Cuadernos del CIPeCo

DOSSIER
Escenarios contemporáneos del periodismo: reflexiones teóricas, análisis y experiencias

Publicación semestral del Centro de Investigaciones en Periodismo y Comunicación "Héctor Toto Schmucler" (FCC - UNC)

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]

Educar e informar: estrategias de comunicación para prevenir estafas digitales

Giuliana Mercol
Facultad de Ciencias de la Comunicación (FCC-UNC)
giulianamercol@mi.unc.edu.ar

Resumen

La forzada digitalización del 2020 y el desconocimiento digital de muchos usuarios generaron un incremento del 3.000% en las estafas digitales. Los ciberdelitos proliferaron en un contexto de fragmentación de las campañas de prevención, las que proveen información incompleta y, por lo general, solo apuntan a un tipo de estafa. Retomando una investigación iniciada en la tesis de grado de la Licenciatura en Comunicación Social[1], el artículo expone y analiza el estado de la cuestión, revisa críticamente la comunicación de las entidades bancarias, y propone tópicos y estrategias que se deberían considerar a la hora de diagramar una campaña para concientizar sobre los ciberdelitos.

Palabras claves: estafas digitales, ciberdelitos, estrategias de comunicación, alfabetización digital, ingeniería social

Introducción

La pandemia por COVID-19 trajo aparejada no solo una crisis económica y sanitaria, sino que también emergieron otras problemáticas. El aislamiento consecuente obligó a digitalizar numerosos trámites que previamente se realizaban de manera presencial. Por ejemplo, hasta el 2020, a la hora de gestionar cuentas bancarias, la comunidad solía dirigirse a una sucursal física y allí, en persona, realizaba los trámites necesarios. Lo mismo

[1] "A este cuento mejor que no te lo cuenten" C. Angeletti y G. Mercol. Tesis de grado (no publicada). FCC-UNC.

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]

sucedía a la hora de solicitar créditos, pagar cuentas u otros movimientos de dinero. En ese interín de adaptación, proliferaron los ciberdelitos, fundamentalmente los financieros.

Esta situación, sumada a la falta de conocimiento digital de muchos usuarios, desencadenó un incremento exponencial de los casos de estafas o fraudes relacionados con las entidades bancarias. Argentina no cuenta con estadísticas centralizadas para determinar el verdadero estado de situación, pero de acuerdo a los reportes del Observatorio de Delitos Informáticos de Latinoamérica (ODILA), en 2021 los fraudes bancarios, las estafas por correo y las estafas telefónicas se duplicaron o triplicaron. Estas estafas utilizan en su mayoría técnicas de ingeniería social. Dicha estrategia consiste en:

> …obtener información de los usuarios normalmente mediante teléfono, correo electrónico, webs, correo tradicional o contacto directo. Los atacantes de la ingeniería social usan la fuerza persuasiva y se aprovechan de la inocencia del usuario haciéndose pasar por un compañero de trabajo, un técnico o un administrador, etc. (Berenguer Serrato, 2018, p. 4)

La particularidad de dicha metodología es que se estructura en tres momentos: una fase de acercamiento para ganarse la confianza del usuario; una fase de alerta, para desestabilizarlo y observar la velocidad de su respuesta, y una tercera fase tranquilizadora en la que todo ha vuelto a la normalidad. Desde ODILA (2021) sostienen que este mecanismo para engañar a las víctimas suele manifestarse como lo que se conoce popularmente como el cuento del tío y que en el 2020 estas estafas han crecido un 3.000%, en tanto más del 50% de las víctimas no denuncian.

En este marco, los bancos y otras entidades lanzaron campañas preventivas alertando sobre nuevos modos operativos para delinquir virtualmente, ya que esta digitalización acelerada y forzada aumentó la vulnerabilidad de aquellas personas sin conocimientos digitales y proliferaron las estafas virtuales. Esto se vio reflejado en los medios, que publicaron con frecuencia relatos de víctimas de estafas, y en las cifras publicadas por organismos oficiales y ONGs.

En tal sentido, en diálogo con un medio nacional, Horacio Azzolin, fiscal federal a cargo de la Unidad Fiscal Especializada en Ciberdelincuencia (UFECI), sostuvo que:

> …desde que se decretó el aislamiento obligatorio aumentó exponencialmente el tiempo de exposición frente a diversos dispositivos informáticos y con ello el peligro de caer en manos de delincuentes virtuales. (...) Las organizaciones criminales aprovechan para intentar quedarse con algo de nuestro dinero. (Infobae, 10/04/2020)

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]

En la misma línea, Walter Martello, el Defensor del Pueblo adjunto de la provincia de Buenos Aires, advirtió que durante el 2020:

> …quedó demostrado que una de las situaciones derivadas de los mayores niveles de conectividad, producidos por la pandemia, es la proliferación de ciberdelitos. Algunos registros, como los informados por la Asociación Argentina de Lucha contra el Cibercrimen, hablan de un incremento promedio del 60%. (Martello, 2021, s/p)

Así, a las estafas ya conocidas se les sumaron las vinculadas a temas sanitarios. Desde marzo del 2020, la UFECI alertó sobre diversas conductas que podían aparecer y que efectivamente circularon, como las noticias falsas vinculadas a la pandemia, engaños para captar datos personales, fraudes en compras en línea y ataques informáticos que pueden desactivar ciertos servicios críticos conectados a Internet. Los medios nacionales y locales también han dado cuenta de esta situación en sus titulares. A los fines prácticos, retomamos algunos fragmentos de notas de medios digitales (imagen 1, 2, 3 y 4).

Ante este escenario, entidades financieras privadas y organismos públicos comenzaron a publicar una serie de recomendaciones a seguir y así evitar ser víctima de un ciberdelito o fraude. Sin embargo, estas sugerencias están dispersas y generalmente alojadas en la Web o en aplicaciones de los bancos y la Administración Nacional de la Seguridad Social (ANSES). Esto deja al margen a usuarios poco digitalizados, pero también víctimas de estafas.


LA CIUDAD

Advierten sobre estafas a adultos mayores con la excusa de la vacunación contra el covid

La Defensoría del Pueblo aclara que el plan de vacunación de la provincia no requiere la difusión de ningún dato bancario de los receptores de la vacuna

Imagen 1. Noticia sobre estafas a adultos mayores. Fuente: La Capital (16/04/2021)

EQUIPO DE INVESTIGACIÓN | SEGURIDAD 23-10-2020 12:39

Cibercrimen: aumentaron las denuncias en CABA

La Unidad Fiscal Especializada en Delitos y Contravenciones Informáticas (UFEDyCI) del Ministerio Público Fiscal de CABA, explicó el trabajo que realizan. El abogado penalista Jorge L.Litvin da consejos para no caer en la trampa.

Imagen 2. Noticia sobre cibercrimen en la capital del país. Fuente: Perfil (23/10/2020)

SUCESOS / ESTAFA

Córdoba, capital nacional del "cuento del tío"

Cómo funciona una de las industrias delictivas que más se expandieron en los últimos tiempos. Investigaciones judiciales de todo el país tienen a la provincia como el "punto cero" de estas estafas. Las cárceles, un lugar clave para los que delinquen con esta modalidad.

Juan Federico

Domingo, 5 de septiembre de 2021 - 00.01 hs

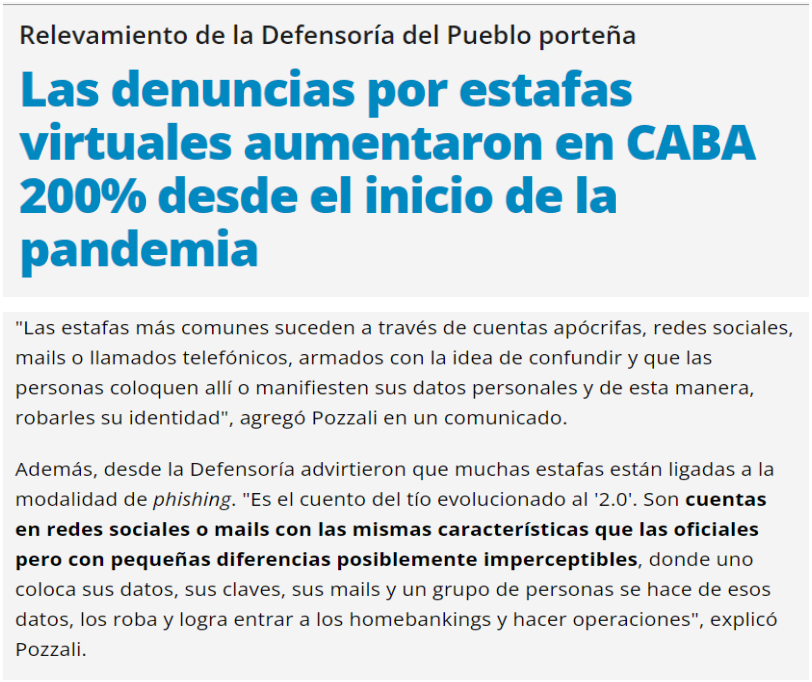
Fueron casi 30 órdenes de allanamientos simultáneos que se ejecutaron en la ciudad de Córdoba, San Francisco, Cosquín, Brinkmann y Río Cuarto. En total, atraparon a 10 de los 30 sospechosos. En Tucumán, los fiscales dirían después que los detenidos eran sólo un eslabón menor de una larga cadena de estafadores: los "muleros bancarios" o prestanombres. O sea, quienes a cambio de unos pesos abrían cuentas corrientes y cedían sus CBU para que otros se aprovecharan.

Se trata de una de las industrias que más ha proliferado en Córdoba desde el inicio de la cuarentena el año pasado: el cuento del tío.

Sólo en Tucumán, se sospecha que fueron cordobeses los autores de más de 3.000 engaños con diferentes ardides: siempre por teléfono, los estafadores simular ser funcionarios de la Anses, de una sucursal bancaria, o de una firma que otorgaba suculentos premios. También ofrecían ventas tentadoras en las red social de Facebook o creaban perfiles bancarios apócrifos en Instagram.

Imagen 3. Noticia sobre estafas en Córdoba. Fuente: La Voz del Interior (05/09/2021)

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]



Relevamiento de la Defensoría del Pueblo porteña

Las denuncias por estafas virtuales aumentaron en CABA 200% desde el inicio de la pandemia

"Las estafas más comunes suceden a través de cuentas apócrifas, redes sociales, mails o llamados telefónicos, armados con la idea de confundir y que las personas coloquen allí o manifiesten sus datos personales y de esta manera, robarles su identidad", agregó Pozzali en un comunicado.

Además, desde la Defensoría advirtieron que muchas estafas están ligadas a la modalidad de *phishing*. "Es el cuento del tío evolucionado al '2.0'. Son **cuentas en redes sociales o mails con las mismas características que las oficiales pero con pequeñas diferencias posiblemente imperceptibles**, donde uno coloca sus datos, sus claves, sus mails y un grupo de personas se hace de esos datos, los roba y logra entrar a los homebankings y hacer operaciones", explicó Pozzali.

Imagen 4. Noticia sobre el aumento de las estafas. Fuente: Página 12 (05/07/2021)

Ingeniería social y ciberdelitos: ¿se pueden evitar?

Los canales de comunicación a través de medios digitales cobraron protagonismo indiscutible a partir de la pandemia. En este contexto, tal como reconoce el Banco Central de la República Argentina (BCRA) –entidad que en el último año ha denunciado más de 20 perfiles falsos en Facebook-, se perfeccionaron las modalidades de estafas y fraudes: los perfiles falsos en redes sociales, las llamadas telefónicas, mensajes de texto o de WhatsApp y los correos electrónicos engañosos para obtener datos personales[2] y bancarios han proliferado en los últimos meses. Por su parte, el Ministerio de Justicia y Derechos Humanos de la Nación (MJyDH, 2020) define a este tipo de conductas ilegales realizadas en el ciberespacio a través de dispositivos electrónicos y redes informáticas como ciberdelitos. Dentro de esta figura penal, el organismo oficial tipifica una serie de conductas que se conocen como ingeniería social:

- *Vishing*: obtienen información a través de una llamada telefónica. El nombre proviene de la expresión en inglés que se forma con las palabras "*voice*" (voz) y

[2] El artículo 2 de la Ley de Protección de Datos Personales los define como "información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables". (Ley N° 25.326)

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]

"*phishing*" (que proviene de "fishing" –pesca-). El mencionado ministerio distingue tres tipos de llamadas frecuentes:

a) Desde un *call center*. Pueden hacerse pasar por personas que trabajan en un *call center*. En esos casos pueden simular sonidos ambiente que existen en los centros de atención al cliente.

b) Simulan ser un familiar que pide ayuda. Asustan a la víctima haciéndole creer que un familiar está en peligro.

c) Ofrecen ayuda económica. Aseguran que el dinero de una cuenta bancaria está en riesgo y solicitan extraer el dinero de la cuenta o dar información sobre el banco (MJyDH, 2020). Ejemplos:

La denuncia fue radicada en la madrugada de esta viernes, poco antes de las 4, cuando personal policial fue convocado a una vivienda de calle Lamadrid al 1100 donde reside una jubilada de 73 años que recibió un llamado telefónico y mediante engaños entregó una suma de dinero a un desconocido.

Momentos más tarde, se percató de que se trataba de una estafa. Personal Policial inició averiguaciones para esclarecer el hecho.

Imagen 5. Noticia sobre *vishing*. Fuente: La Voz de San Justo (10/09/2021)

Luego de las medidas adoptadas por el Banco Central de la República Argentina (BCRA) que impuso mayores medidas de seguridad para la solicitud de créditos a través de home banking, entre otras, se redujeron enormemente las estafas por las que engañaban a personas haciéndose de las claves de sus cuentas bancarias. Ahora, según se informó a UNO desde la Fiscalía de Paraná, los delincuentes volvieron a apuntar a los adultos mayores mediante los cuentos del tío y secuestros virtuales.

La señora mayor recibió un llamado en el cual le dijeron que su hija estaba secuestrada y debía entregar dinero a cambio para que la liberen. Durante la comunicación telefónica la mujer escuchaba gritos y llantos. Se desesperó y llegó a creer que era cierto. No le permitían cortar la llamada para poder llamar a su hija y chequear si era verdad.

Imagen 6. Noticia sobre un falso secuestro. Fuente: Diario Uno (18/08/2021)

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]

- *Phishing*: En esta modalidad, los ciberdelincuentes se contactan por correo electrónico y fingen ser empresas de servicios, oficinas de gobierno o un amigo de algún familiar y solicitan datos para suplantar la identidad de la víctima. Con la información obtenida, gestionan cuentas en bancos, perfiles en las plataformas y redes sociales, servicios y aplicaciones web. También pueden utilizar dispositivos maliciosos, como por ejemplo un *pendrive*, que está conectado a una computadora pública, y de esa manera obtienen información. También existe el *spear phishing,* en donde los delincuentes conocen a la persona a la que intentan robarle los datos y lo hacen porque saben que maneja información sensible. Ejemplos:


ECONOMÍA

Ciberdelincuentes se hacen pasar por el Correo Argentino: en qué consiste la nueva estafa y cómo evitarla

A través de un correo electrónico, los ciberdelincuentes simulan ser la compañía estatal y piden más de $10.000 a los usuarios. Tips para prevenir este tipo de fraude

Imagen 7. Noticia sobre ciberdelincuencia. Fuente: Infobae (29/03/2022)


¡ATENTOS!

Alerta ANSES: un video muestra cómo son las estafas por e-mail para cobrar un falso IFE 4

Un abogado dio a conocer cómo es la modalidad de estafas para cobrar bonos de ANSES truchos mediante un mail que envían por correo electrónico.

Imagen 8. Noticia sobre estafa vía *e-mail*. Fuente: La Opinión Austral (24/09/2021)

- El *smishing* es una modalidad de estafa similar a la anterior, pero en este caso se realiza mediante mensajes de texto o cualquier aplicación de mensajería. Ejemplo:

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]

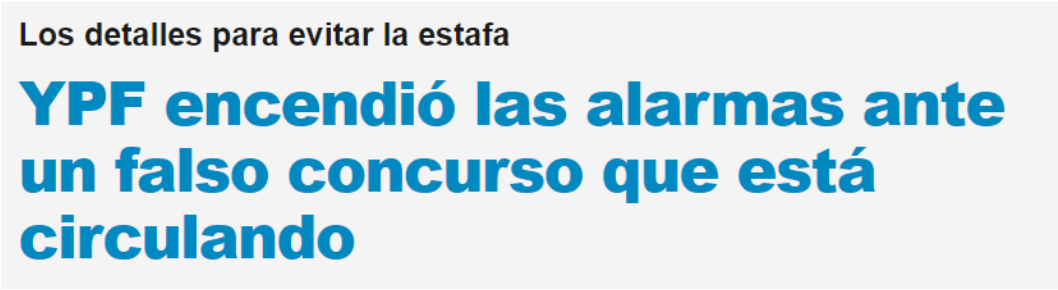
Inseguridad

La estafa de los huevos de Pascua a través de Whatsapp

Prolifera un nuevo tipo de "cuento del tío" bajo un supuesto regalo o falsos premios. El objetivo de los delincuentes: robar datos personales para vaciar las cuentas bancarias.

Imagen 9. Noticia sobre estafa por WhatsApp. Fuente: Cadena 3 (14/04/2022)

- *Concursos falsos*: informan a la persona que ha ganado un premio para obtener información personal. Ejemplo:



Los detalles para evitar la estafa

YPF encendió las alarmas ante un falso concurso que está circulando

Imagen 10. Noticia sobre falsos sorteos. Fuente: Página 12 (27/05/2021)

- *Pharming*: surge de la unión de las palabras *farm* (granja) y *phishing*. Los atacantes manipulan el tráfico de un sitio web para obtener información. También roban cuentas reales de correos electrónicos para cometer ilícitos entre los contactos de la víctima, enviar *software* malicioso u obtener información personal. Ejemplo:

WhatsApp: un correo dice tener una copia de nuestros chat pero en realidad es un virus

El engaño simula ser una comunicación de la plataforma de mensajería. Al abrirlo, instala un malware en los dispositivos.

Imagen 11. Noticia sobre virus creado para robar información. Fuente: TN (24/09/2021)

El denominador común en estas modalidades es que, más allá del medio, necesitan que la víctima les brinde los datos necesarios para poder ejecutar la estafa. Esta estrategia de recolección de datos se conoce como “ingeniería social” (Berenguer Serrato, 2018). La

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]

complejidad de su prevención radica en que no existe un *software* que pueda evitarlo, sino que la única herramienta es brindarle a los "eslabones más débiles de la cadena (...) los conocimientos suficientes para evitar caer en un engaño o al menos minimizar las consecuencias asociadas a él" (Berenguer Serrato, 2018, p. 4). Se considera una forma de ingeniería social porque manipula a los usuarios para que compartan información confidencial o cometan errores al realizar operaciones inseguras y así sus datos queden expuestos. Para generar verosimilitud en el relato, el operador de la estafa crea un escenario, una identidad y un rol.

En tal sentido, el Instituto Nacional de Ciberseguridad de España (INCIBE, 2019) reconoce una serie de principios básicos utilizados por los ciberdelincuentes:

- *Respeto por la autoridad.* En general se tiende a respetar las autoridades, por lo que este tipo de atacantes suelen presentarse como responsables o autoridades de organismos públicos o con reconocimiento social.
- *Voluntad de ayudar.* Los usuarios tienden a ser colaborativos para resolver un problema y los atacantes lo saben. Por eso, fingen ser compañeros de trabajo o un técnico de informática que necesita acceder a su computadora.
- *Temor a perder un servicio.* Bajo el pretexto de un cambio de política o actualización de datos, los ciberatacantes obtienen información confidencial. El *phishing* es la forma más habitual.
- *Respeto social.* El modo más frecuente es la sextorsión. Los usuarios no quieren ser expuestos ante la sociedad y caen ante la amenaza de un supuesto video o imagen –en general inexistente- que pondría en juego su reputación social.
- *Gratis.* Se ofrece un servicio o producto a cambio de información privada. Este tipo de fraude suele llevarse a cabo por medio de páginas web emergentes que suelen aparecer cuando se navega por sitios poco legítimos. También es común en mensajes de redes sociales o aplicaciones de mensajería.

Reconocer las manifestaciones que tienen estas formas de ingeniería social y los mecanismos habituales en los que opera es fundamental, en tanto la prevención supone la concientización y educación de las potenciales víctimas o la rápida acción para realizar un control de daños si se brindaron datos.

Estafas digitales: ¿una cuestión etaria?

Un estudio llevado a cabo por *Microsoft* (2016) demuestra que las estafas virtuales no conocen límites de edad. Comúnmente se cree que las personas mayores son más proclives a ser víctimas de ciberdelitos; sin embargo, no es así. Por el conocimiento que

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]

tienen sobre las redes sociales e Internet, las personas jóvenes tienen un sentimiento de falsa seguridad que las coloca en el primer puesto si de víctimas de estafas digitales se trata: los estafadores los engañan para que cliqueen en enlaces alojados en correos electrónicos y en ventanas emergentes, lo que les permite el acceso al dispositivo y a la información personal (Microsoft, 17/10/2016). Según los datos relevados por la empresa, el 13% de las personas que tienen entre 18 y 24 años, ha sido víctima de estafas telefónicas y/o digitales; mientras que solo el 3% de las mayores de 65 años ha sido estafada. Según se desprende del análisis, entonces, los intentos de estafas, las estafas efectivas y el impacto económico es mayor entre las personas más jóvenes.

Relevamiento de campañas

El Observatorio de Delitos Informáticos de Latinoamérica (2021)[3] realizó un relevamiento de la cantidad de fraudes denunciados en Argentina y publicó un ranking provincial de estafas. Según esta organización, Córdoba se encuentra en el puesto número cuatro, después de Buenos Aires, la Ciudad Autónoma de Buenos Aires (CABA) y Santa Fe. Además, estableció un ranking de entidades financieras según los casos reportados. Los resultados fueron los siguientes:

1. Galicia
2. BBVA
3. Santander
4. Banco Provincia de Buenos Aires (BAPRO)
5. Banco Nación Argentina (BNA)
6. Macro
7. ICBC
8. Patagonia
9. Brubank
10. Banco Ciudad de Buenos Aires
11. Mercado Pago
12. Supervielle
13. Banco Santa Fe
14. Banco de Corrientes
15. Banco Entre Ríos
16. HSBC

[3] La muestra se inició el 02/01/2021 y finalizó el 07/06/2021. Los datos se encuentran disponibles en: https://www.odila.org/analisis-fraude

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]

17. Itaú
18. Banco Santa Cruz
19. Bancor
20. Credicoop
21. Industrial (BIND)
22. ING Direct
23. Servicios y Transacciones
24. Banco de Tierra del Fuego (BTF)
25. UALA

Teniendo en cuenta estos datos y la creciente campaña de concientización de los bancos y del Estado nacional y provincial, relevamos las recomendaciones que brindan: el Banco de Córdoba (Bancor), el Banco de la Nación Argentina y los bancos o entidades financieras privadas que funcionan en la ciudad de Córdoba. Para ello, navegamos por las redes sociales y páginas web de dichas entidades. En cuanto a las redes, tomamos las publicaciones realizadas en *Instagram*, *Facebook*, *Twitter* y *YouTube* durante los primeros diez meses del 2021 y, para el análisis de las páginas web, ingresamos a los portales todos los lunes de septiembre y octubre. En cuanto a las redes, en general, la plataforma más completa es *Instagram* y, por eso, la mayor parte de las publicaciones serán tomadas de esta red social. Es preciso señalar que el contenido de las redes se suele replicar de idéntica manera en todas las plataformas. Asimismo, relevamos campañas publicitarias en medios tradicionales.

Antes de presentar las publicaciones de cada entidad financiera, plantearemos algunas consideraciones surgidas a partir de la exploración de las redes sociales y páginas webs de los bancos. En primer lugar, la única entidad financiera que posee un acceso directo vinculado a estafas en su web, es Bancor. El resto de los bancos analizados tienen información en sus páginas, pero se debe navegar e ingresar a diferentes secciones y subsecciones para llegar al núcleo informativo. Además, observamos que no todas las firmas financieras dan consejos para todos los tipos de estafas. Muchas de ellas se limitan a brindar consejos para redes sociales –por ejemplo, cómo asegurarse de que la cuenta esté verificada-, pero no mencionan correos, llamadas o contactos por mensajería instantánea. Asimismo, es preciso considerar que, al momento de escribir este texto, cuatro entidades financieras habían cerrado los comentarios en sus cuentas de redes

sociales porque constituyen un nuevo canal para detectar posibles víctimas de estafas.

> ¿Sabías que los comentarios en las publicaciones son una fuente de contacto para los estafadores? A través de perfiles falsos toman tus datos, como claves o usuarios, y así concretan la estafa. Por este motivo, decidimos cerrar los comentarios en nuestras publicaciones. (BBVA, 2021)

Finalmente, menos de la mitad de los bancos analizados publican en sus redes o de manera accesible en su web, los canales de denuncias o indicaciones respecto de qué hacer ante la sospecha o efectiva estafa. Esto es aún más preocupante entre las entidades financieras ciento por ciento *online* –por ejemplo, *Ualá*-, porque no hay ningún espacio físico de consulta y, por lo tanto, si se desconocen los canales institucionales, se debe recurrir directamente a la justicia.

Galicia

En el Instagram oficial del banco hay una sección de historias destacadas con *tips* de seguridad. Sin embargo, las primeras publicaciones son –cuanto menos- imprecisas. La información proporcionada está incompleta y puede prestarse a confusión. A modo de ejemplo, compartimos las capturas de las cuatro placas que conforman uno de los videos:

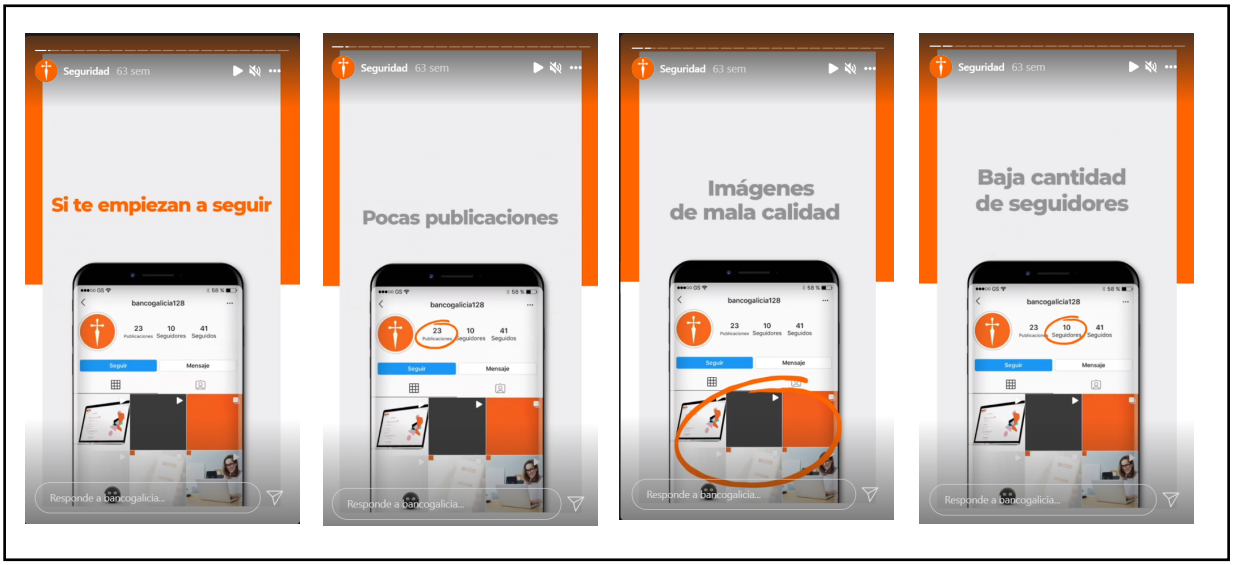


Imagen 12. Las cuatro imágenes que forman el video. Fuente: Banco Galicia (2021)

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]

En las demás historias, los consejos que la entidad brinda a los usuarios incluyen:

- Tené cuidado. En los comentarios hay usuarios que publican números falsos para luego estafar a quienes llaman.
- Si no tiene tilde azul, no es Galicia.
- Consejos para usar el homebanking de manera segura: evitá buscar el sitio desde Google porque corrés el riesgo de llegar a páginas falsas, podés escribir la palabra desde la barra de direcciones de tu navegador, chequeá siempre que el sitio tenga el candado de conexión segura.
- ¿Recibiste un correo o mensaje dudoso? Escribí la palabra seguridad en el chat de Gala por WhatsApp o enviá tu caso por correo.
- Si tenés una consulta, hacela por privado. (Banco Galicia, 2021)

Asimismo, el *feed* de sus redes sociales cuenta con un amplio contenido de consejos para evitar las estafas: a razón de un tercio de sus publicaciones están vinculadas con esta temática. Se han publicado, además de algunas de las mencionadas, las siguientes recomendaciones:

- ¡Cuidate de las estafas! Desde el banco nunca vamos a contactarte por redes sociales ni pedirte tus claves. ¿Necesitás ayuda? Escribinos a nuestro WhatsApp 1144398558 las 24 horas y contactate de la forma más segura y confiable.
- No compartas tus claves con nadie, nunca.
- Nunca vamos a pedirte tus claves.
- Nunca vamos a pedirte que actualices tus datos vía mail ni que lo hagas accediendo a un link desconocido.
- Si sospechás de un correo, no lo respondas ni ingreses a links desconocidos. (Banco Galicia, 2021)

Por otra parte, cabe destacar que el banco realizó una campaña en redes con Marcos –su icónico personaje- pero cambiando completamente el tono con respecto a sus avisos publicitarios habituales. “Sé que no están acostumbrados a verme así de serio, pero hoy quiero hablarles de un tema que no da para chiste: las estafas por Internet, por teléfono y en las redes” (Banco Galicia, 2021). Este

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]

video se complementa con otro similar, que pone énfasis en no compartir las claves personales. Asimismo, en todas sus redes Galicia ha creado campañas para cada tipo de estafa. Así, hay publicaciones que se titulan “Las estafas por mail existen”, “Las estafas por redes sociales existen” y “Las estafas telefónicas existen”, que muestran personas en contextos reales que reciben mensajes, *mails* o llamadas que son una estafa. Los consejos brindados son pertinentes para cada tipo de estafa y una de las publicaciones es protagonizada por un adulto mayor. Sin embargo, si bien se trata de una publicación con fuerza, se ha utilizado una única vez en Instagram y no todas las piezas se han replicado en todas las redes sociales del banco.

BBVA

Aunque no se encontró una gran cantidad de publicaciones, sí se han rastreado algunos consejos en sus cuentas de Instagram, Facebook y Twitter, aunque en esta última red solo se ha realizado una publicación vinculada a estafas:

- El banco nunca va a iniciar una conversación por privado ni va a pedirte que realices una transferencia o que inicies una videollamada. Nunca vamos a solicitarte clave SMS, usuario homebanking, token, números de tarjeta o claves.
- Recordá que las cuentas oficiales están verificadas con una tilde azul. Si necesitás comunicarte con nosotros, utilizá canales oficiales.
- No facilites datos personales.
- Si una llamada parece sospechosa, cortá.
- No accedas a ser guiado por teléfono para operar ningún canal del banco.
- Sospechá de las llamadas urgentes de desconocidos.
- Antes de aceptar un DEBIN, verificá que la transacción sea la correcta.
- Tener en cuenta que el vendedor es el que debe generar la operación y no el comprador.
- Recordar que la autorización de un DEBIN implica un débito en la cuenta, no un ingreso.
- No facilitar información confidencial como nombres de usuarios, claves, números de tarjeta por teléfono, correo o SMS. Son personales e intransferibles. (Banco Francés, 2021)

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]

Santander

El banco presentó una campaña en redes sociales con publicaciones en carrusel con una serie de consejos para evitar estafas, principalmente, en redes sociales y *phishing*. Las imágenes tienen una gran carga textual:

Imagen 13. Campaña en Instagram. Fuente: Santander (2021)

Los consejos que recabamos de esta entidad financiera fueron:

- Operá con seguridad a través de nuestras redes. Recordá que todas nuestras cuentas están verificadas con una tilde azul, y que nunca iniciaremos una conversación solicitando tus datos confidenciales.
- Muchas personas sufren de las ciber estafas, y vos también podés ser una víctima. Por eso, ¡deslizá para aprender cómo frenar esta problemática! Si sospechás, reportalo al 0800 666 0330.
- Evitá el phishing. Prestá atención al nombre del remitente. Leé cuidadosamente el cuerpo del mail y no actúes con urgencia. Si te piden hacer clic en un enlace, no lo abras. El banco nunca va a solicitar tus claves personales a través de correo electrónico.
- Si te solicitan tus claves personales, no se las brindes. ¡Son personales, no las necesitamos!
- Nunca vamos a pedirte: Datos de tu tarjeta de crédito; Usuario, clave o códigos confidenciales; Dirección de e-mail o contraseña.

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]

- Nunca vamos a dirigirte al login a través de e-mail para que ingreses a tus claves.
- Nunca te acerques a un cajero automático asistido por alguien. (Santander, 2021)

Banco Nación Argentina

En el período relevado, solo ha realizado dos publicaciones en *Facebook* e *Instagram* vinculadas a estafas, que se ubican en la primera mitad del año 2021. En ambos casos, se limitan a advertir sobre el *phishing*. En la publicación más completa, recomienda y advierte lo siguiente:

- Los mails engañosos tienen estas características:
  Dicen que te van a bloquear o cerrar tu cuenta.
  Te piden que hagas clic en un enlace o botón falso, ¡no lo oprimas!
  Te solicitan información confidencial o que actualices tus datos personales.
  Recordá: NUNCA vamos a solicitar tus claves o datos de tarjetas a través de un mail o red social. (BNA, 2021)

Macro

En los últimos meses, el banco ha utilizado dos tipos de campañas en sus redes sociales. Por un lado, comenzó priorizando el texto en el *flyer* y luego desarrolló una sola oración a modo de título. El estilo, en este caso, fue interrogativo o imperativo y la entidad se sirvió del *copy* para ampliar la información.

Imagen 13. Posteo en Instagram sobre estafas virtuales. Fuente: Banco Macro (2021)
Imagen 14. Consejos de seguridad. Fuente: Banco Macro (2021)

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]

Otros consejos que se visualizan a lo largo de diversas publicaciones son:

- Al consultar por las redes, verificá que el perfil tenga la tilde azul
- No compartas tus datos personales
- Si recibís una transferencia, revisá el comprobante
- Conocé cómo funciona el debin y evitá estafas
- ¿Cómo detectar un comprobante falso?
- ¿Qué hago si me estafaron?
- ¿Te pidieron tus datos personales?
- ¿Fuiste víctima de un fraude?
- ¡No des tus datos!
- Prestá atención a los fraudes
- Mantené tus datos seguros, evitá que te estafen. Siempre debés tomarte un minuto antes de actuar
- Mantené tus datos seguros, evitá las estafas. Ante cualquier duda, comunicate con nosotros. (Banco Macro, 2021)

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]

ICBC

En promedio, uno de cada cuatro posteos que realizó la entidad financiera son de su sección de "consejos de seguridad". El formato privilegiado es el audiovisual y la portada consiste en un interrogante.

Imagen 15. Portada de carrusel con consejos de seguridad. Fuente: ICBC (2021)

Gran parte de los consejos se repiten a lo largo de las piezas, por lo que, para no redundar, sistematizamos únicamente las recomendaciones vinculadas a estafas digitales.

Recomendaciones generales:

- Verificar que se comuniquen por los canales oficiales.
- Recordar que nunca pedirán información confidencial.

Recomendaciones vinculadas a llamadas:

- No responder si piden claves.
- No aceptar orientación telefónica para generar claves.
- Nunca compartir todos los datos de las tarjetas o cuentas.
- No brindar datos o información confidenciales.

Recomendaciones vinculadas a email:

- Verificar quién es el remitente.
- Leer atentamente el contenido.
- Las temáticas de fraude pueden ser el cierre de cuenta, el bloqueo de acceso, la pérdida de dinero, etc. Suelen estar mal redactados y tener errores ortográficos.

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]

- Verificar a dónde te llevan sus links.
- Es común que se incluyan links con sitios fraudulentos para obtener tus datos.
- Evitar descargar archivos adjuntos. Solo hacerlo si se está seguro del contenido y su relación con tus productos o servicios, y si el emisor es de confianza.
- Además, sus publicaciones se caracterizan porque siempre aparecen los medios de contacto para denunciar posibles estafas. Incluso, cuentan con una cuenta de correo específica para gestionar este problema.

Patagonia

Al momento del relevamiento, el banco había realizado solo dos publicaciones durante el 2021. Una es un *flyer* plano y la otra un breve video. En ambos casos hace énfasis en que solo se comunicarán desde cuentas oficiales.

Brubank

Este banco cien por ciento digital comparte *tips* de seguridad bajo el paraguas de "consejos de seguridad". Así, ha publicado en los últimos meses estas recomendaciones:

- Si un mail te parece sospechoso, no lo respondas. No abras ni descargues archivos adjuntos de casillas sospechosas. Contactate inmediatamente con nuestro equipo de Atención al Cliente mediante el chat en la app de Brubank o a nuestro mail denuncias@brubank.com
- Todas nuestras cuentas oficiales están verificadas. Si recibís mensajes en nombre de Brubank desde cuentas no verificadas, no respondas.
- No compartas tu clave de la app con nadie. No ingreses tu mail ni tu contraseña del mismo en ningún sitio. Te recomendamos elegir una contraseña que no contenga tu fecha de nacimiento, número de DNI, ni la altura de tu domicilio. Si tu dispositivo te lo permite, activa el face-id o el touch-id. (Brubank, 2021)

Mercado Pago

Solo cuenta con dos publicaciones que apuntan únicamente a contactos por redes sociales. En ellas el banco informa que no se pone en contacto con sus clientes y que la cuenta oficial está verificada. Además, advierte que, si un usuario tiene pocos seguidores y/o pide datos confidenciales, es falso.

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]

Supervielle

Cuenta con una única publicación que data de mayo del 2021. Se trata de un video que aconseja:

> Durante el último año se multiplicaron los casos de estafas virtuales. La gente es contactada por cuentas falsas que se hacen pasar por el banco: usan nuestro logo, nuestro nombre y solicitan información que jamás pediríamos. No hagas click en links que provengan de remitentes desconocidos, sea por mail o SMS. No respondas ningún mensaje que solicite información sensible como usuario, contraseña o código de seguridad de tu tarjeta, clave SMS. Nunca des información personal ni de tu cuenta. (Supervielle, 2021)

Esta pieza audiovisual está acompañada con un breve *copy* (ocho palabras) que refuerza la idea de no compartir datos sensibles y un número para hacer la denuncia, pero no aclara si se trata de un teléfono institucional o estatal, por ejemplo, la División Delitos Tecnológicos de la Policía Federal Argentina.

HSBC

El banco publicó a lo largo del año una serie de piezas audiovisuales con consejos construidos en oraciones afirmativas. Los consejos que brindó fueron:

> Sobre llamadas
>
> ¡Ante la mínima duda, CORTÁ llamadas o comunicaciones peligrosas! Tené en cuenta posibles estafas y NO brindes tus datos privados por teléfono a nadie.
>
> El banco NUNCA te va a llamar para pedirte datos privados. Si notás un tono de voz alarmante (que está apurado o te pide datos de manera urgente), CORTÁ inmediatamente.
>
> No caigas en las amenazas que te "venden" los estafadores, como decirte que te van a cortar el servicio de tus tarjetas o paquete de cuentas por no pasar tus datos privados. ¡NO LES CREAS!
>
> Ante la duda, cortá la llamada y comunicate por mail a contactenos@hsbc.com.ar (HSBC, 2021)

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]

> Sobre transferencias bancarias
>
> Si recibís un aviso sobre un error al realizar una transferencia bancaria, no respondas.
>
> Ante cualquier duda, comunicate con el banco.
>
> Usá contraseñas con mayúsculas, minúsculas y números. No incluyas fechas de nacimientos o direcciones. No uses equipos públicos o de otras personas para entrar a apps, redes o cuentas. Mantené actualizado el navegador y sistema operativo de los equipos y aplicaciones. Tenemos que estar atentos a nuestra seguridad virtual. Es muy importante. (HSBC, 2021)
>
> Sobre correos y mensajes
>
> ¿Viste que a veces te llegan mensajes diciendo que ganaste algo? No los abras. Tampoco mails que no esperás. Jamás te vamos a pedir datos de tus tarjetas, cuentas, claves o contraseñas. Si recibís este tipo de cosas como sorteos o premios, tenés que saber que son estafas e ignorarlas. Es importante estar atentos a la seguridad virtual. (HSBC, 2021)

Itaú

En Instagram, posee una sección fija en historias destacadas en la que, durante el 2021, ha brindado tres consejos para evitar estafas: uno vinculado a WhatsApp, otro al correo y un tercero, a redes sociales. En el mismo período, publicaron ese contenido en el *feed* de Instagram. Las piezas plantean el testimonio de una persona que ha sido víctima y a qué estar atento/a para evitar caer en una estafa.

En Facebook, también se publicó esta campaña una única vez y fijaron en la parte superior la publicación para prevenir estafas mediante redes sociales. Lo mismo sucedió en Twitter.

Bancor

Es el único banco que al momento del relevamiento contaba con información vinculada a estafas de manera visible y de fácil acceso en su web. Lo primero que se visualiza es el número para denunciar y luego, al ingresar a la nota, se despliegan 11 consejos que son los que se replican en las redes sociales:

- Ante la duda, eliminá los mensajes, bloqueá esas cuentas y cortá las llamadas.
- Nunca compartas tus claves ni datos de seguridad de tus cuentas. Ningún banco te va a pedir esos datos.

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]

- Siempre que tengas dudas, desconfiá y comunicate con el banco.
- Comunicate siempre a través de los canales oficiales de Bancor.
- Las únicas maneras de acceder a Bancon son a través de la web de Bancor y la app.
- El banco nunca se va a contactar para pedirte datos ni claves.
- Bancor nunca te va a llamar para pedirte datos de seguridad.
- Nunca sigas instrucciones para ir a un cajero, ni compartas tu pin o clave de acceso.
- Tené cuidado con las transferencias falsas.
- Si fuiste víctima de un ciberdelito, denuncialo. (Bancor, 2021)

En los últimos meses, el banco provincial aumentó la cantidad de publicaciones vinculadas a estafas y comparte estos consejos bajo la campaña "Ojo con las estafas", que tiene como imagen a tres periodistas de la ciudad de Córdoba. En redes, estos consejos se especifican aún más y son presentados en videos.

Credicoop

Este banco posee menos canales que las demás entidades financieras –solo Facebook y YouTube-, ha realizado una única publicación en 2021 y ha decidido cerrar los comentarios como medida de seguridad. Su publicación está vinculada a esta decisión.

Imagen 16. Único posteo en Facebook. Fuente: Banco Credicoop (2021)

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]

UALA

Al momento de relevar esta cuenta, registramos que las últimas publicaciones son de marzo del 2021 y que aconsejan lo siguiente:

> Nuestras redes sociales oficiales están verificadas con una tilde azul. Nunca nos vamos a poner en contacto con vos si no es a través de estas redes sociales.
>
> Nunca compartas tus claves ni contraseñas con nadie, incluso si el contacto pareciera venir de Ualá.
>
> Desconfiá de toda comunicación que contenga links sospechosos y/o que te pida las claves de tu Ualá o cualquier otra información confidencial para darte un beneficio a cambio. (Ualá, 2021)

Ahora bien, en relación a las cuentas no verificadas, nos preguntamos qué tan frecuentes son. En tal sentido, en las publicaciones seleccionadas, asegurarse de que el usuario de la red social es el oficial fue el consejo más frecuente. No solo está presente en todos los bancos analizados, sino que la mayoría lo ha repetido en más de una oportunidad. En vistas de esto, decidimos explorar las redes en busca de cuentas *fake* y descubrimos, por ejemplo, que Banco Galicia cuenta con más de 20 usuarios falsos en Twitter, y que Bancor tiene al menos seis cuentas gemelas. Esta situación se repite para todos los bancos. Así, cada entidad financiera tiene, al menos, dos cuentas falsas en alguna red social.

Consideraciones para una propuesta de comunicación

A raíz de esta investigación –de tipo exploratoria y fuertemente anclada en una detallada investigación de contenido bibliográfico y del material generado por entidades bancarias-, establecimos criterios a tener en cuenta a la hora de crear una campaña de comunicación que busque evitar las estafas digitales.

a. *Campaña transversal y multimedial*. Las acciones que cada banco realiza en sus redes están atomizadas y no tienen una continuidad en otros medios. Sería oportuno diseñar una estrategia armónica, por ejemplo, con un mismo lema, y que circule por diarios, TV, radio y redes.

   Además, limitar la prevención a un solo medio, excluye a quienes no lo consumen. Por ejemplo, según la última Encuesta de Consumos Culturales (2017), las personas mayores se caracterizan por los siguientes consumos: el 77,4% escuchó radio en el último año y los tipos de programas más consumidos fueron informativos/noticieros

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]

(76.55%) y musicales (50.19%). Por otra parte, un 25,75% oyó programas de actualidad o *magazines*, un 20,98% deportivos, el 5,32% religiosos y en los últimos lugares el 3,64% culturales y 0,51% de chimentos. El 76.5% leyó algún diario digital o en papel durante el último año. El 96.8% consumió TV en el último año y la señal más consumida fue por cable (73,3%). En tanto, un 13,2% utilizó televisión satelital; un 1,2% televisión digital abierta mediante decodificador y un 12,2% solo utilizó canales de aire analógicos. El 42.8% no utiliza Internet y el 91.2% no acostumbra a usar WhatsApp ni redes sociales, ni en el celular, computadora, televisión u otro dispositivo. De quienes tienen redes sociales, el 67,1% navega en Facebook, transformándola en la plataforma dominante en este segmento etario.

Si bien estimamos que estas cifras pueden haberse modificado –sobre todo a partir del confinamiento con la consecuente digitalización acelerada y obligada que alcanzó a la mayoría de la población-, estos son los últimos datos disponibles y evidencian que, para este grupo etario, una campaña en redes sociales no sería tan efectiva como una publicidad radial o televisiva.

b. *Representaciones diversas.* En las campañas solo aparecen representadas personas blancas, de clase media y de un rango etario de 30 a 50 años. No aparecen, por ejemplo, las personas mayores, quienes también son usuarios digitales y víctimas potenciales de estafas. Tampoco se hacen presentes las personas jóvenes, quienes resultan las principales víctimas de estafas.

   Es menester colocar en el centro de la escena a estos grupos, porque solo así se puede romper con la falsa seguridad que expone a diario a los jóvenes, así como con la creencia de que las personas mayores no son usuarias de redes y que, por lo tanto, solo pueden ser víctimas del *cuento del tío*.

c. *Información clara.* La cifra negra, es decir, la cantidad de dinero que se ha perdido en estafas y no se ha denunciado, supera los 332 millones de pesos. Esto es el 52% de las estafas. En parte, sucede porque las campañas no indican un número de denuncia. Excepcionalmente, algunas entidades financieras publican un número de teléfono para gestiones o reclamos internos. En este sentido, es necesario que las campañas no solo sean de prevención, sino que también eduquen y brinden información clara, concreta y concisa sobre qué hacer si una persona detecta que fue víctima de una estafa. En una encuesta realizada para esta investigación, el 50% de las personas consultadas respondió que, cuando intentaron estafarlas, les hubiera gustado tener información sobre a dónde dirigirse o cómo hacer una denuncia.

[Vol. 2, Nº 3, enero - junio 2022. ISSN 2796-8383]

Este punto también contempla la terminología utilizada en las campañas. En ocasiones, las entidades financieras denominan a los ciberdelitos por sus nombres técnicos, que son legalmente correctos pero públicamente desconocidos. El más frecuente es el *phishing.* Por ejemplo: "están creciendo los casos de *phishing*" o "evitá el *phishing*". En estos casos, es recomendable utilizar frases y conceptos conocidos por todos los usuarios, así se detendrán a leer la información y la comprenderán de manera más sencilla. Por ejemplo, para los casos anteriores se podría utilizar: "están creciendo las estafas por correo" o "evitá las estafas por correo". Además, es importante recordar que no todas las personas conocen la jerga de cada plataforma o red social, incluso siendo usuarias. Lo que puede parecer obvio para quienes diseñan la campaña, puede ser desconocido para otros. Por ejemplo, si se habla de "correos *spam*" o "cuenta verificada", es necesario hacer una aclaración o referencia de qué se entiende como tal.

d. *Múltiples medios, múltiples estafas.* La ingeniería social se filtró en redes sociales, correos electrónicos, páginas web y llamadas. Podríamos decir que es omnipresente y las campañas de prevención e información también deberían serlo.

   En este sentido, no solo es importante que estén presentes en múltiples medios, formatos y plataformas, sino también que abarquen todas las formas de estafas. En general, se habla de las estafas por mensajería privada en redes sociales, sin embargo, en los canales oficiales, son escasamente mencionadas las estafas vía sitios web o el peligro que implica comentar en la red social de un banco. Un comentario es público y es la carnada justa para los atentos y oportunistas estafadores. El problema es que quien puede morder el anzuelo, es el estafado.

e. *Actualización y educación constante.* Relacionado con el punto anterior, las campañas de educación y prevención deben estar en constante actualización. Es evidente que las formas de estafas mutan y no siempre será posible preverlas. Sin embargo, sí podremos educar sobre puntos centrales, por ejemplo, no brindar datos personales o exponer cuáles son los mecanismos que utilizan los ciberdelincuentes. No obstante, además, es necesario que las campañas estén a la vanguardia de todas las formas que adoptan las estafas y cuáles son sus estructuras. De lo contrario, siempre estaremos en una profunda desventaja.

Estas estrategias son necesarias, sin embargo, al igual que las estrategias de comunicación utilizadas para educar y prevenir estafas, deben ser revisadas y actualizadas. Estamos en tiempos de extrema vertiginosidad y es necesaria la urgente intervención desde distintos organismos públicos y privados. Esto incluye políticas públicas de seguridad, alfabetización tecnológica y un real compromiso de las propias

entidades bancarias y financieras. El análisis y la propuesta es un primer paso a ser expandido y renovado mediante campañas sostenidas y actualizadas en el tiempo. Este camino ya ha sido abierto y queda en las autoridades y entidades competentes el compromiso de tomarlo, continuarlo y actualizarlo.

Referencias bibliográficas

Berenguer Serrato, D. (2018). Estudio de metodologías de Ingeniería Social. Trabajo final. Universitat Oberta de Catalunya. Recuperado de https://openaccess.uoc.edu/bitstream/10609/81273/6/dbs14TFM0618memoria.pdf

Otras fuentes consultadas

Banco BBVA (14 de septiembre de 2021). ¿Sabías que los comentarios en las publicaciones son una fuente de contacto para los estafadores? A través de perfiles falsos... [*Twitter*, hilo con imágenes adjuntas]. Recuperado de https://twitter.com/bbva_argentina/status/1437859170359947459

Banco de Córdoba (Bancor) (s.f.). Ojo con las ciberestafas. Recuperado de https://www.bancor.com.ar/718_APP/ojo-con-las-ciberestafas

Banco CREDICOOP. (s.f.) Inicio [Página de Facebook]. Recuperado de https://www.facebook.com/bancocredicoopcl

Banco de la Nación Argentina [Perfil de Instagram] (s.f.) Consultado el 06/09/2021. Recuperado de https://bit.ly/3jpX7bs

Banco Francés [Perfil de Instagram] (s.f.) Consultado el 06/09/2021. Recuperado de: https://www.instagram.com/bbva_argentina/?hl=es-la

Banco Galicia (10 de junio de 2021). Las estafas por mail existen y tenemos que cuidarnos. Recordá que nunca te vamos a pedir que realices una acción... [Video Adjunto]. Facebook. Recuperado de https://www.facebook.com/bancogalicia/posts/4852589191434888

Banco Galicia (16 de junio de 2021). Las estafas por redes sociales existen. [Video] YouTube. Recuperado de https://www.youtube.com/watch?v=q9bWn_2b5kM

Banco Galicia [Perfil de Instagram] (s.f.). Recuperado de https://bit.ly/2Xyh73L

Banco HSBC [Perfil de Instagram @hsbc_ar] (09 de septiembre de 2021). ¡Ante la mínima duda, CORTÁ llamadas o comunicaciones peligrosas! Tené en cuenta posibles estafas y

NO brindes tus datos privados. [Video]. Recuperado de https://www.instagram.com/p/CTnGg3bHfYZ

Banco HSBC (28 de enero de 2021) ¿Viste que a veces te llegan mensajes diciendo que ganaste algo? No los abras, tampoco mails que no esperás. [Video]. Recuperado de https://www.instagram.com/p/CKI-HX7n2TY

Banco HSBC (30 de abril de 2021) Tips de seguridad virtual Los riesgos y amenazas a la seguridad bancaria varían y se adaptan continuamente. Esto afecta a... [Video]. Recuperado de https://www.instagram.com/p/COTctH2Dy6Z

Banco ITAU Argentina [Perfil de Instagram @itauargentina] (22 de julio de 2021). ¿Te hablaron desde un perfil dudoso? No le respondas y conversá con nosotros por nuestras cuentas oficiales (verificadas). [Fotografías]. Recuperado de https://www.instagram.com/p/CRoqGtXMUnZ

Banco ITAU Argentina (s.f.). Seguridad [Destacados] Consultado el 11/10/2021. Recuperado de https://www.instagram.com/stories/highlights/17862194924022642/?hl=es-la

Banco Macro [Perfil de Instagram @bancomacro] (28 de julio de 2021). ¿Te llamaron para decirte que ganaste un premio? Es falso, estás ante un fraude telefónico. Nadie te regala nada, así... [Fotografía] Recuperado de https://www.instagram.com/p/CR3y4iDF8Ih

Banco Macro (29 de septiembre de 2021). Cuando aceptás un DEBIN, el dinero se debita de tu cuenta automáticamente y pasa directo a la de quien te lo solicitó. [Fotografía]. *Instagram*. Recuperado de https://www.instagram.com/p/CUaBlaArdjW

Banco Patagonia [Perfil de Instagram @banco_patagonia] (s.f.). Consultado el 06/09/2021. Recuperado de https://www.instagram.com/banco_patagonia/?hl=es

Banco Santander [Perfil de Instagram @santander_ar]. (s.f.). Recuperado de https://www.instagram.com/santander_ar/?hl=es-la

Banco Superville [@bancosupervielle] (16 de abril de 2021). Están circulando mails y mensajes SMS que se hacen pasar por nosotros, nunca brindes información sensible. Denuncialos llamando al 4959-4959. [Video]. *Instagram*. Recuperado de https://www.instagram.com/p/CNvNmvhJeBE

Brubank [Perfil de Instagram @brubank] (s.f.). Consultado el 20/09/2021. Recuperado de https://www.instagram.com/brubank

Cadena 3 (14 de abril de 2022). La estafa de los huevos de pascua que circula por WhatsApp. Recuperado de https://www.cadena3.com/noticia/sociedad/la-estafa-de-los-huevos-de-pascua-a-traves-de-whatsapp_322137

Defensoría del Pueblo Ciudad Autónoma de Buenos Aires. (10 de febrero de 2021). Estafas Bancarias: Respuesta del Banco Central. Recuperado de https://defensoria.org.ar/noticias/estafas-bancarias-respuesta-del-banco-entral/

Diario Uno (18 de agosto de 2021). Cesaron estafas bancarias y volvieron los engaños a ancianos. Recuperado de https://bit.ly/3iUxOxV

Federico, J. (05 de septiembre de 2021). Córdoba, capital nacional del "cuento del tío". *La Voz del Interior.* Recuperado de https://bit.ly/3lBSHPY

Gómez, S. (23 de octubre de 2020). Cibercrimen: aumentaron las denuncias en CABA. *Perfil.* Recuperado de https://bit.ly/3FLciFu

Infobae (29 de marzo de 2022). Ciberdelincuentes se hacen pasar por el Correo Argentino: en qué consiste la nueva estafa y cómo evitarla. Recuperado de https://www.infobae.com/economia/2022/03/29/ciberdelincuentes-se-hacen-pasar-por-el-correo-argentino-en-que-consiste-la-nueva-estafa-y-como-evitarla/

Instituto Nacional de Ciberseguridad de España [INCIBE] (05 de septiembre de 2019). Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse. Recuperado de https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse

La Capital (16 de abril de 2021). Advierten sobre estafas a adultos mayores con la excusa de la vacunación contra el Covid. Recuperado de https://bit.ly/3iZdVFY

La Opinión Austral (24 de septiembre de 2021). Alerta ANSES: un video muestra cómo son las estafas por e-mail para cobrar un falso IFE 4. Recuperado de https://bit.ly/3vbORjH

La Voz de San Justo. (10 de septiembre de 2021). Le hicieron el "cuento del tío" a una jubilada y le robaron dinero. Recuperado de https://bit.ly/2YKRop0

Lavieri, O. (10 de abril de 2020). Coronavirus en Argentina: cómo evitar caer en las estafas virtuales, en aumento durante la pandemia. *Infobae.* Recuperado de https://bit.ly/3BGg9Bc

Martello, W. (19 de abril de 2021). Phishing y proliferación de estafas virtuales en tiempos de pandemia. *Blog de Walter Martello*. Recuperado de https://bit.ly/3lJBWTn

Mercado Pago [Perfil de Instagram @mercadopago.arg] (25 de septiembre de 2021). Nunca vamos a pedirte claves personales, códigos de seguridad o tu número de teléfono.

Si alguien lo solicita... [Fotografía]. Recuperado de https://www.instagram.com/p/CUPtmetjhCE

Microsoft (17 de octubre de 2016). Youngsters more likely to be scam victims than pensioners, study reveals. Recuperado de https://news.microsoft.com/en-gb/2016/10/17/scams

Ministerio de Cultura de la Nación Argentina (2017). Informe general sobre la Encuesta de Consumos Culturales 2017. Recuperado de https://datos.gob.ar/dataset/cultura-encuesta-nacional-consumos-culturales-2017/archivo/cultura_9a97dde5-3a33-4689-8333-24a2fa5b4a6e

Ministerio de Justicia y Derechos Humanos de la Nación Argentina [MJyDH] (s.f.). Phishing. Una guía y un glosario para conocer sus modalidades y prevenirlas. Recuperado de https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/informes-de-la-direccion-1

MJyDH (s.f.). Riesgos en el Mundo Digital y Cómo Prevenirlos: Phishing. Recuperado de https://www.argentina.gob.ar/jefatura/innovacion-publica/gobierno-abierto-y-pais-digital/paisdigital/navegacion-segura/riesgos-en-el-mundo-digital-y-como-prevenirlos-phishing

MJyDH (19 de diciembre de 2020). ¿Qué es el ciberdelito? Recuperado de https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-el-ciberdelito

MJyDH (21 de diciembre de 2020). ¿Qué hago si me piden mis datos personales por teléfono? Recuperado de https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-hago-si-me-piden-datos-personales-por-telefono

Observatorio de Delitos Informáticos de Latinoamérica [ODILA] (2021). Campaña para combatir el fraude electrónico. Recuperado de https://www.odila.org/analisis-fraude

Página 12 (27 de mayo de 2021). YPF encendió las alarmas ante un falso concurso que está circulando. Recuperado de https://bit.ly/3lD4jSO

Página 12 (05 de julio de 2021). Las denuncias por estafas virtuales aumentaron en CABA 200% desde el inicio de la pandemia. Recuperado de https://bit.ly/3v6KCpE

TN (24 de septiembre de 2021). WhatsApp: un correo dice tener una copia de nuestros chat pero en realidad es un virus. Recuperado de https://bit.ly/3FJncvG

UALÁ [Perfil de Instagram @uala_arg] (s.f.). Recuperado de https://www.instagram.com/uala_arg/?hl=es-la