



Esté alerta para evitar a estafadores tratando de aprovecharse de la pandemia de coronavirus, enviando correos electrónicos de suplantación de identidad o “phishing” para robarle su información personal y financiera.

En la estafa de correos electrónicos “phishing”, ladrones fingen ser oficiales de salud incluyendo a la Organización Mundial de la Salud y Centros para el Control y la Prevención de Enfermedades. Envían correos electrónicos de suplantación de identidad que podrían instalar un virus en su aparato electrónico y robar su información, lo cual incluye a contraseñas y nombres de usuario.



## CONSEJOS ÚTILES

- Verifique la validez de las compañías, organizaciones benéficas o individuos enviándole información sobre el coronavirus. Inspeccione toda dirección electrónica cuidadosamente para asegurarse de que viene de una página de internet legítima.
- Tenga cuidado con cualquiera que le envíe un correo electrónico de ofertas para suministros o tratamientos para coronavirus o que pida información personal. Busque palabras mal escritas o errores gramáticos.
- Mantenga al día los programas antivirus en su computadora.
- Denuncie presunta actividad fraudulenta a la policía.

Si usted o alguien a quien usted conoce ha sido víctima de una estafa, comuníquese con su departamento de policía local.

Fiscalía de Distrito del  
Condado de Los Ángeles

# Estafa de “phishing” por Correo Electrónico



To learn about other frauds, visit  
<http://da.lacounty.gov/community/fraud-alerts>

<http://da.lacounty.gov>

 @LADAoffice #FraudFriday



*Jackie Lacey*  
District Attorney