ANDORRA DIGITAL

ANC-AD
Agència Nacional de Ciberseguretat d'Andorra

AGÈNCIA NACIONAL DE CIBERSEGURETAT D'ANDORRA

CONSCIENCIACIÓ EN CIBERSEGURETAT

RISCOS I RECOMANACIONS A L'HORA DE FER SERVIR WHATSAPP

Abril 2024
Document d'ús públic

1. INTRODUCCIÓ BREU

La **MISSATGERIA INSTANTÀNIA** és flexible, fàcil de fer servir i les notificacions són pràcticament instantànies, per la qual cosa WhatsApp ha esdevingut un dels canals de comunicació més popular en l'àmbit personal i professional.

El gran nombre d'informació personal sensible que es comparteix cada dia a través d'aquesta plataforma, juntament amb l'escassa percepció de **RISC** que tenen els usuaris en relació amb els dispositius mòbils, ha fet que WhatsApp sigui un entorn molt atractiu per als intrusos i els ciberatacants.

Una de les **FEBLESES** més important que té aquesta plataforma és el **procés d'alta i de verificació dels usuaris**. Aquest procés pot arribar a propiciar que un intrús aconsegueixi el compte d'un usuari de WhatsApp, llegeixi els seus missatges i fins i tot enviï missatges en nom d'una altra persona.

I, finalment, una altra feblesa important d'aquesta aplicació és que fa poc s'ha descobert que WhatsApp **NO** elimina completament les converses que l'usuari ha esborrat.

2. RISCOS PRINCIPALS EN L'ÚS DE WHATSAPP

Un dels riscos principals de fer servir WhatsApp és que aquesta aplicació de missatgeria instantània **NO esborra totalment els xats**, malgrat que l'usuari els hagi esborrat.

Dels possibles **RISCOS** que tenim pel fet d'usar aquesta aplicació, en destaquem els següents:

1. Escassa seguretat en el moment de donar-se d'alta en aquesta aplicació. La mancança més important de la plataforma fins a aquest moment rau en el **procés d'alta i de verificació dels usuaris.** S'ha detectat que durant el procés un intrús pot apropiar-se del compte d'usuari de WhatsApp d'una altra persona, llegir els seus missatges o enviar-ne en nom d'un altre usuari.

2. Segrest de comptes de WhatsApp aprofitant errors en la xarxa. En el cas que un atacant aconsegueixi accedir a aquesta eina aprofitant un **error en la xarxa**, podria interceptar o enregistrar les trucades telefòniques, llegir missatges aliens, detectar la localització del dispositiu de l'usuari, etc. En aquest cas, per evitar això, es recomana que s'activi l'opció de **Mostrar notificacions de seguretat** a WhatsApp.

3. Eliminació insegura de xats. També es qualifica d'insegura l'**eliminació de les converses /xats**, atès que, en versions més antigues, ja s'utilitzaven tècniques forenses per obtenir els registres de les converses. Com a mesura preventiva, es recomana **desinstal·lar l'aplicació i tornar-la a instal·lar** per esborrar de manera segura les converses, malgrat que aquest procés NO elimina les possibles **còpies de seguretat** que s'hagin pogut fer al núvol.

4. Difusió d'informació delicada durant la connexió inicial. Si es difon informació delicada a través d'aquesta aplicació, tant la versió de l'aplicació que s'estigui fent servir com el número de telèfon de l'usuari registrat durant la connexió inicial poden quedar exposats davant de qualsevol atacant en cas que s'utilitzin **xarxes wifi públiques o de dubtosa procedència**. L'única manera de resoldre aquest problema és que s'empri una **connexió VPN** per enviar informació delicada.

5. Riscos de descarregar-se aquesta aplicació en llocs no oficials. És perillós descarregar WhatsApp en **llocs no oficials**, atès que els ciberdelinqüents ho poden aprofitar per cometre fraus.

6. Atacs de pesca en el web de WhatsApp. Fer servir aquesta aplicació a través de la seva pàgina web també implica el risc que un atacant pugui **monitorar un codi QR del web oficial** i quan l'usuari se subscrivís a alguna promoció, estaria autoritzant l'accés web des de la seva sessió de WhatsApp.

7. Furt de comptes mitjançant SMS o trucada telefònica. També es poden robar comptes mitjançant SMS, trucades de telèfon o accés físic. El robatori mitjançant SMS està relacionat amb **el sistema de registre de l'aplicació** (un atacant podria utilitzar un telèfon propi o un emulador de terminal i començar el procés de registre amb el número de la víctima, com si es tractés d'un canvi de terminal). També es pot segrestar una sessió de WhatsApp fent servir l'opció de **verificació per trucada telefònica**.

8. Pèrdua del terminal de telèfon. Una persona amb accés físic a un telèfon pot segrestar la sessió de WhatsApp d'una manera molt senzilla. El problema d'això rau en la dificultat per evitar-ho, atès que no existeix cap opció, ni per a Android ni per a iPhone, que obligui l'usuari a desbloquejar el seu telèfon per poder respondre a la trucada, per la qual cosa un atacant amb accés físic al telèfon pot respondre i completar l'atac.

9. Emmagatzematge de la informació a la base de dades. WhatsApp utilitza **SQLite** per emmagatzemar els xats, els fitxers i els missatges a la base de dades, per la qual cosa si un atacant aconseguís obtenir aquest fitxer, podria accedir a totes les converses i les dades privades de l'usuari.

9. Intercanvi de dades entre WhatsApp i Facebook. Altres riscos que s'han detectat deriven de l'**intercanvi de dades personals amb Facebook,** ja que WhatsApp transfereix les dades dels seus usuaris a Facebook i a la resta d'empreses que té el grup per a altres tipus d'activitats. Malgrat que no comparteix els missatges, les fotos i la informació del perfil, sí que pot intercanviar informacions com, per exemple, el número de telèfon de l'usuari, els seus contactes telefònics o l'hora de la darrera connexió.

3. RECOMANACIONS D'ÚS DE WHATSAPP

RECOMANACIONS

WhatsApp és l'aplicació de missatgeria instantània més coneguda i més important del món. És tan popular que fins i tot la fa servir la **gent gran**, fet que té un impacte molt positiu en la majoria dels casos (afavoreix la socialització de les persones grans i que no quedin aïllades socialment).

Podem destacar les següents **RECOMANACIONS** d'ús:

1. Xats de grup a WhatsApp. És recomanable mantenir cert ordre en les converses.

2. Activa la verificació en dos passos per millorar la seguretat a l'hora d'usar aquesta aplicació. Els sistemes de verificació en dos passos representen una millora important pel que fa a la seguretat, atès que afegeixen una **capa extra de protecció** al nostre compte de WhatsApp.

3. Compte amb l'emmagatzematge, fer servir aquesta aplicació «embruta» el telèfon. És recomanable desactivar la descàrrega automàtica de continguts multimèdia al WhatsApp.

4. Comprova quins membres del grup han llegit els teus missatges amb la verificació de lectura.

5. Crea sons personalitzats per a alguns dels teus contactes més especials. Això ens permet saber si el missatge rebut és de la nostra parella, del nostre millor amic o, per contra, és d'un contacte menys rellevant.

RECOMANACIONS

6. Et destorben els grups de WhatsApp de què formes part? Si la resposta és que sí, el millor que pots fer és **silenciar les notificacions de forma permanent.** Per fer-ho, cal que entris al perfil del grup que vols silenciar, toca l'opció **Silenciar** i tria el temps que vols que duri aquest silenci.

7. Del teu WhatsApp al PC en segons i sense necessitat de fer servir cables.

8. Pots canviar la font del text per emfasitzar-lo, i hi pots incloure cursives, negretes o ratllats.

9. Exporta els xats que no vulguis perdre, però que tampoc els vulguis continuar tenint en el teu telèfon. Per fer-ho, el millor és que els exportis directament del xat en qüestió i te'ls enviïs al teu correu, per exemple.

10. Aprofita l'opció que hi ha ara d'enviar missatges i fotos d'una sola visualització o d'ús temporal. Aquest tipus de continguts tenen un gran valor en termes de privacitat, seguretat i protecció de la teva informació personal. Aquestes opcions et permeten crear missatges i fotos de WhatsApp que **només estan disponibles durant un temps determinat**. Un cop passat aquest temps, desapareixen sense que hagis de fer res més.

Avís Legal

Aquest document conté informació pública.

El seu objectiu és la conscienciació en ciberseguretat pels ciutadans, empreses i entitats d'Andorra.