

VOICE OF THE FIELDS

California

May 2026

FREE

Volume 36, Number 5

How to Avoid Phishing Scams

SCAM MESSAGES are becoming more and more common, especially through text messages, emails, and even phone calls. These scams are designed to trick people into sharing personal information or sending money.

While they can sometimes look real, knowing what to look for to determine whether the message is real or a scam can help keep you safe.

What is Phishing?

Phishing is a type of scam where someone pretends to be a trusted company, organization, or person to try to get your personal or financial information. This can include things like bank account numbers or a social security number.

Phishing scams can come through different methods of communication including:

- Emails that look like they are from a bank or company
- Text messages asking you to click a link or respond
- Phone calls pretending to be customer service or a government agency

These messages often look convincing, but the goal is to trick you into acting quickly, without thinking.

Common Signs of a Phishing Message

These messages often follow a similar pattern and are designed to

make you react quickly. Many of these phishing messages create a sense of urgency such as a warning that your account will be locked or

Continued on next page

PHISHING SCAMS: HOW TO STAY PROTECTED

According to a recent report by Ironscales, phishing scams are the root cause of 95% of all successful cyberattacks worldwide.

TOP 5 RED FLAGS	HOW TO STAY PROTECTED
<p>Web links lead to unfamiliar sites (hover over them to check!).</p>	<p>1 </p> <p>Don't click any links or attachments you can't verify with total certainty.</p>
<p>There's an attachment you weren't expecting.</p>	<p>2 </p> <p>Call to verify requests (even if it seems to come from someone or somewhere you know!)</p>
<p>You notice poor spelling and grammar throughout (this is on purpose!).</p>	<p>3 </p> <p>When in doubt, contact the SupportCenter for help!</p>
<p>It asks for personal information like passwords or bank information.</p>	<p>The sender doesn't address you by name.</p>



Phishing

Continued from previous page

that you must act immediately. They may claim there is a specific activity or a problem with your account, even if nothing is actually wrong. It is also common for these messages to ask for specific personal or financial information, include unexpected links or attachments, or even appear to be from companies you may not have an account with. Some may even offer deals that seem too good to be true, like prizes or free money. Even if a message seems to look official, these warning signs can help you to recognize when something is not quite right.

How to Protect Yourself

Protecting yourself from scams starts with being cautious about the messages that you receive. If something feels unexpected, avoid clicking on links or downloading any attachments, especially if you don't recognize the sender. It is also important to remember never to share personal or financial information through email or text, even if it appears to have come from a trusted source. You should regularly update your phone and other devices to protect against new security threats and can maximize safety

and protection by using strong passwords and enabling multi-factor authentication. Together, these habits can significantly reduce your risk and make it harder for scammers to gain access to your information.

Here are a few common examples of phishing scams:

- A message saying your bank account has had some suspicious activity and asking you to click a link to verify the information.
- A text claiming you have won and prize and that you need to provide details to receive it
- An email about a bill or subscription that you do not recognize.

to gain access to your information.

What To Do If You Get a Suspicious Message

If you receive a message that doesn't seem right, it is important that you neither click on any link or attachments, nor

reply to the message. Ask yourself if you have an account with this company mentioned and if you would like to confirm that the message is real, contact them using a trusted number. Open the company's website and call the number provided, do not use the contact information from the message.

What To Do If You Already Clicked or Shared Information

If you think that you have interacted with a scam message, it is best to take action immediately. Start by changing your passwords, especially for important accounts like email, banking, or other accounts that contain personal information. If financial information was shared,

contact your bank right away so that they can monitor your account.

How To Report Scams

If you receive a phishing message or believe you have been targeted by a scam, reporting it can help protect you and others. Scam emails can be forwarded to reportphishing@apwg.org, the Anti-Phishing Working Group and suspicious activity can be reported to the Federal Trade Commission at www.reportfraud.ftc.gov.

If you would like to learn more about how to recognize and report phishing scams, visit the America's cyber defense Agency website at cisa.gov/secure-our-world/recognize-and-report-phishing. Remember, scammers often rely on urgency and confusion to trick people. Taking a moment to pause, verify information, and think before responding can go a long way in protecting your personal information and keeping you safe.

VOICE OF THE FIELDS

California Circulation: 22,500 copies bi-monthly

www.LaCooperativa.org

Published monthly by:

La Cooperativa Campesina de California

1107 9th Street, Suite 420, Sacramento, CA 95814

Phone 916.388.2220 • Fax 916.388.2425

This product is copyrighted by the institution that created it. Internal use by an organization and/or personal use by an individual for non-commercial purposes is permissible. All other uses require the prior authorization of the copyright owner.

Content produced by ALZA Strategies, a full-service strategy firm that offers quality media relations, crisis communications, public affairs services, and expertise into the growing Latino market.



LA VOZ DEL CAMPO

California

mayo de 2026

GRATIS

Volumen 36, Número 5

Cómo Evitar las Estafas de Suplantación de Identidad o "Phishing"

LAS ESTAFAS POR MENSAJE son cada vez más comunes, especialmente a través de mensajes de texto, correos electrónicos e incluso llamadas telefónicas.

Estas estafas están diseñadas para engañar a las personas con el objetivo que compartan información personal o envíen dinero. Si bien a veces pueden parecer reales, saber qué buscar para determinar si el mensaje es real o una estafa puede ayudarlo a mantenerse seguro.

¿Qué es el "phishing"?

El "phishing" es un tipo de estafa en la que una persona se hace pasar por una compañía, una organización o una persona de confianza para obtener su información personal o financiera. Esto puede incluir datos como números de cuenta bancaria o un número de seguro social.

Las estafas de "phishing" pueden emplear distintos métodos de comunicación, incluidos los siguientes:

- Correos electrónicos que parecen ser de un banco o una compañía.
- Mensajes de texto en los que se le pide ingresar a un enlace o responder.
- Llamadas telefónicas haciéndose pasar por un servicio de atención al cliente o una agencia del gobierno.

Estos mensajes suelen parecer convincentes, pero el objetivo es engañarlo para que actúe en forma rápida, sin pensar.

Signos Comunes de un Mensaje de "Phishing"

Estos mensajes suelen seguir un

patrón similar y están diseñados para que usted reaccione rápidamente. Muchos de estos mensajes de "phishing" generan

Continúa en la página siguiente

ESTAFAS DE PHISHING: CÓMO PROTEGERSE



De acuerdo con un informe de Ironscales, las estafas de phishing son la causa principal del 95% de todos los ciberataques exitosos en todo el mundo

5 SEÑALES DE ALERTA

Enlaces web llevan a sitios desconocidos (pase el cursor sobre el enlace para verificar).



Hay un documento adjunto que no se esperaba.

Nota que el texto está lleno de errores ortográficos o gramaticales (lo hacen a propósito).



Se piden datos personales como contraseñas o datos bancarios.

El remitente no se dirige a usted por el nombre.



CÓMO PROTEGERSE



No haga clic en enlaces o documentos adjuntos que no puede verificar con absoluta seguridad.



Llame para verificar solicitudes (aunque parezca que proviene de alguien o de un lugar que usted conoce).



Cuando tenga alguna duda, contáctese con el Centro de Asistencia para obtener ayuda.



Phishing

Continuación de la página anterior

una sensación de urgencia, como una advertencia de que su cuenta se bloqueará o de que debe actuar de manera inmediata. Pueden indicar que hay una actividad o un problema específico con su cuenta, aunque en realidad no exista ningún problema. También es común que estos mensajes le pidan información personal o financiera específica, incluyan enlaces o archivos adjuntos inesperados, o incluso parezcan ser de compañías en las que no tiene una cuenta. Algunos hasta pueden ofrecer cosas demasiado buenas para ser reales, como premios o dinero en forma gratuita. Incluso si un mensaje parece ser oficial, estos signos de advertencia pueden ayudarlo a reconocer cuando algo no esté del todo bien.

Cómo Protegerse

El primer paso para protegerse de estafas es tener cuidado con los mensajes que recibe. Si algo parece inesperado, evite ingresar a enlaces o descargar archivos adjuntos, especialmente si no reconoce el remitente. También es importante recordar que nunca debe compartir información personal o financiera por correo electrónico o mensajes de texto, aunque la fuente parezca confiable. Debe actualizar su teléfono y otros dispositivos en forma periódica para estar protegido contra nuevas amenazas

a la seguridad y puede maximizar la seguridad y la protección mediante el uso de contraseñas seguras y la autenticación multifactorial. La suma de estos hábitos puede reducir significativamente el riesgo y dificultar el acceso de los estafadores a su información.

Qué Hacer Si Recibe un Mensaje Sospechoso

Si recibe un mensaje sospechoso que no parece real, es importante que no haga clic en ningún enlace o archivo adjunto, ni responda el mensaje. Piense si tiene una cuenta en la compañía que se menciona en el mensaje y, si desea confirmar que el mensaje es real, comuníquese con la compañía a un número conocido.

Abra el sitio web de la compañía y llame al número que figure allí, no use la información de contacto del mensaje.

Qué Hacer Si Ya Hizo Clic o Compartió Información

Si piensa que ha interactuado con un mensaje de estafa, lo mejor es tomar medidas inmediatamente. Comience cambiando sus contraseñas, especialmente en las cuentas importantes como correo electrónico, cuentas bancarias y otras cuentas que contienen información personal. Si compartió información financiera, comuníquese con el banco de inmediato para que puedan monitorear su cuenta.

Cómo Denunciar Estafas

Si recibe un mensaje de “phishing” o cree que ha sido víctima de una estafa, hacer la denuncia puede ayudar a protegerlo y proteger a otras personas. Los correos electrónicos de estafas pueden reenviarse a reportphishing@apwg.org, el Grupo de Trabajo Anti-Phishing (Anti-Phishing Working Group) y las actividades sospechosas pueden informarse a la Comisión Federal de Comercio (Federal Trade Commission) en www.reportfraud.ftc.gov.

Si desea obtener más información sobre cómo reconocer y denunciar estafas de “phishing”, visite el sitio web de la Agencia de Ciberdefensa de Estados Unidos (America’s Cyber Defense Agency) en cisa.gov/secure-our-world/recognize-and-report-phishing. Recuerde, los estafadores se aprovechan de la urgencia y la confusión para engañar a las personas. Tomarse un momento para hacer una pausa, verificar la información y pensar antes de responder puede ser de gran ayuda para proteger su información personal y mantenerlo seguro.

LA VOZ DEL CAMPO

Circulación California: 22,500 ejemplares bimestrales

www.LaCooperativa.org

Una publicación mensual de: La Cooperativa Campesina de California

1107 9th Street, Suite 420, Sacramento, CA 95814
teléfono 916.388.2220 • fax 916.388.2425

Este producto es propiedad de la institución que lo creó. El uso interno de una organización y / o el uso personal por un particular para fines no comerciales está permitida. Todos los demás usos requieren la autorización previa del titular de los derechos de autor.

Este contenido ha sido producido por ALZA Strategies, una empresa que ofrece estrategias íntegras para lograr relaciones de alta calidad con los medios informativos y gestionar comunicaciones en situaciones de crisis, además de servicios sobre asuntos públicos y pericia sobre el creciente mercado latino.

