Análisis

Jaime **Delgado**
CATEDRÁTICO DE LA UPC

Hay soluciones, pero no se aplican

Para atajar el problema hay que cambiar el funcionamiento, lo que supone cambiar el modelo de negocio

guiente nivel de problemas es cuando alguien quiere perjudicar a otro públicamente y sin esconderse. Un insulto, una difamación, descubrir algo secreto o íntimo, lo puede hacer cualquier conocido. Si lo hace a través de una red social, el efecto maligno se multiplica llegando rápidamente a todos sus *amigos*. Luego está la credibilidad de lo divulgado, pero esta es otra cuestión. El primer daño puede estar hecho.

Pasemos ahora a los ataques encubiertos, es decir, aquellos en los que el atacante intenta esconderse. De entre todos los posibles, concentrémonos en la suplantación de personalidad. Esta puede hacerse básicamente de dos maneras. En la primera, el suplantador accede a una cuenta existente de otra persona y, haciendo creer a los demás que es el suplantado, publica información o vierte comentarios para dañarle. El mecanismo que use el suplantador para obtener acceso a la cuenta es otro tema, pero hay muchas formas de *robar* (o perder por descuido) una contraseña, que es básicamente lo único que se necesita.

La segunda manera de llevar a cabo una suplantación requiere que la víctima no tenga cuenta en la red social donde se comete el ataque. Cualquiera puede darse de alta tomando otra personalidad, que puede ser la de una persona que existe. Lamentablemente, en este caso (en aras de simplificar el acceso), los proveedores de redes no verifican los datos cuando un usuario se da de alta.

Recursos tecnológicos

La última cuestión es esta: ¿qué puede hacer la tecnología para evitar estos problemas? La realidad es que la tecnología ya dispone de soluciones, pero el problema es que para aplicarlas se deben cambiar los modelos de funcionamiento, que implican cambios de modelo de negocio en los proveedores y cambios de comportamiento en los usuarios, lo que no siempre es fácil.