**Nota:** <https://www.welivesecurity.com/la-es/2020/04/29/programa-quedate-casa-engano-busca-robar-informacion-usuarios/>

**¿Qué tipo de amenaza es?** Phishing

**¿Cómo comienza y cómo se propaga esta amenaza?**

Phishing es el delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito. Las víctimas reciben un mensaje de correo electrónico o un mensaje de texto que imita a una persona u organización de confianza, como un compañero de trabajo, un banco o una oficina gubernamental.

**¿Hay más de una amenaza aplicada ?** No

**¿Qué solución o medida recomendarían?**

* No abra correos electrónicos de remitentes que no le sean familiares.
* No haga clic en un enlace dentro de un correo electrónico a menos que sepa exactamente a dónde le lleva.
* Para aplicar esa capa de protección, si recibe un correo electrónico de una fuente de que la que no está seguro, navegue manualmente hasta el enlace proporcionado escribiendo la dirección legítima del sitio web en la dirección legítima del sitio web en su navegador.
* Busque el certificado digital del sitio web.
* Si se le pide que proporcione información confidencial, compruebe que la URL de la página comienza con “HTTPS” en lugar de simplemente “HTTP”. La “S” significa “seguro”. No es una garantía de que un sitio sea legítimo, pero la mayoría de los sitios legítimos utilizan HTTPS porque es más seguro. Los sitios HTTP, incluso los legítimos, son vulnerables para los hackers.
* Si sospecha que un correo electrónico no es legítimo, seleccione un nombre o parte del texto del mensaje y llévelo a un motor de búsqueda para ver si existe algún ataque de phishing conocido que utiliza los mismos métodos.
* Pase el cursor del ratón por encima del enlace para ver si es legítimo.