Guía de recomendaciones para evitar el Fraude

DICCIONARIO DEL FRAUDE DIGITAL

¡Conocer cómo operan los fraudes es tu mejor defensa! ¡Infórmate, mantente alerta y actúa con precaución!

SERNAC
Servicio Nacional del Consumidor

¡Cuando entiendes el lenguaje del fraude, dejas de ser víctima y te conviertes en defensor de tu información!

¡El conocimiento es tu mejor escudo. Aprende los términos, detecta los engaños, protégete!

¡Comparte esta información!

DICCIONARIO

Término	Significado
Phishing	**Es un tipo de fraude digital donde los estafadores intentan engañarte para que entregues tus datos personales o claves. Lo hacen enviando correos electrónicos, mensajes o realizando llamadas que parecen ser de una empresa, banco o institución oficial legítima. La víctima cae porque cree que está interactuando con un mensaje o solicitud real.**
Smishing	**Una forma de phishing que se realiza específicamente a través de mensajes de texto SMS. Estos mensajes suelen incluir enlaces a sitios web falsos o te piden escanear cupones maliciosos para robar tus datos o instalar programas dañinos.**
Vishing	**Es un tipo de estafa telefónica. El delincuente te llama y se hace pasar por un representante de una entidad de confianza (como un banco, un servicio público o una empresa) para manipularte y obtener tus datos personales, claves o que autorices transferencias de dinero.**
Quishing (QR Phishing)	**Es una modalidad de phishing que utiliza códigos QR maliciosos. Al escanear un QR fraudulento, este te redirige a una página web falsa (clonada) o inicia la descarga de un programa dañino (malware). La trampa está en que tú mismo autorizas la acción, pensando que el QR es legítimo.**
Angler Phishing	**Se refiere al phishing que ocurre en redes sociales. Los delincuentes crean perfiles falsos que imitan a empresas o bancos y se hacen pasar por "atención al cliente" para interactuar con usuarios que buscan ayuda, con el fin de robarles datos personales o bancarios.**

DICCIONARIO

Término	Significado
Malware	Es una abreviación de "software malicioso". Son programas dañinos que se instalan en tu dispositivo (computadora, celular o tablet) sin que te des cuenta. Su objetivo es espiar, controlar o robar tu información, a menudo para cometer fraudes financieros o suplantar tu identidad.
Keylogger	Un tipo de malware que registra todas las teclas que presionas en tu teclado. Esto permite a los estafadores robar contraseñas, mensajes y cualquier otra cosa que escribas.
Spyware	Un "software espía" que monitorea tu actividad en el dispositivo, incluyendo tu ubicación, correos, uso de la cámara, y otros datos, para robar información personal o corporativa.
RAT (Remote Access Trojan):	Significa "Troyano de Acceso Remoto". Es un tipo de malware que permite al atacante tomar el control total de tu computadora o dispositivo a distancia, sin que tú lo notes.
Banking Trojan	Un malware diseñado para robar información de tus aplicaciones bancarias, billeteras digitales o sistemas de pago en línea. A menudo se disfraza de una aplicación legítima o se superpone a la real para capturar tus datos de acceso.
Ransomware	Un tipo de malware que bloquea todos tus archivos (los "cifra") y luego exige un pago (un "rescate") para devolverte el acceso a ellos. Si no pagas, podrías perder tus archivos para siempre.
Adware con fraude oculto:	Es un software que llena tu pantalla de anuncios, pero que también puede tener funciones ocultas para redirigir tus pagos o capturar tu actividad de navegación para robar información.
APK	Es el formato de archivo que usan las aplicaciones en dispositivos Android. Cuando se menciona una "descarga de APK malicioso", significa que estás a punto de bajar una aplicación que contiene malware.

DICCIONARIO

Término	Significado
SIM Swapping / Portabilidad Numérica Fraudulenta	**Son dos términos relacionados que describen un tipo de fraude donde un delincuente consigue que tu número de teléfono sea transferido a una nueva tarjeta SIM o a otra compañía telefónica sin tu permiso, usando tu identidad. El objetivo principal es tomar control de tu número para interceptar códigos de verificación (OTP) y acceder a tus cuentas bancarias o de redes sociales. La portabilidad numérica fraudulenta es cuando se traslada tu número a otra compañía, y el SIM swapping es cuando se repone tu SIM en un chip nuevo.**
IMEI	**Es un número único de identificación para cada teléfono móvil. Es fundamental tenerlo anotado, ya que lo necesitarás para bloquear tu celular con tu compañía telefónica en caso de robo.**
Shoulder Surfing	**Una técnica de espionaje donde el delincuente mira por encima de tu hombro (o graba) mientras ingresas tu PIN, patrón o contraseña en tu celular o cajero, para luego robar el dispositivo y desbloquearlo.**
Port-out lock (Bloqueo de portabilidad)	**Opción que impide que tu número sea portado sin tu autorización previa.**
CAP (Código de Autorización de Portabilidad)	**SMS de 4 dígitos que tu compañía envía para confirmar que realmente quieres portar tu número.**
PIN / NIP	**Son números de identificación personal que usas para desbloquear tu celular o acceder a ciertas aplicaciones y servicios. Es importante que sean complejos y no fáciles de adivinar.**
WAP billing	**Pago a través de servicios de mensajería móvil que factura directamente al número de teléfono.**

DICCIONARIO

Término	Significado
Skimming	**Una técnica de estafa donde los delincuentes usan un dispositivo para copiar la información de tu tarjeta de crédito o débito cuando la pasas por un lector falso en cajeros automáticos o puntos de venta.**
Carding	**Implica el uso fraudulento de datos de tarjetas robadas para realizar compras. Los delincuentes obtienen estos datos, a menudo en foros clandestinos o a través de phishing, los validan mediante microcargos ("pruebas de $1") para asegurar que la tarjeta está activa, y luego procesan compras de alto valor o venden la información a terceros. La consecuencia es la aparición de cargos desconocidos en tu tarjeta.**
Card-not-present	**Se refiere a fraudes donde se utiliza tu tarjeta sin tenerla físicamente, solo con los datos como el número, la fecha de vencimiento y el CVV (código de seguridad). Este tipo de fraude se asocia comúnmente con el "carding".**
CVV	**Es el código de seguridad de tu tarjeta de crédito o débito, generalmente de 3 o 4 dígitos, que se encuentra en la parte de atrás (o a veces adelante). Se pide para realizar compras en línea. ¡Nunca debes entregarlo por redes sociales ni en sitios no seguros!.**
Selfie Fraudulenta	**Se refiere al uso de una foto o imagen manipulada para engañar los sistemas de verificación de identidad que piden una "selfie" (una foto tuya) para confirmar quién eres.**
Deepfake	**Una técnica muy avanzada que crea videos, audios o imágenes falsas y extremadamente realistas de personas. Se menciona en el contexto de "selfie fraudulenta" como una forma de burlar la verificación de identidad.**

DICCIONARIO

Término	Significado
VoIP (Voice over Internet Protocol)	Es una tecnología que permite hacer llamadas de voz a través de internet. Los estafadores la usan para hacer llamadas falsas.
Caller-ID Spoofing	Es la técnica que usan los estafadores para falsificar el número que aparece en la pantalla de tu teléfono cuando te llaman. Hacen que parezca que la llamada viene de un número legítimo (como tu banco), aunque no sea así.
DTMF (Dual-Tone Multi-Frequency)	Es la tecnología que permite que cada número que presionas en el teclado de tu teléfono emita un sonido distinto. Los delincuentes pueden grabar esos sonidos y usarlos para descifrar qué números marcaste, incluso tus claves.
Spoofing / Sitio "clonado"	Falsificación de una web o del número de teléfono para hacerse pasar por la entidad real.
Clickbait	Es un contenido web (como un título, imagen o enlace) diseñado para captar tu atención de forma llamativa o sensacionalista y animarte a hacer clic, aunque la información real pueda ser engañosa o no cumplir lo prometido.
SEO (Search Engine Optimization)	Son técnicas que se usan para que un sitio web aparezca en los primeros lugares de búsqueda en internet. Los estafadores lo utilizan para que sus sitios web falsos sean encontrados fácilmente por las víctimas.
Malvertising	Publicidad en internet que contiene malware escondido.
Cuenta bancaria de "mule"	Cuenta usada por delincuentes para recibir o mover dinero robado.

DICCIONARIO

Término	Significado
Onboarding Digital	**Es el proceso de registro y activación de un nuevo cliente o usuario de forma completamente en línea, sin necesidad de ir a una oficina. Los delincuentes lo aprovechan para abrir cuentas bancarias o solicitar créditos fraudulentos usando la identidad de sus víctimas.**
Biometría Fuerte	**Se refiere a métodos de seguridad que usan tus características físicas únicas, como tu huella dactilar o el reconocimiento facial, para desbloquear un dispositivo o acceder a una cuenta. Son difíciles de falsificar.**
Autenticación de Dos Pasos (2FA)	**Es una capa extra de seguridad para tus cuentas. No basta solo con tu contraseña; también necesitas una segunda forma de verificación (como un código enviado a tu celular o generado por una aplicación) para poder iniciar sesión. Se recomienda usar apps de autenticación para esto, ya que son más seguras que los SMS.**
OTP (One-Time Password) o Código de Verificación	**Es un código de un solo uso que se envía a tu teléfono o correo para confirmar tu identidad o autorizar una transacción. Los estafadores buscan interceptarlos para acceder a tus cuentas.**
FIDO2	**Estándar de llaves físicas o biométricas que reemplaza los códigos SMS y hace el inicio de sesión más seguro.**
TOTP (Time-based One-Time Password)	**Código que genera tu app de autenticación (Authy, Google Authenticator) y cambia cada cierto tiempo.**
Token	**Dispositivo, app o código que entrega claves temporales para más seguridad.**

DICCIONARIO

Término	Significado
Gestor de Contraseñas	**Es una aplicación o programa que almacena todas tus contraseñas de forma segura, protegidas por una única "clave maestra" o tu huella dactilar/reconocimiento facial. Así, no necesitas recordar todas tus claves y puedes usar contraseñas más complejas.**
Keychain	**Llavero digital (iCloud/Chrome) que guarda todas tus contraseñas; si acceden, tienen todo.**
Clave Única	**Es tu identificación digital personal para trámites con el Estado en Chile. Es como una firma electrónica que te permite acceder a diversos servicios y beneficios en línea de forma segura. Si te la roban, un estafador puede acceder a plataformas con tus datos personales, de impuestos, de salud y financieros.**
Firma Electrónica Avanzada	**Es un tipo de firma digital que tiene un alto nivel de seguridad y validez legal, similar a una firma manuscrita notarial. En fraudes como las transferencias vehiculares virtuales, un estafador podría intentar obtenerla además de tu Clave Única.**
Escrow	**Es un servicio de protección al comprador donde el dinero de una compra es retenido por un tercero neutral hasta que el producto o servicio se entrega y el comprador lo aprueba. Si hay un problema, el dinero no se libera al vendedor. Se recomienda usar plataformas que ofrezcan este servicio en compras en línea.**
HTTPS	**Es un protocolo de seguridad para sitios web. Cuando ves "https://" y un candado en la dirección web (URL), significa que la información que envías está protegida (cifrada). Es importante verificarlo al realizar compras o ingresar datos. Sin embargo, no siempre certifica que el sitio sea el legítimo; un clon también puede tener candado.**

DICCIONARIO

Término	Significado
Ciberlocales	**Son lugares donde hay computadoras de uso público (como cibercafés). Pueden ser peligrosos porque los delincuentes podrían instalar programas (keyloggers) para capturar las claves que digitas.**
Wi-Fi Públicas	**Son redes de internet inalámbricas disponibles en lugares públicos. Muchas veces no son seguras, lo que facilita que los estafadores intercepten tu información si te conectas a ellas.**
Dark Web	**Es una parte de internet que no es accesible a través de navegadores comunes y que a menudo se usa para actividades ilegales. Es un lugar donde los estafadores pueden comprar o vender información robada, como credenciales y datos personales.**
Bot	**Es un programa informático que realiza tareas repetitivas de forma automática en internet. Un dispositivo infectado con ciertos tipos de malware puede ser controlado por un estafador y usarse como "bot" para cometer otros fraudes.**
VPN (Red Privada Virtual)	**Es un servicio que crea una conexión segura y privada a internet, incluso cuando estás usando redes Wi-Fi públicas que no son seguras. Es como un túnel seguro para tu información.**
Firewall	**“Muro” de software que filtra y bloquea conexiones peligrosas antes de que lleguen a tu equipo.**
Pop-up	**Ventana emergente que salta de golpe y, si haces clic, puede llevarte a fraude o malware.**
MitM (Man-in-the-Middle)	**Cuando un delincuente se “sitúa” entre dos comunicadores (por ejemplo, tú y tu banco) y puede leer o alterar lo que se envían sin que lo adviertan.**

DICCIONARIO

Término	Significado
Heurística de Urgencia / Escasez	**Los estafadores te presionan con frases como "¡Solo por hoy!", "Últimas unidades" o "Oferta termina en X minutos". Esto te hace sentir que debes actuar rápido para no perder la oportunidad, impulsándote a hacer clic o comprar sin pensar.**
Aversión a la Pérdida	**Los mensajes te alertan sobre algo que podrías perder ("Si no actúas, perderás tu dinero", "Tu paquete será devuelto"). El miedo a perder algo importante te lleva a actuar de forma impulsiva para evitarlo, sin verificar la autenticidad.**
Sesgo de Optimismo	**Es la tendencia a creer que las cosas malas (como el fraude) "les pasan a otros" y no a uno mismo. Esto hace que bajes la guardia y no verifiques detalles importantes, como la dirección de una página web.**
Prueba Social (Social Proof)	**Los estafadores usan supuestos "testimonios", "miles de compradores" o comentarios positivos falsos para hacerte creer que muchas personas ya confiaron en ellos y, por lo tanto, son legítimos y seguros.**
Sesgo de Autoridad	**Tendemos a confiar y obedecer a figuras de autoridad. Los estafadores se aprovechan de esto imitando logos, nombres y el lenguaje de bancos, instituciones gubernamentales o grandes empresas, haciendo que creamos automáticamente que son legítimos y sigamos sus instrucciones.**
Anclaje de Precios	**Consiste en mostrar un precio original muy alto (tachado) y luego ofrecer un gran "descuento". Esto crea la ilusión de que estás obteniendo una oferta increíble, haciendo que compares con el precio inflado y compres impulsivamente.**

DICCIONARIO

Término	Significado
Familiaridad y Comodidad Tecnológica	**Caemos porque asociamos tecnologías como los códigos QR o las interacciones digitales con algo moderno y seguro, y los usamos en la vida diaria sin sospechar.**
Anonimato del Canal	**El hecho de que un QR o un enlace no te muestran directamente a dónde te llevarán o quién los puso, hace que subestimes el riesgo y bajes la guardia.**
Refuerzo Multicanal	**Cuando un mensaje fraudulento te llega por diferentes medios (correo, WhatsApp, anuncios, etc.). Esto da una sensación de mayor legitimidad y coordinación, reforzando el engaño.**
Peticiones Escalonadas	**Los estafadores comienzan pidiéndote información "simple" (como tu nombre o correo) y luego, una vez que has empezado a colaborar, te piden datos más sensibles (claves o códigos). Se hace difícil decir "no" una vez que ya entregaste algo.**
Lenguaje Técnico Intimidante	**Usan términos complicados o muy especializados para que te sientas abrumado y prefieras "delegar" la decisión al supuesto experto, sin cuestionar.**
Aislamiento del Canal	**Te piden que no cortes la llamada o que no hables con nadie más hasta terminar el proceso. Esto es para evitar que consultes o pidas ayuda, dejándote solo en la trampa.**
Reciprocidad Simulada	**El estafador finge estar "ayudándote" o haciéndote un "favor", esperando que tú "correspondas" colaborando y siguiendo sus instrucciones.**
Pretexting	**Variante de ingeniería social donde el atacante inventa una excusa (p. ej., “soy del soporte técnico”) para ganarse tu confianza y obtener datos.**
Ingeniería social	**Conjunto de métodos psicológicos que usan los estafadores para manipularte y que reveles información o realices acciones que no harías.**