Medidas de seguridad para el sistema Popular en Línea del BPDC

a. Al ingresar al sistema Popular en Línea del Banco Popular asegúrese de hacerlo digitando usted mismo la dirección **https://www.bancopopular.fi.cr/** en la barra de direcciones del navegador de internet nunca hacerlo a través de enlaces (links) o buscadores de internet.

b. Una vez que se encuentre en nuestro sitio, debe verificar que cuenta con el certificado de seguridad emitido exclusivamente para **https://www.bancopopular.fi.cr/**, por lo general esta información se puede validar dando clic en el icono del candado que se muestra el navegador de internet en la parte superior o inferior dependiendo del navegador de internet que se esté utilizando.

c. Recuerde que por motivos de seguridad sus claves no aparecen en la pantalla al momento de ser digitadas. Nunca entregue su clave a terceras personas y mantenga seguridad de esta.

d. Asegúrese de que nadie le esté observando al digitar su clave de acceso; sí sospecha que alguien la conoce, cámbiela inmediatamente.

e. Al ingresar su contraseña de forma incorrecta más de tres veces, esta será bloqueada por seguridad.

f. Al finalizar el uso del sistema Popular en Línea, siempre debe oprimir la opción **"Desconectar".**

g. No realice sus transacciones financieras si se encuentra conectado en redes públicas de internet, como internet cafés, centros comerciales, aeropuertos, entre otros.

h. Su clave de acceso es secreta, el Banco Popular nunca se la solicitará a través de ningún medio; ni por funcionarios, ni correos electrónicos, ni redes sociales, sí recibe este tipo de solicitudes, repórtelo inmediatamente al Banco Popular por medio de nuestro número telefónico de Banca Fácil 2202-2020 o al correo popularenlinea@bp.fi.cr.

i. El Banco Popular nunca le solicitará que cambie o que actualice sus datos con información sensible como Usuarios, Contraseñas, Pines de Tarjetas o Códigos de Verificación vía correo electrónico, teléfono, página web, redes sociales o mediante algún enlace (link o hipervínculo), sí recibe alguna solicitud de este tipo debe reportarlo inmediatamente al Banco Popular por medio de nuestro número telefónico de Banca Fácil 2202-2020 o al correo popularenlinea@bp.fi.cr.

j. En ninguna circunstancia atienda solicitudes de instalar aplicaciones de acceso remoto en su computadora o dispositivo móvil, ya que a través de estas un tercero podría observar su información, y/o descargar e instalar software malicioso de dudosa procedencia en su computadora o dispositivo móvil.

Reglas para crear su contraseña

Cuando usted crea su contraseña en el sistema Popular en Línea, se recomienda usar las siguientes características seguridad:

a. El tamaño de la contraseña debe crearse con al menos 10 caracteres y con un máximo de 16.
b. La contraseña debe combinar números (dígitos del 0 al 9) y letras (mayúsculas y minúsculas), sin usar caracteres iguales en secuencia.
c. Validar que la contraseña no contenga el código de usuario.

d. No se puede utilizar contraseñas creadas previamente.
e. No se puede utilizar caracteres especiales, por ejemplo: letra ñ, o símbolos (¡ ” # $ % & entre otros).
f. No use datos personales en sus contraseñas ni palabras del diccionario o frases comunes, que son fáciles de adivinar por los ciberdelincuentes.
g. Utilice los métodos de doble factor de autenticación en su correo electrónico.

Medidas de seguridad con las amenazas informáticas.

El **“robo de información”,** es el método más usado para realizar robo de identidad en Internet, consiste en obtener información confidencial de los usuarios de los sistemas de información, indicando fraudulentamente ser la entidad financiera, utilizando algunos de sus medios de contacto, el estafador puede usar comúnmente las siguientes modalidades:

a. Ingeniería Social:

El término **“Ingeniería Social”** hace referencia a una técnica persuasiva que se vale de la inocencia o desconocimiento de las personas para poder obtener información y de esta manera vulnerar sistemas de seguridad, por lo general el atacante se hace pasar por otra persona y de esta manera engaña o persuade al usuario.

Cuáles son las etapas en que incurren los ciberdelincuentes que utiliza la ingeniería social:

i. ACERCAMIENTO para ganarse la confianza del usuario, haciéndose pasar por un integrante de la institución financiera.
ii. ALERTA, para desestabilizar al usuario y observar la velocidad de su respuesta. Por ejemplo, “necesitamos actualizar sus datos o podría tener problemas con sus cuentas”.
iii. DISTRACCIÓN, es decir, una frase o una situación que tranquiliza al usuario y evita que se concentre en la alerta. Ésta podría ser un agradecimiento que indique que todo ha vuelto a la normalidad, en caso de que sea mediante correo electrónico o un link a una página web falsa, generando la redirección a la página web autentica de la institución posterior a obtener los datos.

¿Mediante qué medios puede presentarse un ataque de ingeniería social?

- **Correo electrónico (Phishing).**
- **Llamada telefónica (Vishing)**.
- **Mensaje de texto (Smishing).**

i. Por medio de un correo electrónico (Phishing)

Esta técnica consiste en engañar a las personas por medio de un correo electrónico en nombre de la entidad financiera, indicando la necesidad de actualización de datos. Seguidamente lo invita por medio de un link (enlace o hipervínculo) a visitar la página falsa de dicha entidad. Posteriormente le solicitará información confidencial como son sus datos personales, contraseñas, entre otra información sensible.

Después de capturada la información los ciberdelincuentes ingresan a la página original del Banco y realizan transacciones en sus cuentas y servicios.

ii. Por medio de una llamada telefónica (Vishing)

La persona recibe una llamada donde un tercero se hace pasar por un funcionario de la entidad bancaria, en ocasiones utilizan una grabación supuestamente de la entidad financiera informando que su cuenta, tarjeta de crédito, entre otros, está siendo utilizada y que debe llamar al número indicado a continuación, el número puede ser un número gratuito falso de la

entidad, una vez realizada la llamada por la víctima se le solicita información confidencial (credenciales de acceso a sistemas, información de tarjetas, entre otros).

iii. Por medio de un mensaje de texto (Smishing)

Por medio de un mensaje de texto enviado al celular alertan al usuario y lo invitan a ingresar a una página falsa, donde se solicitará información confidencial.

iv. ¿Cómo puedo protegerme?

La mejor manera de protegerse contra las técnicas de ingeniería social es utilizando el sentido común y no divulgando información que podría poner en peligro la confidencialidad de mis datos.

Sin importar el tipo de información solicitada, se aconseja que:

- Averigüe la identidad de la otra persona al solicitar información precisa (apellido, nombre, institución, número telefónico).
- Ante la duda verifique la información proporcionada, directamente con la entidad financiera.
- Pregúntese qué importancia tiene la información requerida.

b. Por medio de código malicioso (Virus, software espía, otros).

Un **"código malicioso"** en un software que tiene por objeto alterar el normal funcionamiento de la computadora o dispositivo móvil, sin la autorización o el conocimiento del usuario, el mismo se puede adquirir por diversos medios como, por ejemplo: correos electrónicos al ejecutar archivos adjuntos, instalación de aplicaciones, navegando en sitios riesgosos de internet, entre otros.
Los códigos maliciosos pueden tener varios objetivos tales como: mostrar publicidad, robar información personal, realizar ataques distribuidos, entre otros.

i. ¿Cómo me puedo proteger?

Seguidamente se citan algunas medidas de seguridad que se deben considerar, para aumentar el nivel de protección de su computadora y/o dispositivo móvil:

- **Actualizar el sistema operativo**

Mantener actualizado el sistema operativo de su computadora o dispositivo móvil, los proveedores de los sistemas operativos ponen a su disposición actualizaciones en línea que deben ser descargadas e instaladas, a fin de poder corregir las fallas y vulnerabilidades de los sistemas operativos. Un dispositivo correctamente actualizado está más protegido y tiene menos probabilidad de ser infectado.

- **Uso de Antivirus**

Un antivirus es un programa capaz de detectar la presencia de virus informático en una computadora y tomar acciones para su protección.

Para proteger la PC o dispositivo móvil cuando se navega en internet es necesario tener instalado un antivirus y mantenerlo actualizado, con el fin de estar al día con las últimas protecciones contra códigos maliciosos.

- **Uso de Antispyware**

El spyware es otro tipo de software malicioso, similar al virus, pero cuyo objetivo es recolectar información del usuario para luego generar ataques o realizar robo de información. Algunos antivirus no se encargan de este problema, porque no está dentro de la categoría de virus por lo cual se debe usar un software antispyware que proteja su computadora de este tipo de ataques.

- **Uso del Firewall (Pared de fuego),**

Un firewall, es un sistema que permite proteger la computadora de las intrusiones procedentes de Internet, el firewall permite filtrar los paquetes de datos que se intercambian entre su computadora con la red de internet.
Una buena práctica de seguridad es asegurarse de tener activo el Firewall del sistema operativo, sí su sistema operativo no cuenta con este sistema existen productos de terceros para este fin.