

PRIVACIDAD EN REDES SOCIALES

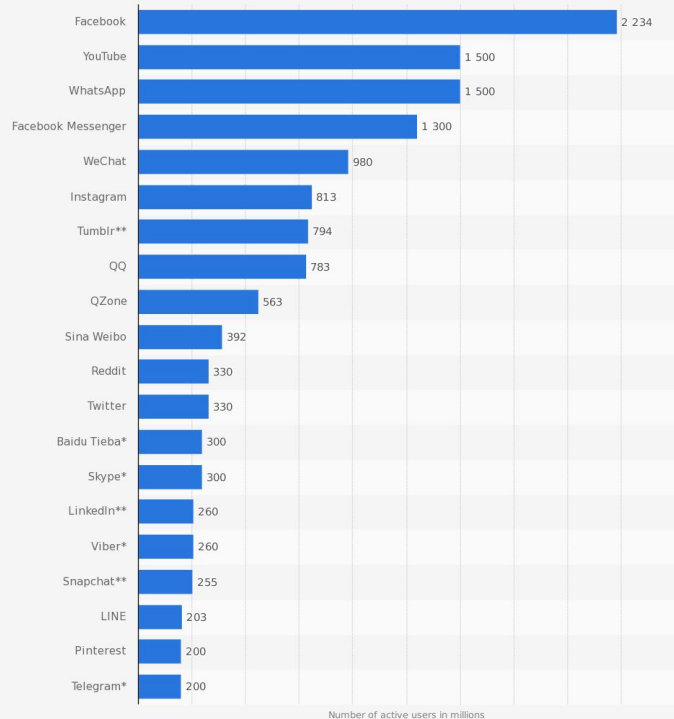
LO QUE NO TE ESTÁN CONTANDO

PARTE I



INTRODUCCIÓN

Most popular social networks worldwide as of April 2018, ranked by number of active users (in millions)



Sources

We Are Social; Kepios; SimilarWeb; TechCrunch; Apptopia; Fortune © Statista 2018

Additional information:

Worldwide; We Are Social; SimilarWeb; TechCrunch; Apptopia; Fortune; Fortune; as of April 12, 2018; social network app/volp included

LAS REDES SOCIALES SON LA HERRAMIENTA DE OCIO MÁS UTILIZADA ACTUALMENTE. POR ELLO, ES IMPORTANTE QUE CONOZCAMOS LA RESPUESTA A ESTAS DOS PREGUNTAS:

¿QUÉ CONOCEN DE NOSOTROS Y CÓMO UTILIZAN ESA INFORMACIÓN?

¿A QUÉ ACTIVIDADES DE RIESGO NOS EXPONEN Y CÓMO SOBRELLEVARLAS?

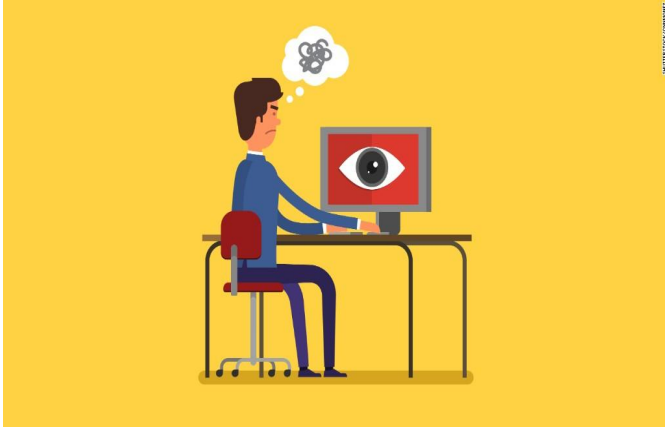
NUESTROS DATOS Y LAS REDES SOCIALES



LA PRIVACIDAD EN INTERNET
GOOGLE
FACEBOOK
WHATSAPP



LA PRIVACIDAD EN INTERNET



AL NAVEGAR POR INTERNET, CEDEMOS NUESTROS DATOS, DE FORMA INCONSCIENTE, A EMPRESAS Y PRESTADORES DE SERVICIOS. POR MEDIO DE LAS COOKIES, UNOS MICROPROGRAMAS QUE DESCARGAMOS AL ENTRAR EN LA WEB, DATOS COMO NUESTRA DIRECCIÓN IP , EL TIEMPO QUE DURA NUESTRA CONSULTA A LA WEB E INFORMACIÓN DE SITIOS QUE ESTEMOS VISITANDO AL MISMO TIEMPO, SON RECABADOS Y EMPLEADOS POR LA EMPRESA PARA INFERIR INFORMACIÓN SOBRE NOSOTROS:

- ¿SOMOS VISITANTES HABITUALES?
- ¿QUÉ USO HACEMOS DE DICHA WEB?
- ¿EN QUÉ SECUENCIA Y CÓMO ACCEDEMOS A OTRAS WEBS?

LA PRIVACIDAD EN INTERNET

PRÁCTICAS HABITUALES:

- EMPRESAS PAGAN A LA WEB PARA INSTALAR SUS PROPIAS COOKIES
- EL PROPIETARIO DE LA WEB VENDE NUESTROS DATOS A TERCEROS



LA PRIVACIDAD EN INTERNET



MICROTARGETING: METODOLOGÍA DE LA MERCADOTECNIA QUE TIENE COMO OBJETIVO INFLUIR EN LAS DECISIONES DEL CLIENTE, POR MEDIO DE LA GESTIÓN DE GRANDES CANTIDADES DE DATOS EN LOS QUE SE BUSCA EXTRAER PATRONES MEDIANTE CRITERIOS DE SELECCIÓN COMO INTERESES, HÁBITOS, SITUACIÓN SOCIOECONÓMICA, ETC.

GOOGLE

¿QUÉ DATOS ALMACENA?

UBICACIÓN



HISTORIAL DE BÚSQUEDA



INFORMACIÓN PERSONAL

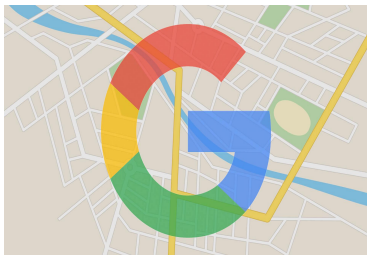


GOOGLE

¿EN QUÉ EMPLEA NUESTROS DATOS?

MEJORA DE PRODUCTOS

AGILIZACIÓN DE GOOGLE MAPS,
MEJORA DEL BUSCADOR O MOSTRAR LOS
MEJORES VÍDEOS DE YOUTUBE.



SEGURIDAD

GMAIL Y SU FILTRO ANTI SPAM.



ANUNCIOS

SE BASA EN EL HISTORIAL DE BÚSQUEDA
PARA MOSTRAR LOS ANUNCIOS QUE
MÁS SE AJUSTAN A LOS GUSTOS DEL
USUARIO.



FACEBOOK

¿QUÉ DATOS ALMACENA?

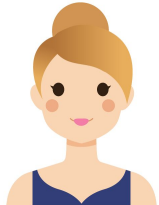
DATOS PERSONALES

NOMBRE

CORREO ELECTRÓNICO

NÚMERO DE TELÉFONO

INFORMACIÓN ADICIONAL



GUSTOS Y HÁBITOS

REACCIÓN A PUBLICACIONES

HORAS DE CONEXIÓN

BÚSQUEDAS EN EL BUSCADOR

RELACIONES CON OTRAS
PERSONAS

HERRAMIENTAS UTILIZADAS



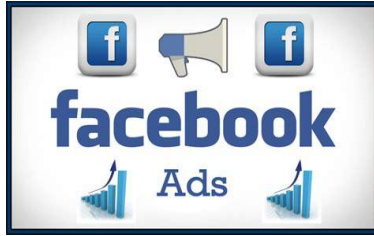
INFORMACIÓN COMPARTIDA

LA APD HA MULTADO RECIENTEMENTE
A FACEBOOK POR COMPARTIR DATOS
ENTRE FACEBOOK Y WHATSAPP: SECCIÓN
DE "PERSONAS QUE QUIZÁ CONOZCAS".



FACEBOOK

¿EN QUÉ EMPLEA NUESTROS DATOS?



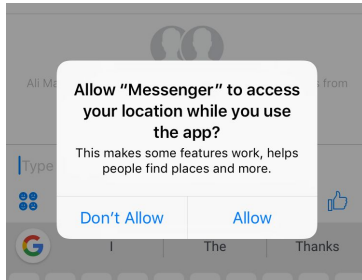
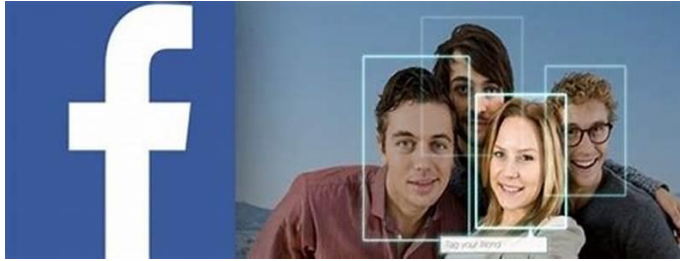
FACEBOOK DA ACCESO A MÁS DE 2000 MILLONES DE USUARIOS:

- EMPRESAS SE PROMOCIONAN A TRAVÉS DE POSTS DIRIGIDOS A PERFILES DE USUARIO A LOS QUE ESTÁN INTERESADOS EN VENDER.
- FACEBOOK PROPORCIONA ACCESO A OTRAS APLICACIONES, CEDIÉNDOLES LOS DATOS CUANDO SE AUTORIZA DICHO ACCESO.



FACEBOOK

¿EN QUÉ EMPLEA NUESTROS DATOS?



- SI SE USA FACEBOOK DESDE UN TELÉFONO, PUEDE ACCEDER A LA UBICACIÓN SI SE TIENE EL GPS ACTIVADO.
- INSTALADO EN UN MÓVIL, SABE QUÉ APLICACIONES SE TIENEN INSTALADAS EN ÉL.
- INFERENCIA DE INFORMACIÓN ADICIONAL A TRAVÉS DE UN SISTEMA DE RECONOCIMIENTO DE IMÁGENES QUE ANALIZA LOS METADATOS (LUGAR, HORA, ETC).

WHATSAPP



¿QUÉ DATOS ALMACENA?

UBICACIÓN

HORA DE CONEXIÓN

METADATOS

HORA A LA QUE ENVÍA MENSAJES
A OTROS USUARIOS

¿DÓNDE SE ALMACENAN?

LOS DATOS SE ALMACENAN EN SERVIDORES
FÍSICOS.



PRIVACY SHIELD

AL COMUNICARNOS POR WHATSAPP, SE PRODUCE
UNA TRANSFERENCIA INTERNACIONAL DE DATOS.
PARA QUE SE HAGA DE FORMA SEGURA, LA
APLICACIÓN TIENE QUE SER APROBADA POR LA APD.
PARA ELLO, FUE CREADO EL PRIVACY SHIELD, QUE
WHATSAPP NO CUMPLE.

PRIVACIDAD EN REDES SOCIALES

LO QUE NO TE ESTÁN CONTANDO

PARTE II



ACTIVIDADES DE RIESGO EN REDES SOCIALES

SEXTING

GROOMING

CIBERBULLYING

HACKING

PHISHING

ES NECESARIO CONOCER EL SIGNIFICADO Y LOS RIESGOS DE ESTAS ACTIVIDADES

SEXTING



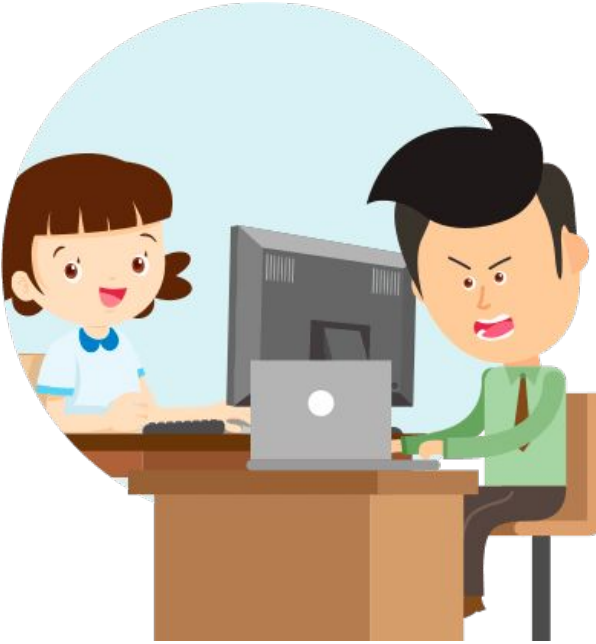
CONSISTE EN EL ENVÍO DE MENSAJES CON CONTENIDO PORNOGRÁFICO A TRAVÉS DE REDES SOCIALES.

EL PRINCIPAL PELIGRO ESTÁ EN LA POSIBILIDAD DE QUE ESA FOTO SEA OBTENIDA POR TERCEROS.

TAMBIÉN PUEDE LLEVAR A SITUACIONES EMBARAZOSAS.

ES IMPORTANTE CONOCER AL DESTINATARIO DE LOS MENSAJES ANTES DE ENVIARLO PARA EVITAR ALGUNOS DE ESTOS PELIGROS

GROOMING



ES UN CONJUNTO DE CONDUCTAS Y ACCIONES DELIBERADAMENTE EMPRENDIDAS POR UN ADULTO CON EL OBJETIVO DE GANARSE LA CONFIANZA DE UN MENOR DE EDAD CREANDO UNA CONEXIÓN EMOCIONAL CON EL MISMO CON EL FIN DE DISMINUIR SUS INHIBICIONES Y PODER ABUSAR DE ÉL.

CIBERBULLYING



TAMBIÉN DENOMINADO ACOSO VIRTUAL, SE REALIZA A TRAVÉS DE REDES SOCIALES O MEDIOS DE COMUNICACIÓN DIGITALES PARA ACOSAR A UNA PERSONA MEDIANTE ATAQUES PERSONALES Y/O DIVULGACIÓN DE INFORMACIÓN CONFIDENCIAL O FALSA ENTRE OTRO MEDIOS. IMPLICA UN DAÑO RECURRENTE Y REPETITIVO INFLIGIDO A TRAVÉS DE LOS MEDIOS ELECTRÓNICOS

HACKING



EN TÉRMINOS GENERALES EL HACKING INCLUYE ACTIVIDADES ORIENTADAS A ROMPER LA SEGURIDAD DE ORDENADORES Y/O SERVIDORES.

EN EL CASO DE HACKING DE REDES SOCIALES CONSISTE EN HACERSE CON LA INFORMACIÓN ENTREGADA POR LOS USUARIOS EN SUS PERFILES DE REDES SOCIALES, POR LO QUE UNA DE LAS MEDIDAS DE SEGURIDAD MÁS IMPORTANTES ES CONTROLAR QUÉ Y CUÁNTO SE COMPARTE EN ELLAS.

LOS HACKERS CLONAN PERFILES DE FACEBOOK O TWITTER Y DISEÑAN JUEGOS O PASATIEMPOS CON EL FIN DE HACERSE CON MÁS INFORMACIÓN E INCLUSO CONTRASEÑAS.

PHISHING



ES UN MÉTODO QUE LOS CIBERDELINCUENTES UTILIZAN PARA ENGAÑAR A LAS VÍCTIMAS Y CONSEGUIR QUE REVELEN INFORMACIÓN PERSONAL, COMO CONTRASEÑAS O DATOS DE TARJETAS DE CRÉDITO Y DE LA SEGURIDAD SOCIAL Y NÚMEROS DE CUENTAS BANCARIAS.

GENERALMENTE LOS DELINCUENTES SE HACEN PASAR POR OTRAS PERSONAS O ENTIDADES (COMO BANCOS) POR MEDIO DE MENSAJES DE CORREO ELECTRÓNICO U OTRAS REDES SOCIALES COMO FACEBOOK E INTENTAN QUE PAREZCA UNA COMUNICACIÓN CONFIABLE Y LEGÍTIMA Y EL USUARIO RESPONDA CON SUS CONTRASEÑAS E INFORMACIONES CONFIDENCIALES.

RECOMENDACIONES

CAMBIAR PERIÓDICAMENTE LA CONTRASEÑA.

UTILIZAR CONTRASEÑAS DE ACCESO DIFERENTES PARA CADA RED SOCIAL

ESTABLECER CONTRASEÑAS QUE NO SEAN CORRELATIVAS O CON VARIANTES OBIAS UNAS DE OTRAS

EMPLEAR SIEMPRE LA PÁGINA OFICIAL DE CADA RED SOCIAL PARA ENTRAR EN ELLA, YA QUE CIRCULAN ACCESOS QUE SIMULAN SERLO PERO EN REALIDAD ESTÁN PENSADOS PARA HACERSE CON LA CONTRASEÑA

MUCHAS GRACIAS

