

« به نام خالق آرامش »

نام کتاب: امنیت در windows ۱۰

نام نویسنده: shabakeh-mag.com

تعداد صفحات: ۵۰ صفحه

تاریخ انتشار: _____



کافئین بوکلی

CaffeineBookly.com



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly



امنیت در Windows 10

پنجره‌های سیستم خود را امن بسازید!



www.shabakeh-mag.com



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

بهترین ضدویروس برای ویندوز ۱۰ چیست؟ | ۳

ده ویژگی برتر و پنهان ویندوز ۱۰ | ۱۲

آموزش راهکاری برای فرار از جاسوسی مایکروسافت در ویندوز ۱۰ | ۳۴

چگونه یک صفحه قفل لاگین ویندوز ۱۰ ایجاد کنیم؟ | ۴۳



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

آیا Windows Defender کافی است؟

بهترین ضدویروس برای ویندوز ۱۰ چیست؟



ویندوز ۱۰ مثل ویندوز ۷ شما را برای نصب یک ضدویروس به دردمر نمی‌اندازد. از ویندوز ۸ به بعد، ویندوز یک ضدویروس داخلی با نام Windows Defender درون خود دارد. اما آیا این بهترین راهکار برای حفاظت از کامپیوتر است؟ به اندازه کافی خوب عمل می‌کند؟ Windows Defender آخرین نسخه - Microsoft Security Essentials، یک برنامه ضدویروس از شرکت مایکروسافت است که برای ویندوز ۷ عرضه شد. حالا این برنامه درون ویندوز جاسازی شده و سطح پایه حفاظت ضد ویروسی را برای کامپیوترهای ویندوز ۱۰ حاصل می‌کند.



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

آیا Windows Defender کافی است؟

این ضدویروس به صورت پیش فرض روی ویندوز اجرا می شود. Windows Defender به صورت خودکار برنامه هایی که باز می کنید را اسکن کرده و آخرین به روزرسانی ها برای شناسایی ویروس های جدید را از Windows Update دانلود می کند و رابط کاربری ای در اختیار شما می گذارد که می تواند پیچیده ترین اسکن ها را انجام دهید.

اما این ضدویروس چقدر خوب عمل می کند؟ خب، اگر بخواهیم راستش را بگوییم، ضدویروس مایکروسافت وقتی پای تست های نرم افزاری قیاسی به میان می آید، از ضدویروس های دیگر کمی عقب تر است. پیش تر هم هشدارهایی در این زمینه داده شده بود و نگرانی ما بیشتر به این خاطر بود که قبلا از محصول ضدویروس مایکروسافت خیلی تعریف کرده بودیم.

Windows Defender مزایای بسیاری دارد. درون خود ویندوز جاساز شده است، شما را با پیام های پیاپی آزار نمی دهد و درخواست پول نمی کند و از رقبای خود سبک تر است. این ضدویروس داده های وب گردی شما را جمع آوری نمی کند و از آنها پول در نمی آورد. چنان که بعضی برنامه های ضدویروس رایگان شروع به این کار کرده اند تا از این راه سودی بدست آورند.



@caffeinebookly



caffeinebookly



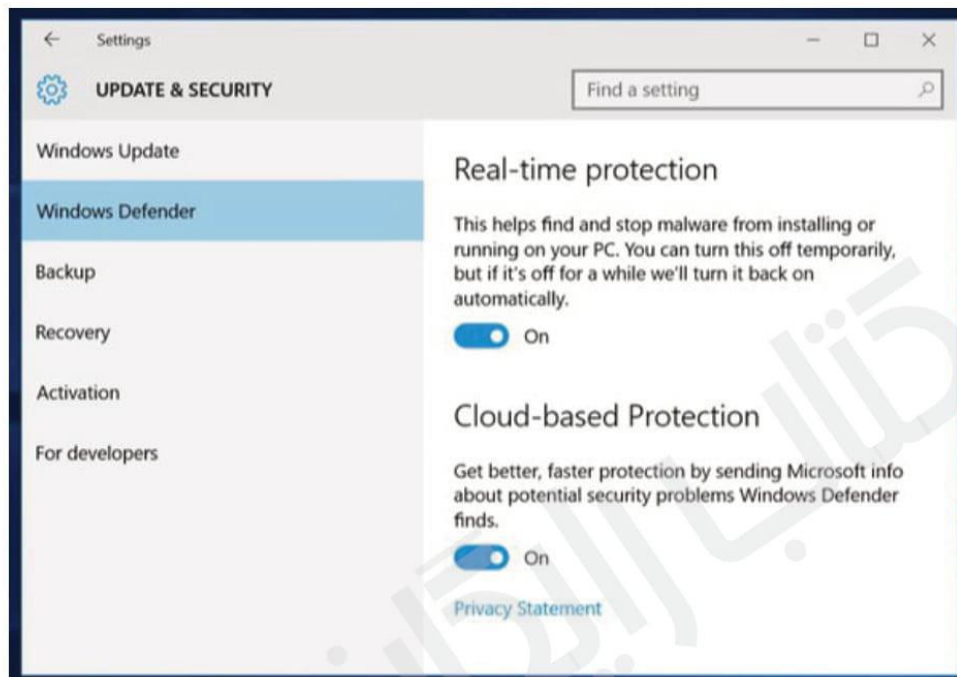
@caffeinebookly



caffeinebookly



t.me/caffeinebookly



به طور کلی Windows Defender حفاظت بدی را در اختیار شما نمی‌گذارد. البته با فرض این که ویندوزتان را به‌روز نگه دارید (که حالا به صورت خودکار انجام می‌شود) و از یک مرورگر به‌روز استفاده کنید، از افزونه‌های بالقوه خطرناک مثل جاوا دوری کنید. Windows Defender و ترکیب آن با کارهای پیش‌گیرانه‌ای که باید برای امنیت کامپیوتر انجام دهید، یک حفاظت خوب را برای‌تان به ارمغان می‌آورد.

علی‌رغم امتیازات پایینی که Windows Defender از AV-Test گرفته



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

است (فقط ۰.۵٪ از ۶ در زمینه حفاظت)، اما Windows Defender. حدود ۹۵ درصد از بدافزارهای شایع و متداول در ماه ژوئن ۲۰۱۵ و همچنین ۸۵ درصد از حملات روز صفر (zero-day) را شناسایی کرده است. BitDefender از پس صد درصد و صد در صد نمونه‌های آزمایشی بر آمد و Kaspersky هم صد درصد و ۹۵ درصد را شناسایی کرد. بنابراین علی‌رغم این اختلاف زیاد در امتیازات، Windows Defender باز هم کارش را خوب انجام می‌دهد. در گذشته مایکروسافت مدعی شده بود که تمرکزش روی بدافزارهایی است که در دنیای واقعی شایع هستند و در این آزمایش‌ها گنجانده نشده‌اند و دیگر فروشندگان ضد ویروس محصولاتشان را طوری سامان‌دهی کرده‌اند که در این آزمایش‌ها خوب عمل کنند. در هر حال مایکروسافت دیگر در مورد نتایج آزمایش‌ها اظهار نظری نمی‌کند.

ویندوز ۱۰ هم شامل همان حفاظت‌های جانبی مختلفی است که در ویندوز ۸ معرفی شده بود. مثلاً فیلتر SmartScreen که راه شما را برای دانلود و اجرای بدافزار سد می‌کند. کروم و فایرفاکس هم Safe Browsing (وب‌گردی امن) شرکت گوگل را در خود دارند که دانلود بسیاری از بدافزارها را مسدود می‌کند.

Windows Defender در کنار یک عقل سلیم و دیگر کارهای



@caffeinebookly



caffeinebookly



@caffeinebookly

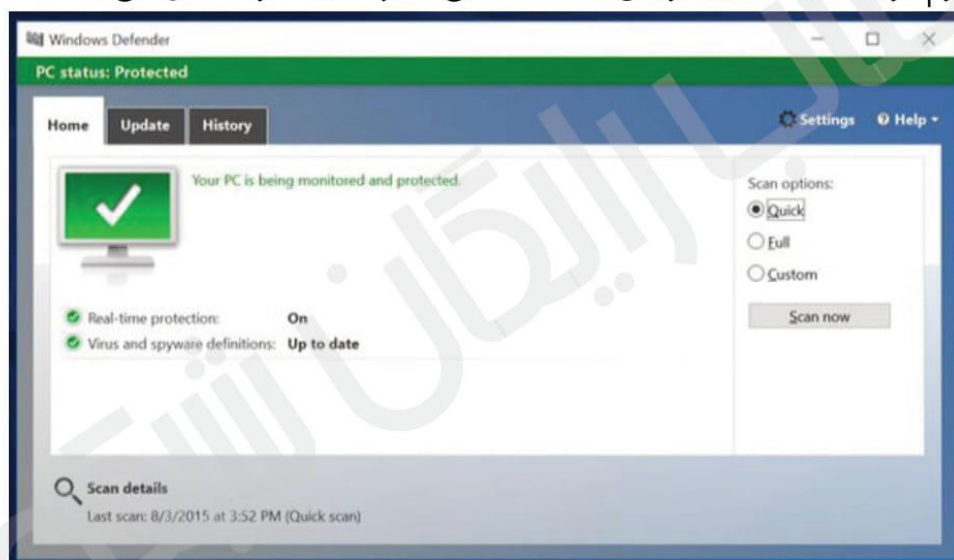


caffeinebookly



t.me/caffeinebookly

پیش‌گیرانه امنیتی، احتمالاً برای اکثر کامپیوترهای شخصی کفایت می‌کند. البته اگر مدام در حال دانلود اپلیکیشن‌های غیرقانونی هستید و فعالیت‌هایی با ریسک بالا دارید، شاید بهتر باشد بی‌خیال Windows Defender شوید و ضدویروسی را به خدمت بگیرید که در برابر مجموعه‌ای از بدافزارهای نمونه که در آزمایش‌های نرم‌افزارهای ضدویروس استفاده می‌شوند، بهتر عمل می‌کند.



از نرم‌افزار ضد سو استفاده **MalwareBytes** هم استفاده کنید ما همچنین پیشنهاد می‌کنیم که از یک برنامه ضد سو استفاده برای حفاظت از مرورگر وب و افزونه‌ها استفاده کنید؛ چرا که این‌ها بیشتر هدف مهاجمین قرار می‌گیرند. نرم‌افزار ضد سو استفاده **MalwareBytes** برنامه پیشنهادی ماست. عملکرد آن مشابه



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

ابزار امنیتی EMET خود مایکروسافت است. اما رابط کاربری کاربرپسندتری دارد و قابلیت‌های امنیتی بیشتری ارائه می‌کند. این برنامه کمک می‌کند تا تکنیک‌های سو استفاده‌گری معمول را سد کنید، حتی اگر حملات روز صفری باشند که تا حالا مشاهده نشده‌اند. نرم‌افزار ضد سو استفاده MalwareBytes. برای مثال تمام آن حملات روز صفر فلشی که اخیراً در مورد آن‌ها شنیده‌اید را سد می‌کند. این نرم‌افزار، مرورگر، افزونه‌ها و دیگر اهدافی که محاجمان مورد هدف قرار می‌دهند را مستحکم می‌کند و از شما در مقابل تکنیک‌های شایع حملات حفاظت می‌کند.

Windows Defender در کنار نرم‌افزار ضد سو استفاده MalwareBytes یک ترکیب خوب، رایگان و بدون دردسر از برنامه‌های امنیتی است که ما آن را برای امن نگه داشتن کامپیوترهای عادی ویندوز ۱۰ توصیه می‌کنیم. کامپیوترهای شخصی با ویندوز ۱۰ Enterprise اغلب Windows Defender و Microsoft EMET را به طور همزمان اجرا می‌کنند اما Windows Defender و MalwareBytes برای یک کامپیوتر معمولی خانگی ترکیب بهتری است.

(خود MalwareBytes یک برنامه قوی ضد بدافزار است که به عنوان مکمل هر برنامه ضد ویروسی، از جمله Windows Defender، به خوبی عمل می‌کند. این نرم‌افزار قابلیت پیدا کردن برنامه‌های بالقوه



@caffeinebookly



caffeinebookly



@caffeinebookly

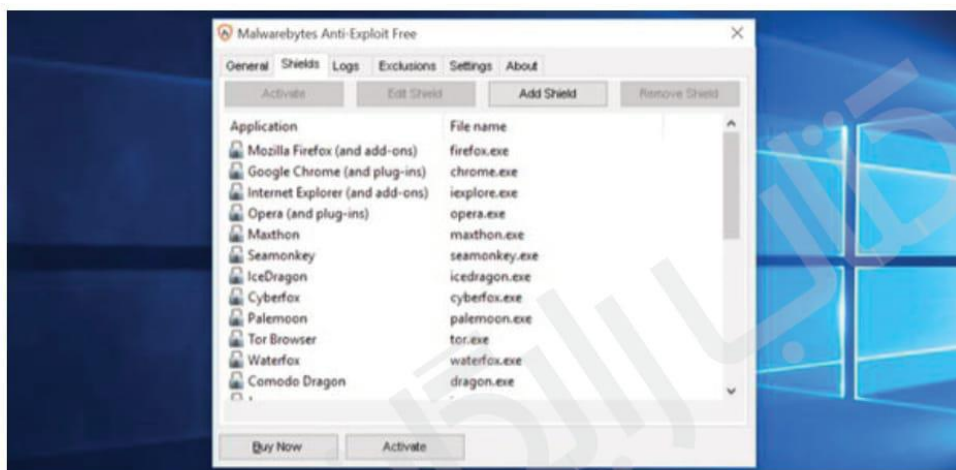


caffeinebookly



t.me/caffeinebookly

ناخواسته و دیگر junkware هایی را دارد که یک ضدویرس معمولی نمی‌تواند پیدا کند، اما نرم‌افزار ضد سو استفاده MalwareBytes یک برنامه جداگانه است.)



اما بهترین ضدویرس کدام است؟

بسیار خوب، شاید شما با Windows Defender خشنود نیستید و می‌خواهید ضدویرس دیگری را بجای آن انتخاب کنید. اگر به دنبال یک محصول ضدویرس پولی هستید، Kaspersky و BitDefender دائما در رتبه‌های بالای آزمایش‌های ضدویرس‌های مختلف قرار دارند. شاید بخواهید خودتان کمی بیشتر تحقیق کنید و آخرین نسخه‌های آزمایش‌ها را خودتان امتحان کنید و ببینید کدام برنامه‌های ضدویرس بهترین عملکرد را دارند. اما اگر حاضرید دست داخل جیب‌تان کنید، Kaspersky و BitDefender هر دو گزینه‌های قوی و قابل احترامی هستند.



@caffeinebookly



caffeinebookly



@caffeinebookly



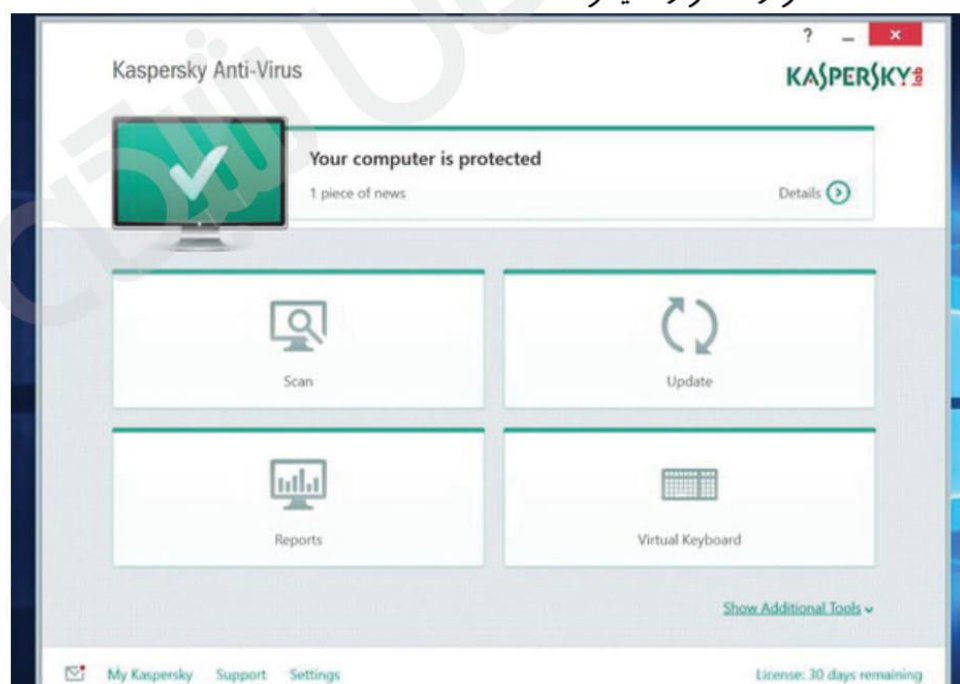
caffeinebookly



t.me/caffeinebookly

اگر به دنبال یک راهکار رایگان هستید، Windows Defender انصافاً خوب کار می‌کند. اما اگر چیز دیگری می‌خواهید، حتماً از نصب هر نوار ابزار و افزونه مرورگری که ضدویروس می‌خواهد نصب کند اجتناب کنید. شرکت‌های ارائه‌کننده ضدویروس‌های رایگان برای درآوردن مخارجشان به این نرم‌افزارهای جانبی و جمع‌آوری داده روی آورده‌اند.

وقتی یک ضدویروس ثالث نصب می‌کنید، Windows Defender به طور خودکار خود را غیرفعال می‌کند و اگر آن ضدویروس ثالث را حذف کنید مجدداً خود را فعال می‌کند. این برنامه طوری طراحی شده که سر راه قرار نگیرد.



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

هر ضدویروسی که انتخاب کنید از کامپیوتر شما به طور کامل محافظت نمی‌کند. اگر برنامه‌های مضر را دانلود و نصب می‌کنید، دیر یا زود به دردسر خواهید افتاد. انتخاب یک ضدویروس که امتیازات بهتری در برابر بدافزارهایی که شاید هرگز با آنها روبرو نشوید کسب کرده است، شاید به امن‌تر بودن شما کمک کند، اما انجام پیش‌گیری‌های امنیتی مهم‌تر هستند.

و در آخر، در نظر داشته باشید که این روزها ترسناک‌ترین حملات، حملات روز صفر هستند که از حفره‌های افزونه‌های مرورگرها و خود افزونه‌ها برای دست‌کاری سیستم شما استفاده می‌کنند. نرم‌افزار ضد سو استفاده MalwareBytes احتمالاً به نسبت ضدویروس‌های جایگزین، امنیت بهتری در برابر خطرناک این حملات ارائه می‌کند.



@caffeinebookly



caffeinebookly



@caffeinebookly



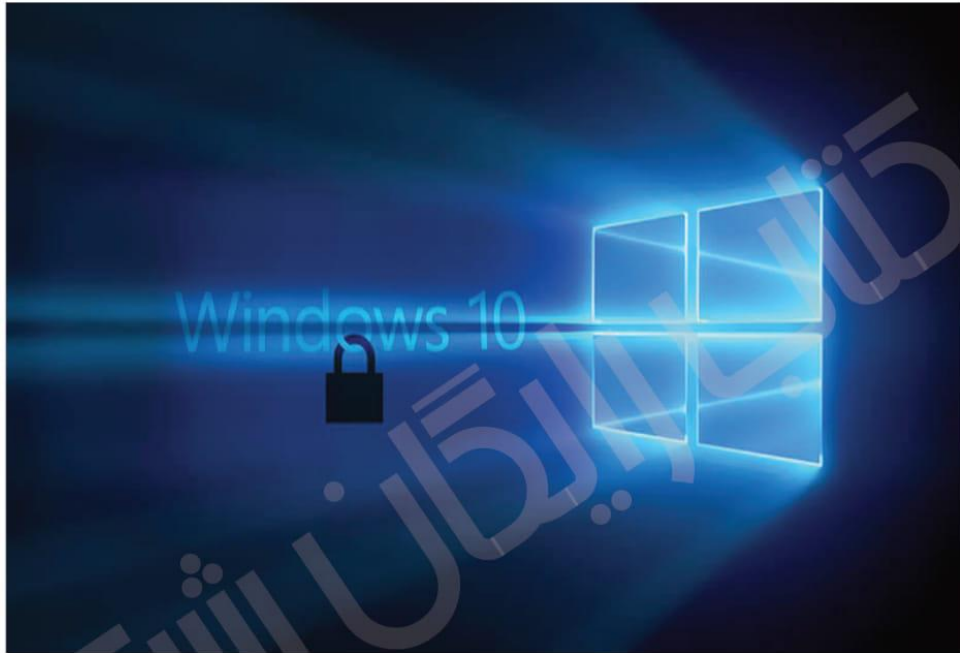
caffeinebookly



t.me/caffeinebookly

اسرار ویندوز ۱۰

ده ویژگی برتر و پنهان ویندوز ۱۰



هر زمان سیستم عامل جدیدی از خانواده ویندوز عرضه می شود، از خود می پرسیم آیا ویندوزم از من در برابر حملات محافظت می کند یا همچون گذشته من باید از ویندوزم در برابر مخاطرات امنیتی محافظت کنم. به نظر می رسد ویندوز ۱۰ این بار با تمام توان پا به میدان گذاشته است. جو بلفیوری در وبلاگ ویندوز نوشته است: «گروه طراحی ویندوز ۱۰ تمام توان خود را در طراحی یک سیستم عامل امن به کار بسته اند.»



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

مقایسه ویژگی‌های امنیتی ویندوز ۷ و ۱۰

ویندوز ۷ موفق‌ترین و در دسترس‌ترین سیستم‌عامل تاریخ مایکروسافت بود و در پنج سال گذشته خدمات زیادی به ما ارائه داد. اما واقعیت دیگری درباره ویندوز ۷ وجود دارد. ویندوز ۷ نتوانست سطحی از حفاظت در برابر تهدیدات امنیتی جدید ارائه کند که با آن‌ها روبه‌رو بودیم. تاریخ به ما نشان داد، هرچند امکان اضافه کردن لایه‌های دفاعی با استفاده از محصولات ثالث در اختیار ما قرار دارد، اما هیچ‌کدام از محصولاتی که از طرف سازمان‌های امنیتی بزرگ که هر روزه درباره آن‌ها مطالبی می‌خوانیم و محصولات امنیتی در اختیار ما قرار می‌دهند، کافی نبودند. به همین دلیل چالش‌های جدید نیازمند یک پلتفرم جدید هستند.

Windows Hello

از زمانی که چرخه ساخت ویندوز ۱۰ آغاز شد، گروه طراحی ویندوز زمان و انرژی زیادی صرف پیاده‌سازی محاسبات شخصی سازی شده کرد، به گونه‌ای که دستگاه‌های مجهز به ویندوز ۱۰ توانایی تشخیص کاربر و درک آن‌چه کاربر به آن‌ها می‌گوید را داشته



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

باشند. نتیجه فعالیت‌های انجام گرفته در این زمینه به وجود آمدن ویژگی محاسبات شخصی در ویندوز ۱۰ است. روزگاری مایکروسافت وعده داده بود، شما به وارد کردن گذرواژه در کامپیوترهای شخصی مجهز به ویندوز ۱۰ نیازی نخواهید داشت. آن وعده سرانجام با Windows Hello رنگ واقعیت به خود دید. Windows Hello یک مکانیسم احراز هویت بیومتریک است که امکان دسترسی سریع به دستگاه‌های مجهز به ویندوز ۱۰ را امکان‌پذیر می‌سازد. با استفاده از ویژگی Windows Hello کاربر توانایی نشان دادن چهره یا اثر انگشت خود را به دستگاه‌های جدیدی که ویندوز ۱۰ روی آن‌ها اجرا می‌شود خواهد داشت، به طوری که این دستگاه‌ها در یک بازه زمانی کوتاه توانایی شناسایی او را دارند. نه تنها به کارگیری Windows Hello راحت‌تر از تایپ گذرواژه است، بلکه امن‌تر هم به نظر می‌رسد. این ویژگی باعث می‌شود تا احراز هویت کاربر در برنامه‌های کاربردی، محتوای سازمانی و حتی محتوای آنلاین بدون نیاز به استفاده از گذرواژه‌ای انجام شود که در دستگاهش یا در سرور شبکه ذخیره شده باشد.

این ویژگی چگونه کار می‌کند؟

Windows Hello سیستمی را معرفی می‌کند که از احراز هویت بیومتریک پشتیبانی می‌کند. این سیستم از چهره، عنبیه یا اثر انگشت برای باز کردن دستگاه‌ها استفاده می‌کند که به مراتب



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

امن‌تر از گذرواژه‌های سنتی است. رمز موفقیت Windows Hello در ترکیب دو عامل کاربر و دستگاهی که از آن استفاده می‌کند قرار دارد. ترکیب این دو عامل باعث می‌شود، به‌جای آن‌که از یک دسته از حروف و اعداد تصادفی که به‌راحتی فراموش شده، هک شده یا باید در مکانی نوشته شوند، از حس‌گرهای پیش‌رفته استفاده شود که توانایی تشخیص ویژگی‌های منحصر به‌فرد کاربر را دارند. این حس‌گرهای پیش‌رفته به کاربر اجازه می‌دهند به دستگاهی که از ویندوز ۱۰ پشتیبانی می‌کند، وارد شوند.

چه دستگاه‌هایی از این ویژگی پشتیبانی می‌کنند؟

در حال حاضر، طیف گسترده‌ای از دستگاه‌های مجهز به ویندوز ۱۰ که از این ویژگی پشتیبانی می‌کنند در حال ساخته شدن هستند. اگر دستگاه شما به یک حس‌گر اثر انگشت مجهز باشد، شما می‌توانید برای باز کردن دستگاه خود از Windows Hello استفاده کنید. برای تشخیص چهره یا عنبیه، Windows Hello از ترکیب سخت‌افزار و نرم‌افزار ویژه‌ای که از دقت بالایی برخوردار است استفاده می‌کند. به طوری که اگر یک عکس از خودتان را به آن نشان دهید یا اگر شخصی سعی کند تصویر خود را به‌جای شما به دستگاه نشان دهد، Windows Hello به‌راحتی این موضوع را متوجه خواهد شد (شکل ۱).



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly



شکل ۱: کپی برابر اصل نیست!

دوربین‌هایی که از فناوری مادون قرمز برای شناسایی چهره یا عنیبه استفاده می‌کنند، می‌توانند شما را در یک وضعیت نوردھی مناسب شناسایی کنند. Windows Hello یک درجه امنیت سازمانی که مطابق با نیازهای یک سازمان است را با پیاده‌سازی دقیق‌ترین نیازها و مقررات ارائه می‌کند. امنیت به کار رفته در این فناوری باعث می‌شود تا دولت‌ها و سازمان‌های مالی، بهداشتی و دفاعی به منظور افزایش امنیت کلی خود به‌سادگی از آن استفاده کنند. کارکرد برنامه‌های احراز هویت، محتوای سازمانی و تجربیات آنلاین همگی بدون نیاز به گذرواژه‌ها امروزه گذرواژه‌ها اصلی‌ترین روشی هستند که ما برای محافظت از داده‌ها و اطلاعات شخصی از آن‌ها استفاده می‌کنیم. اما گذرواژه‌ها دردسرساز و ناامن هستند. آن‌ها به آسانی هک می‌شوند و حتی زمانی که پیچیده می‌شوند نیز مؤثر نخواهند بود. بیش‌تر ما به گذرواژه ساده‌ای نیاز داریم که



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

به سادگی بتوانیم آن را به خاطر آوریم؛ بنابراین، از گذرواژه‌های ساده استفاده می‌کنیم که همین موضوع باعث می‌شود امنیت گذرواژه‌ها به حداقل برسد. همچنین، اگر نیاز به سطح بالایی از امنیت وجود داشته باشد، لازم است از ده‌ها گذرواژه برای ورود به دستگاه‌ها و سرویس‌ها استفاده کنیم. تا به امروز نزدیک به ۱,۲ میلیارد نام کاربری و گذرواژه در سایت‌های مختلف هک شده است. Passport (گذرنامه) نام ویژه‌ای برای سیستم‌های برنامه‌نویسی است که مدیران آی‌تی، طراحان نرم‌افزار و نویسندگان سایت‌ها از آن به‌عنوان روش امنیتی استفاده می‌کنند که به کاربر اجازه ورود به سایت‌ها یا برنامه‌هایشان را می‌دهد. به‌جای آن‌که از یک راز به اشتراک گذاری شده یا به اشتراک گذاشته شده شبیه به یک گذرواژه استفاده کنید، ویندوز ۱۰ به شما کمک می‌کند به‌صورت امن هویت خود را به برنامه‌ها، سایت‌ها و شبکه‌ها بدون آن‌که نیازی به ارسال گذرواژه‌ها وجود داشته باشد، نشان دهید. به این شکل، هیچ گذرواژه به‌اشتراک گذاشته شده‌ای که روی سرورها ذخیره شده و خطر بالقوه‌ای از جانب هکرها آن‌ها را تهدید می‌کند وجود نخواهد داشت. ویندوز ۱۰ از شما می‌خواهد هویت خود را قبل از آن‌که احراز هویت انجام گیرد، با یک پین‌کد یا دستگاه‌های مجهز به حس‌گر بیومتریک نشان دهید. یک بار که احراز هویت با Passport انجام شد، توانایی دسترسی سریع به سایت‌ها و سرویس‌های مختلف شخصی یا تجاری را که روی



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

شبکه‌های تجاری قرار دارند، خواهید داشت. Passport همچنین با هزاران سرویس Azure Active Directory که در حال اجرا هستند کار خواهد کرد. مکانیسم حذف گذرواژه‌ها با استفاده از فناوری‌های پیش‌رفته رویکردی است که توسط سازمان FIDO در حال پیگیری است. سازمانی که میکروسافت نیز به عضویت آن درآمده است. این سازمان در نظر دارد گذرواژه‌ها را با انواع مختلفی از سرویس‌های امنیتی پیش‌رفته جایگزین کند.

چرا بعضی کاربران شانس استفاده از Windows Hello را از دست خواهند داد؟

برای آن که بتوان از Windows Hello استفاده کرد، به دوربین‌های گران‌قیمتی نیاز است که از عمق زیاد برای نشان دادن واقعیت به کامپیوترها پشتیبانی کنند. این دوربین‌ها در همه جا در دسترس نیستند. همان‌گونه که اشاره کردیم ویژگی Windows Hello و Passport به دوربین‌هایی با عمق زیاد که از نور مادون قرمز استفاده می‌کنند نیاز دارد. این دوربین‌ها توسط اینتل ساخته می‌شوند (دوربین‌های RealSense). تحلیل‌گران و برخی سازندگان کامپیوترهای شخصی بر این باور هستند که ساخت آن‌ها برای کامپیوترهای شخصی ارزان‌قیمتی (با وب‌کم‌های ارزان‌قیمت) که بیش‌تر مصرف‌کنندگان ترجیح می‌دهند از آن‌ها استفاده کنند، بیش از اندازه گران تمام می‌شود. همچنین، بعید به نظر می‌رسد،



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

ماژول‌های این مدل از دوربین‌ها درون بیش‌تر مانیتورهای کامپیوترهای خانگی و لپ‌تاپ‌ها قابل نصب باشد. به این نکته توجه داشته باشید که میلیون‌ها نوت‌بوک مجهز به ویندوز ۷ و ۸ وجود دارند که قصد ارتقا به ویندوز ۱۰ را دارند، اما این دوربین‌ها روی آن‌ها وجود ندارد.

چگونه می‌توان از Windows Hello و اثر انگشت برای ورود به ویندوز ۱۰ استفاده کرد؟

مایکروسافت تمام توان خود را به کار گرفته است تا یکی از امن‌ترین سیستم‌عامل‌هایی را که در تاریخ این شرکت ساخته شده است، عرضه کند. مایکروسافت دو ویژگی Windows Hello و Passport را برای شناسایی چهره و اثر انگشت در سیستم‌عامل ویندوز ۱۰ قرار داده است. با توجه به این‌که هنوز زمان لازم است تا سخت‌افزارهای ویژه که از Windows Hello پشتیبانی می‌کنند به‌طور عمومی عرضه شوند، می‌توان از فناوری دیگری استفاده کرد که Windows Hello از آن پشتیبانی می‌کند. به دلیل این‌که اسکنرهای اثر انگشت از مدت‌ها قبل وجود داشته‌اند، می‌توان از آن‌ها برای ورود به ویندوز ۱۰ استفاده کرد. برای این منظور به یک اسکنر اثر انگشت نیاز است که با ویندوز ۱۰ سازگار باشد. در حال حاضر، با استفاده از اسکنر اثر انگشت (K-Byte Biometric Fingerprint Scanner) به



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

قیمت ۱۱ دلار که در سایت آمازون به فروش می‌رسد و همراه با دو کابل یواس‌بی عرضه می‌شود، می‌توان این کار را انجام داد (شکل ۲).



شکل ۲: سیستم بیومتریک K-Byte که برای احراز هویت مورد استفاده قرار می‌گیرد. این دستگاه از یک طرف به یواس‌بی دستگاه و از طرف دیگر به خود دستگاه متصل می‌شود. در پایین دستگاه مکانی قرار دارد که



شکل ۳: تجهیزات احراز هویت K-Byte



@caffeinebookly



caffeinebookly



@caffeinebookly

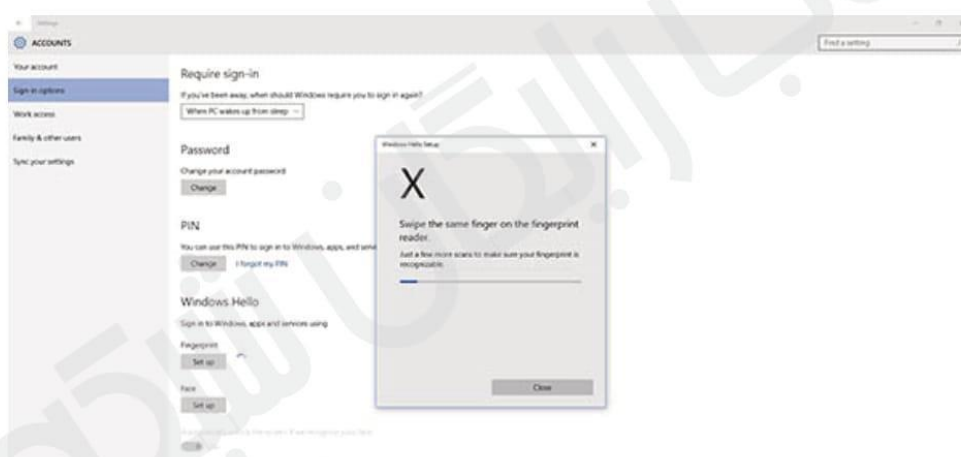


caffeinebookly



t.me/caffeinebookly

برای دریافت اثر انگشت مورد استفاده قرار می‌گیرد (شکل ۳). این دستگاه به خوبی با ویندوز ۱۰ کار کرده است و برای آن که بتوان از آن استفاده کرد، به نصب هیچ درایوری نیاز نیست. زمانی که اسکنر به سیستم متصل شد، با مراجعه به تنظیمات قرار گرفته در نشانی Settings-> Accounts-> Sign-in و پیدا کردن گزینه Windows Hello و انتخاب گزینه Face یا Fingerprint می‌توانید فرآیند پیکربندی را آغاز کنید (شکل ۴).



شکل ۴: فرآیند تنظیم Windows Hello

با کلیک روی گزینه تنظیم اثر انگشت فرآیند تنظیم آغاز می‌شود و از شما برای ورود با PIN/Password سؤال می‌کند. به محض این که فرآیند ثبت یک تصویر خوب از اثر انگشت به اتمام رسید، رهگیری اثر انگشت در سیستم انجام می‌شود و می‌تواند تصویر درستی از اثر انگشت را نشان دهد. زمانی که فرآیند ثبت



@caffeinebookly



caffeinebookly



@caffeinebookly

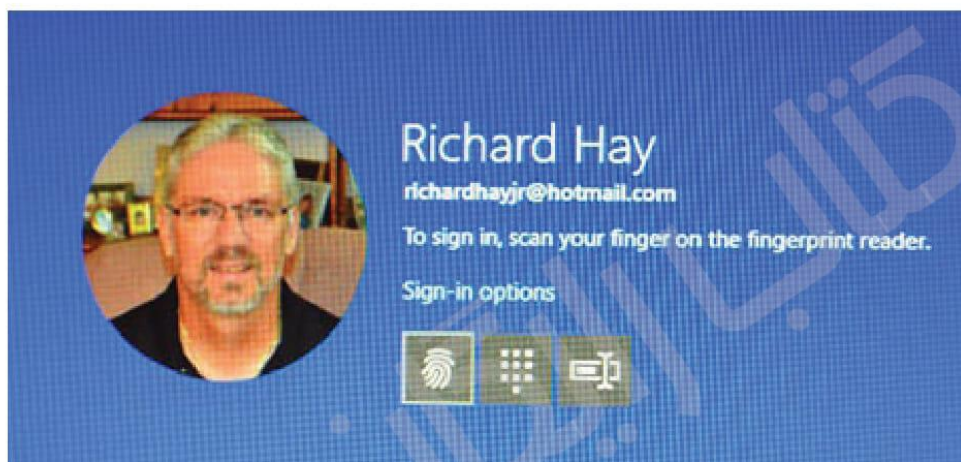


caffeinebookly



t.me/caffeinebookly

اثر انگشت به اتمام رسید، همه پنجره‌ها را ببندید و از ویندوز ۱۰ خارج شوید. در ورود مجدد گزینه‌ای را مشاهده خواهید کرد که شامل به کارگیری اثر انگشت است (شکل ۵).



شکل ۵: گزینه احراز هویت اثر انگشت با استفاده از Finger Print Reader

در این حالت، اگر از یک اثر انگشت غیرمعتبر استفاده شود، سیستم به آسانی آن را تشخیص می‌دهد و مانع از ورود شما به سیستم می‌شود.

Device Guard

زمانی که صحبت از حملات سایبری به میان می‌آید، این حملات دو زاویه اولیه دارند؛ به سرقت بردن هویت کاربر و ورود به شبکه و دوم اجرای نرم‌افزارهای مخرب از درون سازمان. البته اغلب اوقات



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

حملات هر دو حالت را در خود جای می‌دهند. متوقف کردن این حملات یکی دیگر از زمینه‌های تخصصی ویندوز ۱۰ به شمار می‌رود که در آن خوش می‌درخشد. زمانی که یک حمله فیشینگ از طریق ایمیل روی دستگاهی رخ دهد که ویندوز ۱۰ روی آن نصب بوده و Device Guard روی آن فعال است، نصب برنامه مخرب متوقف می‌شود، زیرا آن برنامه قبل از آن که اجرا شود، توسط یک منبع قابل اعتماد امضا نشده است. به عبارت دیگر، نفوذ قبل از آن که حتی شروع شود متوقف می‌شود. Device Guard می‌تواند ترکیبی از ویژگی‌های امنیتی سخت‌افزاری و نرم‌افزاری باشد. زمانی که این دو مؤلفه با یکدیگر ترکیب شوند، یک دستگاه را به گونه‌ای قفل می‌کنند که تنها با اجرای برنامه‌های قابل اعتماد باز شود.

Windows Hello کاربر توانایی نشان دادن چهره یا اثر انگشت خود را به دستگاه‌های جدیدی که ویندوز ۱۰ روی آن‌ها اجرا می‌شود خواهد داشت، به طوری که این دستگاه‌ها در یک بازه زمانی کوتاه توانایی شناسایی او را دارند.

اگر برنامه‌ای قابل اعتماد نباشد، امکان اجرا پیدا نخواهد کرد. این ویژگی همچنین به این معنا است که حتی اگر هکری توانایی اعمال مدیریت و کنترل روی کرنل ویندوز را به دست آورد، بعد از آن که کامپیوتر راه‌اندازی شود، کم‌ترین شانس را برای اجرای کدهای مخرب اجرایی خواهد داشت. همچنین، این که چطور



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

درباره آن چه می‌تواند اجرا کند یا اجرا خواهد کرد تصمیم‌گیری می‌کند؟ Device Guard از یک مکانیسم امنیت مجازی‌ساز محور، برای جدا کردن سرویس کد یک پارچه از کرنل ویندوز ۱۰ استفاده می‌کند. Device Guard به سرویس کد یک پارچه اجازه می‌دهد از امضاهایی که با سیاست کنترلی سازمان تعریف شده است، برای تعیین آنچه قابل اطمینان است استفاده کند.

چرا از Device Guard استفاده کنیم؟

با وجود هزاران فایل مخربی که هر روزه ساخته می‌شود، دیگر نمی‌توان از روش‌های سنتی همچون شناسایی امضامحور برای مبارزه با بدافزارها استفاده کرد، به دلیل این که یک دفاع ناکارآمد به شمار می‌روند. Device Guard به گونه‌ای طراحی شده است که وقتی برنامه‌ای اجرا می‌شود، در برابر بدافزارها از کاربران محافظت کند. به طوری که به ویندوز اجازه می‌دهد درباره قابل اعتماد بودن یا نبودن برنامه‌ها تصمیم بگیرد. در صورتی که برنامه‌ای قابل اعتماد نباشد، پیام هشدار به کاربر نشان داده خواهد شد.

Device Guard چگونه کار می‌کند؟

Device Guard محدودیت‌هایی را برای سیستم‌عامل ویندوز ۱۰ به وجود می‌آورد که فقط کدهایی را اجرا کند که امضاکنندگان معتبر امضا کرده باشند. همچنین، هر پردازشی را که قرار است



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

داخل حافظه اصلی سیستم بارگذاری و اجرا شود، مورد بررسی قرار می‌دهد، به طوری که از اجرای برنامه‌هایی که فاقد امضا هستند ممانعت به عمل می‌آورد و اجازه نمی‌دهد این برنامه‌ها درون حافظه سیستم بارگذاری شوند.

برای اجرای Device Guard چه چیزی نیاز است؟

برای استفاده مؤثر از ویندوز ۱۰ به نصب سخت‌افزار و نرم‌افزارهای زیر نیاز دارید.

• **Windows 10:** Device Guard فقط با دستگاه‌هایی کار می‌کند که ویندوز ۱۰ را اجرا می‌کنند.

• **UEFI:** نسل جدید میان‌افزارها یا UEFI شامل یک ویژگی امنیتی به نام راه‌اندازی امن Secure Boot هستند که از یک پارچگی دستگاه شما با خود سفت‌افزار محافظت می‌کند و به شما اطمینان می‌دهد ویندوز قبل از اجرای هر گونه نرم‌افزار مخربی اجرا می‌شود.

• **Trusted Boot:** بخشی از سیستم عامل است که بر ویژگی راه‌اندازی ایمن UEFI برای جلوگیری از اجرای برنامه‌های مخربی که در مدت زمان بارگذاری سیستم عامل اجرا می‌شوند، تکیه می‌کند. راه‌اندازی ایمن تغییری در معماری است که به محافظت در برابر حملات روت‌کیت‌ها کمک می‌کند. حملاتی که با هدف دسترسی به سیستم سعی می‌کنند فرآیند راه‌اندازی ویندوز را



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

دست کاری کنند.

اگر دستگاه شما به یک حس گر اثر انگشت مجهز باشد، شما می‌توانید برای باز کردن دستگاه خود از Windows Hello استفاده کنید .

۱ . Virtualization-based security

یک کانتینر محافظت شده Hyper-V است که فرآیندهای حساس ویندوز ۱۰ را ایزوله می‌کند. این کار باعث می‌شود، حتی اگر کرنل ویندوز ۱۰ در دسترس قرار گیرد، دست کاری در فرآیندها برای استخراج داده‌های ضروری که در حملات مورد استفاده قرار می‌گیرند، برای بدافزارها مشکل شود. برای استفاده از امنیت مبتنی بر مجازی‌سازی لازم است تا افزونه‌های مجازی‌ساز روی سیستم اجرا شده باشند.

۲ . Package inspector tool

ابزاری است که به شما کمک می‌کند تا کاتالوگی از فایل‌هایی ایجاد کنید که برای اجرای برنامه‌های کلاسیک ویندوز مورد استفاده قرار می‌گیرند. زمانی که این کاتالوگ ساخته شود، برنامه‌ها به آسانی توسط یک امضاکننده معتبر امضا می‌شوند. البته برای پیاده‌سازی Device Guard در یک سازمان لازم است به یک سری از دستورالعمل‌ها که از سوی مایکروسافت در این باره ارائه شده است، توجه کنید.



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

۳ . Enterprise Data Protection (محافظة از داده‌های سازمانی)

با افزایش دستگاه‌های شخصی متعلق به کاربران در سازمان‌ها، ریسک افشای تصادفی اطلاعات از طریق برنامه‌ها و سرویس‌هایی که خارج از کنترل یک سازمان هستند وجود دارد. برنامه‌هایی همچون ایمیل، شبکه‌های اجتماعی و فضای ابری عمومی ریسک افشای اطلاعات را افزایش می‌دهند. ویژگی حفاظت از داده‌های سازمانی EDP تجربه کاربری ویژه‌ای را ارائه می‌کند، به طوری که به جداسازی بهتر و کمک به محافظت از برنامه‌های سازمانی بدون نیاز به اعمال تغییرات در محیط یا برنامه‌ها کمک می‌کند. همچنین، EDP زمانی که همراه با RMS (سرنام Rights Management Services) کاربرد دارد، می‌تواند برای محافظت از داده‌های محلی سازمان نیز مورد استفاده قرار گیرد. تداوم حفاظت از داده‌ها حتی زمانی که داده‌های شما به اشتراک گذاشته شده‌اند، از مزیت‌های EDP به شمار می‌رود.

زمانی که یک حمله فیشینگ از طریق ایمیل روی دستگاهی رخ دهد که ویندوز ۱۰ روی آن نصب بوده و Device Guard روی آن فعال است، نصب برنامه مخرب متوقف می‌شود، زیرا آن برنامه قبل از آن که اجرا شود، توسط یک منبع قابل اعتماد امضا نشده است.

۴ . Microsoft Passport

در ویندوز ۱۰، Microsoft Passport جایگزین گذرواژه‌ها شده است.



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

Microsoft Passport به کاربران اجازه می‌دهد احراز هویت را با یک حساب مایکروسافتی، یک حساب اکتیو دایرکتوری (Active Directory)، یک حساب (Microsoft Azure Active Directory AD) یا حتی سرویس غیر مایکروسافتی که از احراز هویت (FIDO) Fast ID Online پشتیبانی می‌کند، انجام دهند. بعد از آن که تأیید اولیه دو مرحله‌ای که در مدت زمان ثبت Microsoft Passport انجام می‌شود سپری شد، گذرنامه مایکروسافت روی دستگاه کاربر تنظیم می‌شود و کاربر این توانایی را دارد تا از مواردی همچون Windows Hello یا PIN استفاده کند. کاربر این ژست‌ها را برای بررسی هویت آماده می‌کند. در ادامه، ویندوز از Microsoft Pass-port برای احراز هویت کاربران استفاده و به آن‌ها برای دسترسی به منابع و سرویس‌های محافظت شده کمک می‌کند.

۵ . Provisioning packages

این ابزار به شما اجازه می‌دهد با سرعت و کارایی بالا به پیکربندی یک دستگاه بدون نیاز به داشتن یک تصویر جدید از آن پردازید. بسته‌های تأمینی (Provisioning Package) شامل مجموعه مختصری از دستورالعمل‌ها است و به کارگیری آن‌ها به اندازه کافی ساده است. به طوری که یک دانش‌آموز یا یک کارمند غیرفنی می‌توانند از آن‌ها برای پیکربندی دستگاه‌های خود استفاده کنند. در نتیجه، زمان لازم برای پیکربندی چند دستگاه در



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

یک سازمان به میزان قابل توجهی کاهش می‌یابد.

مزایای به‌کارگیری Provisioning packages

- پیکربندی سریع یک دستگاه جدید بدون نیاز به نصب یک تصویر جدید؛
- صرفه‌جویی در زمان با پیکربندی چند دستگاه با استفاده از یک بسته تأمینی؛
- پیکربندی سریع دستگاه‌های کارمندان در یک سازمان بدون نیاز به زیرساخت MDM (سرنام Mobile Device Management)؛
- تنظیم یک دستگاه بدون آن‌که هیچ ارتباط شبکه‌ای را در اختیار داشته باشد؛
- آن‌ها می‌توانند با استفاده از رسانه‌های قابل حمل همچون فلاپی درایوهای یواس‌بی یا کارت SD نصب شوند؛
- آن‌ها می‌توانند به یک ایمیل ضمیمه شوند.
- آن‌ها می‌توانند از طریق یک اشتراک شبکه‌ای دانلود شوند.

یک بسته تأمینی را چگونه می‌توان ایجاد کرد؟

در ویندوز ۱۰ می‌توانید از Windows Images و ابزار Configuration Designer (ICD) برای ساخت بسته‌های تأمینی استفاده کنید. برای نصب Windows ICD و ساخت بسته‌های تأمینی ابتدا باید Windows Assessment and Deployment Kit (ADK) RC



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

را نصب کنید.

برای نصب کیت ارزیابی و استقرار ویندوز، ابتدا باید آن را از Windows Insider (برای دانلود این کیت لازم است عضوی از Windows Insider باشید):

همچنان که در حال نصب ADKsetup.exe هستید، ویژگی‌هایی که در دیالوگ مربوط نشان داده می‌شوند را انتخاب کنید. این ویژگی‌ها عبارتند از:

• Deployment Tools

• (Windows Preinstallation Environment (Windows PE

• (Windows Imaging and Configuration Designer (ICD

• (Windows User State Migration Tool (USMT

البته لازم به توضیح است که اجرای درست Windows ICD به ابزارهای دیگر وابسته است. اگر فقط Windows ICD را در ویزارد نصب انتخاب کرده باشید، ابزارهایی که به آن‌ها اشاره کردیم، به‌طور خودکار انتخاب و نصب می‌شوند. زمانی که Windows ICD را نصب کردید، می‌توانید از آن برای ساخت بسته‌های امنیتی استفاده کنید. جزییات مربوط به ساخت و استفاده از بسته‌های تأمینی در این نشانی وجود دارد.

فونت‌ها می‌توانند آسیب‌پذیری‌هایی را که به حملات (سرنام EOP (Elevation of Privilege منجر می‌شوند، تولید کنند. حملات EOP امکان دسترسی از راه دور به سیستم کاربر را به یک هکر می‌دهد.



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

۶ . Untrusted font blocking

از آنجا که فونت‌ها از ساختارهای داده‌ای پیچیده استفاده می‌کنند و درون صفحات وب و اسناد قرار می‌گیرند، می‌توانند آسیب‌پذیری‌هایی را که به حملات (سرنام EOP (Elevation of Privilege منجر می‌شوند، تولید کنند. حملات EOP امکان دسترسی از راه دور به سیستم کاربر را به یک هکر می‌دهد. این دسترسی زمانی رخ می‌دهد که کارمندان در حال به اشتراک گذاری فایل‌ها یا مرور وب هستند. برای محافظت از سازمان‌ها در برابر این گونه حملات، مایکروسافت ویژگی بلوکه کردن فونت‌های غیرقابل اعتماد را پیشنهاد داده است.

این ویژگی چگونه کار می‌کند؟

این ویژگی به سه روش می‌تواند مورد استفاده قرار گیرد:

On: زمانی که این گزینه فعال باشد، هر فونتی که توسط GDI به کار رود، مورد بررسی قرار می‌گیرد. این فرآیند بارگذاری فونت‌هایی را متوقف می‌کند که خارج از پوشه %/Fonts%/windir قرار دارند. همچنین، گزارشی از این عملیات در فهرست رویدادها ثبت می‌شود.

Audit: فعال بودن این گزینه امکان ثبت گزارش را ایجاد می‌کند، اما بارگذاری فونت‌ها را بلوکه نمی‌کند. نام برنامه‌هایی را که از فونت‌های تأیید نشده استفاده کرده‌اند، در فهرست گزارش ثبت می‌کند.



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

Exclude apps to load untrusted fonts: فعال بودن این گزینه باعث می‌شود تا برنامه‌های خاصی را به صورت انحصاری درآورید. به عبارت دیگر، به آن‌ها اجازه دهید فونت‌های تصدیق نشده را بارگذاری کنند. حتی اگر این ویژگی فعال باشد. برای تنظیم این ویژگی به یکی از سه وضعیت اشاره شده لازم است تا مراحل زیر را انجام دهید:

۱. رجیستری را باز کنید و به مسیر زیر بروید:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Kernel
```

۲. اگر کلید MitigationOptions وجود ندارد، کلیک راست کرده و این کلید را (64-bit) QWORD اضافه کنید. دقت کنید نام آن را MitigationOptions قرار دهید.

۳. از کلید MitigationOptions مقدار Value Date را به روزرسانی کنید. دقت کنید مقادیر شما یکی از مقادیری باشد که در پاراگراف قبل به آن‌ها اشاره کردیم.

To turn this feature on. Type 1000000000000

To turn this feature off. Type 2000000000000

To audit with this feature. Type 3000000000000

نکته مهم: مقداری که در MitigationOptions وجود دارد، باید در مدت زمان به روزرسانی ذخیره شود. به طور مثال، اگر مقدار



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

جاری برابر با 1000 است، مقدار به روزرسانی شده شما باید 1000000001000 باشد.

۴. در این مرحله، لازم است تا سیستم یک بار راه اندازی شده تا تغییر مورد نظر اعمال شود. بعد از آن که این تغییر اعمال شد، با استفاده از مؤلفه ناظر رویدادها Event Viewer می‌توانید گزارش‌های تولید شده را مشاهده کنید.

شبکه در windows 10

دانلود رایگان کتابچه راهنمای تنظیمات شبکه در ویندوز ۱۰

یکی از ویژگی‌های جذاب ویندوز ۱۰ نسبت به نسخه‌های قبلی سیستم عامل مایکروسافت، امکانات و ابزارهای زیاد ارایه شده در بخش شبکه است. کاربران شبکه می‌توانند در ویندوز ۱۰ انواع تنظیمات و گزینه‌های دلخواه را انجام و با سرعت بیشتری مشکلات شبکه یا اینترنت را شناسایی و رفع کنند. این کتاب الکترونیکی همین موضوع را هدف قرار گرفته است و مجموعه‌ای از ۵ مقاله پیرامون تنظیمات شبکه در ویندوز ۱۰، مدیریت آداپتورها و رفع مشکلات اینترنت در ویندوز ۱۰ است.



www.shabakeh-mag.com



@caffeinebookly



caffeinebookly



@caffeinebookly



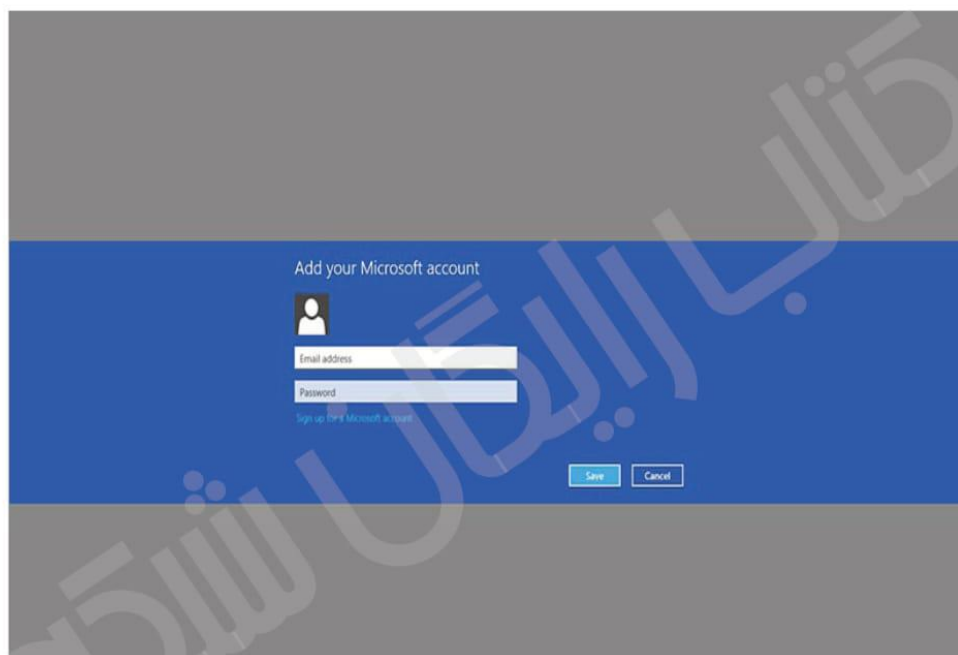
caffeinebookly



t.me/caffeinebookly

حذف کامل حساب کاربری مایکروسافت

آموزش راهکاری برای فرار از جاسوسی مایکروسافت در ویندوز ۱۰



اگر شما هم نگاهی به سرتیتر اخباری که نشان می‌دهد مایکروسافت چگونه در همه حال مراقب شما است انداخته باشید، تعجب خواهید کرد که چگونه ویندوز ۱۰ به یک موفقیت جهانی تبدیل شده است. تا به حال بیش از ۷۲ میلیون نسخه از آخرین سیستم‌عامل این غول دنیای نرم‌افزار روی سیستم‌های سراسر جهان نصب شده است و در بیشتر موارد با واکنش‌های بسیار مثبتی از جانب مطبوعات و مردم مواجه شده است. اما مسائلی



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



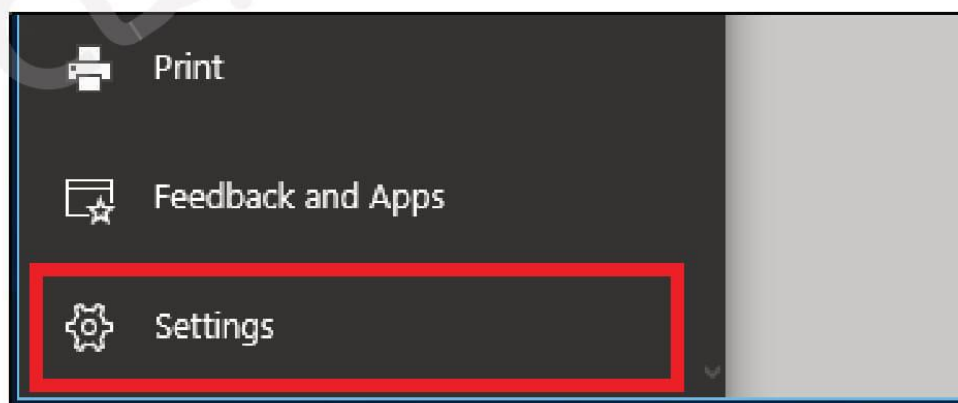
t.me/caffeinebookly

همچون بسیاری از موارد نقض حریم خصوصی، منوی استارت آزاردهنده و تعداد زیاد نرم افزارهای جعلی در ویندوز ۱۰ را چگونه می توان تحمل کرد؟

یکی از بهترین روش ها برای اطمینان از اینکه هیچ کدام از داده های شما بدون رضایت شما توسط این شرکت استفاده نخواهد شد، حذف حساب کاربری مایکروسافت شما است. با این کار شما خود را از بانک اطلاعاتی ویندوز نیز حذف خواهید کرد، بنابراین منابع ثالث تایید نشده دیگر نیز نمی توانند هیچ اطلاعاتی را بدون اجازه شما جمع آوری کنند.

حذف حساب کاربری به صورت محلی

اولین مرحله از انجام این فرآیند حذف حساب کاربری مایکروسافت از روی کامپیوتر محلی شما است.



@caffeinebookly



caffeinebookly



@caffeinebookly

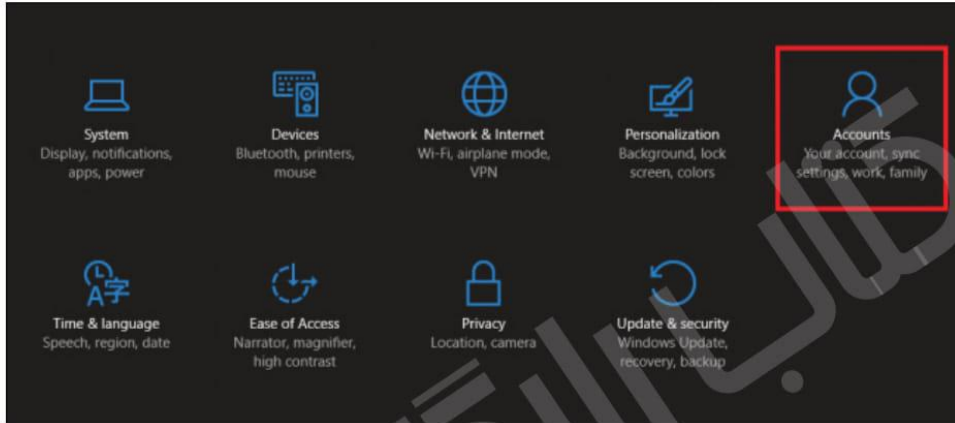


caffeinebookly

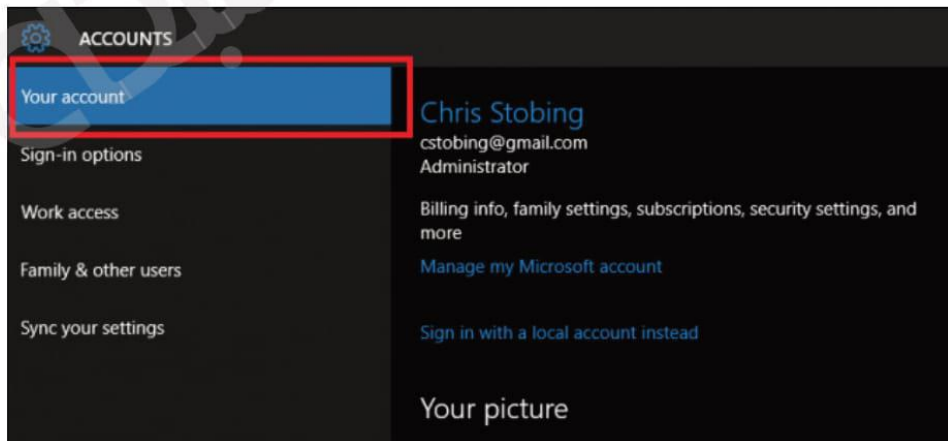


t.me/caffeinebookly

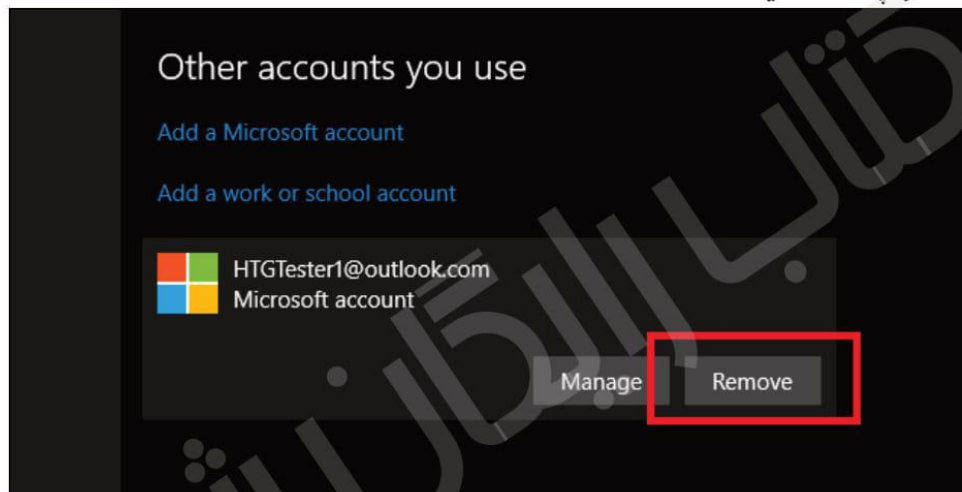
برای انجام این کار، به بخش Settings رفته و روی قسمت Accounts کلیک کنید.



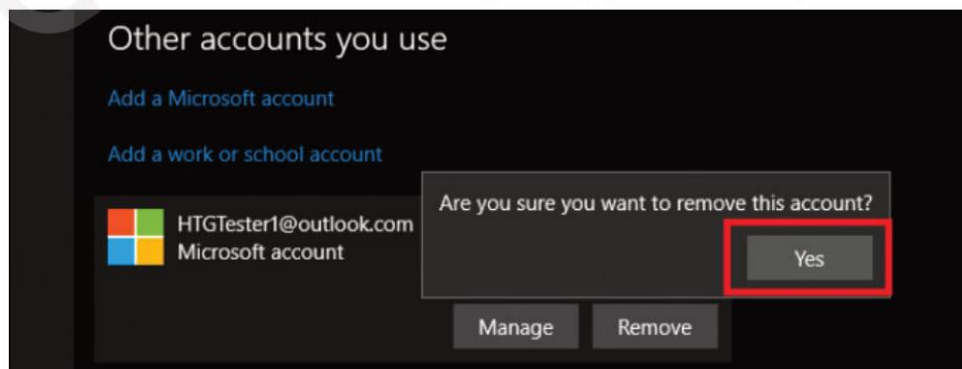
همان گونه که در تصویر زیر مشخص شده است، با ورود به این قسمت شما می‌توانید گزینه حذف حساب کاربری مایکروسافت را در قسمت انتهایی تب Your account پیدا کنید.



توجه داشته باشید که شما نمی‌توانید همان حساب کاربری را که در حال حاضر با آن به سیستم وارد شده‌اید را حذف کنید. شما یا باید ابتدا یک حساب کاربری جداگانه ایجاد کرده و به وسیله این حساب به سیستم وارد شوید، و یا کل محتوای نصب ویندوز ۱۰ را پاک کنید.



بعد از اینکه شما با یک حساب کاربری جداگانه به سیستم وارد شدید، حسابی را که از ابتدا قصد پاک کردن آن را داشتید را انتخاب کنید و بعد از ظاهر شدن کادر مربوطه گزینه Remove را انتخاب کنید.



عجله نکنید هنوز یک مرحله دیگر برای حذف این حساب از اینترنت باقی مانده است.

پاکسازی حساب کاربری از وبسایت مایکروسافت

حتی بعد از پاک کردن حساب کاربری مایکروسافت شما از روی کامپیوتر محلی، تمام داده‌ها و اطلاعات شخصی موجود در آن همچنان روی سرورهای اختصاصی مایکروسافت نگهداری می‌شود. برای خلاص شدن از یک حساب کاربری به طور کامل، شما باید از ابزار موجود در وبسایت مایکروسافت استفاده کنید.

توجه داشته باشید که قبل از حذف کامل حساب کاربری خود، مطمئن شوید که موجودی کیف پول دیجیتال خود را از Windows Store خالی کرده باشید، هرگونه اشتراکی را که مربوط به این حساب است را لغو کرده باشید و از تمام اسناد، تصاویر یا داده‌های شخصی که می‌خواهید روی کامپیوتر خود ذخیره کنید، نسخه پشتیبان تهیه کنید. با این روش شما می‌توانید اطمینان حاصل کنید که حتی بعد از بسته شدن این حساب کاربری، شما همچنان در مواقع لزوم به تمام فایل‌های خود دسترسی خواهید داشت.

بعد از انجام تمام این اقدامات احتیاطی، از طریق این لینک به وبسایت مایکروسافت بروید. بعد از لود شدن کامل صفحه، از شما خواسته می‌شود که وارد حساب کاربری خود شوید. بعد از ورود



@caffeinebookly



caffeinebookly



@caffeinebookly

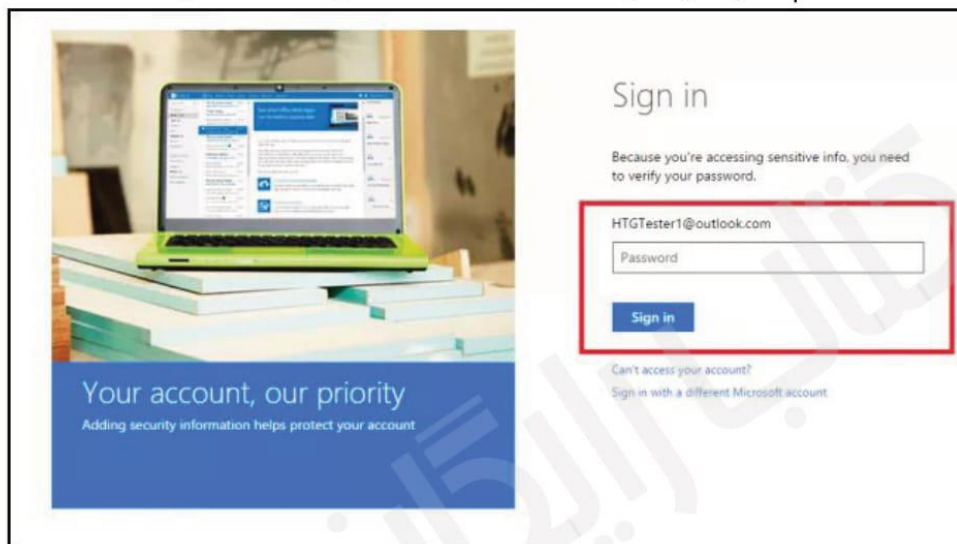


caffeinebookly

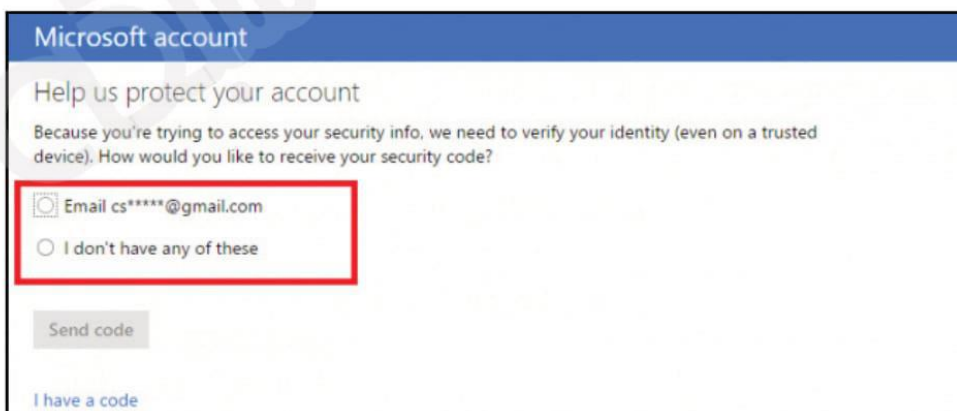


t.me/caffeinebookly

باید بخش Close your account را پیدا کنید.
بعد از انجام این مراحل، شما به صفحه زیر هدایت خواهید شد، در

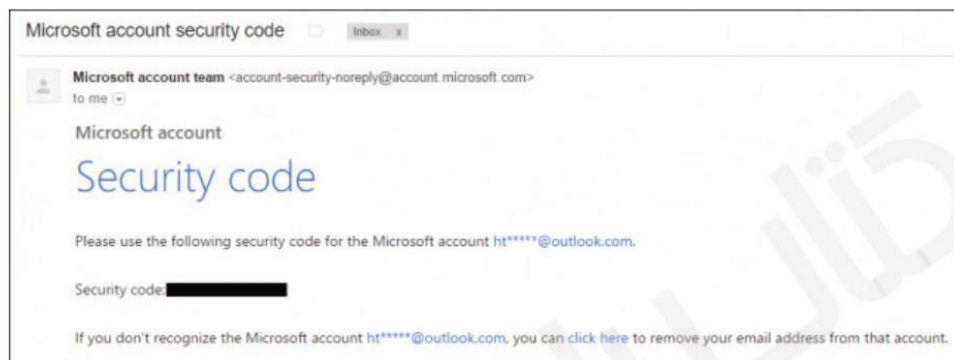


اینجا برای تعیین هویت واقعی شما باید مرحله وارد کردن آدرس ایمیل پشتیبان یا شماره تلفن خود را پشت سر بگذارید.



بعد از پشت سر گذاشتن این مرحله، یک کد به ایمیل شما یا

به صورت پیامک برای شما ارسال خواهد شد (چیزی شبیه به تصویر زیر)



کد دریافت شده را در قسمت نوار تاییدیه وارد کنید. بعد از پشت سر گذاشتن این صفحه مایکروسافت برای اطمینان از اینکه شما کاملاً از عواقب ناشی از بستن حساب کاربری خود آگاهی دارید از شما می‌خواهد که روی چندین کادر مشخص شده کلیک کنید.

Mark htgtester1@outlook.com for closure

After 60 days, this account will be unrecoverable, and will lose access to any service where it's used to sign in. You might use your account for more than you're thinking of right now; the most common effects of closure are listed below, but we recommend you [read more about account closure](#).

Select the check boxes to acknowledge you've read each item below. Once this account is closed, 60 days from now:

- You might lose any account balances and will lose access to subscription services such as Office365, Xbox, and OneDrive.
Note - Don't close this account until you have verified that it has no subscriptions or outstanding balances.
- You will lose access to Outlook.com, Hotmail, and OneDrive.
You'll no longer have access to any mail, documents, or photos you've stored using these Microsoft services.



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

آنها شما را با حقایق آشکاری نظیر اینکه شما دیگر قادر به وارد شدن به این حساب کاربری نخواهید بود، اینکه اکس باکس شما دیگر آن گونه که شما انتظار دارید کار نخواهد کرد، و اینکه دسترسی به ایمیل شما هم در Outlook و هم Hotmail مسدود خواهد شد، به ستوه خواهند آورد. هر کسی که قبلاً تجربه قطع عضویت در Xbox Live را داشته این تجربه را دارد که مایکروسافت تمام تلاش خود را می کند تا شما از لغو عضویت خود منصرف شوید.

You'll lose access to data you've stored anywhere you use this account to sign in. Information you've managed using family settings, HealthVault, MSN Money, and Messenger contacts added to Skype will be lost.

Your devices with Reset Protection enabled could become unusable. Reset Protection prevents your phone from being easily reset or reused by an unauthorized person. If you want to continue to use Reset Protection, do not close your account. Otherwise, [be sure to disable Reset Protection here](#).

Still want to close this account? We're sorry to see you go. Before you do so, please tell us why you're leaving.

I no longer want any Microsoft account

By clicking Mark account for closure, I confirm that I understand I will lose access to sites, services and data associated with this Microsoft account. I have reviewed [the effects of closing an account](#).

بعد از اینکه شما روی تمام این کادرها کلیک کردید، مایکروسافت تازه از شما سوال می کند که چرا تصمیم گرفته اید که حساب خود را حذف کنید. یک دلیل محکمه پسند وارد کنید و بعد روی



@caffeinebookly



caffeinebookly



@caffeinebookly

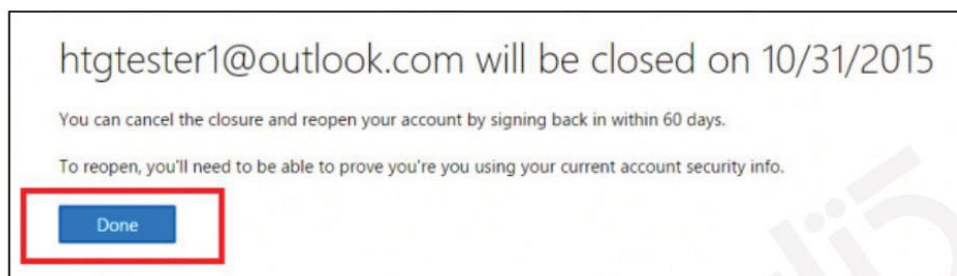


caffeinebookly



t.me/caffeinebookly

Mark account for closure کلیک کنید.



در نهایت و محض احتیاط برای اینکه اگر روزی به اشتباه خود پی بردید و از کرده خود پشیمان شدید، مایکروسافت این لطف را در حق شما خواهد کرد تا بتوانید ظرف ۶۰ روز آینده دوباره حساب کاربری خود را بازیابی کنید.

از زمان انتشار ویندوز ۱۰، هر روز کاربران بیشتری متوجه این موضوع می‌شوند که داشتن یک حساب کاربری آنلاین ساده از مایکروسافت می‌تواند چه مسائل امنیتی را برای آنها به وجود آورد. مشکلاتی که شما هرگز تصور آن را هم نمی‌کردید. اگر شما هم ترجیح می‌دهید اطلاعات خود را از دسترس این غول دنیای نرم افزار محفوظ نگه دارید. یک بار برای همیشه حساب کاربری خود را به طور کامل از این شرکت حذف کنید و مطمئن شوید به جز مواردی که خود شما صلاح می‌دانید، داده‌های شما به هیچ شکل دیگری مورد استفاده قرار نخواهد گرفت.



@caffeinebookly



caffeinebookly



@caffeinebookly

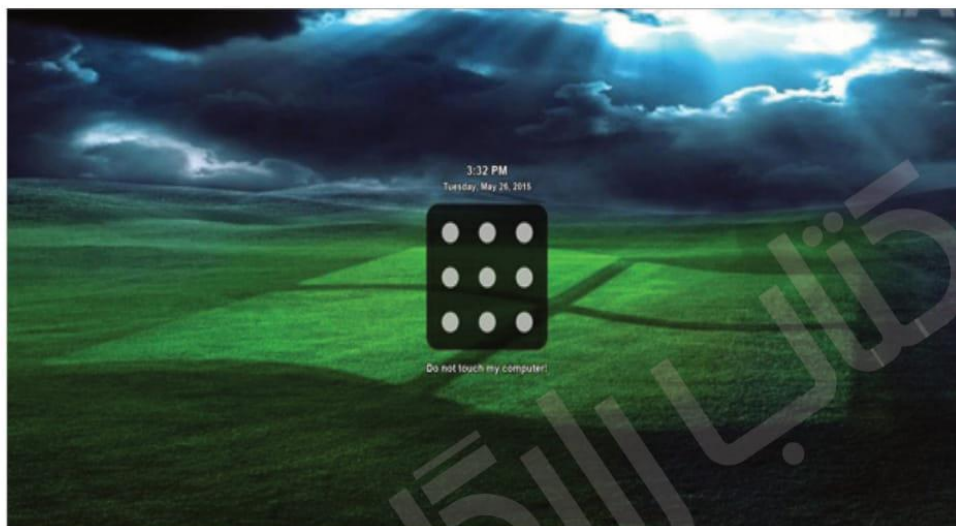


caffeinebookly



t.me/caffeinebookly

چگونه یک صفحه قفل لاگین ویندوز ۱۰ ایجاد کنیم؟



ویندوز ۱۰ در بخش‌های مختلفی دست‌خوش تغییرات اساسی گشت. از جمله بخش‌هایی که تغییرات چشم‌گیری را به خود دیده است، صفحه قفل لاگین ویندوز ۱۰ است. رویکردی که مایکروسافت در ارتباط با صفحه قفل در پیش گرفته است بی‌ارتباط با حالتی که در دستگاه‌های تلفن همراه آن را مشاهده کرده‌ایم؛ نیست. این ویژگی اکنون به کامپیوترهای دسکتاپ وارد شده است. کاربران دسکتاپ ویندوز ۱۰ اکنون این توانایی را دارند تا صفحه قفل را آن‌گونه که به آن نیاز دارند طراحی کنند. ما در این مقاله قصد داریم این روش‌ها را به شما نشان دهیم.

به کارگیری گذرواژه‌ها از اولین مکانیزم‌هایی است که توسط کاربران عادی و حرفه‌ای مورد استفاده قرار می‌گیرد. به کارگیری



@caffeinebookly



caffeinebookly



@caffeinebookly

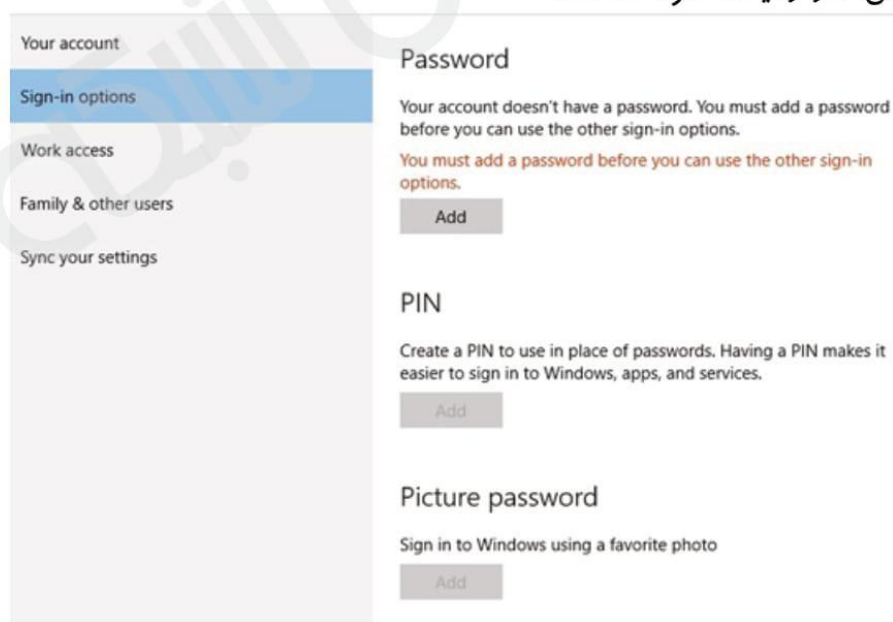


caffeinebookly



t.me/caffeinebookly

گذرواژه‌ها کار چندان سختی نبوده و به آسانی قابل تنظیم است. برای این منظور ابتدا پنجره Settings را باز کرده، روی گزینه Accounts کلیک کرده و در ادامه گزینه Sign-in Options را انتخاب کنید. در پنجره ظاهر شده، به سه روش مختلف می‌توانید به یک ماشین وارد شوید. اولین روش، همان تکنیک معروف تنظیم گذرواژه‌ها برای حساب کاربری است. در این مکانیزم با تلفیق اعداد و کاراکترها دسترسی به دسکتاپ سیستم امکان‌پذیر می‌شود. پیکربندی این گزینه پیچیدگی خاصی نداشته و همچون گذشته (سیستم عامل ویندوز ۸،۱) می‌تواند مورد استفاده قرار گیرد. برای آن که بتوانید به مکانیزم‌های دیگر دسترسی داشته باشید ابتدا لازم است گذرواژه‌ای را تنظیم کنید. در ادامه این گزارش تصویری مراحل کار را یاد خواهد داد:



@caffeinebookly



caffeinebookly



@caffeinebookly

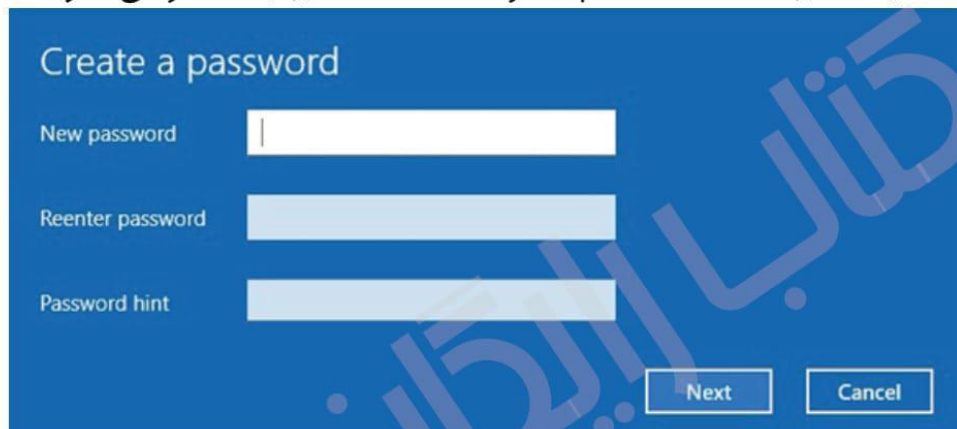


caffeinebookly



t.me/caffeinebookly

همان‌گونه که در تصویر مشاهده می‌کنید، هنوز هیچ گذرواژه‌ای تعیین نشده است، برای آن‌که به دیگر گزینه‌های موجود در این قسمت دسترسی پیدا کنید، ابتدا باید گذرواژه‌ای را مشخص کنید. با کلیک روی دکمه Add پنجره ساخت گذرواژه ظاهر می‌شود.



در پنجره ظاهر شده باید گذرواژه را در فیلدهای مربوطه وارد کنید. بعد از وارد کردن گذرواژه خود روی دکمه Next کلیک کنید.



عد از آن‌که گذرواژه خود را به درستی وارد کردید در پنجره ظاهر شده روی دکمه Finish کلیک کنید.



@caffeinebookly



caffeinebookly



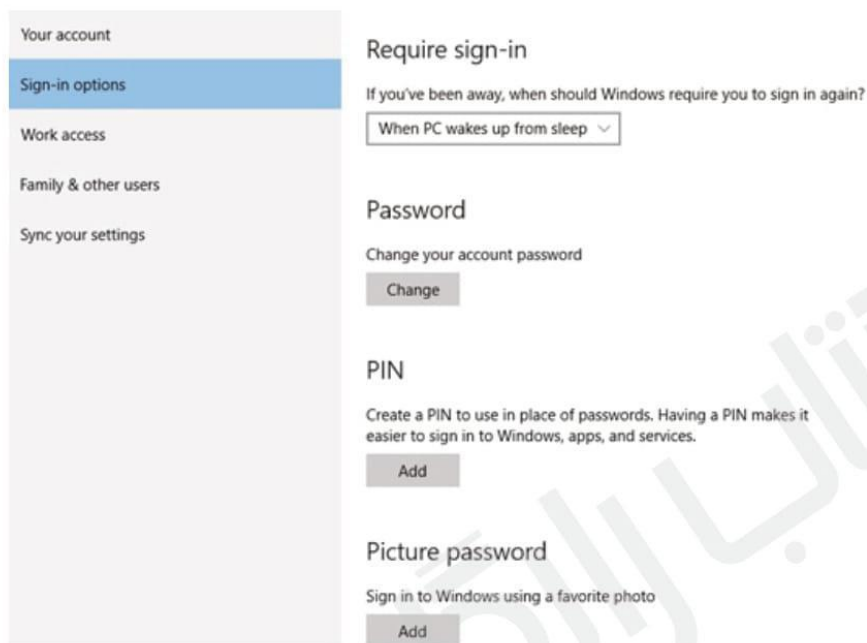
@caffeinebookly



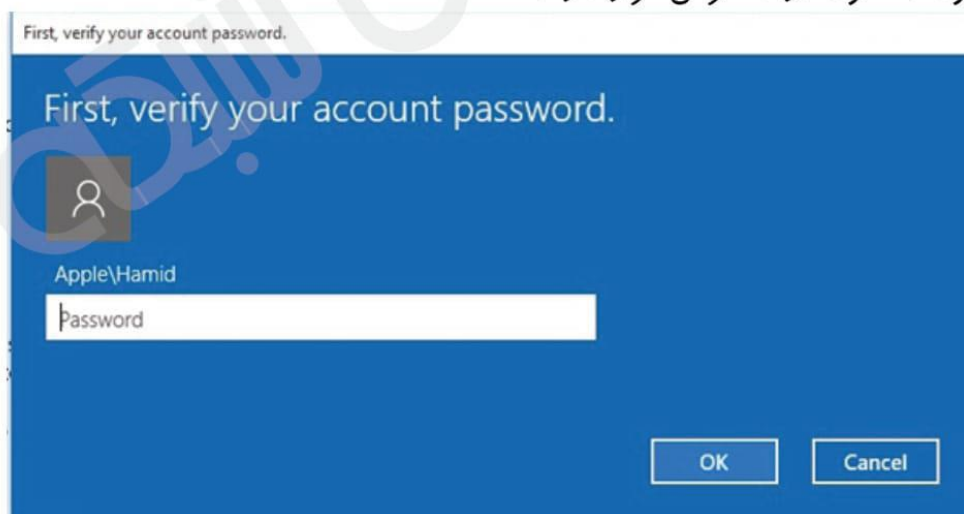
caffeinebookly



t.me/caffeinebookly

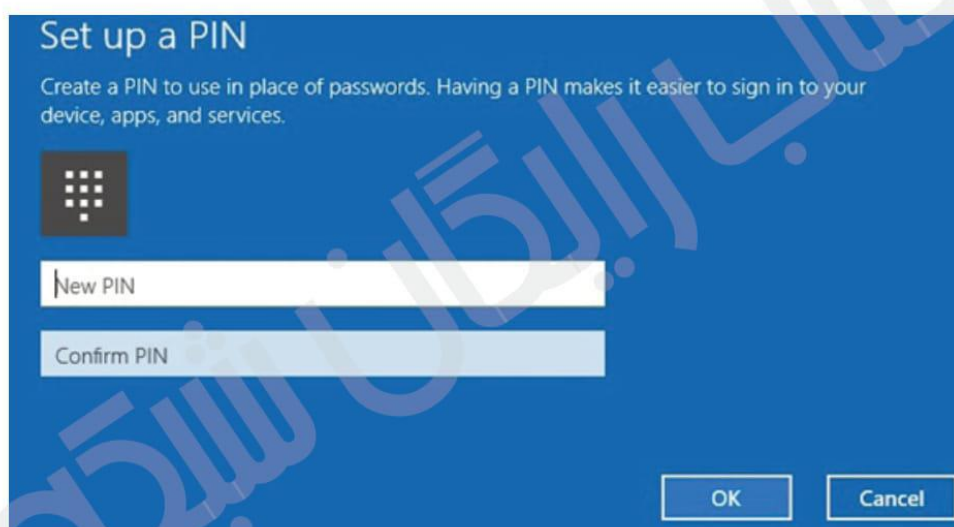


همان گونه که در تصویر مشاهده می کنید، اکنون گزینه هایی که غیر فعال بودند اکنون در دسترس قرار دارند.



گزینه دیگری که در این قسمت قرار دارد در ارتباط با PIN است.

این گزینه به شما اجازه می‌دهد تا روی ماشین خود به آسانی به حساب ویندوز همچون برنامه‌ها و سرویس‌هایی که مورد استفاده قرار می‌دهید، دسترسی داشته باشید. زمانی که روی گزینه PIN کلیک کنید، پنجره‌ای همانند تصویر فوق ظاهر می‌شود. در این پنجره ابتدا باید گذرواژه‌ای که آنرا در قسمت قبل وارد کرده‌اید را تایپ کرده و روی دکمه Ok کلیک کنید.



در پنجره ظاهر شده باید پین کدی را وارد کنید که در مکان گذرواژه ظاهر می‌شود. مزیت به کارگیری پین کد در این است که می‌توانید به راحتی به برنامه‌ها، دستگاه‌ها و سرویس‌ها وارد شوید. بعد از وارد کردن پین کد روی دکمه Ok کلیک کنید. پین کد وارد شده حداقل باید دارای چهار کاراکتر باشد.



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

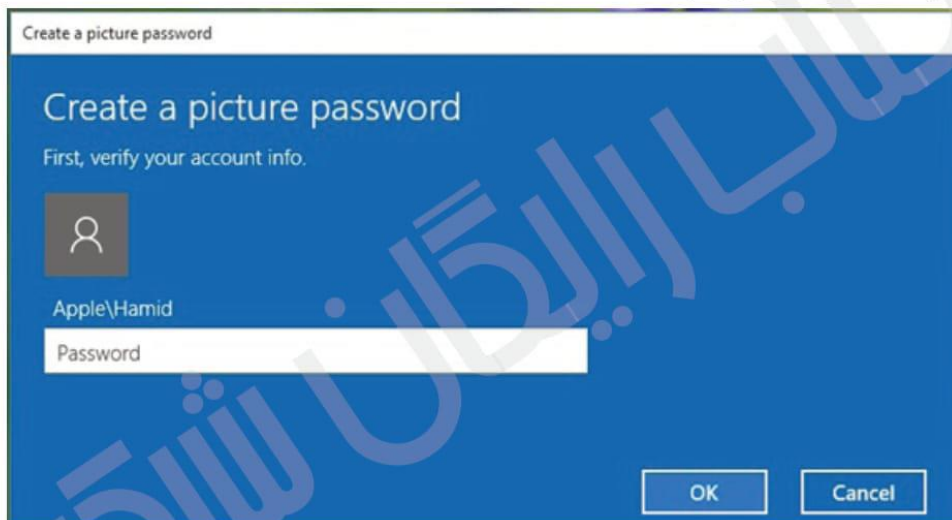
PIN

You can use this PIN to sign in to Windows, apps, and services.

Change

[I forgot my PIN](#)

بعد از وارد کردن پین کد، این بار در پنجره Setting پیغامی مبنی بر استفاده از پین کد ظاهر می‌شود.



سومین روشی که می‌توانید از آن استفاده کنید، قفل تصویری است. امروزه بیشتر کاربران با مکانیزمی که توسط این روش مورد استفاده قرار می‌گیرد آشنایی دارند. برای به کارگیری این روش نیازمند یک تصویر هستید. زمانی که روی دکمه Add در بخش Password کلیک می‌کنید، ابتدا پنجره‌ای ظاهر می‌شود که در آن باید گذرواژه وارد شده را تایپ کنید. در سمت چپ تصویر روی دکمه Choose picture کلیک کنید.



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly

Welcome to picture password

Picture password is a new way to help you protect your touchscreen PC. You choose the picture — and the gestures you use with it — to create a password that's uniquely yours.

When you've chosen a picture, you "draw" directly on the touchscreen to create a combination of circles, straight lines, and taps. The size, position, and direction of your gestures become part of your picture password.

Choose picture

اکنون باید تصویری که تمایل دارید از آن به عنوان گذرواژه استفاده کنید، را مشخص کنید. با کلیک روی دکمه **Choose Picture** پنجره‌ای ظاهر می‌شود که در آن تصویر مورد نظر خود را می‌توانید انتخاب کنید.

How's this look?

Drag your picture to position it the way you want.

Use this picture

Choose new picture

در سمت چپ تصویر دو دکمه در اختیارتان قرار دارد. اگر در نظر دارید تا تصویر را عوض کنید روی دکمه **Choose new picture** کلیک کنید. اگر تصویر مطابق نظرتان است روی دکمه **Use this picture** کلیک کنید.



@caffeinebookly



caffeinebookly



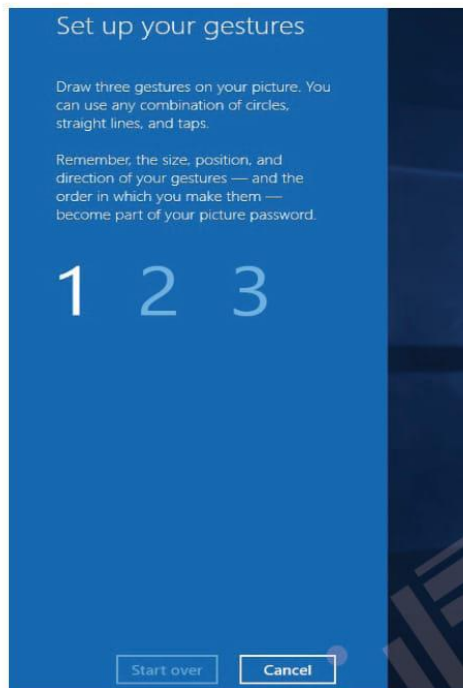
@caffeinebookly



caffeinebookly



t.me/caffeinebookly



اکنون باید در سه مرحله ژست‌هایی که در نظر دارید را تعیین کنید. بعد از آن که ژست‌ها را تنظیم کردید روی دکمه Start Over کلیک کنید. همچنین اگر از ادامه کار منصرف شده‌اید می‌توانید روی دکمه cancel کلیک کنید.

کتابخانه دیجیتال



@caffeinebookly



caffeinebookly



@caffeinebookly



caffeinebookly



t.me/caffeinebookly