuentran en el piso o en la calle son conectadas a una computadora, generalmente dentro de las 10 horas posteriores a haber sido recogidas.

Parches de Software

Los parches son actualizaciones regulares de su software, sistemas y aplicaciones. La actualización de sus dispositivos puede ser un poco tediosa, pero estas actualizaciones de seguridad son críticas y protegen contra los piratas informáticos que buscan grietas para pasar.

CONSEJOS: Actualice siempre todos sus dispositivos tan pronto como sea posible.

80% de los ataques usan vulnerabilidades en las computadoras, para los cuales ya existen parches.

En 2019, se reportaron **812.67 millones** de infecciones con malware.

Secuestro de Datos

El "Ransomware" es un tipo de malware (software malicioso) que impide o limita el acceso a sus sistemas o dispositivos y le exige que pague un rescate antes de cierto plazo, para que puedan volver a tener el control sobre sus datos.

CONSEJOS: No pague el rescate. Desconecte su dispositivo de Internet o de otras conexiones en red (como Wi-Fi residencial) tan pronto como sea posible para prevenir que la infección se propague. Informe el ataque a la policía nacional. Visite www.nomoreransom. org para corroborar si su sistema fue infectado con alguna de las variantes de "Ransomware" contra las cuales ya hay herramientas para desencriptar sin costo alguno.

20% de los propietarios de pequeñas empresas informan haber sido víctimas de uno o más ataques de "Ransomware".

$377,000 es el promedio de dinero solicitado en casos de secuestro de datos.

16.2 días es la duración media de un el incidente de secuestro de datos.

En Mastercard, nuestra misión es clarificar y simplificar la preparación cibernética. Nuestro programa gratuito de Preparación Cibernética lo guía a través de la selección de un Líder Cibernético, para ayudarlo en la implementación de políticas prácticas y lograr el compromiso de su fuerza laboral. Proporcionamos recomendaciones, materiales de capacitación y kits de comunicación desarrollados por los principales expertos para que su organización tenga la preparación cibernética necesaria de manera rápida y eficiente.

Para obtener más información, visite: **https://www.mastercard.com.mx/es-mx/empresas/empresas-pequenas-medianas/ciberseguridad.html**

Acerca de Mastercard

Master Your Card es un programa educativo de empoderamiento a la comunidad patrocinado por Mastercard que trabaja con aliados comprometidos en todo el país para brindar información sobre los beneficios de la tecnología de pagos electrónicos para que las comunidades desatendidas forjen futuros financieros más promisorios. El programa facilita presentaciones y talleres en ciudades de todo el país, proporcionando educación financiera a millones de personas, incluyendo estudiantes, a través de programas, materiales educativos y eventos con nuestros aliados.