Privacidad y Seguridad en las Redes Sociales

VS

Introducción

Gran crecimiento de las redes sociales.

Ventajas de las redes sociales

- Comunicación con amigos lejanos.
- Recuperar amistades del colegio o instituto.
- Sociabilidad
- Fácil de usar y comunicarse con los demás.
- Interfaz amigable con el usuario

Desventajas de las redes sociales

- La privacidad en ocasiones puede quedar en entredicho.
- La seguridad, no sólo los grandes agujeros de seguridad de los portales, sino la filtración de los datos personales.
- Posible atacantes por la información tan «jugosa» que hay en las redes sociales.

Problema: Sociabilidad y usabilidad VS privacidad y seguridad

¿cuáles deberían ser los objetivos de los diseños de seguridad y privacidad?.

Cuando tratamos la seguridad y la privacidad, entramos en el conflicto.

Seguridad y Privacidad VS Sociabilidad y usabilidad

Debe haber un equilibro entre ellas

Principales funcionalidades de las redes sociales

Comunicación con nuestros amigos y conocidos.

Una red social es la representación digital de sus usuarios y sus relaciones sociales.

¿Qué nos proporciona la red social?

Crearnos un perfil de nosotros mismos.

Mejorar la comunicación entre estos perfiles (nosotros)

Permiten modificar o incluso eliminar el perfil de la red social.

Administrar la lista de nuestros contactos. Agregar y quitar.

Grupos de personas. Amigos o trabajo. Permisos diferentes a cada uno de ellos.

Fotos, vídeos, juegos, aplicaciones de terceros para sacar el máximo partido a todas las opciones (programas Twitter), comentarios en los tablones de una forma pública (a todos los contactos).

Comunicación privada: mensajes privados que sólo podrá leer una persona.

Chat: conversaciones en tiempo real (como messenger).

Búsqueda de perfiles (personas)

Las redes sociales no sólo se limitan a mantener las relaciones existentes, sino también agregar personas y a eliminarlas.

Dos formas para la búsqueda:

Búsqueda global: podemos hacer una búsqueda por toda la red social, acotando parámetros como el nombre, edad, sexo, colegio, aficiones etc. Se nos presentará un listado de gente coincidente y por la foto del perfil (o más datos si lo tiene abierto) podremos decidir si esa es la persona que estábamos buscando.

Cruce social: también podemos ver los amigos que nuestros contactos tienen agregados (si tienen los permisos necesarios activados) y así decidir si es la persona que estábamos buscando o si nos hemos equivocado.

Un usuario puede restringir a los demás que vean sus contactos agregados, aunque esto quita sociabilidad (a cambio de una mayor privacidad), como podéis ver el conflicto privacidad VS sociabilidad está en todos los aspectos.

También podemos tener los perfiles abiertos, a la vista de todos. Esto potencia la sociabilidad porque podremos ver toda su información sin necesidad de que nos agregue. La privacidad será nula.

Arquitectura de las redes sociales

Cliente-servidor:

Red centralizada.

Almacenamiento de los datos en los servidores centrales.

Acceso a los servicios en la propia web de la red social.

Peer-To-Peer:

Posibilidad para ser la siguiente generación de redes sociales.

Esquema descentralizado, cada usuario sería su propio servidor.

Intercambio directo de información.

Almacenamiento en nodos.

Proximidad geográfica para proporcionar servicios sin necesidad de internet.

Problema: búsqueda global.

Privacidad y seguridad en las redes sociales

Principales estándares de seguridad en internet:

Confidencialidad: requiere que la información sea accesible únicamente a las entidades autorizadas. Es de vital importancia en las redes sociales porque un mal uso de la información podría traer graves consecuencias en la vida de las personas.

Integridad (requiere que la información sólo sea modificada por las entidades autorizadas).

Disponibilidad (requiere que los recursos del sistema estén siempre disponibles).

No repudio (ofrecer protección a un usuario frente a otro que niegue posteriormente que realizó cierta comunicación).

Proteger los datos privados de los usuarios.

La intimidad en el contexto de las redes sociales

Anonimato de la identidad del usuario

Algunas redes no nos permiten ser anónimos, nos obligan a poner nuestros nombres reales, sin embargo hay otras en las que podemos poner seudónimos.

Si usamos nuestro nombre, ayudaremos a potenciar la sociabilidad para que la gente nos encuentre más rápido.

Privacidad del espacio personal

Visibilidad del perfil.

Permisos para ver ese perfil.

Listas de amigos (personas agregadas).

Privacidad de la comunicación del usuario

Datos adicionales: tiempo de acceso, fecha y hora de acceso, dirección IP, historial de acciones deben ser también privados.

Tipos de ataques a las redes sociales

Robo de identidad

Un atacante se puede hacer pasar por otra persona o por varias personas. Podrá perjudicar tanto a los usuarios como a la propia red social ya que la gente podría dejar de usarlas si esto no se controla. En ocasiones piden DNI para la identificación (Tuenti).

Mala conducta

Algunas redes sociales son usadas por empresas y la mala conducta no debe estar presente.

Atacantes internos: están registrados en la red social y actúan de manera maliciosa.

Atacantes externos: intrusos, ataques a la infraestructura, DoS.

Conflicto del diseño

Seguridad y privacidad VS sociabilidad y usabilidad

Búsqueda social global: perfiles abiertos o cerrados (conflicto)

Búsqueda social transversal: abierto o cerrado (conflicto).

Minería de datos VS Privacidad

La ingente cantidad de datos son importante fuente para el análisis social.

Los datos pueden servir para mejorar la red social.

Privacidad y que no recojan los datos VS mejorar la red social mirando los comentarios de los usuarios.

Arquitectura cliente-servidor

Ventajas:

- Búsqueda glogal rápida.
- Búsqueda transversal
- Minería de datos más eficaz.
- Almacenamiento en sus propios servidores y siempre online.

Desventajas:

- Intrusión en las redes y robo de datos
- Modificar datos por piratas informáticos.
- Pueden compartir información personal sin nuestro consentimiento.
- Las fotos quedan almacenados y no se borran si das de baja tu perfil (Facebook).
- Servidor centralizado propenso a ataques DoS.
- Cambio de las condiciones de uso del servicio.

Arquitectura P2P

Ventajas: Seguridad reforzada por estar descentralizado, Almacenamiento de datos por los propios usuarios, Mayor privacidad, Posibilidad de cifrar los datos sin necesitar a terceros.

Desventajas: Búsqueda global y transversal difícil, la sociabilidad disminuye

Direcciones de investigación

Introducir un término medio en las relaciones sociales. No sólo puede haber dos opciones: permisos totales o sin permisos. Debe haber un punto intermedio.

Incluir tipos de relaciones (personal, trabajo etc), la confianza y la cantidad de interacciones (cantidad y calidad de los comentarios) con los distintos usuarios para asignarles más permisos o menos.

Creaciones de grupos (amigos, compañeros, trabajo) para evitar confusiones. Facebook ya lo implementa.

Proteger los grafos sociales

La información recogida en la red social debe ser protegida.

Las relaciones entre los distintos perfiles ayudan a proteger la red social de intrusos.

Facilidad de un usuario malintencionado crearse perfiles falsos. Solución: pedir identificación.

Usar la red de relaciones de la vida real para comprobar que alguien es quien dice ser.

Aunque es fácil cambiarse el nombre en la red, no podrás ocultar tus relaciones con los amigos agregados.

Es difícil que alguien no se de cuenta de que un «amigo» no es quien dice ser.

Conclusiones

Debemos mitigar los conflictos de diseño. Seguridad y privacidad VS usabilidad y sociabilidad.

Las autoridades competentes también deben actuar. Como la LOPD en España, para garantizar la seguridad de los datos.

Los usuarios deben ser conscientes de que cualquier comentario puede afectar negativamente a la vida real. Como comentarios del trabajo.

La seguridad y la privacidad en las redes sociales comienza por nosotros mismos.