اطلاعات روز

# کتابچه راهنمای امنیت دیجیتال

راهنمای جامع هویت و امنیت در فضای مجازی

## فهرست مطالب


مفاهیم پایه ..... ۱
انترنت و نحوه کار آن ..... ۱
آدرس آی‌پی (IP Address) ..... ۱
وی‌پی‌ان (VPN) ..... ۱
وی‌پی‌ان‌ها امن هستند؟ ..... ۲
چه اطلاعاتی برای شرکت‌های سرویس‌دهنده‌ی انترنت و یا شرکت‌های ارائه‌دهنده وی‌پی‌ان قابل مشاهده است؟ ..... ۲
رمز گذاری (Encryption) ..... ۳
چرا رمز گذاری مهم است و مزایای آن چیست؟ ..... ۳
پیام‌رسان‌ها ..... ٤
توصیه‌های امنیتی برای استفاده از پیام‌رسان‌ها ..... ٤
توصیه‌های امنیتی در هنگام تماس‌های تصویری و جلسات آنلاین ..... ٥
اقدامات موثر در مواقعی که سرعت انترنت پایین است ..... ٦
قابلیت‌های امنیتی و حریم‌خصوصی در پیام‌رسان‌ها ..... ٦
ایمیل ..... ٦
توصیه‌های امنیتی برای بالابردن امنیت ایمیل ..... ۷
سرویس‌های پیشنهادی ایمیل ..... ۷
شبکه‌های اجتماعی ..... ۷
اقدامات امنیتی برای بالا بردن امنیت حساب شبکه‌های اجتماعی ..... ۸
امنیت دستگاه‌ها ..... ۹
توصیه‌های امنیتی برای بالا بردن امنیت دستگاه‌ها ..... ۹
فعالیت ناشناس در وضعیت جاری ..... ۱۰
مهم‌ترین نکات و اقداماتی که باید در نظر بگیرید ..... ۱۰
اقدامات زمان قطع کلی انترنت ..... ۱۲

توصیه‌های کلی برای فعالیت و کار ناشناس ..... ۱۳
پیام‌رسان‌ها ..... ۱٤
شبکه‌های اجتماعی ..... ۱٤
امنیت دستگاه‌ها ..... ۱٤

# مفاهیم پایه

## انترنت و نحوه کار آن

زمانی که به انترنت وصل می‌شوید و از آن استفاده می‌کنید، اطلاعات شما در اختیار سرویس دهنده انترنت قرار می‌گیرد و سپس به انترنت فرستاده می‌شود. سپس این اطلاعات توسط سرور (وبسایت مورد نظر) خوانده شده و موارد مورد نیاز را در اختیارتان قرار می‌دهد.
این روند برای باز کردن یک صفحه و یا دانلود تکرار می‌شود. برای اینکه این اطلاعات توسط انترنت جابه‌جا شوند، نیاز به آدرس‌دهی است تا معلوم شود این اطلاعات از کجا آمده و به کجا می‌روند.
با توجه به اطلاعاتی که جابه‌جا می‌شوند، شیوه‌های آدرس‌دهی متفاوتی وجود دارد؛ با این حال در بالاترین سطح، آدرسی وجود دارد که به آن آدرس IP یا نشانی IP گفته می‌شود.

## آدرس آی‌پی (IP Address)

یک IP یک مجموعه‌ای از عدد و رقم است که به ترتیب خاصی در کنار هم قرار گرفته‌اند و به یک دستگاه دیجیتال، یک سرور یا یک وب‌سایت تعلق دارد.
آدرس IP برای هر دستگاهی مختص همان دستگاه است. در واقع این یکتایی IP ویژگی بسیار مهمی است که امکان ارتباط انترنتی را فراهم کرده است. در صورتی که دو دستگاه دارای یک آدرس IP باشند، در شبکه اختلال به‌وجود می‌آید و تا زمانی که این مشکل حل نشود، ارتباطی شکل نخواهد گرفت.

همان طور که برای تماس گرفتن با یک فرد یا ارسال نامه به شماره تلفن و آدرس پستی مختص همان فرد نیاز داریم، در انترنت هم برای ارتباط دو کامپیوتر (یا هر دستگاه الکترونیکی دیگر) وجود آدرس IP لازم و ضروری است.

## وی‌پی‌ان (VPN)

وی‌پی‌ان در حقیقت این امکان را برای شما فراهم می‌کند که دستگاه خود را از یک فضای ناامن و شلوغ دور و در بستر یک تونل امن به یک شبکه خصوصی دیگر در انترنت متصل کنید. به این صورت یک اتصال کاملاً امن و بدون اینکه اطلاعات شما در دسترس وب‌سایت‌های دیگر قرار بگیرد، خواهید داشت.

استفاده از وی‌پی‌ان در دو صورت برای شما می‌تواند مفید باشد. اول اینکه با فعال کردن وی‌پی‌ان شما می‌توانید با استفاده از سرورهای آن، از کشوری دیگر به شکل غیرواقعی وارد فضای انترنت شوید. معمولاً از این مورد برای دسترسی به محتواهای غیرقابل دسترس در کشور استفاده می‌شود. مورد دوم برای پنهان کردن آدرس IP واقعی شما در هنگام گشت‌وگذار در انترنت است.

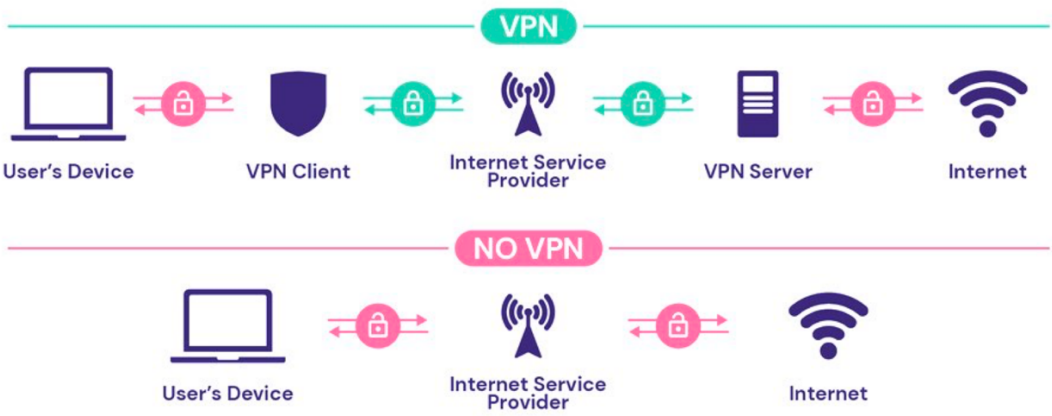
برای مثال: فرض کنید شما با استفاده از وی‌پی‌ان قصد بازدید از وبسایت گوگل را دارید و کامپیوتر شما در افغانستان است و سرور وی‌پی‌ان در کانادا. در این حالت درخواست‌های شما از کامپیوتری که در کانادا است، برای سرورهای گوگل ارسال شده و جواب به آن باز خواهد گشت. از طرف دیگر، با رمزنگاری اطلاعات تان از طریق وی‌پی‌ان، شخص خارجی، برای مثال هکر، شرکت سرویس دهنده انترنت و غیره قادر به خواندن اطلاعات شما نخواهد بود.

## وی‌پی‌ان‌ها امن هستند؟

پاسخ کوتاه بله است. بسیاری از وی‌پی‌ان‌ها روش‌های عالی برای محافظت از ترافیک انترنتی، وب‌گردی، پنهان کردن موقعیت مکانی و حفظ حریم خصوصی در دنیای دیجیتال هستند. اما وی‌پی‌ان‌هایی هم هستند (اکثراً رایگان) که کاملاً ایمن و امن نیستند. آن‌ها ممکن است شما را در معرض بسیاری از خطرات حفظ حریم خصوصی و شیوه‌های تبلیغاتی پنهان قرار دهند.

## چه اطلاعاتی برای شرکت‌های سرویس‌دهنده‌ی انترنت و یا شرکت‌های ارائه‌دهنده وی‌پی‌ان قابل مشاهده است؟

بدون وی‌پی‌ان، شرکت‌های سرویس‌دهنده خدمات انترنت می‌توانند هر کاری را که به صورت آنلاین انجام می‌دهید، مشاهده کنند. این شامل تاریخچه‌ی گشت‌وگذار شما در انترنت، ویدیوهایی که تماشا می‌کنید و وب‌سایت‌هایی که بازدید می‌کنید می‌شود.




اما وقتی از وی‌پی‌ان استفاده می‌کنید، در حالی که وی‌پی‌ان‌ها به مخفی کردن اطلاعات شما کمک می‌کنند، شرکتهای سرویس‌دهنده‌ی انترنت همچنان می‌توانند گزارش‌های اتصال شما را

ببینند، آدرس IP سرور وی‌پی‌ان را ببینند، زمان استفاده شده و حتا میزان ترافیک به و از دستگاه شما را داشته باشند.

## رمز گذاری (Encryption)

رمزگذاری به پروسه‌ای گفته می‌شود که یک متن قابل مشاهده و درک توسط انسان، به شکلی تغییر می‌یابد تا کاملاً غیر قابل درک و فهم باشد. اساساً به این متن غیر قابل درک "ciphertext" یا متن رمزی گفته می‌شود. به عنوان یک مثال فرض کنید کلمه «سلام» قرار است encrypt یا رمزنگاری شود تا هیچ انسانی درک درستی از این کلمه نداشته باشد. در این صورت این کلمه به حالت زیر در می‌آید:

## چرا رمز گذاری مهم است و مزایای آن چیست؟

امروزه با حجم بسیار زیاد داده‌ها در انترنت، حفظ امنیت کاربران و حریم شخصی آن‌ها باید اولویت اول هر کسب و کار انترنتی یا آنلاین باشد. از همین رو مزیت‌های اساسی و اصلی رمزگذاری حفظ حریم شخصی و افزایش امنیت اطلاعات است.

رمزگذاری داده‌ها (دیتا) این تضمین را می‌دهد که هیچ‌کسی قادر به مشاهده اطلاعات شخصی کاربران یا داده‌هایی که توسط آن‌ها روی یک سایت یا سرور منتقل می‌شود، نخواهد بود. این موضوع باعث کاهش سوءاستفاده بسیاری از گروه‌ها از جمله: هکرها، کمپین‌های تبلیغاتی، ارائه‌دهنده‌های خدمات سرویس انترنت و حتا دولت‌ها، جهت استفاده از اطلاعات و داده‌های کاربران خواهد شد.

روش‌ها و الگوریتم‌های زیادی برای رمزگذاری داده‌ها وجود دارد، اما یکی از روش‌های مصون و پرکاربرد در برنامه‌های مشهور امروزی مثل واتساپ، سگنال و زوم، روش رمزگذاری سرتاسر (End-To-End Encryption) است. در این روش کلیدهای رمزنگاری مورد استفاده (کلید عمومی و خصوصی) برای رمزگذاری و رمزگشایی پیام‌ها در سمت کاربران (Endpoints) ذخیره می‌شوند. به همین دلیل، حتا در سمت سرور هم محتوای پیام‌ها قابل خواندن نیستند.

## پیام‌رسان‌ها

هرگونه مکالمه‌ای که شما برای ارتباط با دوستان، خانواده و همکاران‌تان دارید، نیازمند مراقبت و حفاظت است. امروزه، چت‌های خصوصی و گروهی از ساده‌ترین روش‌ها برای برقراری ارتباط هستند. اما چقدر از حریم خصوصی مکالمات خود اطمینان دارید؟

برای این‌که بتوانیم یک پیام‌رسان را قابل اعتماد بدانیم، باید ویژگی‌های امنیتی و محافظتی پیام‌رسان را بررسی کنیم.

| ویژگی‌ها | SIGNAL | WIRE | WHATSAPP | TELEGRAM | iMESSAGE | FACEBOOK MESSENGER |
|---|---|---|---|---|---|---|
| ارائه‌گزارش‌شفافیت | ✓ | ✓ | ✓ | ✗ | ✓ | ✓ |
| جمع‌آوری اطلاعات کاربران | ✗ | ✗ | ✓ | ✓ | ✓ | ✓ |
| رمزگذاری پیش‌فرض | ✓ | ✓ | ✓ | ✗ (secret chats only) | ✓ | ✗ |
| متن باز (کد و سرور) | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| متادیتای رمزگذاری‌شده | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ |
| ذخیره‌سازی آی‌پی و زمان | ✗ | ✓ | ✓ | ✓ | ✓ | ✓ |
| آیا ازدادن اطلاعات به سازمان‌های اطلاعاتی خودداری کرده؟ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ |

## توصیه‌های امنیتی برای استفاده از پیام‌رسان‌ها

- **کد ثبت‌نام و یا تغییر رمز عبور را هرگز با هیچ‌کس به اشتراک نگذارید!**

کدی که از طریق شماره تلفن به شما ارسال می‌شود را با هیچ‌کس به اشتراک نگذارید. با اشتراک‌گذاری این کد در حقیقت شما اجازه‌ی تغییر رمز عبور و دسترسی به حساب تان را برای شخصی دیگری اعطا می‌کنید.

- **فعال‌سازی تایید دو مرحله‌ای**

تایید دومرحله‌ای یک لایه امنیتی مستحکمی است که دیگران حتا با داشتن رمز عبور تان نمی‌توانند وارد حساب شما شوند. همه‌ی پیام‌رسان‌های امروزی از این ویژگی پشتیبانی می‌کنند و با رفتن به قسمت تنظیمات امنیتی در این برنامه‌ها می‌توانید این گزینه را فعال کنید.

- **بررسی تنظیمات حریم خصوصی**

اکثر پیام‌رسان‌ها این اجازه را به شما می‌دهد تا تصمیم بگیرید چه قسمتی از اطلاعات شخصی و وضعیت فعالیت تان را در پلتفرم شان در معرض نمایش عمومی قرار بدهید و چه اطلاعاتی را خصوصی نگهدارید. با رفتن به قسمت تنظیمات حریم خصوصی می‌توانید کنترل بیشتری روی حریم خصوصی تان داشته باشید.

- **استفاده از پیام‌های رمزگذاری‌شده در گفت‌وگوی‌های حساس**

اگر محتوایی که در پیام رد و بدل می‌کنید، حساس است و می‌خواهید محرمانه باقی بمانند، از پیام‌رسان‌هایی استفاده کنید که حالت End-To-End Encryption را پشتبانی می‌کنند. مثل: واتساپ، سگنال، تلگرام و مسنجر (این حالت تنها در چت مخفی یا Secret Chat در دسترس هستند).

- **مراقب چیزهایی که به اشتراک می‌گذارید باشید!**

هر محتوا و یا پیامی که ارسال می‌کنید قابلیت ذخیره شدن و یا کپی شدن توسط مخاطب شما را دارد، پس مواظب باشید چه چیزی را به اشتراک می‌گذارید!

- **از ویژگی‌های ایمنی و امنیتی استفاده کنید.**

پیام‌رسان‌ها به‌طور پیش‌فرض ویژگی‌های امنیتی زیاد در اختیار کاربران می‌دهند تا با استفاده از آن‌ها بتوانید امنیت حساب تان را افزایش دهید. قفل دسترسی، مخفی‌سازی چت‌ها و تایید دو مرحله‌ای از مواردی است که می‌توانید آن‌ها را از قسمت تنظیمات امنیتی پیام‌رسان‌ها فعال‌سازی کنید.

- **مخاطبین و پیام‌های مشکل‌ساز و مخرب را بلاک کنید و گزارش دهید**

بعضی از مخاطبان شما ممکن است به صورت عمد/غیر عمد محتواهای مشکل‌ساز را با شما به اشتراک بگذارد، بلاک کردن مخاطبین و گزارش (Report) کردن این کاربران کمک می‌کند که از خود و دیگران در آن پلتفرم محافظت کنید. برای مثال: پیام‌هایی با پیشکش‌های باورنکردنی از سوی مخاطبین تا ممکن است با شما به اشتراک گذاشته شود و با باز کردن لینک متوجه می‌شوید که به یک وبسایت غیرمعتبر هدایت شده‌اید. برای جلوگیری از گسترش چنین پیام‌هایی، پیام و مخاطبین مشکوک را گزارش دهید.

- **هرگز از نسخه‌های غیررسمی پیام‌رسان‌ها استفاده نکنید!**

در حالی که نسخه‌های غیررسمی اغلب جذاب هستند و ویژگی‌های اضافه‌ی زیادی را ارائه می‌کنند، اما خطرات امنیتی قابل توجهی نیز به همراه دارند. نسخه‌های غیررسمی ممکن است داده‌های کاربران را سرقت کنند و از آن‌ها برای مقاصد مخرب سواستفاده کنند.

- **در صورت از دست دادن تلفن، حساب تان را غیرفعال کنید.**
- **استفاده از قابلیت پیام‌های مدت‌دار یا disappearing message**

این گزینه به صورت پیش‌فرض در پیام‌رسان‌ها غیرفعال است. با فعال‌سازی این گزینه پیام‌ها به صورت اتومات بعد از مدت تعیین‌شده پاک خواهند شد.

## توصیه‌های امنیتی در هنگام تماس‌های تصویری و جلسات آنلاین

- **استفاده از نوارچسپ برای پوشاندن وب‌کم**
- **پنهان‌سازی محتوا، اشخاص و نشانه‌های حساس پس‌زمینه و اشیای شامل کادر**
- **استفاده از وی‌پی‌ان برای پنهان‌سازی موقعیت و فعالیت**
- **خاموش نگه داشتن میکروفون**
- **وقتی از ابزار جدیدی برای تماس و یا جلسات استفاده می‌کنید، قبل از وصل شدن به جلسه چند دقیقه‌ای وقت بگذارید تا با ابزار و قسمت‌های مختلف آن آشنا شوید.**

## اقدامات موثر در مواقعی که سرعت انترنت پایین است

- خاموش کردن وب‌کم (کامره) برای کاهش حجم مصرفی انترنت و بهبود کیفیت جلسه
- بستن برنامه‌های اضافی (ممکن است برنامه‌های اضافی از انترنت شما مصرف کنند پس در نتیجه بر روی کاهش سرعت انترنت تاثیر داشته باشند)
- وصل شدن از طریق کیبل به روتر
- از دیگران بخواهید استفاده‌ی سنگین از انترنت را کاهش دهند

## قابلیت‌های امنیتی و حریم‌خصوصی در پیام‌رسان‌ها

بعضی از قابلیت‌هایی که با فعال کردن آن‌ها در پیام‌رسان‌ها می‌توانید امنیت و حریم‌خصوصی تان را قوی‌تر بسازید.

| | | |
|---|---|---|
| ▪ تایید دو مرحله‌ای<br>▪ پیام‌های مدت‌دار<br>▪ عکس‌ها و فیلم‌های محوشونده<br>▪ فعال‌سازی Touch ID و Face ID (تنها در آیفون)<br>▪ گزارش و بلاک مخاطبین و محتوای مشکوک<br>▪ فعال‌سازی قفل چت | ▪ تایید دو مرحله‌ای<br>▪ چت خصوصی (Secret Chat) برای چت‌های حساس<br>▪ قفل برنامه<br>▪ پیام‌های مدت‌دار<br>▪ مخفی‌سازی شماره‌تلفن | ▪ چت خصوصی<br>▪ پیام‌های محوشونده<br>▪ امنیت بیشتر با قفل برنامه |

* تلگرام و مسنجر به صورت پیش‌فرض از حالت رمزگذاری End-to-end در هنگام ارسال پیام پشتیبانی نمی‌کنند، با استفاده از حالت چت خصوصی (Secret Chat) می‌توانید از این قابلیت بهره‌مند شوید.

## ایمیل

روزانه حدود ۳۰۰ میلیارد ایمیل در سراسر جهان ارسال و دریافت می‌شود. با توجه به اهمیتی که ایمیل در زندگی شخصی و کاری مان دارد، چنین عددی دور از تصور نیست. در واقع، بیشتر سازمان‌ها بدون آن، احتمالاً دچار مشکلات اداری و ارتباطی خواهند شد. برعکس مفهوم ساده‌ای که ایمیل و استفاده آن دارد، اما ایمیل ریسک‌های زیادی را برای کسب‌وکارها به همراه دارد که بیشتر افراد از آن آگاه نیستند.

ایمیل یکی از اهداف محبوب برای هدف قرار گرفتن حملات انترنتی است. بنابراین، شرکت‌ها و افراد باید حساب‌های ایمیل خود را در برابر حملات رایج و تلاش برای دسترسی غیرمجاز به حساب‌ها یا محتوای ارتباطات ایمن کنند.

## توصیه‌های امنیتی برای بالابردن امنیت ایمیل

- کارمندان را آموزش دهید

با دایر نمودن جلسات آموزشی مدیران، کارمندان آی‌تی و متخصصین شرکت‌ها اهمیت امنیت ایمیل، ارزش داده‌های حساس و عواقب یک حمله یا فیشینگ را درک می‌کنند.

- تنظیمات امنیتی ایمیل را بهینه‌سازی کنید
- تایید دو مرحله‌ای را فعال کنید
- ایمیل‌های حساس را رمزگذاری کنید
- متوجه ایمیل‌های مخرب، لینک‌ها و فایل‌های ضمیمه شده باشید؛ مخصوصاً ایمیل‌هایی که در پوشه Spam هستند
- فایل‌ها / لینک‌ها را قبل از دانلود اسکن کنید و یا از پیش‌نمایش استفاده کنید.
- ایمیل تان را وارد هر سایتی نکنید!
- از سرویس‌های ایمیل معتبر و رمزگذاری شده استفاده کنید.

## سرویس‌های پیشنهادی ایمیل

| ProtonMail | Gmail | Outlook |
|---|---|---|
| ▪ متن‌باز، حریم شخصی محور و رمزگذاری (E2E) پیش‌فرض<br>▪ رایگان<br>▪ تنظیمات امنیتی پیشرفته | ▪ امنیت بالا<br>▪ سازگاری بالا با خدمات دیگر گوگل<br>▪ رایگان<br>▪ حریم خصوصی کمتر (در مقایسه با پروتون) | ▪ امنیت بالا<br>▪ رمزگذاری E2E<br>▪ رایگان<br>▪ سازگاری بالا با سایر خدمات مایکروسافت |

## شبکه‌های اجتماعی

وقتی صحبت از امنیت شبکه‌های اجتماعی می‌شود، تهدیدات متعددی وجود دارد که باید از آن‌ها آگاه باشیم. محققان امنیتی می‌گویند: رایج‌ترین کلاهبرداری‌های شبکه‌های اجتماعی توسط هکرهای ماتریکس‌مانند در یک اتاق تاریک انجام نمی‌شود، بلکه معمولاً از طریق مفهومی

به نام «مهندسی اجتماعی» اجرا می‌شود. در این روش از فریب دادن کاربران در جهت انجام اشتباهات امنیتی یا دادن اطلاعات حساس استفاده می‌کنند.
در کنار مسایل امنیتی، حریم و اطلاعات شخصی بحث مهم دیگر در شبکه‌های اجتماعی است که اکثر مردم بدون توجه به آن شروع به اشتراک‌گذاری و نمایش اطلاعات شخصی شان در شبکه‌های اجتماعی می‌کنند. این اطلاعات ممکن است توسط شرکت‌ها برای اهداف تجاری و یا کلاهبرداران برای مقاصد مخرب و سواستفاده، علیه شما استفاده شود.

## اقدامات امنیتی برای بالا بردن امنیت حساب شبکه‌های اجتماعی

- **استفاده از رمز ورود قوی دارای طول ۱۲ حرفی یا بیشتر، دارای حروف کوچک و بزرگ، عدم**
استفاده از کلمات عام، متفاوت از رمزهای گذشته‌ی شما و متشکل از ترکیب کارکترهای مخصوص (#، %،$،@)
کراکرها (هکر و کراکر دو واژه‌ی مختلف با مقاصد مختلف است. کراکرها ابزار جدیدی نمی‌سازند بلکه از ابزارهای دیگری برای اهداف مخرب خود استفاده می‌کنند و به شبکه آسیب می‌رسانند) معمولاً لیستی از ترکیب کلمات و رمزهای پرکاربرد و در معرض خطر قرار گرفته (compromised) استفاده می‌کنند تا وارد یک سیستم شوند و به شخص هدف یا شبکه آسیب برسانند. به همین دلیل از رمز ورود یکسان، قابل حدس و یا در معرض خطر قرار گرفته برای حساب‌های تان در شبکه‌های اجتماعی استفاده نکنید!
- **از یک رمز برای تمام حساب‌های تان استفاده نکنید**
- **تایید دو مرحله‌ای را فعال کنید**
- **تنظیمات امنیتی و حریم خصوصی را بهینه‌سازی کنید**
- **مواظب لینک‌ها و محتوای مخربی که از طریق پیام‌خانه و یا در بین کاربران به‌اشتراک گذاشته می‌شود، باشید!**
برای مثال: در سال ۲۰۲۲، کمپین مخربی «Ducktail» در شبکه اجتماعی لینکدین به قصد هدف قرار دادن کارمندان پیدا شد. آن‌ها یک فایل پیوست حاوی بدافزار را روی شبکه به اشتراک گذاشتند که از کوکی‌های مرورگر برای ربودن حساب‌های تجاری فیسبوک شخص هدف استفاده می‌کرد. به همین دلیل مواظب لینک‌ها و فایل‌هایی که با شما به اشتراک گذاشته می‌شود باشید!
- **مواضب فیشینگ و لینک‌های مشکوک با ضاهر مشابه باشید!**
در این روش مهاجمان با ساختن یک صفحه‌ی جعلی مشابه با صفحه‌ی ورود شبکه‌ی اجتماعی مورد نظر، قصد دزدی مشخصات ورود شما و در دست گرفتن کنترل حساب شما را دارند! در این روش همیشه صفحات لینک متفاوتی دارند و مهاجمین سعی دارند با ایجاد تشابه و یا حداقل شامل‌سازی نام شبکه‌ی اجتماعی شما را فریب دهند. برای مثال، استفاده از آدرس‌هایی همچون: yuotube.com یا youtube.ml و یا حتا youtube-login-page.com به جای youtube.com که دومین رسمی وبسایت یوتیوب است.
- **خودداری از اعطای مجوز به برنامه‌های شخص ثالث برای دسترسی به پروفایل شما**

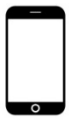
برخی از اپ‌ها و وبسایت‌ها ادعای جذب فالور، کسب درآمد، تایید حساب و یا ادعاهای مشابه را دارند، اعطای مجوز به آن‌ها اجازه سرقط و سواستفاده از اطلاعات شخصی و داشتن کنترل قسمی حساب تان را می‌دهد.

## امنیت دستگاه‌ها

امنیت دستگاه، دفاع از دارایی‌های دیجیتال در برابر آسیب و استفاده غیرمجاز است. اگرچه اصطلاح «امنیت دستگاه» به اندازه «امنیت سایبری» به طور گسترده مورد استفاده قرار نمی‌گیرد، اما مفهومی مرتبط است که به طیف گسترده‌ای از اقدامات برای ایمن‌سازی کامپیوترهای شخصی رومیزی، لپ‌تاپ‌ها، تلفن‌های هوشمند، تبلت‌ها یا دستگاه‌های دیگری که قابلیت اتصال به انترنت را دارد، اشاره می‌کند.

برای دفع مطمئن تهدیدات امنیتی مدرن، یک استراتژی امنیتی دستگاه باید چند لایه باشد، با چندین راه‌حل امنیتی که در پشت سر هم با یکدیگر کار می‌کنند. علاوه بر این، هم پرسنل امنیتی و هم کاربران (End-users) باید با بهترین شیوه‌ها، مانند به‌روز نگه‌داشتن نرم‌افزار و استفاده از نقاط دسترسی (Access Points) یا دروازه‌های (Gateways) مناسب هنگام دسترسی از راه دور به برنامه‌ها، هم‌سو باشند.

## توصیه‌های امنیتی برای بالا بردن امنیت دستگاه‌ها



### تلفن‌های هوشمند

- استفاده از رمز صفحه پیچیده.
- بروزرسانی مداوم سیستم‌عامل و برنامه‌های کاربردی.
- خودداری از استفاده‌ی برنامه‌ها و فایل‌های نصبی کرک شده (برنامه‌های کرک‌شده معمولاً حاوی بدافزار هستند که ممکن است به محتوا و دستگاه شخصی تان آسیب برساند).
- بررسی مجوزهای دسترسی برنامه‌ها
- پنهان‌سازی نمایش اعلانات حساس در قفل صفحه نمایش.
- بهینه‌سازی تنظیمات امنیتی حساب گوگل متصل به تلفن.

### کامپیوترهای شخصی

- استفاده از رمز ورود (ترجیحاً رمز پیچیده)
- رمزگذاری هارد / فایل‌های حساس
- خودداری از نصب و استفاده نرم افزارهای کرک شده
- استفاده از ابزارهای امنیت و افزایش حریم خصوصی. مثل: آنتی ویروس و وی‌پی‌ان
- پشتیبان‌گیری (بکاپ) از اطلاعات حساس و مهم به‌صورت منظم در یک فضای ابری
- احتیاط و بررسی در اتصال و استفاده‌ی دیوایس‌های جانبی (مثل فلش و مموری)

| | |
|---|---|
| ▪ خودداری از ذخیره‌سازی اطلاعات حساس در حافظه‌های جانبی.<br>▪ فعال‌سازی قفل سیم‌کارت. | ▪ قفل یا خاموش کردن کامپیوتر قبل از ترک آن |

## فعالیت ناشناس در وضعیت جاری

این راهنما برخی از بهترین روش‌ها برای امنیت دیجیتال در وضعیت کنونی افغانستان را پوشش می‌دهد، به‌ویژه برای جلوگیری از نظارت بر ارتباطات، مکان و هویت شما. به یاد داشته باشید، هیچ امنیت کاملی وجود ندارد. در هر شرایطی ممکن است بر پرتکل‌های امنیتی شما غلبه کنند، اما هرچه کار آن‌ها را سخت‌تر کنید، احتمال تلاش آن‌ها کم‌تر می‌شود و منابع کم‌تری برای هدف قرار دادن دیگران خواهند داشت. شما می‌توانید اقدامات لازم را انجام دهید تا از یک هدف‌گیری آسان و حتا حمله جلوگیری کنید.

همه‌چیز با روش‌های جدید هدف گیری اطلاعات افراد و همین‌طور در مقابل، روش‌های جدید برای محافظت در برابر این تهدیدات دایماً تغییر می‌کند. مسأله‌ی مهم این است که از تازه‌ترین روش‌های امنیتی باخبر و بروز باشید تا سیستم‌ها و اطلاعات شما در برابر حملات جدید محافظت شوند.

## مهم‌ترین نکات و اقداماتی که باید در نظر بگیرید

1. همیشه نرم‌افزارهای تان را بروز (Updated) نگهدارید.
2. تایید دو مرحله‌ای را فعال کنید.

قدم اول: از نو شروع کنید

الف: شخصیت جدید بسازید. (ابزارهای متن‌باز زیادی برای ایجاد یک شخصیت تصادفی وجود دارد)

ب: تصویر پروفایل تصادفی استفاده کنید.

ت: شخصیت تازه ساخته شده را برای ایجاد حساب‌های دیجیتالی خود استفاده کنید. از ایمیل، شماره تماس و تلفن مشعل (burner) در مواقع حساس (مخصوصاً در هنگام تظاهرات) استفاده کنید.

قدم دوم: مکان خود را پنهان کنید (مکان فعلی و قبلی)

الف: بررسی تنظیمات پیش‌فرض مکانی در تلفن

- آندروید: https://support.google.com/accounts/answer/3467281?hl=en
- آیفون: https://support.apple.com/en-us/HT207092
- https://lifehacker.com/psa-your-phone-logs-everywhere-you-go-heres-how-to-t-١٤٨٦٠٨٥٧٥٩

ب: کیف/کیسه فارادی دستگاهی است که از سیگنال‌هایی که از تلفن شما می‌آید و می‌تواند مکان شما را ردیابی کند، جلوگیری می‌کند. توصیه می‌کنیم تلفن و لپتاب خود را در کیف فارادی

در مواقعی که از آن استفاده نمی‌کنید، نگهداری کنید. پیچاندن تلفن‌ها و لپ‌تاپ‌ها با قلع/المونیم همچنان می‌تواند کمک کند.

ت: از ابزارهایی مانند قفل مایک (Mic Lock) برای مقابله با شنود استفاده کنید.

قدم سوم: محافظت از داده‌ها و ارتباطات

الف: امنیت اطلاعات، ایمیل، لیست مخاطبین، تصاویر، ویدیوها و غیره...

- رمزگذاری (Encryption) را در تلفن‌های شخصی تان فعال کنید:
  - آیفون: https://www.zdnet.com/article/how-to-turn-on-iphone-ipad-encryption-in-one-minute/
  - آندروید: https://www.androidcentral.com/how-enable-encryption-android
- رمزگذاری را در لپتاب‌های تان فعال کنید:
  - مک‌اواس: https://support.apple.com/en-us/HT204837
  - ویندوز: https://support.microsoft.com/en-us/windows/turn-on-device-encryption-0c453637-bc88-5f74-5105-741561aae838
- ورود از طریق بایومتریک را خاموش کنید (شناسایی چهره و یا اثر انگشت) و رمز عبور را روشن کنید. این کار از ورود از طریق بیومتریک شما، برای باز کردن دستگاه شما در حالاتی که تحت فشار و شکنجه‌ی فزیکی هستید، جلوگیری می‌کند.

ب: هنگام گشت‌وگذار آنلاین ایمن باشید

- از مرورگر تور استفاده کنید.
- از سیستم‌عامل Tails استفاده کنید. این سیستم‌عامل به منظور اجرا از طریق فلش ساخته شده است و از پرتکل امن تور برای وب‌گردی استفاده می‌کند.
- از وی‌پی‌ان استفاده کنید. وی‌پی‌ان‌های رایگان متعددی وجود دارند که می‌توانند ردیابی فعالیت‌های آنلاین شما را دشوار سازد.
  - TunnelBear, ExpressVPN, NordVPN همه گزینه‌های خوبی هستند. درحال حاضر TunnelBear ۱۰ جی‌بی پهنای باند مصرفی رایگان برای کاربران افغانستان در نظر گرفته است.
  - ProtonVPN و Lantern از دیگر وی‌پی‌ان‌های رایگان و متن‌باز است.
  - وی‌پی‌ان‌های خوب برای دور زدن سانسور: Mullvad، Bitmask، VPNGate.
  - با استفاده از OpenVPN می‌توانید وی‌پی‌ان خود تان را راه‌اندازی کنید. اما سطح دانش تخنیکی بالاتری نیاز دارد و امنیت آن متکی به کاربر است تا یک سازمان.
  - اگر از هیچ‌یک از این وی‌پی‌ان‌ها استفاده نکردید و به سلیقه خود یکی دیگر را انتخاب کردید، مطمئن شوید که خوب کار می‌کند و رتبه‌ی خوبی بین کاربران و سازمان‌های شخص ثالث (Third-party) دارد.

ت: دسترسی به انترنت

- وای‌فای تان را روشن نکنید تا زمانی که مطمئن نشدید شبکه‌ای که قصد وصل شدن به آن را دارید مصون است.
- از کیف / کیسه فارادی برای محافظت از سیگنال‌های وقتی که درحال حرکت هستید برای لپتاپ یا تلفن تان استفاده کنید. یا با قلع / آلمونیم بپیچانید.

ث: پیام‌رسان‌های سراسر مصون (End-to-end Encrypted)

- گزینه‌های زیادی برای این کار وجود دارد. سیگنال، تلگرام و واتساپ بهترین گزینه‌ها هستند.
- تلگرام امن هست؟ نه به صورت پیش‌فرض، مطمئن شوید قابلیت Secure Chat فعال است.
- سیگنال به‌خاطر شرایط حریم خصوصی آن بهتر از واتساپ است. اگر از واتساپ استفاده می‌کنید، آخرین نسخه‌ی رسمی آن‌را دانلود کنید و قابلیت پیام‌های محو شونده (بعد از ۱ هفته) را فعال کنید.

ج: ایمیل‌های رمزگذاری‌شده. سرویس‌های ایمیل رایگان و مصون وجود دارند که شامل:

- ProtonMail – عنوان ایمیل را رمزگذاری نمی‌کند.
- Tutanota – عنوان ایمیل را رمزگذاری می‌کند.
- برای فایل‌های ضمیمه‌شده‌ای رمزگذاری‌شده از Sendsafely استفاده کنید.
- Gmail هم امن است.

قدم چهارم: از خود در برابر بدافزارها محافظت کنید

- مبایل – حملات فیشینگ از طریق اس‌ام‌اس:
  روی لینک‌های که از طرف شماره‌های ناشناس دریافت می‌کنید، کلیک نکنید!
- کامپیوتر – حملات فیشینگ از طریق ایمیل:
  روی لینک‌هایی که از طریق ایمیل‌های ناشناس دریافت می‌کنید، کلیک نکنید!
- آنتی‌ویروس – آنتی‌ویروس‌های رایگان می‌تواند شما را کمک کند:
  - Sophos at home
  - Bitdefender
  - Adaware
  - AVG

قدم پنجم: از انتقال فایل ناشناس استفاده کنید

- لیست خدمات ذخیره‌سازی فایل آنلاین که نیازی به ثبت نام ندارند با رمزگذاری تا ۳۰ روز.

## اقدامات زمان قطع کلی انترنت

آماده بودن برای قطع کامل، خواه عمدی، خواه بر اثر قطع برق یا حوادث طبیعی، و برنامه‌ریزی‌های اساسی برای استفاده از ابزارهای که بتوانید با دوستان/ همکاران به‌طور مصون در تماس باشید را در نظر بگیرید.

یادداشت: هرگونه اپلیکیشن که سبک «توری» (Mesh) دارد از نظر حریم خصوصی و امنیت یک معامله بده‌بستان می‌باشد. برای اینکه در یک اپلیکیشن داخل شوید و از آن کار بگیرید، باید قصد اتصال تان را پخش و نشر کنید که ممکن مورد بررسی و ردیابی قرار بگیرید، حتا اگر پیام‌های ارسالی رمزگذاری شده هم باشند.

- Briar – تنها در سیستم عامل آندروید موجود است. در صورت موجود بودن، از Tor استفاده می‌کند و یا با سایر کاربران Briar از طریق بلوتوث یا وای‌فای هنگامی که در مجاورت قرار بگیرند، پیام ارسال می‌کند. فقط در صورتی کار می‌کند که افراد برای بلوتوث (۳۰ متر) یا وای‌فای (حداکثر ۱۰۰ متر) به اندازه‌ی کافی نزدیک باشند.
- Bridgefy – برای هردو سیستم عامل آندروید و آی‌اواس در دسترس است. امنیت کمتری دارد، نسبت به Briar اما تیم کاری شان در جهت بهبود امنیت برنامه تلاش‌های زیادی دارند.
- Silence.im – چت رمزگذاری شده را از طریق پیامک (SMS) ارائه می‌دهد بنابراین اگر پیامک (SMS) هنوز کار می‌کند و هر دو طرف اپلیکیشن Silence را دارند، می‌توانند ارتباط مصونی را برقرار کنند.

## توصیه‌های کلی برای فعالیت و کار ناشناس

- **جداسازی حساب‌ها، دیتاها، سیم‌کارت‌ها و دستگاه‌های کاری و شخصی**
- **رد پا به‌جا نگذاریم!**

هرگونه رد پایی که منجر به، به‌خطر افتادن هویت و جان شما می‌شود را پاک و یا منتقل کنید. این شامل تاریخچه‌ی فعالیت شما در دیوایس‌های شما، فایل‌های شما، برنامه‌های مورد استفاده و مخاطبین تان می‌شود.

- **استفاده از ایمیل به‌جای شماره‌تلفن در وقت ثبت‌نام**

از ایمیل برای ثبت‌نام و ورود به حساب‌های شبکه‌های اجتماعی و یا سایر حساب‌های فضای مجازی تان استفاده کنید. ایمیل امنیت بیشتری دارد و تنها شما دسترسی به آن دارید.

- **اشتراک‌گذاری گذرواژه‌های دستگاه‌ها، حساب‌های آنلاین و غیره با یک فرد قابل اعتماد که در معرض خطر نیست!**

این کار باعث می‌شود زمانی که در معرض خطر هستید و امکانات و زمان کافی برای دسترسی و ایجاد تغییرات در حساب‌های آنلاین تان را ندارید، با تماس با فرد مورد نظر، از او بخواهید این کار را برای تان انجام دهد.

- **با اقداماتی که باید انجام شود، به عنوان اولین واکنش به بازداشت احتمالی خود موافقت کنید.**

زمانی که شما بازداشت می‌شوید یا قرار است مورد بازجویی قرار بگیرید، فرصت کافی برای تصمیم‌گیری و برنامه‌ریزی برای اقداماتی که باید انجام بدهید ندارید، پس بهتر است این موارد را از قبل برنامه‌ریزی کنید.

- **بعد از بررسی دستگاه‌های تان حتماً برای تنظیمات کارخانه و یا نصب‌دوباره سیستم‌عامل اقدام کنید.**

اگر دستگاه‌های تان بررسی می‌شود و دوباره برای تان بازگردانیده شد، در صورت مشکوک بودن می‌توانید دستگاه تان را به تنظیمات کارخانه برگردانید تا از نبود نرم‌افزارهای شنود مطمئن شوید.

## پیام‌رسان‌ها

- استفاده از ایمیل به‌جای شماره
- جداسازی سیم‌کارت‌های کاری و شخصی
- فعال‌سازی گزینه حذف خودکار پیام‌ها / حذف دستی چت‌های حساس + حذف فایل‌های ضمیمه
- استفاده از نسخه‌های تحت وب پیام‌رسان‌ها، در حالت ناشناس مرورگر

## شبکه‌های اجتماعی

- شبکه‌های اجتماعی امن نیستند!
- استفاده از حساب‌های ناشناس
- تغییر کامل اطلاعات در صورت تغییر هویت
- مخفی‌سازی هویت در همه‌ی شبکه‌های اجتماعی
- استفاده از ایمیل در ساخت حساب‌ها

## امنیت دستگاه‌ها

- کامپیوترهای شخصی
  - استفاده از حالت ناشناس در مرورگر
  - حذف و غیرقابل بازیافت نمودن فایل‌های حساس
  - ذخیره و نگهداری فایل‌ها در فضای ابری / رمزگذاری و ذخیره در فضاهای قابل حمل (فلش)
  - استفاده از نرم‌افزارهای مدیریت رمز عبور
  - استفاده از ابزارهای آنلاین تحت‌وب برای امور کاری:
    - مجموعه‌ی آفیس گوگل
    - تلگرام تحت وب
    - فوتوپیا (فتوشاپ آنلاین) و دیگر ابزارهای مورد نیاز...
- تلفن‌های هوشمند
  - رمزگذاری و ذخیره فایل‌ها در فضای کلود
  - جداسازی حساب کاری و شخصی
  - از حساب‌های کاری و حساس خارج شوید
  - حافظه را غیر قابل بازیابی کنید
  - وبگردی‌های حساس را در حالت ناشناس انجام دهید
  - مواظب مخاطبین دفترچه تلفن تان باشید

منابع:


1. https://humanrightsfirst.org/library/steps-to-protect-your-online-identity-from-the-taliban-digital-history-and-evading-biometrics-abuses/

2. https://helpdesk.rsf.org/digital-security-guide/afghanistan-digital-care-guide/

3. https://www.accessnow.org/online-safety-resources-afghanistan/

4. https://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/privacyconfidentiality/DigitalSecurityBasics-Privacy-Advocacy-Guides_v2.pdf

موفق و پیگیر باشید!