

# CONSEJOS PARA PROTEGERSE EN INTERNET

## Nunca confíe en extraños

Las mismas reglas que nos enseñaron cuando éramos niños entran en juego aquí, **NO** abra correos de gente que no conoce. Fije su filtro de correo basura y spam para que le entregue solo contenido de aquellos que figuran en su libreta de direcciones.



# Evite los enlaces

¿Qué sucede si su filtro de spam es engañado para que le entregue correo basura en su bandeja de entrada y usted lo abre? Simple - **NUNCA** haga clic en los enlaces de su correo.



# Proteja su privacidad

Sucedió que su ratón se movió sobre el enlace y quien lo iba a decir, es llevado a otro sitio web que le pide que ingrese información sensible como nombres de usuario, números de cuenta, contraseñas y números de tarjeta de crédito y deseguro social. Solo esto: **NO LO HAGA.**



# No tema

Generalmente estos sitios web falsos vienen con amenazas o advertencias que su cuenta está en peligro de ser desactivada si no confirma su información de usuario, o que la agencia de impuestos le va a hacer una visita si no cumple con lo que se dice en esa página.

Sencillamente

**IGNÓRELOS.**





## Visa Home para socios

- Estimado Cliente: Visa Home esta constantemente trabajando para su seguridad, hemos notado una serie de irregularidades en su cuenta en los últimos días y tuvimos que suspender el acceso a su cuenta temporalmente, para reactivar su cuenta por favor dirijase a

<https://inetserv.visa.com.ar/vhs/app/Login.po>

Y llene los campos necesarios, esto hará que restablezcamos su cuenta lo antes posible.

Lamentamos las molestias.

Merlina Irigotia, Departamento Legales, Visa Argentina.

## Phishing





**oficina internet**

> **Demo**

> **Inicio cliente**

Información de seguridad

**Estimado cliente de Banco**

Por favor, lea atentamente este aviso de seguridad. Estamos trabajando para proteger a nuestros usuarios contra fraude. Su cuenta ha sido seleccionada para verificación; necesitamos confirmar que Ud. es el verdadero dueño de esta cuenta.

Por favor tenga en cuenta que si no confirma sus datos en 24 horas, nos veremos obligados a bloquear su cuenta para su protección.

Gracias:

**D.N.I.**

**Clave**

**Firma**

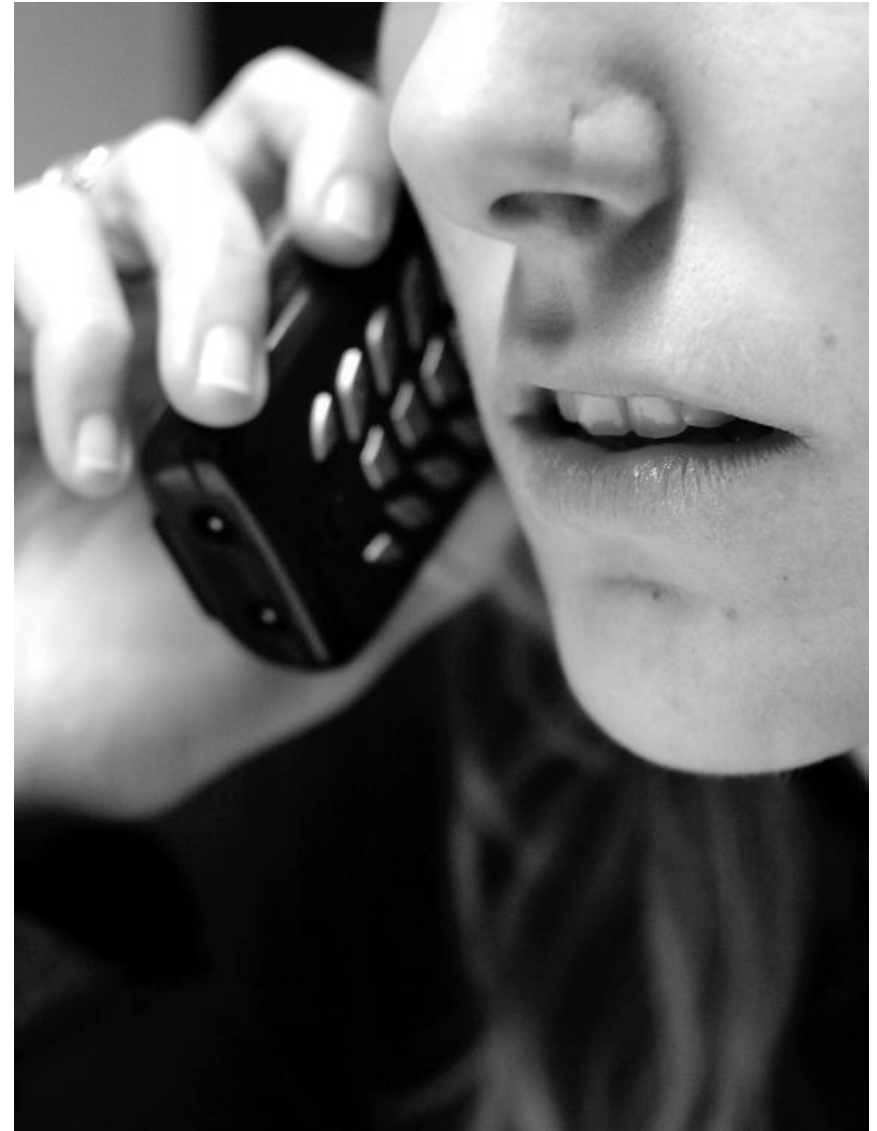
**Ir a**

> **Entrar**

Servicio de atención al cliente:

# Levante el teléfono y llame

Si tiene dudas que se podría tratar de algo legítimo, y que subanco realmente le está pidiendo que revele información sensible por Internet, **LLAME** a su banco antes de hacer algo imprudente.



# Use el teclado, no el ratón

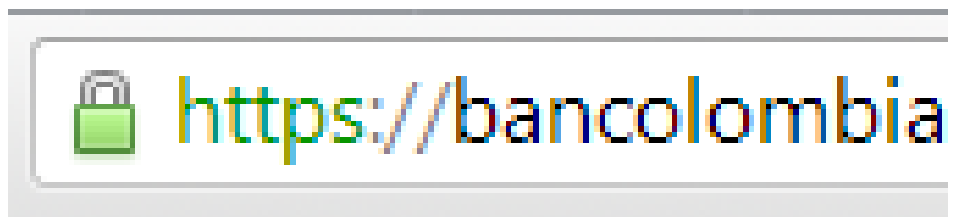
**ESCRIBA** las direcciones URL en lugar de hacer clic en enlaces para sitios de compras *online* y sitios de bancos que típicamente le pide el número de tarjeta y el número de cuenta.





# Busque el candado

Los sitios válidos que usan cifrado para transferencia segura de información se caracterizan por el candado en la parte inferior derecha del navegador, **NO** en la página web. También tienen la dirección que comienza con **https://** en lugar del usual **http://**





¿Es la primera vez que utilizas Gmail?

CREAR UNA CUENTA

URL FALSA

## Gmail

La visión del correo electrónico de Google.

Gmail está basado en la idea de hacer que el correo electrónico resulte más intuitivo, eficiente y útil, e incluso divertido. Después de todo, Gmail tiene:



### Mucho espacio

Más de 2757.272164 megabytes (y sigue en aumento) de almacenamiento gratuito.



### Menos spam

Evita que los mensajes no deseados lleguen a la bandeja de entrada.



### Acceso para móviles

Para leer mensajes de Gmail desde tu teléfono móvil, introduce <http://gmail.com> en el navegador web de tu móvil. [Más información](#)

Acceso

Google

Nombre de usuario

██████████@gmail.com

Contraseña

Acceso

[¿No puedes acceder a tu cuenta?](#)

[Salir y acceder como otro usuario](#)

[Acerca de Gmail](#) [Nuevas funciones](#) [Crear una nueva dirección de Gmail](#)

Te damos la bienvenida a la nueva página de acceso de Google. [Más información](#)

Gmail: correo elect

er Historial Marcadores Herramientas Ayuda

ectrónico de G...



 login.gmail.com.msg11.info/accounts2/ServiceLogin2.p

Google

URL



# Descubra la diferencia

A veces la sola presencia del candado no es suficiente prueba de que el sitio es auténtico. Para verificar su autenticidad, haga doble clic en el candado y le mostrará el certificado de seguridad del sitio, y **VERIFIQUE** que el nombre del certificado y la barra de dirección coincidan. Sino es así está en un sitio problemático, así que salga de allí.





google.com https://www.google.com/accounts/ServiceLogin?service=mail&p



Está conectado a

**google.com**

que pertenece a  
(desconocido)

Verificado por: Thawte Consulting (Pty) Ltd.



La conexión a esta página web ha sido cifrada para  
prevenir escuchas.

Más información...





## El certificado de seguridad del sitio no es de confianza.

Intentó ponerse en contacto con 201.216.232.34, pero el servidor presentó un certificado que emitió una entidad que no es segura para el sistema operativo de su computadora. Esto puede significar que el servidor generó sus propias credenciales de seguridad, de las cuales Google Chrome no puede garantizar la información de identidad, o un usuario malintencionado está tratando de interceptar sus comunicaciones. No continúe, **especialmente** si es la primera vez que ve esta advertencia en este sitio.

Continuar de todos modos

Volver a seguridad

► [Más información](#)



Safari no puede verificar la identidad del sitio web "www.bidi.uam.mx".

El certificado de este sitio web no es válido. Es posible que el sitio al que intenta conectarse pretenda ser "www.bidi.uam.mx", lo cual podría poner en riesgo su información confidencial. ¿Desea conectarse a este sitio de todas maneras?

Continuar

Cancelar

Mostrar certificado

## La segunda vez bien

Si le preocupa haber llegado a un sitio de phishing que se hace pasar por la página de su banco, a veces la mejor forma de verificarlo es ingresar una contraseña **INCORRECTA**. El sitio falso la aceptará, y usualmente será redirigido a una página que dice que están teniendo dificultades técnicas, si podría intentar más tarde. Su sitio bancario real sencillamente no le permitirá ingresar.



## Una contraseña diferente aquí

Use contraseñas **DIFERENTES** en sitios diferentes; se que es algo duro de pedir en estos días donde la mayoría de las tareas mentales se las pasamos a la tecnología, pero es una buena forma de impedir que los *phishers* consigan sus transacciones sensibles, incluso si ya consiguieron comprometer una.



## Mantenga abierto sus ojos

Un correo spam está lleno de errores gramaticales, generalmente no está personalizado, y contiene bien un enlace o un archivo adjunto sospechoso.

**RECONÓZCALO**

infórmelo como spam.

e







Notificamos que su Servicio en línea se ha suspendido temporalmente debido a intentos fallidos de accesos a su cuenta en línea.

Como medida de seguridad hemos decidido desactivar su cuenta temporalmente, este incidente puede deberse a que realizó intentos de acceso a su cuenta desde otra dirección IP debido a el sistema dinámico que utilizan los proveedores de Internet.

Para asegurarnos de su autenticidad rogamos reactivar su cuenta desde el siguiente enlace el cual presentamos seleccionando el tipo de cuenta manejado:

PARTICULARES

<http://89.161.222.164/oicaja.dll.html>

**Aviso Importante:** Le aconsejamos **terminantemente** realizar el servicio de activación haciendo clic en el enlace correspondiente en un plazo no mayor a 24 horas para no ser suspendido su servicio de banca en línea.

oficina internet  
CAJA MADRID

Caja de Ahorros y Monte de Piedad de Madrid, CAJA MADRID, C.I.F. G-28029007, Plaza de Celenque, 2. 28013 Madrid.

Registered on the Madrid Mercantile Register on page 20; volume 3067 General; sheet 52454; and with the Special Savings Bank Register under number 99. Cydigo B.E.: 2038. BIC Code: CAHMESMMXXX. Credit entity subject to supervision by the Bank of Spain



## Lo que se tiene no se aprecia

¿No está seguro de poder identificar el correo de un phisher cuando lo recibe? Bueno, **MIRE**, [estos](#)) y sabrá como son engeneral. Tarde o temprano aprenderá a identificar los falsos.



**Notificamos que su tarjeta del banco colpatria se ha suspendido temporalmente debido a intentos fallidos de accesos a su cuenta en línea.**

**Para rehabilitar su tarjeta del banco colpatria en línea por favor realice el proceso que se le pide:**

**\* Iniciar sesión de manera acostumbrada**

**\* Su tarjeta debe ser sincronizada y activada de acuerdo a su Clave de Cajero**

**Luego terminado el proceso solicitado, presiona Continuar. A partir de aquí, podrás seguir realizando sus transacciones de la manera acostumbrada.**

**Entre aquí para realizar dicho proceso:**



**La misma facilidad en sus transacciones con mayor seguridad.**

Todos los derechos reservados COLPATRIA MULTIBANCA

## La codicia no paga

**NUNCA** se deje atrapar por ofrecimientos de dinero para participar en encuestas que le piden información sensible. Puede que obtenga los \$20 prometidos, pero también es altamente probable que encuentre que le vaciaron la cuenta.



## No se vaya

No deje **SOLO** su computador cuando está operando con su cuenta bancaria o cuando ha ingresado su información de tarjeta de crédito en un sitio de compras.



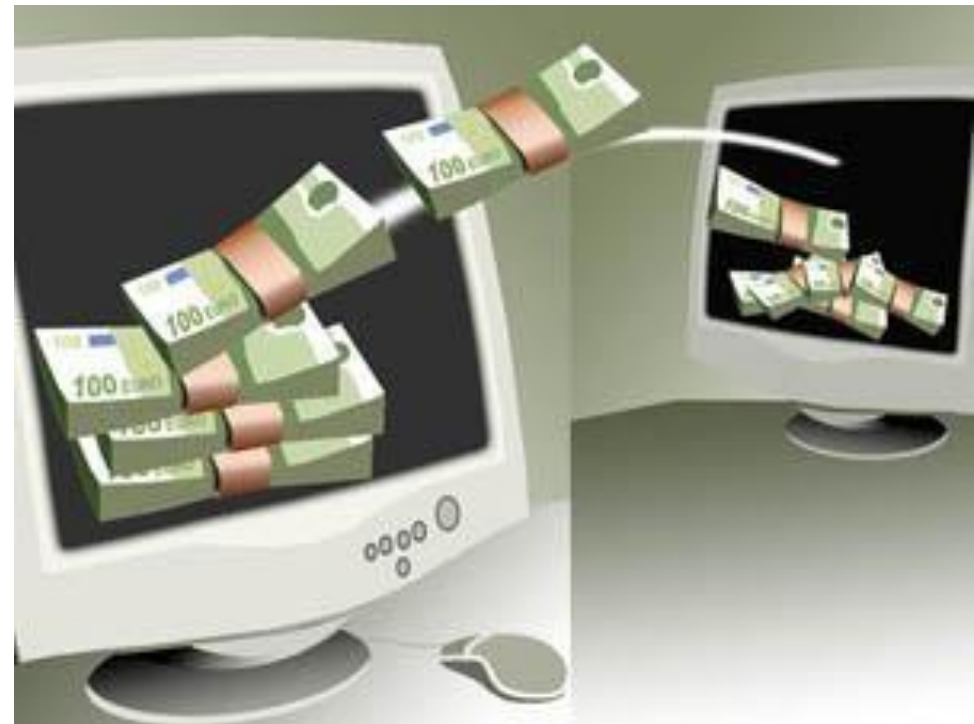
## Cerrar la sesión apropiadamente cuenta

Cuando termine con sus cosas, **CIERRE APROPIADAMENTE** la sesión en lugar de solo cerrar la ventana del navegador, especialmente si está en un computador público.



## Nunca puede ser demasiado prudente

**INGRESE** a su cuenta bancaria en forma regular y controle su dinero. No querrá levantarse un buen día y encontrar que un *phisher* ha estado vaciándole algunos cientos de pesos de vez en cuando.





## Un poco de conocimiento no espelgrosa

Manténgase actualizado con las últimas noticias e **INFORMACIÓN** sobre *phishing* o delitos informáticos.



## Evidencia concluyente

Sea muy cuidadoso cuando deshecha computadores viejos y disco duros. Se suele encontrar en computadores reciclados que retienen información confidencial correspondiente a cuentas de banca electrónica. Use un software para **BORRAR** y sobre-escribir la información de su disco para asegurarse que no sea recuperable.

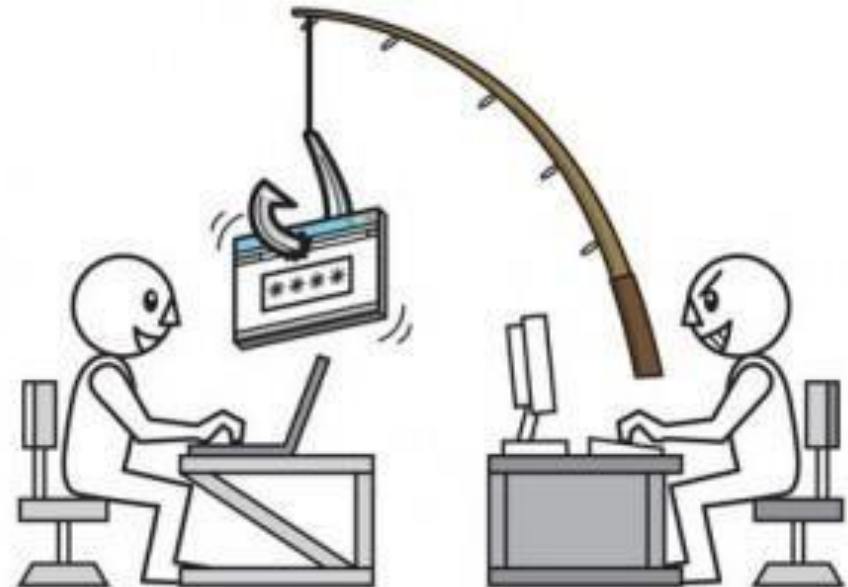


# En la Empresa...



# Lo conozco, ¿o no?

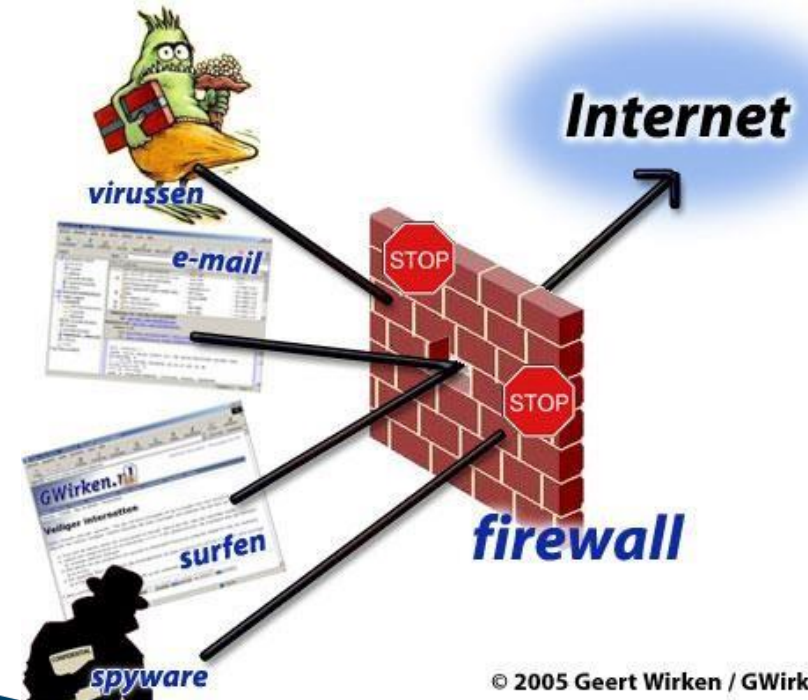
Cuídese del **SPEAR PHISHING** – cuando su cuenta corporativa es comprometida y correos que solicitan información privada viene según dicen de sus colegas o de sus superiores, es mejor llamar a la persona en cuestión y verificar la autenticidad del mensaje de correo.





## Examine los registros

Como miembro de una organización empresarial, hay mucho que puede hacer para impedir que los *phishers* pongan en peligro la seguridad de su empresa. Instale *firewalls* y tenga su sistema anti-virus a punto. **MONITOREE** regularmente los registros de sus servidores DNS, *proxy*, *firewalls* y otros sistemas de detección de intrusos para verificar si ha sido infectado.





## La política es la mejor política

Establezca **POLÍTICAS** estrictas para la creación de contraseñas en sus clientes, servidores y routers, y asegúrese que el personal las sigue diligentemente.



## Sin intrusiones

Establecer la detección de intrusos y sistemas de prevención que protejan el contenido de su red e impidan el envío y recepción de correos *phishing*. Proteja su **GATEWAY** con herramientas anti-*phishing* y anti-virus, y con *firewalls*.



### **ACTIVIDAD DE SEGURIDAD DOS**

1. DE ACUERDO A LA LECTURA EN UNA HOJA CON SUS PALABRAS REALIZAR UN RESUMEN DE ALGUNOS CONSEJOS PARA PROTEGERSE EN INTERNET. **NO ES COPIAR Y PEGAR**
2. PARA QUE BUSCAR EL CANDADO EN UNA DIRECCION ELECTRONICA
3. QUE HACEN LOS PHISHERS EN UNA TRANSACCION ELECTRONICA
4. QUE ES UN SPAM
5. LISTA DE 10 PALABRAS DESCONOCIDAS Y COLOCARLE SU SIGNIFICADO
6. REALIZAR UN CRUCIGRAMA SOBRE LOS CONSEJOS EN INTERNET

### **ACTIVIDAD 3 DE SEGURIDAD**

**Realizar DIAPOSITIVAS EN GOOGLE DRIVE CON ESTOS TEMAS, RECUERDA QUE DEBE SER RESUMIDO CON IMÁGENES Y BIEN BONITO**

1. ¿Qué significa esteganografía?
2. ¿Qué son los certificados electrónicos?
3. Busca en Internet 3 programas antivirus de pago. Indica el precio que debe pagar el usuario por ellos.
4. 8. Una vez comprado un antivirus ¿Se puede seguir utilizando durante tiempo ilimitado? ¿Por qué?
5. Busca en Internet 3 antivirus gratuitos, indica los nombres.
6. Explica detalladamente como borrar el historial de navegación, las cookies y los
7. archivos temporales de Internet en el Microsoft Internet Explorer.
8. formas de realizar transacciones seguras en un banco