Presentación

Seguro que has oído hablar de los ataques que reciben las grandes compañías o los bancos a través de sus sistemas informáticos, pero ¿sabes a qué te expones tú cada vez que te conectas a Internet?

Objetivos

- Conocer las amenazas del mundo de las tecnologías de la información: los virus, el «malware», los intentos de intrusión y el robo de información confidencial, entre otros.
- Estudiar las principales amenazas y saber cómo funcionan para protegernos ante ellas, adquiriendo técnicas preventivas que harán que nuestra documentación y privacidad estén a salvo.

Seguridad de la información

Las medidas técnicas son solo una parte de la solución para una política eficaz de protección de la información. La forma en que los empleados manejan la información de la empresa es también fundamental.

La **ciberseguridad** es el conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos.

Vulnerabilidades

En informática, una vulnerabilidad es una debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad.

Los términos vulnerabilidad y amenaza informática suelen confundirse, pero no son iguales. Mientras que la vulnerabilidad hace referencia a un **fallo interno**, la amenaza son las **acciones externas que intentan aprovechar este fallo**.

Ingeniería social

La ingeniería social manipula a las personas para que compartan información que no deberían compartir, descarguen software que no deberían descargar, visiten sitios web que no deberían visitar, envíen dinero a delincuentes o bien cometan otros errores que comprometan sus activos o seguridad personal o empresarial.

La **Ingeniería social** es una técnica que emplean los ciberdelincuentes para ganarse la confianza del usuario y conseguir así que haga algo bajo su manipulación y engaño, como puede ser ejecutar un programa malicioso, facilitar sus claves privadas o comprar en sitios web fraudulentos.

Un correo electrónico que parece proceder de un proveedor fiable en el cual se solicita información actualizada de la tarjeta de crédito, un buzón de voz amenazante que afirma ser del administrador de sistema o una notificación de Hacienda son solo algunos ejemplos de ingeniería social.

¿Como y por qué funciona?

- Fingen ser una marca fiable
- Fingen ser una agencia gubernamental o figura de autoridad
- Inducen miedo o una sensación de urgencia
- Apelan a la codicia
- Apelan a la buena voluntad o la curiosidad

Tipos de ataques de ingeniería social

- Mensaje de texto.
- Llamadas falsas.
- Estafas por redes sociales.
- Productos gratis.
- Correos spam.
- Tailgating

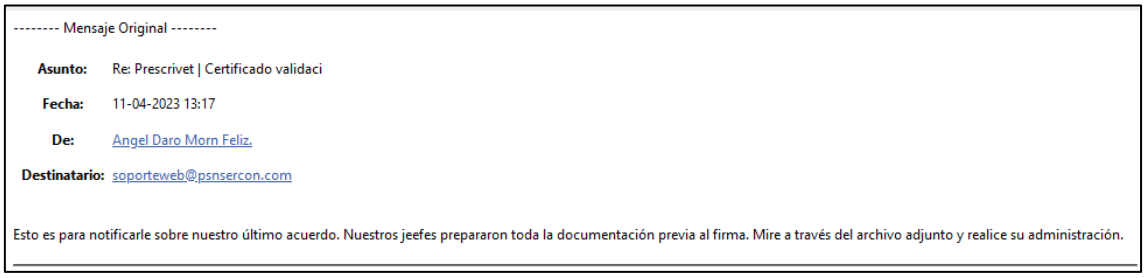
Tailgating

El tailgaiting es una violación de seguridad común en la cual un delincuente sigue a una persona autorizada a un área restringida con el fin de ganar acceso a esta. Este tipo de ataque de ingeniería social se aprovecha la cortesía humana para ayudar a los demás, por lo que el ejemplo más común es sujetar la puerta a un individuo desconocido que transita detrás de la víctima.

Ransomware

Es un software malicioso que impide el acceso a la información o al equipo de los usuarios. Básicamente, es un secuestro de información o de equipo y exige el pago de cierta cantidad para poder recuperarlos. Es uno de los ataques más populares con el que los criminales extorsionan a empresas y consumidores.

Normalmente, en este tipo de ataque, el usuario recibe un correo con un documento adjunto y le dan indicaciones de lo que debe hacer. Para evadir los antivirus, suele ser un documento protegido con algún código o contraseña, la cual se la indican en el correo. Para comprobar este documento podemos usar la web www.virustotal.com en la podemos cargar el documento y así analizarlo con varios antivirus.



-------- Mensaje Original --------

Asunto: Re: Prescrivet | Certificado validaci

Fecha: 11-04-2023 13:17

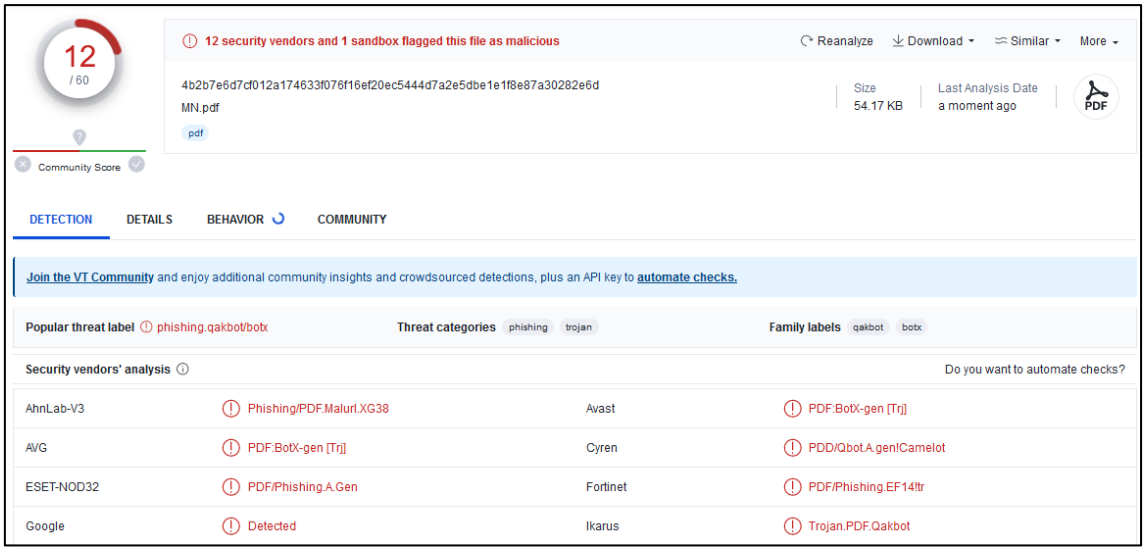
De: Angel Daro Morn Feliz.

Destinatario: soporteweb@psnsercon.com

Esto es para notificarle sobre nuestro último acuerdo. Nuestros jeefes prepararon toda la documentación previa al firma. Mire a través del archivo adjunto y realice su administración.

Al abrir el archivo podemos ver lo siguiente:

Tras analizar el documento adjunto con virus total, podemos ver que el pdf es un archivo infectado con virus.



Phishing

Todos los días, los delincuentes intentan robar información confidencial mediante el uso de ingeniería social y otras formas de engaño.

El **phishing** o suplantación de identidad es un tipo de ciberataque que tiene la finalidad de obtener información confidencial de los usuarios, normalmente información bancaria o de aplicaciones con acceso a pagos. Consiste en la creación de una comunicación al usuario, por lo general correo electrónico, cuya manipulación tiene una apariencia de veracidad.

El phishing continúa siendo uno de los ciberataques más exitosos por las siguientes razones:

- Utiliza canales de comunicación habituales de los usuarios.
- Conocen los gustos, actividades y tendencias de sus víctimas.
- Emplean mensajes personalizados, usando su nombre, correo electrónico o número de teléfono.
- Juegan con el sentido de urgencia o utilizan ganchos promocionales

Recomendaciones para prevenir ataques de Phishing

- Identificar los correos sospechosos, este tipo de correos suelen utilizar nombres e imagen de empresas reales, incluyen webs muy parecidas a las originales, utilizan regalos o promociones como ganchos, incluso la pérdida de la cuenta o información.
- Verificar la fuente de tus correos entrantes, tu banco no te pedirá tus datos personales y claves de acceso por correo.
- No entrar a links incluidos en correos electrónicos, ya que te redireccionan a una web fraudulenta para obtener tu información. Teclea directamente la página web a la que deseas acceder.
- Los ataques pueden llegar en cualquier idioma, generalmente tienen mala redacción o traducción lo que puede servir como un indicador para tener cuidado.
- Rechazar cualquier correo electrónico que requiera tu información, que sea una fuente sospechosa

Identificar el phishing

No basta sólo con saber su significado, debemos intentar evitarlo. Como norma, debemos eliminar cualquier correo que no esperemos, aun conociendo al remitente, ya que este ha podido ser víctima de un ataque que divulgue de forma descontrolada correos con el objetivo de extender el fraude. Si decidiéramos abrirlo, debemos verificar la extensión del archivo adjunto y revisar los enlaces a posibles sitios web fraudulentos.

Ejemplo de correo phishing

Aviso de notificación de la Agencia Tributaria - dario.moron@colvet.es

Agencia Tributaria <info@aeat.es>
Para hAqYzJFwlefCdXG2Nb

Responder Responder a todos Reenviar Borrar

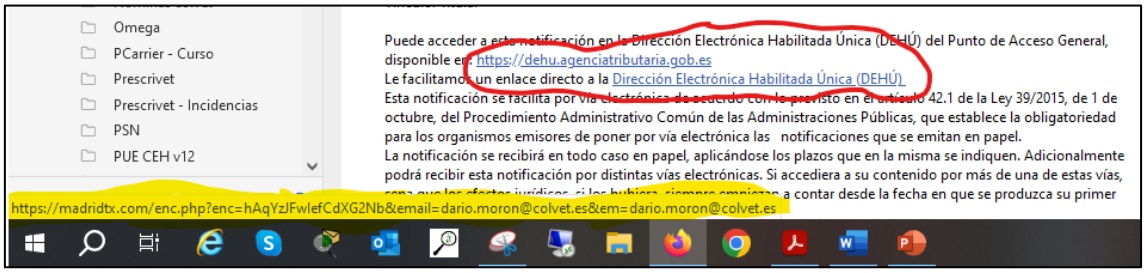
ESTE EMAIL SE CORRESPONDE CON UN AVISO DE UNA NOTIFICACIÓN POSTAL.

Le informamos que está disponible una nueva notificación para dario.moron@colvet.es Titular con los siguientes datos:

Titular: dario.moron@colvet.es
Organismo emisor: Agencia Estatal de Administración Tributaria, con DIR3: EA0028512
Identificador: 2299031217395
Concepto: Notificación administrativa
Vínculo: Titular

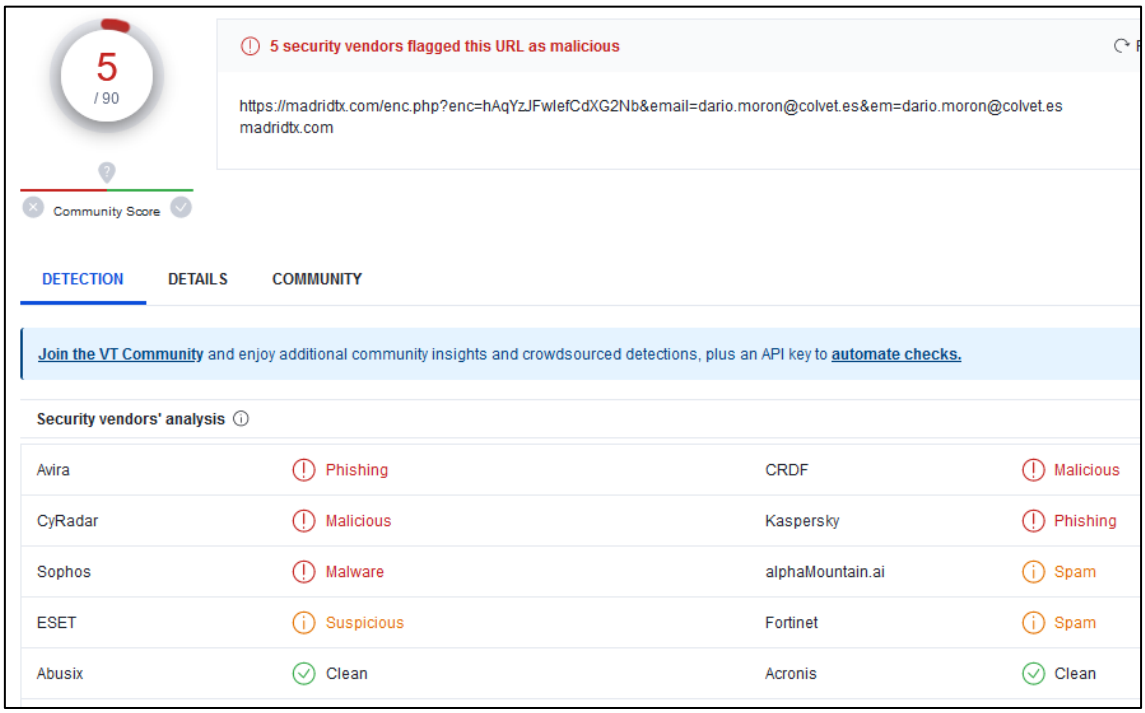
Puede acceder a esta notificación en la Dirección Electrónica Habilitada Única (DEHÚ) del Punto de Acceso General, disponible en: https://dehu.agenciatributaria.gob.es
Le facilitamos un enlace directo a la Dirección Electrónica Habilitada Única (DEHÚ)
Esta notificación se facilita por vía electrónica de acuerdo con lo previsto en el artículo 42.1 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que establece la obligatoriedad para los organismos emisores de poner por vía electrónica las notificaciones que se emitan en papel.
La notificación se recibirá en todo caso en papel, aplicándose los plazos que en la misma se indiquen. Adicionalmente podrá recibir esta notificación por distintas vías electrónicas. Si accediera a su contenido por más de una de estas vías, sepa que los efectos jurídicos, si los hubiera, siempre empiezan a contar desde la fecha en que se produzca su primer acceso.

Para comprobar si enlace es correcto y que nos lleva donde dice que nos llevaría, colocamos el ratón encima del enlace sin hacer clic (**CUIDADO SIN HACER CLIC**). Veremos que en la barra de estado *(ubicada en la parte inferior izquierda de la pantalla)* nos muestra el enlace al que nos va a dirigir cuando hagamos clic.



Como podemos observar en la imagen, el correo dice que tenemos una notificación electrónica en la sede DEHú. Pero si miramos bien en la barra dirección, el enlace nos lleva a DEHú sino a otro sitio web, que posiblemente contiene algún tipo de malware o ramsonware.

Ahora vamos a comprar si este enlace contiene alguna trampa. Primero, hacemos clic con el botón derecho encima del enlace (***Cuidado, con el botón derecho***), luego clic en copiar o copiar enlace. Segundo, entramos a www.virutotal.com , al entrar hacemos clic en **URL,** y pegamos el enlace que acabamos de copiar y presionamos **Enter.** Virustotal, nos dirá si ha encontrado alguna amenaza en él.



El sitio oficial de DEHú o Red Sara es: https://dehu.redsara.es/

La Dirección Electrónica Habilitada Única (DEHú) es un servicio electrónico de notificaciones para facilitar a los ciudadanos el acceso y comparecencia a sus notificaciones y/o comunicaciones emitidas por las Administraciones Públicas adheridas.

Más información en:
https://sede.mjusticia.gob.es/es/TramitesSede/Documents/Manual%20acceso%20a%20notificaciones%20de%20Nacionalidad%20en%20la%20DEHu.pdf

Defensas de ingeniería social

Los ataques de ingeniería social son notoriamente difíciles de impedir porque se basan en la psicología humana en lugar de vías tecnológicas. La superficie de ataque también es significativa: en una gran organización, basta con el error de un empleado para comprometer la integridad de toda la red empresarial. Algunas de las medidas que los expertos recomiendan para mitigar el riesgo y el éxito de las estafas de ingeniería social incluyen:

- Formación en concienciación de la seguridad
- Políticas de control de acceso

Seguridad física

Las amenazas más importantes contra las que la seguridad física que protege a una organización son las amenazas intencionadas de las personas, como pueden ser el robo o el acceso accidental.

Los accesos físicos son un problema de seguridad que involucran el robo de documentos confidenciales y otros objetos físicos de valor, tales como computadoras y unidades de almacenamiento.

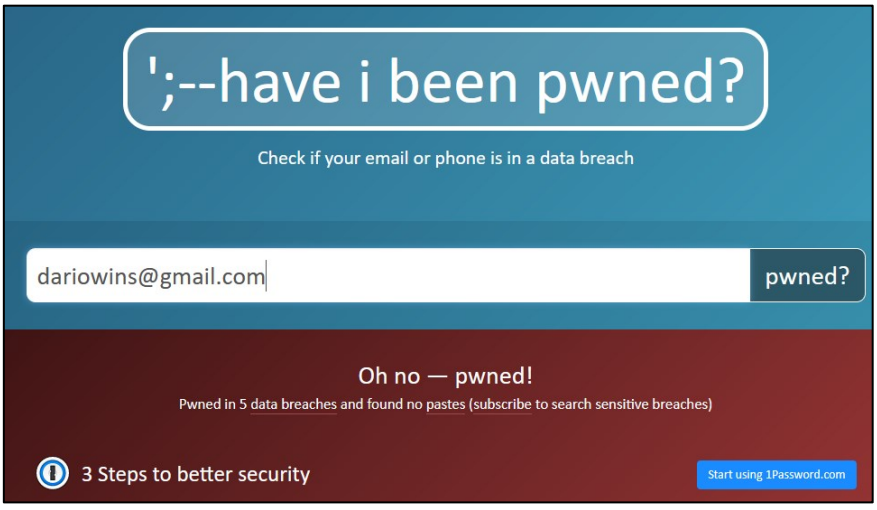
Redes sociales y trabajar en la nube

Las redes sociales le permiten llegar a una gran audiencia, pero también son una fuente de robo de identidad. Los servicios en la nube son muy accesibles, pero en ocasiones, el proveedor de servicios tiene los mismos derechos de acceso a tu información que tú.

Uso de contraseñas

Una buena política de seguridad comienza con una buena contraseña. Las contraseñas seguras garantizan que las personas no autorizadas no tengan acceso a información confidencial. Explicar cuales son los riesgos de una mala política de contraseñas.

En el sitio web: https://haveibeenpwned.com/ podemos comprobar si algún sitio donde estemos registrado, ha sido hackeado, de ese modo sabremos que en esa web han robado nuestra contraseña. Los usuarios por lo general usan las mismas cuentas y contraseñas para todos sus servicios, con lo cual, cuando un sitio es comprometido, los delincuentes informáticos tratan de acceder a todos los sitios donde el usuario este registrado.



Ciberseguridad para usuarios: Protección y Prevención

Gestión de las contraseñas.

Debemos crear y recordar contraseñas con una mínima seguridad. Una forma sencilla de estar protegido es utilizar contraseñas únicas para cada sitio web y dirección de correo electrónico. También es recomendable cambiarlas periódicamente.

Control de acceso de los usuarios al sistema operativo

Mediante una buena gestión de control de acceso al sistema se pueden evitar números riesgos ya que evitan el acceso no autorizado. Por ejemplo, que un usuario solo tenga acceso a sus archivos y no pueda tener acceso a la información de sus compañeros a menos que, compartan alguna información.

Protección frente a código malicioso

- Antivirus
- Cortafuegos (firewall)
- Antimalware

Seguridad en nuestro equipo

- Seguridad básica de nuestro equipo (actualizado, antivirus, contraseña).
- Importancia de bloquear el equipo (*es muy importante también* ***cerrar sesión antes de dejar el equipo****. Es posible que abramos nuestras cuentas de redes sociales, correo electrónico o incluso que utilicemos WhatsApp Web).*
- Pen drive, dispositivos USB y otros puntos de riesgo

Seguridad en nuestro email

- Cómo tratar e identificar correos de servicios no solicitados o de origen dudoso (correos, hacienda, bancos, etc). Ejemplos más actuales.
- Elementos que se deben revisar siempre en los correos
- Problemas vinculados a enviarse documentación de la empresa al correo personal.
- Gestión del spam.
- Que hago si tengo duda sobre un correo que he recibido

Seguridad web.

- Identificación y cómo tratar websites fraudulentos.
- Identificación y cómo tratar servicios no seguros.

- Por qué nunca usar aplicaciones pirateadas mediante cracks en modo portable, explicación de los peligros asociados al malware y tipología del malware (troyanos, rabbits, ransomware, etc…).
- No realizar uso en ningún caso de almacenamiento en nube no controlados y nunca subir información de la empresa a esos servicios.
- No hacer uso de aplicaciones gratuitas online a las que se suba información de la empresa.

Seguridad en la red.

- Redes confiables, wifis gratuitas, aeropuertos etc.

El antivirus.

La razón más evidente por la que debe mantener actualizado su software antivirus es que los nuevos virus y otros programas maliciosos atacan regularmente los ordenadores. Cada día, los ciberdelincuentes avanzan más en la creación de virus y malware más sofisticados, lo que podría dañar no solo su dispositivo sino también su reputación, ya que estos delincuentes se dirigen a su dispositivo para obtener acceso a su información personal.

Tener cuidado con las Wi-Fi públicas

Antes de conectarnos a una red Wi-Fi pública deberíamos tomar precauciones y sobre todo evitar las gratuitas.

Tomar precauciones con nuestro móvil

Dado que nuestros móviles contienen información confidencial, tanto personal como de empresa, debemos tomar las mismas precauciones que con nuestros ordenadores, pero teniendo en cuenta que se trata de un dispositivo que llevamos en todo momento con nosotros y podemos perder el control sobre él. Establecer un código de bloqueo para el acceso, desactivar la localización, wifi o bluetooth cuando no lo necesitemos, instalar alguna solución de seguridad contra virus o malware, cifrar los datos y no rootearlo, son algunos de los consejos de ciberseguridad que podemos daros para mantener nuestro móvil seguro.

Usar el sentido común

Debemos aplicarlo, como lo hacemos en otros aspectos de nuestra vida, como colocar una alarma en casa o no dejar la puerta abierta para que entre un extraño.

Siguiendo simplemente estas recomendaciones de ciberseguridad, podrá mejorar de manera significativa la seguridad de su negocio, pero no estará totalmente protegido.

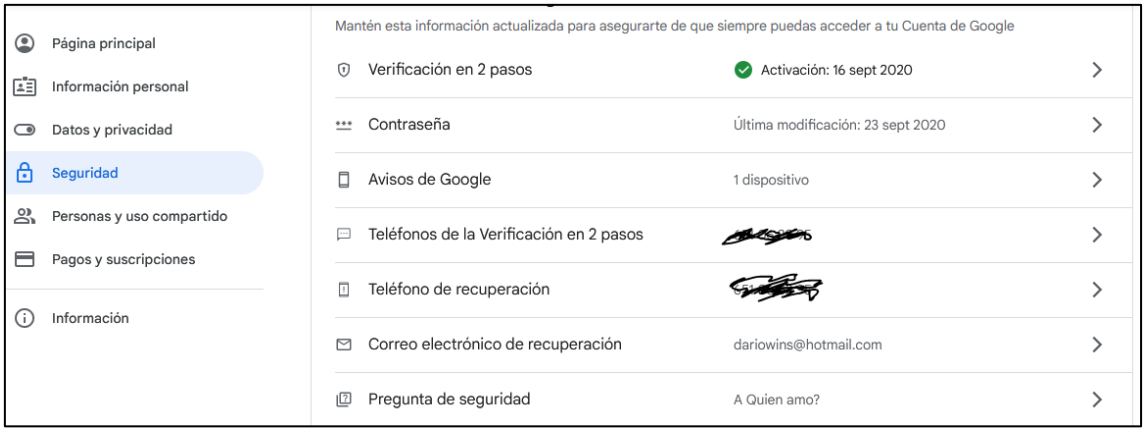
Conclusión

Los ataques de ingeniería social tienen éxito debido al error humano y la imposibilidad de identificar los patrones usados por los piratas informáticos; dicho esto, las organizaciones están en la obligación de educar a sus empleados sobre el impacto de estos ataques.

Enlaces de interés

Activar autenticación en dos pasos cuenta de Google

https://support.google.com/accounts/answer/185839?hl=es&co=GENIE.Platform%3DDesktop



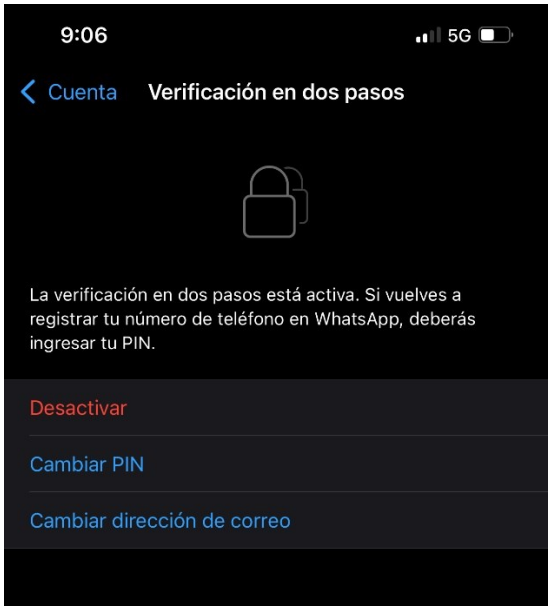
Activar autenticación en dos pasos cuenta Microsoft (Hotmail, Outlook)

https://support.microsoft.com/es-es/account-billing/activar-o-desactivar-la-verificaci%C3%B3n-en-dos-pasos-de-una-cuenta-de-microsoft-b1a56fc2-caf3-a5a1-f7e3-4309e99987ca

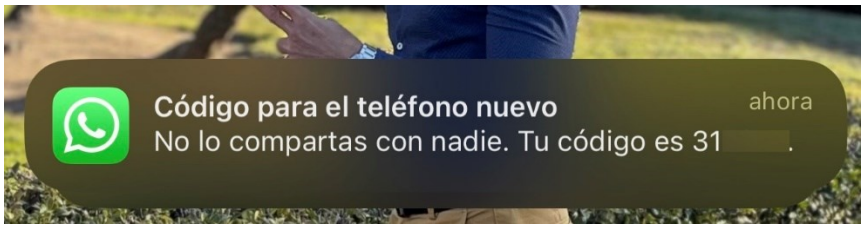
Para ayuda y soporte llamar al Consejo General de Colegios Veterinarios de España al número: 914 35 35 35 y preguntar por Dario.

Anexos

Verificación en dos pasos de WhatsApp



Configurar WhatsApp en otro móvil que no tiene nuestra SIM



En el otro móvil le pide esto: