شماره بیست و ششم - اسفند ۱۳۹۷

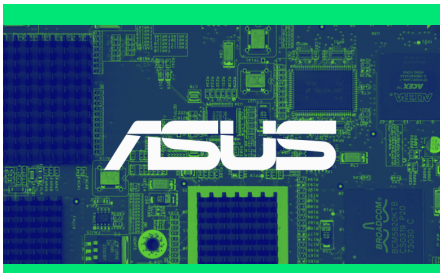
خبرنامه "آپا" دانشگاه خوارزمی

KHARAZMI CERT
COORDINATION CENTER
مرکز تخصصی آپا خوارزمی

در این شماره خواهید خواند:

آسیب پذیری‌های نرم افزار WINRAR به ۱۰۰ عدد رسید!

اگر شما نرم افزار WinRAR را داشته باشید، اطمینان حاصل کنید که به آخرین نسخه آن که آسیب پذیری امنیتی بحرانی را پچ کرده است، به روز شده است. در حال حاضر هکرهای فرصت طلب از این آسیب پذیری استفاده می‌کنند تا کاربران آسیب پذیر به طور ناشناخته‌ای را قبل از اینکه بتوانند پچ کنند هدف قرار دهند. - صفحه ۲



هشدار: سرور به روز رسانی نرم افزار ASUS هک شده!

محققان امنیتی امروز شاهد یک حمله گسترده زنجیره تامین بوده‌اند که بیش از ۱ میلیون کامپیوتر تولید شده توسط ASUS را به خطر انداخته است. - صفحه ۳

آسیب پذیری در محصولات بیسیم Logitech

شرکت Logitech یکی از تامین کننده‌های مشهور وسایل جانبی در نیا می‌باشد که تا کنون چندین بار در سرخط خبرها قرار گرفته است. هنگامی که آسیب پذیری امنیتی رخ می‌دهد، تاثیر آن می‌تواند گسترده و فاجعه آمیز باشد. - صفحه ۴

هکر هلندی مجرم به DDoS بخشیده شد!

در یکی از شهرهای کشور هلند به گونه‌ای کاملا مسالمت آمیز با یک هکر برخورد شده است و تنها در مقابل معذرت خواهی وی، از شدت مجازات او کاسته شده است. - صفحه ۵

کشف آسیب پذیری در خودرو تسلا!

برنامه‌های کشف آسیب پذیری همیشه همیشه هکرها و محققان امنیتی را تشویق می‌کند تا با کشف و اثبات آسیب پذیری بتوانند برنده‌ی جایزه‌ی ده هزار دلاری ویا صدهزار دلاری شوند. در جدید ترین رویداد Pwn2Own، شرکت تسلا با اثبات آسیب پذیری در محصولاتش مجبور به پرداخت پاداش شد. - صفحه ۶

پسوردهای فیس بوک بدون رمزگذاری ذخیره می‌شوند!

جای فیس بوک یکی از بزرگترین شبکه‌های اجتماعی در جهان باشد که مدعی حفاظت تمام و کمال از داده‌های کاربران است. اما جای تعجب است که بر اساس آماری جدید، به خاطر یک سهل انگاری امنیتی، نزدیک به ۶۰۰ میلیون پسورد فیس بوک در خطر افشا هستند. - صفحه ۷

آسیب پذیری‌های نرم افزار WINRAR به ۱۰۰ عدد رسید!

اگر شما نرم افزار WinRAR را داشته باشید، اطمینان حاصل کنید که به آخرین نسخه آن که آسیب پذیری امنیتی بحرانی را پچ کرده است، به روز شده است. نسخه‌های آسیب پذیر فایل‌های آرشیو مخرب، تحت پوشش این آسیب پذیری قرار می‌گیرند و در حال حاضر هکرهای فرصت طلب از این حمله استفاده می‌کنند تا کاربران آسیب پذیر را به طور ناشناخته، قبل از اینکه بتوانند نرم افزار خود را به روز رسانی کنند، هدف قرار دهند.

در فوریه، شرکت امنیتی cybersecurity یک آسیب پذیری را که در ۱۹ سال گذشته در WinRAR وجود داشت، منتشر کرد.

این آسیب پذیری به دلیل پشتیبانی از WinRAR برای فرمت آرشیو قدیمی ACE می‌باشد، به این ترتیب می‌توان با هدف تخریب یک فایل ACE با یک فرمت rar ایجاد کرد و سپس پس از راه اندازی مجدد، آن را به عنوان یک تله موقت برای اجرای کد مخرب از یک پوشه راه اندازی شده در دستگاه استفاده کرد.

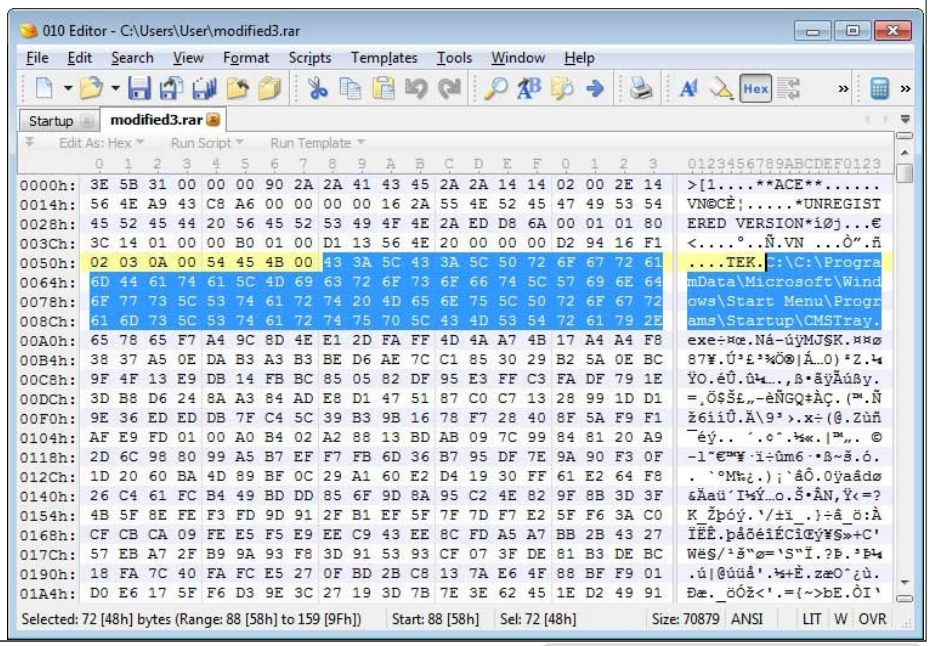
کسانی که از آخرین نسخه استفاده نمی کنند، در معرض خطر هستند. اکنون هکرها قبل از به روز رسانی کاربران، سوءاستفاده را برای رسیدن به سیستم های آسیب پذیر به کار می‌گیرند.

محققان بیش از ۱۰۰ سوء استفاده منحصر به فرد را شناسایی کرده‌اند.

احتمالا اولین بدافزار از طریق ایمیل ارسال شده است تا از آسیب پذیری WinRAR بهره ببرد. Backdoor توسط MSF تولید می‌شود.

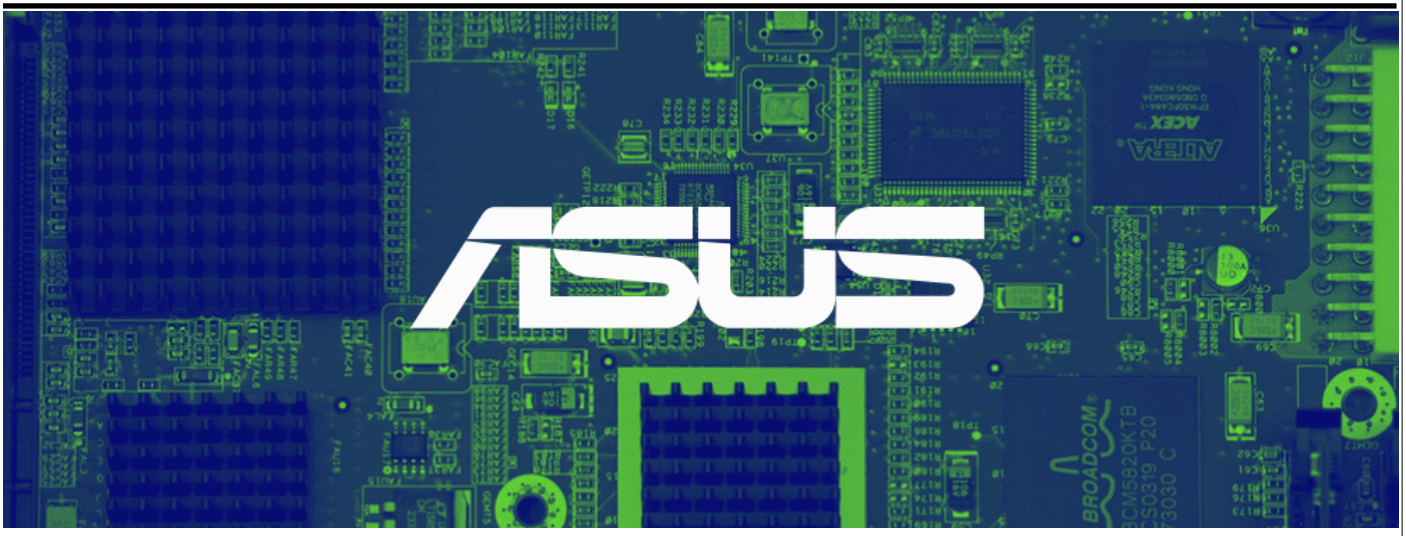
آسیب پذیری ثبت شده دارای شناسه‌ی CVE-2018-20250 می‌باشد.

WinRAR بالغ بر ۵۰۰ میلیون کاربر دارد که بیشتر آنها احتمالا در مورد این آسیب پذیری‌ها چیزی نمی‌دانند و سطح حمله مطلوب را برای مهاجمین ایجاد می‌کنند. این حمله مستلزم جذب بیشتر در آینده است، بنابراین لطفا با دوستان و خانواده خود به اشتراک بگذارید، اگر می‌دانید WinRAR را نصب کرده‌اند حتما از جدیدترین نسخه نرم افزار استفاده کنید.



گردآورنده: امیرحسین ضرغامی

هشدار: سرور به روز رسانی نرم افزار ASUS هک شده!



محققان امنیتی امروز شاهد یک حمله گسترده در زنجیره تامین بوده‌اند که بیش از یک میلیون کامپیوتر تولید شده توسط ASUS را به خطر انداخته است.

گروهی از هکرهای تحت حمایت دولت سال گذشته موفق به ربودن سرور به روزرسانی خودکار نرم افزار ASUS Live در ماه ژوئن و نوامبر ۲۰۱۸ شدند و به روز رسانی‌های مخرب را برای نصب بیش از یک میلیون کامپیوتر ویندوز در سراسر جهان تحت حمله قرار دادند.

به گفته محققان امنیتی سایبری از آزمایشگاه کسپرسکی روسیه، که این حمله را کشف و به نام Operation ShadowHammer نامگذاری کرده است.

پس از تجزیه و تحلیل بیش از ۲۰۰ نمونه از به‌روز رسانی‌های مخرب، محققان متوجه شدند که هکرها نمی خواستند همه کاربران را هدف قرار دهد، بلکه فقط یک لیست خاص از کاربران شناسایی شده توسط آدرس‌های MAC منحصر به فردآن ها به بد افزارهای مخرب آلوده کرده و مورد هدف قرار داده اند.

فایل‌های مخرب با گواهینامه‌های دیجیتالی ASUS به طور قانونی امضا شده‌اند تا با به روز رسانی نرم افزار رسمی از شرکت برای مدت طولانی نادیده گرفته شوند.

Kaspersky تشخیص داده که اکثر قربانیان آلوده شده از روسیه، آلمان، فرانسه، ایتالیا، و ایالات متحده هستند، هر چند این بدافزار آلوده کاربران را از سراسر جهان مورد تهدید قرار می‌دهد.

Kaspersky و سایر شرکت‌های آنتی ویروس از این حمله مطلع هستند این در حالی است که تحقیقات در مورد این موضوع همچنان ادامه دارد.

شرکت‌های امنیتی آنتی ویروس همچنین یک ابزار خودکار برای کاربران برای بررسی اینکه آیا آن‌ها به طور خاص توسط تهدید دائمی پیشرفته ShadowHammer هدف قرار داده شده اند یا خیر منتشر کرده‌اند.

گردآورنده: امیرحسین ضرغامی

آسیب پذیری در محصولات بیسیم Logitech

شرکت Logitech یکی از تامین کننده‌های مشهور وسایل جانبی در نیا می‌باشد که تا کنون چندین بار در سرخط خبرها قرار گرفته است. هنگامی که آسیب پذیری امنیتی رخ می‌دهد، تاثیر آن می‌تواند گسترده و فاجعه آمیز باشد.

محقق امنیتی آقای David Sopas به تازگی به وجود یک آسیب پذیری در موس بیسیم شرکت Logitech در مدل M185 پی‌برده است.

این در حالی است که این موس دارای کارایی بالایی است و قیمت آن ۲۵ دلار می‌باشد. این خصوصیت‌ها و ویژگی بیسیم بودن آن باعث شده است که افرادی اغلب سفر می‌کنند و یا فقط به دنبال یک موس با حداقل قیمت و حداکثر کارایی هستند به این گزینه‌ی مناسب روی آورند.

با تمامی این زمینه‌ها موس M185 دارای آسیب پذیری MouseJack می‌باشد.

آسیب پذیری MouseJack به مهاجمان این امکان را می‌دهد که با یک وسیله‌ی ارسال و دریافت امواج رادیویی ارزان قیمت بتوانند از فاصله‌ی ۱۰۰ متری با موس‌های آسیب پذیر ارتباط برقرار کنند.

پس از آن، مهاجم می‌تواند با کنترل، موس قربانی را در اختیار بگیرد. البته باید یادآور شد که تمامی موس‌ها آسیب پذیر نمی-باشند.

در خصوص هک انجام شده توسط Sopas ، وی از موس خود برای هک استفاده نموده است و از حمله برای نمایش ماشسن حساب پیش فرض ویندوز استفاده کرده است. وی از این آسیب پذیری برای نمایش یک آسیب استفاده نکرده است. بلکه مستندات وی تنها نماینده‌ی اثبات آسیب پذیری می‌باشد.

اگرچه وجود این آسیب پذیری در استفاده کوتاه مدت از موس‌های مختلف آنچنان به چشم نمی‌آید. اما با این وجود به روز رسانی نرم افزاری موس‌های مختلف باعث رفع این نقص‌ها خواهد شد.

در ادامه لیستی از موس‌های آسیب پذیر به حملات MouseJack آمده است.

- Wireless Mouse MG-0975
  USB dongle RG-0976 (USB ID 04f2:0976))
- Dell KM714 Wireless Keyboard and Mouse Combo
  KM714 USB dongle (USB ID 046d:c52b)
- KM632 Wireless Mouse
  USB dongle (USB ID 413c:2501)
- K7600 wireless keyboard USB dongle (USB ID 04b4:0060)
- Wireless Elite v2 keyboard Elite
  USB dongle (USB ID 03f0:d407)
- ...

برای اطلاعات بیشتر می‌توانید به لینک زیر مراجعه کنید.

https://www.bastille.net/research/vulnerabilities/mousejack/affected-devices

گردآورنده: محمد مرتضوی

هکر هلندی مجرم به DDoS بخشیده شد!

همیشه انتظاری که ما از قانون داریم این است که با هکرها و مجرمان سایبری که در زندگی مردوم اختلال ایجاد می‌کنند با اشد مجازات برخورد شود. اما این بار قضیه فرق می‌کند و در یکی از شهرهای کشور هلند به گونه‌ای کاملا مسالمت آمیز با یک هکر برخورد شده است و تنها در مقابل معذرت خواهی وی، از شدت مجازات او کاسته شده است.

هکر هلندی که با ساخت ربات DDoS از قربانیان زیادی مبلغ ۱۵۰۰۰۰ دلار اخاذی کرده بود بخاطر قبول کردن اشتباه خود و معذرت خواهی از قربانیان به زندان نرفت.

در سال ۲۰۱۶ و ۲۰۱۷ یک هکر سایت‌های زیادی از جمله BBC و Yahoo News را با حملات DDoS و با استفاده از بدافزار Mirai تحت حمله قرار داد.

در طی ۱۲ ماه، آنها تقریبا ۱۵۰۰۰۰ دلار را از طریق حمله و سپس از طریق درخواست برای جبران خسارت، درخواست کردند. در اکتبر سال ۲۰۱۷ یک مظنون در رابطه با این حملات دستگیر شد و این حملات پایان یافت.

مظنون دستگیر شده در دنیا با نام S شناخته می‌شود. زیرا در زمان دستگیری وی زیر سن قانونی بود. بنابراین دولت هلند از انتشار اسم وی خودداری نمود. این کار تا این لحظه که وی بالای ۲۰ سال است نیز ادامه دارد.

براساس گذارش ZDNet این فرد مظنون در دادگاه اعتراف کرد و جرم خود را پذیرفت. وی همچنین در ادامه بخاطر اعمال خود معذرت خواهی نمود. لذا جرم وی از زندان به ۱۲۰ ساعت کار در خدمات عمومی تغییر یافت.

وی زمانی زیادی را در بازداشت مخصوص نوجوانان به سر میبرده است.

در طول پروسه‌ی دادرسی، S بیان نمود که وی هک کردن را از سال ۱۳ یا ۱۴ سالگی شروع کرده است و حملات DDoS و باج افزاری را به این خاطر شروع کرده که خانواده‌ی آن توانایی حمایت مالی از وی را نداشته‌اند.

وی به دلیل جرمی که انجام داده است به ۲ سال زندان و پرداخت خسارت محکوم شده بود که عذرخواهی وی باعث شد تا قاضی متوجه گردد که به زندان رفتن برای وی پاسخگو نیست.

در حال حاضر S آزاد شده است و آزادی مشروط آن درصورتی است که ۳۶۰ روز هیچ جرم دیگری را مرتکب نشود و قانونی را زیر پا نگذارد.

گردآورنده: محمد مرتضوی

کشف آسیب پذیری در خودرو تسلا!

برنامه‌های کشف آسیب پذیری همیشه همیشه هکرها و محققان امنیتی را تشویق می‌کند تا با کشف و اثبات آسیب پذیری بتوانند برنده‌ی جایزه‌ی ده هزار دلاری ویا صدهزار دلاری شوند. در جدید ترین رویداد Pwn2Own، شرکت تسلا با اثبات آسیب پذیری در محصولاتش مجبور به پرداخت پاداش شد.

تسلا ارتباط خوبی با جامعه هکرها دارد. سال گذشته این شرکت جایزه‌ی خود را در ازای کشف آسیبپذیری به ۱۵۰۰۰ دلار افزایش داد. در این هفته نیز در رویداد Pwn2Own آن‌ها پای خود را فراتر گذاشتند و در قبال کشف هر آسیب پذیری وعده دادند که یک خودروی تسلا مدل 3 را به گروه یا شخصی که کنترل خودرو را در دست بگیرد، هدیه خواهند داد.

رویداد Pwn2Own یک گردهمایی سالانه در بین هکرها می‌باشد که اگر یک هکر بتواند با استفاده از آسیب پذیری‌هایی که قبلا کشف نشده است، یک وسیله را هک کند، صاحب آن وسیله خواهد شد به علاوه‌ی سایر جوایزی که به وی تعلق خواهد گرفت.

شرکت تسلا امسال به عنوان اولین شرکت تولید کننده‌ی خودرو در این رویداد نقش ایفا می‌کند.

در آخرین روز این رویداد، چالش ایجاد شده توسط تسلا از طرف تیم‌های بسیاری مورد بررسی قرار گرفت. یک تیم دو نفره به نام Fluoroacetate توانستند به سیستم اطلاعاتی این خودرو نفوذ کنند.

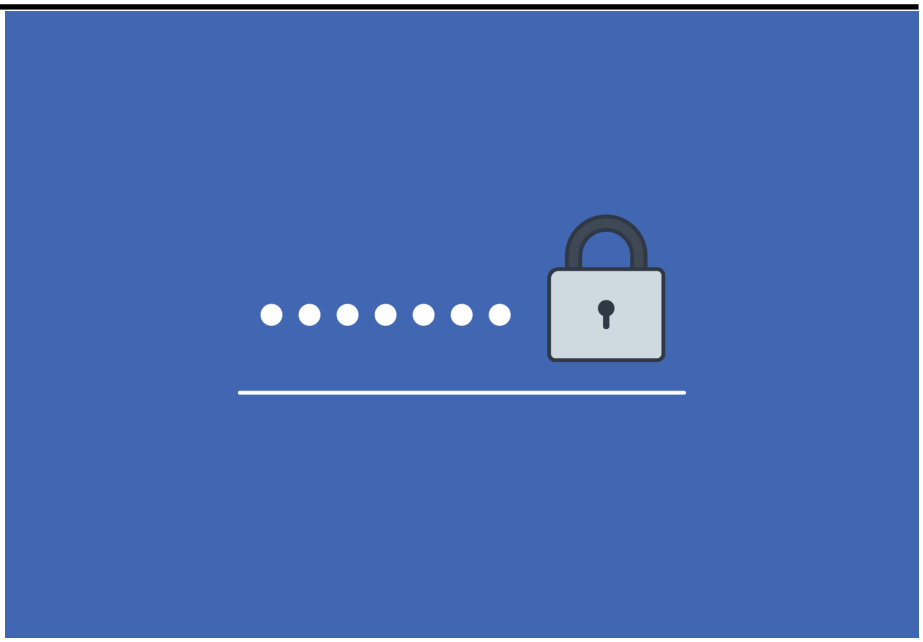
این دو هکر برنده با نام‌های Amat Cama و Richard Zhu اطلاعات زیادی در خصوص اینکه چطور توانستند به سیستم اطلاعاتی این خودرو نفوذ و آن را تحت مدیریت خود درآورند، ارائه نکردند. آن‌ها به گفتن اینکه از طریق یک آسیب پذیری در مرورگر خودرو این هک را انجام دادند بسنده کردند. اما اگر ادعای آنان درست باشد، شرکت تسلا پیشنهاد داشده است که با انتشار آن آسیب پذیری و مشخص کردن آن می‌توانند خودرو را به عنوان جایزه برای خود نگه دارند.

نماینده‌ی شرکت تسلا در این رویداد بیان کرده است که: "همیشه ما در حال توسعه‌ی بهترین و ایمن‌ترین سیستم‌ها برروی خودروهای تسلا هستیم اما این همکاری برای ما ارزشی دوچندادن دارد."

با این همکاری مشترک بین شرکت تسلا و هکرها، حالا شرکت تسلا یک قدم نزدیکتر به امنیت می‌باشد.

گردآورنده: محمد مرتضوی

پسوردهای فیس بوک بدون رمزگذاری ذخیره می‌شوند!



جای فیس بوک یکی از بزرگترین شبکه‌های اجتماعی در جهان باشد که مدعی حفاظت تمام و کمال از داده‌های کاربران است. اما جای تعجب است که بر اساس آماری جدید، به خاطر یک سهل انگاری امنیتی، نزدیک به ۶۰۰ میلیون پسورد فیس بوک در خطر افشا هستند.

در روز سه شنبه در ماه ژانویه و در طول یک بازنگری معمول امنیتی، فیس بوک اظهار کرد که پسورد برخی از کاربران آن به صورت متن ساده یا Plain Text در دیتابیس‌هایش ذخیره شده است. سخنگوی این شبکه‌ی اجتماعی بزرگ بیان نمود که پسوردهای این افراد از بیرون از فضای این شرکت و از طریق اینترنت قابل مشاهده نیست. حتی کارمندان فیس بوک نیز نمی‌توانند به آنان دسترسی داشته باشند.

فیس بوک پس از اثبات این مسئله بیان نمود که به کاربرانی که در خطر هستند حتما اعلان خواهد شد.

یکی از کارمندان بلندمرتبه در فیس بوک به KrebsOnSecurity گفت که تحقیقات نشان می‌دهد که بین ۲۰۰ تا ۶۰۰ میلیون نفر از کاربران ممکن است پسوردشان به صورت متن ساده ذخیره شده باشد. بدتر از اینکه هنوز آن کاربران توسط ۲۰۰۰۰ کارمند فیس بوک از طریق نسخه-های پشتیبان مربوط به سال ۲۰۱۲ هنوز در دسترس هستند.

به طور رسمی نیاز است تا فیس بوک به صدها میلیون از کاربران فیس بوک، ده‌ها میلیون از کاربران نسخه لایت فیس بوک و به صدها نفر از کاربران اینستاگرام این مخاطره را اطلاع رسانی کند.

این اولین باری نیست که روش‌های حفاظت اطلاعات فیس بوک مورد سوال و تجسس قرار گرفته است. چندین هفته‌ی گذشته فیس بوک در اقدامی شماره تلفن بسیاری از کاربران خود را که برای احراز هویت دو مرحله‌ای ثبت کرده بودند را منتشر ساخت.

مثل اینکه دردسرهای فیس بوک تمامی ندارد و کاربران با گذشت زمان هرچه بیشتر به ایمن نبود این شبکه‌ی اجتماعی پی میبرند.

حال باید منتظر بود و دید که راه حل فیس بوک برای حل این مشکل تازه چه چیزی خواهد بود.

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.