Resuelve tu problema con un guiño

Vendo un sofá, ¿y el comprador quiere los datos de mi tarjeta?

Cómo comprar y vender de forma segura en los portales de anuncios clasificados



Max Paradox

Vendo un sofá, ¿y el comprador quiere los datos de mi tarjeta?

Cómo comprar y vender de forma segura en los portales de anuncios clasificados

Max Paradox

Rozwiąż swój problem z przymrużeniem oka

ISBN: 9788384905913

ALL-IN Rafał Płonkowski



ÍNDICE

INTRO 5

Capítulo 1 - Cuando un anuncio corriente se convierte en una trampa 11

Capítulo 2 - ¿Por qué un estafador resulta más convincente que tu propio sentido común? 21

Capítulo 3 - Siete señales de alarma que deberían detener tu transacción 32

Capítulo 4 - La falsa sensación de seguridad: cómo le facilitamos el trabajo al estafador 43

Capítulo 5 - No todas las oportunidades son auténticas: cómo comprar sin desconectar el sentido común 55

Capítulo 6 - El vendedor también debe tener cuidado: cómo evitar entregar el dinero junto con el artículo 65

Capítulo 7 - Pagos seguros: por qué el dinero no debería viajar fiándose de la palabra de nadie 76

Capítulo 8 - No tienes que ser amable a cualquier precio: el arte de terminar conversaciones sospechosas 87

Capítulo 9 - Una transacción bajo control: desde el primer mensaje hasta la última confirmación 100

Capítulo 10 - Detective digital sin lupa: cómo comprobar la información antes de creerte un anuncio..... 110

Capítulo 11 - ¿Un enlace para recibir dinero o un enlace hacia los problemas? Cómo reconocer mensajes y páginas de pago falsos 121

Capítulo 12 - Tu cuenta no es un guardarropa compartido: cómo proteger el acceso a los portales y a la banca electrónica.....130

Capítulo 13 - El paquete ha llegado, pero la realidad se ha olvidado de la descripción. Cómo resolver disputas después de una compra 141

Capítulo 14 - Antes de que el estafador desaparezca con tu dinero. Qué hacer cuando una transacción sospechosa se convierte en una amenaza real 153

Capítulo 15 - Cuando una estafa tiene varios niveles: casos difíciles en los que la prudencia habitual no es suficiente 164

Capítulo 16 - Cuando la prudencia pierde frente a la realidad: qué hacer si no tienes tiempo, conocimientos ni condiciones ideales.....175

Capítulo 17 - Me han estafado. ¿Y ahora qué? Cómo recuperar el control cuando el daño ya está hecho 187

Capítulo 18 - Comprar de forma segura sin vivir en una paranoia permanente: cómo mantener los buenos hábitos 198

Capítulo 19 - Cuando el sentido común se va de vacaciones: cómo reconocer el regreso de los viejos errores 210

Capítulo 20 - Vende tu sofá, no tu tranquilidad. Cómo tomar decisiones seguras por tu cuenta 222

INTRO

Pones un sofá a la venta. Las fotos están hechas, el precio es razonable y la descripción es honesta. Hasta has colocado los cojines para que parezcan más satisfechos con la vida que tú un lunes por la mañana. Pasan siete minutos y llega un mensaje. El comprador está decidido, no regatea, no pregunta por las medidas, no le interesa el color ni el hecho de que el reposabrazos izquierdo todavía conserve recuerdos de su anterior propietario. Quiere comprarlo inmediatamente. Solo tiene una petición: debes hacer clic en el enlace que te ha enviado, introducir los datos de tu tarjeta y confirmar la recepción del dinero.

Qué curioso. Estás vendiendo un sofá por seiscientos eslotis y alguien se comporta como si acabara de invitarte a gestionar un sistema interbancario de compensación.

Y aquí comienza una historia que puede terminar de tres maneras. La primera: reconoces la estafa, te niegas y vuelves a ver tu serie. La segunda: empiezas a sospechar que algo no encaja, pero el amable comprador explica el procedimiento con tanta soltura que finalmente haces clic. La tercera: unos minutos después, miras el teléfono preguntándote por qué, en lugar de recibir seiscientos eslotis, acabas de autorizar una operación que jamás habías pensado realizar.

Este libro existe para que el primer escenario se convierta en tu reacción natural. Sin necesidad de obtener un doctorado en ciberseguridad, desarrollar una paranoia permanente ni tratar a cualquier persona interesada en una mesita de segunda mano como si perteneciera a una organización criminal internacional.

Los portales de anuncios clasificados son un invento fantástico. Permiten vender cosas que ya no necesitamos, encontrar artículos usados a buen precio y entregar a otra persona un objeto que en nuestra casa no hace más que ocupar espacio. Gracias a ellos, un objeto puede tener una segunda vida y nuestro hogar puede recuperar un trozo de suelo. El problema es que, allí donde coinciden desconocidos, dinero, prisas e internet, también aparecen personas que han decidido ganarse la vida aprovechándose de la confianza ajena.

Algunas estafas son bastante rudimentarias. El mensaje parece haber sido traducido automáticamente de un idioma que su autor nunca ha escuchado, y el enlace conduce a una página cuya dirección recuerda a una contraseña inventada por un gato mientras paseaba sobre el teclado. Otras son mucho más convincentes. El estafador puede conocer el nombre de un portal popular, utilizar sus elementos gráficos, imitar las notificaciones de una empresa de mensajería o hacerse pasar por un empleado del banco. Sabe hablar con calma, educación y firmeza. A veces da la impresión de conocer los procedimientos mejor que el verdadero servicio de atención al cliente.

Sin embargo, lo más importante es que un estafador no necesita ser un genio de la informática. Le basta con comprender bien a las personas.

Sabe que quien vende algo se alegra cuando encuentra comprador rápidamente. Sabe que quien compra teme perder una buena oportunidad. Sabe que la mayoría queremos terminar la operación sin complicaciones, evitar parecer excesivamente desconfiados y no hacer preguntas que puedan sonar tontas. Por eso, un estafador rara vez empieza la conversación diciendo: «Buenos días, me

gustaría robarle su dinero». En lugar de eso, propone una solución cómoda, asegura que todo es seguro y te invita a dar un pequeño paso más.

Ese pequeño paso puede convertirse en el clic más caro de toda la historia.

Lo interesante es que la víctima no tiene por qué ser alguien que se lleve mal con la tecnología. Puedes utilizar la banca electrónica todos los días, comprar habitualmente desde el móvil y entender perfectamente cómo funciona un pago con tarjeta. Y, aun así, dejarte sorprender en una situación en la que tienes la atención puesta en algo completamente distinto. Porque, al fin y al cabo, no te sientas delante del ordenador con la intención de participar en un ejercicio de detección de ciberdelitos. Quieres vender una bicicleta infantil, comprar un teléfono usado o deshacerte de un armario que lleva dos años bloqueando el acceso a un enchufe.

La estafa se aprovecha precisamente de esa normalidad.

También existe la otra cara de la transacción. Quien compra tiene sus propios motivos para actuar con prudencia. Un precio atractivo, unas fotografías excelentes y la afirmación «estado impecable, usado solo unas pocas veces» no significan automáticamente que el artículo exista. Hay anuncios falsos, intentos de conseguir anticipos fraudulentos, presiones para pagar fuera del sistema oficial y paquetes cuyo contenido se parece tanto a la descripción como la fotografía de un hotel de lujo a una noche en un armario de escobas. Sin embargo, no todas las transacciones fallidas son estafas. A veces el vendedor realmente no ha advertido un defecto, el mensajero ha confundido los paquetes o las dos partes han interpretado los acuerdos de manera diferente. Saber distinguir entre un

error, una disputa y un engaño deliberado es tan importante como reconocer enlaces sospechosos.

No pretendo convencerte de que internet sea una jungla donde detrás de cada anuncio acecha un delincuente con un portátil y una carcajada siniestra. La mayoría de las transacciones cotidianas pueden realizarse con normalidad y seguridad. Se trata de algo mucho más práctico: aprender a reconocer el momento en que una compraventa normal empieza a parecerse a una representación cuidadosamente dirigida por alguien que quiere tomar el control de tus decisiones.

En este libro examinaremos por qué resulta tan fácil confiar en un mensaje aparentemente creíble, cómo funcionan los falsos justificantes de pago, qué puede significar que alguien te pida un código, los datos de tu tarjeta o una autorización adicional, y por qué un mensaje urgente de un supuesto repartidor no siempre procede de una empresa de mensajería. También abordaremos cómo elegir ofertas de manera segura, comprobar la fiabilidad de los vendedores, acordar las condiciones de una transacción y dejar constancia de lo pactado para que, si surgen problemas, no te quedes únicamente con una conversación titulada «Pero usted me lo había prometido».

No vamos a construir nuestra sensación de seguridad sobre una única regla mágica. La advertencia habitual «nunca hagas clic en los enlaces» suena contundente, pero por sí sola enseña bastante poco. Un enlace puede llevar a una página auténtica o a una imitación extraordinariamente bien preparada. Del mismo modo, no todas las solicitudes de información adicional indican que se esté cometiendo un delito. Lo importante es el contexto: quién te pide algo, para qué, a través de qué canal, si puedes verificar la solicitud

por tu cuenta y qué estás autorizando realmente. La seguridad no consiste en memorizar cien prohibiciones, sino en comprender unos cuantos mecanismos que aparecen una y otra vez bajo distintas formas.

También será importante saber qué hacer cuando algo ya ha salido mal. Porque una persona que descubre su error después de hacer clic necesita medidas concretas, no una conferencia sobre lo mucho que debería haberse cuidado. Dependiendo de la situación, puede ser necesario ponerse rápidamente en contacto con el banco, bloquear la tarjeta, proteger la cuenta, conservar las pruebas o denunciar lo ocurrido ante las instituciones correspondientes. No todas las pérdidas pueden recuperarse, pero retrasar la reacción por vergüenza puede empeorar todavía más las cosas. Nadie recupera su dinero por pasarse tres horas llamándose idiota.

¿Y si hasta ahora nunca te ha ocurrido nada parecido? Mucho mejor. La lección más barata sobre las estafas es aquella que no tienes que pagar con tus propios ahorros.

No necesitas dejar de confiar en las personas después de leer este libro. Basta con que dejes de considerar la amabilidad, la urgencia y un mensaje de apariencia profesional como pruebas de fiabilidad. Puedes seguir vendiendo, comprando, negociando y disfrutando de una buena oportunidad. Solo que, antes de seguir una instrucción poco habitual, te harás algunas preguntas adecuadas y comprobarás aquello que puedas verificar independientemente de lo que diga tu interlocutor.

Porque cuando vendes un sofá, lo que debería interesarle al comprador es, ante todo, el sofá.

Y si muestra más interés por el número de tu tarjeta, quizá convenga plantearse que, en realidad, no está buscando un sitio donde sentarse.

Capítulo 1 - Cuando un anuncio corriente se convierte en una trampa

Pones a la venta una cafetera. Funciona, tiene un aspecto bastante decente y su único defecto es que últimamente ha servido más como decoración de la encimera que como aparato para preparar bebidas. Fijas el precio en trescientos eslotis, añades unas fotografías y publicas el anuncio. No han pasado ni cinco minutos cuando aparece una persona interesada. No pregunta por la marca, el estado técnico ni el motivo de la venta. Ni siquiera intenta conseguir un descuento de veinte eslotis, algo que, en el mundo de los anuncios por internet, resulta casi tan extraordinario como encontrarse un unicornio en el aparcamiento de un supermercado.

El comprador escribe que todo le parece perfecto. Quiere pagar inmediatamente y contratar un servicio de mensajería. Te envía un enlace para confirmar la transacción. Tiene un aspecto profesional, incluye elementos gráficos familiares y muestra un aviso indicando que el dinero está esperando a ser recibido. Solo tienes que introducir los datos de tu tarjeta bancaria.

Durante un instante te preguntas por qué hace falta una tarjeta si eres tú quien debe recibir el dinero. Pero el comprador responde rápidamente, con educación y absoluta seguridad. Explica que así funciona el nuevo sistema de pagos. Añade que lo ha utilizado muchas veces. Finalmente, te recuerda que el mensajero llegará pronto, de modo que lo mejor es resolverlo todo cuanto antes.

Acabas de entrar en una situación en la que el desarrollo de la transacción ya no depende de la cafetera. El producto más importante se ha convertido en tu atención.

¿Por qué es tan fácil confundir el interés con la fiabilidad?

Cuando vendemos algo por internet, esperamos que las cosas sigan un desarrollo determinado. Alguien encuentra la oferta, hace algunas preguntas, acordamos las condiciones, se realiza el pago y entregamos el artículo. Si el comprador se muestra educado y declara que está dispuesto a pagar, automáticamente lo situamos dentro de ese escenario. Nuestro cerebro no analiza cada mensaje como si fuera una prueba independiente de una investigación criminal. Recurre a experiencias anteriores, reconoce patrones familiares e intenta ahorrar energía. Si tratáramos cada conversación cotidiana como un interrogatorio a un sospechoso, hacer la compra llevaría más tiempo que reformar un apartamento.

Los estafadores aprovechan esta tendencia natural a simplificar la realidad. Sus mensajes suelen empezar exactamente como deberían comenzar las conversaciones auténticas. Preguntan si el artículo sigue disponible, confirman su interés, proponen una forma de pago y hablan del envío. Solo después aparece el elemento que cambia la naturaleza de la transacción: un enlace inusual, una solicitud de datos, una comisión adicional o la necesidad de autorizar una operación.

Conviene comprender que una estafa por internet rara vez consiste en una única gran mentira. Con mucha más frecuencia se desarrolla mediante una sucesión de pequeños pasos, cada uno de los cuales parece una consecuencia razonable del anterior. Primero aceptas vender. Después aceptas realizar el envío. A continuación, accedes a comprobar cierta información. Finalmente,

pueden pedirte que hagas algo que jamás habrías aceptado si te lo hubieran planteado al principio de la conversación.

Es un poco como si alguien viniera a ver tu frigorífico y, diez minutos después, consiguiera convencerte de que para comprarlo necesita tener acceso a tu cuenta bancaria. Si hubiera empezado con semejante propuesta, probablemente le habrías cerrado la puerta. Sin embargo, una historia presentada de la manera adecuada puede conseguir que algo absurdo empiece a parecer un procedimiento perfectamente normal.

Las tres partes de una misma transacción

En un anuncio corriente participan al menos dos personas: el vendedor y el comprador. A menudo también intervienen una plataforma de anuncios, un proveedor de servicios de pago o una empresa de transporte. Cada participante desempeña una función determinada. El vendedor ofrece el artículo, el comprador paga por él y las demás entidades pueden facilitar el pago, la comunicación o la entrega.

El problema empieza cuando una sola persona intenta asumir el papel de todas las demás.

Imagina a un comprador que te envía personalmente un enlace a un supuesto sistema de pagos, te explica cómo funciona, garantiza que es seguro y te informa de que todo ha sido aprobado. Toda la información sobre la transacción procede de una única fuente. No tienes ninguna confirmación independiente y, aun así, puedes tener la impresión de que estás participando en un proceso supervisado por varias instituciones profesionales.

Esta es precisamente una de las trampas más importantes: confundir la información proporcionada por tu

interlocutor con la información confirmada por un sistema independiente.

Si alguien escribe que ya ha pagado, eso todavía no significa que el dinero se haya transferido realmente. Si envía una captura de pantalla con un justificante de transferencia, no tienes la certeza de que el documento sea auténtico ni de que la operación haya finalizado correctamente. Si recibes un mensaje que se parece a una notificación de la plataforma, deberías comprobarlo en el servicio oficial o en la aplicación que hayas abierto por tu cuenta.

Una captura de pantalla es una imagen. Puede representar la realidad, pero también puede representar una realidad que nunca ha existido. Del mismo modo, una fotografía de una persona junto a un coche de lujo no demuestra que sea su propietaria. Quizá simplemente le haya pedido al verdadero dueño que se aparte un momento del capó.

La señal de alarma no siempre es roja

Muchas personas esperan que un mensaje sospechoso tenga una apariencia sospechosa. Los errores lingüísticos, los caracteres extraños, un número de teléfono extranjero o las expresiones poco naturales pueden ser, efectivamente, señales de advertencia. Sin embargo, no conviene aferrarse a la imagen del estafador torpe que redacta mensajes tan desastrosos que hasta el corrector automático se niega a colaborar.

Los mensajes actuales pueden estar perfectamente escritos, ser educados y hacer referencia al artículo que vendes. El estafador puede responder a tus preguntas, mencionar la ciudad en la que vives e incluso utilizar detalles

concretos de tu anuncio. Nada de esto demuestra que sea honrado. Significa únicamente que alguien ha leído la oferta o ha aprovechado la información que tú mismo has publicado.

Por eso, resulta más útil examinar el sentido de sus solicitudes que juzgar su manera de expresarse. ¿La petición tiene realmente relación con la transacción acordada? ¿Es indispensable realizar esa acción? ¿Puedes llevarla a cabo dentro del servicio oficial en lugar de utilizar el enlace recibido? ¿Comprendes exactamente qué ocurrirá cuando confirmes la operación?

Cuando vendes un artículo, resulta especialmente preocupante que alguien te exija los datos completos de tu tarjeta, el código CVV/CVC, códigos de autorización o las credenciales de acceso al banco simplemente para recibir el pago. Una transferencia bancaria ordinaria no exige proporcionar esa información al comprador. Los sistemas oficiales de pago pueden tener sus propios procedimientos, pero deberías consultarlos dentro de una aplicación o un servicio de confianza, no siguiendo las instrucciones de un desconocido.

Esto no significa que cualquier petición poco habitual constituya automáticamente una prueba de delito. A veces una persona realmente desconoce las normas de la plataforma, utiliza otro método de entrega o simplemente explica sus intenciones con poca habilidad. La diferencia está en cómo reacciona cuando intentas comprobar tranquilamente la información. Un comprador honrado puede impacientarse, pero no debería exigirte que reveles datos confidenciales ni que autorices una operación que no comprendes.

La confianza no es una suscripción ilimitada

Las personas suelen abordar las transacciones de manera bastante radical. O confían en alguien o lo consideran sospechoso. Sin embargo, la confianza puede concederse gradualmente y solo en la medida en que sea realmente necesaria.

Puedes confiar lo suficiente en tu interlocutor como para responder a una pregunta sobre el estado del artículo. Puedes acordar una fecha de recogida y un método de pago. Pero eso no significa que tengas que facilitarle información sobre tu tarjeta, los movimientos de tu cuenta o los códigos que recibes del banco. Haber realizado correctamente una acción no concede a nadie el derecho de exigir las siguientes.

Supongamos que vendes una cámara fotográfica usada. El comprador solicita una fotografía adicional en la que se vean el modelo y el objetivo. Es una petición comprensible, aunque al hacer la foto conviene prestar atención a los documentos y otros datos privados que puedan aparecer al fondo. Después, tu interlocutor pregunta si puedes enviar el paquete. Eso también encaja dentro de una transacción normal. La línea se cruza cuando exige que accedas a tu banco desde una página indicada en su mensaje. Esa petición ya no tiene ninguna justificación relacionada con la venta de la cámara.

Por tanto, la frontera de la seguridad no se encuentra entre hablar con un desconocido y guardar silencio absoluto. Se encuentra entre la información necesaria para realizar la transacción y el acceso a tu dinero y tus cuentas.

Conviene recordar una regla sencilla: aceptar una cosa no significa aceptar todo lo que a tu interlocutor se le ocurra pedir después.

El primer minuto de sensatez

La habilidad más útil al comienzo de una transacción consiste en detenerse cuando alguien cambia inesperadamente las reglas. No necesitas conocimientos especializados para darte cuenta de que habíais acordado vender un artículo y, de repente, la conversación gira en torno a tus datos bancarios.

Puedes realizar una comprobación rápida mediante cuatro preguntas:

1. ¿Qué estoy vendiendo o comprando exactamente y qué condiciones hemos acordado ya?
2. ¿Qué nueva acción me está pidiendo mi interlocutor y por qué?
3. ¿Puedo confirmar por mi cuenta, mediante una fuente oficial, que esa acción es necesaria?
4. ¿Qué riesgo corro si la realizo sin comprobarla?

Estas preguntas son especialmente útiles cuando tu interlocutor intenta acelerar la decisión. Para responderlas no hace falta emprender una investigación de varias horas. Basta con interrumpir la conversación, abrir la aplicación oficial y comprobar si realmente existe la transacción indicada o si hay alguna acción pendiente.

Si un mensaje afirma que tienes un pago esperando a ser recibido, pero no encuentras ninguna operación correspondiente dentro del sistema oficial, no intentes solucionar la situación siguiendo más instrucciones del comprador. Antes debes determinar si la notificación es auténtica.

Es posible que el comprador proteste. Puede escribir que no tiene tiempo, que ya ha pagado y que tu comportamiento

está complicando algo muy sencillo. En ese caso, basta con responder tranquilamente: «Realizaré la transacción únicamente a través del sistema oficial. No abro enlaces externos para confirmar pagos».

No necesitas justificar tu decisión mediante quince mensajes. Vender de forma segura no es un concurso para ver quién presenta los argumentos más convincentes.

Cuando al otro lado hay una persona de verdad

Llegados a este punto, conviene hacer una aclaración importante. La desconfianza excesiva puede dificultar las transacciones normales. No todos los compradores que responden rápidamente son estafadores. No todos los que aceptan el precio sin negociar están preparando un fraude. Existen personas que realmente necesitan una cómoda de segunda mano, saben cuánto quieren pagar y no tienen ningún interés en participar en negociaciones que parecen sesiones parlamentarias.

El objetivo no es elaborar una lista de características de personalidad que permita reconocer a un delincuente. Esa lista sería poco fiable. Lo importante es observar comportamientos concretos relacionados con el dinero, la información y el control de la transacción.

Un buen ejemplo es la recogida en persona. El comprador puede pedir que le permitan examinar el artículo y proponer pagar en el momento de recogerlo. No hay nada extraño en ello. El vendedor, por su parte, puede fijar el lugar de encuentro, solicitar puntualidad y establecer claramente las condiciones. La prudencia consiste aquí en escoger un lugar razonable, proteger la privacidad y asegurarse de que el pago se haya realizado realmente antes de entregar el objeto.

Si alguien paga en efectivo, puedes comprobar tranquilamente la cantidad recibida. En caso de transferencia, debes verificar que el dinero se haya abonado efectivamente en tu cuenta, en lugar de confiar exclusivamente en un mensaje o una imagen del justificante. Cuando se utiliza un sistema oficial de pagos y protección de transacciones, hay que respetar sus normas vigentes y comprobar el estado de la operación en la propia cuenta.

Estas medidas no significan que estés acusando a la otra persona de actuar de mala fe. Son componentes normales de un intercambio responsable.

En un restaurante no insultas al camarero cuando compruebas la cuenta. Del mismo modo, un comprador no debería sentirse ofendido simplemente porque verifiques el pago. Aunque, por supuesto, puedes hacerlo con una expresión tan grave como si acabaras de descubrir una trama internacional relacionada con la venta de una lámpara de noche usada. En ese caso, es posible que el ambiente se vuelva un poco tenso.

La diferencia más importante

En una transacción honrada, ambas partes buscan realizar un intercambio: un artículo a cambio del pago acordado. Pueden surgir preguntas, negociaciones y complicaciones organizativas, pero el objetivo fundamental sigue estando claro.

En una estafa, el artículo suele convertirse únicamente en un pretexto para conseguir que realices otra acción. Puede que al estafador no le interese comprar ni vender absolutamente nada. Lo que necesita son tus datos, tu dinero, acceso a tu cuenta o la autorización de una operación. Por eso conviene fijarse no solo en lo que dice tu

interlocutor, sino también en la acción hacia la que intenta conducirte una y otra vez.

Si la conversación sobre una cafetera usada tiene cada vez menos relación con la cafetera y cada vez más con tu banco, es evidente que algo ha cambiado de dirección.

La próxima vez que recibas un mensaje de un comprador extraordinariamente decidido, no tienes que suponer automáticamente lo peor. Puedes responder, acordar los detalles y continuar tranquilamente con la venta. Pero conserva siempre el derecho a verificar por tu cuenta cualquier operación relacionada con tu dinero o tu información confidencial.

Un buen comprador quiere completar la transacción. Un estafador quiere que dejes de hacer preguntas.

Y precisamente por eso, unas cuantas preguntas sensatas pueden valer más que el filtro antispam más avanzado.

Capítulo 2 - ¿Por qué un estafador resulta más convincente que tu propio sentido común?

Son las 21:43. Estás sentado en el sofá, revisando mensajes y preguntándote si todavía merece la pena preparar un té cuando dentro de poco deberías estar durmiendo. De repente, el teléfono anuncia una nueva notificación. Alguien quiere comprar tu móvil usado. El precio es de ochocientos eslotis y la persona interesada asegura que pagará inmediatamente.

En circunstancias normales, leerías el mensaje, responderías y volverías a tus asuntos. Esta vez, sin embargo, la conversación empieza a acelerarse. El comprador escribe que necesita un envío rápido porque el teléfono será un regalo. Asegura que el pago ya se ha realizado, pero que el sistema requiere una confirmación adicional. Poco después te envía una captura de pantalla y te recuerda que la transacción podría cancelarse si no completas el procedimiento en unos minutos.

No eres una persona especialmente crédula. Sabes utilizar internet y no tienes ninguna intención de regalar tu dinero a desconocidos. Sin embargo, empiezas a actuar más deprisa de lo que normalmente tardas en tomar decisiones.

¿Por qué?

Porque el estafador no intenta convencerte únicamente mediante argumentos. Intenta influir en las condiciones en las que tomas la decisión.

Las prisas cambian nuestra manera de pensar

Imagina dos situaciones. En la primera, alguien te pregunta si estarías dispuesto a introducir los datos de tu tarjeta en una página que no conoces para recibir el dinero de un teléfono vendido. Tienes tiempo para pensar. Probablemente considerarías sospechosa la propuesta.

En la segunda situación, recibes información de que el comprador ya ha pagado, el mensajero está esperando la confirmación y el sistema cerrará la transacción dentro de cinco minutos. Ya no analizas tranquilamente si todo el procedimiento tiene sentido. Empiezas a pensar qué debes hacer para no perder la venta.

Esta diferencia es fundamental. La sensación de urgencia puede desplazar tu atención desde la pregunta «¿Es seguro?» hacia otra muy distinta: «¿Me dará tiempo?».

Los estafadores comprenden perfectamente el valor de ese cambio. Por eso utilizan mensajes que sugieren que la oferta está a punto de desaparecer, que el pago será devuelto o que la posibilidad de recibir el dinero caducará. No siempre recurren a amenazas directas. A veces basta con un recordatorio educado: «Por favor, confirme rápidamente porque no puedo seguir esperando».

En las ventas auténticas también existen limitaciones de tiempo. Un comprador puede tener libre una sola tarde y un vendedor puede necesitar una decisión rápida. Las prisas, por sí solas, no demuestran que exista una estafa. Se vuelven especialmente peligrosas cuando alguien las utiliza para obligarte a realizar una acción que no comprendes o que no puedes verificar de manera independiente.

La respuesta más sencilla es esta: no permitas que el horario de otra persona sustituya tu propio criterio de seguridad.

Si una transacción exige realizar una operación desconocida relacionada con el dinero, detente. Aunque tu interlocutor asegure que solo quedan tres minutos. Perder la oportunidad de vender un teléfono usado resulta menos doloroso que perder el dinero de tu cuenta bancaria.

Además, una transacción honrada que no puede soportar unos minutos de comprobación probablemente merezca una reflexión adicional.

Una autoridad que nadie ha comprobado

Otra manera de ganarse la confianza consiste en invocar instituciones. El estafador ya no habla exclusivamente en su propio nombre. Afirma representar a una plataforma de anuncios, un departamento de pagos, una empresa de mensajería o un banco. Utiliza nombres, logotipos y vocabulario que transmiten la impresión de estar siguiendo un procedimiento oficial.

Las personas suelen tomarse más en serio las comunicaciones institucionales que los mensajes de un desconocido. Es comprensible. Un banco puede enviar información importante, una plataforma puede exigir determinadas acciones y una empresa de mensajería puede necesitar datos adicionales para entregar un paquete.

El problema es que afirmar que se representa a una institución no demuestra la identidad del remitente.

Un mensaje firmado por el «Departamento de Seguridad» no se convierte automáticamente en seguro. El logotipo de una empresa puede copiarse. El nombre del remitente puede ser engañoso, igual que el número de teléfono que aparece en la pantalla. Ni siquiera conocer correctamente tu nombre y los detalles del anuncio demuestra que estés hablando con un empleado autorizado.

El estafador puede escribir: «De acuerdo con el procedimiento del proveedor de servicios de pago, es necesario confirmar su identidad». Suena serio. Especialmente si el mensaje incluye referencias a la seguridad de la transacción, un número de incidencia y la garantía de que todos los pasos son habituales.

Sin embargo, utilizar un lenguaje profesional no demuestra que el mensaje proceda de un profesional. Es perfectamente posible describir con gran elegancia una operación absurda. La frase «Para completar la transferencia de fondos, le rogamos que autorice el cargo en su cuenta» puede seguir significando que alguien quiere quitarte dinero. Ponerle un traje a una petición fraudulenta no cambia su naturaleza.

Por eso debes comprobar la autenticidad de una comunicación fuera del canal indicado por el interlocutor sospechoso. Si alguien afirma representar a una plataforma, abre por tu cuenta su aplicación oficial. Si se presenta como empleado del banco, termina la conversación y contacta con la entidad mediante un número o una aplicación que conozcas por una fuente fiable.

No utilices el número proporcionado por la misma persona cuya identidad estás intentando comprobar. Sería parecido a preguntarle a un desconocido si es un estafador y considerar su respuesta «Por supuesto que no» como una confirmación suficiente.

La amabilidad que sale cara

No todas las manipulaciones se basan en el miedo. Algunas aprovechan nuestros buenos modales.

El comprador puede resultar extraordinariamente simpático. Escribe frases completas, se disculpa por la hora,