شبکه

کتاب شبکه | ۱۰

۲ | Windoes 10

امنیت در Windoes 10

پنجره‌های سیستم خود را امن بسازید!

www.shabakeh-mag.com

فهرست

تو ویژه هستی...

یک واقعه ویژه نیز انتظار تو را می‌کشد...

۱۵ بهمن ساعت ۸ صبح بیا به

www.shabakeh-mag.com

آیا Windows Defender کافی است؟

بهترین ضدویروس برای ویندوز ۱۰ چیست؟

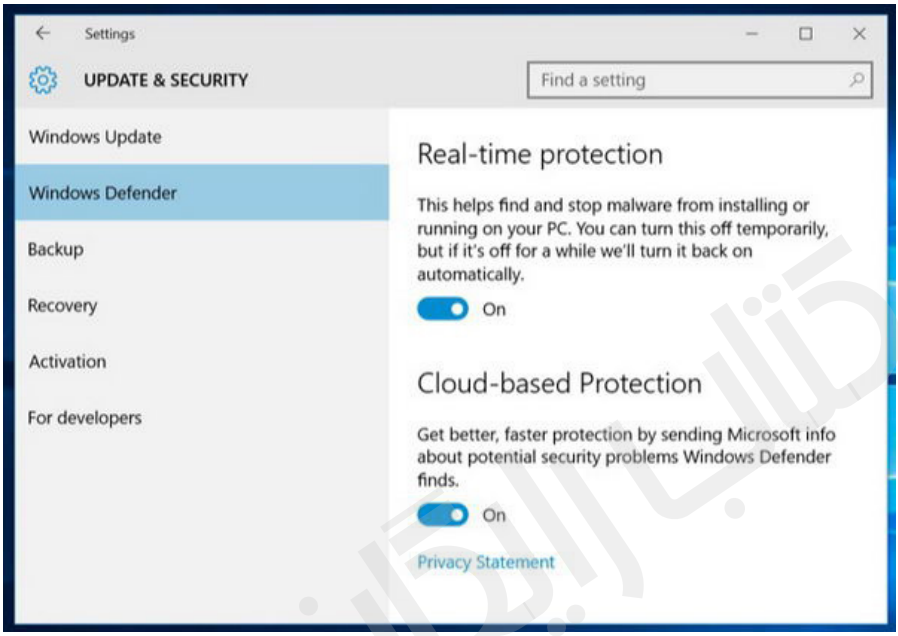
ویندوز ۱۰ مثل ویندوز ۷ شما را برای نصب یک ضدویروس به دردسر نمی‌اندازد. از ویندوز ۸ به بعد، ویندوز یک ضدویروس داخلی با نام Windows Defender درون خود دارد. اما آیا این بهترین راهکار برای حفاظت از کامپیوتر است؟به اندازه کافی خوب عمل می‌کند؟ Windows Defender آخرین نسخه Microsoft Security Essentials، یک برنامه 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.

آیا Windows Defender کافی است؟

این ضدویروس به صورت پیش‌فرض روی ویندوز اجرا می‌شود. Windows Defender به صورت خودکار برنامه‌هایی که باز می‌کنید را اسکن کرده و آخرین به‌روزرسانی‌ها برای شناسایی ویروس‌های جدید را از Windows Update دانلود می‌کند و رابط کاربری‌ای در اختیار شما می‌گذارد که می‌تواند پیچیده‌ترین اسکن‌ها را انجام دهید.

اما این ضدویروس چقدر خوب عمل می‌کند؟ خب، اگر بخواهیم راستش را بگوییم، ضدویروس مایکروسافت وقتی پای تست‌های نرم‌افزاری قیاسی به میان می‌آید، از ضدویروس‌های دیگر کمی عقب‌تر است. پیش‌تر 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 پیام‌های پیاپی آزار نمی‌دهد و درخواست پول نمی‌کند و از رقبای خود سبک‌تر است. این ضدویروس داده‌های وب‌گردی شما را جمع‌آوری نمی‌کند و از آن‌ها پول در نمی‌آورد. چنان که بعضی برنامه‌های ضدویروس رایگان شروع به این کار کرده‌اند تا از این راه سودی بدست آورند.



به طور کلی Windows Defender حفاظت بدی را در اختیار شما نمی‌گذارد. البته با فرض این‌که 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.

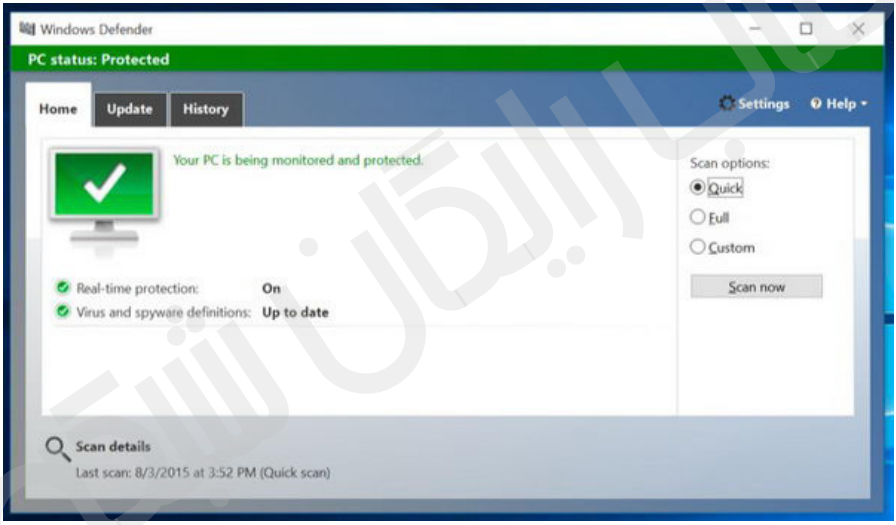
علی‌رغم امتیازات پایینی که Windows Defender از AV-Test گرفته

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 ازمایشی 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 هرحال 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. مثلا 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

پیش‌گیرانه امنیتی، احتمالا 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

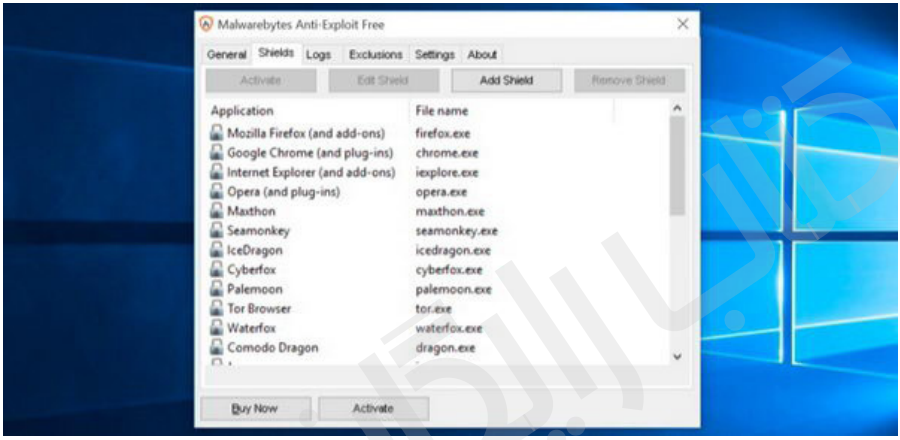
ما همچنین پیشنهاد می‌کنیم که از یک برنامه ضد سو استفاده برای حفاظت از مرورگر وب و افزونه‌ها استفاده کنید؛ چرا که این‌ها بیشتر هدف مهاجمین قرار می‌گیرند. نرم‌افزار ضد سو استفاده MalwareBytes برنامه پیشنهادی ماست. عملکرد آن مشابه

ابـزار امنیتـی EMET خـود مایکروسـافت اسـت. امـا رابـط کاربـری کاربرپسـندتری دارد و قابلیت‌هـای امنیتـی بیشـتری ارائـه می‌کنـد. ایـن برنامـه کمـک می‌کنـد تـا تکنیک‌هـای سـو اسـتفاده‌گری معمـول را سـد کنیـد، حتـی اگـر حمـلات روز صفـری باشـند کـه تـا حـالا مشـاهده نشـده‌اند. نرم‌افـزار ضـد سواسـتفاده MalwareBytes، بـرای مثـال تمـام آن حمـلات روز صفـر فلشـی کـه اخیـرا در مـورد آن‌هـا شـنیده‌اید را سـد می‌کنـد. ایـن نرم‌افـزار، مرورگـر، افزونه‌هـا و دیگـر اهدافـی کـه محاجمـان مـورد هـدف قـرار می‌دهنـد را مسـتحکم می‌کنـد و از شـما در مقابـل تکنیک‌هـای شـایع حمـلات حفاظـت می‌کنـد.

Windows Defender در کنـار نرم‌افـزار ضد سـو اسـتفاده MalwareBytes یـک ترکیـب خـوب، رایـگان و بـدون دردسـر از برنامه‌هـای امنیتی اسـت کـه مـا آن را بـرای امـن نگـه داشـتن کامپیوترهـای عـادی ویندوز ۱۰ توصیـه می‌کنیـم. کامپیوترهـای شـخصی بـا ویندوز ۱۰ Enterprise اغلـب Windows Defender و Microsoft EMET را بـه طـور همزمـان اجـرا می‌کننـد امـا Windows Defender و MalwareBytes بـرای یـک کامپیوتـر معمولـی خانگـی ترکیـب بهتـری اسـت.

(خـود MalwareBytes یـک برنامـه قـوی ضدبدافـزار اسـت کـه بـه عنـوان مکمـل هـر برنامـه ضدویروسـی، از جملـه Windows Defender، به خوبی عمـل می‌کنـد. ایـن نرم‌افـزار قابلیـت پیـدا کـردن برنامه‌هـای بالقـوه

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

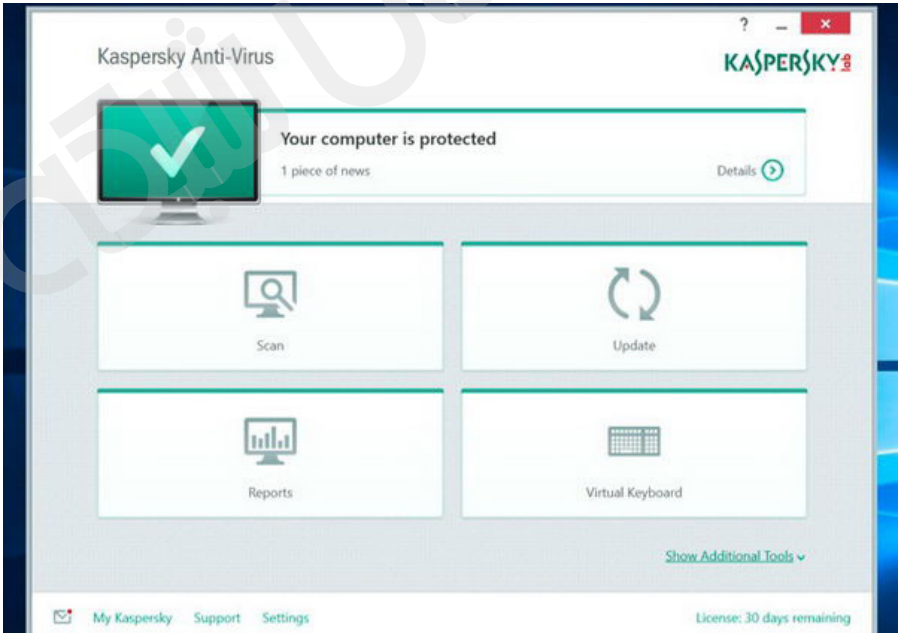


اما بهترین ضدویروس کدام است؟

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

اگر به دنبال یک راهکار رایگان هستید، Windows Defender انصافا خوب کار می‌کند. اما اگر چیز دیگری می‌خواهید، حتما از نصب هر نوار ابزار و افزونه مرورگری که ضدویروس می‌خواهد نصب کند اجتناب کنید. شرکت‌های ارائه کننده 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 مجددا خود را فعال می‌کند. این برنامه طوری طراحی شده که سر راه قرار نگیرد.

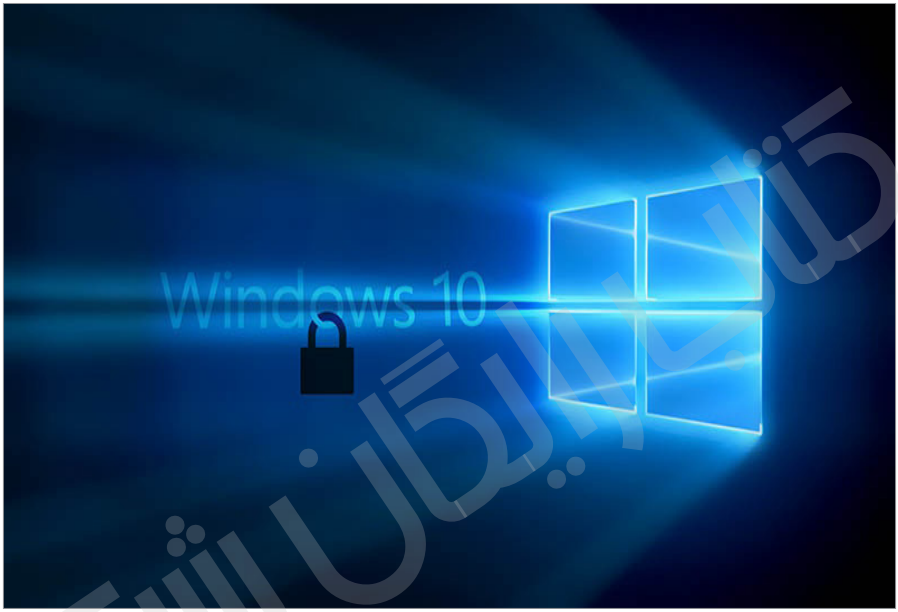


هر ضدویروسی که انتخاب کنید از کامپیوتر شما به طور کامل محافظت نمی‌کند. اگر برنامه‌های مضر را دانلود و نصب می‌کنید، دیر یا زود به دردسر خواهید افتاد. انتخاب یک ضدویروس که امتیازات بهتری در برابر بدافزارهایی که شاید هرگز با آنها روبرو نشوید کسب کرده است، شاید به امن‌تر بودن شما کمک کند، اما انجام پیش‌گیری‌های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

اسرار ویندوز ۱۰

ده ویژگی برتر و پنهان ویندوز ۱۰



هر زمان سیستم‌عامل جدیدی از خانواده ویندوز عرضه می‌شود، از خود می‌پرسم آیا ویندوزم از من در برابر حملات محافظت می‌کند یا همچون گذشته من باید از ویندوزم در برابر مخاطرات امنیتی محافظت کنم. به‌نظر می‌رسد 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 سیستم‌عامل امن به کار بسته‌اند.»

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

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 به‌کارگیری Windows Hello راحت‌تر از تایپ گذرواژه است، بلکه امن‌تر هم به‌نظر 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

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).

شکل ۱: کپی برابر اصل نیست!

دوربین‌هایی که از فناوری مادون قرمز برای شناسایی چهره یا عنبیه استفاده می‌کنند، می‌توانند شما را در یک وضعیت نوردهی 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 به‌منظور 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 به‌آسانی هک می‌شوند و حتی زمانی که پیچیده می‌شوند نیز مؤثر نخواهند بود. بیش‌تر ما به گذرواژه ساده‌ای نیاز داریم که

به‌سادگی 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 ۱,۲میلیارد 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 اشتراک‌گذاری 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

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 مایکروسافت 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 آن‌که 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. همان گونه 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 به‌نظر می‌رسد،

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

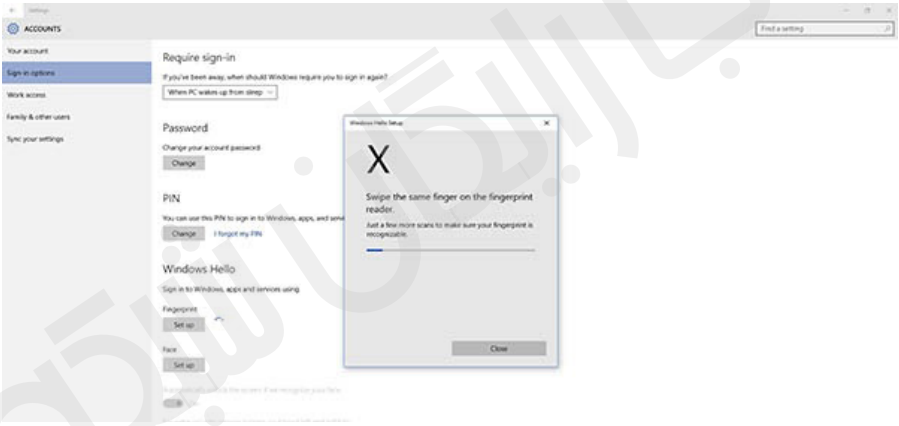
قیمت ۱۱ دلار که در سایت آمازون به فروش می‌رسد و همراه با دو کابل یواس‌بی عرضه می‌شود، می‌توان این کار را انجام داد (شکل ۲).

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

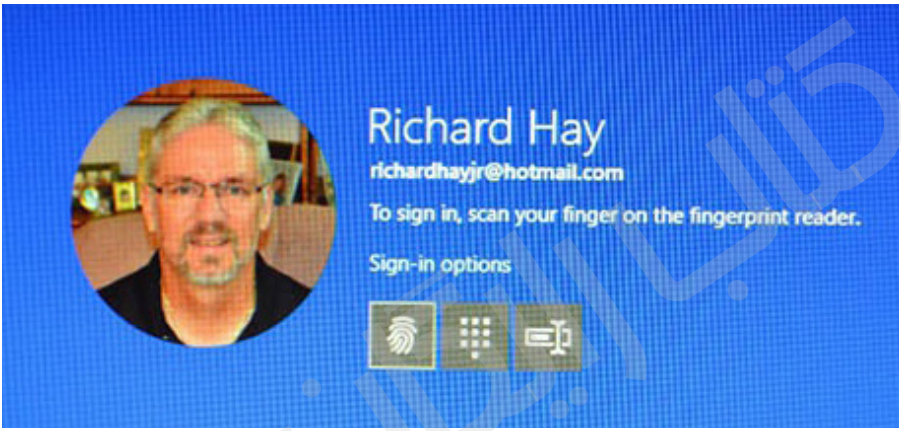
برای دریافت اثر انگشت مورد استفاده قرار می‌گیرد (شکل ۳). این دستگاه به‌خوبی با ویندوز ۱۰ کار کرده است و برای آن‌که بتوان از آن استفاده کرد، به نصب هیچ درایوری نیاز نیست. زمانی که اسکنر به سیستم متصل شد، با مراجعه به تنظیمات قرار گرفته در نشانی Settings-> Accounts-> Sign-in و پیدا کردن گزینه Windows Hello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



شکل ۴: فرآیند تنظیمWindows Hello

با کلیک روی گزینه تنظیم اثر انگشت فرآیند تنظیم آغاز می‌شود و از شما برای ورود با PIN/Password سؤال می‌کند. به محض این‌که 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

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 به‌کارگیری 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 به‌آسانی 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

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 آن‌که اجرا شود، توسط یک منبع قابل اعتماد امضا نشده است. به عبارت دیگر، نفوذ قبل از آن‌که 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 آن‌که کامپیوتر راه‌اندازی شود، کم‌ترین شانس را برای اجرای کدهای مخرب اجرایی خواهد داشت. همچنین، این‌که چطور

درباره آن‌چه می‌تواند اجرا کند یا اجرا خواهد کرد تصمیم‌گیری می‌کند؟ Device Guard از یک مکانیسم امنیت مجازی‌سازمحور، برای جدا کردن سرویس کد یک‌پارچه از کرنل ویندوز ۱۰ استفاده می‌کند. Device Guard به سرویس کد یک‌پارچه 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 این‌که 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 هشداری 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 پردازه‌ای را که قرار است

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.

- **Windows10**: Device Guard فقط با دستگاه‌هایی کار می‌کند که ویندوز ۱۰ را اجرا می‌کنند.
- **UEFI**: نسل جدید میان‌افزارها یا UEFI شامل یک ویژگی امنیتی به‌نام راه‌اندازی امن Secure Boot هستند که از یک‌پارچگی 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 سیستم‌عامل است که بر ویژگی راه‌اندازی ایمن UEFI برای جلوگیری از اجرای برنامه‌های مخربی که در مدت زمان بارگذاری سیستم‌عامل 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

دست‌کاری کنند.

اگر دستگاه شما به یک حس‌گر 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، دست‌کاری 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 به‌آسانی 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.

۳ . Enterprise Data Protection (محافظت 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 آن‌که اجرا شود، توسط یک منبع قابل اعتماد امضا نشده است.

۴ . Microsoft Passport

در ویندوز ۱۰، Microsoft Passport جایگزین گذرواژه‌ها شده است.

Microsoft Passport به کاربران اجازه می‌دهد احراز هویت را با یک حساب مایکروسافتی، یک حساب اکتیودایرکتوری (Active Directory)، یک حساب (Microsoft Azure Active Directory AD) یا حتی سرویس غیر مایکروسافتی که از احراز هویت (Fast ID Online (FIDO پشتیبانی می‌کند، انجام دهند. بعد از آن‌که 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 بپردازید. بسته‌های تأمینی (Provisioning Package) شامل مجموعه مختصری از دستورالعمل‌ها است و به‌کارگیری 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

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

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.

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

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 اشتراک‌گذاری 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 windir%/Fonts% 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.

Exclude apps to load untrusted fonts: فعال بودن این گزینه باعث می‌شود تا برنامه‌های خاصی را به‌صورت 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 QWORD (64-bit) اضافه کنید. دقت کنید نام آن را MitigationOptions قرار دهید.

۳. از کلید MitigationOptions مقدار Value Date را به‌روزرسانی 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

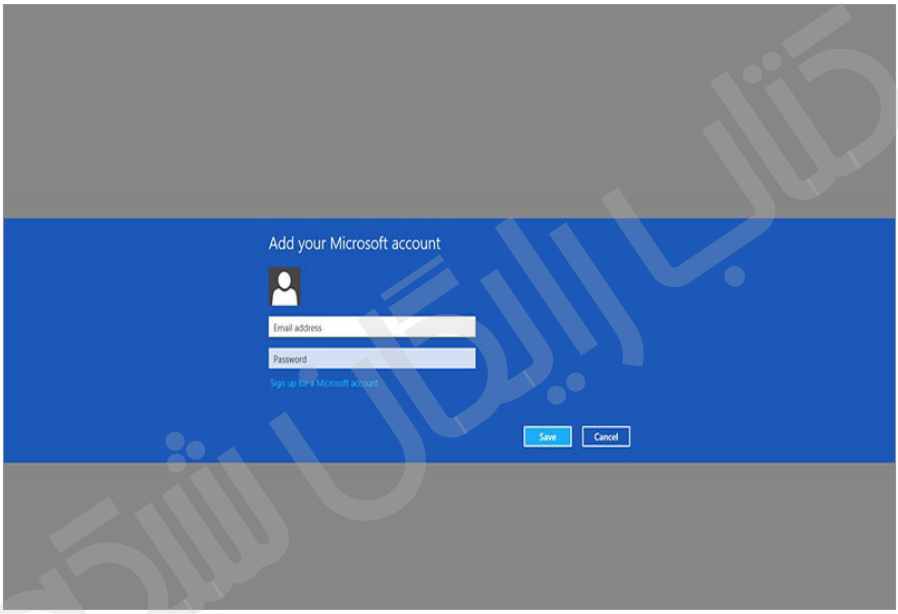
نکته مهم: مقداری که در MitigationOptions وجود دارد، باید در مدت زمان به‌روزرسانی ذخیره شود. به‌طور مثال، اگر مقدار

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

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

حذف کامل حساب کاربری مایکروسافت

آموزش راهکاری برای فرار از جاسوسی مایکروسافت در ویندوز ۱۰



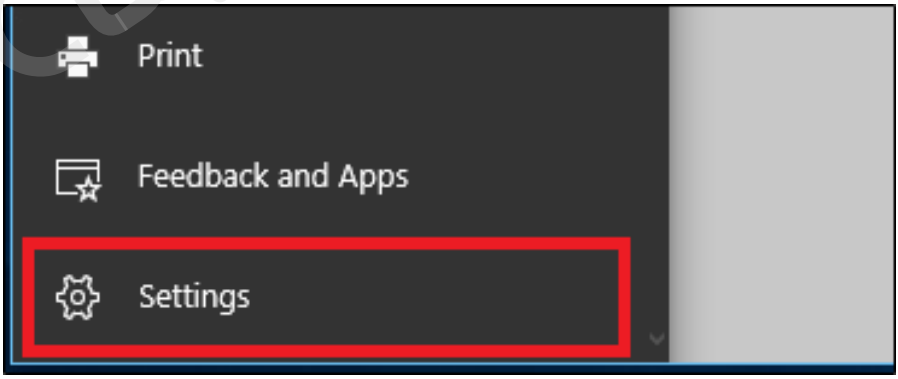
اگر شما هم نگاهی به سرتیتر اخباری که نشان می‌دهد مایکروسافت چگونه در همه حال مراقب شما است انداخته باشید، تعجب خواهید کرد که چگونه ویندوز ۱۰ به یک موفقیت جهانی تبدیل شده است. تا به حال بیش از ۷۲ میلیون نسخه از آخرین سیستم‌عامل این غول دنیای نرم‌افزار روی سیستم‌های سراسر جهان نصب شده است و در بیشتر موارد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

همچـون بسـیاری از مـوارد نقـض حریـم خصوصـی، منـوی اسـتارت آزاردهنـده و تعـداد زیـاد نرم‌افزارهـای جعلـی در ویـنـدوز ۱۰ را چگونـه می‌تـوان تحمـل کـرد؟

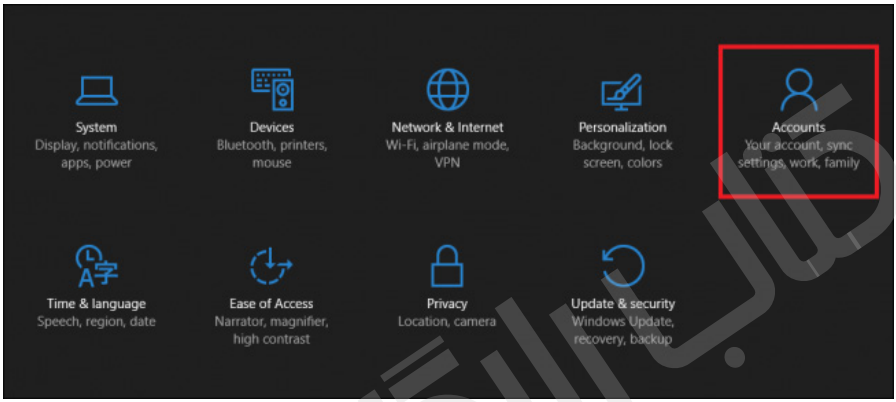
یکـی از بهتریـن روش‌هـا بـرای اطمینـان از اینکـه هیـچ کـدام از داده‌هـای شـما بـدون رضایـت شـما توسـط ایـن شـرکت اسـتفاده نخواهـد شـد، حـذف حسـاب کاربـری مایکروسـافت شـما اسـت. بـا ایـن کار شـما خود را از بانـک اطلاعاتـی ویـنـدوز نیـز حـذف خواهیـد کـرد، بنابرایـن منابـع ثالـث تاییـد نشـده دیگـر نیـز نمی‌تواننـد هیـچ اطلاعاتـی را بـدون اجـازه شـما جمـع‌آوری کننـد.

حذف حساب کاربری به صورت محلی

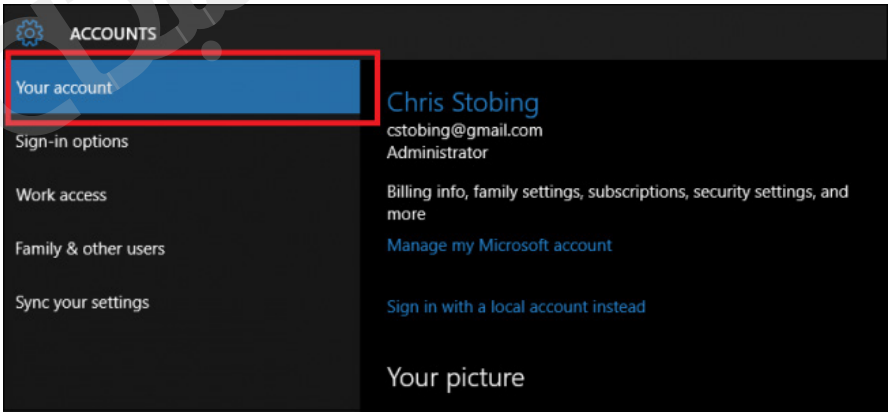
اولیـن مرحلـه از انجـام ایـن فرآیند حـذف حسـاب کاربری مایکروسـافت از روی کامپیوتـر محلی شـما اسـت.



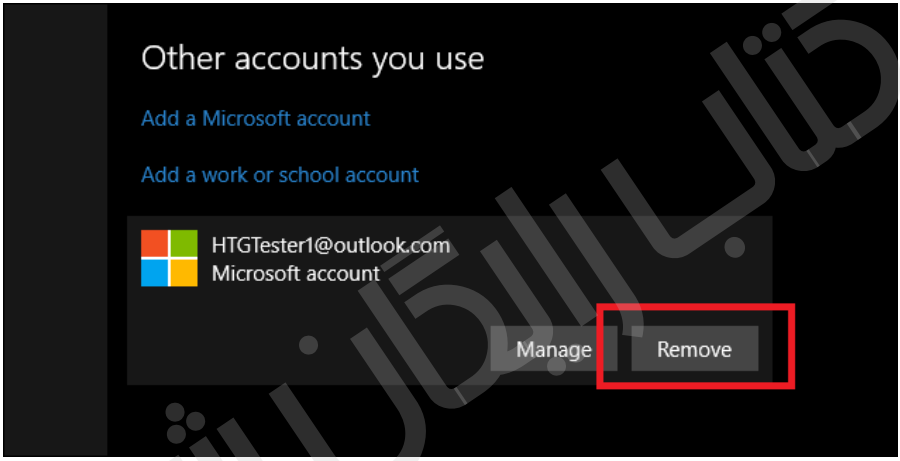
برای انجام این کار، به بخش Settings رفته و روی قسمت Accounts کلیک کنید.



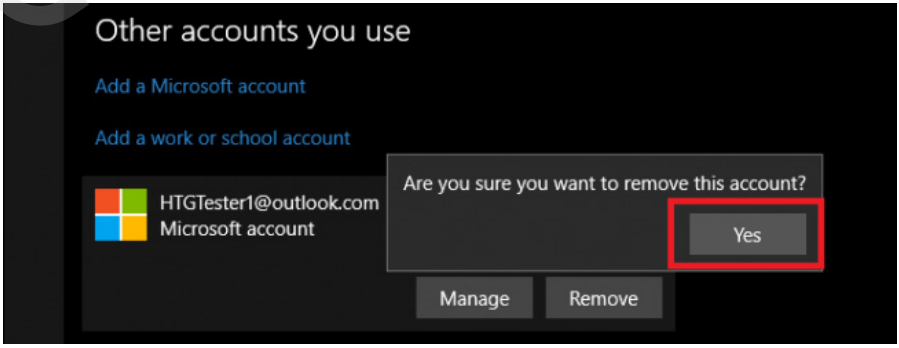
همان گونه که در تصویر زیر مشخص شده است، با ورود به این قسمت شما می‌توانید گزینه حذف حساب کاربری مایکروسافت را در قسمت انتهای تب Your account پیدا کنید.



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

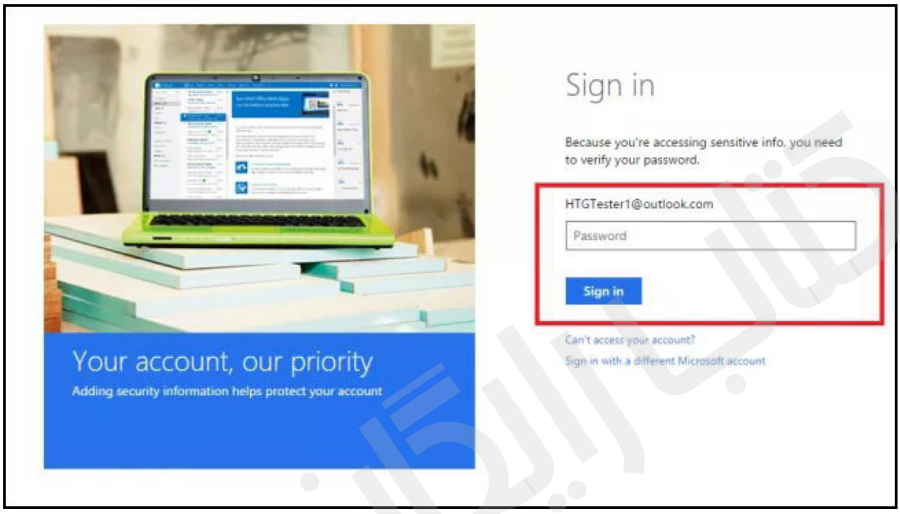
حتی بعد از پاک کردن حساب کاربری مایکروسافت شما از روی کامپیوتر محلی، تمام داده‌ها و اطلاعات شخصی موجود در آن همچنان روی سرورهای اختصاصی مایکروسافت نگهداری می‌شود. برای خلاص شدن از یک حساب کاربری به طور کامل، شما باید از ابزار موجود در وب‌سایت مایکروسافت استفاده کنید.

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.

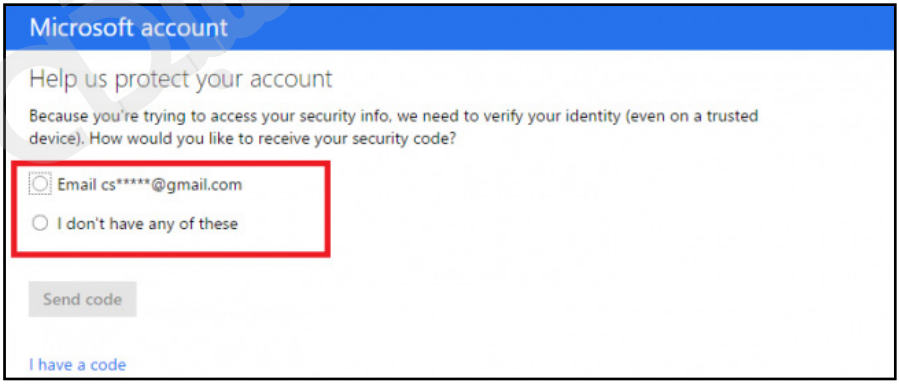
بعد از انجام تمام این اقدامات احتیاطی، از طریق این لینک به وب‌سایت مایکروسافت بروید. بعد از لود شدن کامل صفحه، از شما خواسته می‌شود که وارد حساب کاربری خود شوید. بعد از ورود

بایـد بخـش Close your account را پیـدا کنیـد.

بعـد از انجـام ایـن مراحـل، شـما بـه صفحه زیـر هدایـت خواهید شـد، در

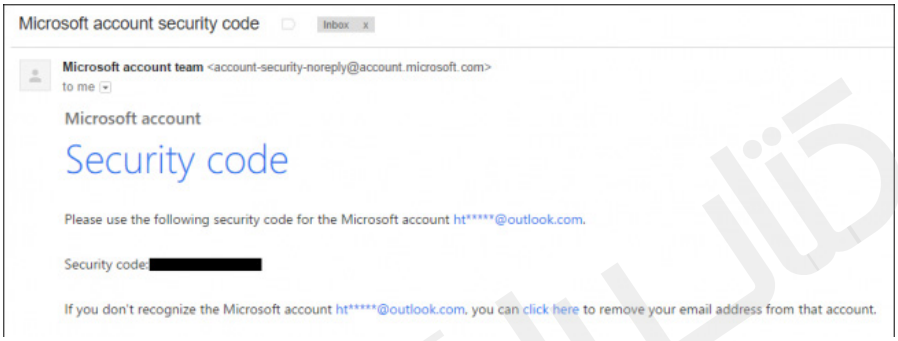


اینجـا بـرای تعییـن هویـت واقعـی شـما بایـد مرحلـه وارد کـردن آدرس ایمیـل پشـتیبان یـا شـماره تلفـن خـود را پشـت سـر بگذارید.

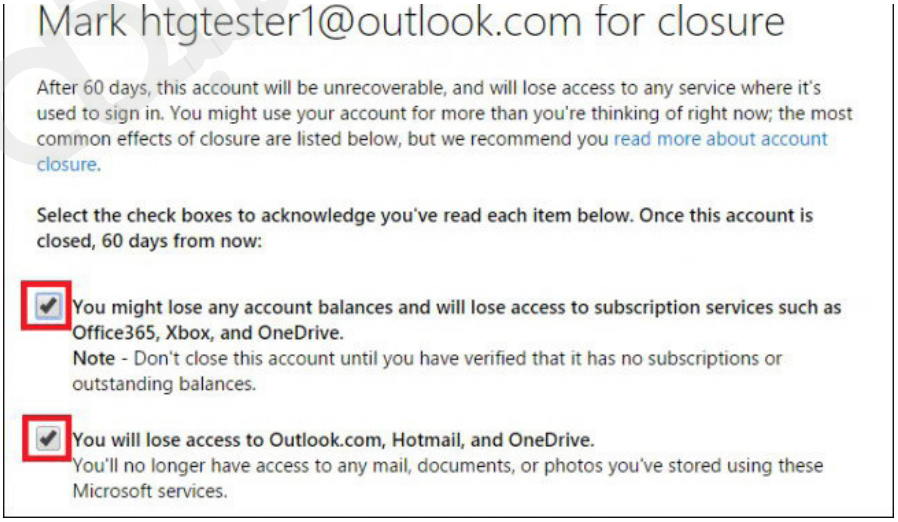


بعـد از پشـت سـر گذاشـتن ایـن مرحلـه، یـک کـد بـه ایمیـل شـما یـا

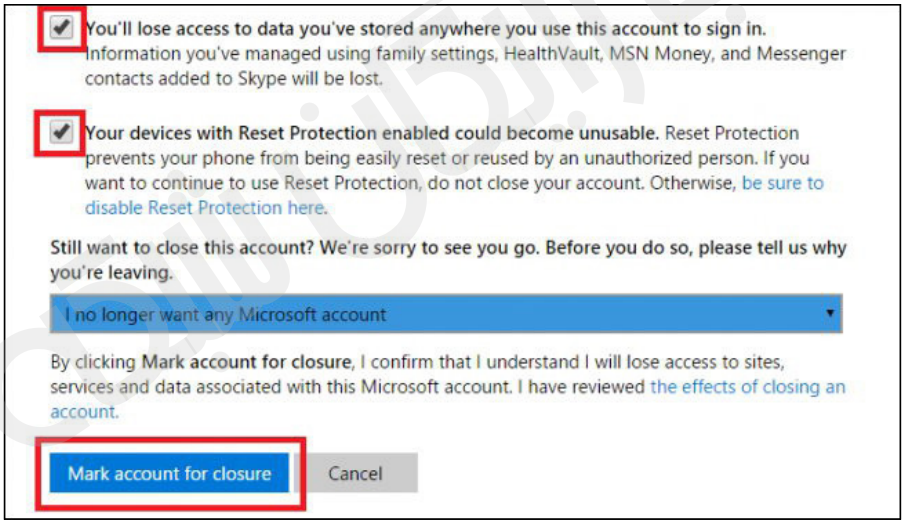
به صورت پیامک برای شما ارسال خواهد شد (چیزی شبیه به تصویر زیر)



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

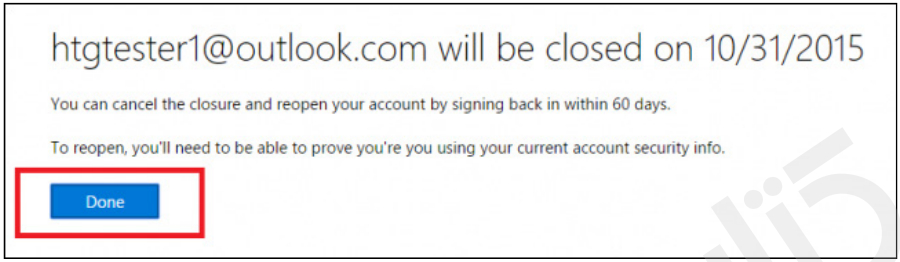


آنها شما را با حقایق آشکاری نظیر اینکه شما دیگر قادر به وارد شدن به این حساب کاربری نخواهید بود، اینکه اکس باکس شما دیگر آن گونه که شما انتظار دارید کار نخواهد کرد، و اینکه دسترسی به ایمیل شما هم در Outlook و هم Hotmail مسدود خواهد شد، به ستوه خواهند آورد. هر کسی که قبلا تجربه قطع عضویت در Xbox Live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



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

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.

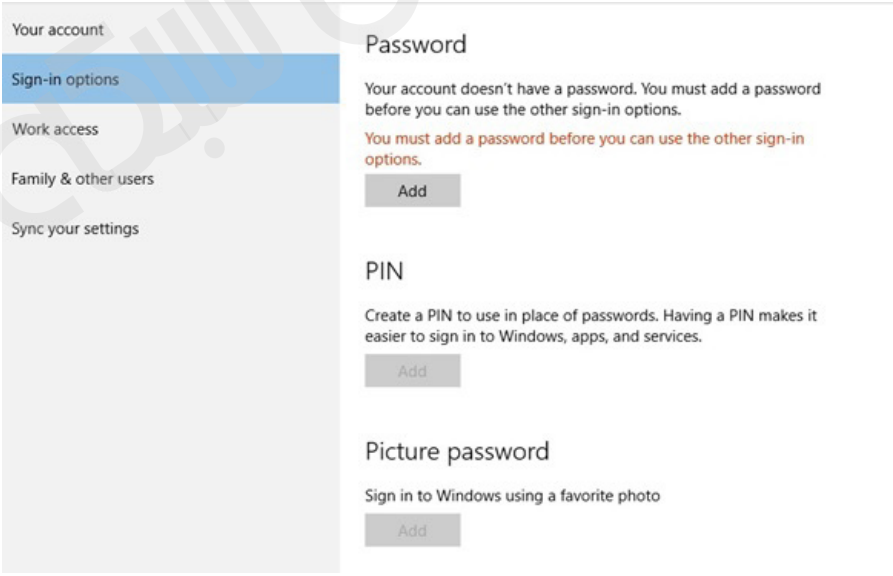
از زمان انتشار ویندوز ۱۰، هر روز کاربران بیشتری متوجه این موضوع می‌شوند که داشتن یک حساب کاربری آنلاین ساده از مایکروسافت می‌تواند چه مسائل امنیتی را برای آنها به وجود آورد. مشکلاتی که شما هرگز تصور آن را هم نمی‌کردید. اگر شما هم ترجیح می‌دهید اطلاعات خود را از دسترس این غول دنیای نرم افزار محفوظ نگه 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.

چگونه یک صفحه قفل لاگین ویندوز ۱۰ ایجاد کنیم؟

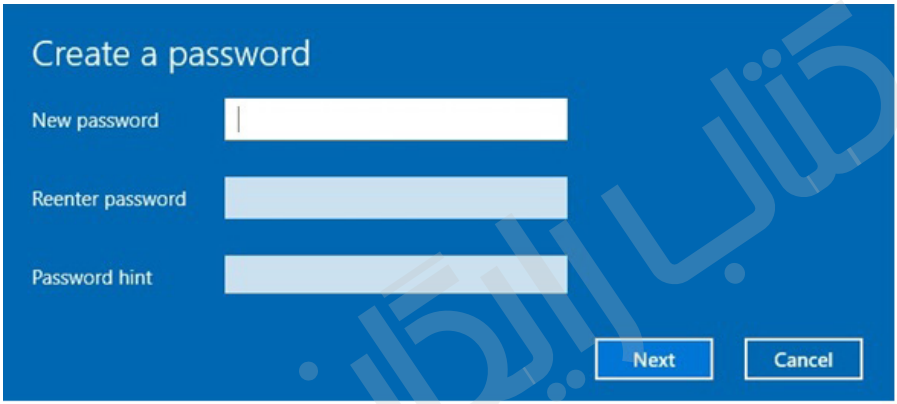
ویندوز ۱۰ در بخش‌های مختلفی دست‌خوش تغییرات اساسی گشت. از جمله بخش‌هایی که تغییرات چشم‌گیری را به خود دیده است، صفحه قفل لاگین ویندوز ۱۰ است. رویکردی که مایکروسافت در ارتباط با صفحه قفل در پیش گرفته است بی‌ارتباط با حالتی که در دستگاه‌های تلفن‌همراه آن‌را مشاهده کرده‌ایم؛ نیست. این ویژگی اکنون به کامپیوترهای 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.

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

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 مکانیزیم با تلفیق اعداد و کاراکترها دسترسی به دسکتاپ سیستم امکان‌پذیر می‌شود. پیکربندی این گزینه پیچیدگی خاصی نداشته و همچون گذشته (سیستم‌عامل ویندوز ۸٫۱) می‌تواند مورد استفاده قرار گیرد. برای آن‌که 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:

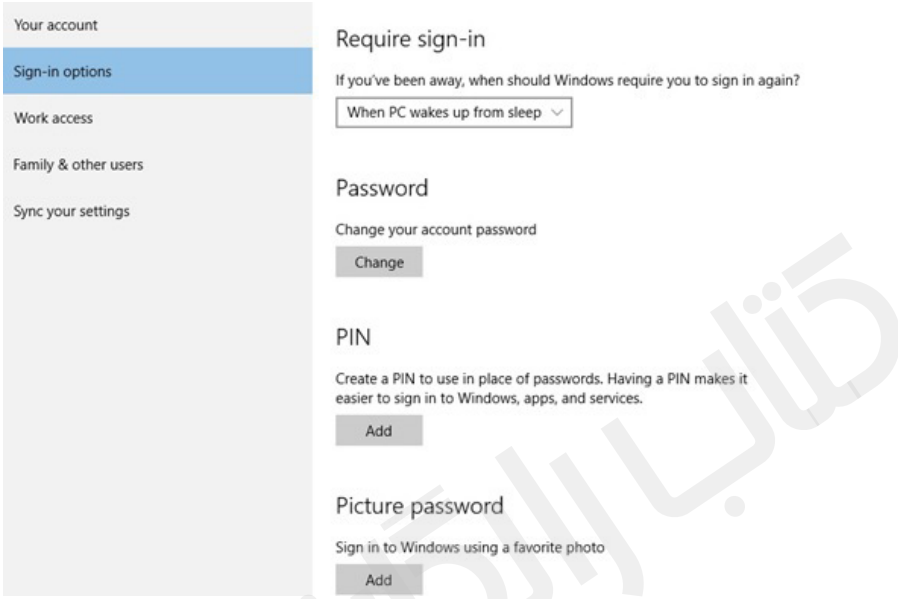


همان‌گونه که در تصویر مشاهده می‌کنید، هنوز هیچ گذرواژه‌ای تعیین نشده است، برای آن‌که به دیگر گزینه‌های موجود در این قسمت دسترسی پیدا کنید، ابتدا باید گذرواژه‌ای را مشخص کنید. با کلیک روی دکمه Add پنجره ساخت گذرواژه ظاهر می‌شود.

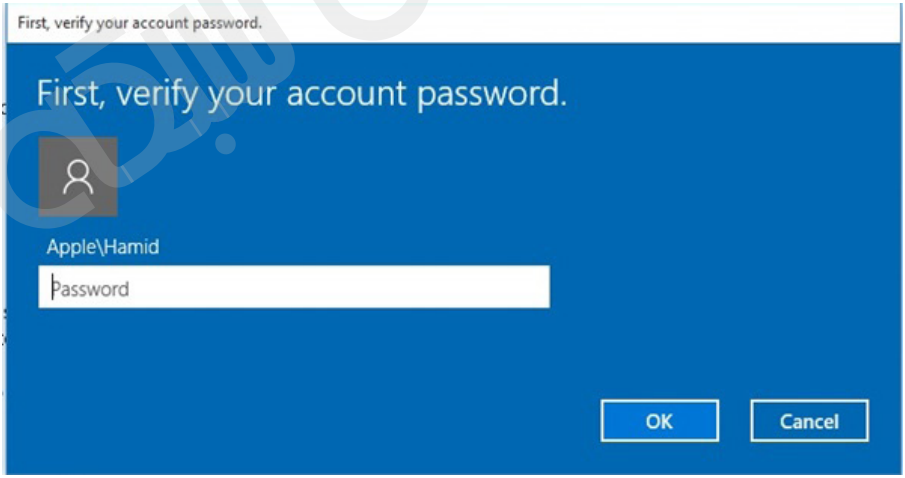


در پنجره ظاهر شده باید گذرواژه را در فیلدهای مربوطه وارد کنید. بعد از وارد کردن گذرواژه خود روی دکه Next کلیک کنید.

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

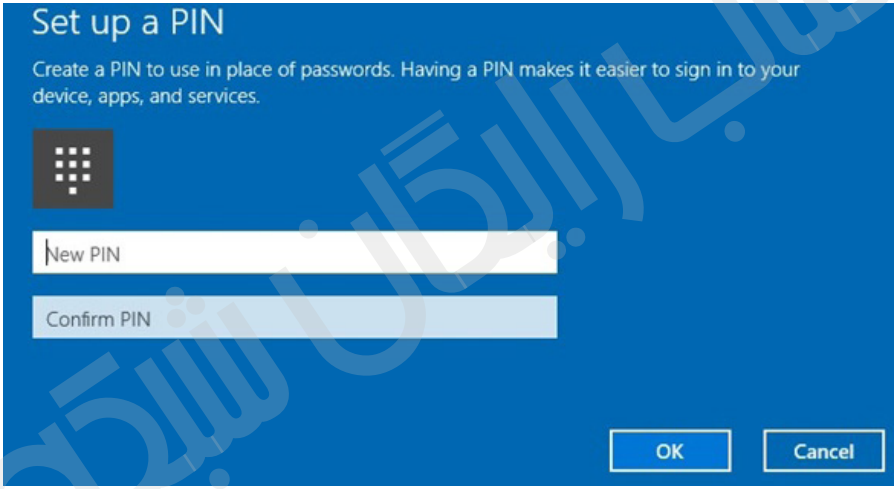


همان‌گونه که در تصویر مشاهده می‌کنید، اکنون گزینه‌هایی که غیر فعال بودند اکنون در دسترس قرار دارند.

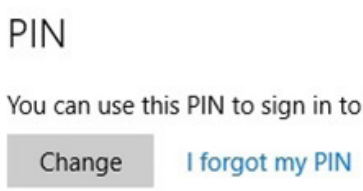


گزینه دیگری که در این قسمت قرار دارد در ارتباط با PIN است.

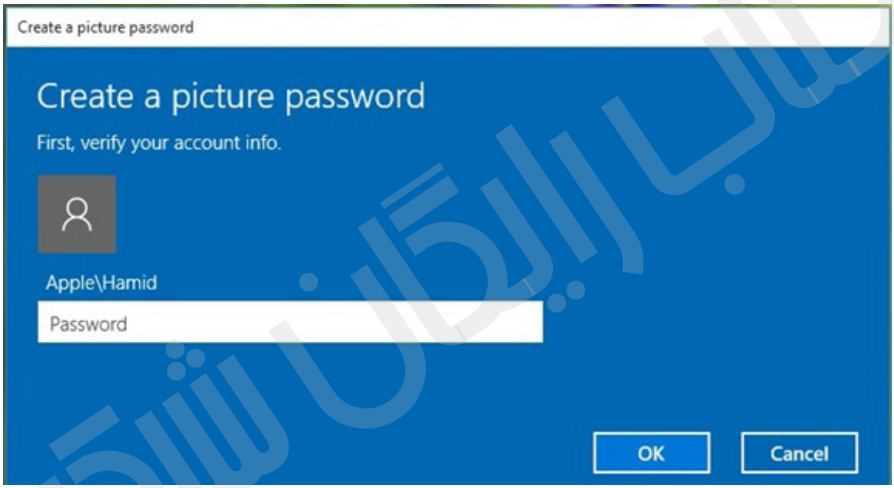
این گزینه به شما اجازه می‌دهد تا روی ماشین خود به آسانی به حساب ویندوز همچون برنامه‌ها و سرویس‌هایی که مورد استفاده قرار می‌دهید، دسترسی داشته باشید. زمانی‌که روی گزینه PIN کلیک کنید، پنجره‌ای همانند تصویر فوق ظاهر می‌شود. در این پنجره ابتدا باید گذرواژه‌ای که آن‌را در قسمت قبل وارد کرده‌اید را تایپ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



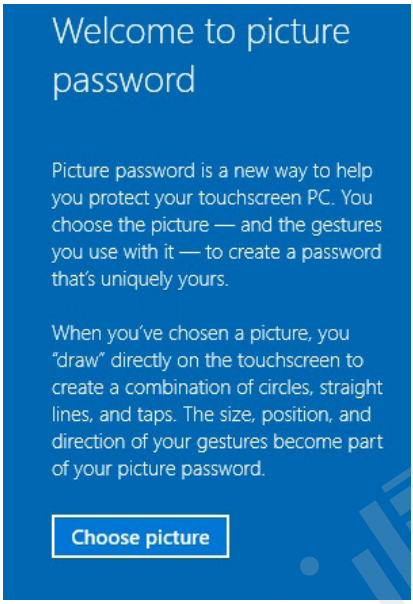
در پنجره ظاهر شده باید پین کدی را وارد کنید که در مکان گذرواژه ظاهر می‌شود. مزیت به کارگیری پین‌کد در این است که می‌توانید به راحتی به برنامه‌ها، دستگاه‌ها و سرویس‌ها وارد شوید. بعد از وارد کردن پین‌کد روی دکمه Ok کلیک کنید. پین‌کد وارد شده حداقل باید دارای چهار کاراکتر باشد.



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

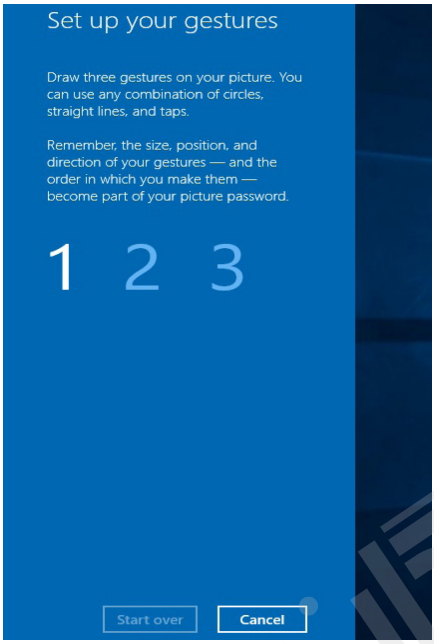


سومین روشی که می‌توانید از آن استفاده کنید، قفل تصویری است. امروزه بیشتر کاربران با مکانیزمی که توسط این روش مورد استفاده قرار می‌گیرد آشنایی دارند. برای به کارگیری این روش نیازمند یک تصویر هستید. زمانی‌که روی دکمه Add در بخش Password کلیک می‌کنید، ابتدا پنجره‌ای ظاهر می‌شود که در آن باید گذرواژه وارد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



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.

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.



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

تو ویژه هستی...

یک واقعه ویژه نیز انتظار تو را می‌کشد...

۱۵ بهمن ساعت ۸ صبح بیا به

www.shabakeh-mag.com

کتاب‌های الکترونیک منتشر شده ماهنامه شبکه