Medidas de protección del Covid-19 en la banca digital

5 de junio de 2020

Autor: Soledad Solano Rojo
Miembro del equipo de trabajo de Edufinet

Ante la crisis sanitaria mundial debida al COVID-19, los ciudadanos han modificado sus comportamientos y hábitos de consumo, evitando multitudes, mejorando la higiene personal, trabajando desde casa, recibiendo clases “on line”…

Todo ello ha llevado a un mayor uso de las nuevas tecnologías, al aumento de las personas conectadas a la Red, a un mayor número descargas de plataformas de video llamadas, mensajes por telefonía móvil, y, a su vez, a una mayor proliferación de virus y amenazas informáticas.

Al igual que aumentamos las medidas de seguridad para combatir el coronavirus, debemos aumentar las medidas de seguridad para combatir los "ciber-riesgos" y los "cibercrímenes".

A pesar de que desde 2019 está implantada la Directiva 2015/2366, sobre servicios de pago en el mercado interior, o **PSD2** (*Payment Services Directive 2*), norma cuyo principal objetivo es establecer un marco regulatorio en el mercado europeo de los servicios de pago, fundamentalmente, en los pagos digitales, y mejorar la seguridad para prevenir el fraude, no debemos bajar la guardia, ya que los "ciberdelincuentes" están aprovechando estos momentos de preocupación de los ciudadanos por el coronavirus para cometer estafas electrónicas y obtener información privada de los usuarios.

Algunas recomendaciones de seguridad te ayudarán a detectar este tipo de ciberataques y a proteger adecuadamente tu información sensible y tus dispositivos:

1. **Ningún organismo oficial solicita datos personales a través de correo electrónico o SMS**, así que no los proporciones por ninguno de estos
2. **Verifica el remitente de los correos electrónicos y los enlaces que estos incluyen,** y desconfía si contienen letras y caracteres extraños. Siempre debes comprobar la dirección web a la que te intenta dirigir un enlace antes de
3. **No descargues ningún archivo adjunto relacionado con el coronavirus COVID-19 sin antes asegurarte de su origen legítimo.** Tal como exponen las autoridades, la cura del coronavirus no la recibirás por correo electrónico.
4. **No descargues aplicaciones no oficiales** para conocer el alcance global del
5. **Evita difundir contenido que no haya sido contrastado**, ya que puede formar parte de una campaña malintencionada de
6. **Ten precaución si recibes alguno de los siguientes correos electrónicos** o mensajes fraudulentos relacionados con el coronavirus que están circulando durante estos días por la Red:
    - Correo electrónico en el que suplantan al **departamento interno de la empresa** y en el que invitan a descargar un PDF, infectado con *malware*, con el **protocolo que la compañía ha activado para enfermedades contagiosas**.
    - Correo electrónico de la **Organización Mundial de la Salud** (OMS) que incluye un botón para descargar las medidas de seguridad (escrito en inglés, ***Safety measures***).
    - Correo electrónico del **Centro para el Control y la Prevención de Enfermedades** (CDC) en el que se informa del avance del coronavirus y se solicitan donaciones **a través de *bitcoins***. El correo, redactado en inglés, está firmado por la *Division of eHealth Marketing*.
    - Correos que contienen las **últimas estadísticas sobre contagios**.
    - También han sido detectados diversos mapas "on line" que muestran el número de infectados por el coronavirus en cada uno de los países. **Las páginas web y aplicaciones que los albergan contienen *software* espía y *malware*** y han sido diseñadas para infectar los dispositivos de los usuarios.
7. Por ningún motivo se debe compartir el código de activación de ninguno de los canales financieros.

En resumen, puede ser suficiente con hacer uso del sentido común, y preguntarse, por ejemplo, ¿para qué se necesita la información solicitada? No es lógico que una institución necesite el usuario o la contraseña de nuestras cuentas bancarias para acceder a información pública.

Autoría de la imagen: freepik