

GUÍA PARA EL CISO: PROTECCIÓN DE SUS CLIENTES

ADMINISTRACIÓN DE CUENTAS

- Exija que los clientes utilicen nombres de usuario y contraseñas seguros para iniciar sesión en sus servicios. Aconséjeles que no utilicen la misma contraseña que para otras cuentas.
- Utilice verificación instantánea, verificación en tiempo real, verificación de depósito de prueba, verificación de identidad o preguntas de autenticación para validar clientes reales y reducir la oportunidad de fraude.
- Ofrezca, si no puede exigirlo, la autenticación de dos factores para que los clientes la utilicen al iniciar sesión en sus servicios.
- Compruebe periódicamente las cuentas de usuario para detectar signos de fraude.

PROTECCIÓN DE DATOS

- Considere qué datos de clientes su organización *debe* recopilar para prestar sus servicios y tenga cuidado para evitar recopilar datos de clientes que vayan más allá de eso.
- Establezca y distribuya políticas de retención de datos. Elimine los datos del cliente cuando ya no sean necesarios.
- Cifre los datos del cliente en tránsito y en reposo.
- Ponga en marcha políticas de seguridad de datos para aclarar qué métodos de transferencia de datos están aprobados y cuáles restringidos, y que especifiquen qué es aceptable para todos los empleados cuando se trata con datos de clientes. Garantice que estas políticas se documenten, se comuniquen, se apliquen a todos los empleados y se revisen y actualicen periódicamente.

PROTECCIÓN DE APLICACIONES WEB PÚBLICAS

- Implemente HTTPS en las aplicaciones web orientadas al público de su organización y redirija todo el tráfico HTTP a HTTPS.
- Utilice una política de seguridad de contenido en su(s) sitio(s) web para evitar ataques de scripting, clickjacking y otras inyecciones de código.
- Habilite la colocación de claves públicas en su(s) sitio(s) web para evitar ataques de tipo “Man in the middle”.
- Asegúrese de que sus aplicaciones web orientadas al público nunca utilicen cookies para almacenar información de clientes muy confidencial o crítica (como contraseñas) y de que tengan fechas de caducidad conservadoras para las cookies (el menor tiempo posible). Considere cifrar la información almacenada en las cookies que utilice.
- Considere contratar un servicio de pruebas de penetración para evaluar la seguridad de sus aplicaciones web orientadas al público al menos una vez al año.

Asesoramiento individual para que los clientes y empleados protejan los datos financieros

Aconseje a sus empleados y a sus clientes que sigan las siguientes directrices de ciberseguridad en su comportamiento personal para aumentar su preparación y proteger sus datos financieros frente a amenazas cibernéticas.

1. Implemente prácticas básicas de higiene cibernética en sus dispositivos.

- Utilice contraseñas seguras en todos los dispositivos personales y profesionales, y considere utilizar un gestor de contraseñas.
- Mantenga actualizados los sistemas operativos, otro software y aplicaciones en sus ordenadores y dispositivos móviles.
- Instale software antivirus, antimalware y antiransomware que prevenga, detecte y elimine programas malintencionados.
- Utilice un programa cortafuegos para evitar el acceso no autorizado a su ordenador.
- Utilice únicamente productos de seguridad de empresas fiables. Lea las revisiones de las publicaciones de ordenadores y consumidores, y considere la posibilidad de consultar al fabricante de su ordenador o sistema operativo.

2. Tenga cuidado con la información confidencial.

- No envíe contraseñas de cuentas bancarias ni otros datos de cuentas financieras confidenciales a través de correo electrónico sin cifrar.
- Sea inteligente sobre dónde y cómo se conecta a Internet para acciones bancarias u otras comunicaciones relacionadas con información personal confidencial. Las redes Wi-Fi públicas y los ordenadores en lugares como bibliotecas o centros de negocios de hoteles pueden ser arriesgadas.

3. Resista el phishing.

- No abra de inmediato archivos adjuntos de correo electrónico ni haga clic en enlaces en correos electrónicos no solicitados o sospechosos. Pare. Piense. Haga clic.
- Sospeche si alguien se pone en contacto con usted inesperadamente en línea o por teléfono y le pide su información personal. Incluso cuando se comunique con direcciones conocidas, minimice el intercambio de información personal por correo electrónico.
- Recuerde que ninguna institución financiera le enviará un correo electrónico o le llamará y solicitará información confidencial que ya tenga sobre usted.
- Suponga que una solicitud de información de un banco donde nunca ha abierto una cuenta es una estafa.
- Verifique la validez de un correo electrónico de aspecto sospechoso o un mensaje emergente antes de proporcionar información personal. Preste mucha atención a la dirección de correo electrónico.

FORMACIÓN PARA EMPLEADOS

- Enseñe a sus empleados la responsabilidad y las estrategias para minimizar los errores humanos que podrían exponer los datos del cliente. Esto significa aconsejarles:
 - Minimizar el acceso y la transmisión de los datos del cliente a solo lo necesario para realizar sus funciones laborales.
 - Mantener prácticas de seguridad sólidas en todos los dispositivos y cuentas que tratan con los datos de los clientes utilizando contraseñas seguras, habilitando autenticación de dos factores, manteniendo actualizado el software y no haciendo clic en enlaces sospechosos.
 - Informar de cualquier posible incidente de seguridad interno o externo, amenazas o manipulación indebida de datos al personal técnico de su organización o a la gerencia superior.
- Asegúrese de que sus empleados entienden y han firmado documentos para cumplir con las políticas de seguridad y protección de datos de su organización, de modo que no las incumplan, y para que puedan tratar con los clientes con fluidez y no se comuniquen con ellos de forma desprotegida.

NOTIFICACIÓN A LOS CLIENTES

- Comprenda el entorno normativo de su organización cuando se trata de gestionar la vulneración de datos de los clientes para asegurarse de que está preparado para cumplir con los incidentes.
- Cuando su organización tenga conocimiento de un incidente de acceso no autorizado a información confidencial del cliente, investigue con prontitud la probabilidad de que la información se haya utilizado o se utilice de forma incorrecta. Siga las prácticas recomendadas de notificación y notifique al cliente o clientes afectados lo antes posible con:
 - Una descripción general del incidente y la información a la que se ha tenido acceso.
 - Un número de teléfono para obtener más información y asistencia.
 - Un recordatorio de “permanecer alerta” durante los próximos 12 a 24 meses.
 - Una recomendación de que los incidentes de sospecha de robo de identidad se notifiquen de inmediato.
 - Una descripción general de los pasos adoptados por la institución financiera para proteger la información contra un mayor acceso o uso no autorizado.
 - Información de contacto para agencias de informes crediticios.
 - Cualquier otra información exigida por las normativas con las que su organización debe cumplir.

