CAPÍTULO IX

Del phishing que casi arruinó al señor del segundo y de por qué el miedo es la mejor llave maestra

Aurelio Campos tenía setenta años, había pasado treinta y dos de ellos como funcionario de Correos y era el tipo de persona que imprime los extractos bancarios y los guarda en una carpeta ordenada por trimestres. Desconfiaba de las aplicaciones de móvil, pagaba el seguro del coche en ventanilla y consideraba que la banca online era una comodidad razonable para los jóvenes y un riesgo innecesario para quien ya tenía un sistema que funcionaba.

Este perfil —ordenado, prudente, escéptico ante las novedades tecnológicas— es exactamente el perfil que los manuales de ciberseguridad describen como de riesgo elevado ante el phishing. No porque las personas prudentes sean menos inteligentes, sino porque la prudencia construye una confianza en los propios criterios que puede convertirse en el punto ciego por el que entra el engaño. Quien cree que nunca caería en una trampa digital es, en cierta medida, más vulnerable que quien sabe que podría caer.

Aurelio Campos recibió el SMS un miércoles a las once y diecisiete de la mañana.

El SMS decía, con la sobriedad y el tono institucional que Aurelio asociaba a los mensajes legítimos de su banco: *"BankCorp: hemos detectado un acceso no autorizado a su cuenta. Para proteger sus fondos, verifique su identidad en el siguiente enlace en las próximas 2 horas."*

El enlace llevaba a una página web que era, para cualquier observador sin conocimientos técnicos específicos, indistinguible de la página real del banco. Mismo logotipo, mismo esquema de colores, mismo formulario de acceso. La única diferencia, imperceptible sin buscarla expresamente, era la dirección del navegador: *BankCorp-verificacion-segura.com* en lugar de *BankCorp.es*.

Aurelio leyó el SMS. Miró el reloj. Pensó en sus ahorros, en los treinta y dos años de nóminas depositadas, en la pensión que llegaba puntual el primer día de cada mes. Pensó en *acceso no autorizado* y en *las próximas 2 horas*. Sintió lo que el SMS estaba diseñado para que sintiera: urgencia y miedo.

Hizo clic en el enlace.

— ✦ —

Del mecanismo y de sus piezas

El phishing —del inglés *fishing*, pescar— es una técnica de ingeniería social basada en la suplantación de identidad digital. El atacante se hace pasar por una entidad legítima para obtener de la víctima sus credenciales de acceso o sus datos bancarios.

Lo que hace eficaz al phishing no es la sofisticación técnica, que en muchos casos es mínima. Lo que lo hace eficaz es la palanca psicológica: la urgencia fabricada. *Tiene dos horas. Su cuenta está en riesgo. Actúe ahora.* Esa presión temporal desactiva el pensamiento crítico de la misma manera que lo desactiva cualquier emergencia percibida. El cerebro en modo de alerta no verifica URLs. El cerebro en modo de alerta actúa.

Aurelio introdujo su DNI, su contraseña de banca online y el código de verificación que llegó por SMS a su móvil —un código real, generado por el sistema del banco real, que el sitio falso solicitó en tiempo real al banco real haciéndose pasar por Aurelio. En el tiempo que Aurelio tardó en leer el código y escribirlo en el formulario, alguien en algún lugar del mundo completó una operación de transferencia desde su cuenta hacia una cuenta mula en un banco de Europa del Este.

Cuarenta y siete minutos después de haber recibido el SMS, Aurelio Campos tenía dos cuentas vacías. La suma total era de dieciséis mil trescientos euros.

Lo descubrió tres horas más tarde, cuando fue a mirar el saldo para verificar que la pensión había llegado.

— ✦ —

De cómo don Justo no lo había visto venir

Don Justo se enteró esa misma tarde, cuando Aurelio llamó a su puerta con la cara de quien acaba de recibir una noticia que todavía no ha terminado de procesar.

—Me han vaciado las cuentas —dijo Aurelio.

Don Justo lo hizo pasar. Lo sentó. Le puso agua. Y mientras Aurelio le explicaba lo del SMS y el enlace y el formulario, don Justo sintió algo que no había sentido en muchos meses de investigación: la incomodidad específica de quien reconoce que no estaba mirando donde debía.

Llevaba meses vigilando furgonetas, aparcamientos, persianas y ventanas. Llevaba meses construyendo teorías sobre bandas organizadas y patrones de punto fijo. Y mientras él elaboraba diagramas de flujo sobre el mercadillo de segunda mano del sótano, Aurelio Campos había perdido en cuarenta y siete minutos los ahorros de años sin que hubiera ni furgoneta, ni persiana, ni nada que señalar con el dedo.

No había escena del crimen. No había agresor con perfil. No había nada que encajara en el esquema visual del true crime que don Justo había consumido durante meses. El crimen de Aurelio era invisible, rápido, limpio y devastadoramente efectivo. Y era, estadísticamente, mucho más probable que cualquiera de los crímenes sobre los que había tomado notas.

Anotó en el cuaderno, esa noche, con letra más pequeña que de costumbre:

> *El true crime me enseñó a buscar el crimen dramático. El crimen real es este.*

— ✦ —

De las señales que permiten detectarlo y de por qué importan

Acompañó a Aurelio a interponer la denuncia al día siguiente. Durante el camino, don Justo le explicó lo que sabía sobre el phishing. No desde el cuaderno: desde la memoria.

> —Las señales están siempre —dijo don Justo—. El problema es que las vemos después. La primera es la urgencia: cualquier comunicación que te exige actuar en pocas horas es una alerta. Los bancos reales bloquean cuentas cuando detectan actividad sospechosa, no te piden que actúes tú en dos horas. La segunda es el enlace: nunca hay que hacer clic en un enlace de un SMS o un correo que diga ser de un banco. Si hay un problema real, se entra directamente escribiendo la dirección en el navegador o llamando al número del dorso de la tarjeta. La tercera es la petición del código de verificación: ningún banco legítimo te pide que introduzcas en ningún formulario el código que acaba de llegarte por SMS. Ese código es para autenticarte tú, no para dárselo a nadie más.

Aurelio escuchó en silencio.

—¿Y por qué no me lo dijo antes? —dijo, sin acritud.

Don Justo no contestó durante unos pasos.

—Porque estaba mirando otras cosas —dijo finalmente.

Era la respuesta más honesta que había dado en meses. Y las dos personas que la escucharon —Aurelio y él mismo— sabían exactamente a qué se refería.

— ✦ —

Del sesgo del superviviente en el true crime

Inés lo había explicado en el episodio 44 de *La Raíz del Asunto*, que don Justo recordaba bien: el **sesgo del superviviente** aplicado al true crime. La industria del entretenimiento criminal selecciona los casos más extremos, más dramáticos, más estadísticamente excepcionales, porque esos son los que generan audiencia. El resultado es una percepción completamente distorsionada de la realidad criminal.

> —Los delitos más frecuentes —decía Inés en ese episodio— no tienen serie de plataforma. No tienen podcast de diez episodios. No tienen canal de YouTube con ochenta mil suscriptores. Los delitos más frecuentes son los fraudes informáticos, las estafas telefónicas, los hurtos, la violencia en el entorno de pareja. Son los que más personas sufren cada año en España. Son los que más probabilidades tiene cualquier ciudadano de sufrir en su vida. Y son los que menos aparecen en el contenido de true crime, precisamente porque no tienen la forma dramática que el entretenimiento requiere.

Esa noche, después de dejar a Aurelio en su portal, don Justo releyó esa anotación en el cuaderno. Y añadió debajo, con letra diferente, más despacio:

> *Me pasé un año vigilando lo que no iba a pasar. No vi lo que pasó. Aurelio perdió dieciséis mil euros mientras yo dibujaba diagramas de flujo sobre el mercadillo del aparcamiento.*

Cerró el cuaderno.

Remedios, que había visto entrar a don Justo con la cara que tenía, puso el guiso al fuego sin decir nada. Algunas noches, la mejor respuesta es el olor a caldo caliente en una cocina pequeña.

Notas

Los fraudes informáticos son el delito de mayor crecimiento en España en la última década y representan ya cerca del 20% de los delitos conocidos. Ante un SMS o correo que solicite datos bancarios con urgencia: no haga clic en ningún enlace, llame directamente al número del dorso de su tarjeta y acceda a su banca online únicamente escribiendo la dirección en el navegador. Si ha sido víctima de phishing, contacte de inmediato con su banco y denuncie en cualquier comisaría o en el portal online del Ministerio del Interior.

No son casos. Son personas.

CAPÍTULO X

De la sextorsión del chico del tercero, el silencio más difícil y lo que don Justo Severo aprendió sobre el daño que no se ve

CONTINUARÁ …

— Don Justo Severo Recio, portero jubilado de Olmeda del Espino —

En mis tiempos de portería aprendí que el daño casi nunca llega
anunciándose. Llega por un SMS que parece del banco,
por una pantalla encendida a deshora, por el silencio
de quien tiene vergüenza de contar lo que le pasó.

Ya no hay gigantes que combatir. Ni siquiera molinos de viento.
Los enemigos de hoy no tienen cuerpo ni cara: son algoritmos,
son perfiles falsos, son puertas que alguien dejó abiertas sin querer.

Y no hay bálsamo de Fierabrás que cure esto.
Solo hay ciencia: la que estudia cómo operan quienes hacen daño.
Y hay entendimiento: el de quien aprende a ver las señales
antes de que el daño ya esté hecho.

Quien auxilio requiera, que hable.

No hace falta que sea un caso.
Hace falta que sea una persona. Y eso ya lo es.

No prometo hazañas. Prometo escuchar, preguntar a quien sabe más
que yo, y no inventarme el remedio si no lo conozco.
Que eso, ya lo he aprendido a tiempo, suele ser suficiente.

Dulcinea del True Crime · No son casos. Son personas.