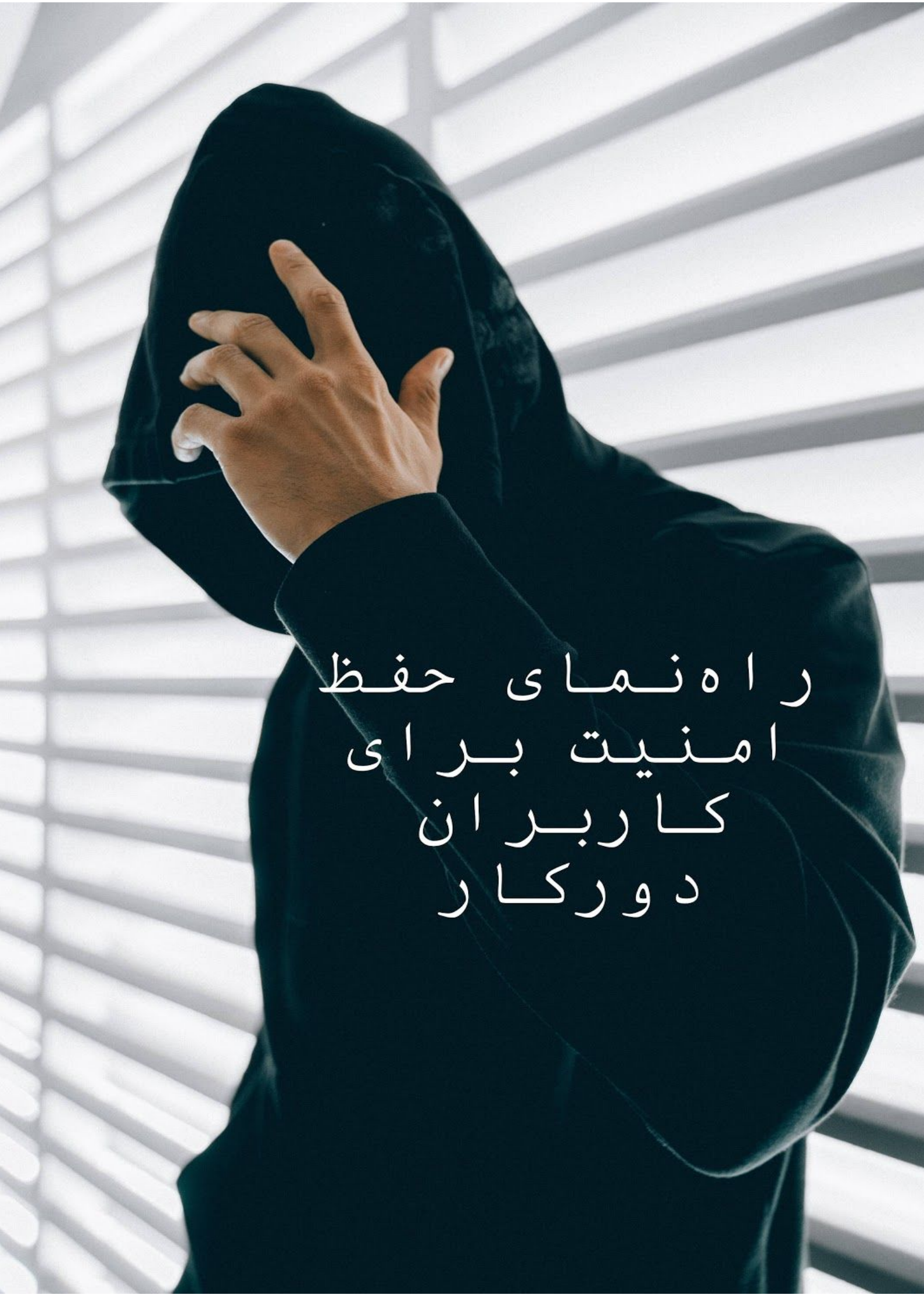


راهنمای حفظ امنیت برای کاربران دورکار

راهنمای حفظ امنیت برای کاربران دورکار

به همراه معرفی سرویس‌هایی که در دورکاری به کارتان می‌آیند

تهیه کننده: محسن احمدی، مدیر محصول، مدیر پروژه و اسکرام مستر

یادداشت گردآورنده

اگرچه کار از راه دور در بین شرکت‌های نرم‌افزاری پیش از این نیز رایج بوده است، اما بسیاری از شرکت‌ها در پاسخ به شیوع ویروس کرونا و شرایط اضطراری پیش‌رو؛ برای اولین بار دورکاری را با تیم‌های توزیع‌شده تجربه می‌کنند.

ایده اصلی این مستند یکپارچه‌سازی و اشتراک‌گذاری تجربیات، راهنماها و ایده‌هایی‌ست که توسط معتبرترین و موفق‌ترین شرکت‌ها [که از سالیان گذشته با تیم‌های توزیع‌شده پروژه‌های خود را به‌پیش برده‌اند] به صورت پراکنده در قالب مقالات و مستندات مختلف انتشار یافته و مرجعی برای شرکت‌ها و کسب‌وکارهایی‌ست که با تیم‌های توزیع‌شده و دورکار پروژه‌های خود را به پیش می‌برند.

در روزهای ابتدایی شروع این مستند، می‌خواستم تا این راهنما در دو بخش مجزا (ویژه کسب‌وکارها و خاص افراد و اعضای تیم‌های توزیع‌شده) تهیه شود که در ادامه و به دلیل جلوگیری از مطول شدن راهنما، بر آن شدم تا مستند در قالب کتابچه‌هایی با عناوین مختلف و کوتاه‌تر منتشر شود.

این کتابچه، اولین بخش از این مجموعه بوده و امیدوارم، راه‌نما و راه‌گشای افراد، کسب‌وکارها و شرکت‌هایی باشد که با تیم‌های توزیع‌شده مشغول به کار هستند.

در صورت وجود هر ابهام، انتقاد و یا پیشنهادی، می‌توانید از طریق وب سایت من، با من در ارتباط باشید.

محسن احمدی

مدیر محصول، مدیر پروژه و اسکرام مستر

اردیبهشت ۹۹

فهرست مطالب

یادداشت گردآورنده

اطمینان از ایمنی داده‌ها

رمزگذاری دستگاه‌ها

به‌روز رسانی مداوم سیستم عامل

به‌روز رسانی مداوم نرم‌افزارها

غیرفعال سازی ورود خودکار

فعال سازی قفل خودکار

از رمز یا پین‌های قوی استفاده کنید

تایید هویت دو مرحله‌ای را فعال کنید

در شبکه‌های عمومی یا غیر قابل اعتماد از VPNهای امن استفاده کنید

لیستی از ابزارهای کاربردی

اطمینان از ایمنی داده‌ها

در حالی که تیم‌های توزیع‌شده، در حال افزایش‌اند، با این حال برخی از سازمان‌ها و رهبران آن‌ها به دلیل خطرات امنیتی درک شده برای فعالیت از راه دور کارمندان خود مقاومت می‌کنند. دسترسی کارمندان به داده‌های مهم سازمان از طریق یک وای‌فای عمومی ناایمن در یکی از دور افتاده‌ترین مناطق دنیا، از کابوس‌های به‌جای مدیران کسب‌وکارهاست. اما همانطور که پیش‌تر هم گفته شد، باید با این حقیقت کنار آمد که آینده، راهی به‌جز تعامل و به‌کارگیری تیم‌های توزیع‌شده برای ما باقی نخواهد گذاشت و شرکت‌ها باید ضمن حفظ امنیت داده‌های‌شان، روش‌هایی را پیدا کنند که قابلیت انعطاف‌پذیری مکانی را برای کارمندان و تیم‌های خود محیا کنند.

تا زمانی که دستگاه‌های ما به اینترنت متصل‌اند، ما در معرض خطر قرار داریم. از لپ‌تاپ‌های شخصی گرفته تا لوازم آشپزخانه یا دستیاران صوتی و دستگاه‌های جدیدی که هر روز به خانه‌های‌مان وارد می‌کنیم.

براساس گزارش HIBP ، بیش از ۱۳۰ میلیون اکانت شخصی، در بیش از ۴۰۰ سرویس و در مجموع بیش از ۹ میلیارد بار مورد سوءاستفاده قرار گرفته است. این گزارش ترسناک، تنها بخش کشف شده‌ای از این سوءاستفاده‌ها و نقض‌های حریم شخصی و داده‌های افراد است. حملات هدفمند و مهندسی‌های اجتماعی، روز به‌روز بیشتر می‌شود و ما همچنان نوک این کوه یخ را می‌بینیم.

رهنمودها و توصیه‌های شرکت‌های بزرگ به کارمندان‌شان اغلب بسیار ساده‌تر از آن چیزی‌ست که ما تصور کنیم.

در این بخش به حداقل اقداماتی که اعضای تیم‌های توزیع شده یا دورکار لازم است که برای محافظت از اطلاعات شرکت‌ها انجام دهند بیان شده است. هرچند که بسیاری از این نکات ساده، در حفظ امنیت داده‌های شخصی آنان نیز موثر است، اما هدف ما در این‌بخش صرفا تاکید بر حفاظت از داده‌های سازمانی توسط این تیم‌هاست.

رمزگذاری دستگاه‌ها

رمزگذاری به جلوگیری از دسترسی غیر مجاز به داده‌های موجود در دستگاه‌های شما کمک می‌کند. این کار را با ابزارهای ساده کدگذاری اطلاعات به روشی انجام دهید که کشف آن توسط افراد غیرمجاز دشوارتر شود. این امر می‌تواند [به ویژه در صورت از بین رفتن یا دزدیده شدن دستگاه] از اهمیت بالایی برخوردار باشد.

در اینجا می‌توانید چگونگی فعال کردن و رمزگذاری دستگاه‌تان را ببینید؛

- نرم‌افزار بیت‌لاکر[1] در مایکروسافت ویندوز را فعال کنید.
- فایل ولت[2]، مک‌او اس را فعال کنید.
- دی‌ام‌کریپت[3] یا نرم‌افزار مشابهی در لینوکس را بارگیری کنید.
- اندرویدهای بالاتر از نسخه ۶ و آی‌او اس بالاتر نسخه ۸ این امکان را به صورت پیش‌فرض در خود فعال کرده‌اند.

به‌روز رسانی مداوم سیستم عامل

حتی اگر توسعه‌دهندگان سیستم‌های عامل از چندین نسخه اصلی آخر پشتیبانی می‌کنند، اما آسیب‌پذیری‌های امنیتی به طور مداوم در حال کشف شدن‌اند و می‌توانند بر همه یا یک نسخه خاص از سیستم عامل تاثیر بگذارند. سیستم عامل‌های قدیمی‌تر که دیگر مورد پشتیبانی سازندگان آن‌ها نیستند، بیشترین امکان را برای دسترسی‌های غیرمجاز به داده‌های‌تان فراهم می‌کنند. مهم است که اطمینان حاصل کنید که همواره از نسخه‌های قابل پشتیبانی سیستم عامل‌ها استفاده می‌کنید و تمامی وصله‌های امنیتی را بر روی آن نصب کرده‌اید.

چگونگی به‌روز رسانی مک‌او اس

- ویندوز؛ این چک‌لیست را مرتبا بررسی کنید.

[1] BitLocker
[2] FileVault
[3] dm-crypt

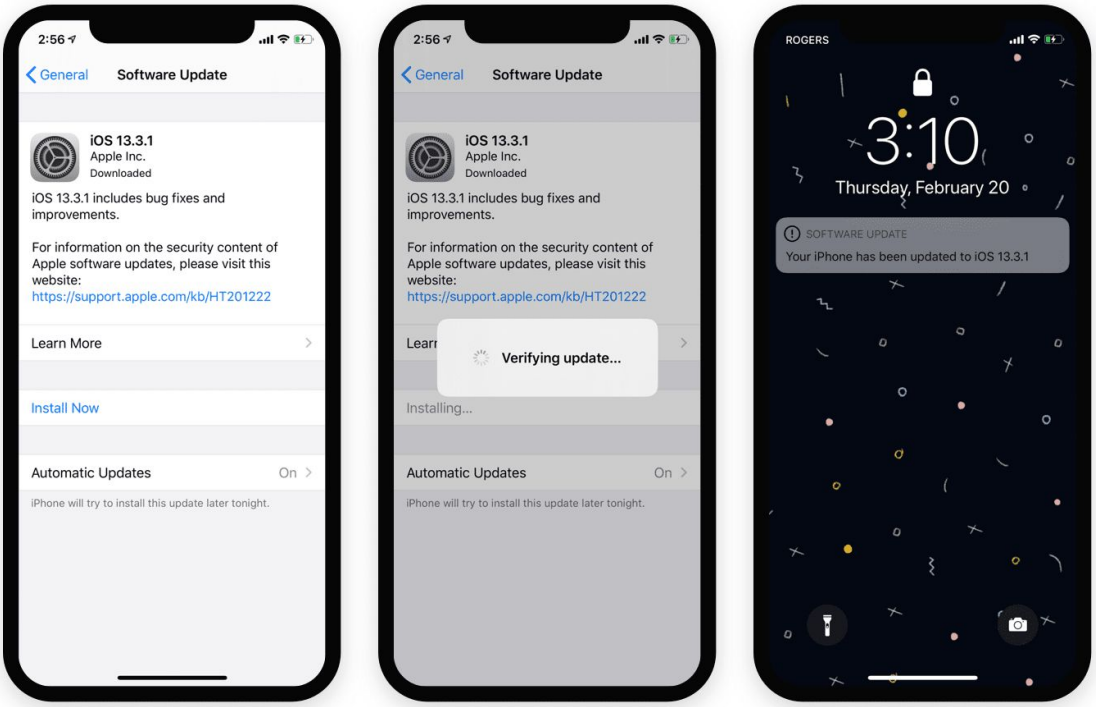
- مک‌او اس؛ اپل در مورد سیاست‌های خود برای به‌روز رسانی‌های مک‌او اس، شفاف نیست. اما به تجربه مشخص شده است که به‌روز رسانی‌های امنیتی برای جدیدترین نسخه و دو نسخه قبل هدف‌گیری شده‌اند.
- لینوکس؛ اکثر توزیع‌های فعال به خوبی پشتیبانی می‌شوند.
- اندروید؛ به‌روز رسانی‌های امنیتی ۲ نسخه اصلی و آخر هدف‌گیری شده‌اند.
- آی‌او اس؛ اپل در مورد سیاست‌های خود برای به‌روز رسانی‌های آی‌او اس نیز مانند مک‌او اس، شفاف نیست. اما به تجربه مشخص شده است که به‌روزرسانی‌های امنیتی برای جدیدترین نسخه اصلی و ۳ نسخه آخر هدف‌گیری شده‌اند.

میانگین زمان افشای آسیب‌پذیری‌های امنیتی تا وضوح آن بیش از ۲ ماه به‌طول می‌انجامد[4]. این یک موضوع بسیار مهم است و به نفع شماست که این روند را بیشتر به تاخیر نیاندازید. برای به‌دست آوردن هرچه سریع‌تر وصله‌های امنیتی، اطمینان داشته باشید که به‌روز رسانی خودکار دستگاه‌تان را روشن و آن‌ها را اعمال کرده‌اید. هرچند که به‌روز رسانی‌های خودکار به‌طور پیش‌فرض در اکثر دستگاه‌های جدید فعال است.

به‌روز رسانی مداوم نرم‌افزارها

لایه بعد از سیستم عامل، نرم‌افزارهایی است که توسط شما روی دستگاه‌های‌تان نصب شده است. از مرورگرهای اینترنتی گرفته تا خانواده مایکروسافت آفیس و... آنها نیز ممکن است آسیب‌پذیر باشند و به همان دلایلی که در بالا ذکر شد، لازم است که آن‌ها را نیز به صورت مداوم به‌روز رسانی کنید.
اکثر نرم‌افزارهای مدرن، به صورت خودکار به‌روز رسانی‌های امنیتی را اعمال می‌کنند یا در صورت غیرفعال بودن این قابلیت از شما می‌خواهند که این کار را انجام دهید.
حتما و حتما لازم است که به صورت دوره‌ای بررسی کنید که آخرین نسخه نرم‌افزارهای مورد استفاده‌تان روی دستگاه‌تان نصب باشد.

[4] Edgescan 2019 Vulnerability Statistic Report



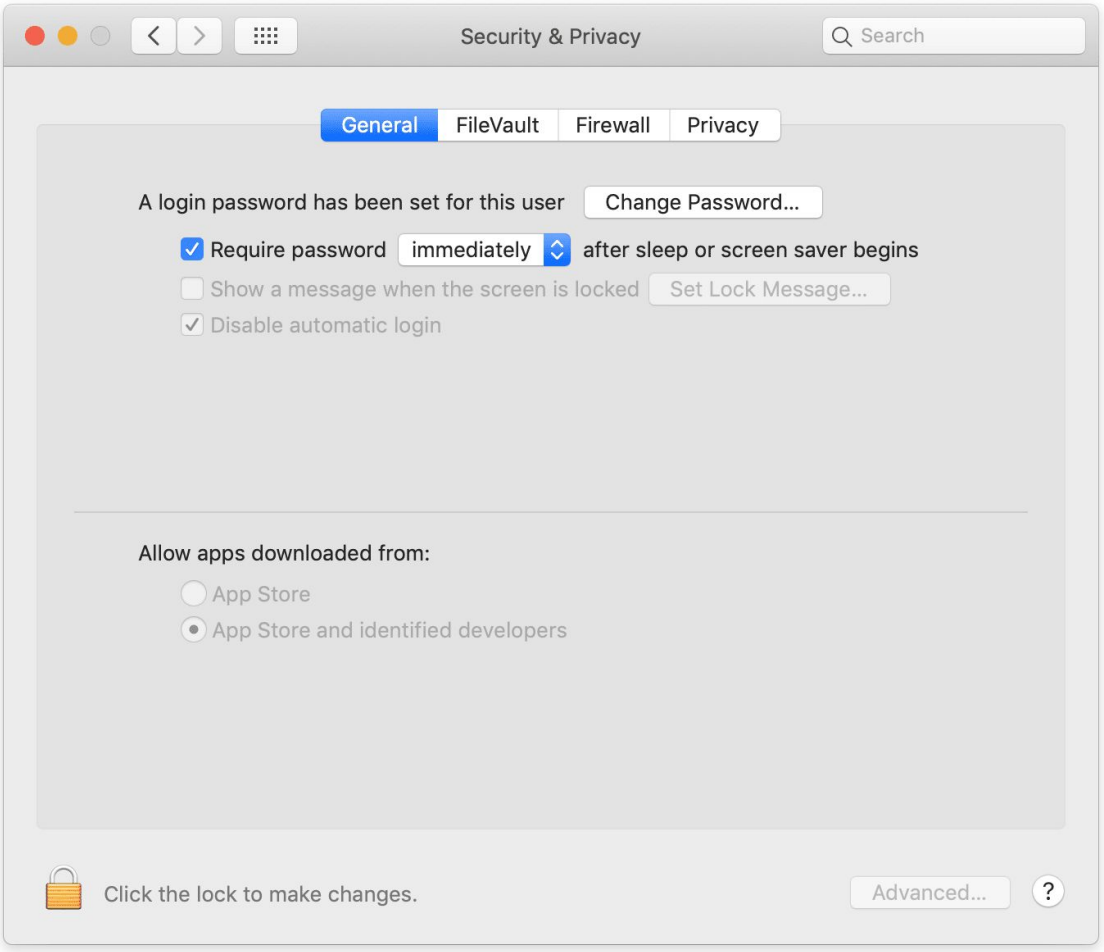
غیرفعال سازی ورود خودکار

دستگاه‌های بدون محافظت، اهداف آسانی برای چشم‌های کنجکاوند مگر اینکه اطمینان داشته باشید که فقط خودتان به آن دسترسی دارید. برای این کار، از فعال بودن قابلیت ورود خودکار اطمینان حاصل کنید. توجه کنید که به اشتراک گذاشتن رمز عبور یا پین‌کد خود با دیگران، شما را آسیب‌پذیر می‌کند.

ورود خودکار در اغلب دستگاه‌های به‌روز غیر فعال است.

فعال سازی قفل خودکار

اگر در فضای مشترک یا فضاهای عمومی مشغول به کار هستید و می‌خواهید که از دستگاه خود فاصله بگیرید، آن‌را قفل کنید. اما اشتباه یا فراموش کردن ممکن است اتفاق بیافتد. برای همین قفل اتوماتیک را برای محافظت از دستگاه‌های خود فعال کنید.



قفل خودکار و یک بازه زمانی رمز عبور را در دستگاه خود فعال کنید

اطمینان حاصل کنید که مقداری از زمان را برای این کار پیکربندی کنید که راحت باشید و مزاحمتی برای‌تان نداشته باشد. زمان ۳۰ ثانیه برای دستگاه‌های تلفن همراه و یا ۵ دقیقه برای لپ‌تاپ‌ها منطقی‌ست. قفل اتوماتیک هم به طور پیش‌فرض در اکثر دستگاه‌های به‌روز فعال است.

از رمز یا پین‌های قوی استفاده کنید

اگر پین، رمز عبور یا گذرواژه‌های دستگاه‌های شما به راحتی قابل حدس زدن باشند، تمام این احتیاط‌ها در معرض خطر است. هیچ‌گاه از هر چیزی که پیدا کردن آسان باشد، مانند تکرار یک شماره (مثل ۰۰۰۰)، دنباله اعداد (مثل ۱۲۳۴) و موارد مشابه دیگر استفاده نکنید.

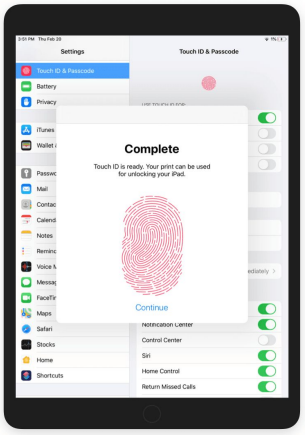
لیست رمزهای عبور متداول را چک کنید تا اطمینان پیدا کنید که از چیزی استفاده نمی‌کنید که با راحتی قابل حدس زدن باشد.

Top 25 most common passwords

1 123456	6 12345678	11 abc123	16 654321	21 888888
2 123456789	7 12345	12 qwerty123	17 555555	22 princess
3 qwerty	8 iloveyou	13 1q2w3e4r	18 lovely	23 dragon
4 password	9 111111	14 admin	19 7777777	24 password1
5 1234567	10 123123	15 qwertyuiop	20 welcome	25 123qwe

برخی رمزهای عبور متداول که نباید از آن‌ها استفاده کنید

از این مهمتر، از هیچ عبارتی که به نحوی با شما در ارتباط باشد مثل تاریخ تولد، پلاک ماشین، شماره شناسنامه و... استفاده نکنید. بهترین رویکرد برای انتخاب یک رمز عبور قوی، عبارتی تصادفی شامل اعداد، حروف بزرگ و کوچک و نشانه‌هاست که حداقل یازده کاراکتر طول داشته باشد.



احراز هویت‌های بیومتریک یکی از بهترین گزینه‌هاست

تایید هویت دو مرحله‌ای را فعال کنید

تایید هویت دو مرحله‌ای به معنای استفاده از دو عامل مختلف برای تایید هویت شما به منظور ورود به یک برنامه یا یک وب‌سایت است. حالت دوم معمولا می‌تواند شکل‌های زیادی داشته باشد اما به طور معمول یک کد یک بار مصرف است.

آگاهی از انتخاب‌های بی‌خطر برای عامل دوم هم از اهمیت بالایی برخوردار است. مثلا ارسال پیامک یک گزینه محبوب در میان کاربران است اما ثابت شده که به طور کامل امن نیست. بهترین روش استفاده از یک برنامه تایید کننده مانند `Google Authenticator` یا `Authy` است.

صرف نظر از امن بودن این روش‌ها، استفاده از تایید دو مرحله‌ای توانسته است به طور چشم‌گیری کلاهبرداری‌های دیجیتالی را برای سرقت اطلاعات کاهش دهد. مهاجمان و هکرها دیگر با دانستن رمز عبور شما نمی‌توانند به اطلاعات‌تان دسترسی داشته باشند. ضمن اینکه این کدها یک‌بار مصرف بوده و هر چند ثانیه منقضی و غیرقابل استفاده می‌شوند.

احراز هویت دو مرحله‌ای اپل

فعال کردن تایید هویت دو عاملی، برای همه مواردی که دارای داده‌های حساس مانند رمز عبور، ایمیل، اینترنت بانک، میزبان‌های داده‌ای مثل گوگل‌درایو یا دراپ‌باکس و... امری ضروری‌ست. هرچند که بهتر است آن را برای همه‌جا فعال کنید.

در شبکه‌های عمومی یا غیر قابل اعتماد از VPNهای امن استفاده کنید

یک `VPN` می‌تواند اتصال ایمن و رمزگذاری شده‌ای را با شبکه اینترنت برقرار کرده و ترافیک شما را از داخل آن عبور دهد. انجام این کار در شبکه‌های غیر قابل اعتماد به طور قابل ملاحظه‌ای می‌تواند به حفظ حریم خصوصی و فعالیت ناشناس شما در اینترنت کمک کند.

هرچند که استفاده از `VPN` در بسیاری از کشورها غیر قانونی‌ست اما شرایط دورکاری این روزها، ایجاب می‌کند تا برای حفظ امنیت داده‌های کسب‌و کاری که برای آن کار می‌کنید، حتما از این ابزار استفاده کنید و از آن طریق به شبکه محلی و ابزارهای محل کارتان متصل شوید.

اگرچه لیست موارد امنیتی به این موارد منتهی نشده و امنیت داده‌های شما را به طور کامل تضمین نمی‌کند اما رعایت موارد بالا و برخی دیگر از مواردی که در لیست زیر آورده شده است، می‌تواند تا حد خوبی به حفظ حریم خصوصی و داده‌های شما کمک کند. این موارد عبارتند از؛

- استفاده از نرم‌افزارهای مدیریت گذرواژه‌ها
- فعال کردن امکان پیدا کردن و پاک کردن اطلاعات دستگاه از راه دور
- از بین بردن داده‌های دستگاه در صورت مفقودی
- باز نکردن فایل‌های ضمایم ایمیل در صورت ناشناس بودن ارسال کننده
- عدم نصب نرم‌افزار از فروشگاه‌های غیر معتبر
- عدم نصب افزونه‌های مرورگر بدون اطمینان از امن بودن آن
- کلیک نکردن بر روی هشدارهای امنیتی که در مرورگر و در قالب یک صفحه اینترنتی به شما نمایش داده می‌شوند

مهم نیست که ما جف بزوس باشیم یا جان دویی، مهم داده‌های شخصی و سازمانی‌مان است. همه‌مان وظیفه داریم که از دستگاه‌ها و اطلاعات خود به نحو شایسته‌ای محافظت کنیم. خوشبختانه حفظ ایمنی آنلاین چندان هم پیچیده نیست. چند عامل یک طرفه و تعداد انگشت‌شماری از قواعد ساده می‌تواند تا حدود بسیار زیادی ارتباطات ما را ایمن کند. بولت‌های بالا و تمام موارد دیگری که در این بخش گفته شد، به منظور حفاظت از داده‌های شما بوده است.

لیستی از ابزارهای کاربردی

Best Visual Collaboration Tools for Remote Work

- Milanote
- Wurkr
- Metro Retro
- Tweakr.io
- Conceptboard
- Oroson
- ReviewStudio
- TeamSuccess
- Mural
- Kantree
- UIReview
- Visual Collaboration
- CoScreen
- A Web Whiteboard

Best Virtual Desktop Software for Remote Work

- V2 Cloud
- OpenSource...
- Windows Virtual...
- Paperspace
- Amazon WorkSpaces
- Workspot
- Virtual Desktop

Best Video Conferencing Apps for Remote Work

- Remo.co
- Zoom
- urLive
- Kallu Conference...
- Wisp | Remote...
- Livestorm
- Lito
- Outklip
- Unmeeting
- Collabify
- Tandem
- Roundee
- Jackfruit
- Appear.in
- EmuCast
- Pragli
- Clapboard
- Skype
- Meet
- Hibox
- Remotehour
- GoToMeeting
- Adobe Connect
- MeetMenu
- Pukka Team
- Team.Video
- Proficonf
- Video Window
- Join.me
- HelloCecil
- UnRemot
- easyUp
- Spike Secure...
- Teleport.fm
- Meeting Owl Pro
- 8x8 Video Meetings

Best Time Tracking Apps for Remote Work

- Apploye
- Hubstaff
- Toggl
- DueFocus
- Day Lineup
- Worklog
- Code Time
- Time Doctor
- AttendanceBot

- Friday
- ProjChat
- Carrot
- Scyre
- ScrumGenius
- Toasty.ai
- Fleep
- YAC (Legacy)
- RumbleTalk
- Brosix
- ChatFox
- Bunch.ai
- Webwide
- Workplace
- Internal
- Slack Scheduler
- Unit.chat
- Scenery
- Crisp
- LocalBrackets
- Flock
- OI Chat
- Humble Dot
- Flujoapp

Best Support Ticketing Tools for Remote Work

- Zendesk
- Groove
- Freshdesk
- Room.sh

Best Remote Standup Meeting Tools for Distributed Teams

- DailyBot
- Geekbot
- Olaph
- WhatGotDone
- Status Hero
- Standups
- Timely PWA
- Portlr
- WorkHours
- TopTracker
- Pomobaro
- TimeCamp
- TimeTurtle
- ActivityWatch
- Harvest
- My Hours
- TouchTime
- Timemator 2
- HourStack
- Workpuls
- Monitask
- Atto
- Staff timer app
- Focus To-Do
- TimeStack
- WakaTime
- TimeKeeper
- Deepwork.today
- Worked today
- Quidlo Timesheets
- Clockwise for Slack
- Timewise
- Timehacker
- Timist
- Spacetime
- Timing
- WorkingHours
- Peak Planner
- Willed Calendar

Best Team Chat Apps for Remote Work

- Slack
- Twist
- Karma
- Unison

- Avocode
- Design Cuts
- Axure

Best Tools for Digital Nomads

- RemoteYear
- Eddy Travels
- NomadWallet
- Nomad Rest
- Nomad List
- TownChat
- Visa List
- nomadhubb
- Person8
- Trip Noodle
- Travellar
- Nomad Radar
- Nomadpick
- Culture Trip
- Seat Surfing
- TripCost
- Krowspot

Best Document Collaboration Tools for Remote Work

- Slite
- Additor
- Yousign
- ntile
- Google Docs
- Slab
- JobAider
- lokki.cloud
- Helpjuice
- uman.ai
- Ripley
- Goals
- Tettra
- Emvi
- I Done This
- Tatsu
- Jell

Best Bug Tracking Tools for Remote Work

- Toybox
- Github Issues
- JIRA Software
- Deep Work Stats
- DoneDone
- Assist
- Zoho Bug Tracker
- ReQtest
- Sifter

Best Code Collaboration Tools for Remote Work

- CloudRepo
- CodePen
- Live Share for VS
- JSFiddle
- CodeTogether
- GitDuck
- TeleType for Atom
- TeamHub

Best Code Version Control Tools for Remote Work

- Github
- Gitlab
- Bitbucket

Best Design Collaboration Tools for Remote Work

- Figma
- InVision
- Vectorly
- Zeplin
- Marvel

- Brightest
- 15Five
- ThirstySprout
- Culture Amp
- Stories
- Kolay
- Dawfin
- Sketch for teams
- Lattice Pulse
- WaterCooler

Best File Hosting Websites for Remote Work

- Dropbox
- Google Drive
- BlackHole
- OneDrive
- BlockDoc
- Box

Best Hiring Talent Solutions for Remote Teams

- Remote.io
- Work From Home Jobs
- Remote Woman
- 6nomads
- Upwork
- Flexiple
- CloudPeeps
- Hubstaff Talent
- RemoteMore
- Remote Planet
- Minty
- HelloRemote
- Deel
- FlatWorld.co
- Naprok
- InterviewPass
- TECLA
- NerdFeedr
- Coda.io
- Arcane Docs
- Elium
- Arcane Sheets
- Dropbox Paper
- Confluence
- Sheet.chat
- PaymentX
- Archbee
- DottedSign
- ONLYOFFICE
- GitBook
- Craft
- Quip
- TaskQue
- Elephant Drive

Best Employee Management Software Solutions for Remote Work

- CoachBot
- Hilo
- HiStaff
- Plai
- QuizBreaker
- Peoplebox
- Achieved
- Teamworki
- Leapsome
- Eureka
- Elin.ai
- bttr
- Tydy Onboard
- Intro30
- Glint
- Spyrix Employee...
- Calamari
- Slido
- Sora
- Trakstar

Best Document Scanner Apps for Remote Work

- Receipt Lens
- CamScanner
- Prizmo
- Scannable
- Scanbot

Best Appointment Scheduling Apps and Booking Software for Remote Work

- SuperSaaS...
- Chili Piper
- Calendly
- TeamTimes for Mac
- Elephant
- Inviited
- Campstarter
- Timy
- Doodle
- Accelo
- Waqt
- Vyte
- Instagantt
- Zynq Scheduler
- Smoopit
- MeetFox
- Arrangr
- Doodle Bot for Slack
- Rendez
- Woven
- Catchup Calendar
- neatCal

Best Tools for Remote Product Management

- Conduit
- productboard
- Aha!
- ProdPad
- Willo
- andRemote
- Dynamite Jobs
- You Team
- Zimo
- Skip the Drive
- Toptal

Best Idea Management Tools for Remote Work

- Retrium
- TeamRetro
- FunRetro
- Ideanote
- Idea Drop
- Upvoty
- Neatro
- Sprint Boards
- Ideascale
- The Worklist Digest
- Spigit
- Sideways6

Best Interactive Whiteboard Tools for Remote Work

- RealtimeBoard
- GroupMap
- Explain Everything
- SketchBoard

Best Mail Communication Tools for Remote Work

- Loop Email
- Gmail (Business)
- North App
- Outlook
- Mattermost
- Yahoo (Business)

- Invoice Quickly
- Asana
- OfficeAmp
- Zenkit
- Azendoo
- Inyo
- Teamwork
- Binfire
- HeySpace
- Runrun.it
- Zepel
- Basecamp
- Hubstaff Tasks
- Outro
- Winio.io
- Kissflow
- Jira
- Slenke
- Pivotal Tracker
- Cage
- Wethos
- Birdseye
- Smartsheet
- Zenhub
- Podio
- Redbooth
- Subtask
- Teamweek
- Claritask
- Confeur
- ProProfs Project
- GitScrum
- Github Projects
- Chopstix
- Active Collab
- GanttPRO
- Chief
- Produck
- Estimator for Jira
- Macaw
- ProductPlan

Best Note Taking Apps for Remote Work

- Fireflies.ai
- Notion
- Notejoy
- Zoho Notebook
- Tactiq
- Evernote
- OneNote
- Google Keep
- Stashany
- Jottit
- Simplenote
- Allegory
- Amplenote
- ListPal
- TheNote.app
- FastEver 3
- pNotes
- Filterize
- QuickJots
- Taky

Best Remote Project Management Tools for Distributed Teams

- Paymo
- Nifty
- Lumeer
- Vabotu
- ProofHub
- Trello
- Beat
- Avion
- Resolvd
- ClickUp
- Montera
- 10,000ft

- Reetro
- Status Page
- WP Project Manager
- Hassl Business
- Harve