FRAUDES BANCARIOS EN INTERNET

RECONOCIMIENTO, RECOMENDACIONES Y SOLUCIONES

Organizan:

FABZ

UCARAGÓN
Unión de Consumidores de Aragón

Colabora:

GOBIERNO DE ARAGON

A día de hoy, Internet se ha convertido en un vehículo de trabajo, comunicación, intercambio, información y entretenimiento, habitual y accesible para cualquier ciudadano, convirtiéndose así en una prácticamente imprescindible herramienta que, como tal, tiene sus ventajas y sus inconvenientes.

Como avance tecnológico, sus aportaciones son incuestionables y facilitan nuestra vida, pero, al mismo tiempo, se ha abierto una nueva puerta a la comisión de delitos por parte de actores invisibles cuyo objetivo va a ser cualquier navegante de la red. Debemos estar preparados y prevenidos, conociendo cómo hemos de proceder ante cualquier posible ataque del que podamos ser víctimas.

¿QUÉ BUSCAN QUIENES AMENAZAN NUESTRA SEGURIDAD EN INTERNET?

Engañarnos y manipularnos para inducirnos a ejecutar acciones que pondrán en peligro:

- Datos personales.
- Información bancaria, tarjetas, números de cuenta, contraseñas.
- Contactos, correos electrónicos, teléfonos.

¿QUÉ MEDIOS UTILIZAN PARA VULNERAR EL USO SEGURO DE LA RED?

Correo Electrónico - Es el más frecuente. El remitente suplanta una identidad legítima. Para detectar un correo malicioso debemos fijarnos en los siguientes puntos, pudiendo confluir uno, varios o todos:

Remitente del correo

· Suele ser una empresa, entidad bancaria o entidad (pública o privada) conocida y visitada y/o utilizada con asiduidad general.
· Relativamente eficaz, pues alos atacantes pueden haber usado el dominio auténtico del suplantado.

Mensaje, su forma y contenido

· Capta nuestra atención con avisos de urgencia o propuestas atractivas.
· Suele utilizar formas genéricas para dirigirse a nosotros, como "Estimado cliente". No personalizan.
· Los errores ortográficos y gramaticales son frecuentes.
· Incluye enlaces que suelen redireccionarnos a un sitio web fraudulento.
· Adjuntan archivos que, una vez descargados y ejecutados, instalan virus.

SMS - Difícil de rastrear, suele incluir un enlace fraudulento.
Llamadas telefónicas - Persiguen información privada.
Redes sociales - Ofrecen cupones descuento, juegos y concursos en los que puedes ganar algo.

¿CÓMO PODEMOS RECONOCER SI UNA PÁGINA WEB ES SEGURA?

Comprobar el tipo de Protocolo que aparece al principio de la dirección: HTTP o **HTTPS**. El protocolo HTTPS garantiza que la comunicación no se podrá manipular y que la información personal y privada estará protegida.

Certificado de Seguridad. Expedido por una autoridad de certificación, nos indica que es una página legítima.

Sello de Confianza. Acredita que esa web ha sido revisada por un tercero que la valida conforme a un Código de buenas prácticas.av

RECOMENDACIONES

- Comprobar las formas de pago:
  · **Seguras:**
  Plataformas de pago (PayPal), contra reembolso, pago con el móvil.
  · **Menos seguras pero respaldadas**:
  Tarjeta de crédito, débito o prepago, transferencia bancaria (salvo al extranjero o vendedor fraudulento).
  · **Poco seguras:**
  Transferencia instantánea (Western Union).
- Nunca responder a un correo o SMS.
- No compartir información.
- Utilizar antivirus y mantenerlo actualizado.
- Cambiar con frecuencia las contraseñas utilizadas.
- Nunca descargar archivos adjuntos si otras señales nos indican posible actividad fraudulenta.
- Nunca hacer clic en los enlaces de correos sospechosos.
- En caso de ser víctimas de un fraude y, según proceda, contactar con la entidad bancaria, cambiar contraseñas, recopilar información para interponer denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado, línea 017 del INCIBE (Instituto Nacional de Ciberseguridad).
- Una entidad bancaria jamás nos solicitará a través de un correo electrónico o SMS que le facilitemos claves, contraseñas, números de cuenta o tarjeta o cualquier otro dato personal.
- Detectado el correo fraudulento, eliminarlo y bloquear al remitente. Vaciar la papelera con regularidad.
- Poner el cursor sin hacer clic sobre un enlace y compararlo con la que sería la dirección legítima del remitente, localizada en otra página del navegador.