GUÍA DE USUARIO
DELITOS INFORMÁTICOS

El uso de la Internet, además de darnos mucha información, también involucra acciones delictivas que se tipifican como delitos informáticos. Al igual que nuestro mundo real, en el mundo virtual también existen personas inescrupulosas dedicadas a cometer actos fraudulentos. Por ello nuestra obligación es mitigar estos riesgos, pero para lograrlo, antes debemos estar informados.

CAJA TACNA, siempre en constante preocupación por su seguridad, tiene a bien presentarles las modalidades de robo que emplean tecnologías de información como correos electrónicos, mensajes de texto y llamadas telefónicas entre otros.

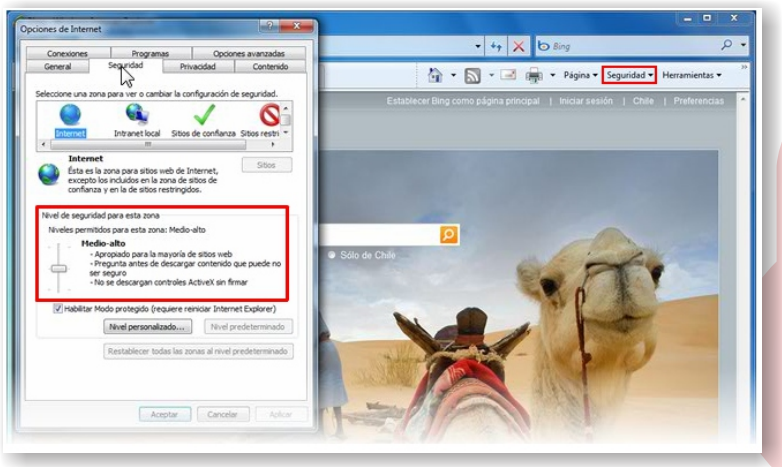
FRAUDES MAS FRECUENTES

1 Malware (software malicioso)

Son todos los tipos de programas o códigos de computadora cuya función es dañar un sistema o causar un mal funcionamiento. El Malware tiene como objetivo infiltrase en el sistema y dañar la computadora sin el conocimiento de su dueño, con finalidades muy diversas.

Reglas de oro para su seguridad

- Asegúrese de tener un programa de antivirus en su computadora.
- Realice las actualizaciones automáticas que le pida el programa, porque contienen cientos de archivos de protección contra los nuevos virus que aparecen cada día.
- Cuando reciba la alerta de que el programa esta por expirar, no ignore la actualización, no tendrá que comprar otro producto, sólo deberá autentificarlo para continuar teniendo actualizaciones.
- Nunca abra un archivo adjunto de un e-mail de un remitente desconocido.
- Si recibe un e-mail y este le lleva a una página de Internet desconocida, no acceda al sitio web, porque es seguro que el contenido será malicioso.

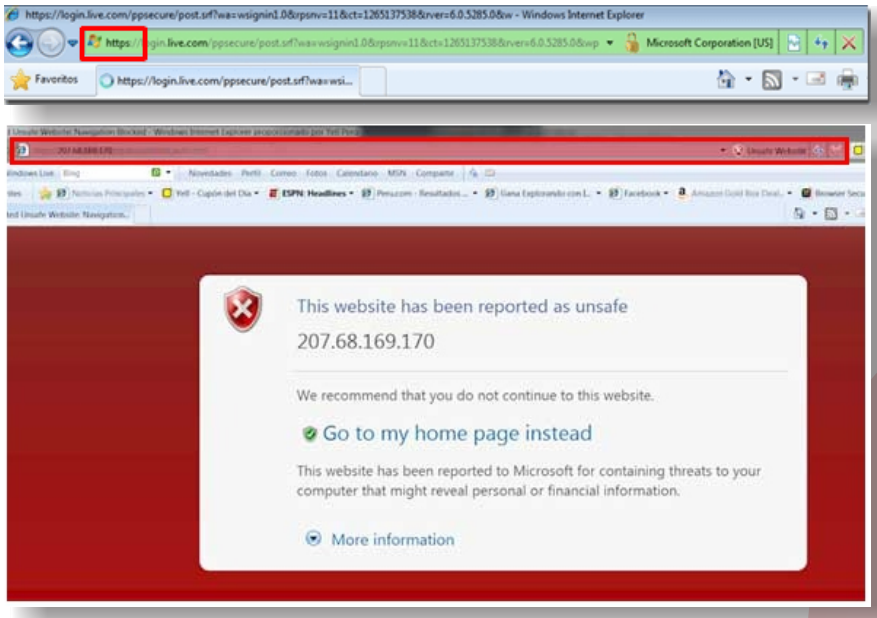


2 Phishing

Es una modalidad de estafa diseñada con la finalidad de robarle la identidad. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes. Los mensajes falsos parecen provenir de sitios Web reconocidos o de su confianza, como el de su institución financiera. Asimismo, se ha identificado la aparición de aplicaciones para dispositivos móviles que cumplen la misma finalidad que los phishing tradicionales: Robar información confidencial. Dichas aplicaciones son desplegadas por personas dedicadas al robo de información a través de Android Market y Apple Store; las mismas que también podrían cargar una dirección URL desde la App sin mostrar la dirección URL en ningún lugar de la App.

Reglas de oro para su seguridad

- Nunca responda a solicitudes de información personal a través de correo electrónico. Si tiene alguna duda, póngase en contacto con la entidad que supuestamente le ha enviado el mensaje.
- Para visitar sitios Web, introduzca la dirección URL en la barra de direcciones.
- Asegúrese de que el sitio Web utilizado sea cifrado.
- Consulte frecuentemente sus saldos financieros (Cuentas de Ahorro, Tarjetas de Créditos).
- Comunique los posibles delitos relacionados con su información personal a las autoridades competentes.
- Verifique que la APP CMAC MOVIL de la tienda Android tenga la siguiente descripción:



3 Dominio Falso

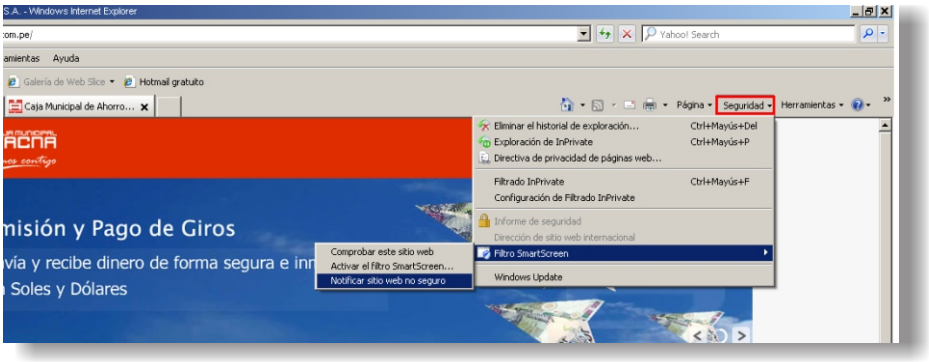
Un dominio falso es un nombre falsificado de un sitio web. Por ejemplo:

El dominio seguro es **www.microsoft.com** y el dominio falso podría ser ***www.microsoft3.com***, se debe tener sumo cuidado con estos dominios falsos, ya que el sitio al que le llevan es exactamente igual al original. Generalmente, estos dominios falsos llegan a través de e-mails fraudulentos que solicitan la actualización de datos en un sitio Web de dominio falso.

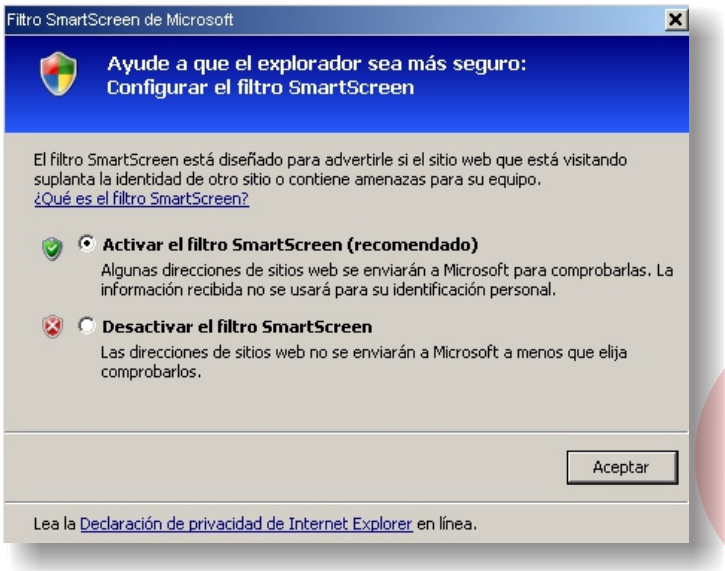
Reglas de oro para su seguridad

- Se debe prestar mucha atención a la URL (Ej: http://www.microsoft.com) del sitio al cual nos conecta el link. Si este no coincide exactamente con la URL original del sitio, es mejor que no siga navegando en él.
- Tenga siempre activas las alertas de su navegador, como también, reportar sitios no confiables cada vez que se encuentre con uno de ellos. Para ello ingrese a Herramientas/Opciones de Internet/Seguridad en tu explorador.

Primero.- Haga clic en la sección Seguridad o Safety.



Segundo.- Siga el Menú de Smart Screen Filter hasta la opción Report Unsafe Website (o reportar sitio inseguro).



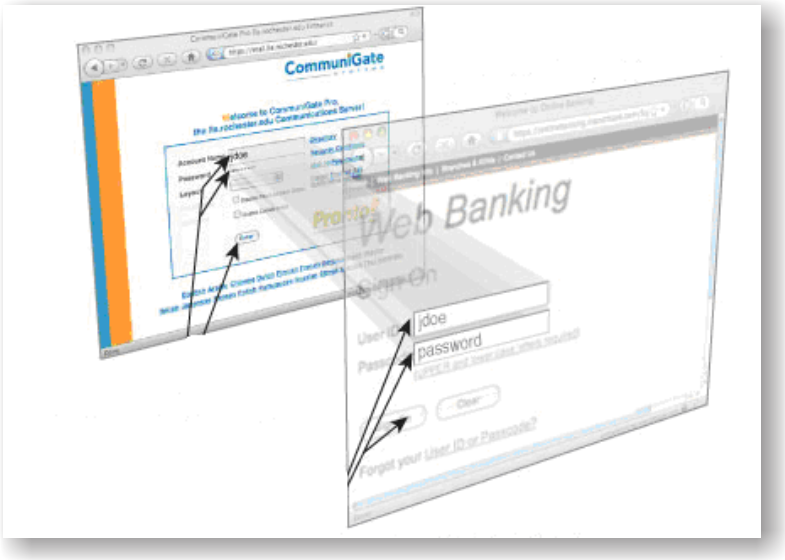
4 Clickjacking (secuestro de clicks)

Es un término que se acuñó hace pocos días y se usa para denominar a los sitios que, escondiendo o camuflando botones y diálogos, hacen que los navegantes acepten enviar información o instalar programas.

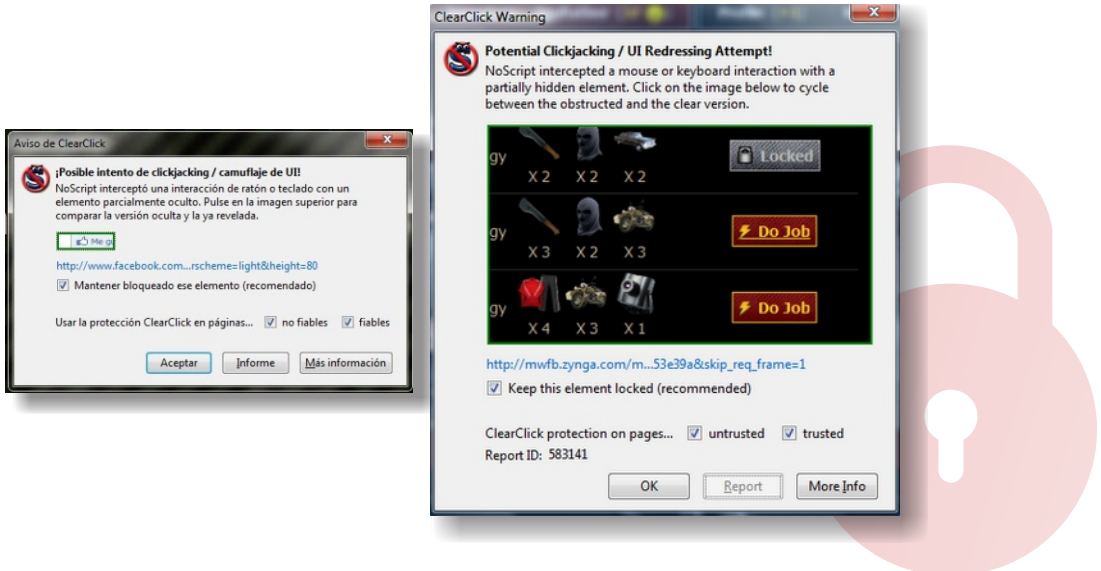
Reglas de oro para su seguridad

- Nunca acceda a su sitio de confianza desde links publicados en sitios desconocidos.
- Dichos links pueden estar montados sobre botones falsos que le llevarán al sitio o archivo malicioso.
- Como siempre, recuerde tener activas las alertas del navegador.

Para tener una idea más clara una imagen le ayudará a entender este delito informático.



Para protegerse usted del Clickjacking puede instalar una nueva tecnología denominada ClearClick, que chequearía que no este usando un botón pensando que es otro y si es así, le avisaría



5 Cross Site Scripting

Es una vulnerabilidad que aprovecha la falta de mecanismos de filtrado en los campos de entrada que permiten el ingreso y envió de datos sin validación alguna, aceptando el envió de scripts completos, pudiendo generar secuencias de comandos maliciosos que impacten directamente en el sitio o en el equipo de un usuario.

Reglas de oro para su seguridad

- Se debe evitar el acceso a sitios potencialmente no seguros a través de links sospechosos.
- Tener activada la protección del navegador de Internet para evitar estos fraudes.

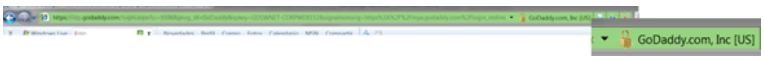
6 Pharming

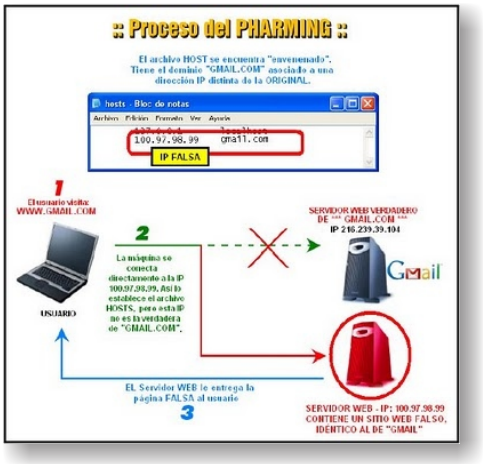
Consiste en suplantar al Sistema de Resolución de Nombres de Dominio (DNS, Domain Name System) con el propósito de conducirle a una página Web falsa. El delincuente al hacer esto altera el proceso de traducción entre la URL de una página y su dirección IP.

Comúnmente el atacante realiza el redireccionamiento a las páginas Web falsas a través de un código malicioso, para esto se requiere que el atacante logre instalar en su sistema alguna aplicación o programa malicioso.

Reglas de oro para su seguridad

- Los delincuentes cibernéticos pueden alterar el servidor DNS (nombre de dominio) de un sitio, pero no pueden adquirir un certificado de seguridad (que el sitio real sí posee), por ende lo más factible es que la página fraudulenta opere siempre bajo el contexto de una conexión no segura (sin https) por lo que el usuario notaría la acción fraudulenta en la barra de dirección.



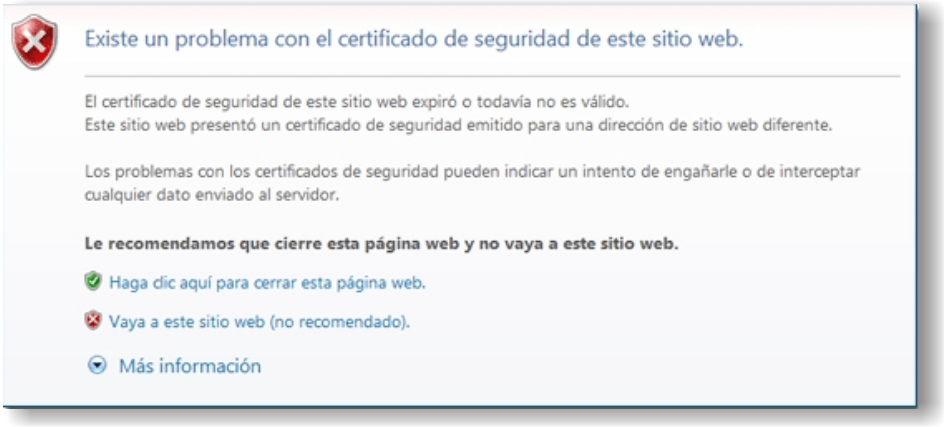


7 Conexiones Inseguras

Se produce cuando intercambiamos datos o nos conectamos con sitios sin certificados de seguridad al día, sin validaciones de seguridad de terceras partes. Las conexiones a sitios sensibles deben estar certificadas por entidades terceras, ya que toda transmisión de información puede ser vulnerada y necesita estar constantemente auditada en las medidas de seguridad que ofrece.

Reglas de oro para su seguridad

- Verificar que exista siempre una conexión segura del tipo (https://...)



8 REGLAS DE ORO PARA LA SEGURIDAD

Para aumentar nuestra seguridad debemos mitigar los riesgos, y para lograrlo, antes debemos conocerlos. Por eso es importante revisar la sección de fraudes más frecuentes antes de seguir las reglas que veremos en esta sección.

Recuerde que la primera regla es: NUNCA hacer clic en enlaces que le lleguen por e-mail queriendo que visite el sitio de su banco y se identifique. Si cree que el e-mail es cierto pues proviene de alguien que conoce o pareciera venir del mismo banco lo mejor es que le pregunte a su amigo si le ha enviado ese e-mail (llamándolo directamente) y digitando usted mismo la dirección del banco para ver si la misma información está publicada allí.

Las reglas de Oro las dividiremos en 3 mensajes:

- **VERIFIQUE** Nunca hagamos clic en enlaces como los mencionados al inicio de esta guía y asegurémonos de estar visitando la página real revisando que la dirección sea la correcta.
- **CUIDE** En una PC compartida no olvide cerrar su sesión para que otras personas no puedan acceder a su información. Recomendamos utilizar el modo PRIVADO para navegar cuando estemos en cabinas públicas.
- **ACTUALICE** Mantenga siempre al día su navegador o explorador de Internet y no descargue archivos de procedencia dudosa.

8 RECOMENDACIONES PARA EVITAR SER VÍCTIMA DE FRAUDE ELECTRÓNICO

- No realice operaciones bancarias a través de redes abiertas disponibles en cafés, restaurantes, aeropuertos o cualquier otro lugar que cuente con este sistema.
- Si va a realizar alguna transacción bancaria por medios electrónicos, hágalo en su casa u oficina, cierre cualquier otra ventana que tenga abierta en su computadora, sobre todo si está conectado a Facebook, Hotmail, My Space o Gmail, etc.
- Evite el acceso a operaciones por Internet desde computadoras personales de uso público ya que estos podrían estar contaminados con programas que capturan la secuencia de caracteres de la clave.
- Cuando este accediendo a Operaciones por Internet no desatienda sus operaciones ausentándose o distrayéndose con otras cosas.
- Cuando reciba un correo electrónico, verifique su autenticidad.
- Nunca acceder a nuestra página Web a través de links o enlaces que lleguen por correo electrónico.
- Realizar compras en comercios electrónicos seguros y confiables, de preferencia en aquellos que utilizan sistemas de autentificación en línea.
- Instalar programas antivirus en la computadora y mantenerlos actualizados.
- Solicite información a su entidad financiera acerca de los productos y servicios bancarios así como de las medidas de seguridad implementadas y que se encuentran a su disposición para poder usarlos con seguridad.
- Revise periódicamente sus estados de cuenta para detectar consumos no reconocidos.
- Actualice el Sistema Operativo y el Navegador de Internet de su computadora, siguiendo las instrucciones indicadas por los fabricantes de estos productos.
- Mantenga su computadora libre de virus informáticos y programas espías.
- No utilice computadoras públicas para efectuar operaciones en la Banca Electrónica.
- No anote ni comparta su Clave Secreta con nadie.
- Verifique que la dirección electrónica que aparece en la parte superior de la página Web corresponda a nuestra entidad. Si no puede verla o duda de la veracidad de un correo, contáctese con nosotros.
- Cuando utilice la Banca por Internet y requiera ingresar su código de usuario y clave personal, verifique que se encuentre en una zona segura presionando el icono del candado que aparece en la parte inferior de su navegador de Internet.
- Elija contraseñas fáciles de recordar, pero difíciles de adivinar. No escriba sus contraseñas ni las almacene en archivos electrónicos.
- Nunca descargue archivos ni baje de sitios desconocidos.
- Cierre la sesión cuando termine de operar.