د پیغامونو رسول او خوندي اړیکې

• زماني موده: 1 ساعت

• زده کړو هدف : ناپېژانده او خوندي اړیکو ترمنځ د تفاوت او ددغو دوو اړیکو ترسره کولو لپاره د وسایلود کارولو زده کړه

رمز لیکنه یا ناپیژاند توب؟

د واټس آپ WhatsApp ، مسنجر Messenger یا ټیلګرام Telegramڅخه د کار اخیستلو پرمهال ستاسو پیغامونه په رمز بدلیږي(یو څه د سوفټ ویر پوري هم تړاو لري) خو د هغو کسانو ادرس چې ورسره اړیکې ټینګوئ په رمز نه بدلیږي. د همدې له امله دا چلوونکي (Operators) (مټا، فیسبوک، تیلګرام) که چیري ستاسو استوونکو محتویاتو ته لاس ونلري، خو کولی شي په دې پوه شي چې تاسو د کومو کسانو سره اړیکې ټینګوئ.

خبریالان د خپلې ډاټا (Datas) د ساتنې لپاره باید دغو وسایلو سره اشنا شي او دا امکان په لاس کې ولري چې په اسانۍ سره خپله ډاټا (Datas) د نورو زیاتو پیغامونو په منځ کې واستولی شي. باید په دې پوه شو چې دا وسایل ممکن نه دي چې په رمز باندې د بل شویو سوفټ ویرونو په اندازه د ابتدا څخه تر هدف (مقصد) پورې خو تاسو ته د خپلې ډاټا د ساتنې او حفاظت لپاره ددې امکان برابروي چې خپله ډاټا په لوړه کچه په ناپیژاندتوب کې پاتې کیدو سره وساتئ.

پیغام رسول او یوڅه کمې او زیاتې خوندي اړیکې

د مړو صندوق

د مړو صندوق هغه ځای دی چې افرادو ته ددې امکان ورکوي چې پرته د یو بل د لیدنې خپل پیغامونه تبادله کړي. ددې میتود څخه کیدای شي په مجازې فضا کې هم کار واخیستل شي:

۱- د ایمیل آدرس له هر خدماتي شرکت څخه چې غواړئ جوړ کړئ.

۲- ایمیل ته د لاس رسي اړوند د هویت (پیژندنې) معلومات په خوندي ډول خپل مخاطب سره شریک کړئ.

۳- پیغامونه یوازې د چټل نویس خاکه کې پرته د استلو ولیکئ.

د مړو ددغه صندوق په کاروني ستاستو ایمیلونه په اینټرنیټ کې ګردش یا حرکت نه کوي. هغه څه چې د اینټرنیټ د خدمتونو وړاندي کوونکي سرورونه(Servers) کولی شي وګوري یوازې د خدمتونو د چمتو کولو د یو شرکت سره ستاسو نښلیدل لکه جي میل (GMail) لیدلی شي. باید پام وکړئ کوم پیغامونه چې په صندوق او خاکه کې لیکلي دي په رمز نه بدلیږي او په حقیقت کې د خدمتونو وړاندې کوونکی شرکت ورته لاس رسی لري. د مثال په توګه جي میل (Gmail) ته د ګوګل (Google) لاس رسی.

په آنلاین بڼه د مقالې او لیکنې خپرول

CryptPad د Google Doc معادل دی چې لیکنې رمز ته په اړول شوي او آنلاین بڼه ذخیره کوي. کولی شئ له دغه امکان څخه د 'مړو د صندوق' د میتود په څېر کار واخلئ. خو د ایمیلونو د خدمتونو د وړاندې کولو د سرویسونو لکه Gmail یا Mail cryptpad Yahoo - پر خلاف ستاسود پیغامونومحتویاتو ته لاس رسی نلري، ځکه چې هغوی دا محتویات د رمز په بڼه ذخیره کوي.

په URLکې د رمز لیکنې (Encryption) کیلي (Key) د # کریکټر د لیکلو وروسته لیکل کیږي. د همدې له امله د دغه سیستم پروتوکول له مخې هرڅه د # څخه وروسته ولیکل شي د URL د دروازې د ادرس پرمخ د سرور (Server) لپاره د لاس رسي وړ نه دی.

انګلیسي مثال ////

/https://cryptpad.fr/pad/#/2/pad/edit/J6KGLGTPSH1lJyc0U1U2zFLz

د پیغامونو رسول او خوندي اړیکې

ایمیلونه

ایمیلونه خوندي نه دي. په اینټرنیټ کې په غیر محرمانه توګه په حرکت کې دي، یعنی تاسو ته د اینټرنیټ د وړاندې کوونکي شرکت له خوا کیدای شي ولیدل شي او ولوستل شي.
ایمیل د یو لیک په څیر دی چې د پاکټ پرته واستول شي او پیغام رسوونکی هغه لولي. د خپلو ایمیلونود محتویاتو د ساتنې کولی شئ د Proton Mail یا Tutanota په څیر د آنلاین خدمتونو څخه کار واخلئ:

Tutanota ایمیل سیستم (Tuta) په خپله نسخه کې د یو ګیګابایټ په اندازه فضا په وړیا ډول د ذخیره کولو لپاره وړاندې کوي.

• Protonmail د freemium په موډل باندي کار کوي یعنی لومړی ستاسو ته د پیغامونو د ذخیرې لپاره د ۵۰۰ مګابایټو په اندازه په وړیا ډول فضا برابروي که له دې اندازې څخه زیاتې فضا ته اړتیا لرئ باید د پیسو په بدل کې یې واخلئ.

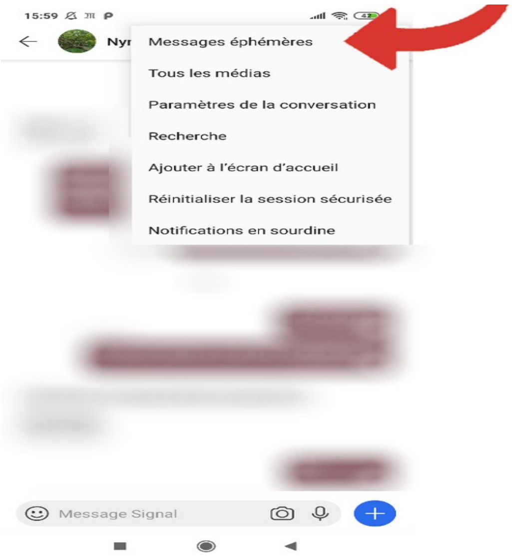
پام باید وکړئ، ددغو شرکتونو پیغامونه د خپلو ایمیلونو لپاره دي یعنی یوازې دProtonmails څځه Protonmail ته اویا دTutanota څخه Tutanota ته استول کیدای شي خوندي او رمز لیکنی (Encryption) دي. د خدمتونو د وړاندې کوونکو دغو شرکتونو څخه د جي میل (Gmail) ته د کار اخیستلو په صورت کې باید پخپله د رمز لیکنې (Encryption) اقدام وکړئ. طبعا ده د رمز لیکلولپاره باید یو رمز د رمز لیکلو او د رمز د پرانیستلو لپاره ایمیل ته واستول شي.

سیګنال

سيګنال پروګرام د ځيرکو ټيليفونونو لپاره جوړ شو ی دی چې په ټيلفون کې ستاسو پيغامونه په رمزي ليکنه باندي بدلوي چې ټيليفون او يا هغه ټيليفون پيغام ترلاسه کوي رمزي لينکې پرانيځي. این رمزنگاری از دا رمزي ليکني د مبدا يا پيل څخه تر مقصد يا پای پورې (End To End Encrpytion) ليکنې دي. يعنی حتی د هدک کيدو په صورت کې هم سيګنال کې ستاسو د پيغام محتويات نشي افشا کيدلی.

سيګنال لوی ډاټا (Metadata) د اړتيا وړ ټاکلي دورې څخه زيات د حرکت لپاره پيغام نه ساتي او يوازې په موقتي ډول يې د فني دلايلو له مخې ساتنه کوي.

په پام کې ولرئ، استول شوي پيغامونه په ټيليفون کې ذخيره کيږي او که چيرې ټيليفون د کوم چا لاس ته ورشي او هغه کد (Code) کړي په دې صورت کې ستاسو پيغامونو ته د لاس رسي امکان شته دی. د همدې له امله سيګنال (او ځينې نور کاروونکي سوفټ ويرونه) ډيرې ګټورې ځانګړتياوې لري: موقتي پيغامونه چې پټپله استوونکي ته د حذفولو امکان په لاس ورکوي شته دی



موقتي پيغامونه

تمرين:

١. https://signal.org/en/download/. د App Store يا د Play Store څخه نصب کړئ.

٢. د نوي پيغام پر مخ کليک وکړئ؛ ستاسو سره د اړيکو د نيوونکو او اشنايانو ليست چې د سيګنال څخه کار اخلي راڅرګنديږي.

٣. د هغوې له ډلې يو ته يې پيغام واستوئ

٤. د نووخبرو تنظيماتو (Settings) ته لاړ شئ او موقتي پيغامونو انتخاب (option) فعال کړئ

٥. د خپل کمپيوټر په ډيسک ټاپ باندې کارونکی سوفټ وير نصب کړئ

٦. هغه د خپل ځيرک ټيليفون سره همغږی يا ونښلوئ

نور کارونکي (عملي) سوفټ ويرونه

اګر که چيرې د Telegram ،iMessage ،WhatsApp ، Discord او نورو؟ **کاروونکو سوفټ ويرونو** څخه کار اخلئ پاملرنه وکړئ چې ايا د کاروونکي سوفټ وير څخه د د مبدا څخه تر

مقصد پوري د رمز ليكنې (Encryptions) څخه كار اخلئ او ددغه جدول له لارې سوفټ ويرونه و ارزوئ.

پيغام رسول او خوندي اړيکې

Wire نرم‌ابزاربرای ارتباط ایمن است که امتیاز آن عدم نیاز به داشتن شماره تلفن است. د اړیکو لپاره Wire يو خوندي سوفټ وير دی چې ځانګړتيا يې داده چې د تيليفون شميرې ته اړتيا نلري.

Briar هم يو كاروونكی عملي سوفټ وير دی چې د (CTP) له فن څخه په ګټې اخيستنې رمز ليكنه (Encryptions)يې شوې ده او يو په يو يا د سيال (counterpart) سره د (Tor) په ملاتړ رمز ليكنه يې كيږي، يعنی د ځيرک تيليفون څخه پيغامونه بل ځيرک تيليفون ته د مركزي سرور (Server) پرته ګردش يا حركت كوي.

Olvid يو بل ساده كارونكی نوم د حساب د پرانيستلو لپاره كفايت كوي. په Olvid، كې اړيکې اوارتباطات او لوی ډاټا (Metadatas) له پيل څخه تر اخيره پوري په رمز باندې ليكل شوي دي. دا پروګرام د معلوماتو د ملي امنيت د معلوماتو د سيستم د (ANSSI) له خوا تصديق شوی دی. Olvid

يوه وړيا نسخه د څو كمو ځانګړتياو سره (د غړيزې اړيكې پرته) وړاندې كوي.

دا معرفي شوي پيغام رسوونكي او عملي سوفټ ويرونه تاسو ته ددې امكان دركوي چې په آنلاين بڼه د خپلو پيغامونو ساتنه وكړئ ، خو له ياده مه اوباسئ چې دا پيغامونه ستاسو او ستاسو د مخاطب په تيليفون كې ساتل كيږي. د خپلو مهمو پيغامونو لپاره حتمی د " موقتي پيغامونو" د ځانګړتيا چې په ټولو معرفي شويو پيغام رسوونكو كې شته دی ګټه واخلئ

د GSM شبكه

د GSM شبكه خوندي نه ده

۱- ستاسو د تيليفون د خدمتونو وړاندې كوونكی شركت كولی شي د اړيكو او د تبادله شويو پيغامونو نوملړ ته لاس رسی ولري.

۲- كلونه كيږي چې د GSM د رمز ليكنې الګوريتم (Encryptions algorithm) سورى (leaked) شوی

د لا زيات پوهاوي لپاره دا وګورئ:

د خوندي پيغام رسوونكو او كاروونكو يا عملي سوفټ ويرونو Totem آنلاين دوره (په فارسی ژبه کې)