# El Fraude Digital en Tiempos del COVID-19

Actualizado: 6 de mayo de 2020

Además de las normas de salud (lavado de manos, distanciamiento social y aislamiento), una nueva norma de la pandemia debe ser la higiene digital: **estar atentos y mantener cautela ante los ataques y fraudes en línea**, los cuales han crecido exponencialmente debido a la necesidad de las personas de mantenerse en contacto con sus familiares, el aumento de compras online y el teletrabajo como herramienta de productividad, entre otros.
La Organización Mundial de la Salud (OMS) alertó en días recientes sobre este tipo de amenazas, indicando que los delincuentes se hacen pasar por este organismo internacional y fingen campañas de donación para obtener información privada y fondos en efectivo.
La tensión y circunstancias únicas de la pandemia han generado un ambiente de incertidumbre que es una oportunidad aprovechada por muchos delincuentes, quienes utilizan su creatividad para cometer fraudes por teléfono, correo electrónico, mensajes de texto o promociones en las redes sociales.

**El Phishing** por correo electrónico siempre ha sido una técnica popular de estafa, pero los millones de correos falsos enviados durante la emergencia del COVID-19 son el mayor aumento en ataques en muchos años.
Otras **estafas basadas en correos electrónicos** fingen contener información relacionada a la salud pública o asociada a la pandemia y piden hacer clic en un enlace. Sin embargo, estos **enlaces son maliciosos y lanzan e instalan malware o troyanos** en el dispositivo de la víctima que extrae nombres de usuarios, contraseñas de cuentas de email y cuentas bancarias, entre otra información. Con este robo de información consiguen suplantar a la persona y engañar a las entidades bancarias y de otros tipos (email, redes sociales, etc.)

Sin importar el tamaño de la inversión que se realice en seguridad informática, identificar estos casos es difícil debido a la complejidad de técnicas y herramientas empleadas para mantener el anonimato y evitar la detección, así como el uso de accesos desde redes anónimas en la dark web o sistemas proxy que ofuscan direcciones IP de origen.

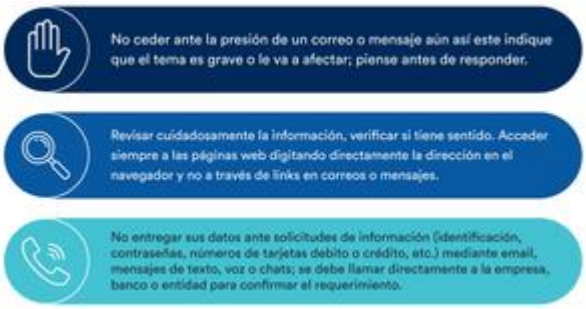

Además, **el teletrabajo** (trabajo en casa) **inhabilita las medidas de seguridad tradicionales** que son usadas diariamente en las oficinas físicas de las empresas pues no necesariamente están disponibles en el domicilio de los trabajadores. Esto dificulta la protección de un personal completamente remoto sin adaptación y expuesto a un entorno complejo.

## Recomendaciones para mitigar los riesgos de seguridad en esta compleja situación:

**El usuario es la primera línea de defensa.** Ante situaciones de incertidumbre, dudas o presión, **no responda a requerimientos de información y consulte directamente con la entidad o persona para verificar la legitimidad de la solicitud.**

Se pueden aplicar los siguientes criterios:

1. PARE
2. MIRE
3. LLAME



A pesar de que el usuario final esté consiente y atento de la seguridad de su entorno, hay situaciones que no son detectables a simple vista debido a la complejidad técnica del ataque. En este punto cobran relevancia las soluciones especializadas en detección de fraude digital para ayudar a las instituciones y personas en la contención del riesgo.
PLUS TI monitorea e investiga continuamente las tendencias actuales y emergentes de fraude digital con el fin de adaptar la evolución de las últimas tendencias en tecnologías de detección basadas en Machine Learning y conocimiento experto, al igual que variadas técnicas y herramientas, para proveer una detección óptima y acciones defensivas en tiempo real, de los cuales destacan:

- Controles de Onboarding digital.
- Conocimiento del cliente y entorno.
- Perfilamiento de dispositivos.
- Integración de APP Móviles mediante SDK (detección de malware y troyanos).
- Fortalecimiento de los procesos de autenticación y autorización dinámica (2FA).
- Monitoreo integral de la sesión del usuario.
- Análisis del comportamiento transaccional.
- Monitoreo y contención en tiempo real.

Monitor Plus® DBFD™ (Digital Banking Fraud Detector) es una de las soluciones mas completas, robustas y escalables de detección de fraudes en entornos digitales que proporciona todos los elementos anteriormente descritos y aplica las mejores prácticas para la detección y contención de riesgos y ciberamenazas.