استفاده از سیمکارت ناشناس

یکی از بزرگترین تهدیدات فعالیت در فضای مجازی امکان کشف ارتباط میان هویت مجادی ناشناس و واقعی است. افرادی که ممکن است در فعالیت های مجازی احتیاط کنند در بخش امنیت اطلاعاتی خود اشتباهاتی میکنن که موجب افشا شدن هویت واقعی خود می شوند و امنیت فیزیکی آن ها را به خطر می اندازند. یکی از مهم ترین موضوعات در این حیطه امنیت شماره تلفنی است که از آن استفاده میکنید.

امنیت سیمکارت های داخلی

طبق اطلاعاتی که از یک دستورالعمل داخلی شرکت مخابرات به دست آمده، تقریبا هر اطلاعاتی که میتوانید تصور کنید از گوشی تلفنی که در داخل کشور از سیمکارت داخلی استفاده میکنند قابل استخراج است. از اطلاعات سخت افزاری تا موقعیت جغرافیایی تا قابلیت پایین آوردن سرعت اینترنت خط. بنابراین استفاده از سیمکارت فیزیکی برای هر فعالیت حساسی همراه با خطر است و در حالت ایده آل دستگاه سیمکارت دار باید کاملا مجزا از دستگاه حاوی اطلاعات حساس باشد. همچنین از ثبت نام در اپلیکیشن ها با استفاده از شماره خط خودداری کنید، زیرا مخابرات قابلیت دریافت لینک های عوض کرن رمز و ورود به تمامی حساب های کاربری مربوط به آن را دارند.

2FA

برای امنیت حداکثری، برای تمام حساب های کاربری حساس خود 2 Factor Authentication را فعال کنید، و از گزینه اپلیکیشن های Authentication مثل نمونه‌ی گوگل استفاده کنید و نه از گزینه ی شماره تلفن. پیام های دریافتی تلفن میتواند توسط دیگران خوانده شود اما نرم افزار های مخصوص Authenticator رمز دوم را در دستگاه تان ذخیره میکنند. به طور کل از شماره سیمکارتتان برای هیچ حساب کاربری حتی Backup ایمیل استفاده نکنید، چرا که حتی اگر امنیت خود حساب ایمیل بالا باشد امنیت آن با شماره تلفن نا امن زیر سوال میرود

استفاده از نرم افزار های ایمن

به هیچ وجه از نرم افزار های جایگزین که بدون فیلتر شکن کار می کنند استفاده نکنید، چرا که این نرم افزار ها توسط دستگاه های اطلاعاتی برای دزدیدن اطلاعات کاربران توزیع می شوند، یکی از معروف ترین نمونه های آن تلگرام طلایی است. از طرف اپلیکیشن سیگنال یکی از ایمن ترین روش های برقراری ارتباط است، تلگرام نیز بخاطر محبوبیت و امنیت بیشتر اطلاعاتی و امکان حذف پیام از دو طرف و امکاناتی مثل Secret chat و Self-destruct، انتخاب خوبی است اما به یاد داشته باشید که اگر شماره‌ی استفاده شده برای ثبت نام ایمن نباشد اکانت نیز ایمن نیست. برای کاربر ایرانی، یک روش ارتباطی امن ایده آل اکانت تلگرامی است که با شماره مجازی ساخته شده، رمز دارد و 2 Factor Authentiction آن فعال است. یک اپلیکیشن محبوب ارتباطی دیگر هم واتس اپ است که با توجه به ساختار و عدم اهمیت به حریم شخصی برای ارتباطات حساس اصلا پیشنهاد نمی شود، بنابراین استفاده از آن را به گفت و گو های عادی محدود کنید.

اهمیت مجزاسازی

همانطور که پیش تر اشاره شد، از آنجایی که حساب های کاربری مختلف میتوانند راه ورود به حساب های دیگر باشند، بهتر است برای امنیت حداکثری چند حساب ایمیل برای حساب های مختلف استفاده کنید، اطلاعات حساب های مختلف مثل رمز را در هیچکدام نگهداری نکنید و از Backup های غیر ایمن استفاده نکنید. در همین راستا، از استفاده از یک رمز برای چند حساب خودداری کنید و رمز های پیچیده استفاده کنید.

اگر برای فعالیتی نیاز به حساب های دائمی ندارید، از شماره و حساب های موقت استفاده کنید و پس از تمام شدن آن را حذف کنید.

مجزا سازی سخت افزاری

تا جای ممکن دستگاه هایی که حاوی اطلاعات حساس هستند را از دستگاه های روزانه تان جدا نگه دارید. همانطور که اشاره شد تلفن های همراه که سیمکارت دار هستند از خیلی روش ها قابل ردیابی هستند. با توجه به این موضوع، و اینکه خرید دستگاه مجزا برای فعالیت های حساس برای اکثر افراد قابل انجام نیست، یک روش ملموس تر ایجاد حساب جدا بر

روی کامپیوتر شخصی با رمز قوی است، تا هم از تلفن همراه جدا باشد و هم قابلیت های ردیابی دستگاه های سیمکارتی را نداشته باشد.

سرویس های پولی دریافت شماره مجازی با قابلیت خرید با ارز مجازی

Telnum.net
Moremins.com
Virtnum.com