SEGURIDAD

CONSEJOS GENERALES

Conoce cómo funcionan los virus, phishing y navega con seguridad en internet.

1. NAVEGA CON SEGURIDAD

De cara a preservar la seguridad de las operaciones realizadas a través de la Banca Online, evite facilitar sus datos y claves personales fuera de las páginas seguras.

- Todas las direcciones de las páginas seguras de la Banca Online de Laboral Kutxa añaden la "s" de sitio seguro y comienzan por https://www.laboralkutxa.com
- Si va a utilizar datos o claves personales, compruebe la vigencia y titularidad de los certificados de sitio seguro de la página pinchando sobre la imagen del candado visible en la barra del navegador.
- Desconfíe de enlaces de acceso a la Banca Online insertados en e-mails o banners, si los utiliza asegúrese que le envían a la dirección correcta (https://www.laboralkutxa.com).
- Nunca desvele sus claves de seguridad y cámbielas periódicamente intentando evitar aquellas triviales o fácilmente deducibles.
- Borre la memoria caché de su ordenador, siempre que sea de uso compartido con otras personas o se encuentre en un sitio público.
- Finalice siempre su sesión de la Banca Online.
- Debe velar por la confidencialidad de sus claves protegiendo la seguridad de su PC. Para ello instale software antivirus en su equipo y manténgalo permanentemente activado, rechazando instalar software de procedencia desconocida o dudosa.

2.VIRUS

Los virus y el spyware son programas que se instalan en el ordenador, con fines maliciosos.
Para evitar las posibles infecciones de virus es conveniente:

- Disponer de un software antivirus actualizado (debe actualizarse periódicamente, no es suficiente que sea más o menos nuevo).
- Verificar los documentos que se han recibido del exterior (vía correo electrónico) con el antivirus.
- Ejecutar sólo aquellos programas de los que tengamos garantía de origen y que no vulneren la propiedad intelectual.

También es muy importante saber que un antivirus puede fallar por dos motivos, puede no detectar un virus porque es diferente de los que conoce, pero también puede detectar como virus un programa inofensivo.
Medidas antivirus para correo electrónico
El correo electrónico es una de las vías más importantes de transmisión de virus, ya que no garantiza el origen del envío, lo que conlleva algunos riesgos inherentes, como que terceros puedan acceder al contenido del correo, que se suplante el remitente o que se envíe el virus.
Para correr los mínimos riesgos posibles cuando lo utilizamos es recomendable:

- No ejecutar directamente los ficheros anexos, es mucho más seguro extraerlos previamente a un directorio del ordenador.
- En caso de recibir correos no solicitados, es recomendable confirmar el envío con el remitente o borrar el mensaje directamente. No debe abrirse nunca, aunque proceda de un remitente conocido.
- No participar en mensajes en cadena.

3. PHISHING

El phishing es una estafa que consiste en suplantar la identidad de una empresa, normalmente una entidad financiera, para conseguir información confidencial de los clientes así como sus claves de acceso.

CÓMO ACTÚA:

- Los ataques se producen mediante correos electrónicos engañosos en los que se suplanta la identidad de la entidad.
- Los correos redirigen a una web fraudulenta que imita el aspecto de la página original. En esta página, se solicita a los usuarios la introducción sus datos y claves personales, como son su número de tarjeta, PIN o claves de acceso.
- Los correos electrónicos fraudulentos tratan de conseguir su información personal. "Laboral Kutxa" nunca le solicitará por correo ninguna información referente a sus usuarios, claves o datos de su tarjeta de crédito.
- La urgencia de los mensajes que le amenazan con la suspensión de la cuenta si no proporciona sus datos inmediatamente tiene que hacerte sospechar. "Laboral Kutxa" nunca usará el correo electrónico para contactar, por este motivo.
- Los errores ortográficos y otros errores en la realización del correo o la web fraudulentos indican un origen sospechoso de los mismos.

En caso de duda llame inmediatamente al Servicio de Atención al Cliente