

Kimtukunieam

Zugu



Guía básica de conceptos de Seguridad Digital

“No se trata de tener derecho a ser iguales, sino de tener igual derecho a ser diferentes.”

líder mapuche.

*Zugu no ta itrokom che nieael kiñe az
mogen, itro gey ta az che few mew
müli ñi rüf ta kom taiñ*

che trokigeael



Este manual fue desarrollado por
South Lighthouse

kiñe: tūfachi chillka küzawfi
South Lighthouse pigechi trokinche.



Con el apoyo de Internews

epu: kelluntukuy Internews



Autor: Andres Alaerkhon-Schiavi.
Arquitecto. Msc. Gerencia de
Proyectos

Meli: zewmafilu tūfa chi chillka ka koneltulu
zugu: Andres Alaerkhon-Schiavi. Arquitecto
Msc. wūnenkülechi troytun zugu mew.

Diseño e ilustraciones: Constanza
Figueroa. Diseñadora y dibujante
feminista

Kūla: Constanza Figueroa. azentukechi ke,
yenielu zomo ñi zuam.

Revisión de Contenidos: Carlos
Guerra. Experto en Seguridad Digital

Kechu: güneytufilu chumechi chillkantukulen
faw: Carlos Guerra. pepiluwlu tūfachike zugu
mew koneltulelu chillka mew.

Traducción: Pegeiypang Maripil
Maripil. Mujer mapuche pewenche

Kayu: rulpafilu mapuzugun mew tūfa chi
chillka. Pegeiypang Maripil Maripil. mapuche
pewenche zomo.



Introducción

¿Cuántas de nuestras interacciones sociales se realizan a través de aplicaciones de mensajería? ¿Cuán seguros debiéramos sentirnos? ¿Cuánto realmente sabemos acerca de las capacidades de los gobiernos para vulnerar nuestra privacidad? Algunos antecedentes en la región muestran intentos, exitosos o no, de utilizar tecnologías de vigilancia con fines ilícitos haciendo a un lado tanto ordenamientos jurídicos nacionales como estándares internacionales en el tema, vulnerando directamente a comunidades en severo riesgo.

Para formarnos un criterio sobre lo anterior, quizá debemos ir a la base de todo. ¿Qué es el internet y cómo funciona? ¿Qué es la telefonía móvil y cómo funciona? Primero, el “Internet” está formado por redes que se conectan entre sí a través de varias maneras. Cuando un equipo se conecta a Internet tiene acceso a esas vías de comunicación, y por lo tanto puede consultar y enviar información a cada uno de los equipos conectados en cualquier parte del mundo. Se puede acceder a Internet de diversas formas, un usuario particular accede desde su casa a través de un módem conectado a un proveedor de Internet, y también desde redes inalámbricas públicas o un teléfono celular. Todas estas interacciones dejan un rastro a través de nuestra dirección IP que es como el número de identidad de nuestro equipo dentro de la red de servicio a la que estamos conectados.

Por su parte, un teléfono celular es un dispositivo de comunicación inalámbrica que usa ondas de radio tanto para enviar información como para

Konünpan zugu.

Chumten chi taiñ zuguluwün taiñ kimüwün taiñ chumlen fantenmu tripakey “aplicaciones” chew amulgekey kiñe müfü az zugu. Kimiyin kam kimlayin taiñ tüng küleafel fey ta chi zugu mew. Chem am kimiyin taiñ güneytuñmageken taiñ chumeken fey ti chi pu az zugu mew, pu “gobierno” ta yamkelay fey ti chi zugu taiñ amulnieken fey mew. Fantenmu ta kimgey ñi tripaken ta inayegen ta che wezalkageael, fey mew wente ñi “ordenamiento Juridico” niechi pu wigka rupakey tūfachi zugu, chumte mülen kakerume azelkawün chumleafel fey ti che ñi az ka fey ti pu trawünche ñi felen.

Taiñ küme kima el tūfa chi zugu, müli taiñ kima el chew am llituy tūfa chi zugu. Chem am ta Internet ka chumечи am az küley ka tripakey fill antü. Chem am ta telefonía móvil pigechi zugu ka chem az niey, chumечи am tripakey. Fey ti chi Internetet nüwküley redes mew nüwkey tūfa chi pu redes müfü az mew. Kiñe equipo koneltuyim Internet mew puwkey fey ti chi pu amulkawe zugu, fey mew pey fillke zugu ka pepi amulüy zugu chew rume chew ñi pin amulal fey ti chi zugu, kañpüle ta amulafüy ñi zugu ka ñi inaramtun. Ka müley kiñe az chumечи am konal fey ti chi Internet mew kiñeke, ruka mew kiñe pichi maquina modem pigelu fey ti chi modem nüwküley kiñe trokiñ wülkelu ti internet ka müley fey ti chi redes inalámbrica pigelu kam teléfono mew chi . kom tūfa chi pu zugu elkeygün kiñe pūnon reke kiñe dirección IP pigey, fey ti chi dirección IP taiñ wigka run reke, welu tūfa mew taiñ teléfono mew inatuniegeyiñ taiñ chumeken fey ti chi redes mew.

Ka femuechi kiñe teléfono celular kiñe amulkawe zugu ka zugun Inalámbrica pigelu, fey nüwküley ka pūnekey fey ti chi

recibirla. Esta información puede ser tanto voz como datos digitalizados viajando a la velocidad de la luz. Puede ser absorbida y reflejada por objetos en la zona antes de llegar a la torre celular más cercana, que toma las señales de radio y las convierte en datos eléctricos. Muchos teléfonos inteligentes modernos además de la antena celular, también pueden tener antenas Wi-Fi, Bluetooth y / o GPS.

La fuerza de la señal recibida desde la torre celular se denomina “intensidad de la señal”, que comúnmente se indica mediante las “barras” en su teléfono. Una recepción deficiente (menos barras) normalmente indica una larga distancia y / o mucha interrupción de señal entre el teléfono celular y la torre celular. Cuando su teléfono celular tiene poca conectividad, transmite una señal más fuerte para conectarse a la torre y, como resultado, la batería se agota más rápido. Es por eso que una buena conectividad no solo reduce las llamadas caídas, sino que también ahorra batería.

Con todo esto es fácil caer en cuenta que los equipos de telefonía celular que usamos día a día se han convertido en herramientas de comunicación básica y omnipresente, usados no solo para hacer llamadas, sino también para acceder a internet y enviar mensajes a través de cualquiera de las aplicaciones destinadas para eso. Sin embargo, los teléfonos móviles, no fueron diseñados para asegurar privacidad al usuario, sus características básicas para proteger las comunicaciones son muy pobres, y nos exponen muy especialmente en el rastreo de nuestra localización. La infraestructura de telefonía móvil de forma involuntaria permite

Ondas de radio pigechi zugu, amulal zugu ka llowam zugu. Tüfa chi pu zugu amuafüy zugun mew kam wirintukun chillka mew fey amuy chumechi amukey pelon antü reke. Fey kimgaefüy ka pegeafüy kake Objetos mülelü petu ñi puwnon fey ti chi Torre celular zoy püchü tripa mülelu, fey ta nükey fey ti chi señales de radio pigelu fey rulpatukefi datos eléctricos mew. Epe kom pu we ke teléfono fantenmu mülelu pünekey fey ti chi antena celular welu ka pünekey fey ti chi antenas Wi-fi, Bluetooth kam GPS pigechi pu zugu.

Fey ti chi az señal llowgekulu torre celular me feypigey “Intensidad de la señal” fey ga pegengekey kiñe, epu barras mew teléfono mew, fey ti barras mew kimgakey mülen kam mülenun señal, kiñe barra niele fey müte mülenun ka kümenun señal kam alütripa mülen fey ti torre celular wülkelu señal ti teléfono mew. Taiñ teléfono püchü nieyim señal zoy newentu amukey ñi señal puwam torre mew, fey mew zoy müchay amukey ñi carga batería mew. Fey mew küme señal niele che küme tripay ti amulzugun ka zoy amuy antü mew ti carga batería.

Fey ta chi zugu mew ka chumechi amulen tüfa chi zugu fantenmu ti telefonía celular fantenmu fillantü ka itrokom mew ta müley ka miawi, zuamyagetuy taiñ kimüwküleal ka fill püle ka fillke zugu mew miawi, mütrümüwal ka püneael fey ti chi internet zugu, amulael kiñe wirin zugu fey ti chi azkan mülelu aplicaciones pigechi zugu mew. Welu fey ta chi pu teléfono móvil zewmagelay ñi kiñmagenoeal taiñ chumeken, fey ta chi kake che ñi kimnoael taiñ chumeken gelay fey ti malal reke, kom taiñ chumeken püz yawi reke fey mew kimüñmageyiñ chew taiñ miawken chew taiñ anülüwkülen. Fey ta chi pu telefonía móvil anülüwkülelu inchiñ taiñ pin

el rastreo de sus usuarios en la red, a través de:

- El número IMEI para saber en qué zona geográfica está el teléfono móvil.
- La tarjeta SIM (número de teléfono) para saber la identidad de la persona a la que está asociado ese número de teléfono.

A grandes rasgos, la tecnología, y en especial el internet tienen un alto grado de penetración en países del cono sur, incluyendo sectores rurales en donde poblaciones originarias hacen vida. Miembros de estas comunidades están usando estas tecnologías e insertándose en sus interacciones diarias para acceder al conocimiento, comunicarse y organizarse. Cabe mencionar el hecho de que durante los últimos años estas comunidades han estado en constante tensión, debido a ciertos intereses por parte de instituciones tanto públicas como privadas en cuanto al uso y explotación de sus territorios, existiendo múltiples precedentes de líderes y activistas víctimas de vigilancia de sus comunicaciones, que por razones geográficas y culturales se han mantenido aisladas del resto de la comunidad activista digital.

Debemos saber que, aunque pongas en práctica todas las recomendaciones de esta guía, tu información nunca estará 100% segura. Solo estarás disminuyendo la probabilidad de que algo malo suceda, por ello es conveniente que puedas realizar con regularidad una evaluación de las mismas y diseñar planes para su mitigación.

mew no, fantenmu kizuegün ta pepi kimi egün iñi am chumekey fey ta red mew fey ta kimi egün tüfa chi pu troy mew:

- Fey ti wirin rakikan IMEI pigelu kimam chem mapu mew mülen fey ti chi teléfono móvil.
- Fey ti chi tarjeta SIM (taiñ número de teléfono mew) kimael iney ta niefiel fey ti chi número de teléfono.

Kiñe epu troy mew fey ta chi tecnología zoyel fey ta chi internet rume konpay fey ta chi trokin mapu cono sur pigelu, ka femgechi fey ta chi mapu mew chew am mülelu pu mapu mew nüwküle chi che. Pu che mülelu fey ti chi üytün mapu mew ka femuechi pünenieyegün fey ta chi pu tecnología tañi zuguluwküleael egün kam kimüwküleal egün . ka femgechi fey ta chi pu che konkülekey kiñekew mew awükan zugu mew, mapu ñi zuam mew ka kake zugu mew, fey ta chi awükan küpaley fey ta chi pu institución pública pigelu kam privada fey ta awükapayal ta mapu uzamkapayal ta mapu apumpayal ta itrofill mogen, fey ta kimgey fey ta chi pu che eluwnolu ñi femgeael ta mapu fey may allmalltuniegeyegün, ka kimniegey ñi chumeken egün tañi mapu mew, ka alü mapu mülelu egün waria mew kam kara mew müte konyawkelayegün fey ta chi pu che kellu kelu digital zugu mew.

Müley taiñ kimael chumte kuñiwtulelmi kom tüfa chi pu troy zugu triapayal tüfa chi chillka mew tami zugu küme zapillkülelayay. Re zoy pichiken kuñiwtuleaymi rupanoael weza ke zugu tami mogen mew , fey mew müli tami güneytuafiel kom tüfa chi pu zugu ka kimnieael chumam tripale kiñe weza ke zugu.

Guía de contenidos

¿Para quién es este manual?

¿Para qué sirve?

¿Cómo se hizo?

- 1. Correo electrónico**
- 2. Contraseñas**
- 3. Autenticación de dos factores (2FA o doble paso)**
- 4. Aplicaciones maliciosas (Malware)**

- 5. Telefonía Móvil**
- 6. Mensajería segura**
 - A. Whatsapp**
 - B. Signal**
- 7. Phishing**
- 8. Protección de dispositivos**
- 9. Protección de Información en físico**

- 10. Protección en redes sociales**

Referencias de las web.

Chem zugu ñi wirintulen tūfa chi chillka mew.

iney gael tūfa chi chillka

chem zugu am azkonküley

chumgechi am zewmagey kam chillkantukugey

- 1. fey ta chi correo electrónico**
- 2. fey ta chi contraseña pigechi zugu**
- 3. epurume chi autenticación pigechi zugu**
- 4. fey ti chi pu wezalkake chi kam/ Aplicaciones Maliciosas pigelu (malware pigelu)**
- 5. fey ta chi Telefonía móvil**
- 6. fey ta chi mensajería segura pigechi zugu**
 - A. Whatsapp pigechi zugu**
 - B. fey ta chi signal zugu**
- 7. Phishin pigechi zugu**
- 8. fey ta chi Protección de dispositivo**
- 9. fey ta chi Protección de información físico, chew taiñ mülen**
- 10. Kuñiwtulen redes sociales mew.**

Fey ta chi referencias de la web pigechi zugu

Resumen:

El proyecto “Kimtukunieal zugu” es un manual de seguridad en comunicaciones digitales en la cual se establecen objetivos y procedimientos para garantizar y preservar la privacidad dentro de comunidades en riesgo de pueblos originarios en el cono sur. La intención es fortalecer a través del conocimiento a las organizaciones indígenas y afines de la región, generar un cambio de consciencia dentro de las comunidades indígenas a fin de que tomen posesión de su derecho a la privacidad, y recomendar las medidas que pueden tomar para evadir la potencial persecución y vigilancia a través de medios digitales.

Troytun zugu.

Tüfa chi proyecto kimtukunieal zugu kiñe chillka gey fey ta iñ kuñiwruküleael fey ta chi comunicaciones digital mew, fey ta mew wirintukuley chem zuam mew am tripay, chumechi am kuñiwrukülefel fey ta chi pu che lof mew tuwlu , mapu mew nüwkülelu, fey ta chi cono sur pu wigka üytün mapu mew. Feyta chi zugu tripay ta ñi pu che ñi kimtukunieael fillke zugu nüwkülelu fey ta chi derecho a la privacidad pigechi zugu mew ka femgechi ñi kuñiwruküleael kiñe troy zugu mew ka chumechi am pegelnienoeael taiñ chumeken fey ta chi zugu mew ka ñi miawnoael weza ke zugu mew fey ta chi zuam mew mülenmu ta persecución digital ka vigilancia pichechi zugu mew medios digitales zugu mew.

Proyecto Kimtukunieal zugu

1. ¿Qué es?

Es un manual de seguridad en comunicaciones digitales en la cual se establecen objetivos, normas, y procedimientos para garantizar y preservar la privacidad dentro de la comunidad.

2. ¿Para quién es este manual?

- Para las comunidades en riesgo de latinoamérica y muy especialmente en el cono sur.
- Para grupos criminalizados, perseguidos y/o en riesgo de vigilancia digital.
- Para comunidades que buscan proteger el derecho a la privacidad, y estar informadas de forma segura.

3. ¿Para qué sirve?

- Para fortalecer a través del conocimiento a organizaciones indígenas y afines de la región.
- Para capacitar tanto a personas como a comunidades de pueblos originarios y afines en riesgo.
- Para poner a disposición de las comunidades un conjunto de soluciones inmediatas al problema de la vigilancia y persecución de las comunidades indígenas y afines de la región.
- Para generar un cambio de conciencia dentro de las comunidades indígenas a fin de que tomen posesión de su derecho a la privacidad.

Proyecto Kimtukunieal zugu

1. Chem am

Fey ta kiñe chillka chew am koneltuley fey ti chi seguridad en comunicaciones digital zugu mew chew am wirintukuley chem zuam mew tripay tūfa chi chillka, chumechi am azüy ka fillke zugu inakonkülelu fey ta chi kuñiwatun zugu taiñ nieael privacidad pigechi zugu chew taiñ mülen ka taiñ trokin che mew.

2. Iney ñi zuam tripay tūfa chi chillka

- Fey ta chi pu che kuñiwatuleael Latinoamérica mew ka cono sur üytün mapu.
- Fey ta chi pu che inagekelu, allmalltuniegelu kam zuamniegelu ñi wechalkageael
- Fey ta chi pu trokin mapu chew am zuamyey fey ta chi derecho a la privacidad pigechi zugu mew ka ñi kimtukunieael zugu.

3. chem zugu am azkonküley kam chem zugu mew am pünegeafel

- Müli ñi kuñiwatuleael ka kimtukunieal zugu pu trokiñche nüwkülelu fey ta chi zugu ka mapu mew
- Fey ta chi pu che kam trokiñ mapu nüwkülelu mapu mew müli ñi kimtunieael zugu.
- Fey ta chi pu trokin mapu ñi kimnieal ñi chumal niele fey ta chi zugu vigilancia ka inayawülgele ñi mapu mew
- Pu che müli ñi günezuamael ñi kuñiwüngen feyta chi zugu ka mülen fey ti chi derecho a la privacidad pigechi zugu.
- Müli ñi azküleael fey ti derecho humano pigechi zugu fill mapu mew ka pu che nüwkülechi mapu mew fey genmew fey ti chi

- Para asegurar los derechos humanos de las comunidades, pueblos originarios del cono sur y afines, por ser un grupo especialmente vulnerable dentro de la sociedad.
- Para visibilizar la situación de los Pueblos y Comunidades Indígenas y afines de la región en todas las comunicaciones públicas, y recomendar sobre las medidas que se pueden tomar para evadir la potencial persecución y vigilancia a través de medios digitales.
- Para propiciar la uniformidad de los procedimientos de seguridad dentro de las comunidades, permitiendo que diferentes miembros puedan realizar diferentes tareas de forma segura.

4. ¿Cómo se hizo?

- Se investigaron los requerimientos en seguridad digital a través de miembros activos dentro de las comunidades de pueblos originarios del cono sur.
- Está escrito con apoyo gráfico y didáctico de los contenidos desarrollados.
- Está desarrollada en Castellano para la comunidad indígena andina, y en Mapudungun para la comunidad Mapuche de la región.

pu che zoy kuñiwutuleael.

- Fey ti chi pu che nüwkülechi mapu mew müli ñi pewfaluwal ñi chumekegen ka chumechi am konyawnoael fey ti chi persecución ka vigilancia tripakelu fey ti chi medios digitales mew.
- Müli kom kimnieal ñi chumam rupale feyta chi pu zugu fillke mapu mew ka zoy küme tripayal fey ti chi azkünuwün tūfa chi zugu mew.

4. *chumgechi am zewmagey kam chillkantukugey*

- Inatuzugugey fey ti chem ñi zuamel ti seguridad digital pu che mew konkülelu fey ta chi pu mapu mew chew ñi mülen weichan kam wiñotun mapu mew
- Wirintukuley ka azentun ta niey zoy küme kimgeael pu zugu inakönküleu faw.
- Ka wigkazugun mew wirintukuley pu pikun mapu mülechi che ñi zuam mew ka mapuzugun mew wirintukuley pu mapuche ñi zuam mew.

1. fey ta chi correo electrónico



Correo electrónico

1. Correo electrónico

1.1 ¿Qué es?

Es un servicio de red digital y personal. Existen varios proveedores que superficialmente todos ofrecen lo mismo, con algunas variaciones. Algunos muy conocidos son gratuitos.

1.2 ¿Para qué sirve?

Actualmente es una de las formas más usadas de intercambiar datos y comunicarnos a distancia. Es el medio preferido para enviar archivos adjuntos o materiales “pesados”.

1.2.1 Riesgos.

- Tus conversaciones privadas podrían quedar expuestas.
- Tendrán acceso a tus contactos y documentación importante enviada/recibida por correo electrónico.
- Puedes perder el acceso a la cuenta si cambian tu contraseña de acceso o los métodos de recuperación de cuenta alternativos: Otra dirección de email, número de teléfono, etc.
- Problemas de seguridad.
- Suplantación de identidad y comprometer tu reputación.

1. Fey ta chi correo electrónico

Chem am

Fey ta chi zugu gey kiñe servicio de red digital ka pu che ñi zuam mew. Nüwkülekey müfü proveedores mew, kiñe müfü müley, itrokom feypileyegün chem ñi wülken kom trürleyegün welu kishu ka niey ñi az egün. Kiñeke zoy kimniegey fey kulligekelay.

Chem zugu mew am pünegekey

Fantenmu zoy pünegekey fey ta chi amulgeael wirin kam chillka ka kimuwküleael fey ta chi pu che kañpüle mülelu. Ka femgechi zoy zulligekey ñi amulgeael fey ta chi pu wirin zoy fanelu reke kam pünantukuael kake wirin kam chillka.

chem zugu mew müli taiñ kuñiwtuleael

- Tami wirintukun fey ta mew kake che peafüy, kimlayafüymi norume
- Kimmageafüymi kom tami pu contacto ka wirin kam documentación tami amulel kam llowel tami correo electrónico püle.
- Ñamümafüymi tami cuenta correo mew kake che niele tami contraseña kam chumechi mi wiñonietuael fey ti chi cuenta ka contraseña, kam número de teléfono , itrokom kimageafüymi.
- Kimfal lay ñi rüf allmalltuniegen kam femnegeun.
- Kake che eyimi reke nieafüy kiñe cuenta ka eyimi reke zuguafüy , welu kimlayafüymi rume tami chumekegen

1.3 ¿Qué se recomienda?

Idealmente, un buen servicio de proveedor de correo electrónico debería ofrecer:

- Autenticación en dos factores (2FA). ¿Qué es?
- Actualizaciones continuas en todas sus versiones, en caso de que uses programas o aplicaciones. (escritorio, y aplicaciones)
- Cifrado de extremo a extremo, y/o la posibilidad de cifrar por nuestra cuenta cualquier información a través de PGP/GPG, en este momento muy pocos proveedores soportan esto.
- Es importante saber dónde está registrada legalmente la compañía que te provee servicios de correo electrónico, dado que deben apegarse a las leyes dependiendo de la jurisdicción donde operan. En otras palabras, si lo indica la ley, pueden o no estar obligadas a entregar información de los usuarios a sus gobiernos.
- Revisar las políticas de privacidad, particularmente los datos que recopila el servicio de correo electrónico, el uso que le dan y cómo se comportan frente a la solicitud de información por parte de instituciones gubernamentales.

Si usas Gmail:

- Comprobar que tengas activa la verificación en dos pasos, que los dispositivos conectados sean conocidos, que las contraseñas de aplicación se correspondan con los servicios que has activado por esta vía y que la “actividad reciente relacionada con la seguridad” no muestre actividad sospechosa.

chem zugu am müli taiñ kimtukunieael

Fey ti chi zoy trokifalel niey kiñe küme servidor fey ti chi wülkelu correo electrónico müli ñi nieael.

- Epurume autenticación pigechi zugu (2fa) chem am
- Müley ñi nieael fey ti zugu Actualización pigechi troy chumechi amulen antü müli ñi tripaleael fey ti zugu nielmi programas kam aplicaciones zugu.
- Fey ta chi cifrado gey kiñe azelkan chew llitun zugu azümfali weli tripale kam katrütügele kimfalay chem pilen, welu müte gelay fey ta ke proveedor ñi azniefiel ka niefiel.
- Müli kimgeael chew am wirintukuley fey ti chi compañía wülpelu ti correo electrónico, fey ti zugu müli ñi azküleal chumechi am feypiley fey ti jurisdicción chew ñi mülen. Kam chem pilen fey ti chi ley kizuegün wülafüy taiñ üy kam kake zugu fey ta pu gobierno.
- Müli ñi gunezuamgeael fey ti chi políticas de privacidad, zoyelafiel fey ti chi zugu chem datos ñi püneken fey ti chi correo electrónico, chem zuam mew kizuegün wülkeyegün taiñ üy kam chem pileyegün feypieliu pu instituciones gubernamentales egün ñi wülal fillke üy pu che nielu fey ta chi zugu

nielmi Gmail.

- Müli tami aznieal fey ti chi verificación en dos pasos pigechi troy, ka fey ti chi pu dispositivos müli tami kimnieafiel ka fey ti chi contraseña müli ñi nüwküleal kom fey ti chi pu troy chew tami miawkeel ka fey ti chi actividad reciente relacionada con la seguridad , fey mew müli ñi pegelnoeael tami kuñiw tuleael.

- Ir a la ruta: Configuración>Filtros y direcciones bloqueadas, chequea que no exista ningún correo al que se reenvíe la información que recibes.
- Ir a la ruta: Configuración>Reenvío y Correo POP/IMAP, se recomienda inhabilitar ambas opciones, a menos que utilices un programa de correos como Outlook.
- Leer los informes de transparencia de Google. Incluyen reportes relacionados a la privacidad y seguridad de la compañía, solicitudes de retiros de contenido y solicitudes particulares en todo el mundo.
- Utilizar distintas cuentas de correo para tus actividades, tratando de mantener separadas las comunicaciones personales de las de trabajo.
- Utilizar correos desechables para servicios o herramientas que quieras probar y requieran de un registro con correo electrónico. Se recomienda 10minutemail.com.
- Müli tami amuael configuración mew, inagechi filtro mew , inagechi direcciones bloqueadas, fey mew güneytuaymi ñi mülenun kake correo chew ñi ka rüputuken tami pu correo amulkeel ta eyimi.
- Müli tami amuael configuración mew inagechi reenvio mew inagechi correo pop/IMAP mew , fey ta mew müley tami güneytuafiel Inhabilitar ambas opciones, welu pünekelmi fey ti chi Outlook correo müley ta mi femnoael.
- Müli tami chillkatuafiel feyti chi informe de transparencia pilelu google me . fey mew tripay fey ta chi zugu nüwkülelu privacidad zugu mew ka seguridad de la compañía pigechi zugu, ka fey ti chi wiñonentutun fillke zugu tami koneltuel fey mew ka kiñe zuam fill mapu mew.
- Müley tami püneael kiñe epu correo tami zugu mew, ka ñi wichuleael tami che gen zugu ka tami küzaw zugu.
- Ka müley fey ti ci correos desechables pigelu fey ti troy zuamyelmi kiñerupa müten tami wülal tami correo , fey ta 10minutemail.com zoy kümi piam.

2.

fey ta chi contraseña
pigechi zugu



Contraseñas

2. Contraseñas

2.1 ¿Qué son?

Una contraseña es como un candado o como una cerradura. Pueden definirse como una serie secreta de caracteres de números, letras o símbolos que combinados ofrecen acceso a algo que, sin dicho código, resulta inaccesible. Se trata de una barrera inicial de seguridad. A pesar de que existen múltiples formas de autenticación (pines de 4-6 dígitos, patrones, reconocimiento de voz y facial), las contraseñas siguen siendo la principal puerta de acceso a nuestras cuentas de usuario y dispositivos. Es por esto que hoy en día, resulta fundamental tener contraseñas de acceso seguras, que difícilmente puedan ser hackeadas.

2.2 ¿Para qué sirven?

- Las contraseñas ayudan a asegurar que los usuarios desautorizados no tengan acceso a la información alojada en tus equipos. Las contraseñas son tan importantes como la información que proteges. Con ellas cuidamos que nuestra información privada no se transforme en material de dominio público.
- En otras palabras, son fundamentales porque dan acceso a tus dispositivos y servicios y en consecuencia a tu información personal.

2.2.1 Riesgos.

Si alguien conoce tu contraseña podría comprometer tu privacidad, haciendo cosas tales como:

2. Fey ta chi contraseña pige-chi zugu

Chem am

Kiñe contraseña kiñe nüfküntukuwe reke. Feypigeafüy kiñe müfü series re kiñe che ñi kiamel chuchi gen, yeniey fillke az wirin fey ti chi wirin mew kompukey reke che kiñe zugu mew, fey nienole fey ti chi az wirin pepi konfally , fey ta kiñe malal reke chew ñi rupayal fey ti chi niel ti código müten . welu chumte mülele kakerume az konael fey ta chi pu zugu zuamyelu contraseña (kiñe ke zuamyey wirintukuael wigka rakin meli wirin), kam azentun, zugun mew konpuael kam nentuz age mew, fey ti chi pu contraseña gey fey ti chi wülgiñ reke konael taiñ cuenta mew , fey mew fantenmu zuamyey niel rüf kúme az contraseña kimfalgenoael .

chem zugu mew am pünegekey

- Fey ti chi pu contraseña zuamyey ñi chuchike che no rume ñi konpuanoel taiñ pu cuenta mew kam taiñ pu equipo mew, fey mew müli ñi rüf günezuamafel ñi pepilfalnun kake che mew taiñ contraseña. Fey mew inchiñ zapilltuayíñ reke taiñ zugu llowkeel kam amulkeel, fey kake che ñi kimnoael.
- Ka femgechi taiñ contraseña kimfalgele kake che pepi konafüy taiñ üy mew kam fillke zugu mew chumte inchiñ pinoliyíñ taiñ kimageael.

Chem zugu mew müli taiñ kuñiw tuleael

Kiñe che kimle tami contraseña kimafüy kam pegelafüy ey mi tami pu zugu niel fey mew

- Publicar con tu nombre en redes sociales.
- Leer y contestar correos electrónicos haciéndose pasar por ti.
- Acceder a tus servicios online.
- Comprar en tu nombre si a la cuenta del servicio tienen asociado un medio de pago.

2.3 ¿Qué se recomienda?

A la hora de crear una contraseña segura, hay que saber que son varios los consejos a tener en cuenta. Nos estamos refiriendo a los siguientes:

- Usar distintos tipos de caracteres. Diseñar una contraseña alfanumérica, es decir, que tenga tanto números como letras con un mínimo de 14 caracteres en total. (mientras más largas las contraseñas, más seguras son).
- Elige contraseñas fuertes o robustas de al menos 14 caracteres y compuestas por:
 - mayúsculas (A, B, C...)
 - minúsculas (a, b, c...)
 - números (1, 2, 3...)
 - y caracteres especiales (\$, &, #...)
- No utilizar como contraseñas cosas fáciles de identificar a través de ingeniería social (datos que se obtienen a través de publicaciones en las redes sociales u otros sitios en la web), tales como:
 - Nombre o apellidos,
 - Fechas importantes,
 - Nombre de familiares,
 - Nombre de mascotas,
 - Matrículas de vehículos etc., dado que todos esos datos son fáciles de identificar con la persona y, por tanto, son más vulnerables.
- No dejar copias físicas o digitales accesibles, tales como notas en el celular, documentos de

- Eymi tami üy mialafüy redes sociales mew, eyimi reke zuguafüy , welu eyimi kimlafüymi norume
- Wiñolzuguafüy eyimi tami üy mew
- Konafüy tami servicios en línea mew
- Güllakayafüy eyimi tami üy mew nielmi kiñe zugu fey ti chi pago asociado pigelu .

chem zugu am müli taiñ kimtukunieael

Zewmalmi tami contraseña müli tami güneytuael kiñe müfü troy wüne.

- Müli tami wirintukuael itrofill wirin wülkelu ka nielu wirin az, rakin wirin ka zoy mari meli wirin niele zoy kümey,
- Müley tami nieael kiñe alüchi contraseña niele zoy mari meli wirin ka niele fey ti chi:
 - mayúscula pigechi wirin
 - minúscula pigechi wirin
 - wigka rakin wirin
 - kake az wirin
- Müli tami nienoael contraseña pepilfalu, kiñe ke che ta pepilfali ka küzawkey fey ta chi pu zugu mew fey mew tripacey kiñe troy nüwkülelu ta che mew :
 - Tami üy, chaw ka ñuke püle
 - Fey ti el antü, lleglu chi antü mu che kam tami pu che.
 - Tami pu che ñi üy mew
 - Tami pu zapillkulliñ ñi üy
 - Pu vehículo ñi wirin , fey ta pepilfali , ka pepi kimgey ineygen fey ti chi vehículo.
- Müley ta elgenoael wirin mew kam teléfono mew kiñe wirin , tushpu müli ñi wirintukugenoael fey ti chi contraseña chew norume tami zoy pegenoael tami

texto en el computador, notas adhesivas en los monitores y las anotaciones de contraseñas en pizarras y libretas son considerados como malos hábitos si nuestro objetivo es tener la mayor seguridad posible en nuestras cuentas.

- No compartir tus contraseñas con nadie. Ese es un dato muy personal que solo debe estar en manos de a quién le pertenece.
- No tener una misma contraseña para las tarjetas bancarias, emails, teléfono móvil, tablet, redes sociales, dado que perder el control de una cuenta, equivale a perder el control de todas tus cuentas.
- No responder 'sí' cuando te solicitan guardar la contraseña en el navegador de un dispositivo público.
- Si manejar muchas contraseñas y recordarlas todas te parece extenuante, utiliza un gestor de contraseñas. Es un programa que te permite almacenar de forma segura tus claves de acceso a los diferentes servicios.

Solo necesitas recordar la clave de acceso al gestor de contraseñas, conocida como clave maestra, para consultar el resto de tus contraseñas. Eso sí, si la olvidas no podrás consultar el resto, por tanto, memorízala bien en tu cabeza. Una de las características más importantes de una contraseña segura es que sea fácil de recordar y difícil de adivinar para otros.

Nota. Tomar en cuenta que las leyes sobre la revelación de contraseñas difieren de un lugar a otro. En algunas jurisdicciones, es posible que puedan impugnar legalmente la demanda de tu contraseña. Por lo general las amenazas de daño físico son empleadas para obligar a alguien a dar su contraseña.

chumekeken fey ta chi zugu mew.

- Müley ta wülnoael ineynorume ta mi contraseña.
- Müley tami nienoael kiñe contraseña müten fillke zugu mew tarjetas bancaria mew, email mew, teléfono mew, fey mew zoy pepilfali tami ñamümael tami günenieael tami cuenta ka ke che ñi günenienotuafiel eyimi tami cuenta.
- Müley tami wiñolzugunoafiel ramtugelmi tami piel ñi "guardar contraseña" fey ti chi navegador público mew.
- Nielmi müfü contraseña ka goymakefilmi kiñeke müley kiñe gestor de contraseña pigechi troy zugu, fey mew pepi niegekey ta contraseña fey ta ka ke che penoafiel kam kimgenoael.

Zuamyeymi goymanoael fey ti chi clave de acceso nielu ti gestor de contraseña, ka kimgkey clave maestra pin zugu mew, fey mew güneytuafimi tami pu contraseña.welu goymafilmi pepi azkintulayaymi tami kake contraseña fey müley ta mi rüf lonkontukuafiel. Fey ta chi contraseña niey ñi goymagekenun ka pepilfalnün kake che mew.

Kimfali: fey ta chi pu leyes mülelu fey ta chi contraseña zugu mew wichuley fill mapu mew. Ka femgechi küpa kimmagelmi tami contraseña ka femafüy pu kake che. Kiñe ke mew fey ta chi allmalltun kam ulelkachen pünegekey tami wülal ta mi contraseña.

3.

epurume chi
autenticación
pigechi zugu



Autenticación de dos factores

3. Autenticación de dos factores (2FA o doble paso)

3.1 ¿Qué es?

La Autenticación de Dos Factores es una herramienta que ofrecen varios proveedores de servicios en línea, que cumple la función de agregar una capa de seguridad adicional al proceso de inicio de sesión de tus cuentas de Internet. La mecánica es simple: cuando el usuario inicia sesión en su cuenta personal de algún servicio online, esta herramienta le solicita autenticar la titularidad de su cuenta, proporcionando dos factores distintos. El primero de estos, es la contraseña. El segundo elemento puede ser:

- **Algo que sabes:** Consiste en agregar una segunda contraseña para lograr obtener el acceso a tu cuenta.
- **Algo que tienes:** Consiste en introducir un código que solo tú podrás obtener a través de un mensaje de texto, una aplicación o un dispositivo específico o token.
- **Algo que eres:** Consiste en utilizar la identificación biométrica, es decir, las características del cuerpo de una persona, para verificar su identidad. Por ejemplo, a través de huellas dactilares, cara u ojos. Debido al riesgo de filtración de datos y lo vulnerables que pueden ser estos métodos, la autenticación a través de información biométrica no es el método que recomendamos cuando esta información es almacenada en servidores externos.

3.2 ¿Para qué sirve?

- De esta manera estaremos más seguros por-

3. Fey ta chi Autenticación de dos factores pige chi zugu.

3.1 Chem am

Fey ti chi autenticación de dos factores gey kiñe troy zugu nielu müfü proveedores pigekey fey ti wülkelu pu servicio en línea, tüfachi zugu epurume nüfküntukun reke gey tami pu cuenta intertet mew. Femechi tripakey, fey ti chi che pünealmu ñi cuenta kiñe servicio en línea mew , tüfachi zugu feypikey ñi tripayael fey ti chi autenticación de cuenta fey ramtuafüy kiñe epu troy, wüne tami contraseña kam:

- **Kiñe troy zugu eyimi müten tami kimnieel,** fey ta mew nieaymi kiñe mür contraseña konael tami cuenta mew.
- **Kiñe troy eyimi tami nieel:** müley tami wirintukuael kiñe código eyimi müten tami kimel, fey ta puway kiñe mensaje mew kam kiñe aplicación mew kam kake zugu mew.
- **Chem zugu tami nieel , tüfa mew müli tami pegelafiel tami az kalül, kimgeael eyimi gen tami konpeyel tami cuenta mew, tami az chagüllgeafüy kam tami age, kam kuralge.** Welu müte kümelay tami puneafiel tüfa chi zugu, fantenmu kimgelay pepilniegen kañpüle weñeymageam tami üy.

3.2 Chem zugu mew am pünegekey

- Fey ta mew zoy pepilfal-lay tami

que se necesitan ambas vías de autenticación para lograr obtener el acceso.

- Para mas información, consulta <https://twofactorauth.org>

3.3 ¿Qué se recomienda?

Habilitar el doble factor en todos los servicios que tengan esta opción. Dependiendo del caso, puede consistir en:

- El envío de un SMS. Un código verificador llegará a tu teléfono celular a través de un mensaje de texto. Este método no es muy recomendado si sospechas que tus llamadas y mensajes están siendo interceptados.
- Aplicaciones de autenticación. Encontrarás un código de acceso dentro de una aplicación que no requiere señal telefónica o internet para funcionar.
- Segunda Clave. Introducir una segunda clave o código de 6 dígitos (en el caso de WhatsApp).
- Token. Consiste en un dispositivo físico que muestra códigos de autenticación.
- Activación de una llave de seguridad. Consiste en un dispositivo físico que se conecta a través de puertos USB o de forma inalámbrica para autenticar tu identidad.
- Buscar la opción de códigos de emergencia o de seguridad, en los servicios que lo permitan para que puedas tener acceso a tus cuentas en caso de no poder acceder los otros métodos de autenticación. Estos códigos se deben guardar de la manera más segura posible, por ejemplo, anotados bajo llave o en un administrador de contraseñas.

weñeymageael tami üy kam tami zoy güfküntukunieael tami cuenta.

- Ka femechi küpa zoy kimilmi güneytufige tüachi página: <https://twofactorauth.org>

3.3 chem zugu am müli taiñ kimtukunieael

Müli tami nieafiel fey ti chi doble factor zugu kom tami pu servicio mew :

- Kiñe wirin llowgekelu teléfono mew, puwkey kiñe codigo teléfono mew fey mew kiñe llag wirin mew , welu tami teléfono allmalltulel kümelay tufachi zugu.
- Müley aplicaciones de autenticación, pegelfali kiñe código ka kiñe aplicación mew , zuamyenun señal telefónica kam internet .
- Epuchi contraseña: müley ñi konünpayael ka kiñe contraseña kayu wirin nielu(fey ti chi whats app mew pünegekey tufa.)
- Token pigey kiñe dispositivo güillagekelu kam wülgekelu fey mew pegekey kiñe código de autenticación.
- Nieael kiñe llave de seguridad; fey ta mew müli ñi mialael kiñe dispositivo tukugekelu puerto USB mew kam re femechi müten ka femgechi kimfali eyimi gen kam eymigenun.
- Ka müli taiñ kintual códigos de emergencias kam seguridad pigelu, fey ti chi pu servicios mew pepi niegelu fey ti chi troy zugu, pepi niegenolu kake az autenticación. Tüfa chi pu código müli ñi zoy trapümniegeael , wirintukugeael chew ñi pegenoael kam kiñe administrador de contraseña mew.

¿Cómo activar la verificación de dos factores en algunos servicios importantes?

Para la mayoría de las cuentas que tiene, normalmente encontrarás la opción de verificación de dos factores en la configuración de seguridad de tu cuenta. Esto significa encontrar las opciones de configuración, que normalmente es sencillo. La mayoría de los servicios en los que inicia sesión tendrán una opción, pero estos son algunos de los servicios más populares:

Cómo habilitar la verificación de 2 pasos de Google

Para tu cuenta de Gmail / Google, inicia sesión en cualquier servicio de Google, o simplemente ve a Google.com y haz clic en la imagen de tu perfil en la esquina superior derecha, luego selecciona "Mi cuenta". Haz clic en la opción "iniciar sesión en Google" en la pestaña Inicio de sesión y seguridad. Busca la [opción de verificación en dos pasos](#) y elige activarla. Aquí puedes agregar tu número de teléfono, elegir obtener un mensaje de Google en tu teléfono, configurar algunos códigos de respaldo que puedes imprimir o descargar e instalar la aplicación Autenticador de Google en tu teléfono Android o iPhone.

Cómo habilitar la verificación de inicio de sesión de Twitter

Inicia sesión en Twitter en el escritorio y haz clic en la miniatura de la imagen pequeña en la barra de herramientas, luego selecciona "Configuración y privacidad" en el menú desplegable. Marca la casilla "Verificar solicitudes de inicio de sesión" en las opciones de seguridad y, si aún no lo has hecho, ingresa tu número de teléfono móvil para que puedas enviarle códigos SMS. También puedes usar la aplicación

Chumechi am niefiyin fey ti verificación de dos factores kiñe troy zugu mew

Epe kom zugu mew pegengekey fey ti chi verificación de dos factores fey ti chi troy configuración de cuentas mew. Fey mew müley tami peafiel fey ti chi opciones de configuración pilechi wirin, epe kom servicio konünpan zugu mew müley fey ti chi wirin , welu tūfa kiñe troy zugu tami kimtukunieael.

Chumechi am nieafimi tūfachi verificación de dos paso google mew

Tami gmail mew kam google mew, konünpan zugu mew fey müli tami konael google.com mew fey konaymi fey ti chi wirin mew "perfil" mew wenu man püle, inagechi konaymi "mi cuenta" mew , inagechi konaymi "iniciar sesión en Google" fey ti chi wirin inicio de sesión y seguridad pilelu, ka femechi kintuafüymi [opción de verificación en dos pasos](#) fey mew may piafimi, fey mew koneltuafimi tami número de teléfono, kam azümkayafimi fey ti chi codigos de respaldo pigechi troy fey ti chi zugu pepi azentufali kam nieafel feyt i chi autenticador de Google tami teléfono mew.

Chumgechi am azelkageafüy ñi rüfgen ka ñi küme kimgeal koneltuael Twitter mew.

Koneltuge Twitter chew elgepëyüm kom zugu ka güpafige fey ti pichi azentun mülelu chew pepilkagekey zugu, inagechi chew feypuley " configuración y privacidad" chew troytulen zugu. Konletuge chew feypiley "verificar solicitudes de inicio de sesión " chew müley "opciones de seguridad" petu femnulmi, koneltufige tami número de teléfono móvil mew fey ta mi pepi amulael pu código SMS

móvil de Twitter para generar códigos al iniciar sesión abriendo el menú de la barra lateral, dirigiéndose a Configuración y privacidad> Cuenta> Seguridad> Generador de código de inicio de sesión.

Cómo habilitar la autenticación de dos factores de Facebook

En Facebook en el sitio de escritorio, haz clic en el pequeño icono de globo en la barra de herramientas, luego ve a Configuración> Seguridad e inicio de sesión, luego elige "Usar autenticación de dos factores". Puedes agregar su número de móvil para códigos de mensajes de texto, agregar claves de seguridad para iniciar sesión por USB o NFC, o generar códigos en la aplicación móvil de Facebook. También puedes generar contraseñas de aplicaciones específicas para usar una vez para aplicaciones que no admiten la autenticación de dos factores de Facebook.

Cómo habilitar la verificación en dos pasos de Apple

Para tu ID de Apple o cuenta de iCloud, ve a appleid.apple.com, luego inicia sesión en tu cuenta y busca la verificación en dos pasos en la sección Seguridad, y elige activarla. Luego pasarás por un proceso de configuración que es realmente fácil de seguir. Además, asegúrate de crear una clave de recuperación y luego toma nota de ella en algún lugar seguro, donde sepa que nunca lo perderá.

pigelu. Ka femechi müley fey ti chi aplicación móvil chew tami nieael Twitter fey mew pepi nentugey ti código koneltun zugu mew, fey mew koneltuael menú pigelu chew troytuley kake zugu, inagechi configuración y privacidad fey ti chi cuenta mew ka seguridad zugu mew ka chew tripakey código koneltuam faw.

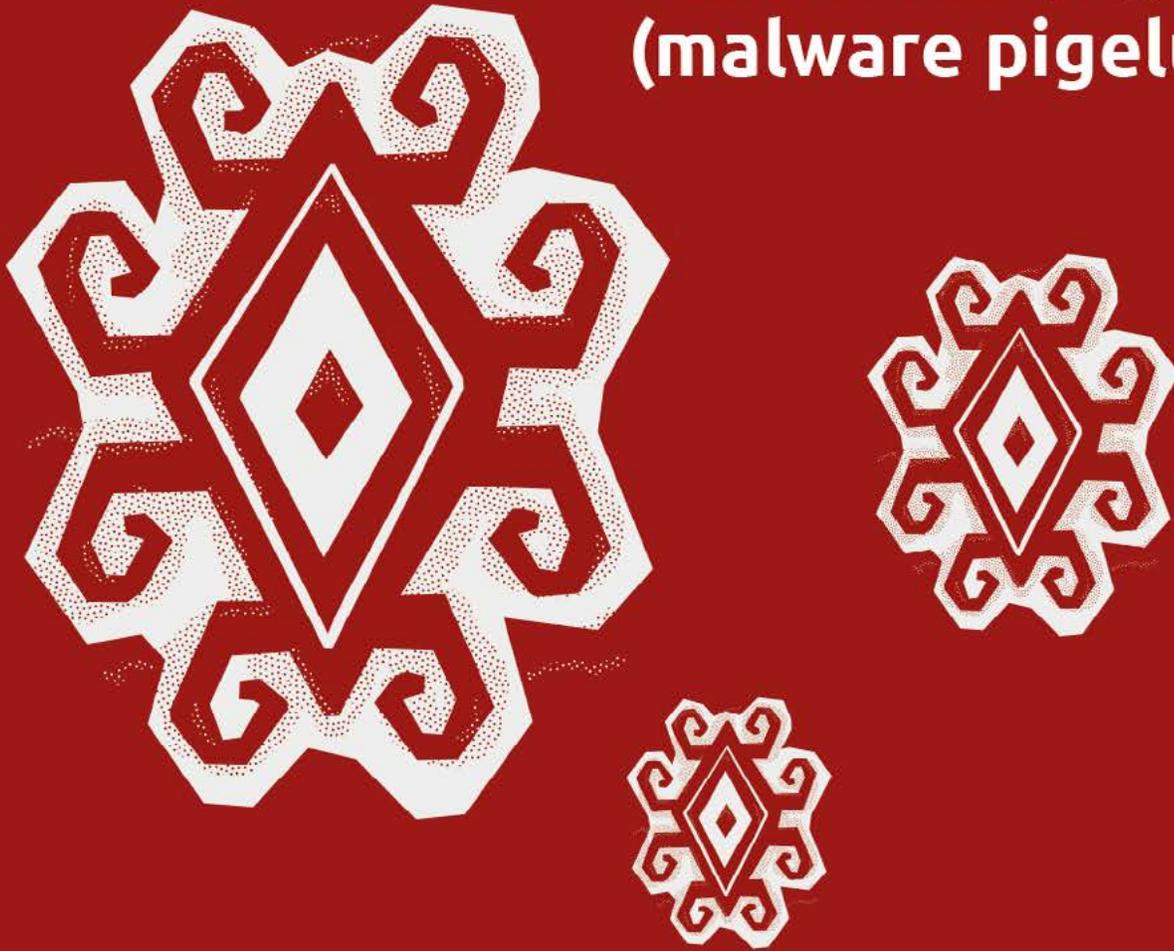
Chumechi am nieafimi fey ti chi autenticación facebook mew

Facebook mew fey ti chi escritorio mew müley kiñe pichi azentun barra de herramientas mew, inagechi konaymi configuración mew, inagechi seguridad e inicio de sesión mew fey mew feypiafimi "usar autenticación de dos factores". Ka fey küpa tukufilmi tami número de teléfono ka femafüymi llowam fey ti chi código de mensaje de texto mew, kam tukuafüymi fey ti chi claves de seguridad konünpayal fey mew fey ti chi USB kam NFC kam nieael código fey ti chi aplicación facebook mew. Ka femgechi pepi nieafüymi contraseña de aplicaciones pigechi zugu chew am pepi nienolmi fey ti chi autenticación de dos factores facebook mew.

Chumechi am nieafimi fey ti chi verificación de dos pasos apple mew

tami ID apple mew kam cuenta ;Cloud mew konaymi appleid.apple.com, inagechi konünpayaymi tami cuenta mew, inagechi kintuaymi fey ti chi verificación de dos pasos mew fey ti chi wirin sección de seguridad mew, fey müli ta activa yafiel, inagechi güneytua fimi kom ti pu wirin tripayelu fey mew. ka femechi niefüymi fey ti chi clave de recuperación pigechi wirin, fey mew müli tami nieafiel chew ey mi müten tami kimafiel chew mülen.

**4. fey ti chi pu
wezalkake chi
kam/Aplicaciones
Maliciosas pigelu
(malware pigelu)**



Aplicaciones maliciosas

4. Aplicaciones maliciosas (Malware)

4.1 ¿Qué son?

Se definen como aplicaciones que hacen cosas indeseadas sin autorización. Somos vulnerables a ellas a través de correos electrónicos, descargas en internet, documentos adjuntos, memorias USB, y/o en general cualquier material descargable en nuestros dispositivos.

4.2 ¿Para qué sirven?

- Para monitorear sin autorización tus contenidos personales.
- Para afectar el uso de tus equipos.
- Para hacer acciones maliciosas en nombre de otra persona.

4.2.1 Riesgos

- Pueden tomar el control de los componentes de tus equipos, tales como activar la cámara, "leer" lo que escribes en el teclado, guardar tus contraseñas y archivos e incluso borrarlos.
- Puede activar información de los sensores como el micrófono, la cámara, el GPS para saber dónde está el teléfono y monitorear el ambiente, aparentar estar apagado y con la pantalla en negro, convirtiendo el teléfono en un espía.

4. Fey ta chi pu wezake aplicaciones (Malware pigelu)

4.1 Chem am

Fey ta chi pu trokin zugu koneltukey wezalkayal ta che , fey kimgekelay norume ñi miawün kam mülen , fey miawkey correo mew kam nakümyim kiñe ke zugu internet mew kam pünantukulmi kiñe chillka kam chew tukugekey chillka USB pigelu kam chem rume chew taiñ konken tüfa chi zugu mew.

4.2 Chem zugu mew am pünegekey.

- Allmalltuel tami chumeken , welu kimlaymi norume tami femekegen.
- Tami wechalkaymageael tami pu equipo
- Nentuel wezake zugu ka üyche mew.

4.2.Chem zugu mew müli taiñ kuñiw tuleael

- Tüfa chi zugu pepi güneniefüy reke tami equipo, pegelgeafüy tami az, chillkatuafüy chem tami wiripeyel, kam nieymayafeymu tami contraseña kam ñapumafüy tami pu wirin chillka.
- Ka femechi üyümafüy fey ti chi micrófono, pegelwe, GPS ka, tami kimgeael chew mülen tami teléfono, azkintuel chew tami mülen, chogümkülelu reke müleafüy tami teléfono welu kom güneytunieymageafüy tami mogen.

4.2.2 ¿Cómo detectar aplicaciones maliciosas?

Cada vez se hace más difícil detectar estas aplicaciones en nuestros equipos debido a la creatividad de quienes las crean. Necesitamos estar totalmente desconectados de internet, para estar seguros de que no tenemos aplicaciones maliciosas instaladas en nuestros dispositivos. Sin embargo, acá alguna lista de potenciales indicadores:

- Consumo excesivo de batería.
- Consumo excesivo de datos.
- El equipo se apaga de manera espontánea, no puedes volver a encenderlo o el sistema se bloquea de repente.
- El equipo funciona más lento de lo normal (debido a la carga de trabajo extra de la aplicación maliciosa).
- La velocidad de Internet es más lenta de lo normal (debido a un elevado tráfico de datos).
- Aumenta lo seguido que aparecen contenidos no deseados de Internet, tales como ventanas emergentes, reenvío automático a ciertas direcciones de Internet o acceso repentino a una nueva página web, buscador o nuevas barras de herramientas en el navegador.
- Las aplicaciones se desinstalan o bloquean de repente. Algunos elementos dañinos pueden, incluso, desactivar aplicaciones antivirus, lo que se convierte en otro indicio de que el sistema ha sido infectado.
- Se instalan aplicaciones no deseadas y algunas se abren solas.
- Redirecciones en tu navegación: ¿Quieres acceder a una web pero acabas en otras?

4.2.2 Chumgechi am kimgeki ñi mülen kam miawün fey ti chi trokin.

Pepilfal-lay kimgael ñi mülen taiñ equipo mew , ellagechi pepiluwü fey ta chi pu zewmafilu. Zuamyeiñ taiñ koneltulenuael fey ta chi internet mew fey mew allmaltugelayayiñ ka kuñiw tulelayaiñ taiñ nienun ta wezake aplicacione taiñ equipo mew.

- Taiñ batería müchay müten afi.
- Taiñ internet müchay müten afi..
- Taiñ equipo kizu chogüy ka pepi üyümfalay kam pepi pünefal-lay.
- Taiñ equipo zoy ñochiley (fey ti chi weza aplicación ñi zuam mew zew koneltulenmu)
- Ka ti internet ka ñochi yawi (zoy ñi pünekenmu fey chi zugu)
- Ka femechi wepay kareume zugu tripakelu internet mew, kam kizu amuluwkey kiñeke troy zugu mew mülelu internet mew kam koneltukey kake página web mew, chew ñi kintugeken zugu kam chew ñi azelkageken ta zugu.
- Kake aplicación nielu ta che pepi pünefalay kam ñamtukey, ka kiñekemew wezake trokin nentutuafü fey ti antivirus taiñ nieel, fey mew kimfali taiñ nien fey ti chi weza troy zugu.
- Akukey kake aplicaciones inchiñ taiñ zuamyenofiel rume ka kizu ta gülakey.
- Kañpüle ta amukey koneltugeyim fey ti chi troy chew kintugekey zugu. Eymi kintukeymi kiñe welu kake web mew puwkeymi.

4.3 ¿Qué se recomienda?

- Instalar aplicaciones bien conocidas y descargadas a través de los canales oficiales.
- Descargar solo contenidos en sus páginas oficiales, evitando contenidos no legítimos o “piratas”.
- Mantener actualizado el sistema operativo de nuestros equipos.
- Instalar un anti aplicaciones maliciosas (anti-malware). Son distintos a los antivirus, por lo tanto, trabajan en tu equipo de forma diferente, complementando el antivirus tradicional.
- Mantener actualizado el programa antivirus.

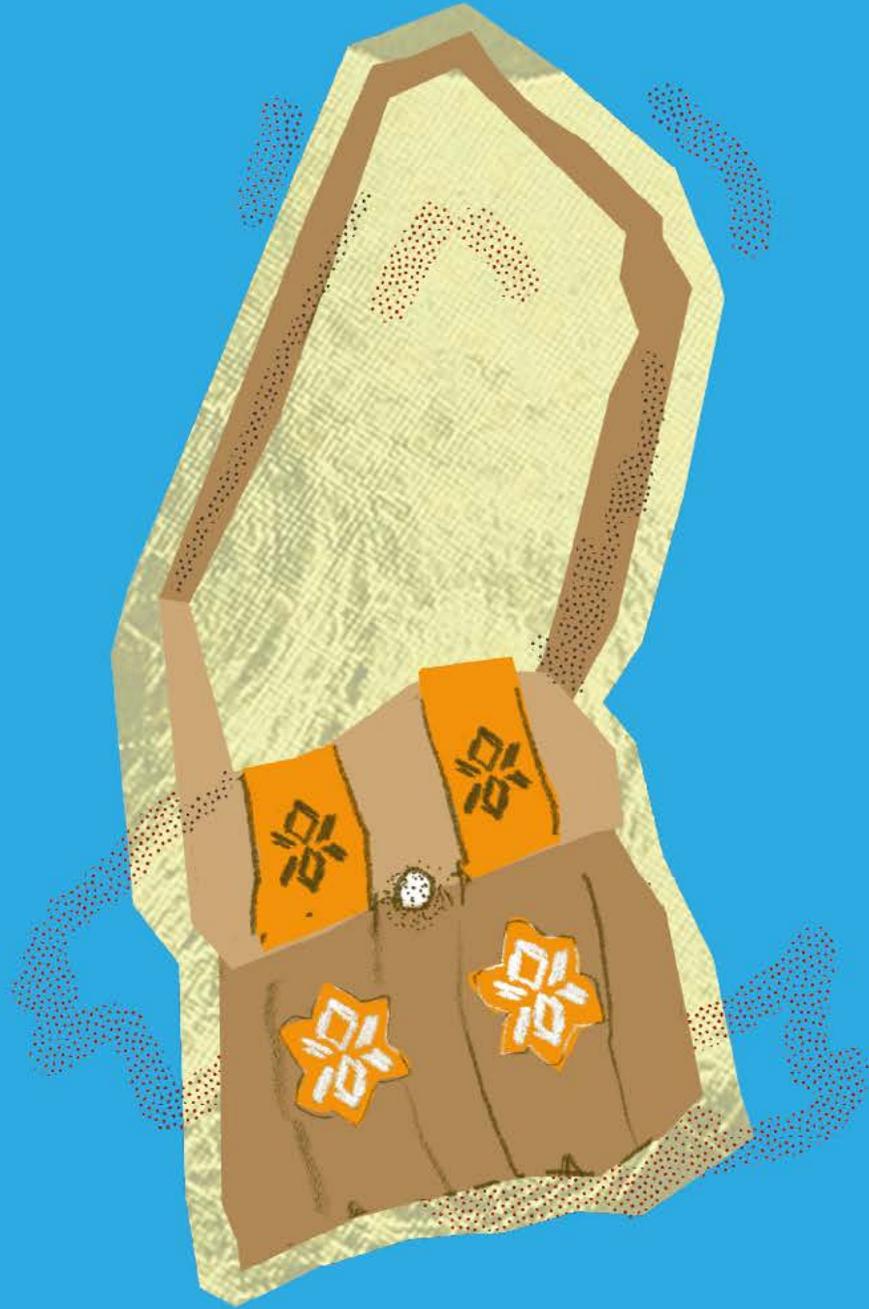
Nota. Instalar más de un antivirus conduce al mal funcionamiento e incluso dejando tus equipos aún más vulnerables.

4.3 chem zugu am müli taiñ kimtukunieael

- Müley tami nieal fey ti chi pu aplicacione zoy kimfal-lu ka chew ñi nakümgeken
- Nakümal zugu chew ñi rüf kimgen ñi mülen kam tripaken zugu, nakümnoael fey ti chi kimgelu chew ñi küpan.
- Tami sistema operativo müley ñi azleael fill antü taiñ equipo mew.
- Müley tami nakümal kiñe aplicación chew fey ti chi wezake aplicación pepi koneltulayay tami equipo mew. Tüfa ka az niey fey ti chi pu antivirus mew ka az zugu nentuy.
- Fey tami antivirus müley ñi azleael .

Kiñe troy: epu antivirus nielmi zoy wezalkawafüy tami zugu.

5. fey ta chi Telefonía móvil



Telefonía Móvil

5. Telefonía Móvil

5.1 ¿Qué es?

Es un servicio público de telecomunicaciones entre dispositivos que no están conectados mediante cables.

5.2 ¿Para qué sirve?

- Para facilitar la comunicación telefónica sin imponer restricciones en cuanto a ubicación y desplazamiento de sus usuarios.
- Permite comunicarse desde cualquier lugar. Aunque su principal función es la comunicación de voz, como el teléfono convencional, su rápido desarrollo ha incorporado otras funciones como son cámara fotográfica, agenda, acceso a Internet, reproducción de música, video e incluso soporte GPS.

5.2.1 Riesgos:

Rastreo de Localización.

Puede revelar tu ubicación durante todo el día a través de las señales que envían los teléfonos celulares. Existen al menos cuatro formas en que un teléfono celular puede ser rastreado por otros:

Rastreando la Señal de las torres de telefonía móvil

- Es posible debido a cómo funciona la red móvil, usando una técnica comúnmente llamada triangulación. Un operador puede calcular donde está localizado el teléfono de una

5. Telefonía móvil zugu.

5.1 Chem am

Fey ta kiñe zugu chew amulkagekey reke fillke zugu fey nüwküley pu dispositivo kiñe füw kam zef mew reke.

5.2 Chemu am pünegekey .

- Zoy pepilfalam fey ti chi zugulkawün kake mapurume mülele pu che ka femechi amuy ñi zugun.
- Chew rume müleafüy che welu pepi zuguluwi fey chi zuam mew wef-füy welu fantenmew zoy amuley ñi azümkawün nentuael az, chillkantukuael, koneltuwal internet mew, allkütuael wigka ülkantun, kam video kam fey ti chi GPS.

5.2.1 Chem zugu mew müli taiñ

kuñiwtuwküleal.

Kimfali chew taiñ mülen:

pepi kimfali chew tami mülen tami teléfono celular ta wülkey fey chi zugu . ka müley meli troy zugu chumechi am tami teléfono kimgeafüy chew mülen.

Inayegele fey ti chi torre chew mülelu ti telefonía móvil mew

- Chumechi ñi azkülen tüfa chi red móvil pigechi zugu fey mew nentugekey ti triangulación pigechi zugu, chew kiñe operador pepi kimafüy chew ñi müleun

persona en particular, siempre y cuando el teléfono esté encendido y registrado con la red. La exactitud con la cual es posible saber la ubicación del usuario puede variar, pero muchas veces, es tan exacta que pueden ubicarse al otro lado de una calle.

- No hay manera de escapar de este tipo de rastreo siempre y cuando tu teléfono móvil esté encendido y con señal operando en tu celular.
- Normalmente solo el operador del teléfono celular puede desarrollar este tipo de rastreo, pero un gobierno puede forzar al operador que le entregue cualquier clase de información respecto a la localización de cualquier usuario tanto en tiempo real, como en registros históricos.
- Los gobiernos también pueden pedir al operador de servicio móvil una lista de todos los teléfonos celulares que estuvieran presentes en un lugar, y en un determinado momento. Esto puede ser usado para investigar un crimen, o para saber quien estuvo presente en una protesta en particular.
- Solo apagar el celular no es una solución, dado que el teléfono celular puede simular estarlo aunque realmente se mantiene encendido y en la capacidad de monitorear las conversaciones.
- Limitarse a cambiar la tarjeta SIM o mover una tarjeta SIM de un dispositivo a otro ofrece una protección mínima, porque la red de teléfonos móviles observa a ambos juntos, la tarjeta y el dispositivo. En otras palabras, el operador de la red sabe la historia de cual tarjeta SIM ha sido usada en qué dispositivo, y puede rastrear ya sea de manera individual o ambas juntas.
- Los gobiernos han desarrollado técnicas de análisis de localización de teléfonos móviles donde el rastreo de la localización puede servir para

kiñe teléfono celular welu üyümkülele fey ti teléfono ka ñi koneltulen red mew. Rüf ñi kimgen chew ñi mülen fey ti chi teléfono kiñekemew müte külligekelay welu kiñekemew rüf küllikey fey wekun ruka reke puwkey zugu.

- Pepi kañpülenentuwlay ta che fey ta chi zugu mew üykülel ti teléfono ka nienmu señal kimgeafüy chew ñi mülen ka ñi chumeken.
- Welu fey ti chi pu günenielu fey ti teléfono chew ñi güllagemun feyegün pepi nentuafüy fey ti inayafiel ta che, welu fey ti chi pu gobierno ka feypiafüy fey ti operador ñi femal ñi allmaltuafiel ta che.
- Pu gobierno feypiafüy fey ti chi pu operador ñi wüla kiñe wirin kom fey ti chi pu celular mülen kiñe üytün mapu.ka kiñeke zugu tripawmelu kiñe üytün mapu mew. Tüfa chi zugu koneltugeafüy kiñe wechafemeken mew kam kiñe nentuzugun fütake trokin che mew.
- Chogümgele ti celular zugu no, kiñekemew chogümfaluwküley welu kom allküñmaniegey kom ñi gütram ta che.
- Ka tarjeta SIM tukuafin ñi teléfono mew piliyiñ welu fey ta kañpüle nentulay ti zugu, kizu egün ta kom kimnieafüy chem teléfono mew am tukugey ti tarjeta sim ka mür inayegekey.
- Pu gobierno aznieyegün ñi kima el egün chuchi ke teléfono niel ta kiñe che, kam mügü ñi nien ta kiñe che.

generar una guía o hipótesis sobre sí múltiples dispositivos pertenecen a la misma persona.

- El modelo de llamadas tiende a ser extremadamente distintivo, es decir, puedes hacer llamadas habituales a miembros de tu familia y a tus compañeros de trabajo. Inclusive cuando cada una de estas personas recibe llamadas de una cantidad muy variada de personas, es probable que la única persona en el mundo que las llama a todas desde un mismo número eres tú. Esto no está basado en el solo hecho que llamaste a un número en particular, sino en las combinaciones únicas de todos los números a los que tú has llamado.

Rastreo de la Señal del Móvil ó Recolectores IMSI

- Un gobierno u otra organización también puede recolectar directamente información de ubicación, a través de un recolector IMSI (una torre de teléfono celular portátil falsa que pretende ser una torre real, de tal modo que pueda detectar la presencia física de un usuario en particular como espiar sus comunicaciones. Se denomina IMSI a la Identidad Internacional de Suscriptor de Móviles (el número que identifica a la tarjeta SIM de un usuario. El dispositivo recolector de IMSIs necesita ser transportado a la localidad de interés, si es que se quiere encontrar o monitorear un teléfono celular en esa área. En la actualidad, no hay una defensa confiable contra todos los recolectores IMSI.

Rastreo del Bluetooth y Wi-Fi:

- Estas señales son transmitidas con menos poder que una señal del móvil y pueden ser normalmente recibidas sólo en un rango de distancias cortas, dentro de un mismo salón o dentro de un mismo edificio, aunque a

- Fey ta chi az mütrümüwün zoyel kimfali, fillantü mütrümülmi tami pu che kam tami pu trür küzawken . welu chumte fey ti pu che llowkey kake che ñi mütrümkeyew welu eyimi tami número müten ta zulliley, fey ta chi zugu trürkülelay fey ta chi número tami mütrümel , zoyelküley fey ti azelkawün pu número fey ta mi mütrümkeyel.

Inayen fey ti chi señal tripalu móvil mew kam fey ti chi llowkelu IMSI.

- Fey ta pu gobierno kam kake trokin ka femechi llowafüy fey ta chi chew ñi mülen ta che, fey ta llowkelu IMSI (kiñe torre celular reke welu koila torre gey fey mew kiñe rüf torrereke müley welu re ñi niefiel chew ñi mülen ka chumeken kiñe che). Femechi feypigey fey ta chi troy chew llowgekey kam inagekey fey ti chi tarjeta SIM iney mew am nüwküley fey ta chi SIM. Ka fey ti chi nükelu reke fey ti chi zugu müley ñi yegeael chew ñi zuamyegen , fey ñi küpa kimniegele fey mew müleyechi teléfono. Fantenmu ta gelay chumechi taiñ kimael ñi mülen ka mülenun fey ta chi pu IMSI

Inayegen fey ti Bluetooth ka wi-fi.

- Fey ta chi zugu müte alümapu puwlay zoy pichi amuy fey ti chi señal móvil mew ka pepi llowgey zoy pichi tripa müten, kiñe wellin mew kam kiñe ruka mew, welu ka müley kiñeke antena ta pepiluwlu llowafiel fey ti

veces usando una antena sofisticada es posible detectar estas señales a distancias más largas. Estas formas de rastreo pueden ser muy exactas cuando una persona entra o sale de un edificio.

- Los operadores de una red Wi-Fi también pueden ver la dirección IP de cada dispositivo que se una a su red, lo cual significa que ellos pueden reconocer un dispositivo en particular en un tiempo dado y deducir si eres la misma persona que se unió a su red anteriormente, incluso si no entras con tu nombre o dirección de e-mail en algún sitio.

Análisis Forense de Teléfonos Celulares Confiscados

- Existen cuerpos gubernamentales especializados en el análisis de teléfonos celulares capaz de sobrepasar el bloqueo de pantalla.

Análisis Computarizado de Patrones de Uso de Teléfono

- Consiste en analizar información sobre muchos usuarios de teléfonos para encontrar ciertos patrones de llamadas automáticamente, tales como:
- Averiguar si ciertas personas se conocen entre sí.
- Identificar la fuente confidencial de un investigador o periodista.
- Detectar cuando una persona usa múltiples teléfonos o intercambia teléfonos.
- Detectar cuando un grupo de personas viajan juntas o se reúnen regularmente con unos y otros.
- Detectar cuando grupos de personas usan sus teléfonos de manera inusual o sospechosa.

chi zugu tripayelu fey ta mew, fey ka zoy amuafüy fey ta chi señal, tūfachi inayen che rüf kūme koneltuafüy inayen mew konpule kam tripatule kiñe wellin mew.

- Fey ta chi pu günenielu pu red wi-fi ka femechi inayafüy tati dirección IP kom fey ti pu dispositivo mew nüwküel fey ti red mew, fey mew kimgeafüy ka fey chi che gen ñi ka koneltupeyel fey red mew, chumte koneltunolmi tami úy mew kam tami e-mail mew.

Fey ti chi pu teléfonos nūgelu ta kom güneytugekey.

- Müley kiñe trokin zoy pepiluwkülen fey ta chi zugu mew ñi güneytuafiel ta ti pu teléfono ñi zoy rumeael fey ti chi wezalkayafiel ti pagilwe.

Fey ti chi computador mew ka güneytugekey chem zugu mew koneltugekeyel kiñe teléfono.

- Fey mew güneytugeki kiñe müfü che ñi teléfono ñi pegeafiel kiñe zugu trürlu fey ti chi zuguluwün ti pu che fey mew.
- Fey mew müley ñi güneytugeael kimüwün chi pu che.
- Müley ñi kimgeal fey ti che gen kiñe pepiluwün zugu mew investigador kam periodista.
- Müli ki kimgeal fey ti che ñi nien müfü teléfono kam weluluwken teléfono kake che mew.
- Müley ñi kimgeael mülele kiñe trokin che ñi trawüken kam miawken ka mapu püle trürwen.
- Kimgeael mülele kiñe trokin che ñi püneken teléfono kakewma zugu mew kam weza ke zugu mew.

5.3 ¿Qué se recomienda?

En los dispositivos que permiten esto, puede ser de mucha ayuda:

- Inhabilitar el soporte en 2G de tal manera que tu dispositivo solo se conecte a las redes de 3G y 4G.
- Incapacitar el roaming si no esperas viajar fuera del área de servicio de tu portador. Estas medidas pueden protegerse contra ciertos tipos de recolectores IMSI.
- Apagar el Wi-Fi y el Bluetooth en un teléfono celular inteligente puede prevenir este tipo de rastreo, aunque esto puede ser incómodo para el usuario que quiera usar estas tecnologías frecuentemente.
- Remover las baterías ante la sospecha de tener una aplicación maliciosa escuchando o viendo lo que hacemos. Sin embargo, si muchas personas hacen lo mismo en una misma localidad a la misma vez, le deja saber a los proveedores de servicio y atacantes que esta fue una decisión grupal planificada. Una alternativa sería dejar los teléfonos en otra habitación donde los micrófonos no podrían captar las conversaciones.
- Existe un gran número de aplicaciones para teléfonos celulares capaces de inhibir o prevenir el análisis forense en los equipos, cifrando la información para hacerla imposible de leer, o haciendo un borrado de seguridad remoto que le permite al dueño del teléfono o a alguna otra persona designada por el dueño decirle al teléfono que borre cierta información. Sin embargo, se debe tener en cuenta que la destrucción intencional de evidencia y obstrucción de una investigación se puede considerar como un delito adicional.

5.3 Chem zugu müli ñi kimtugeael.

Fey ti chi pu dispositivo mew chew pepi tripay fey ta chi zugu tüfa ke zugu kelluntukuafüy.

- Fey ti 2G ñi koneltugenuael re ñi koneltugeael fey ti chi red 3G ka 4G re ñi tüfa chi red mew müten ki kineltuael.
- Ñi koneltugenuael fey ti chi roamin zugu miawnolmi ka mapu mew femülmi fey fey ti chi pu koilla torre reke nükelu zugu.
- Müli ñi chogümgeael fey ti chi wifi ka bluetooth fey ti chi celular inteligente pigelu fey mew pepi konletugelayafüy fey ti chi allmaltun zugu, chumte afeluwle fey ti chi che ñi püneafiel fey ta chi tecnología fillantü.
- Müli ñi nentuñmageael fey ti chi bateria kimfale ñi koneltulen kiñe weza aplicación petu güneytulu taiñ chumeken, welu kom che mülelu kiñe trawün mew ka femle fey ka pegeluway ñi kom gütramkawkülen ñi femael kimgenual ñi chumeken ta che.
- Müley fentren aplicaciones teléfono geael ñi pepi koneltugenoael pu weza ke zugu kam allmaltugenuael ta che, kam ñi ñamümgeael kiñe ke wirin , müley kiñe azkünuwün chew fey ti chi allmaltupelu pepi chillkatulayafi tati pu zugu, ka fey mew pepi nentugetuy kiñe troy zugu kam wirin , welupegele ti che ñi femeken ka femechi wezalkageafü.

**6. fey ta chi mensajería
segura pigechi zugu**



Mensajería segura

6. Mensajería segura

Whatsapp

6.1a ¿Qué es?

Es una aplicación de mensajería digital instantánea gratuita. Utiliza un protocolo de cifrado de extremo a extremo para todas las comunicaciones. Es decir, los mensajes que salen de tu teléfono móvil o computador son transformados a algo que no se puede entender (o cifrados), y sólo se descifran cuando llegan al móvil del receptor. De esta manera, si alguien los intercepta por el camino, no podrá leerlos. Cuenta con una versión para computadoras pero no ofrece todos los servicios disponibles en la aplicación móvil. Todo lo que hagas en la web se sincronizará y se mostrará en la aplicación de iPhone o Android.

6.2a ¿Para qué sirve?

Ofrece el intercambio de mensajes, video, audio, imágenes, documentos y llamadas de una forma simple. Está disponible en teléfonos celulares y en formato web en todas partes del mundo. Cabe destacar que:

- Sabemos que hoy en día la transmisión de los mensajes entre usuarios de Whatsapp utiliza un protocolo considerado seguro (Signal), sin embargo, el código de la aplicación y sus servidores no permite auditar cómo están implementadas las medidas de seguridad.

6. Wirin zugulwe

Whatsapp

Amulkawe zugu zugun mew, wirin mew ka azentun mew.

6.1a Chem am

Tüfa gey kiñe aplicación chew amulgekey zugu ka fey mew kulligekelay. Fey ta mew koneltuley kiñe troy chew fey ti chi zugu amulgekelu fey puwle computador mew pepilfaltulay kam ka az nietuy ñi kimgenuam chem zugu ñi amulnien ta che. Fey mew ka küme llowtufi fey ti che ñi amulelgelu ti zugu. Fey mew katrükönküle ka che kam katrütüfile ti zugu pepilfal-lay. Ka fey müley kiñe troy nieael computador mew welu fey ta nielay kom zugu nielu fey ti chi nielu teléfono mew, fey kom tami femün computador mew pegengetuay tati aplicación iPhone kam Android mew.

6.2a Chem zugu mew am pünegekey.

Fey ta mew amulgekey wirn zugu, azentun, zugun kam nentu az , chillka . fey ta pepi niegey teléfono mew ka web mew ka femechi pepi pünegey welu müli kimtukunigeael.

- Kimnieyin ñi fantenmu fey ta chi zugu nielu tüfachi Whatsapp niey kiñe azelkan ñi kumeaz nien(signal pigey) welu fey ta chi rakin wirin nielu ka fey ti pu servidore pilayegün ñi kimgael chumechi am nieyegün fey ta chi kuñiwuwün kam ñi kake che ñi kimnoael chumken ta che faw.

- El modelo de negocios de Facebook, la empresa detrás de Whatsapp, está basado en la entrega de publicidad y recopilación de datos de los usuarios para generar una mejor segmentación, con varios episodios negativos en términos de privacidad de sus usuarios.

6.3a ¿Qué se recomienda?

Algunas medidas posibles de implementar apuntan a evitar escenarios de riesgo. Estas prácticas cobran particular relevancia para todos aquellos que, por su trabajo, se encuentran particularmente expuestos a convertirse en blanco de ataques. Tales recomendaciones pueden resumirse en la forma siguiente:

- Evitar usar Whatsapp para comunicaciones sensibles.
- No habilitar los respaldos en la nube del historial de conversaciones.
- Borrar frecuentemente las conversaciones del equipo celular.
- Comprobar frecuentemente qué equipos están afiliados a Whatsapp Web en tu dispositivo móvil.
- Mantener bloqueos de pantalla en los dispositivos móviles lo más difíciles de vulnerar posibles, como contraseñas largas o con factores biométricos.
- No desatender los equipos móviles en ningún momento. Por ejemplo, entregar en custodia para acceder a algún recinto o sala de reuniones.
- No cargar los dispositivos móviles en computadoras, especialmente si no son de confianza.
- No instalar aplicaciones ni abrir enlaces de dudosa procedencia o confianza.

- Fey ta chi troy zugu facebook tripalu ka fey ti chi trokin güne nielu whatsapp aznieyegün fey ta pegeluwam kake zugu ka fey ti chi pu che ñi koneltulelu zugu mew ñi kimgeael chem ñi zuamün fey mew kiñekemew müte kuñiwtukelay fey ti pu che nielu fey ta chi pu aplicación.

6.3a Chem zugu müli taiñ kimtukunieael

Kiñeke azkunuwün rupanual wezake zugu . tüfa chi pu troy zoyelfali fey ti chi pu che ñi küzaw ñi zuam allmaltugeafüy, fey ta chi pu zugu famechi troytuley.

- Müli amulnuael zugu whatsapp küpa kimfalgenulel.
- Müli taiñ nienoafel fey ti elgepeyüm gütram, nube pigelu.
- Ñi nentugeatuael Whats App mew tripachi gütram
- Müley taiñ allmaltuael chuchi ke equipo nielu WhatsApp web nüwküley tami teléfono mew.
- Müley taiñ nieal fey ti chi kake che ñi konoael taiñ telefono mew fey ti pepilfalnuael pegeafiel ka alükechi contraseña kam fey ti llowkelu azentun.
- Ñi el kunünuael tami teléfono chew norume, trawün che mew kam gütramnentun mew.
- Koneltugenuael teléfono computador mew , kake che mew.
- Müley taiñ nakümnoaefiel fey ti chi aplicaciones kagentufal kam kingelu chew tuwün.

B. Signal

6.1b ¿Qué es?

Es una aplicación de mensajería digital instantánea gratuita. Utiliza un protocolo de cifrado de extremo a extremo para todas las comunicaciones. Es decir, los mensajes salen de tu teléfono móvil o computador ya cifrados, y sólo se descifran cuando llegan al móvil del receptor. De esta manera, si alguien los intercepta por el camino, no podrá leerlos. Cuenta con una versión para computadoras.

6.2b ¿Para qué sirve?

Permite enviar mensajes de texto, fotos y vídeos, documentos, hacer llamadas y videollamadas, GIF, contactos, ubicación y archivos de forma gratuita, al igual que otras aplicaciones como WhatsApp.

Se pueden activar o desactivar los recibos de lectura, activar o desactivar los indicadores de escritura, elegir si deseas que las llamadas aparezcan o no en tu lista de recientes y elegir retransmitir todas las llamadas a través de un servidor de señal para evitar revelar tu dirección IP.

6.3b ¿Qué se recomienda?

Activar mensajes que desaparecen.

- Si deseas que los mensajes enviados y recibidos en un chat desaparezcan cuando se hayan visto, activa las funciones Desaparecer mensajes.

B. Fey ti chi signal pigelu

6.1b Chem am

Fey ta kiñe aplicación chew amulgekey zugu pürum ka kulligekelay. Fey mew zapillküley fey ta ñi kimgenuael chempiwmeken ta che , fey ta chi zugun tripay tami teléfono mew fey ka az niey fey puwlu chew ñi amulgel fey mew ka wiñoazgetuy. Fey mew katrüntukugele petu ñi puwnon fey kimfalay chem zugu amulen fey mew. Ka femechi müley kiñe az ñi niegeam computador mew.

6.2b Chem zugu mew am pünegekey

Fey ta mew pepi amulgey wirin, azentun, chillka, ka pepi zuguluwüy che pewüy ta che , Gif, ka niey fey ti iney gen, chew mülen ka chew ñi elam pu chillka fey ta kulligekelay fey Whats App reke feley.

Fey ta mew pepi niey kam nielay che fey ti ñi kimgeael ñi chillkatugen tizugu amuelel kam femnuael ka ñi müleal fey ti chi üy ineywen ñi zuguluwpen ta che ka ñi ka amulgeael ti zuguluwün kiñe servidor de señal mew chew ñi kimgenuael iniygen ta che kam tami dirección IP pigelu.

6.3b Chem zugu müli taiñ kimtuniegeael.

Ñi ñamnagal ti pu wirin

- Pilmi ñi ñamnagal ti pu wirin inagechi ñi amulgen ka ñi llowgen müley tami azkünueafiel chew feypile Desaparecer mensajes.

- Abrir el chat> Tocar el nombre del contacto en la parte superior para acceder a la configuración> Activar / Desactivar mensajes> Usar el control deslizante para elegir la hora a la que desea que desaparezcan los mensajes.
- Las opciones de tiempo son: 5 segundos, 10 segundos, 30 segundos, 1 minuto, 5 minutos, 30 minutos, 1 hora, 6 horas, 12 horas, 1 día o 1 semana.

Desactivar recibos de lectura

- Desactivar los recibos de lectura se desactivan para todos los chats y tampoco los verás para los mensajes enviados.
- Abrir Signal> Tocar el ícono de tu cuenta en la esquina superior izquierda> Privacidad> Alternar en los recibos de lectura.

Apagar los indicadores de escritura

- Desactivar los indicadores de escritura se desactiva para todos los chats y, al igual que con los recibos de lectura, tampoco los verás cuando se escriban mensajes.
- Abrir Signal> Tocar el icono de tu cuenta en la esquina superior izquierda> Privacidad> Activar los indicadores de escritura.

Eliminar un mensaje

- Puedes eliminar un mensaje después de enviarlo, tal como lo hace WhatsApp, Abrir el chat> Mantener presionado el mensaje que desea eliminar> Tocar el ícono de la papelera sobre el teclado en iOS, o el ícono de la

- Gülafige ti amulzugulpeyüm inagechi chew müley ti üyche wenuntu fey mew müley chew azkünugekey fey mew müli tami feypial ñi elafiel kam femnual pu wirin zugu, ka müli tami zulliael chem troy antü mew ñi ñamnagal ti pu wirin.
- Fey ti chi pu troy kechu segundos, mari segundos, küla mari segundos, kiñe minuto, kechu minuto, küla mari minuto, kiñe hora, kayu hora, mariepu hora, kiñe antü kam kiñe semana.

Nentutuafiel fey ti chi zew chillkatugen ti amulzugun

- Nentutuafiel fey ti chi pu wirinzugu fey nentutukey kom ti pu wirin mew ka fey ti chi wirin amulfel ta eyimi.
- Koneltufilmi signal güpafige chew müley tami cuenta wenu wele püle, chew feypiley privacidad, fey mew feypiley ñi weluketu müleael fey ti llowlu ti wirin kam chillkatufilu.

Chogümafiel ti kimelkel ñi wirinutkumeken

- Nentutuafiel fey ti chi kimelkel ñi wirinutkumeken ta che kom fey ti chi wirin mew ka femechi fey ti llowfiel ka chillkatufiel, ka pelayafimi wirinutkumeken ti zugu.
- Koneltufilmi signal güpafige tami cuenta wenu wele püle chew feypiley privacidad fey mew müli tami nieafiel fey ti chi feypilu ñi wirimeken che.

Ñamnagtuael wirin

- Pepi ñamnagfali fey ti chi pu wirin inagechi ñi amulfel chumechi femgekey Whats App mew, koneltugekey chew wiripeyüm inagechi güpanakümfige fey ti pu wirin tami ñamnakümafiel. Inagechi chew puwkey pu

papelera en la esquina superior derecha de Android.

Activar el bloqueo de registro

- Activar el bloqueo de registro significa que se requiere tu PIN de Signal para registrar tu número de teléfono con Signal nuevamente. Si olvida su PIN de señal, se le bloqueará tu cuenta durante siete días.
- Abrir Signal> Tocar el icono de tu cuenta en la esquina superior izquierda> Privacidad> Activar / desactivar Bloqueo de registro.

Vincular / desvincular un iPad o computadora portátil

- Si deseas ver tus chats de Signal en otro dispositivo, como tu iPad o tu computadora portátil, deberás descargar Signal a la plataforma y seguir las instrucciones a continuación.
- Abrir Signal en ambos dispositivos> Haz clic en el icono de tu Cuenta en la esquina superior izquierda de la aplicación de tu teléfono> Dispositivos vinculados> Vincular nuevo dispositivo> Escanea el código QR.
- Para desvincular un dispositivo vinculado: Abra Señal> Haz clic en el icono de tu cuenta en la esquina superior izquierda de la aplicación del teléfono> Dispositivos vinculados> Toca Editar en la esquina superior derecha> Elimina el dispositivo que deseas desvincular.

Cambiar lo que se muestra en una notificación

- Las notificaciones de llamadas y mensajes pueden aparecer cuando el teléfono está bloqueado, pero es posible que solo desee que aparezca información específica, o casi ninguna información.

chillka ka chew wirigepeyüm fey iOS kam chew puwkey pu chillka wenu manpüle Android mew.

Nieafiel ñi genuael wirintukun

- Nieafiel ñi genuael wirintukun zuamyey kiñe PIN pigechi zugu tripalu Signal mew fey mew elgekey número feymu gechi fey goymafilmi tami PIN fey pepi koneltulayami regle antü mew tami cuenta mew.
- Koneltual signal ka tami cuenta mew wenu wele püle privacidad mew fey niefiel fey ti chi genuael wirintukun.

Nüwküleal kam femnual kiñe iPad ka computadora portátil pigechi zugu..

- Küpa pelmi tami wirinzugu ka dispositivo mew iPad mew kam computadora mew müli tami nieafiel signal chew ñi makümgeken fey tami femal chem wirintutripayel fey mew.
- Epu dispositivo mew nieael signal, chew müley tami cuenta wenu welepüle tami teléfono mew chew wirintukuley chuchimew ñi nüwkülen fey inagechi müli tami azentuafiel kiñe código QR.
- Nüwkülenuam epu dispositivo, koneltual señal, chew müley tami cuenta wenu manpüle, fey mew nentufige fey ti chi dispositivo ñi nüwkülenuael.

Welukütü pewfaluwkel chem ñi rupayen faw

- Feypigekey che chem ñi nien kam llowün ñi zugugepen kam mütrümgepen fey mew müley tami küpa kimün kam kimnuael tami llowkülen kam femnun fillke zugu.

- Abrir Signal> Haga clic en el icono de tu cuenta en la esquina superior izquierda de la aplicación de su teléfono> Notificaciones> Mostrar> Elige entre Nombre, contenido y acciones, Solo nombre y Sin nombre o contenido.

Enviar una vista solo una vez

- Es posible que desees enviar una imagen pero solo permitir que el destinatario la vea una vez. Tal vez una selfie muy mala. Sin embargo, ten cuidado ya que el destinatario aún puede capturar la imagen y Signal no le dice si lo hace.
- Abrir Signal> Abra el chat> Toca el ícono "+" en la esquina inferior izquierda al lado del campo de entrada del mensaje> Selecciona el ícono Galería o desplázate por tus fotos> Selecciona la imagen> Toca el ícono del círculo con el enlace esquina inferior izquierda para cambiarlo a un círculo con un 1x en el medio> Presione la flecha azul en la parte inferior derecha para enviar.
- Si desea enviar una nueva foto tomada con la cámara en la aplicación Signal: abrir Signal > Abra el chat> Toca el icono de la cámara a la derecha del campo de entrada del mensaje> Toma la foto> Toca el icono del círculo con el enlace en el medio para cambiar al círculo con 1x> Presiona la flecha azul en la parte inferior derecha para enviar.

Eliminar llamadas de Signal de listas de llamadas

- Es posible que no desees que tus llamadas Signal aparezcan en tus registros de llamadas. En tal caso:
- Abrir Signal> Haz clic en el icono de tu Cuenta en la esquina superior izquierda de la aplicación de tu teléfono> Privacidad> Activar

- Koneltual signal mew chew müley tami cuenta wenu wele püle aplicación teléfono mew, notificacion pilelu, müley ñi pegelafel fey mew azümkafige chem tami piel.

Amulael pen zugu kiñe rupa müten.

- Amulfilmi kiñe azentun , fey ti llowalu peafile kiñe rupa müten, kiñekewmew küme tripakelay azentun, fey mew fey ti llowlu pepi nentuafüy fey ti azentun, fey ti Signal feypikelay ñi femün.
- Koneltufige Signal, inagechi fey ti chi amulkawe zugu wele püle nageltu inaltu chew müley ti llowkelu wirin zugu müley chew ñi mülen pu azentun fey mew koneltuge, fey zullifige kiñe azentun fey mew müley kiñe wall fey nüwküley ka kiñe zugu mew fey mew müley nageltu wele püle fey müli ka kiñe wall ragiñ mew, ka fey müley kiñe kallfu waiki reke nageltu manpüle.
- Küpa amulülmi kiñe azentun fey ti chi signal mew koneltufige fey ti wirinzugulwe chew müley ti cámara manpüle chew llowgekey zugu, nentufige ti azentun ka güpafige ti wall chew feypile kiñex fey ka güpafige fey ti kallfu waiki reke amulafel.

Ñamümnagal fey ti zuguluwün zugu mütrümüwün fey ti chi wirin mew.

- Küpa nienofilmi fey ti chi wirin inayeymu tami zuguluwkel fey tüfa kiñe zugu,
- Koneltufige ti signal tami cuenta mew wenuwele püle tami teléfono mew chew privacidad feypiley, müley tami feypiafel ñi pegengeafel kam femnuael iney am

Mostrar llamadas en recientes.

- Dejar de aparecer la señal en el selector de aplicaciones.
- Es posible hacer que solo la pantalla azul de Signal aparezca en el selector de aplicaciones en iOS, lo que impide que pueda ver la pantalla de chat.
- Abrir Signal> Haz clic en el icono de tu cuenta en la esquina superior izquierda de la aplicación de tu teléfono> Privacidad> Activar Activar seguridad de pantalla.

Activar bloqueo de pantalla

- Activar el bloqueo de pantalla te permite requerir Touch ID, Face ID o su contraseña de iOS para desbloquear la pantalla de Signal. Es una capa adicional de seguridad.
- Abrir Signal> Haga clic en el icono de su cuenta en la esquina superior izquierda de la aplicación de su teléfono> Privacidad> Activar/desactivar bloqueo de pantalla.

Para mayor información visitar <https://signal.org/es/>

zuguluwpeymu.

- Ñi pegengenuael fey ti chi zullikeyel aplicaciones pigechi zugu..
- Kiñe ke mew re pegengekey fey ti kallfu az fey ti chi selector de aplicaciones mew, ¡OS pigelu, fey ta rupalay ñi pegengeal chew amukey ta wirin zugu.
- Koneltuafel signal, inagechi tami cuenta fey wenu wele püle ti aplicación mew privocidad piley fey mew müley tami feypiafiel chem ñi chumal.

Pegenuael ti az teléfono.

- Femneafel ñi pegengenuael chem az nien tami teléfono fey zuameyegey Touch ID pigelu ka Face ID pigelu kam fey ti chi contraseña ¡OS ñi nentugetuael fey ti chi az signal mew. Fey ta kiñe güfküntukun zugu reke ñi kimüñmagenuael tami zugu.
- Koneltufige Signal inagechi tami cuenta mew wenu wele püle müley fey ti chi privacidad pilelu fey mew inagechi koneltuafimi fey ti ñi chumkunuafeke tami pantalla.

zoy küpa kimülmi fey ta chi zugu koneltufige faw: <https://signal.org/es/>

7. Phishin pigechi zugu



Phishing

7. Phishing

7.1 ¿Qué es?

El phishing es una técnica de ataque digital, que consiste en engañar a las personas para que compartan información confidencial como contraseñas y datos personales, y otras acciones indeseadas. Un ataque de phishing tiene tres componentes:

- El ataque se realiza mediante comunicaciones electrónicas, como un correo electrónico o una llamada de teléfono.
- El atacante se hace pasar por una persona u organización de confianza.
- El objetivo generalmente es obtener información personal confidencial, como credenciales de inicio de sesión o números de tarjeta de crédito.
- La mayoría de los mensajes de phishing usan estas historias para llamar nuestra atención:
- Problemas de facturación.
- Las autoridades van por usted.
- Alguien quiere darle dinero.
- Ha ganado un gran premio.
- Negocio urgente.

7.2 ¿Para qué sirve?

- Buscar engañar a la víctima para que entregue información sensible, descargue un archivo infectado o ingrese su contraseña en una página web.
- Eliminar nuestras cuentas de correo, redes sociales o bancos al darle nuestra contraseña

7. Phishin pigechi zugu

7.1 Chem am

Fey ta ti Phising allmaltun digital zugu mew , fey mew welulkagekey che ñi wülal ñi iney gen , wülal ñi contraseña kam kake sugu. Fey ta chi zugu mew müley ta ñi müleael küla troy.

- Fey ta chi wezakan zugu tripakey amulzuguyim wirin zugu mew kam kiñe correo mew kam kiñe zugulkawe mew.
- Fey ti femekelu ka che reke zugukey kam kiñe trokin che mew .
- Kizuegün ñi zuam kimael ka nentuymayafiel ñi ineygen ti che chem zugu mew koneltulen chew ñi nien rang.
- Epe kom fey ta chi pu zugu feypikey kiñe ke tüfa ke chi zugu.
- Pepi nentunael reke kiñe zugu.
- Fey ta pu karü yemeaymew.
- Elugealu rang ta eyimi
- Llowalu kiñe premio pigekey ta che
- Kiñe negocio müchay müten ñi tripayael.

7.2 Chem zugu mew am koneltuley.

- Zuamniey ñi wezalkayal ta che ñi wülal ñi iniygen kam ñi llowal kiñe weza chillka kam wülal ñi contraseña kiñe wirin web mew.
- Ñamüm mageael taiñ cuenta correo mew, kam redes sociaeles mew kam banco mew chi, nieñmageliyin taiñ contraseña fey ka

al atacante, quien puede cambiarla y dejarnos afuera de nuestras propias cuentas.

- Publicar información haciéndose pasar por nosotros, haciendo que nuestros contactos también caigan en el mismo ataque.
- Extraer información sensible, como comunicaciones secretas o íntimas, al tener acceso a nuestras cuentas con las claves extraídas.

7.3 ¿Qué se recomienda?

- Desconfiar de mensajes que piden tomar acciones rápidas o de urgencia: estos mensajes se aprovechan de exaltar situaciones de riesgo o emergencia para convencer a la víctima de tomar acciones apresuradas.
- Antes de tomar cualquier acción verifica en páginas oficiales: Si tienes sospechas de que la información que recibes puede ser cierta, la recomendación es que verifiques la información directamente en las páginas oficiales de las entidades bancarias, compañías de correo, entre otras, según sea el caso. Si, por el contrario, el mensaje de alarma que recibiste no se refiere a cuentas comprometidas sino a personas o familiares en riesgo, la sugerencia es que, antes de tomar cualquier acción, intentes contactarte directamente con la persona aparentemente afectada. En ninguno de estos casos es recomendable seguir vínculos incluidos en el mensaje sospechoso.
- Comprobar el emisor del mensaje: Si pretende ser un mensaje de parte de una red social o proveedor de correo electrónico, asegúrate que las cuentas de correo utilizadas sean las oficiales.
- Mantener actualizado el software: Los ataques de phishing que utilizan aplicaciones maliciosas con frecuencia se basan en vulne-

contraseña tukutuafüyegün fey inchiñ pepi koneltuwelafüyin fey mew.

- Amulafüy wirin egün inchiñ ñi üy mew, fey kake che feyentuafüy fey ka wezalkageafüyegün.
- Llowafüy kiñeke zugu inchiñ müten ñi kimnieel kam kake zugu mew, nielegün taiñ clave.

7.3 Chem zugu müli taiñ kimtukunieael.

- Kuñiwtuleael fey ti chi pu wirin llowkelu inchiñ kimfalnole iniygen kam chem zugu koneltulen , fey mew amulgekey fey ti pu che ñi llowafiel ka ñi rakizuamnuael ta che re matu ñi wiñolzuguael.
- Petu ñi wülnoel zugu müley taiñ güneytuafel ñi rüf zugu gen kam feygenun müli taiñ küme güneytuafel chew ñi tuwün ti wirin , chem zugu mew ñi nüwkülen , welu ka zugu gele nüwkülelñi che ñi wezalkalen kam chemkún zugu ñi rupañ reñma mew wüne müli taiñ kimael ñi rüf gen, müli taiñ mopitunuafel fey ta chi pin pürkachi ka ñi koneltunuafel fey ti chi zugu kimgenun ñi rüf gen kam femnun.
- Müli taiñ kimael iniy am inakonküley ti wirin mew , nüwkülele kiñe red social mew kam correo electrónico mew müli kimgeael ñi rüf zugu gen.
- Müli taiñ wenuntinieal tati software; fey mew Phishing pünekeyegün wezake aplicación fey chi ke rupalu pu software mew

rabilidades en el software para comprometer tus dispositivos.

- Utilizar un administrador de contraseñas con relleno automático y de usuario y contraseña: Los administradores de contraseña que tienen esta característica, alojan los datos asociados a la dirección donde se completa esta información. Si el atacante consigue dirigirte a un sitio web malicioso, tu administrador de contraseñas no reconocerá el lugar que pretende acceder a tu información.
- Usar Google Drive para previsualizar documentos. En lugar de descargar directamente los documentos que recibas. Google Drive convierte el documento en una versión web, impidiendo la instalación de aplicaciones maliciosas en tus equipos.
- Activar la autenticación de dos factores. Ver autenticación en dos factores (2FA) de tal modo que el atacante no pueda ingresar a tus cuentas de usuario, a pesar de que llegara a tener la contraseña de acceso.
- No descargar ningún archivo, instalar software o abrir ningún enlace web antes de verificar su procedencia y veracidad: para verificar a dónde se dirige un link acertado te recomendamos utilizar unshorten.me o unshorten.it

Nota. Si te piden que proporciones información confidencial, comprueba que la URL de la página comienza con "HTTPS" en lugar de simplemente "HTTP". La "S" significa "seguro". No es una garantía de que un sitio sea legítimo, pero la mayoría de los sitios legítimos utilizan HTTPS. Los sitios HTTP, incluso los legítimos, son vulnerables para los hackers. Si no puedes ver si el sitio dice HTTP o HTTPS, busca un candado junto a la dirección de la página, si está y

ñi wezalkageñmayal taiñ dispositivo.

- Müli taiñ nieal administrador de contraseña chew kizuke wülkey kom, iniygen ka ñi contraseña, fey ti chi administrador de contraseña llownieyegün chew ñi tuwün ti zugu kam chew ñi koneltugeael ta che , fey mew koneltugelmi wezalkageael fey ti chi administrador de contraseña koneltulayay.
- Müley taiñ azkintuafiel pu chillka google drive mew , ñi nakümnuafel pürkachi, fey ti chi google drive rulpatukefi chillka web mew, fey mew katrütugeki reke ti weza aplicación koneltunuael taiñ equipo mew.
- Müley taiñ nieafel fey ti chi autenticación de dos factores. Koneltuafel fey ta chi zugu , fey mew koneltulalay fey ti chi che wezalkan pilelu, fey mew puwlayay tami contraseña koneltuwal zugu mew.
- Taiñ nakümnoael fey ti chi pu chillka kam software kam wirin web kimgenun chem gen kam chew tuwün, fey tami kimael ñi chem zugu gen müley fey ta chi epu zugu unshorten.me o unshorten.it

Ka kiñe troy: feypigelmi tami wülal iniygen ta ey mi wüne güneytufige ñi llitun HTTPS re feypilele HTTP". Fey ta chi S feypiley ñi mopitufal zugugen. Welu kimfalay ñi rüf rüf zugu gen , welu fey ta ke chi rüf zugu gelu feypilekey HTTPS, welu fey ti chi pu HTTP chumte rüfgeafüy welu fey ti chi pu wezalkakeku zugu faw pepi koneltuafüyegün. Welu pepi güneytunufilmi ti pu wirin HTTP kam HTTPS, azkintufige kiñe candado

se ve cerrado usa HTTPS, si no, usa HTTP.

Para más información ir a:

- <https://phishingquiz.withgoogle.com/.https://phishingquiz.withgoogle.com/>
- <https://www.avast.com/es-es/c-phishing>
- <https://es.malwarebytes.com/phishing/>

güfkükönkülele fey ta HTTPS, welu gülälele fey ta HTTP.

zoy küpa kimtukulmi zugu koneltuge faw

- <https://phishingquiz.withgoogle.com/.https://phishingquiz.withgoogle.com/>
- <https://www.avast.com/es-es/c-phishing>
- <https://es.malwarebytes.com/phishing/>

**8. Fey ta chi
protección de
dispositivo
pigechi zugu.**



**Protección de
dispositivos**

8. Protección de dispositivos

8.1 ¿Qué es?

Es el conjunto de medidas que podemos tomar para asegurar nuestros teléfonos, computadoras, grabadoras, cámaras y cualquier otro equipo en donde guardemos información sensible.

8.2 ¿Para qué sirve?

Para proteger la información de que caiga en manos equivocadas.

8.2.1 Riesgos

- Los equipos pueden ser manipulados por personal equivocado y volverse inaccesibles, o ser filtrados a terceros no autorizados.
- Los equipos pueden ser confiscados para extraer información sensible.
- Los equipos pueden dañarse, perderse o ser robados, pudiendo perderse la información contenida en ellos si no se dispone de una copia en otra parte.

8.3 ¿Qué se recomienda?

Cifrar archivos: Es recomendable cifrar tus archivos en los dispositivos que los contienen para evitar que terceros puedan acceder a ellos frente a situaciones de robo, extravío, entre otras. Este cifrado puedes llevarlo a cabo de las siguientes maneras:

- Cifrado completo de disco duro: A través de la activación de FileVault (usuarios MacOS),

8. Zapillnieel reke pu dispositivo.

8.1 Chem am

Kiñe epu troy chew zapillnieayin reke taiñ teléfono , taiñ computadora, taiñ grabadora, taiñ cámara, kam kake troy zugu taiñ nieel kam chew taiñ koneltunieel inchiñ taiñ zugu müten.

8.2 Chem zugu mew am koneltuley

Kañpüle kam kake che mew amunueal inchiñ taiñ zugu.

8.2.1 Chem zugu mew müli taiñ kuñiwtualeal.

- Taiñ pu equipo kake che mew puwle fey ta wezalkageafüyiñ kam kañpüle amuafüy taiñ zugu.
- Kam muntuñmageafüyiñ taiñ equipo ñi kimageael taiñ chumken.
- Taiñ equipo wezalkawüy, kam ñamafüy kam weñeymageafüyiñ ka femechi amulkayafüyiñ fillke zugu taiñ koneltuniel fey mew.

8.3 Chem zugu muli taiñ kimtukunieal.

Nieael taiñ azelkanieal cifrado mew: fey mew kake che azümlayafi tami pu zugu weñeymagelmi rume kam ñamümfilm rume kam ka zugu mew. Fey ta chi zugu tripayafüy famechi:

- Müli taiñ niel fey ti chi cifrado müllomureke taiñ equipo mew, fey mew tripayafüy FileVault (nielu MacOS), Bitlocker (nielu

Bitlocker (usuarios Windows), LUKS (usuarios Linux) o Veracrypt (para cualquier sistema operativo). Para activar el cifrado del disco completo es necesario configurar con contraseña de acceso al equipo que impida que terceros puedan obtener la información. extraer el contenido del disco fácilmente aún sin tener la contraseña de acceso.

- Cifrado de otros volúmenes de almacenamiento: Una alternativa al cifrado completo del disco duro es cifrar volúmenes de almacenamiento extraíbles tales como unidades USB o volúmenes específicos en el disco duro. Las herramientas que permiten llevar esto a cabo son VeraCrypt (usuarios MacOS y Windows) y BitLocker (usuarios Windows).
- **Borrar archivos:** Al eliminar un archivo en tu computadora, o incluso enviarlo a la “papelera”, realmente no estás borrando la información, solo estás indicando que ese espacio que ocupa el archivo se sobrescribe en cualquier momento con información nueva. Por tal motivo, es posible recuperar los datos “borrados” con algún software disponible o métodos forenses.
- Utilizar programas especializados como CCleaner o Eraser que sobrescriben el espacio que ocupaba la información “eliminada” de forma que haría muy difícil su recuperación si deseas borrar de forma segura la información contenida en unidades de disco tradicionales no en los discos de estado sólido (SSD) o en unidades USB. **Nota.** BitLocker no está disponible en Windows 10 Home.
- Activar el cifrado completo de disco en conjunto con otras estrategias de respaldo y otras medidas adicionales tales como evitar llevar consigo los equipos con información

Windows), LUKS (nielu Linux) o Veracrypt chuchi rume sistema operativo nielu. Ñi nieael cifrado fey ti chi troytuwe zugu mew zuamyefali ñi azelkageael contraseña koneltuam zugu fey ti chi equipo mew, pepi koneltunuael kake che allmaltuael zuh , nentuael fillke zugu fey ti chi disco me , nienun rume fey ti chi contraseña koneltuam zuugu mew.

- Nieal ti cifrado fey kake troy mew chew elegekey kom zugu mu chi kam kiñe troy mu, fey mew pepi koneltugey fey ta chi VeraCrypt (nielu MacOS y Windows) y BitLocker (nielu Windows) mew.
- **Nentutuael wirikan zugu kam troy zugu:** nentugetule kiñe troy computadora mew kam amulgele ti papelera mew, feyta rüf nentugekelay re ta feypileymi chew tami elafel, fey mew ka pepi wiñotukey fey chi troy nentutufilu ta eyimi kiñe software mew kam fey ti chi método forense pigelu chew.
- Müli taiñ nieael kiñe troy zugu CCleaner kam Eraser feypigelu fey mew wente fey ti chi nentutufiel troy mew eluwkey, fey mew pepi wiñotulayafüy fey ti chi troy nentugelu, fey mew rüf küpa nentutulmi kiñe troy tami disco mew kam fey ti pu disco estado solido pigelu kam fey ti chi pu USB pigelu . troy wirin: BitLocker gelay fey ta chi Windows 10 Home mew.
- Nieael tati cifrado kom ti disco mew ka kake kuñiwuwün mew taiñ wezalkagenuael, ka kañpüle amualiyiñ müley taiñ miawnoael taiñ pu equipo nieliyiñ kiñe zugu taiñ

sensible durante viajes para la protección de los archivos contenidos en estas unidades. El borrado seguro en unidades SSD, unidades flash USB y tarjetas SD es muy difícil debido a su diseño.

Respaldar Archivos: Para garantizar la disponibilidad de la información es importante que puedas hacer respaldos o copias de seguridad de tus archivos. Lo recomendable es que los respaldos se realicen a través de servicios/herramientas seguras y tomes en cuenta los siguientes criterios sobre tus copias:

- En internet
- Cifradas
- Ubicación física distante al o los sitios que pueden ser vulnerados
- Frecuentes
- Copias incrementales
- Fácil restitución.

Nota. Tomar en cuenta la estrategia de respaldo llamada “Backup 3-2-1” que consiste en:

- Tener al menos tres (3) respaldos de tus datos.
- Almacenarlas en dos (2) medios diferentes (físico y virtual).
- Conservar una (1) copia en un lugar fuera de las instalaciones que podrían ser vulnerables.

kimgenuael. Kiñe az mew feyta chi unidades SSD, unidades flash USB kam tarjetas SD pepi nentuñmagekelay rüy pu zugu.

Taiñ kañpüle ka nieal fey ti azentun reke:

taiñ nieafel ka kiñe troy zugu kiñe azentun reke chew kafeley taiñ zugu, chillka itrokom müli taiñ nieafel küme troy zugu mew ka müli tami kimnieal kiñe zugu.

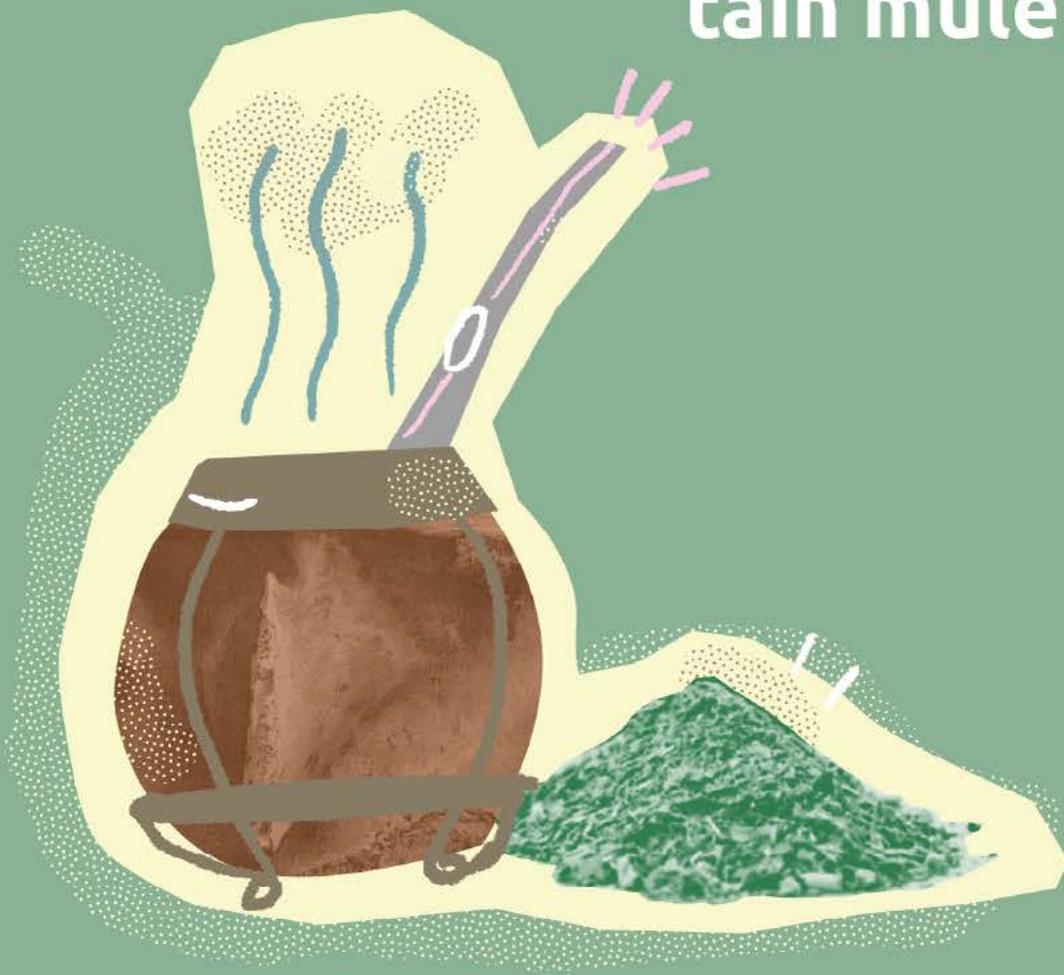
- Internet mew
- Cifrada nieafel
- Chew ñi mülen müte püchütripa ñi mülenuael
- fillantü
- Azentun reke kiñe epu troy mew.
- Pepi wiñoniegefalel

Wirin troy: ñi güneytuafiel fey ta chi elkünuam zugu Backup 3-2-1” pigelu chew tripay.

- Müli taiñ nieafel külatroy mew chew taiñ elal taiñ zugu.
- Epurume elfalmew elafel pegepeyüm ka virtual zugu mew.
- Kañpüle ka ñi elal taiñ zugu, chew ñi koneltugenuael.

9.

fey ta chi
Protección de
información
físico, chew
taiñ mülen



Protección de
Información en físico

9. Protección de Información en físico

9.1 ¿Qué es?

Es el conjunto de medidas que podemos tomar para asegurar los datos recopilados de forma física o tangible, tales como una pieza de papel o un documento de identidad.

9.2 ¿Para qué sirve?

Para proteger la información de que caiga en manos equivocadas.

9.2.1 Riesgos

- La información en físico puede ser extraída por cualquiera que tenga acceso a ella, esto incluye a cualquiera que confisque la información o a ladrones que la roben.
- Puede dañarse en el caso de incendios, inundaciones o deterioro general entre otros.

9.3 ¿Qué se recomienda?

- Mantener la menor cantidad posible de información física: especialmente si esta información puede resultar peligrosa en caso de filtración o pérdida. Una técnica puede ser digitalizar los documentos físicos y destruirlos.
- Mantener la información física muy sensible bajo llave: esto puede ser poco efectivo en eventos en donde somos forzados por vías legales o violentas a proporcionar la información guardada o cuando el lugar en donde se guarda es susceptible a ser violentado para

9. Zapillalreke taiñ zugu nieel ruka mew.

9.1 Chem am

Fey ta kiñeke kuñiwтуwün nieael fey ta chi pu chillka papel mew mülelu, üy mew nüwkülelu.

9.2 Chem zugu mew am koneltuley.

Taiñ kuñiwтуleael kake che mew ñi puwnuael taiñ zugu.

9.2.1 Kuñiwтуwün.

- Fey ta chi troy pepi weñeymageafüymi fey ta chi pu che kintuyawfilu fey ta mew chew rume puwafüy zugu fey ti chi muntulu kam wñelu.
- Kam lüfkonafüy, chapazafüy kam wezalkawüy.

9.3. Chem zugu müli taiñ kimtukunieael

- Müte nienoael fey ti chi zugu papel mew: zoyel fey ti chi zugu wezalkageael ta che. Kiñe troy geafüü rulpatuafiel digital mew fey inagechi getunoael fey ti papel mew mülelu.
- Güfkükönkünieafel fey ti chi zugu taiñ küpa pegelnoafel: welu fey ti pu zugu chew taiñ wezalkamegeken ruka mew ka femechi yegetuafüy.

burlar la seguridad disponible.

- Destruir información física de forma segura: dependiendo de qué tan sensible es la información, puede ser negativo sólo botarla en la basura, en donde puede ser buscada y reconstruida por terceros. Algunas técnicas comunes son triturar el papel, mojarlo o quemarlo entre otras.
- Müley taiñ rüf apümtuafel ti chillkantukulen zugu, re ütrüftukufiliyin pozwe mew ka femechi ka zewmagetuafüy reke kake che mew. Kiñe mew müli taiñ ko mew tukuafel kam lüpümafel.

10.

Kuñiwtulen redes
sociales mew.



Protección en
redes sociales

10. Protección en redes sociales

10.1 ¿Qué es?

Pueden definirse como páginas web que permiten a sus usuarios conectarse con otros usuarios, creando relaciones o comunidades. Su finalidad es servir como una herramienta online de comunicación entre personas de todo el mundo que comparten información en forma de imágenes, vídeos, texto o audio. Las más utilizadas en la región son Facebook, Twitter e Instagram. Pero cuidado, las redes sociales también pueden ser utilizadas por atacantes para comprometer nuestros datos, nuestra seguridad y privacidad.

10.2 ¿Para qué sirven?

Tienen múltiples propósitos, tanto personales como de trabajo. Los principales son:

- Crear conexiones y mantener las existentes.
- Mantenerse actualizado.
- Compartir nuestras ideas.
- Organizar comunidades con intereses afines.
- Construir una red de seguidores y ganar reputación.

10.2.1 Riesgos.

- Publicar en tu nombre en redes sociales. Tus conversaciones privadas podrían quedar expuestas.
- Las empresas detrás de las redes sociales y

10. Kuñiwtulen redes sociales mew.

10.1 Chem am

Fey ta geafüy web chillka reke chew pu che pepi koneltuy zugu kake che mew, chew kimuwkey ka zuguluwkey. Kiñekemew pünegekey taiñ kimüwal kake mapu mülechi zugu ka che, chew welulkawgekey ta zugu, kimün, azentun, chillka kam zugun. Zoyelniegen fey ta facebook, Twitter ka Instagram. Welu müli ñi kuñiwтуwleal ka femechi fey mew koneltuleafüy kiñe che wezalkageam che, nieymageam taiñ iniygen ka itrokom taiñ zugu.

10.2 Chem zugu mew am koneltugekey.

Kiñe epu zuam niey kiñe kizutuw che mew ka kiñe küzaw ñi zuam mew müley welu tufa kiñe zugu ñi m

- Kimael kake che ka kimuwküleal chumlen che ñi kimnieel .
- Kimtukunieael chem zugu ñi rupalen..
- Kimeltuael taiñ rakizuam, kimün kam zugu.
- Ñi trapümüwal kiñe zugu mew.
- Inageal ta inchiñ ka ñi falintugeael.

10.2.1 kuñiwтуn

- Wirintukuliñ taiñ üy mew redes sociales mew. kimgeafüy chem taiñ amulzugupen.
- Fey ta chi pu günenielu redes sociales kam kake che kimnieafüy kom tami pu che chuchi

cualquiera que comprometa tu cuenta tendrá acceso a tus contactos y documentación importante enviada/recibida.

- Problemas de seguridad.
- Puedes perder el acceso a la cuenta si cambian tu contraseña de acceso o los métodos de recuperación de cuenta alternativos: dirección de email, número de teléfono, etc.
- Suplantación de identidad y comprometer tu reputación.

10.3 ¿Qué se recomienda?

- Decidir si tu participación en la red social será a través de tu nombre real o un alias.
- Definir el correo electrónico que estará asociado a esa red social.
- Definir si mostrarás tu rostro en esa red social (dependerá si es una cuenta personal, de trabajo o anónima).
- Configurar una contraseña segura de acceso. Ver la sección Contraseñas de esta guía.
- Activar la autenticación de dos factores.
- Evitar sostener conversaciones sensibles a través de los chats o mensajes directos en redes sociales.
- Revisar las opciones de privacidad y seguridad. Por ejemplo, seleccionar si consideras conveniente que te encuentren a través de tu número de teléfono.
- Configurar las notificaciones de forma que puedan avisarte cuando exista una actividad sospechosa en la cuenta, por ejemplo, el intento de inicio de sesión en un nuevo equipo.
- Revisar las políticas de privacidad, en especial los datos que recoge el servicio, el uso

tami zugulkefel ka kom tami wirin chillka amulkefel ka llowkefel.

- Kūñiwuyawal kam pellkeyawal.
- Ñamümafüy tami cuenta kake che günefile fey ka contraseña tukutuafüy kam chew tami wiñonietuafiel tami pu zugu email kam teléfono chi.
- Eymi tami üymew reke zuguafüy kake che fey eyimi tami üy miawafüy weza zugu mew.

10.3 Chem zugu müli taiñ kimtukunieal

- Müley tami rakizuamal wirintukuael tami üy kam ka üytun mew koneltuael redes sociales mew.
- Müli taiñ zulliael chem correo electrónico ñi nüwküleal red social mew.
- Ñi günezuamal ñi pewfaluwal taiñ az fey kizu niey ñi az kam küzaw ñi zuam gele kam küpa pegelnoimi tami üy.
- Azkünuafel tami contraseña ñi pepilfalnual. Güneytuafel fey ta chi troy contraseña pigelu.
- Nieael autenticación de dos factores pigelu.
- Müli taiñ amulnoael fey ti chi zugu taiñ kimfalgenuael kake che mew.
- Güneytuafiel fey ti privacidad ka seguridad pilechi troy taiñ zugu mew rakizuamal ñi kümen kam kümenun taiñ pegeael taiñ número teléfono mew.
- Azelkayafel chew taiñ feypigeken ñi allmaltumekegen, kake che kontufalmekele taiñ cuenta mew kake equipo mew.
- Güneytuafel fey ti chi politica de privacidad troy zugu, chew ñi feypilen chem zugu

que le dan y cómo se comportan frente a la solicitud de información por parte de instituciones gubernamentales.

- Recordar que, aunque realices las configuraciones adecuadas, todo lo que publicas en las redes está potencialmente sujeto a hacerse público.
- Evaluar antes de publicar la conveniencia de compartir una determinada información.

Nota. En el caso de Twitter se recomienda desactivar las opciones de ubicación en los tweets al igual que las opciones de etiquetado de fotos por terceros.

egün llowken ka chew amukey taiñ iniygen ka chumkeyegüy pu gobierno feypile taiñ wülalegün che ñi üy.

- Müli taiñ kimtukunieal kom taiñ chumeken redes mew pepi kimfali.
- Rakizuamal ñi rüf ñi zuameel fey ti chi amulkan zugu ñi femal kam femnuael zoy kümi chi.

Troy wirin: fey ti chi twitter mew müli taiñ pegengenuam chew taiñ mülen ta che , chew ñi tuwün pu tweets ka ñi nienoafel fey ti chi kake che ñi azentun mew nüwkülenual.

Referencias de las web.

About Gender and Tech Resources (10 de Enero de 2017) ¿Cómo funciona la telefonía móvil y de qué manera mitigar el rastreo de datos? https://gendersec.tacticaltech.org/wiki/index.php/Gender_and_Tech_Resources>About

Agencia Española de Protección de Datos. Oficina de Seguridad del Internauta. (27 de abril de 2019) ¿Por qué son tan importantes las contraseñas? <https://www.osi.es/sites/default/files/docs/contrasenas01.pdf>

Andalucía es Digital (21 de Febrero de 2018) Guía para eliminar y detectar Malware de tu móvil. <https://blog.aesdigital.es/guia-para-detectar-y-eliminar-malware-de-tu-movil/>

Blum, C. (23 de mayo de 2016) The 5 Why Method. How you can shed light on the dark with 5 questions. <https://www.management-circle.de/blog/die-5-why-methode-wie-sie-mit-5-fragen-licht-ins-dunkel-bringen/>

Britta O'Boyle, B. (27 de Mayo de 2020) ¿Qué es Signal y cómo se usa? El rival de WhatsApp explicó <https://www.pocket-lint.com/es-es/smartphones/noticias/152330-que-es-la-senal-como-se-utiliza-caracteristicas-explicadas-consejos-y-trucos>

Chew ñi zoy kimtukugeal zugu kam chew rekülüwüy tñfachi chillka!

About Gender and Tech Resources (10 de Enero de 2017) ¿Cómo funciona la telefonía móvil y de qué manera mitigar el rastreo de datos? Chumechi am tripakey fey ti chi inachegen telefonía mew ka chumechi azelkayal taiñ allmaltugenuael. https://gendersec.tacticaltech.org/wiki/index.php/Gender_and_Tech_Resources>About

Agencia Española de Protección de Datos. Oficina de Seguridad del Internauta. (27 de abril de 2019) ¿Por qué son tan importantes las contraseñas? Chemu ga zoyelfali fey ta chi troy contraseña pigelu. <https://www.osi.es/sites/default/files/docs/contrasenas01.pdf>

Andalucía es Digital (21 de Febrero de 2018) Guía para eliminar y detectar Malware de tu móvil. Chillka chew ñi feypilen chumechi am nentugetuafüy ka kimgaefüy pu malware tami móvil mew. <https://blog.aesdigital.es/guia-para-detectar-y-eliminar-malware-de-tu-movil/>

Blum, C. (23 de mayo de 2016) The 5 Why Method. How you can shed light on the dark with 5 questions. <https://www.management-circle.de/blog/die-5-why-methode-wie-sie-mit-5-fragen-licht-ins-dunkel-bringen/>

Britta O'Boyle, B. (27 de Mayo de 2020) ¿Qué es Signal y cómo se usa? Chem am ta signal chumechi am pñekey, whatsapp ñi kaiñe feypi El rival de WhatsApp explicó <https://www.pocket-lint.com/es-es/smartphones/noticias/152330-que-es-la-senal-como-se-utiliza-caracteristicas-explicadas-consejos-y-trucos>

Bunton, Cam. (3 de febrero de 2020) ¿Qué es la autenticación de dos factores y por qué debería usarla? Además de cómo habilitar para Apple, Google y más <https://www.pocket-lint.com/es-es/aplicaciones/noticias/141559-que-es-la-autenticacion-de-dos-factores-y-por-que-deberia-usarla>

Conexo (7 de junio de 2020) Seguridad Digital: Conceptos y Herramientas Básicas. <https://conexo.org/project/921/>

Digital Guide (22 de agosto de 2019) Cómo identificar y eliminar malware. <https://www.ionos.es/digitalguide/servidores/seguridad/como-identificar-y-eliminar-malware/>

Fernandez, Y. (4 de junio de 2020) Qué es Signal, cómo funciona y qué opciones ofrece <https://www.xataka.com/basics/que-signal-como-funciona-que-opciones-ofrece>

Fundación Mustakis (sin dato) Guía: del color y Cultura Mapuche <https://colorearte.cl/wp-content/uploads/2017/05/Color-y-Cultura-Mapuche.pdf>

GARAY W. (14 de junio de 2018) ¿Confiable y seguro? Un vistazo a las potenciales vulnerabilidades de WhatsApp (2018) <https://www.derechosdigitales.org/publicaciones/confiable-y-seguro-un-vistazo-a-las-potenciales-vulnerabilidades-de-whatsapp-2018/>

Bunton, Cam. (3 de febrero de 2020) ¿Qué es la autenticación de dos factores y por qué debería usarla? Chem am ta autenticación de dos factores pigechi zugu ka chemu ga müli ñi kimafel ka koneltuafel ka kake zugu . Además de cómo habilitar para Apple, Google y más <https://www.pocket-lint.com/es-es/aplicaciones/noticias/141559-que-es-la-autenticacion-de-dos-factores-y-por-que-deberia-usarla>

Conexo (7 de junio de 2020) Seguridad Digital: Conceptos y Herramientas Básicas. Kuñiwtuwal zugu digital mew : chem am ka fillke pepiluwün. <https://conexo.org/project/921/>

Digital Guide (22 de agosto de 2019) Cómo identificar y eliminar malware chumechi am kimgekey ka nentugetukey malware .<https://www.ionos.es/digitalguide/servidores/seguridad/como-identificar-y-eliminar-malware/>

Fernandez, Y. (4 de junio de 2020) Qué es Signal, cómo funciona y qué opciones ofrece. Chem am ta signal ka chem az niey ka chem zugu wülkey. <https://www.xataka.com/basics/que-signal-como-funciona-que-opciones-ofrece>

Fundación Mustakis (sin dato) Guía: del color y Cultura Mapuche. Chillka az ka mapuche ñi femgen <https://colorearte.cl/wp-content/uploads/2017/05/Color-y-Cultura-Mapuche.pdf>

GARAY V. (14 de junio de 2018) ¿Confiable y seguro? Un vistazo a las potenciales vulnerabilidades de WhatsApp (2018) trokifali reke kiñe troy chew kuñiwtofali WhatsApp. <https://www.derechosdigitales.org/publicaciones/confiable-y-seguro-un-vistazo-a-las-potenciales-vulnerabilidades-de-whatsapp-2018/>

Orellana, R. (30 de mayo de 2019) Conoce qué es WhatsApp, para qué sirve y por qué es tan popular ¿Aún no sabes qué es WhatsApp Messenger? <https://es.digitaltrends.com/celular/que-es-whatsapp/>

Sanchez, C. (5 de febrero de 2020) Citar Página Web- Referencia Bibliográfica 7ma edición. <https://normas-apa.org/referencias/citar-pagina-web/>

Sierra, J. (17 de octubre de 2013) Manual de Seguridad Digital y Móvil para periodistas y Bloqueros. https://protege.la/wp-content/uploads/2018/05/0008_guia_ManualFH.pdf

Signal Support (sin dato) ¿Por qué usar Signal? <https://signal.org/es/>

Surveillance Self-Defense. (30 de octubre de 2018) El Problema con los Teléfonos Móviles. <https://ssd.eff.org/es/module/el-problema-con-los-tel%C3%A9fonos-m%C3%B3viles>

Surveillance Self-Defense. (29 de octubre de 2018) Creando Contraseñas Seguras <https://ssd.eff.org/es/module/creando-contrase%C3%B1as-seguras>

Orellana, R. (30 de mayo de 2019) Conoce qué es WhatsApp, para qué sirve y por qué es tan popular ¿Aún no sabes qué es WhatsApp Messenger? Kimge chem am ta WhatsApp, chemu am koneltuley chemu am kom che niefi , petu kimlaymi chem am ta WhatsApp Messenger. <https://es.digitaltrends.com/celular/que-es-whatsapp/>

Sanchez, C. (5 de febrero de 2020) Citar Página Web- Referencia Bibliográfica 7ma edición <https://normas-apa.org/referencias/citar-pagina-web/>

Sierra, J. (17 de octubre de 2013) Manual de Seguridad Digital y Móvil para periodistas y Bloqueros. Chillka chew ñi kimgeken kuñiwтуwün digital mew ka móvil mew pepiluwlu pu che. https://protege.la/wp-content/uploads/2018/05/0008_guia_ManualFH.pdf

Signal Support (sin dato) ¿Por qué usar Signal? Chemu koneltual signal <https://signal.org/es/>

Surveillance Self-Defense. (30 de octubre de 2018) El Problema con los Teléfonos Móviles. Kiñeke zugu tripayelu pu teléfono móvil mew <https://ssd.eff.org/es/module/el-problema-con-los-tel%C3%A9fonos-m%C3%B3viles>

Surveillance Self-Defense. (29 de octubre de 2018) Creando Contraseñas Seguras nieael kümeke contraseña <https://ssd.eff.org/es/module/creando-contrase%C3%B1as-seguras>



visita <https://southlighthouse.org/>