SEGURIDAD EN CANALES ELECTRONICOS

RECOMENDACIONES PARA EFECTYVIRTUAL

- Siempre que ingrese a la página web Efecty hágalo desde un computador seguro, no desde un café internet o sitios públicos, digite la dirección usted mismo en la barra superior del navegador.

- Observe que la dirección empiece con "https" para acceder. De igual manera su navegador presentará un ícono con un candado cerrado color verde, este indica que la encriptación está activa.

- Recuerde que su clave es secreta, única y personal no comparta sus claves.

- No permita que terceros observen su clave secreta al momento de digitarla.

- Cambie con frecuencia su clave de internet, memorícela y no la comunique.

- Instale y mantenga actualizado su computador con herramientas de seguridad informática que le protejan contra espionaje y robo de información.

- Tome precauciones al navegar por internet, ya que existen paginas creadas por delincuentes que instalan aplicaciones para robar información.

- Si recibe algún mensaje sospechoso por correo electrónico o detecta páginas web falsas en las que le solicitan datos personales en nombre de efecty, infórmenos a la mayor brevedad. Recuerde validar la información antes de descargar los archivos adjuntos, pues puede contener archivos maliciosos que pueden infectar su equipo.
- Nunca suministre su clave secreta, información personal, ni información de transacciones a personas que se la soliciten bajo el argumento de participar en concursos, premios o cualquier tipo de oferta.

- Recuerde siempre terminar la sesión de forma segura con el botón “salir” que ofrece la página Efecty.

RECOMENDACIONES APP EFECTY

- En caso de pérdida del celular realice el correspondiente bloqueo al operador y realice los cambios respectivos en contraseñas virtuales.
- Mantenga sus dispositivos móviles con clave de seguridad que impida el fácil accesos a terceros a la información del celular o dispositivo móvil.
- Sólo active las conexiones por bluetooth y wifi cuando vayas a utilizarlas, procure no conectarse a redes públicas cuando realice sus transacciones.
- Evite conectar el celular a equipos públicos que puedan tener virus o archivos infectados.
- No acceda a enlaces enviados a través de mensajes SMS/MMS no solicitados y que impliquen la descarga de contenidos en los dispositivos, direcciones de páginas web fraudulentas o con números telefónicos que aparentan ser de servicio al cliente de entidades falsas.
- Baje las aplicaciones a su dispositivo solo desde sitios conocidos para evitar malware, spyware o virus, y valide las condiciones de uso antes aceptar la instalación.
- Descargue únicamente la APP EFECTY desde las tiendas oficiales de los dispositivos como única fuente fiable .

OTRAS MEDIDAS DE SEGURIDAD EN INTERNET

Ingeniería social

Práctica usada comúnmente por delincuentes a través de teléfono, Internet o presencial para engañar a los usuarios llevándolos a revelar información sensible y apropiarse de su información confidencial, personal o financiera haciéndose pasar por empleados de entidades para solicitar datos personales, confidenciales y financieros como claves y números de identificación.

Evite ofrecer o divulgar información confidencial sin verificar que se está comunicando con las verdaderas entidades financieras.

Redes sociales

- Evite suscribir información personal en formularios en línea que invitan a actualizar datos para participar en supuestas rifas y causarle perjuicios por el uso inadecuado.

- Evite proporcionar datos personales a través del perfiles en las redes sociales. Por medio de redes sociales los delincuentes buscan apropiarse de información confidencial, financiera, laboral y personal.

Vishing

Práctica en la cual los delincuentes ofrecen un número de teléfono para comunicarse en vez de un link. El delincuente marca de forma aleatoria a algunos números hasta que alguien contesta al otro lado de la línea dejando una grabación de supuestas entidades que obligan a la víctima a devolver la llamada a el número falso que le facilitan en la grabación. Al llamar al número informado por los delincuentes, una nueva grabación solicita información confidencial, personal y financiera para ser verificada como códigos de seguridad, fechas de vencimiento y claves que el delincuente utiliza para hacer compras y operaciones fraudulentas.

Evite ofrecer información confidencial sin verificar que se está comunicando con Efecty.

Phishing

Práctica fraudulenta que el delincuente utiliza para captar ilícitamente información confidencial, personal o financiera por medio de link falsos o correos electrónicos de suplantación que buscan captar usuario, clave, números de tarjeta de crédito, códigos de seguridad para realizar operaciones fraudulentas.

Utiliza el correo electrónico de forma segura y no comparta la información confidencial por este medio, de esta forma estará a salvo del Phishing.

Smishing

Práctica fraudulenta en la cual los delincuentes usan mensajes de texto(SMS) a celulares para engañar a través de técnicas de ingeniería social y obtener información confidencial, personal y financiera para realizar compras por internet, robos de identidad y demás operaciones fraudulentas.

Evite revelar información por mensajes de texto recibidos en su celular que le soliciten llamar a números o enviar mensajes de texto con clave personal.

Pharming

Práctica fraudulenta en la cual el delincuente altera la forma de navegación del computador re-direcciona a la víctima a páginas web falsas.

Verifique que la dirección de la página empiece por https:// que el certificado de seguridad esté relacionado a Efecty,. Mantenga actualizado su programa de antivirus.

Key loggers y malware

Con el Key loggers el delincuente utiliza archivos, programas o código malicioso que se instalan al descargar software gratuito desde internet y lo utiliza para infectar el sistema o dispositivo y de esta manera realizar robos de información, ya que el malware captura y registra la actividad del teclado y envía la información al delincuente a través de internet para robar de esta manera los datos de autenticación y realizar transferencias fraudulentas.

Navegue de forma segura y no acceda a sitios engañosos ni descargue software sospechoso.