ارتباطات و پیام‌رسانی ایمن

- مدت زمان: ۱ ساعت
- **موضوع** درس‌نامه : یادگیری تفاوت میان ارتباط ناشناس و ایمن، یادگیری ابزارهای انجام این کارها

رمزنگاری یا ناشناس بودن؟

در هنگام استفاده از نرم‌افزارهای کاربردی مانند واتس‌آپ WhatsApp، مسنجر Messenger یا تلگرام Telegram ، محتوای پیام شما رمزنگاری می‌شود (این کم و بیش بستگی به نوع نرم‌افزار دارد) اما آدرس افرادی که با آنها ارتباط برقرار می‌کنید، رمزنگاری نمی‌شود. بنابراین اپراتورها (متا، فیسبوک، تلگرام) اگر به محتوای ارسالی شما نیزدسترسی نداشته باشد، اما می‌تواند بفهمد که شما با چه کسانی ارتباط برقرار می‌کنید.

برای حفاظت از داده‌های خود روزنامه‌نگاران و کنش‌گران باید بتوانند با این ابزارها آشنا شوند. امکانی تا داده‌های خود به راحتی در میان خیل پیام‌های دیگر ارسال کنند. باید بدانیم این ابزارها شاید نه به اندازه‌ای نرم‌افزارهای رمزنگاری از مبدا تا مقصد، اما به شما امکان حفاظت از داده‌های خود با درصدی بالا از ناشناس ماندن را می‌دهند.

پیام‌رسانی و ارتباطات کمابیش ایمن

صندوق مرده

صندوق مرده مکانی است که به افراد امکان می‌دهد تا بشکل غیردیداری پیام‌های خود را مبادله کنند. این روش می‌تواند درفضای مجازی نیز استفاده شود:

۱- از هر شرکت خدمات دهنده که می‌خواهید، یک آدرس ایمیل بسازید.

۲- نام کاربری و گذرواژه برای دستیابی به ایمیل را به شکلی امن با مخاطب خود به اشتراک بگذارید.

۳- پیام‌ها را تنها در چرک‌نویس بدون ارسال آن بنویسید.

با استفاده از این صندوق مرده، ایمیل‌های شما در اینترنت گردش نمی‌کنند. آنچه که سرویس‌های خدمات دهنده اینترنت می‌توانند ببینند تنها وصل شدن شما به یک شرکت خدمات دهنده مانند جی‌میل یا یاهو و ... است. باید توجه داشته باشید که پیام‌ها در صندوق و خاکه‌ای که نوشته‌اید رمزنگاری نمی‌شوند و شرکت خدمات دهنده به راحتی به آن دسترسی دارد .

به اشتراک گذاشتن مقاله و نوشته به شکل آنلاین

CryptPad معادل Google Doc است که نوشته‌ها را به صورت رمزنگاری شده و آنلاین ذخیره می‌کند. می‌توانید از این امکان نیز به مانند روش صندوق مرده استفاده کنید. **اما** برخلاف دیگر سرویس‌های ایمیل مانند Gmail یا Yahoo این سرویس خدپمات دهنده Mail - cryptpad به محتوای پیام‌های شما دسترسی ندارد. زیرا آنها را به صورت رمزنگاری شده ذخیره می‌کند.

کلید **رمزنگاری** در URL پس از نویسه‌ی # نوشته می‌شود. بنا بر پروتکل این سیستم هر چیزی پس از نویسه‌ی # نوشته شود ، در آدرس URL برای سرور قابل دسترسی نیست.

مثال انگلیسی ////

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

پیام‌رسانی و ارتباطات ایمن

ایمیل‌ها

ایمیل‌ها ایمن نیستند. پیام‌ها و مقالات شما در اینترنت به شکل غیر محرمانه در گردش هستند، یعنی همه‌ی محتوای آنها می‌تواند از سوی شرکت خدمات دهنده اینترنت شما دیده و خوانده شود. ای‌میل مثل نامه‌ای است که بدون پاکت فرستاده شود و پیام‌رسان می‌تواند آن را بخواند. برای حفاظت از محتوای ای‌میل‌های خود می‌توانید از خدمات آنلاین مانند Proton Mail یا Tutanota استفاده کنید:

Tutanota در نسخه رایگان خود یک گیگابایت فضای ذخیره‌سازی ارائه می‌دهد.

Protonmail بنا بر مدل freemium کار می‌کند. یعنی نخست یک سرویس رایگان با ۵۰۰ مگابایت فضای ذخیره‌سازی برای پیام‌های شما ارائه می‌دهد، اگر بیشتر نیاز داشته باشید باید فضای بیشتر را خریداری کنید.

توجه داشته باشید خدمات این شرکت‌ها برای ای‌میل‌های خود است. یعنی تنها ایمیل‌هایی از Protonmail به Protonmail یا از Tutanota به Tutanota فرستاده می‌شوند ایمن و رمزنگاری شده هستند. برای استفاده از این شرکت‌های خدمات دهنده برای مثال ازسال ای میل به جی میل خود باید اقدام به رمزنگاری کنید. و طبعا برای رمزنگاری باید یک رمز برای رمزنگاری و رمزگشایی ایمیل فرستاده شود.

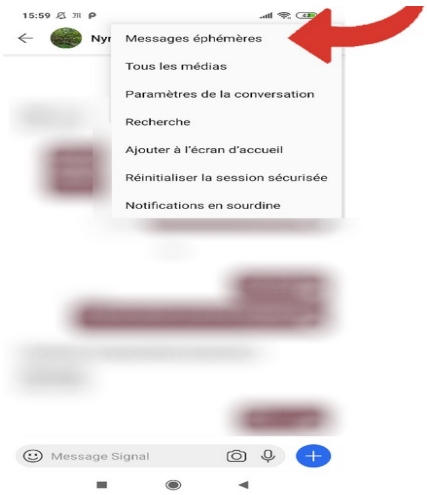
سیگنال

سیگنال یک برنامه برای گوشی‌های هوشمند است که پیام‌های شما را در گوشی فرستنده رمزنگاری کرده و در گوشی یا گوشی‌های گیرنده آنها را رمزگشایی می‌کند. این رمزنگاری از از مبدا به مقصد (End To End Encrpytion) است. یعنی حتا در صورت هک شدن سرورهای سیگنال ، محتوای پیام‌های شما نمی‌تواند فاش شود.

سیگنال داده‌های کلان metadata را فراتر از دوره مورد نیاز برای گردش پیام نگه‌داری نمی‌کند. و تنها یک نگه‌داری موقت به دلایل فنی است.

توجه داشته باشید، پیام‌های ارسالی در گوشی‌ها ذخیره می‌شوند و اگر گوشی‌ها در دسترس کسی قرار گیرد و آن را رصد کند، در این صورت امکان دسترسی به پیام‌های شما وجود دارد. به همین دلیل سیگنال (و برخی

دیگر از نرم‌افزارهای کاربردی) دارای ویژگی بسیار مفید هستند: **پیام‌های موقت که امکان حذف خودکار آن‌ها برای ارسال کننده وجود دارد.**



پیام‌های موقت

تمرین:

۱-. https://signal.org/en/download/ را از App Store یا Play Store نصب کنید

۲- بر روی ارسال پیام جدید کلیک کنید؛ لست آشنایان شما که از سیگنال استفاده می‌کنند نمایان می‌شود.

۳- یک پیام به یکی از آنها ارسال کنید.

۴- به تنظیمات گفتگوی جدید بروید و پیام‌های موقت را فعال کنید.

۵- نرم‌افزار کاربردی را در صفحه **دسکتاپ** (DeskTop) خود نصب کنید.

٦- آن را با گوشی هوشمند خود هم گام و منطبق کنید

دیگر نرم‌افزارهای کاربردی

اگر از **دیگر نرم‌افزارهای کاربردی** استفاده می‌کنید به مانند WhatsApp، iMessage، Discord ، Telegram و غیره؟ دقت کنید که آیا این نرم آفزارکاربردی مورد نظر استفاده‌ی شما، از رمزنگاری از مبدا تا مقصد استفاده می‌کند.

شما با استفاده از این جدول نقاط قوت یا ضعف نرم‌افزارها را بررسی کنید.

پیام‌رسانی و ارتباطات ایمن

Wire نرم‌ابزاربرای ارتباط ایمن است که امتیاز آن عدم نیاز به داشتن شماره تلفن است.

Briar نرم‌افزارکاربردی است که از فن CPT (رمزنگاری شده یک به یک یا همتا به همتا و با کمک Tor رمزنگاری می‌شود. یعنی پیام‌ها از گوشی هوشمند به گوشی‌های هوشمند دیگر بدون نیاز به سرور مرکزی گردش می‌کنند.

اگر این پیام‌رسان‌ها و نرم‌افزارهای کاربردی معرفی شده به شما این امکان را می‌دهند که پیام‌های خود را به صورت آنلاین محافظت کنید، اما فراموش نکنید که پیام‌ها در گوشی شما یا گوشی مخاطب شما نگهداری

میشوند. برای پیام های مهم خود حتما از ویژگی "**پیام‌های موقت**" که در همه پیام رسان‌های معرفی شده وجود دارد، استفاده کنید.

شبکه GSM

شبکه GSM ایمن نیست.

۱- شرکت خدمات دهنده تلفن شما می تواند به فهرست تماس‌ها و پیام‌های مبادله شده دست یابد.

۲- الگوریتم رمزنگاری شبکه GSM سال‌هاست لو رفته است.

برای دانستن بیشتر ببینید :

دوره Totem آنلاین درباره پیام‌رسان‌ها و نرم‌افزارهای کابردی ایمن (در زبان فارسی)