eviivo

UNA GUÍA PARA PROTEGER TU LIQUIDEZ:

PAGOS, DEVOLUCIONES Y PREVENCIÓN DE FRAUDES

Para proteger tu liquidez, necesitas adoptar estrategias operativas diseñadas para:

1. Automatizar los pagos y cobros (en lugar de depender de recordatorios humanos)
2. Evitar devoluciones de cargos
3. Evitar fraudes

Esta guía ofrece consejos de expertos en las tres áreas, adaptados a hoteleros, anfitriones y gestores de propiedades. Sigue leyendo para empezar a salvaguardar tu liquidez.

1. AUTOMATIZACIÓN DE PAGOS

La mejor manera de optimizar tu liquidez es utilizar un PMS (sistema de gestión de propiedades) que ofrezca una pasarela de pagos totalmente integrada.

Este PMS debe ser capaz de:	eviivo Suite
Automatizar el cobro de los pagos en función de cualquier calendario definido por el usuario (entre la fecha de reserva y la salida), sin intervención humana ni errores.	✓
Confirmar automáticamente cualquier pago.	✓
Enviar automáticamente un recordatorio al huésped antes de la fecha de vencimiento.	✓
Determinar automáticamente si se debe o no un reembolso cuando se cancela una reserva.	✓
Procesar automáticamente el reembolso correspondiente.	✓
Confirmar automáticamente cualquier cancelación y el valor de cualquier reembolso.	✓
Controlar automáticamente la entrega de llaves y códigos de acceso si no se han cobrado los pagos previstos.	✓
Preautorizar automáticamente las tarjetas (por ejemplo, mediante una comunicación electrónica completa con el banco del huésped para [1] validar la tarjeta y [2] verificar y autorizar que hay fondos suficientes en la tarjeta para la reserva).	✓
Indicar automáticamente qué parte de la reserva se ha cobrado a través de una OTA y, a continuación, mostrarlo al anfitrión y en la factura del huésped, indicando cualquier saldo restante que deba cobrarse en el momento del check-in o después.	✓

Este PMS debe ser capaz de:	eviivo Suite
Indicar automáticamente si una tarjeta de crédito virtual (VCC) proporcionada por la OTA está disponible y es susceptible de cargo.	✓
Proporcionar informes sencillos sobre depósitos pendientes; saldos de reservas impagados; pagos/transacciones en efectivo por fuente de reserva y/o método de pago.	✓
Proporcionar una conciliación instantánea de los pagos de la OTA - por VCC o transferencia bancaria directa.	✓
Distinguir automáticamente entre una reserva de OTA prepagada y un depósito por adelantado, e identificar cuándo un pago por VCC puede considerarse un depósito por adelantado y cuándo no.	✓
Generar o anular automáticamente y con precisión los registros contables necesarios en función del momento de cualquier cobro o reembolso (por ejemplo, «efectivo/deudor», «efectivo/ingresos diferidos», «efectivo/ingresos e impuestos»).	✓

2. EVITAR DEVOLUCIONES DE CARGOS

¿Qué son las devoluciones?

Una devolución se produce cuando un cliente impugna un pago con tarjeta y pide a su banco que anule la transacción. Los clientes pueden llamar a su banco en cualquier momento y pedir que se les devuelva el importe de una transacción con tarjeta. Normalmente, el banco se pone de parte del cliente y le devuelve el importe de la tarjeta. A continuación, el comerciante deberá demostrar que:

1. El cobro estaba justificado.
2. El huésped autorizó o firmó efectivamente el pago con tarjeta.

Cuando recibas una devolución de cobro, puedes impugnarla, pero la responsabilidad de la prueba recae sobre ti.

- Si ganas el litigio, te quedas con el dinero.
- Si pierdes el litigio, tendrás que tramitar la devolución y es probable que el banco te cobre gastos administrativos.

Bueno saberlo -> En la Unión Europea, los clientes pueden solicitar una devolución de cargo (reembolso) hasta 13 meses después del primer cargo en su tarjeta. Fuera de la Unión Europea, este plazo se reduce a 70-120 días, dependiendo de la política del banco.

Presencia del titular de la tarjeta

Si el titular de la tarjeta está presente cuando se procesa el pago, tienes muchas posibilidades de poder defenderte contra cualquier devolución de cobro. Se considera que un titular está «presente» cuando:

- Introducen su código PIN secreto en un lector de tarjetas o en un cajero automático.
- Pagan en línea y se les pide que respondan a un sistema de seguridad 3DS (o Amex Safekey) en tiempo real. En este caso, se pide a los clientes que introduzcan una contraseña de un solo uso (OTP) como parte del proceso de pago, que su banco suele enviar por correo electrónico o SMS.

Si el titular de la tarjeta no está presente cuando la procesas, es mucho más probable que te expongas a devoluciones de cobro. Este suele ser el caso cuando los datos de la tarjeta te los pasa una OTA, porque el huésped ya no está presente en línea cuando procesas la tarjeta en tu PMS. El pago no fallará necesariamente, pero es mucho más probable que esté expuesto a devoluciones de cobro. Sigue leyendo para obtener recomendaciones sobre cómo evitarlo.

Devoluciones legítimas

Las **devoluciones legítimas** pueden producirse cuando:

- El huésped cancela por un motivo **real, grave e inesperado** (por ejemplo, una «causa de fuerza mayor» como la pandemia COVID-19, una catástrofe natural, prohibiciones de viajar, etc.) y no obtiene ninguna compensación del alojamiento, especialmente si su viaje no estaba asegurado.
- Los huéspedes temen que **el alojamiento o la OTA no les reembolse el importe de una cancelación total o parcial legítima**, sobre todo si el alojamiento tarda demasiado en hacerlo.

Las devoluciones de cobros fraudulentas pueden producirse cuando:

-
- Los huéspedes afirman que nunca se alojaron, cuando sí lo hicieron.
- Has reembolsado al cliente en efectivo, pero éste reclama un segundo reembolso a través de un cargo en su tarjeta.
- Los huéspedes deciden deliberadamente NO alojarse contigo, pero quieren evitar pagar gastos de cancelación tardía y evitar cualquier contacto contigo o con la OTA.
- Un huésped se aloja, pero la estancia fue prepagada por otra persona utilizando una tarjeta robada (y tú no preautorizaste/revalidaste la tarjeta).

¿Cómo puedo evitar las devoluciones?

Siempre debes poner en práctica las siguientes recomendaciones para evitar las devoluciones de cargos:

- **Pide a los huéspedes que reconfirmen** su estancia unos días antes del check-in.
- **Registra correctamente al huésped a su llegada**. Siempre:
  - Insiste en que el huésped envíe los datos de registro. (Esto puede hacerse por correo electrónico/vía link)
  - Solicita al huésped que te vuelva a dar su tarjeta y realiza una comprobación de chip y pin con un lector de tarjetas cuando le entregues sus llaves (si tienes un servicio de recepción o de meet & greet)
  - Haz clic en el botón «Check In» de eviivo Suite para dejar un rastro digital (si utilizas eviivo como tu PMS)

- **Confirma que el titular de la tarjeta y la persona que se aloja contigo son la misma persona**.
  - Si la tarjeta es de otra persona o el pasaporte no coincide, pide al huésped que proporcione una tarjeta a su nombre
  - Si el huésped no puede facilitar un documento de identidad, carga la estancia completa en la tarjeta en el momento del check-in (no esperes hasta el check-out) y/o pide al titular de la tarjeta que confirme sus datos y su acuerdo de pago por correo electrónico

- **Si un huésped cancela por teléfono**, anula la reserva y tramita inmediatamente el reembolso o los gastos de cancelación correspondientes. (Esto puede automatizarse por completo).

- **Si un huésped cancela por teléfono**, anula la reserva y tramita inmediatamente el reembolso o los gastos de cancelación correspondientes. (Esto puede automatizarse por completo).

- **Si el cliente debe recibir un reembolso total o parcial, tramítalo rápidamente**. Los retrasos pueden llevar al cliente a solicitar una devolución a través de su banco, lo que puede acabar costándote más que el reembolso.

- **Guarda un rastro digital**.

- **Cobra los gastos de cancelación (si procede) tan pronto como haya vencido el plazo de cancelación**, idealmente antes del check-in.

- Considera la posibilidad de utilizar un **depósito no reembolsable** (es decir, un anticipo que debe abonarse en el momento de la reserva, o tan pronto como lo permita la ley en las zonas donde la ley impone un periodo de gracia de 24 horas). Para ello es necesario armonizar las políticas de cancelación y depósito.

Recomendaciones relativas al pago de las reservas en línea

Si vas a cobrar a los huéspedes, en lugar de a la OTA, asegúrate de que **utilizas un sistema de gestión de reservas y propiedades con una función de automatización de pagos totalmente integrada y que cumpla la normativa PCI**. Se trata de un sistema que permite automatizar todo el proceso de cobro y reembolso. Debe ser capaz de cobrar un pago en el momento en que vence y procesar un reembolso en el momento en que se cancela una reserva, sin ninguna intervención manual. Un sistema de este tipo también debería ofrecerte:

- **Una amplia selección de procesadores de tarjetas**, para evitar que te quedes bloqueado con un único banco o procesador de tarjetas.
- **Diferentes opciones de configuración**, como cobrar a través de un enlace de pago, una página web segura o un portal de huéspedes; imponer o restringir el método de pago admitido; y seleccionar por adelantado los tipos de clientes que deben o no pagar con tarjeta.

El mejor método es preautorizar/procesar una tarjeta cuando el huésped está presente online, en cuanto recibes una reserva. Por lo tanto, asegúrate de que tu sitio web está habilitado para 3DSecure/Safepay y de que tu PMS es capaz de enviar un enlace de pago al huésped (por correo electrónico, SMS o WhatsApp), llevándole a una página segura en la que puede procesar su tarjeta cumpliendo todos los requisitos de 3DS. En ambos casos, la presencia en línea del huésped en la página y el código de seguridad 3DS sirven como prueba **irrefutable de que tenía intención de pagar y era plenamente consciente de sus términos y condiciones cuando hizo la reserva**.

Si decides procesar la tarjeta tú mismo -con un lector de tarjetas o directamente en un PMS como eviivo Suite- y el huésped ya no puede acceder a teclear un PIN secreto o proporcionar un código de seguridad de un solo uso 3DS, entonces el riesgo de devolución de cargo es alto. Incluso si la tarjeta se procesa con éxito, la devolución puede producirse días o semanas más tarde, y puedes quedar expuesto a un riesgo mucho mayor por parte de huéspedes deshonestos.

¿Cómo puedo mejorar mis posibilidades de ganar un recurso?

Debes aportar pruebas de la estancia del huésped:

- Proporciona un **informe que muestre cómo y cuándo se procesaron los pagos**, junto con una copia de cualquier correo electrónico de confirmación de pago/reserva enviado al huésped que vincule el pago a tus condiciones generales. (CONSEJO: Revisa las condiciones de tu política de cancelación/depósito. Asegúrate de que tu PMS incluye estos términos automáticamente en cualquier email de confirmación de reserva, pago o cancelación).
- **Almacena todas las comunicaciones entre tú y el huésped**.
- **Adjunta una copia de cualquier extracto o factura del huésped**, especialmente si incluye un reembolso en ventanilla.

3. EVITA EL FRAUDE CIBERNÉTICO

Tomar medidas preventivas para evitar el fraude cibernético es fundamental para proteger tu dinero.

Los últimos años han traído consigo un aumento de los ciberataques geopolíticos, por lo que la mayoría de los gobiernos han incrementado las medidas de ciberseguridad y han impulsado requisitos de cumplimiento de la seguridad más estrictos.

El primer paso para proteger tu liquidez es revisar las medidas de seguridad implantadas por tus proveedores de software:	eviivo Suite
¿Qué comprobaciones realizan al dar de alta a nuevos clientes? ¿Realizan comprobaciones exhaustivas de identidad y financieras para asegurarse de que no permiten la entrada de piratas informáticos en sus plataformas? (Si compartes una plataforma con otras empresas, querrás que tu proveedor de plataformas haga todo lo posible para asegurarte de que estás en buena compañía).	✓
¿Cumplen de forma nativa la norma PCI DSS (Payment Card Industry Data Security Standard)? ¿Están auditados y certificados de forma independiente por Visa y Mastercard o por auditores designados? ¿Codifican los datos de las tarjetas y realizan análisis periódicos para evitar su divulgación?	✓
¿Proporcionan sólidas funciones de gestión de usuarios a un nivel suficientemente pormenorizado (es decir, por función, por característica, por equipos y por conjunto de propiedades) al tiempo que permiten a los usuarios ver los datos de todas las propiedades permitidas desde un único calendario de reservas?	✓
¿Proporcionan cortafuegos básicos, detección de intrusos, protección antispam y antiphishing, así como capacidades profesionales de copia de seguridad y recuperación?	✓
¿Disponen de procedimientos para alertarte cuando alguno de tus clientes es pirateado o sufre un ataque de phishing?	✓
¿Cuál es su política en materia de GDPR (Reglamento General de Protección de Datos) y/o DSA (Ley de Servicios Digitales)?	✓

El resto está en tus manos. Debes orientar y formar al personal, aplicar las mejores prácticas y, sobre todo, asegurarte de que todo el mundo esté alerta. También es una buena idea contratar un seguro contra ciberataques si puedes permitírtelo.

Credenciales de los empleados

Una de las formas más sencillas y eficaces de reforzar sus defensas es asegurarse de que cada empleado dispone de credenciales de acceso seguras e individuales. Cada conjunto de credenciales debe incluir lo siguiente:

- Un correo electrónico único (tu nombre de usuario).
- Una contraseña única **que sólo tú conozcas** (cuanto más larga, mejor: opta por un mínimo de 12 caracteres, incluyendo al menos una mayúscula, un número + un carácter especial).
- Una pregunta de seguridad única cuya respuesta sólo tú conozcas (se utiliza si deseas restablecer, recuperar o cambiar tus credenciales en el futuro).
- Un segundo correo electrónico o número de móvil de recuperación (diferente del primero), esencial para ayudar a mitigar rápidamente cualquier daño en caso de que seas víctima de un ciberataque.
- Una segunda pregunta y respuesta de seguridad, conocida TANTO por ti como por el proveedor del software. Esto lo utiliza un proveedor como eviivo para verificar tu identidad cuando te pones en contacto con nosotros por teléfono o videoconferencia.
- Un identificador de propiedad único (eviivo lo denomina shortname).

Elección de contraseñas

Las peores contraseñas (es decir, las que suelen verse más comprometidas) son las que incluyen la palabra «contraseña», las primeras letras de un teclado («Qwerty» o «Azerty»), series numéricas básicas (por ejemplo, "111111" o «1234567»), o los nombres o fechas de nacimiento de tus hijos, cónyuge o pareja.

Las mejores contraseñas tienen más de 12 caracteres e incluyen siempre una mayúscula, un número y un carácter especial. En lugar de una palabra, utiliza una frase **larga y fácil de recordar**. Incluye uno o varios números, una o varias mayúsculas y uno o varios caracteres especiales (por ejemplo, *_-$£).

Si utilizas eviivo y eres el titular principal de la cuenta, puedes, a su vez, dar acceso a otros usuarios y empleados de tu organización a través de la pantalla de gestión de usuarios de eviivo. Puedes acceder a ella haciendo clic en el icono del hombrecillo situado en la parte superior derecha de la pantalla de eviivo Suite.

Buzones de correo públicos y compartidos

Para evitar sorpresas y fallos de ciberseguridad, te recomendamos encarecidamente que adoptes las siguientes precauciones:

Evita compartir credenciales a toda costa. Siempre es mejor asegurarse de que cada empleado tiene su propio conjunto de credenciales. Ignorar esto es la causa más frecuente de ciberfraude en el sector hotelero. Sin embargo, compartir dispositivos e inicios de sesión puede ser conveniente para las actividades de recepción o limpieza. Si realmente «debes» utilizar dispositivos y credenciales compartidos, entonces...

Asegúrate de que las credenciales de usuario compartidas sólo tienen derechos de acceso mínimos. Cualquiera que se ocupe de pagos, procesamiento de tarjetas o información personal de los huéspedes no debería poder hacerlo utilizando credenciales compartidas. Para tu propia protección, necesitas una auditabilidad total. Trata de mantener el menor número posible de ojos en este tipo de información.

No des niveles de permiso máximos a buzones públicos o compartidos. Las direcciones públicas compartidas (por ejemplo, «info@yourplace.com», «contact@yourplace.com», «reservations@yourplace.com», «bookings@yourplace.com» o «hello@yourplace.com») NO deben asignarse a funciones de nivel superior como el «Administrador», el titular de la cuenta principal o el gerente. Ignorar este consejo es la segunda razón más frecuente de fraude cibernético en el sector de la hostelería.

Diferencia siempre tu correo electrónico/contraseña profesional de cualquier correo electrónico personal utilizado para comunicaciones privadas. Utiliza cuentas de correo y contraseñas distintas, e instruye a tus empleados para que hagan lo mismo.

Los buzones públicos y compartidos son mucho más fáciles de vulnerar porque:

- Los piratas informáticos utilizan direcciones de correo electrónico públicas para inducir a los huéspedes a facilitar datos o detalles de sus tarjetas.
- El uso de buzones o cuentas compartidas aumenta las probabilidades de ataque, ya que cualquiera de los múltiples usuarios puede ser engañado para que facilite sus credenciales.
- El fraude interno puede ser cometido por trabajadores temporales o contratados, personal nuevo o contratistas subcontratados que no conoces bien.

Seguridad multiusuario por equipos

Una configuración de seguridad basada en equipos debería ayudarte a gestionar fácilmente una multiplicidad de roles.

Por ejemplo, supongamos que tres personas distintas necesitan el mismo nivel de seguridad. En lugar de crear un buzón compartido, puedes:

1. Asignar a cada persona sus propias credenciales de inicio de sesión.
2. Asignar las tres personas a un «Equipo».
3. Asignar los permisos deseados y los derechos de acceso a las propiedades al «Equipo» en lugar de a cada individuo.

Una configuración basada en equipos es mucho más rápida y fácil de gestionar a medida que los empleados se incorporan o abandonan la empresa. Como cada persona conserva sus propias credenciales, cualquier auditoría de transacciones relaciona cada acción con la persona que la realizó. Por lo tanto, si las credenciales de una persona fueran robadas o vulneradas, el resto del equipo puede continuar sin verse afectado, mientras que con credenciales compartidas, todo el mundo queda inhabilitado.

Phishing: la forma más común de ataque

El phishing es el acto malicioso de intentar engañar a los usuarios para que revelen sus credenciales personales. Los atacantes suelen inducir a los usuarios a revelar información a través de enlaces maliciosos, páginas web falsas o archivos adjuntos a correos electrónicos que contienen programas espía o virus informáticos como troyanos.

Los delincuentes y estafadores falsifican constantemente los logotipos y las páginas de inicio de sesión de empresas reputadas. Son muy hábiles reproduciendo no sólo logotipos, sino también fotos, vídeos e incluso voces.

Los métodos más habituales para entrar en las cuentas son el correo electrónico, las notificaciones a móviles, las redes sociales y las llamadas telefónicas. Los atacantes pueden hacerse pasar por uno de los proveedores de tu empresa, tu banco, tu proveedor de telecomunicaciones o de software, o por diversas autoridades.

Un intento de phishing exitoso puede permitir a un atacante:

- Recopilar nombres de usuario y contraseñas u otra información confidencial.
- Tomar el control de tu buzón de correo electrónico para usos malintencionados.
- Convencerte para que realices pagos en su beneficio.
- Convencerte para que ingreses sumas de dinero en una cuenta no autorizada.
- Instalar programas espía o maliciosos que les permitan vigilar tu actividad en línea.
- Dañar tu ordenador o la red de la organización, cifrar tus datos o pedir un rescate por ellos.
- Obtener acceso a propiedad intelectual, diseños o patentes pendientes.

El resto de esta guía examina las astutas formas en que los estafadores pueden intentar engañarte, y cómo mantenerte alerta.

Spear phishing: falsas confirmaciones de reserva

El spear phishing es una forma dirigida de ataque de phishing. Los autores suelen utilizar información disponible públicamente en Internet, como direcciones de correo electrónico públicas en sitios web, para crear mensajes falsos y animar a su público a hacer clic en enlaces maliciosos.

Un ejemplo podría ser la creación de confirmaciones de reserva falsas para enviarlas a tus huéspedes. Los estafadores pueden obtener una confirmación de reserva original realizando, y luego cancelando, una reserva o un pedido contigo. A continuación, pueden utilizarla para crear una confirmación falsa que parezca provenir de ti (o de eviivo, Airbnb, Booking.com, etc.). Estos mensajes de confirmación falsos engañan a los huéspedes desprevenidos para que proporcionen información personal, credenciales o datos de tarjetas o cuentas bancarias, o incluso para que hagan clic en un enlace para pagar en la cuenta bancaria de los piratas informáticos.

Un método habitual de los ataques de phishing selectivo consiste en disfrazar software malicioso en archivos adjuntos y enlaces aparentemente legítimos, que los autores esperan que se descarguen para infectar el ordenador o la red de destino.

Además, estos botones y enlaces suelen conducir a los usuarios a páginas falsas de inicio de sesión en sitios web para capturar información sensible o personal, que puede utilizarse posteriormente para lanzar nuevos ataques u obtener acceso privilegiado a la cuenta o red organizativa del objetivo.

Para protegerte, ten en cuenta los siguientes puntos que te ayudarán a detectar falsificaciones y trucos de phishing en línea:

Haz clic en el nombre del remitente en la casilla «De» del encabezado del correo electrónico para descubrir su dirección de correo electrónico completa. ¿Parece una dirección legítima? ¿La ortografía coincide al 100% con el correo electrónico oficial de la empresa? Si no es así, es falso.

¿Te pide el correo que hagas algo urgentemente? ¿Te lo esperabas? La mayoría de los estafadores crean una falsa sensación de urgencia, alegando que actúan en nombre de una autoridad superior (por ejemplo, un banco, una institución, una empresa o un alto ejecutivo) y luego te dicen que debes verificar los datos de tu cuenta.

¿Contiene el correo electrónico errores ortográficos o gramaticales inusuales? Muchos delincuentes operan desde el extranjero. Como falsifican notificaciones oficiales, a menudo se pueden detectar errores gramaticales u ortográficos que una empresa legítima evitaría.

Haz clic en el nombre del sitio web en la barra del navegador y comprueba la primera parte de la dirección del sitio web. Por ejemplo, las direcciones web legítimas de eviivo (nombres de dominio URL) siempre empiezan por https://eviivo.com/ o https://on.eviivo.com/ o https://via.eviivo.com/.

Comprueba siempre la ortografía de la dirección de correo electrónico o de la dirección de la página web con sumo cuidado. Todo lo que se necesita para redirigirte a un sitio web falso o a una página de inicio de sesión es que un carácter sea diferente, o que un espacio esté en el lugar equivocado. Ejemplo: Un reciente intento de phishing sustituyó **«eviivo» por "evlivo", mientras que otro decía «eviivo. com» en lugar de «eviivo.com»** - ¡ambos errores ortográficos apenas perceptibles!

CONSEJO

Si eres usuario de eviivo, guarda la dirección URL de la página de inicio de sesión oficial de eviivo en tu navegador y accede siempre desde allí. Esto reduce el riesgo de hacer clic en enlaces dudosos de correos electrónicos falsos o páginas de inicio de sesión.

Whaling

El whaling es un ataque de phishing que se dirige a los usuarios fingiendo ser personas de alto perfil, como ejecutivos de empresas, altos directivos, celebridades o personal con autoridad para proporcionar acceso a sistemas o información sensible.

El objetivo es engañar a alguien para que lleve a cabo una acción o revele información que luego pueda utilizarse para provocar nuevas brechas de seguridad.

Los ataques de whaling son muy personalizados. A menudo incorporan el nombre del objetivo, su puesto de trabajo y otra información relevante (obtenida de diversas fuentes, como sus perfiles en redes sociales u otros aspectos de su huella digital).

Los atacantes se hacen pasar por alguien con mucha autoridad o credibilidad para:

Pedir a sus objetivos un favor o ayuda urgente, de modo que los usuarios deseosos de complacer a su jefe acaban transfiriendo datos, credenciales, ¡o incluso dinero! Para evitarlo, comprueba tres veces cualquier comunicación que recibas firmada por el director general, el vicepresidente o el consejero delegado de una empresa.

Amenazar a los usuarios con cerrarles la cuenta o incumplir ciertas normas si no reconfirman sus credenciales inmediatamente. A continuación, los usuarios son conducidos a una página web falsa donde los hackers les acechan, listos para capturar sus credenciales.

Ofrecer una gran recompensa en metálico o fingir que el usuario tiene dinero que reclamar (por ejemplo, un premio de lotería o una herencia), con el fin de incitarle a facilitar sus credenciales o los datos bancarios o de su tarjeta.

Vishing

Vishing es la abreviatura de «phishing de voz». Significa sencillamente suplantación de identidad a través de llamadas telefónicas o mensajes de voz.

Puede tratarse de alguien que se hace pasar por tu banco, una empresa de telecomunicaciones o un proveedor como eviivo, y te pide que confirmes información confidencial personal o de tu cuenta. El atacante también puede invitarte a compartir tu pantalla para instalar un programa espía que capturará tus pulsaciones y credenciales.

Para comprobar si la persona que le llama procede realmente de la fuente que afirma, simplemente hazle preguntas que sólo usted y esa fuente conocerían.

Por ejemplo, si la persona dice ser de eviivo, podrías preguntarle por:
- El número de referencia de la última reserva realizada.
- El shortname de tu propiedad.
- La (segunda) pregunta y respuesta de seguridad que sólo tú y eviivo compartís.

eviivo -o cualquier otra organización auténtica- nunca se pondría en contacto contigo de la forma descrita en el guión que aparece a continuación:

Hola, soy Candice de eviivo,

Le llamamos porque creemos que ha habido actividad sospechosa en su cuenta. Es urgente que verifiquemos que todo está en orden. ¿Puedo compartir mi pantalla con usted?

Ok, para poder acceder a los detalles de su cuenta, necesito pedirle que reconfirme su contraseña ya que necesitaremos restablecerla durante la llamada. ¿Podría reconfirmar su pregunta y respuesta de seguridad?

CONSEJO

Consejos para mantenerse alerta:

- **eviivo, o cualquier otra empresa de confianza, NUNCA te pedirá que reveles tu contraseña.** Aunque es posible que te pidan la respuesta a una pregunta de seguridad, nunca te preguntarán cuál es la pregunta de seguridad.

- Cuando un proveedor te pida que compartas tu pantalla, deberá hacerlo desde la dirección oficial del sitio web del proveedor (por ejemplo, eviivo.com).

- Recuerda que cualquier empleado del proveedor puede ver y acceder a tu cuenta, así que hazle una pregunta que sólo él pueda saber (por ejemplo, el shortname de tu propiedad, la referencia de la reserva más reciente que entró en tu calendario). Un estafador no sabrá ninguna de estas respuestas.

Smishing

El smishing es el phishing a través de SMS y mensajes de texto. Los estafadores suelen enviar mensajes de texto con la intención de:

- Robar información personal o confidencial del destinatario, o
- Infectar el dispositivo del destinatario con malware.

Los estafadores falsifican con la misma facilidad una cuenta de WhatsApp, utilizando cualquier foto disponible públicamente de alguien conocido, o la foto de una figura pública y/o con autoridad.

Phishing en las redes sociales

El smishing es el phishing a través de SMS y mensajes de texto. Los estafadores suelen enviar mensajes de texto con la intención de:

- Robar información personal o confidencial del destinatario, o
- Infectar el dispositivo del destinatario con malware.

Los estafadores falsifican con la misma facilidad una cuenta de WhatsApp, utilizando cualquier foto disponible públicamente de alguien conocido, o la foto de una figura pública y/o con autoridad.

Phishing en las redes sociales

Los ciberdelincuentes suelen utilizar las redes sociales para llevar a cabo ataques destinados a robar información personal o difundir programas maliciosos. Los atacantes suelen **hacerse pasar por un amigo/compañero/familiar** en las redes sociales para engañarte y que les envíes dinero. Algunos ataques intentan secuestrar tu cuenta para lanzar ataques de seguimiento contra todos los contactos, conexiones, amigos o seguidores de tu agenda.

Este método suele basarse en

- Anuncios falsos que pueden engañarte para que hagas clic en un enlace que te redirige a una página de inicio de sesión falsa que parece legítima -pero no lo es- para capturar tus credenciales o los detalles de tu cuenta.
- Pedirte que pagues una tasa, una penalización o una tarifa ilegítima.

Las comunicaciones auténticas a través de las redes sociales siempre te remiten a la URL del sitio web oficial del vendedor. En el caso de eviivo, la dirección URL, visible en la barra de direcciones, siempre empieza por **https://eviivo.com/ o https://on.eviivo.com/.**


evilivo
Search
Help
Thu, 09 Dec
Fri, 10 Dec
Sat, 11 Dec
Sun, 12 Dec
Mon, 13 Dec
Book

eviivo

PARA MÁS INFORMACIÓN, PONTE EN CONTACTO CON

SALES@EVIIVO.COM | +34 911 876 648