Guía de seguridad de la información para nuevos empleados

Versión online aquí:
kas.pr/x9j7

El acceso a los sistemas y servicios corporativos

1. Utiliza contraseñas seguras para todas las cuentas (con una extensión de al menos 12 caracteres), que no incluya palabras del diccionario, pero sí caracteres especiales y números. Los atacantes podrían forzar con facilidad las contraseñas simples.
2. Genera una contraseña única para cada cuenta. Si reutilizas las contraseñas, la filtración en un servicio podría acabar por comprometer al resto.
3. Mantén las contraseñas en secreto, sin excepción. No las escribas, guardes en un archivo ni compartas con tus compañeros. Cualquier visitante o exempleado resentido podría utilizar tu contraseña para perjudicar a la empresa, por mencionar lo más obvio, pero las posibilidades son prácticamente ilimitadas.
4. Habilita la autentificación en dos pasos para cada servicio que lo permita. Utilizar la 2FA ayuda a evitar que un atacante acceda al servicio, incluso aunque se haya filtrado la contraseña.

Los datos personales

5. A la hora de desechar los documentos, no los tires sin haberlos triturado. Tener información de identificación personal en los contenedores de la empresa puede atraer la atención de los reguladores y sus costosas multas.
6. Utiliza canales seguros para intercambiar los archivos que contengan datos personales (por ejemplo, comparte documentos de Google Docs únicamente con los compañeros que necesiten ver el archivo y no con la opción "cualquier usuario de Internet con este enlace puede ver esto". Por ejemplo, Google indexa los documentos que tengan esta función habilitada, lo que significa que pueden aparecer en los resultados de búsqueda.
7. Comparte los datos personales de los clientes estrictamente con los compañeros que necesiten la información. Más allá de tener problemas con los reguladores, compartir esta información aumenta el riesgo de una filtración de datos.

Las ciberamenazas más comunes

8. Revisa minuciosamente los enlaces en los correos electrónicos antes de acceder a ellos y recuerda que un nombre de remitente convincente no garantiza su autenticidad. Uno de los muchos trucos que los cibercriminales utilizan para que los usuarios hagan clic en sus enlaces de phishing es que personalizan los mensajes de acuerdo con tu negocio o incluso utilizan la cuenta secuestrada de un compañero.
9. Para los directores financieros: Nunca transfieras dinero a cuentas desconocidas basándote exclusivamente en un correo electrónico o mensaje directo. En su lugar, ponte en contacto con la persona que supuestamente ha autorizado la transferencia para confirmar la petición.
10. No conectes medios de almacenamiento desconocidos a un ordenador. Los ataques mediante unidades de memoria USB infectadas no solo aparecen en la ciencia ficción, los ciberdelincuentes ya han utilizado esta técnica con dispositivos maliciosos en lugares públicos y oficinas.
11. Antes de abrir un archivo, comprueba que no sea ejecutable (con frecuencia los atacantes disfrazan los archivos maliciosos como documentos de oficina). No abras o ejecutes archivos ejecutables de fuentes en las que no confíes.

Los contactos de emergencia

12. A quién se debe contactar (nombre y número de teléfono) en caso de un correo electrónico sospechoso, un comportamiento raro en tu ordenador, una nota de ransomware o cualquier otro problema cuestionable. Podría ser el personal de seguridad, un administrador de sistemas o, incluso, el propietario de la empresa.

kaspersky