- **Smishing**: Es una técnica de ingeniería social que se realiza a través de mensajes de texto SMS. Normalmente estos mensajes piden a la víctima que realicen una acción inmediata mediante enlaces o números de teléfono. Estos enlaces están vinculados a acciones maliciosas para acceder a tus datos personales como pasa en los casos anteriores. (Álvaro Melero)
- **Sextorsión:** Es la técnica de ingeniería social en la cual se chantajea a los usuarios con publicar contenidos comprometidos y si no acceden a darles lo que pidan normalmente es a cambio de dinero. El acceso a los datos puede ser real o a veces se amenaza, aunque no hayan tenido acceso a estos datos. (Lucia García)

- **Vishing**: Consiste en llamadas de supuestas empresas donde se piden los datos de acceso. Un claro ejemplo pueden ser las supuestas llamadas de Microsoft para activar Windows. Lo que nos piden es que les facilitemos nuestros datos personales como nuestro número de teléfono, nuestro email, el número de la tarjeta bancaria, el NIP del cajero automático y el código de seguridad. A cambio de eso nos prometen que nuestros datos estarán guardados de una forma segura. (Juan José Pajuelo y Alejandro Baruque)

  Phishing: Es una técnica de ingeniería social que consiste en enviar un correo a miles de personas intentando parecerse a una entidad. Este correo tiene como fin acceder a los datos de alguna persona como puede ser sus credenciales bancarias. Ejemplo de Phishing: Un hacker formula un correo estándar de un cobro en la cuenta del Banco Santander, en este correo nos hace saber que es un cobro alto y que tenemos 24h para parar esa transacción. Por último, añadirá un enlace que te lleva a una página creada por él que se parece a la oficial. (Liam Merchán)

- **Baiting**: Se utiliza un dispositivo de almacenamiento infectado el cual se deja en un lugar fácil de encontrar. Cuando una persona lo encuentre y lo introduzca en su ordenador, inmediatamente un software malicioso se instalará y permitirá a una tercera persona el acceso a los datos personales. (Juan José Pajuelo)
- **Spam**: Es una técnica de ingeniería social muy antigua y se basa en el envío masivo de correos(e-mails) a tu bandeja de entrada. Hay casos en los cuales se trata de una estafa para obtener datos personales y financieros, en otras ocasiones son solo mensajes de publicidad. Hoy en día muchos servidores de correo electrónico revisan los mensajes automáticamente en busca de “spam malicioso” pero es 100% efectivo y puede acabar llegando a nuestra bandeja de entrada. (Alejandro Cano)

- **Pretexting**: Consiste en crear elaborar un escenario o historia ficticia, donde el atacante tratará que su víctima comparta información que, en circunstancias normales, no revelaría. (Sergio Otero)