LISTA DE VERIFICACIÓN

PREVENCIÓN DE SINIESTROS CIBERNÉTICOS DURANTE UNA PANDEMIA:

SEGURIDAD DE LA INFORMACIÓN

El objetivo de este documento es brindar pautas sobre la prevención de siniestros cibernéticos para las organizaciones que operen durante una pandemia. Mantener a su empresa funcionando podría requerir enfoques alternativos, con una fuerte dependencia en el trabajo remoto y en cronogramas y prácticas de participación adaptadas. Junto con las circunstancias que acompañan a la pandemia, estas desviaciones presentan desafíos únicos para la seguridad cibernética. Sin embargo, con una concientización y una vigilancia cibernética adecuadas, puede reducir de forma significativa la probabilidad de que ocurra un ataque cibernético exitoso en su organización.

Los criminales cibernéticos continúan aprovechando las tácticas de suplantación de identidad y de ingeniería social para obtener acceso no autorizado a las redes de las empresas. De hecho, la suplantación de identidad sigue siendo el método de ataque y el vector de infección más prevalente para software malicioso y secuestro de datos.

Use estas pautas para enfocar sus esfuerzos de prevención de siniestros cibernéticos durante la pandemia, en línea con las políticas establecidas de la compañía.

INGENIERÍA SOCIAL

Dado que una pandemia altera el funcionamiento normal de los negocios e impacta la seguridad cibernética, los criminales están usando ataques de ingeniería social para amenazar a los negocios. Protéjase y tenga cuidado con cualquier correo electrónico, llamado telefónico o mensaje en línea con historias convincentes, tales como:

- ☐ Un problema que requiere su "verificación" usando su información personal.
- ☐ Solicitud urgente de ayuda.
- ☐ Notificación de que ganó algo importante, como una lotería o rifa.
- ☐ Correo electrónico de un gerente o colega donde se solicite información interna confidencial.

SUPLANTACIÓN DE IDENTIDAD

Con el fin de obtener acceso no autorizado a las redes de su empresa, los criminales cibernéticos pueden atraerlo a páginas web que parecen legítimas y que ellos controlan, hacer ofertas de empleo que prometen ganar dinero extra con facilidad o pedir donaciones benéficas para falsas organizaciones afectadas por una pandemia. A continuación, se incluyen algunos pasos que pueden adoptarse para mitigar el riesgo de suplantación de identidad:

- ☐ Esté atento y sea cuidadoso al abrir correos electrónicos o archivos adjuntos de extraños, tanto si está trabajando desde casa o en la oficina.
- ☐ Visite únicamente sitios web conocidos, porque hay menos probabilidad de encontrar contenido malicioso.
- ☐ Verifique la fuente de los correos electrónicos.
- ☐ Si está en duda, no corra el riesgo. Comuníquese con el departamento de Seguridad de la Información o de Soporte de TI.

La ansiedad relacionada con esta situación sin precedentes puede llevar a los usuarios a hacer clic en correos electrónicos fraudulentos relacionados con la pandemia que podrían liberar software malicioso en la organización.

FM Global

LISTA DE VERIFICACIÓN PARA PREVENIR SINIESTROS DURANTE UNA PANDEMIA

VIDEOCONFERENCIAS

Los criminales cibernéticos pueden hackear discretamente y robar información confidencial que se está compartiendo en reuniones de negocios mediante software de videoconferencia. Esto pone en peligro información de la compañía y podría impactar sus operaciones. En lo posible, considere adoptar las siguientes medidas de seguridad:

- ☐ Desactive la opción por defecto que permite que los participantes de una reunión compartan su pantalla sin el permiso del anfitrión de la reunión.
- ☐ Habilite la protección con contraseña para evitar usuarios que no hayan sido invitados.
- ☐ Establezca como requisito que el anfitrión esté presente para comenzar una reunión.
- ☐ Antes de compartir su pantalla, cierre las aplicaciones y los documentos no relacionados, a fin de prevenir la divulgación no intencional.
- ☐ Solo permita que se unan a la reunión individuos con un dominio de correo electrónico específico.

PARCHES

Los criminales cibernéticos intentarán aprovecharse de las vulnerabilidades conocidas dentro de sus sistemas operativos y aplicaciones. Con la tendencia creciente de los empleados de usar sus propios dispositivos para fines comerciales y para trabajo remoto, es de especial importancia que sean cuidadosos con los datos a los que acceden o que almacenan en dichos dispositivos. Para salvaguardar los dispositivos y ayudar a proteger los datos:

- ☐ Mantenga actualizados los parches y versiones de los sistemas operativos.
- ☐ Cuando sea posible, active las actualizaciones automáticas.
- ☐ Asegúrese de que los software antivirus y antimalware cuenten con los parches y versiones más actualizados.
- ☐ Siempre que sea posible, consolide las versiones de software de su casa y la oficina.
- ☐ Proteja cualquier dispositivo que pueda integrarse con los servicios y las redes corporativos.

RECURSOS ÚTILES

Teletrabajo: preparar a su organización y al personal (en inglés)
https://www.ncsc.gov.uk/guidance/home-working

Recursos para el hogar y para la oficina (en inglés)
https://www.us-cert.gov/ncas/tips/ST15-002

Comprender los parches y las actualizaciones de software (en inglés)
https://www.us-cert.gov/ncas/tips/ST04-006

Mantener seguro el equipo en casa
https://support.microsoft.com/es-mx/help/4092059/windows-keep-your-computer-secure-at-work

DESCARGO DE RESPONSABILIDAD DE ENLACES EXTERNOS

Aunque se hace todo lo posible por asegurar que estos enlaces sean correctos, actualizados y relevantes, FM Global no asume responsabilidad por las páginas mantenidas por proveedores externos.

Para obtener copias adicionales de esta publicación u otros recursos de FM Global, puede realizar pedidos en cualquier momento desde nuestro sitio web fmglobalcatalog.com. Para obtener asistencia personalizada en cualquier lugar del mundo, comuníquese con el equipo de atención al cliente con sede en EE. UU.:

- Línea gratuita en EE. UU. y Canadá: (1) 877 364 6726
- Fax: (1) 401 477 7010
- Teléfono: +1 (1) 401 477 7744
- C. e.: customerservices@fmglobal.com