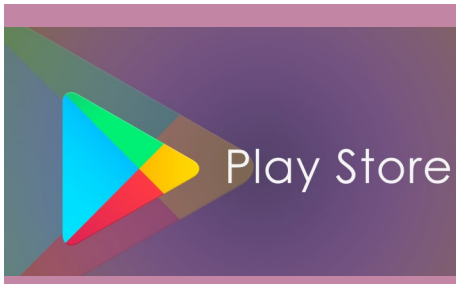
شماره بیست و دوم - آبان ۱۳۹۷

خبرنامه "آپا" دانشگاه خوارزمی

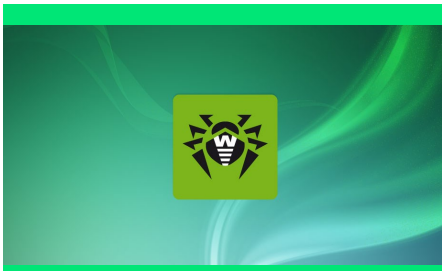
KHARAZMI CERT
COORDINATION CENTER
مرکز تخصصی آپا خوارزمی

در این شماره خواهید خواند:



گوگل ۱۳ بدافزار را از Play Store حذف کرد!

در این هفته‌ی گذشته گوگل مجبور به حذف ۱۳ بدافزار از روی فروشگاه نرم افزاری خود شد. این شرکت بارها این عمل را در گذشته در جهت افزایش بهبود امنیت کاربران انجام داده است. - صفحه ۲



بدافزار جدید لینوکس!

بدافزار جدیدی اخیرا در سیستم عامل لینوکس کشف گردیده است که به استخراج ارز دیجیتال با استفاده از منابع قربانیان می‌پردازد. این بدافزار که در سیستم عامل لینوکس فعال است توسط شرکت Dr.Web کشف شده است. - صفحه ۳

درخواست آمریکا برای عدم استفاده از محصولات هوآوی!

عدم تایید شرکت هوآوی توسط دولت آمریکا بر کسی پوشیده نیست. استفاده از وسایل و دستگاه‌های این شرکت چینی و همتای آن یعنی ZTE در آژانس‌های امریکایی ممنوع هستند اما اخبار جدید نشان دهنده‌ی آن هستند که مدیریت ترامپ قصد توقف کردن آنان را همچنان ندارد. صفحه ۴

خطای آمازون و نشت اطلاعات کاربران!

جمعه سیاه و دوشنبه‌ی مجازی از روزهایی هستند که عموم فروشگاه‌های اینترنتی خدمات ویژه و تخفیفات بالایی را به کاربران و خریداران خود اختصاص می‌دهند. سایت آمازون هم یکی از این فروشگاه‌ها بوده که سود بالایی از این طریق کسب می‌نماید. اما وجود یک نقص امنیتی می‌تواند زمینه را برای رغیبان گسترده و لطمه‌ی بزرگی را به این فروشگاه وارد نماید. - صفحه ۵

فیشینگ با HTTPS

بسیاری از افراد غیر متخصص احساس می‌کنند که در صورت استفاده‌ی یک سایت از SSL، آن سایت قانونی و امن می‌باشد. در صورتی که به هیچ عنوان چنین چیزی نیست. براساس تحقیقاتی که به تازگی در سه ماه سوم سال ۲۰۱۸ انجام شده است ۴۹ درصد سایت‌های فیشینگ از لایه‌ی امن ویا SSL استفاده می‌کنند - صفحه ۶

بهترین آنتی ویروس‌های سال ۲۰۱۸

استفاده از آنتی ویروس برای جلوگیری از آلوده شدن به ویروس و بدافزار یکی از مرسوم‌ترین کارهایی است که کاربران انجام می‌دهند. اما سوالی که ذهن اغلب کاربران را به خود درگیر می‌کند این است که کدام آنتی ویروس از بین تمامی آنتی ویروس‌های تولید شده که کم هم نیستند می‌تواند بهترین محافظت را از آنان در مقابل بد افزارها و تهدیدات انجام دهد. - صفحه ۷

گوگل ۱۳ بدافزار را از Play Store حذف کرد!

در این هفته‌ی گذشته گوگل مجبور به حذف ۱۳ بدافزار از روی فروشگاه نرم افزاری خود شد. این شرکت بارها این عمل را در گذشته در جهت افزایش بهبود امنیت کاربران انجام داده است.

با توجه به هشدارهای شرکت‌های امنیتی در رعایت نکات ایمنی، اما کاربران همچنان با بی‌توجهی به نصب اپلیکیشن‌هایی می‌پردازند که توسعه دهندگان آنان افرادی ناشناس هستند.

شرکت گوگل به تازگی ۱۳ بدافزار را که در مجموع بیش از ۵۶۰۰۰۰ بار دانلود شده بودند، از Play حذف نمود.

این اقدام توسط این قول نرم افزاری زمانی صورت پذیرفت که شرکت ESET این مسئله را چندین بار توییت نموده بود. بر اساس یافته های محقق امنیتی شرکت ESET، ۱۳ اپلیکیشن که بیش از ۵۶۰۰۰۰ بار از Play Store دانلود شده بودند و تمامی آنان توسط یک توسعه دهنده با نام Luiz O Pinto ایجاد گردیده بودند، بدافزارهایی بودند که موبایل کاربران را با مشکل رو به رو می کردند.

بر اساس یافته های این محقق امنیتی، این اپلیکیشن ها هیچ کار غیر قانونی انجام

نمیداند بلکه از کاربر می خواستند تا یک فایل APK اضافی به نام Game Center را دانلود و نصب نمایند. به محض دانلود این فایل، آیکون آن مخفی می گردید و در زمان هایی که قفل گوشی کاربر باز بوده، اقدام به نمایش تبلیغات می کند.

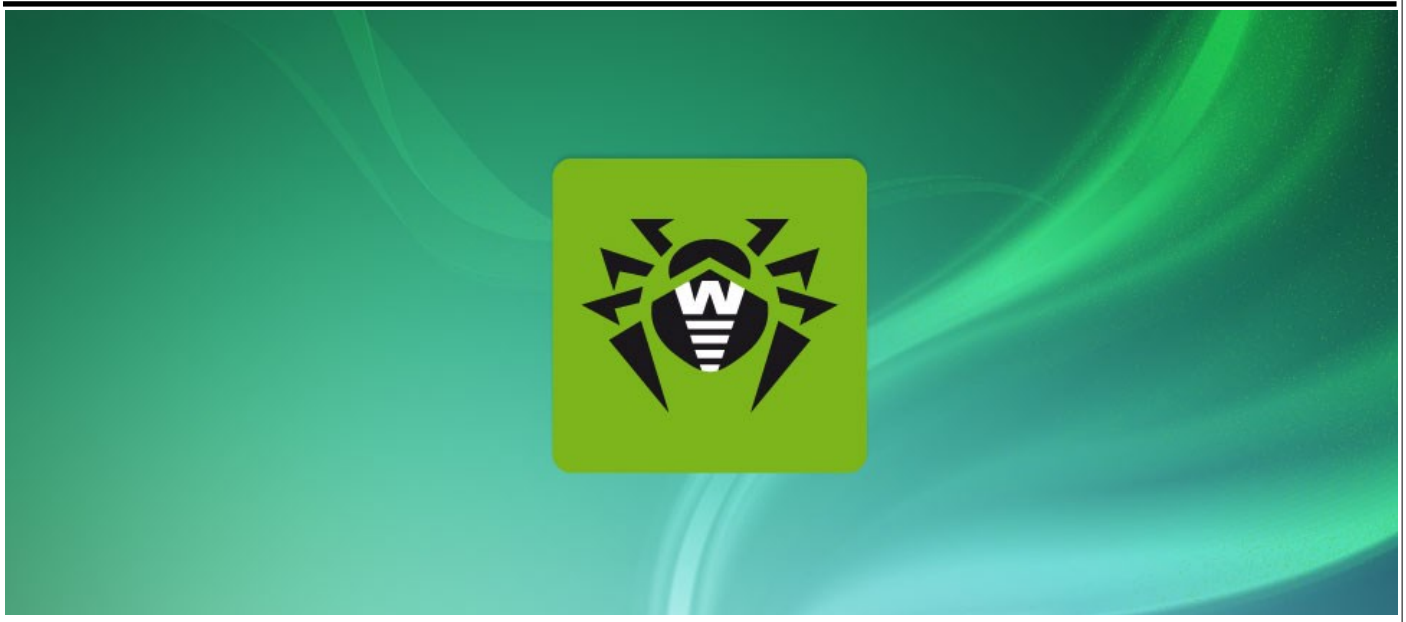
این محقق امنیتی بیان نمود که این فایل با نام Game Center، از کاربران مجوز دسترسی به Wi-Fi، Network و run at startup را اخذ می کند. وی همچنین چندین ویدیو از نحوه ی کار این بدافزار در اینترنت به اشتراک گذاشت. لذا برای جلوگیری از موارد این چنینی، از نصب برنامه های زیر خودداری کنید.

- Truck Cargo Simulator
- Car Driving Simulator
- Car Driving Simulator
- Extreme Car Driving
- Moto Cross Extreme

جالب اینجاست که برخی از این اپلیکیشن ها در play Store دارای امتیاز ۳ ستاره بودند. سال گذشته نیز ۴۱ اپلیکیشن از یک شرکت کره ای که با آلوده کردن موبایل های کاربران قصد ایجاد تبلیغات کلیکی تقلبی را داشت توسط گوگل حذف گردید.

گردآورنده: محمد مرتضوی

بدافزار جدید لینوکس!



بدافزار جدیدی اخیرا در سیستم عامل لینوکس کشف گردیده است که به استخراج ارز دیجیتال با استفاده از منابع قربانیان می‌پردازد.

این بدافزار که در سیستم عامل لینوکس فعال است توسط شرکت Dr.Web کشف شده است.

Linux.BtcMine.174 نامی است که به این بدافزار اختصاص داده شده است که اقدام به استخراج ارز دیجیتال Monero می‌کند.

بخشی از این بدافزار شامل بیش از ۱۰۰۰ خط کد برای مخفی کردن خود در سرویس های سیستمی، پنهان کردن فایل ها و سرقت پسوردها می باشد.

این بدافزار با در دست گرفتن مد root سعی می‌کند تا خود را وارد پوشه‌ای نماید که دسترسی نوشتن داشته باشد. سپس دسترسی خودرا افزایش می‌دهد و از اکسپلویت‌های مربوطه استفاده می‌نماید. سپس خود را به لیست autorun اضافه می‌نماید و اقدام به نصب rootkit می‌کند.

تمامی اینکارها را انجام می‌دهد تا قدرت سیستم را به دست گیرد. این بدافزار توانایی متوقف کردن سایر سرویس‌هایی را که اقدام به استخراج ارز دیجیتال می‌کنند را دارد.

Rootkit نصب شده نیز این امکان را می‌دهد تا بدافزار اقدام به سرقت پسوردهایی کند که کاربر آن را وارد نموده است.

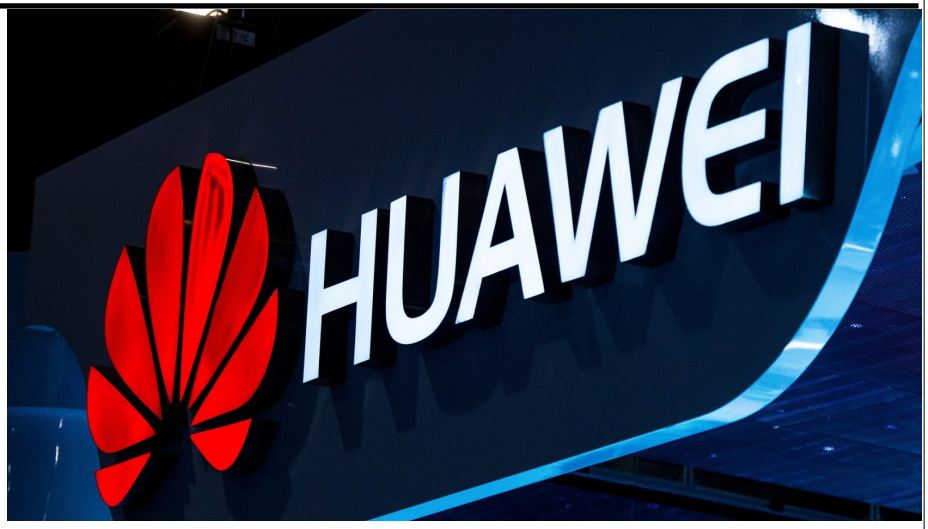
پس از انجام تمامی اقدامات فوق، این بدافزار سعی می‌کند تا کامپیوترهای دیگری را که به کامپیوتر قربانی متصل هستند را آلوده نماید. برای این کار سعی می‌نماید تا از طریق پورت SSH خود را گسترش دهد.

در حال حاضر برای کشف این بدافزار می توان از آنتی ویروس Dr.Web استفاده نمود.

به زودی سایر آنتی ویروس‌ها نیز قابلیت کشف و حذف این بدافزار را خواهند داشت.

گردآورنده: محمد مرتضوی

درخواست آمریکا برای عدم استفاده از محصولات هوآوی!



عدم تایید شرکت هوآوی توسط دولت آمریکا بر کسی پوشیده نیست. استفاده از وسایل و دستگاه‌های این شرکت چینی و همتای آن یعنی ZTE در آژانس‌های امریکایی ممنوع هستند اما اخبار جدید نشان دهنده‌ی آن هستند که مدیریت ترامپ قصد توقف کردن آنان را همچنان ندارد.

براساس گزارش Wall Street Journal، مقامات ایالات متحده به همتایان خود در کشورهایی که از از تجهیزات مخابراتی هوآوی به صورت گسترده استفاده می‌کنند به عنوان یک خطر سایبری بزرگ هشدار داده‌اند. این کشورها شامل آلمان، ایتالیا و ژاپن هستند که آمریکا در آنان دارای مراکز نظامی می‌باشد.

دولت ایالات متحده هشدارهایی را درباره تهدیدات امنیتی توسط هوآوی از سال ۲۰۱۲ منتشر کرده است. در ماه فوریه، کارفرمایان شش سازمان اطلاعاتی ایالات متحده اعلام کردند که با استفاده از یک دستگاه مخابراتی می توان افراد را در معرض خطر دسترسی به اطلاعات شخصی یا سرقت اطلاعات قرار دهد.

در ماه آگوست، رییس جمهور امریکا قانون اقدامات دفاعی را به امضا رسانید که سازمان های دولتی و پیمانکاران امریکایی حق استفاده از محصولات شرکت هوآوی و دیگر محصولات چینی را ندارند.

WSJ با اشاره به افراد ناشناس که از این موضوع مطلع هستند بیان نمود که ممکن است ایالات متحده انگیزه‌ای برای ترک شرکت هوآوی با افزایش کمک مالی خود برای توسعه مخابرات داشته باشد.

Huawei، که توسط یک مهندس ارتش آزادی بخش سابق به نام Ren Zhengfei تاسیس شده است، اخیرا با نزدیک شدن به اپل، به دومین فروشنده بزرگ گوشی‌های هوشمند تبدیل شده است. این شرکت همچنین بزرگترین شرکت تولید کننده‌ی وسایل مخابراتی در جهان است.

علارغم این امتیازات، ارگان‌های امریکایی به این کشور در خصوص خطرات استفاده از محصولات این شرکت اخطار داده‌اند. استرالیا همچنین استفاده از محصولات این شرکت را در تهیه‌ی قطعات شبکه‌ی 5G ممنوع کرده است.

حال باید دید که استراتژی بعدی این شرکت برای باقی ماندن در بازار بزرگ آمریکا چه می‌باشد و قدم بعدی دولتمردان امریکایی چه چیزی می‌باشد؟

گردآورنده: محمد مرتضوی

خطای آمازون و نشت اطلاعات کاربران!

جمعه سیاه و دوشنبه‌ی مجازی از روزهایی هستند که عموم فروشگاه‌های اینترنتی خدمات ویژه و تخفیفات بالایی را به کاربران و خریداران خود اختصاص می‌دهند. سایت آمازون هم یکی از این فروشگاه‌ها بوده که سود بالایی از این طریق کسب می‌نماید. اما وجود یک نقص امنیتی می‌تواند زمینه را برای رغیبان گسترده و لطمه‌ی بزرگی را به این فروشگاه وارد نماید.

از آنجا که وب سایت آمازون دارای سابقه‌ی طولانی در فروش الکترونیکی محصولات و ارائه‌ی خدمات به کاربران دارد، هر ساله شمار بسیار زیادی از مردم در سراسر دنیا به خرید از این فروشگاه می‌پردازند. ارائه‌ی تخفیفات دوره‌ای، تکمیل بودن اقلام و وسایل موجود برروی این فروشگاه، ارسال سریع و به موقع مرسولات و پشتیبانی بالای آنان از کاربران تنها بخشی از خدماتی است که این وب سایت بزرگ فروشگاهی طی سالیان طولانی به آنان مشهور است. از این رو هر صدمه‌ای هرچند که کوچک باشد می‌تواند بدنه‌ی این شرکت را تحت تاثیر خود قرار دهد.

در روز چهارشنبه، شرکت آمازون هشدار داد که به دلیل یک نقص فنی، اطلاعات بخشی از کاربران آن، اعم از نام و آدرس ایمیلشان منتشر گردیده است که خبر بسیار ناگواری در این مقطع زمانی به حساب می‌آمد.

این غول تجاری صحت این خبر را تایید کرده و به کاربران خود هشدار داده است که ممکن اطلاعات آنان نیز نشت پیدا کرده باشد. همچنین این شرکت از تعداد اکانت-هایی که اطلاعاتشان نشت پیدا کرده، حرفی به میان نیاورده است. در پیام اصلی، شرکت آمازون بیان نموده است که علت این نشت اطلاعات مربوط به رفتار کاربران نمی‌شود و نیازی به تغییر پسورد از سوی آنان ویا انجام عملی خاصی نمی‌باشد.

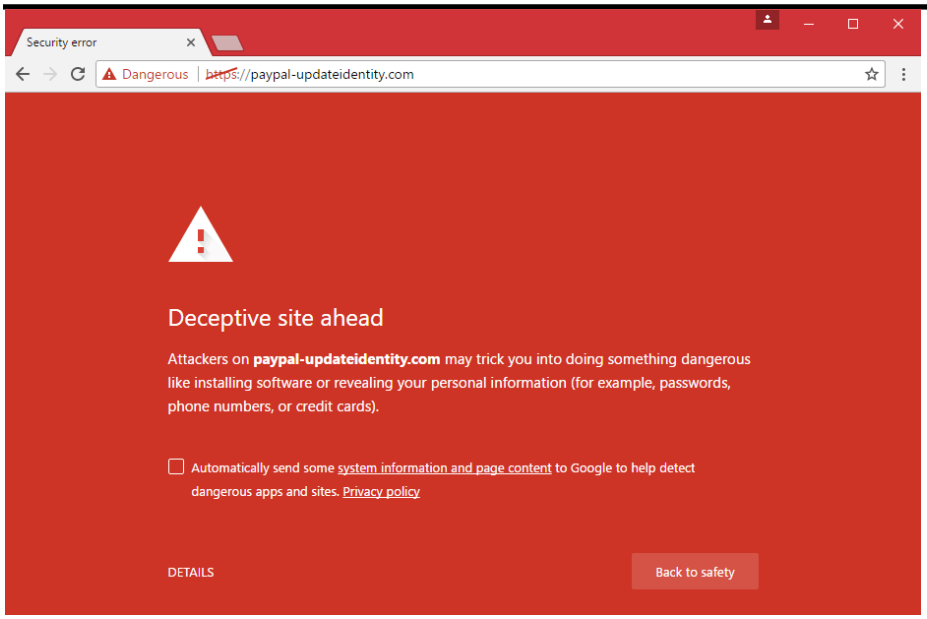
با وجود اطمینان از اطلاعیه‌های این شرکت، تغییر پسورد یکی از راه‌های مطمئن برای کاهش صدمات احتمالی است.

آمازون توضیح داده است که این خطای فنی ارتباطی با اخراج یک کارمند این شرکت که اقدام به اشتراک گذاری و فروش ایمیل کاربران در ماه اکتبر می‌کرده ندارد.

این حادثه‌ی امنیتی در بدترین زمان ممکن یعنی جمعه سیاه و دوشنبه مجازی برای این شرکت رخ داد. این نقص فنی قطعا می‌تواند درآمد ناشی از این فروش بزرگ را در این شرکت تحت تاثیر خود قرار دهد و باید منتظر بود تا با اعلام سود دوره‌ای این شرکت دید که این نقص فنی چه میزان توانسته است تا این شرکت را تحت تاثیر خود قرار دهد.

گردآورنده: محمد مرتضوی

فیشینگ با HTTPS



بسیاری از افراد غیر متخصص احساس می‌کنند که در صورت استفاده‌ی یک سایت از SSL، آن سایت قانونی و امن می‌باشد. در صورتی که به هیچ عنوان چنین چیزی نیست. براساس تحقیقاتی که به تازگی در سه ماه سوم سال ۲۰۱۸ انجام شده است ۴۹ درصد سایت‌های فیشینگ از لایه‌ی امن ویا SSL استفاده می‌کنند. این آمار به ما نشان می‌دهد که سایت‌های HTTPS نیز می‌تواند غیر ایمن ویا حتی ایجاد شده توسط یک هکر خبره باشد که منتظر گرفتن اطلاعات خصوصی نظیر شماره‌ی کارت بانکی، آدرس ایمیل، نام و سایر مشخصات ما است.

گوگل سال‌های زیادی را تلاش کرده است تا وب سایت‌های موجود در اینترنت را با پروتکل HTTPS تطبیق دهد تا اطلاعات رمز شده از طریق SSL/TLS بین مرورگر و وب سایت‌ها منتقل گردد. بسیاری از افراد هنوز معتقد هستند که وجود یک قفل و رمزنگاری مساوی است با امنیت آنان، اما بسیاری از سایت‌های فیشینگ دارای این قفل در نوار آدرس خود هستند.

براساس تحقیقات جدید PhishLab، ۴۹ درصد از سایت‌هایی که برای انجام حملات فیشینگ طراحی می‌شوند دارای SSL هستند که این آمار ۳۵ درصد نسبت به ۳ ماه گذشته و ۲۵ درصد نسبت به سال گذشته افزایش یافته است. از این رو باید دانست که انجام هک حتی می‌تواند با مراحل کاملا قانونی و ایمن انجام گیرد.

با افزایش سایت‌های فیشینگی که سایت خود را ثبت می‌کنند و برای آن Certificate های مربوطه را اخذ می‌کنند، نمایش عبارت Not Secure در مرورگر گوگل کروم مربوط به وب سایت‌هایی می‌شود که فاقد رمزنگاری باشند.

شرکت‌های صادر کننده‌ی Certificate قادر به بررسی کردن وب سایت‌ها از لحاظ قانونی و یا غیر قانونی بودن نمی‌باشند.

در ماه دسامبر سال گذشته، نظر سنجی انجام شده PhishLab نشان می‌دهد که بیش از ۸۰ درصد از پاسخ دهندگان معتقد هستند که قفل نمایش داده شده در مرورگر در خصوص امن یا قانونی بودن آن وب سایت درست نمی‌باشد.

سازندگان مرورگر با همکاری با شرکت های امنیتی برای شناسایی و مسدود کردن سایت‌های فیشینگ جدید مبارزه می‌کنند، اما برخی از این وب سایت‌ها موفق به فرار از این شرایط هستند. امن ترین گزینه این است که اگر شما در مورد یک وبسایت سوء ظن دارید، حتی اگر دارای قفل می‌باشد اطلاعات خود را در آن وارد ننمایید.

گردآورنده: محمد مرتضوی

بهترین آنتی ویروس‌های سال ۲۰۱۸

استفاده از آنتی ویروس برای جلوگیری از آلوده شدن به ویروس و بدافزار یکی از مرسوم‌ترین کارهایی است که کاربران انجام می‌دهند. اما سوالی که ذهن اغلب کاربران را به خود درگیر می‌کند این است که کدام آنتی ویروس از بین تمامی آنتی ویروس‌های تولید شده که کم هم نیستند می‌تواند بهترین محافظت را از آنان در مقابل بد افزارها و تهدیدات انجام دهد.

تحقیقات AVTest برروی آنتی ویروس‌ها نتیجه‌ی جالبی را براساس توانایی‌های آنتی ویروس‌ها در اختیار کاربران قرار می‌دهد.

این شرکت اقدام به رتبه بندی آنتی ویروس-های ویندوز برای مصارف خانگی نموده است که تمامی آنتی ویروس‌های لیست زیر موفق به کسب امتیاز ۶ از ۶ شده‌اند:

- Avira
- Bitdefender
- BullGuard
- Kaspersky
- eScan
- Norton

تمامی این آنتی ویروس‌ها با داشتن حداکثر امتیاز در سطر جدول قرار گرفتند. شما با تهیه‌ی هر یک از این آنتی ویروس‌ها می-توانید با خیال راحت مطمئن شوید که حداکثر محافظت از کامپیوتر شما انجام می-گیرد.

اما اگر می‌خواهید که برای آنتی ویروس پولی پرداخت نکنید Avast و Windows Defender بهترین گزینه می‌باشند.

ویندوز ۱۰ همراه با آنتی ویروس پیش فرض Windows Defender عرضه می‌گردد و براساس تحقیقات انجام شده از سوی AVTest، این آنتی ویروس آنقدرها هم بد نیست و می‌توان آن را در وسط جدول رتبه بندی جای داد.

این ابزار در پروژه‌ای ایجاد شد که مایکروسافت قصد داشت ابزاری را معرفی نماید که قابلیت محافظ از ویندوز را داشته باشد و کارکرد آن را بهبود بخشد.

برای کامپیوترهای خانگی هرچند که گزینه‌های پولی بسیار مناسب هستند اما نباید همیشه این تصور را داشت که آنتی ویروس‌های رایگان ناکارآمد هستند. آنتی ویروسی همچون Windows Defender به آرامی در حال تغییر به یک آنتی ویروس تمام عیار است که این موضوع باعث رفع نیاز کاربران خانگی می‌گردد. اما برای کسب و کارهای بزرگ قطعا نسخه‌های پیشرفته مورد نیاز هستند که تمامی آنان دارای لایسنس-های پولی می‌باشند.

هیچ وقت نباید زمانی را که آنتی ویروس Norton کیفیت پایینی داشت را فراموش نمود. آنتی ویروس‌ها در گذر زمان بهبود پیدا می‌کنند و نباید به دید گذشته به آنان نگاه کرد.

گردآورنده: محمد مرتضوی

KHARAZMI CERT COORDINATOR CENTER

مرکز آپا دانشگاه خوارزمی

رییس مرکز:

دکتر امید مهدی عبادتی

اعضای هیات علمی:

دکتر احسان ملکیان

دکتر امید مهدی عبادتی

کارشناسان مرکز:

محمدحسین خدامی

سمیه نیا خلیلی

محمد مرتضوی

امین زمانی

حسین علیمرادی

شیوا بهادری

محسن نادری

محسن یزدی‌نژاد

فاطمه الهی

نشانی:

کرج - دانشگاه خوارزمی - کتابخانه‌ی مرکزی - طبقه‌ی همکف - مرکز آپا

تلفن:

۰۲۶۳۴۵۷۵۰۱۲

۰۲۶۳۴۵۷۵۰۱۸

۰۲۶۳۴۵۷۹۶۰۰ (داخلی ۲۶۲۲)

پست الکترونیک:

cert@khu.ac.ir

وب سایت:

http://cert.khu.ac.ir/

کانال مرکز آپا خوارزمی:

@khu_cert

دانلود رایگان:

دانلود رایگان مجموعه کامل خبرنامه‌ها از طریق اسکن کد زیر در دسترس است.