امنیت پیام رسان های ایرانی و خارجی (قسمت اول)

امروزه بحث داغی درباره امنیت پیام رسان های اینترنتی همه جا وجود دارد. مخصوصا این بحث با خبر فیلتر شدن احتمالی تلگرام شدت بیشتری گرفته است. عده ای معتقدند که پیام رسان های خارجی مانند تلگرام و واتس اپ (که در ایران بیشتر شناخته شده هستند) از امنیت بسیار بالایی برخوردارند. عده ای هم به هیچ عنوان حاضر نیستند پیام رسان های داخلی را نصب کنند. اما به نظر شما امنیت کدام اپلیکیشن ها بالاتر است؟

منظور از امنیت پیام رسان چیست؟

امنیت پیام رسان به زبان ساده یعنی کسی از اطلاعاتی که شما در این شبکه ها به اشتراک میگذارید، با خبر نشود. این افراد میتوانند سازمان، شرکت، هکر، رسانه، نهاد های امنیتی و یا حتی دولت ها باشند. اطلاعات شما هم همه ی آن چیزی است که درون این برنامه ها وارد میکنید. مانند: عکس، پیام، شماره تلفن، ایمیل، آدرس، موقعیت مکانی(Location) ، نام کاربری، جنسیت و غیره.

هرچقد افراد کمتری بتوانند به این اطلاعات دسترسی داشته باشند، امنیت پیام رسان بالاتر میرود. به عبارتی، هر چقدر دست یابی به اطلاعات شما سخت تر و غیر ممکن تر باشد، برنامه ای که از آن استفاده میکنید امنیت بالاتری دارد.

چگونه دیگران میتوانند به اطلاعات ما دسترسی داشته باشند؟

وقتی که شما در یک سرویس پیام رسان عضو میشوید، حتما باید اطلاعاتی را وارد کنید. در این مرحله برای شما یک حساب کاربری ساخته میشود که از این به بعد معرف شما در دنیای آن پیام رسان خواهد بود. سپس شما میتوانید اطلاعات خود را در این شبکه ها به اشتراک بگذارید. بعضی از سرویس های پیام رسان (یا به طور کلی تر، شبکه های اجتماعی) ممکن است اطلاعات خاص تری را از شما بگیرند.

مثلا اینستاگرام بیشتر روی اشتراک گذاری فیلم و عکس تمرکز دارد. یا در پیام رسان تلگرام شما میتوانید به راحتی با بقیه ی اعضای این پیام رسان، ارتباط داشته باشید و انواع مختلفی از فایل ها را رد و بدل کنید.
اما همه ی این عکس ها، پیام ها، ایمیل ها، شماره تلفن ها و اطلاعاتی که به این سرویس میدهید، در جایی ذخیره میشوند. به عنوان مثال اگر دقت کرده باشید، وقتی با گوشی های دیگری به غیر از موبایل شخصی تان، به اکانت تلگرام خودتان وارد شوید، همه ی چت ها، گروه ها و کانال هایی که روی موبایلتان بود را دوباره خواهید دید.

این مسئله به این معناست که اطلاعات شما در جایی به غیر از حافظه گوشی موبایلتان ذخیره شده اند. در حقیقت همه ی این موارد روی سرور های پیام رسانی که از آن استفاده میکنید ذخیره خواهند شد. در این سرور ها، اطلاعات روی جدول هایی ذخیره میشوند که از مجموعه ی این جداول کنار هم، دیتابیس (پایگاه داده) به وجود می آید.

خب! الان برای رسیدن به اطلاعات، فقط کافی است که کسی بتواند به دیتابیس های اصلی پیام رسان شما (که معمولا در محل شرکت پیام رسان قرار دارند) دسترسی پیدا کند. وظیفه شرکت پیام رسان این است که امنیت این داده ها را در برابر دیگران حفظ کند.

چگونه امنیت پیام رسان حفظ میشود؟

یک پیام رسان با تعریف کردن الگو های رمز نگاری ایمن میشود. یک پیام رسان ایمن، اطلاعاتی که شما به اشتراک میگذارید را رمز گذاری میکند. از این طریق کسی نمیتواند بفهمد که اصل داده ها چه چیزی بوده است. رمزنگاری هم کیفیت های متفاوتی دارد. الگو های رمزنگاری یک پیام رسان ایمن، باید پیشرفته و غیر قابل نفوذ باشند. در مورد انواع رمز نگاری ها، در یک مقاله جداگانه توضیحات کامل تری خواهم داد.

با توجه به گستردگی سطوح امنیت در حوزه پیام رسانها در هفته آینده به ادامه بررسی این مطالب خواهیم پرداخت:

- **امنیت پیام رسان ها خارجی (تلگرام ، واتس اپ، ...)**
- **امنیت پیام رسان ها داخلی (سروش، آی گپ، گپ، ...)**