www.daneshjooyar.com

دانشجویار

ماهنامه تخصصی کامپیوتر و فناوری اطلاعات
شماره پانزدهم - آبانماه ۱۳۹۵ - نسخه ویژه انتشار اینترنتی

یادگیری تضمینی با
مدرسه مجازی

- اندروید ، خدمتکار یا جاسوس!؟
- بررسی حفره های امنیتی وب سایت و مقابله با آن
- ضرورت طراحی Landing Page اختصاصی
- آنتی ویروس جعلی قربانی می گیرد!

SoftGozar.com

حامیان انتشار
ماهنامه تخصصی دانشجویار
متشکریم!

SoftGozar.com

SoftGozar.com

ایام عزاداری سالار شهیدان امام حسین (ع) تسلیت باد

امام حسین علیه السلام فرمودند:

من دلائل العالم إنتقادهٔ لحدیثه و علمه بحقائق فنون النظر.

از نشانه های عالم ، نقد سخن و اندیشه خود و آگاهی از نظرات مختلف است .

(بحارالانوار،ج۷۸،ص۱۱۹)

SoftGozar.com

ماهنامه تخصصی کامپیوتر و فناوری اطلاعات

شماره پانزدهم – آبانماه ۱۳۹۵ – نسخه ویژه انتشار اینترنتی

■ **صاحب امتیاز:**

وب سایت دانشجویار | daneshjooyar.com

■ **مدیر مسئول و سردبیر :**

صادق پاسبان | Sadegh.info@gmail.com

■ **طراحی و صفحه آرایی:**

زهرا نصری | Mag@daneshjooyar.com

■ **سرپرست نویسندگان :**

علی اصغر تقی زاده | Golshan.info@gmail.com

■ **نویسندگان این شماره :**

علی اصغر تقی زاده ، پوریا انجمنی ، عرفان اکبری منش، زهرا نصری ، سهیلا هادی نیا ، حسین جلیلی ، محمد مهدی محمدی

■ **نشانی :**

استان خراسان جنوبی ، شهرستان بیرجند، بلوار آیت ا... مدرس کوچه ۱۷ ، پلاک ۵

■ **تلفن تماس و پست الکترونیک ماهنامه**

Mag@daneshjooyar.com – ۰۵۶۳۲۲۳۲۸۸۴

دانشجویار آماده دریافت مقالات و مطالب شما می باشد.

مطالب و مقالات خود را برای ما ارسال کنید تا پس از بررسی در ماهنامه با نام خودتان چاپ شود.

SoftGozar.com

ماهنامه تخصصی کامپیوتر و فناوری اطلاعات

آنچه در این شماره می خوانید...

SoftGozar.com

سرآغاز سخن

یاران و همراهان دانشجویار سلام؛

ایام عزاداری سرور و سالار شهیدان امام حسین (ع) را خدمت شما عزیزان تسلیت عرض می کنم .

پانزدهمین شماره از ماهنامه دانشجویار هم اکنون پیش روی شماست درطی این چند سالی که در خدمت شما بودیم همواره سعی تیم دانشجویار بر این بوده که به کمک شما عزیزان نقاط ضعف سیستم خود را شناسایی کرده و در جهت رسیدن به آنچه که مورد رضایت کامل شماست آن را مرتفع کنیم . برای رسیدن به این هدف بزرگ با حضور پررنگ شما همراهان همیشگی است که می توانم از موانع و مشکلات سر راه به راحتی عبور کرده و به مقصد نهایی خود برسیم . در این راستا توانسته ایم با راه اندازی مدرسه مجازی ؛ گامی بزرگ در جهت فراگیرشدن آموزش آسان ، مطمئن و البته پروژه محور برداریم .که در این شماره به طور مفصل در این رابطه صحبت خواهیم کرد .

عزیزان دل ؛ قبلا هم به شما یادآور شدم که بازار کار رشته های کامپیوتر و فناوری اطلاعات فوق العاده است. البته برای کسی که تجربه و هنر کافی داشته باشد! به هیچ عنوان به دروس دانشگاه اکتفا نکنید چون کاملا آکادمیک هستند ؛ وقت آن رسیده که دست از کلاس های مدرسه و دانشگاه به عنوان اتاقک های تولید مدرک برداریم و به این اماکن مقدس به عنوان مراکزی برای یادگیری و دانش اولیه نگاه کنیم و بیایید به جای امید داشتن به این که حتما با گرفتن مدرک بالا در آینده شغلی پردرآمد به ما پیشنهاد می شود ، تا دیر نشده از خواب غفلت بیدار شویم و سعی کنیم از هر فرصتی که در مقابلمان قرار دارد برای یادگیری مهارت و فنی درآمدزا استفاده کنیم که هیچ تضمینی برای یافتن شغل برای افراد بی مهارت در آینده وجود ندارد .فیلم ها و کلاس های آموزشی را سرسری نگیریم و به جای سرگرم شدن با فیلم های سینمایی وقت تلف کن ، سعی کنیم لحظه به لحظه مهارت های بیشتر و متنوع تری را بیاموزیم .

دقایقی فکر کنید و ببینید که آیا از این به بعد هم می خواهید به شکل گذشته ادامه دهید و بعد با حسرت از تمام موفقیت هایی که حق شما بود و می توانستید به آن ها دست یابید ؛ یاد کنید !

تصمیم خود را بگیرید و تمام وجودتان را به یک خواستن تبدیل کنید و رسیدن به خواسته تان را به یک نیاز تبدیل کنید ، به توانایی های خود ایمان داشته باشید و همین الان دست به عمل بزنید و ایمان داشته باشید که پیشرفت و موفقیت حق شماست .

سربلند باشید – صادق پاسبان

SoftGozar.com

تازه های فناوری

SoftGozar.com

گردآوری:
زهرا نصری

کشف رخنه جدید امنیتی در اندروید

به‌تازگی رخنه جدید امنیتی در سیستم‌های اندرویدی مشاهده شده است که موجب شده است تا میلیون‌ها دستگاه به خطر بیفتند ولی این رخنه که Rowhammer نام دارد، در حقیقت یک حمله سخت‌افزاری است که از ضعف پیاده‌سازی نرم‌افزار بهره گرفته است.

امروزه امنیت تلفن‌های همراه بیش از امنیت کامپیوترهای خانگی هدف هکرها قرار می‌گیرد که با توجه به محبوبیت بالای این دستگاه‌ها نمی‌توان این امر را چندان غیرمعقول دانست.

رخنه امنیتی جدید سیستم عامل اندروید که Rowhammer نام دارد، در طول چند روز آینده بسیاری کاربران را نگران ساخته است ولی در عمل این حمله چگونه عمل می‌کند و چرا نباید چندان نگران آن بود؟

این عیب امنیتی در حقیقت یک رخنه بر روی تراشه پردازنده است که موجب می‌شود تا دستگاه فرد قربانی به‌صورت ناخودآگاه، به‌واسطه آن روت شود.

در حال حاضر اعمال این حمله برای تمامی دستگاه‌ها ممکن نیست زیرا انجام آن به سخت‌افزار و تراشه‌های حافظه به‌کاررفته در دستگاه بستگی دارد.

تیم امنیتی کاشف این رخنه تائید کرده‌اند که تا به امروز دستگاه‌های زیر با این مشکل روبرو شده‌اند:

نکسوس ۵ ، گلکسی اس ۵ ، گلکسی اس ۴ ، گلکسی اس ۶، ال‌جی جی ۴ ، موتورولا موتو جی و ...

با این وجود این رخنه چندان نگران‌کننده نیست زیرا کاشفان آن یک تیم امنیتی هستند و هکرها هنوز از نحوه انجام آن آگاه نیستند و به همین دلیل نیز نیازی به نگرانی نیست و به‌زودی وصله مناسب برای رفع این مشکل عرضه خواهد شد.

منبع: عصر پایش

جوان اوکراینی نام خود را به «آیفون ۷» تغییر داد!

خیلی از ما شاید به در دست داشتن آخرین مدل اسمارت فون برند محبوبمان خیلی علاقه مند باشیم. ولی آیا برای اینکه چنین گوشی را به رایگان دریافت کنید حاضر به انجام چه کاری هستید؟ یک شرکت کامپیوتری در شهر کیف اوکراین قول داده بود که به پنج نفر اولی که به طور رسمی و قانونی

نام خود را به «آیفون ۷» تغییر دهند یک گوشی آیفون ۷ اپل هدیه دهد. به همین دلیل هم یکی از شهروندان اوکراین، الکساندر تورین، جوانی ۲۰ ساله رسماً نام خود را به iPhone Sim (به معنی ۷) تغییر داد و روز جمعه اسمارت فون رایگان خود را دریافت کرد.

اگر به این ماجرا از منظر مالی رقابت نگاه کنیم، شاید رد کردن چنین پیشنهادی خیلی عاقلانه نباشد. در نظر داشته باشید که در اوکراین آیفون ۷ معادل ۸۵۰ دلار قیمت دارد، در حالیکه تغییر نام فقط ۲ دلار هزینه در پی دارد. با این حال دوستان و خانواده Sim از شنیدن این خبر و اقدامی که او برای تغییر نام و دستیابی به آیفون ۷ انجام داده بود حیرت زده شدند.

تتیانا پنینا خواهر iPhone Sim گفت: پذیرش این موضوع و باور اینکه حقیقت داشته باشد سخت بود. همه به دنبال راهی برای ابراز وجود هستند. خب پس چرا از این طریق نباشد؟

البته تورین تمایلی ندارد که در آینده فرزندانش در خصوص نام آیفون مورد بازخواست قرار بگیرند، بنابراین قصد دارد زمانی که صاحب فرزند شد نام خود را به الکساندر تورین تغییر بدهد.

منبع : تک شات

SoftGozar.com

۷۵ درصد از مردم جهان با تلفن همراه به اینترنت متصل می‌شوند.

در حالی که تا چند سال قبل عموم کاربران اینترنت از رایانه‌های شخصی برای این کار استفاده می کردند، شرایط به نفع کاربران گوشی‌های هوشمند به سرعت در حال تغییر است.

از راه رسیدن اینترنت اشیا و اتصال اکثر ابزار و وسایل موجود در محیط زندگی انسان تعداد ابزار قابل اتصال به دنیای مجازی را به نحو چشمگیری افزایش داده است، اما مهم‌ترین ابزاری که هم اکنون برای اتصال به اینترنت و استفاده از آن به کار می‌رود گوشی‌های هوشمند است و این روند در سال‌های آتی نیز ادامه می‌یابد.

گزارش جدید موسسه Zenith نشان می‌دهد در سال ۲۰۱۲ حدود ۴۰ درصد از کاربران اینترنت از گوشی خود بدین منظور استفاده می‌کردند، اما این رقم در سال ۲۰۱۶ با رشدی خیره کننده به ۶۸ درصد افزایش یافته و بر اساس پیش‌بینی‌های Zenith این رقم در سال ۲۰۱۷ به ۷۵ درصد افزایش می‌یابد.

بر همین اساس در حال حاضر از هر چهار دقیقه استفاده از اینترنت سه دقیقه از آن از طریق گوشی‌های هوشمند و دیگر ابزار الکترونیک قابل حمل مانند تبلت‌ها صورت می‌گیرد. این رقم کماکان افزایش خواهد یافت و در سال ۲۰۱۸ به ۷۹ درصد می‌رسد. بنابراین طی بازه زمانی شش ساله از سال ۲۰۱۲ تا سال ۲۰۱۸ شاهد دو برابر شدن استفاده از اینترنت همراه هستیم.

بر اساس گزارش Zenith بیشترین میزان استفاده از اینترنت موبایلی با رقم ۸۵ درصد، مربوط به اسپانیاست. هنگ کنگ با ۷۹ درصد و چین با ۷۶ درصد در رتبه‌های بعدی هستند و آمریکا با ۷۴ درصد در رتبه چهارم است. هند و ایتالیا هم با کاربرد ۷۳ درصدی به طور مشترک در رتبه پنجم هستند.

پیش‌بینی‌ها حاکیست در سال ۲۰۱۸ هنگ کنگ با کاربرد ۸۹ درصدی اینترنت همراه در رتبه اول باشد و چین و اسپانیا با ۸۷ و ۸۶ درصد رتبه‌های دوم و سوم را به خود اختصاص دهند. آمریکا و ایتالیا هم با استفاده ۸۳ درصدی رتبه چهارم و هند با ۸۲ درصد در رتبه پنجم خواهد بود.

منبع:ایتنا

اپل از وب سایت مخصوص افراد معلول رونمایی کرد.

تیم‌کوک، از وب‌سایتی که به طور مخصوص برای افراد ناتوان جسمی ایجاد شده رونمایی کرد که در آن افراد می‌توانند قابلیت‌های محصولات اپل را مرور کنند. وی در ادامه اعلام کرد که امیدوار است تا این وب‌سایت به عنوان یک منبع برای افراد سراسر جهان تبدیل شود.

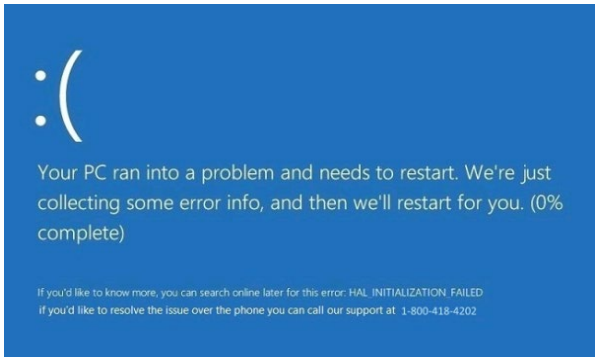
کوک در ادامه افزود: «ما معتقدیم که اگر مردم به محصولات ما دسترسی داشته باشند، می‌توانند قابلیت‌های انسانی خود را ارتقا داده و در مسیر حرکت دنیا، تغییراتی ایجاد کنند.»

این وب‌سایت در واقع شاخه‌ای از وب‌سایت اصلی اپل است. عنوان سایت یاد شده نیز Accessibility بوده که در زیر دسته‌بندی‌ای که Apple Values در پایین وب‌سایت اصلی این شرکت قرار گرفته است. در دسته‌بندی مورد بحث موارد دیگری چون Education، Environment، Privacy، Inclusion And Diversity و Supplier Responsibility نیز به چشم می‌خورند.

منبع:زومیت

nikandroid.com
آموزشگاه تخصصی
برنامه نویسی اندروید

SoftGozar.com



آنتی ویروس جعلی Microsoft Security Essential قربانی می‌گیرد.

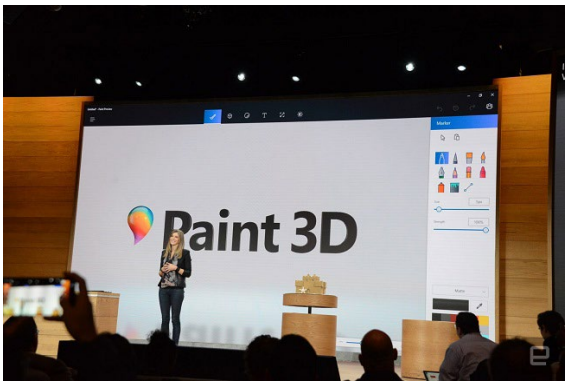
گاهی مجرمین سایبری از شگردهای بسیار جالب و در نوع خود زیرکانه برای فریب قربانیان استفاده می کنند که یکی از تازه ترین آنها به آنتی ویروس Security Essential مربوط می شود. اخیراً یک بدافزار جدید از سوی مایکروسافت شناسایی شده که از طریق نمایش خطای صفحه آبی مرگ (BSOD) جعلی، از کاربران کلاهبرداری می کند.

همانطور که احتمالاً می دانید، در ویندوز ۸ و ۱۰ آنتی ویروس Microsoft Security Essential با Windows Defender جایگزین شده است اما نسخه جعلی این آنتی ویروس بر روی ویندوز ۸ و ۱۰ نیز قابل نصب است. با دریافت و نصب آنتی ویروس جعلی از سوی کاربر از همه جا بی خبر، بدافزار خطای صفحه آبی مرگ جعلی به کاربر نمایش دهد اما خطاهای نمایش داده شده دستکاری شده اند و به کاربر توصیه می شود برای تعمیر رایگان کامپیوتر خود با شماره تماس نمایش داده شده تماس بگیرد. همانطور که می دانید، مایکروسافت هیچ گاه شماره تماس به کاربران ویندوز نمایش نمی دهد، با این حال هیچ بعید نیست بسیاری از کاربران فریب بخورند. با تماس گرفتن کاربر با شماره تماس نمایش داده شده، به دریافت و نصب بدافزارهای بیشتر هدایت می شود که در نهایت به گرفتار شدن در دام باج افزارها و همچنین سرقت اطلاعات می انجامد. با توجه به جدی بودن ماجرا و شدت آلودگی، مایکروسافت به اطلاع رسانی در این باره دست زده است. پیش از هر چیز باید دقت داشته باشید نام فایل اجرایی این بد افزار Setup.exe است، این در حالی است که مایکروسافت از دیگری برای فایل اجرایی نصب آنتی ویروس Security Essential استفاده می کند. همچنین مشخصات و نداشتن امضای دیجیتال می تواند روش دیگری برای پی بردن به آنتی ویروس جعلی باشد.

منبع: شهرسخت‌افزار

برنامه 3D Paint دستیار ساده اما قدرتمند طراحان سه‌بعدی به‌زودی به ویندوز ۱۰ می‌آید.

در حاشیه معرفی ویژگی‌ها و قابلیت‌های جدید به روز رسانی Creators Update برای سیستم عامل ویندوز ۱۰، مایکروسافت نسخه جدیدی از برنامه Paint کهنه کار را معرفی کرد که امکان ساخت اشکال و طرح‌های سه بعدی را بسیار راحت‌تر از قبل می‌کند. 3D Paint برنامه ساده‌ای است است که می‌تواند آینده طراحی اشکال سه بعدی را دچار انقلاب بزرگی کند. برنامه 3D Paint به کاربران گوشی‌های هوشمند و



سیستم‌های دسکتاپ این اجازه را می‌دهد که با اسکن کردن اشیا موجود در طبیعت، از آنها به سادگی طرح‌های سه بعدی ایجاد کنند. این برنامه همچنین امکان ویرایش این طرح‌های سه بعدی را هم فراهم می‌کند.

مایکروسافت برای نشان دادن قابلیت‌های این برنامه با استفاده از یک گوشی هوشمند از یک قلعه شنی کوچک تصویری تهیه کرد. سپس این برنامه مدل سه بعدی زیبایی را از این قلعه ایجاد کرد.

برنامه 3D Paint قابلیت آن را دارد که مدل‌های سه بعدی ایجاد شده را در فرمت‌های مختلفی ذخیره کند تا امکان پرینت سه بعدی از این طرح‌ها ممکن باشد.

مایکروسافت همچنین در برنامه 3D Paint یک فضای ابری فراهم کرده است که کاربران می‌توانند با استفاده از آن به طرح‌های ایجاد شده توسط دیگر کاربران دسترسی پیدا کنند. طرح‌های ایجاد شده توسط این برنامه می‌تواند با استفاده از هدست HoloLens AR به صورت ۳۶۰ درجه مشاهده شود.

طبق اطلاعات منتشر شده از سوی مایکروسافت، نسخه کامل از این برنامه قرار است در به‌روز رسانی Creators Update که در اوایل سال ۲۰۱۷ منتشر می‌شود در دسترس عموم کاربران ویندوز ۱۰ قرار بگیرد.

منبع: Engadget, TheVerge, WccfTech

SoftGozar.com

شماره های قبلی دانشجویار را از دست ندهید...!

۵۰۰۰۰۰

مرتبه دانلود شده

mag.daneshjooyar.com

SoftGozar.com

تخصصی

SoftGozar.com

اندروید؛ خدمتکار یا جاسوس!؟

پوریا انجمنی

اندروید ؛ نیازی به توضیح نیست طبق آمار در ایران تقریبا از هر ۳ نفر ۲ نفر از این سیستم عامل و نرم افزار های آن استفاده میکند و تقریبا همگان آشنایی کامل با آن و برنامه های مختلف آن دارند. بگذارید این بار از یک دید متفاوت به اندروید نگاه کنیم.

فرض کنید در خانه خود نشسته اید و برای هر کار کوچک و بزرگ خود خدمتکاری دارید. هر خدمتکار به راحتی سریع و رایگان به شما خدمت رسانی میکند و شما با خیال راحت در خانه خود به همراه این افراد زندگی میکنید. آنها از همه اطلاعات شما با خبرند و شما به همه انها اجازه داده اید از امکانات خانه استفاده نماید. به نظر عالیست درسته.

حال سوال؟ آیا اگر بخواهید شخصی را به اعضای خانه اضافه کنید چکار میکنید.

مسلما سوالات زیر برای شما پیش می آید؟

۱- این شخص کیست؟ و از کجا آمده است؟

۲- آیا میتواند کاری که از او خواهم خواست انجام دهد؟

۳- آیا آن شخص قابل اعتمادی است و در خانه من مشکلی ایجاد نمیکند؟

۴- چه کسی یا نهادی ضمانت او را می کند که مشکلی ایجاد نکند؟ و .....

حال فرض کنید شخص جدید به عنوان مثال برای آموزش زبان به شما آمده است و در همان ابتدا از شما میخواهد که کلید گاوصندوق اصلی و کمد خانه خود را به او بدهید؟ آیا میدهید؟ چه لزومی دارد یک مدرس زبان کلید در کمد شما یا گاوصندوق شما را داشته باشد. مطمئنا بعد از چنین درخواستی شما به آن فرد مشکوک شده و از استخدام او منصرف می شوید زیرا درخواست غیر معقولی از شما کرده است . حال این مثال چه ربطی به اندروید دارد.

آن خانه دستگاه اندرویدی شماست و آن افراد نرم افزارهای نصب شده بر روی گوشی شما هستند که هر یک وظیفه مشخص خود را دارند. و همه در راستای درخواست های شما کار انجام میدهند. هر کدامشان با توجه به وظیفه ای که انجام میدهند به قسمت های مختلف دسترسی دارند. تمامی امور شما انجام میشود و در صورت نیاز به برنامه ای جدید فورا برنامه را دانلود و در دستگاه خود نصب میکنید. همه چیز به نظر درست است و هیچ مشکلی نیست ....

حال من از شما سوال می کنم؟ فرض کنید یک نرم افزار آموزش زبان انگلیسی نصب کرده اید و هنگام نصب متوجه میشوید این نرم افزار از شما درخواست دسترسی کامل به گالری، مخاطبین، اس ام اس ها و اینترنت را خواسته است ؟ چه می کنید؟ آیا این برنامه را نصب می کنید؟

بگذارید واضح تر بگویم، به عبارتی این نرم افزار توانایی این را دارد که بعد از نصب بدون اجازه شما و حتی بدون شناسایی شدن توسط انتی ویروس و هر نرم افزار امنیتی دیگر تمامی تصاویر ، فیلمها ، مخاطبین ، پیامکها و ... شما را به سازنده خود از طریق بستر اینترنت ارسال نمایید. چرا؟؟ به دلیل اینکه شما در هنگام نصب به این برنامه اجازه دسترسی به تمام منابع خود را داده اید. این

SoftGozar.com

مورد کوچکترین و آسان ترین نوع سودجویی از شما می باشد که مبتدی ترین برنامه نویس اندروید هم میتواند آن را انجام دهد.

در موارد بدتر میتوان به دسترسی مستقیم به دوربین دستگاه دسترسی به حساب های کاربری نرم افزار های مختلف مثل تلگرام و ... ، دسترسی به حساب های بانکی ثبت شده در دستگاه ،دسترسی به موقعیت دقیق شما در هر لحظه و .... اشاره کرد.

طبق آمار تا پایان سال ۲۰۱۵ بیش از ۱,۵ میلیون نرم افزار مختلف برای سیستم عامل اندروید شناسایی شدند که بیشتر از نیازشان به قسمت های مختلف دسترسی داشته اند و درصد بالایی از این برنامه های تنها برای جمع آوری اطلاعات کاربران استفاده می شده اند.

همچنین در یک نظر سنجی مشخص شد به طور میانگین ۸۲ درصد مردم هنگام نصب نرم افزار هیچ دقتی به نوع برنامه، منبع برنامه، و دسترسی های برنامه ، نمی کنند.

یا به عبارتی دیگر اطلاعات ۸۲ درصد مردم فقط و فقط به دلیل سهل انگاری در اختیار افراد سودجو قرار میگیرد.

در بسیاری از موارد مارکت های تا حدودی میتوانند جلوی اینگونه نفوذها را گرفته و اینگونه برنامه ها را انتشار ندهند ولی درصد بالایی از برنامه ها نیز توانایی رد شدن از فیلتر مارکت ها را دارا هستند.

حال راه حل چیست؟ راه حال بسیار ساده است. فقط باید موارد گفته شده زیر را رعایت کنید:

۱- همیشه برنامه های خود را از مارکت های معتبر دریافت کنید

هیچ گاه نرم افزار و یا فایل APK را از اینترنت دانلود و در دستگاه خود نصب نکنید. هیچ گاه نرم افزار هایی که در شبکه های اجتماعی با موضوع آپدیت جدید فلان برنامه منتشر میشوند را نصب نکنید.

۲- در زمان نصب در پنجره ای به شما به صورت واضح میگوید این برنامه به چه قسمتهایی از دستگاه دسترسی خواهد داشت.

برنامه آموزش آشپزی که دسترسی به پیامها و مخاطبین شما را دارد بدون شک جاسوس است. دسترسی کامل به اینترنت تا حدودی بی خطر است اما اگر این دسترسی به همراه دسترسی دیگری باشد به شدت خطرناک است.

۳- هیچ گاه دستگاه اندرویدی خود را ROOT نکنید

در مورد مبحث ROOT کردن در شماره اینده بیشتر صحبت خواهیم کرد. ولی تا این حد بدانید که ROOT کردن دستگاه اندرویدی یعنی دسترسی به اطلاعات و امکانات تمامی قسمتهای دستگاه من برای همه برنامه ها و همه افراد در سطح اینترنت باز است.

۴- همیشه برنامه ها و سیستم عامل خود را به روز نگه دارید

همیشه سعی کنید از آخرین نسخه سیستم عامل و نرم افزار ها استفاده نمایید. زیرا معمولا هر برنامه ای بعد از مدتی دچار مشکلات مختلفی میشود و توسعه دهندگان با ارائه آپدیت های مختلف این مشکلات را رفع میکنند

۵- هیچ گاه به شبکه های وایرلس که نمی شناسید متصل نشوید

شاید جالب باشد بدانید نفوذ به یک دستگاه اندرویدی بدون هیچ گونه فایروال و یا برنامه امنیتی از طریق شبکه وایرلس کمتر از ۵ دقیقه زمان میبرد.

۶- به برنامه های آنتی ویروس و امنیتی اکتفا نکنید

معمولا آنتی ویروس ها و برنامه های امنیتی دستگاه شما را در برابر ویروس ها و برنامه های مخرب شناخته شده محافظت میکنند. نصب چنین برنامه هایی توصیه می شود ولی به معنی محافظت کامل از شما در برابر همه نوع حملات نیست.

۷- اتصال با کابل USB به سیستمهای ناشناخته هرگز

معمولا افرادی هستند که با اتصال دستگاه خود به سیستمهای ناشناخته مثل کافی نت ها و یا سایر سیستمها اقدام به انتقال فایل می کنند. قابل ذکر است در صورت نصب بودن برنامه هایی بر روی سیستم ، به محض اتصال دستگاه شما و یا هرنوع دستگاه ذخیره سازی، بدون اطلاع و اجازه عملیات انتقال همه اطلاعات شروع می شود و ...

۸- کلیک کردن بر روی لینکهای مختلف و ناشناخته ممنوع

بارها شده است که در شبکه های اجتماعی اخباری جالب و یا تبلیغاتی جذاب مشاهده کرده ایم که برای ادامه ما را به کلیک کردن بر روی یک لینک اینترنتی تشویق میکند. در صورت عدم امنیت کافی دستگاه و ورود به این گونه لینک ها احتمال سرقت اطلاعات و یا آسیب به دستگاه بسیار بالا است.

در بالا مهمترین موارد رعایت امنیت دستگاه های اندرویدی گفته شده است هرچند امروزه با پیشرفت علم هر روز یک روش برای سوء استفاده از مردم طراحی میشود اما با رعایت موارد گفته شده میتوان درصد بالایی از این مشکلات را حل کرد.

SoftGozar.com

بخش اول

بررسی حفره های امنیتی وب سایت و مقابله با آن

محمدمهدی محمدی

۱. تزریق به پایگاه داده (SQL Injection) :

تزریق به پایگاه داده (SQL Injection) چیست؟

تزریق به پایگاه داده یا دیتابیس (SQL Injection) نوعی از حملات وب است که در آن فرد حمله کننده یا هکر می‌تواند اقدام به اجرا کردن دستورات دلخواه و مخرب خود بر روی پایگاه داده وب سایت مورد هدف کند. در این حمله، حمله کننده با استفاده از دانش خود (یا تنها با استفاده از یک برنامه ساده!) می‌تواند از نقض‌های امنیتی موجود در کدهای نوشته شده توسط برنامه نویس سایت استفاده کرده و به اصطلاح آن‌ها را اکسپلویت کند. چون در این حمله هکر درواقع به کد اسکیوال، کد دلخواه خود را اضافه می‌کند، تزریق SQL نام گرفته است.

راههای کشف آسیب پذیری (SQL Injection) چیست؟

۱. بررسی QueryString و فرم ها : کدهای فرم صفحه اصلی و دیگر صفحات محتمل را بررسی و تست sql injection را روی پرس و جوهایی که در قالب لینک و یا فرم ارسال داده قرار دارند انجام می دهیم.

۲. استفاده از اسکنر ها: برای کشف حفره های امنیتی میتوانید از اسکنر ها استفاده کنید که سایت رو مورد بررسی قرار میدهند و مشکلات و حفره ها وب سایت رو پیدا میکنند و به ما نمایش میدهند.

۳. بررسی کدهای HTTP واقع در سرآیند: هنگامی که با مرورگر وب سایتی باز می شود در واقع از طریق پروتکل HTTP با سرور ارتباط برقرار می شود و زمانی که درخواستی از طریق این پروتکل به وب سرور فرستاده شود فایل سرآیندی (HTTP Header) در کنار این درخواست به سرور ارسال می شود که در هنگام پاسخ سرور نیز این فایل سرآیند در کنار آن قرار می گیرد تا از صحت اتصال اطمینان به عمل آید. هنگام اتصال به سرور فایل سرآیندی در کنار درخواست ارسالی به سرور و پاسخ های بازگشتی از سرور قرار می گیرد که این فایل سرآیند شامل فیلدهایی می باشد که یکی از آنها کد HTTP می باشد.

انواع حملات (SQL Injection)

واکنش هایی که پایگاه داده ها در هنگام تزریق از خود نشان می دهند باعث شده تا به مرور زمان انواع مختلفی از تزریق ها به وجود آید.

۱. UNION BASED SQL INJECTION (تزریق بر اساس ترکیب دو QUERY) :

نوعی از تزریق که نتایج دو دستور sql از طریق union با هم ترکیب شده و نتیجه یک جا نمایش داده می شود.

SoftGozar.com

۲. ERROR –BASED SQL INJECTION (تزریق بر اساس خطا) :

نوعی از تزریق که عمل تزریق با توجه به خطاهایی که پایگاه داده می دهد طوری انجام می شود که اطلاعات استخراج شود و روال کار به این شکل است که دستوراتی را تزریق می کنیم تا نام ستون و جداول در قالب خطا نمایش داده شود و سپس می توانیم در ادامه تزریق از اطلاعات آنها استفاده کنیم.

۳. BLIND- BASED SQL INJECTION (تزریق کور):

در این نوع تزریق هیچ اطلاعات یا خطایی از طرف پایگاه داده نمایش داده نمی شود و هکر فقط از طریق پاسخ های True/ False که از پایگاه داده دریافت می کند، نتایج را حدس می زند.

از لحاظ تقسیم بندی تزریق کور خود به دو دسته قابل تقسیم است:

۱- Boolean Based : نتایج به شکل True/False می باشد.

۲- Time Based: نتایج به شکل True/False مبتنی بر زمان میباشد.

در هنگام تزریق اگر صفحه وب سایت به درستی نمایش داده شود دستور تزریق شده صحیح (True) و اگر درست نمایش داده نشود غلط (False) می باشد.

در هنگام تزریق اگر وب سایت بعد از تاخیر تعیین شده با استفاده از توابع تاخیر (مثلا ۲ ثانیه) لود شود شرط صحیح (True) و درغیر اینصورت غلط (False) می باشد.

جلوگیری از باگ (SQL Injection) :

در PHP :

۱. همیشه از درستی نوع متغیر ورودی اطمینان حاصل کنید. در زبان PHP انواع متغیرها وجود دارند. می‌توانید با استفاده از توابعی مانند ctype_digit و ctype_alnum و سایر توابع خانواده ctype یا تابع gettype نوع ورودی را کنترل کنید. همچنین می‌توانید با استفاده از (regular expression PCRE) از صحت اطلاعات اطمینان حاصل یابید.

۲. اگر قرار است در دستور SQL عدد وارد شود، با توابعی مانند is_numeric اطمینان حاصل کنید که ورودی حتما عدد است یا همیشه نوع ورودی را با تابعی مانند settype یا intval یا floatval یا ... تغییر دهید.

۳. ورودی‌هایی که از نوع رشته (string) هستند را با توابع پایگاه داده مورد نظر escape کنید (مانند mysql_real_ escape_string یا sqlite_escape_string یا ...) و اگر برای پایگاه داده مورد نظر شما چنین تابعی موجود نیست با استفاده از توابعی مانند addslashes یا str_replace این کار را انجام دهید. این عمل باعث می‌شود تا کاراکتری مانند در ساختار SQL تاثیری نگذارد و ورودی به عنوان متغیر به دستور داده شود و تاثیری بر دستور نداشته باشد.

۴. استفاده از stored procedures یکی از بهترین روش‌های جلوگیری از SQL Injection در پایگاه داده‌هایی است که این قابلیت را دارند. اما متاسفانه همه پایگاه‌داده‌ها این قابلیت را ندارند.

۵. سعی کنید در هیچ شرایطی خطای رخ داده در پایگاه داده

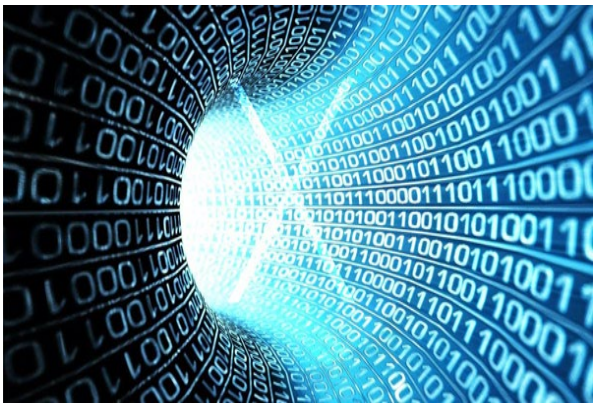
SoftGozar.com

به کاربر نشان داده نشود، چراکه نمایش این خطاها می‌تواند به حمله‌کننده این امکان را بدهد که بداند چه اتفاقی در پایگاه داده انجام گرفته است. در PHP راه‌های مختلفی برای جلوگیری از نمایش خطاها وجود دارد. یکی از معروف‌ترین آنها استفاده از عملگر @ قبل از دستورالعمل مورد نظر است. هنگامی که از این عملگر استفاده شود، PHP از پیام‌های خطای دستور مورد نظر صرف نظر می‌کند.

در ASP.NET:

۱. از ورودی‌ها اطمینان حاصل کنید. سعی کنید تا جای ممکن تمامی ورودی‌ها را از لحاظ نوع داده، طول رشته ، بازه عددی و سایر موارد کنترل کنید. برای این کار می‌توانید از Regex RegularExpressionValidator،یا RangeValidator استفاده کنید.

۲. استفاده از ورودی‌ها در Stored Procedure ها راه بسیار مناسبی است. توجه داشته باشید که استفاده از Stored Procedure ها بدون استفاده از ورودیباعث جلوگیری از SQL Injection نمی‌شود. برای این کار می‌توانیداز SqlParameter



و SqlParameterCollection استفاده کنید.

همچنین درصورتی که مجبور به استفاده از دستورات پویا (Dynamic) هستید،بااستفاده‌از SqlParameterCollection نوع ورودی‌ها را مشخص کنید.

۳. سعی کنید تا جای ممکن از API هایی مانند ADO. Net و قابلیت‌های آن استفاده کنید، چرا که با کمک این رابط‌های برنامه‌نویسی می‌توان نوع دقیقداده‌ها را مشخص کرد و همچنین این اطمینان را داشت که ورودی‌ها به طرزصحیحی Escape می‌شوند.

ادامه دارد...

SoftGozar.com

ضرورت طراحی صفحه‌فرود اختصاصی یا Landing Page برای سایت

حسین جلیلی

landing Page به صفحه ای گفته میشود که کاربر بدون هیچگونه جستجویی ، محتوای مورد نظر خود را در سایت شما پیدا کند ، به عبارتی دیگر توجه کاربران را به محتوای مورد نظر آنها که به خاطر آن وارد سایت شما شده اند جلب کنید .

شما در گوگل و یا هر سایت دیگری تبلیغ می دهید و تعداد بسیار زیادی بازدید کننده را به صفحه ی اول سایت خود ارجاع می دهید ، این یعنی موج بزرگی از بازدید کننده ها که برای آنها تبلیغ هدفمند نمی باشد و فقط معرف یک سایت جدید می باشد.

اگر شما با تغییر روند کاری خود بتوانید بازدید کننده ها را به یک صفحه ی هدفمند و مهم هدایت کنید میتوانید در فروش محصول خود و یا حتی در معرفی سایت خود بیشتر از پیش موفق شوید.

بررسی صفحه فرود برای کمپین ها:

۱. صفحه فرود شلوغ: مورد بسیار مهم ، در طراحی صفحه فرود طراحی مختصر و مفید است. هرچقدر تعداد لینک‌ها و گزینه‌های پیش روی کاربر کمتر باشد، هدف کمپین متمرکزتر می‌شود و در نتیجه به هدف نزدیکتر می‌شوید. قرار دادن لینک‌های زیاد در این صفحه فرود، تجزیه تحلیل و زدن هدف را تقریبا غیرممکن کرده است.به دیگر نمونه صفحه فرود که در مقالات دیگر نمونه موردی معرفی کرده‌ایم نیز نگاهی بیاندازید.

۲. گنگ بودن موضوع فعالیت سایت: طراحی صفحه فرود باید به گونه‌ای انجام شود که کاربر در کوتاه‌ترین زمان ممکن متوجه موضوع و فعالیت وب‌سایت شود و اکشن مورد نظر آگهی دهنده (ثبت نام، خرید، اطلاع رسانی و ...) را انجام دهد.

۳. پیروی از چندین هدف: توجه داشته باشید که در طراحی بنر و صفحه فرود از یک و یا نهایتا دو هدف پیروی کنید. به عنوان مثال: برندینگ و در پایین صفحه دریافت ایمیل کاربر.

منبع : http://saniyeShomar.ir

#daneshjooyar

SoftGozar.com

Virtual School
مدرسه مجازی دانشجویار

عرفان اکبری منش

اگر از دنبال کنندگان دانشجویار باشید حتما این نکته براتون قابل توجه بوده که دانشجویار در مدت ۴ ساله فعالیتش مدام سعی در بهبود فضای آموزش مجازی و ارتقا دانشجو و مخاطبانش از طریق دوره های آموزشی داشته است.

امروز بعد از کسب تجربه ای که در برخورد با حدود ۵۰۰۰۰ مخاطب و ۳۰۰ مدرس کسب کردیم به این نتیجه ی رسیدیم : کاربر با خرید یک پکیج آموزشی و یا مشاهده و دانلود یک دوره آموزشی به تنهایی ، بازدهی بیشتر از ۳۰ درصد را نخواهد داشت ، (این بازدهی در واحد زمان و تخصص سنجیده شده است) و جهت ورود به بازار کار و کسب تجربه ی عملی و تخصصی ، نیاز به پیگیری ، راهنمایی ، مشاوره و آموزش بیشتری خواهد داشت.

اهمیت این مشاوره و راهنمایی زمانی نمایان می شود که یک فرد در شروع کار با انبوه پیشنهادها ، زبان های برنامه نویسی و تکنولوژی ها مواجه می شود، و نمی تواند میان آنها انتخاب کند و گاها به دنبال یادگیری چندین زبان متنوع رفته و زمان بسیاری را صرف آموزش کرده که در نهایت نتیجه ای در بر نداشته ، یک فرد نمی تواند و نباید همه ی زمینه ها را دنبال کند به همین دلیل وجود یک مشاور با سابقه می تواند به راحتی از این موارد جلوگیری کند.

مشاوری که بر خود لازم میداند به شما خدمت کند و همراه و همگام با شما همراه با طرح و برنامه پیش برود.

ممکن است شما هم جزو آن دسته از افرادی باشید که تشویق دیگران بر مسیر پیشرفت شما تاثیر مثبتی میگذارد و این لازمه ی حضور یک همراه در این جاده ی پر از پیچ و خم است .

تقریبا کمتر از ۱۴ روز است که از شروع کار مدرسه مجازی گذشته و ما با سیل عظیمی از درخواست ها مواجه شدیم قریب به ۲۰۰ نفر در این روز های گذشته در دوره های مختلف مدرسه ی مجازی ما فرم نویسی و ثبت نام کرده اند که تاکنون با لغ بر ۱۷۰ نفر از این تعداد ساماندهی شده و همچنان روند ساماندهی ادامه دارد .

شمای کلی از مدرسه ی مجازی ما را در تصویر زیر می بینید :

این روند منظم حاصل برنامه ریزی و تلاش های شبانه روزی تیم مدیریت و پرسنل دانشجویار بوده که به عنایت و لطف خداوند ، نتیجه ی رضایت بخشی در بازخورد اولیه این سامانه حاصل گردید و این موضوع ما را در توسعه ی مدرسه ی مجازی مصمم تر کرد .

برای شفاف تر شدن این مسئله و همچنین آگاهی یافتن شما درباره مدرسه ی مجازی دانشجویار ، اطلاعات و آمار کلی از جزئیات این سامانه را افشا میکنیم .

تعداد کل ثبت نام کنندگان در مدرسه ی مجازی : ۲۰۰ نفر (تاکنون)

تعداد افراد تایید شده جهت شروع کار : ۱۷۲ نفر

تعداد متخصصین تحت عنوان پشتیبان : ۲۲ نفر

بیشترین درخواست ها از سمت کاربران مربوط به دوره های ذیل می باشد :

برنامه نویسی وب با PHP, ASP.NET

برنامه نویسی پیشرفته C# و ASP MVC

برنامه نویسی موبایل با زبان جاوا

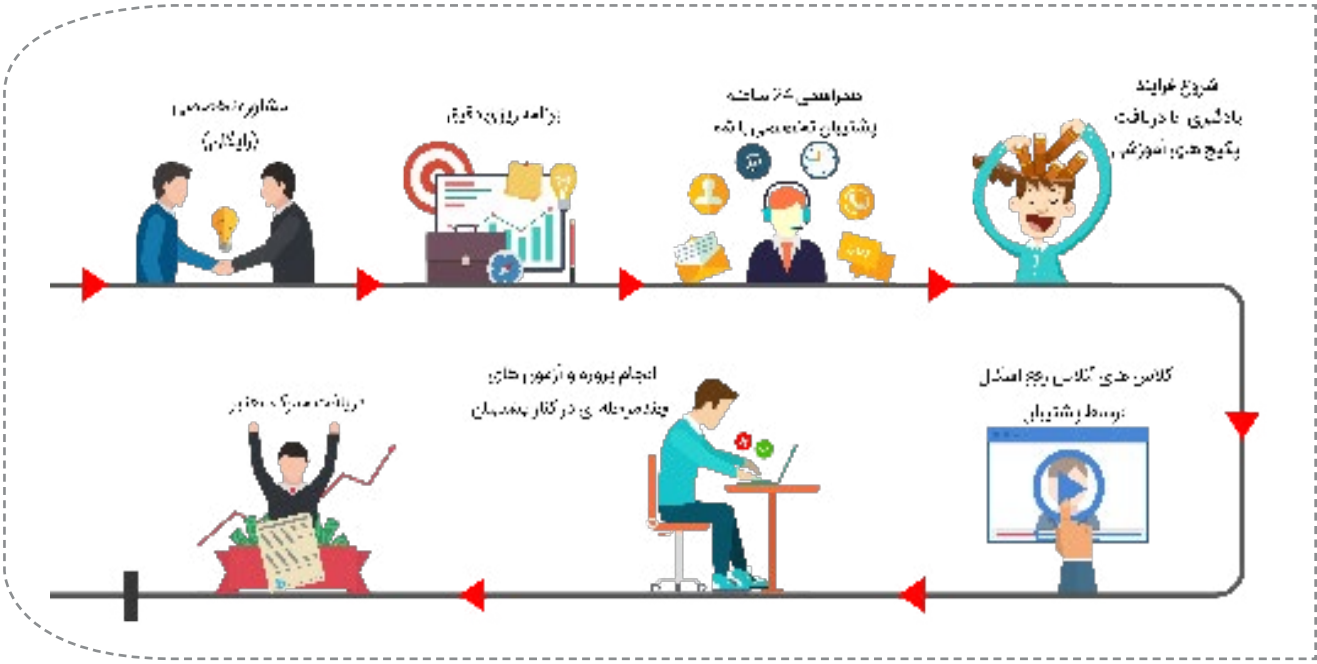
تعداد افراد شرکت کننده در دوره های جاری ما :

طراحی وب استاتیک (مهارت های پایه وب) : ۱۶ نفر

برنامه نویسی در قالب پلتفرم Asp.net : ۲۷ نفر

برنامه نویسی سمت سرور با PHP : ۳۰ نفر

SoftGozar.com



شروع مجدد ثبت نام نیمه دوم آبان ماه

برنامه نویسی تحت ویندوز به زبان C# : ۲۸ نفر

برنامه نویسی اپلیکیشن های موبایل با زبان جاوا : ۲۹ نفر

مباحث مرتبط با شبکه های کامپیوتری : ۲۰ نفر

زبان برنامه نویسی Go : ۵ نفر

زبان برنامه نویسی Python : ۳ نفر

هوش مصنوعی : ۲ نفر

زبان برنامه نویسی Scala : ۲ نفر

طراحی اپلیکیشن موبایل با React Native : ۴ نفر

تحلیل پایگاه داده به طور پیشرفته : ۱ نفر

SoftGozar.com

بپرس ، بدون

سوال: آیا اهمیتی دارد که از Safely Remove Devices در هنگام جداسازی حافظه خارجی از سیستم استفاده کنیم ؟

جواب: اگر در حالی که ویندوز در حال خواندن اطلاعات و داده ها از USB است آن را از سیستم جدا کنید یکی از آسیب هایی که ممکن است پیش بیاید این است که اطلاعات شما از بین می روند یا حافظه خارجی شما دچار مشکل شود . سیستم‌عامل شما الزاما به محض اینکه فایلی را درون حافظه‌ی خارجی کپی می‌کنید به نوشتن آن بر روی حافظه نمی‌پردازد؛ بلکه گاهی ابتدا با کش کردن آن، منتظر چند دستور کپی دیگر نیز می‌ماند تا همگی آن‌ها را یک‌جا اجرا کند. در بعضی از USB ها هنگامی که آنها در حال پردازش اطلاعات هستند یک چراغ چشمک زن بر روی آنها شما را از درگیر بودن آن آگاه می کند اما در دستگاه هایی که این ویژگی را ندارند بهترین کار این است که از همان گزینه Hardware استفاده کنید . در این حالت اگر برنامه ی باز یا در حال پردازشی وجود داشته باشد بعد از اتمام آن سیستم اجازه ی جدا کردن دستگاه را می دهد و این جلوی آسیب ها را می گیرد چرا که آگاهی از اینکه ویندوز یا یک برنامه کاربردی در پشت صحنه در حال کار است همیشه هم ساده نیست .

سوال: چگونه میتوان در اینستاگرام، جلوی نمایش خودکار ویدئوها راگرفت؟ آیا راه حلی برای غیرفعال کردن این امکان وجود دارد؟

جواب: با این که پیش بینی می شد قابلیت نمایش خودکار ویدئوها در اینستاگرام مورد استقبال کاربران قرار گیرد اما بسیاری از کاربران از این ویژگی ابراز نارضایتی کرده اند. در واقع این دسته از افراد تصور می کنند که این امکان تنها برای این منظور شکل گرفته تا میزان بازدیدها را به طور خودکار افزایش دهد. به هر حال برای غیر فعال کردن این ویژگی تنها برای زمانی که شما از اینترنت دیتا استفاده می کنید، راه حلی وجود دارد که به ترتیب موارد زیر می توانید به آ نها عمل کنید:

۱. اینستاگرام را باز کنید و به صفحه پروفایل خود (دکمه ابتدایی از سمت راست) وارد شوید.

۲. سپس به بخش تنظیمات بروید. برای مراجعه به تنظیمات در اندروید دکمه سه‌نقطه عمودی در بالای صفحه و در آیفون دکمه چرخدنده را لمس کنید.

۳. در صفحه تنظیمات Cellular Data Use را انتخاب کرده و گزینه Use Less Data را فعال کنید.

.به این ترتیب بارگذاری خودکار ویدئوها هنگامی که از اینترنت سیم‌کارت استفاده می‌کنید متوقف شده و حجم کمتری از اینترنت شما مصرف خواهد شد. این عملیات همچنین باعث می‌شود برخی تصاویر هنگام ورود به اینستاگرام پیش‌بارگذاری نشود و به این ترتیب تاحد امکان از مصرف حجم اینترنت شما جلوگیری خواهد شد. توجه کنید که راهی برای پیشگیری از بارگذاری ویدئوها هنگام استفاده از اینترنت وای‌فای وجود ندارد.

با هدف شناسایی و معرفی استعدادهای علاقه مندان به حوزه کامپیوتر و برنامه نویسی و با نیت انتقال دانش و تجربیات شخصی از کلیه علاقه مندان در سراسر ایران دعوت به همیاری می نماید .
عزیزان علاقه مند می توانند مقالات خود را در کلیه زمینه های مربوط به علوم کامپیوتر و الکترونیک ، گرافیک و ... به نشانی پست الکترونیک Mag@daneshjooyar.com ارسال نمایند تا با نام خودتان در مجله به چاپ برسد .

کلیه مقالات واجد شرایط ، با رعایت اولویت و ترتیب ، در مجله به چاپ خواهند رسید.

SoftGozar.com

ترفندوب

چطور پسوردهای ذخیره شده در کروم را ببینیم؟!

یکی از دغدغه های اکثر کاربران فراموشی پسوردهای وارد شده هنگام عضویت در وب سایت ها است . هر چند همه سایت ها با گذاشتن گزینه بازیابی رمز عبور این امکان را فراهم کرده اند و پسورد را با طی مراحلی به ایمیلی که به هنگام ثبت نام به آن سایت داده اید ارسال می کند اما روش ساده تری برای مشاهده پسوردهای ورودی سایت ها وجود دارد.

در مرورگر کروم می توانید وارد تنظیمات آن شده و از قسمت سمت راست صفحه عنوان Password and Forms را پیدا کرده در صورتی که تیک گزینه Offer to save your web passwords فعال باشد با کلیک روی گزینه Manage Passwords پنجره ای باز می شود که شامل لیست سایت هایی است که پسورد آن ها را در مرورگر ذخیره کرده اید همانطور که مشاهده می کنید با کلیک روی هر کدام از سایت ها می توانید به نام کاربری و پسورد آن سایت به راحتی دست پیدا کنید .

ناگفته نماند که این یکی از راههای بازیابی پسورد ورودی سایت ها است .

ترفندویندوز

شاید برای شما پیش آمده باشد که فلش مموری خود را قفل کرده باشید و نتوانید آن را فرمت کنید یا اینکه به دلیل ویروسی شدن قادر به فرمت نمی باشید و یا به هر دلیلی فرمت کردن فلش شما به یک مشکل بزرگ تبدیل شده است . خب در این مواقع چاره کار چیست ؟!

مرحله اول : فلش مموری خود را وصل می کنیم . اگر فلش مموری ویروسی باشد فلش مموری را باز نکنید .

مرحله دوم : ابتدا Run را اجرا کرده و سپس در کادر باز شده عبارت Cmd را تایپ کنید و وارد بخش Cmd شوید .

مرحله سوم : دستور زیر را می نویسیم .

در این جا ما فرض کرده ایم درایو فلش شما مثلاً G می باشد و فرمت ما از نوع Fat32 (بهترین حالت فرمت برای فلش) می باشد .

Format G: /FS: FAT32 پس اگر درایو فلش شما چیزی غیر از این بود، به جای عبارت G نام حرف انگلیسی درایو فلشتان را با حروف بزرگ وارد کنید .

مرحله پنجم: کلید اینتر را بزنید .

این نوع فرمت کردن تمام درایو و یا حافظه فلش مموری را خالی و پاک سازی می کند و در آخر فلش مموری شما کاملا به صورت ۱۰۰% فرمت شده است .

معرفی سایت

متون خود را به راحتی در قالب اسلاید در بیاورید

اگر شما هم از آن دسته از افرادی هستید که به دلیل نداشتن وقت یا هم عدم آشنایی با نرم افزارهای ساخت اسلاید به دنبال روشی سریع و راحت برای ساخت اسلاید پروژه ها و ارائه پایانه نامه خود هستید ، پیشنهاد می کنیم حتما به این سایت سر بزنید و از امکانات فوق العاده آن بهره مند شوید.

www. slides.com

اسنپ را بیشتر بشناسید

دنبال یک راه ساده و سریع برای درخواست خودرو هستید؟ اسنپ را از دست ندهید. با اپلیکیشن اسنپ شما تمامی رانندگان اطرافتان را به صورت زنده می‌بینید. فقط کافیست مبدا و مقصدتان را مشخص کرده و درخواست اسنپ دهید تا نزدیک‌ترین خودرو شما را تا مقصد همراهی کند. به وسیله پرداخت آنلاین و اعتباری دیگر نیازی به پول نقد نیست و شما به راحتی می‌توانید هزینه سفر خود را از طریق کارت اعتباری و افزایش اعتبار حساب کاربری خود پرداخت کنید. در حال حاضر اسنپ فقط در شهر تهران فعال است.

www.snapp.ir

مدیریت پروژه آنلاین برای شرکت‌ها

سیستمی آسان برای مدیریت منعطف کارها، گفتگوی آنلاین، ثبت زمان‌های کاری و ارتباط دوطرفه با سایر سرویس‌های آنلاین. تسکولو به شما کمک میکند که مدیریت پروژه‌های خود را به شیوه ای متفاوت مدیریت کنید به طوریکه که بالاترین بازدهی را از کاری تیم خود داشته باشید .

www.taskulu.com

از آخرین تخفیف ها مطلع باشید

تخفیف گرفتن هنگام خرید یک محصول چیزی هست که می تواند مشتری را ترغیب به خرید آن بکند . این سایت بستری است برای ارائه تمامی انواع خدمات و محصولات مورد استفاده در زندگی روزمره. خدماتی شامل انواع رستوران‌ها، مراکز تفریحی، مراکز بهداشتی و آموزشی، سفر تا انواع کالاها و محصولات متنوع ، که با سر زدن به آن می توانید به راحتی کالای موردنظر خود را با تخفیف خریداری کنید.

www.takhfifan.com

SoftGozar.com

#لطفا_با_فرهنگ_باشیم

سهیلا هادی نیا

فرهنگ اون چیزیه که مردم باهاش زندگی می کنن. در واقع فرهنگ کیفیت زندگی افراد یک جامعه است که با آموزش از نسلی به نسل بعد منتقل میشه. «فرهنگ عمومی» قلمرو یا بُعدی از فرهنگ تعریف میشه که رابطه مستقیم با عموم مردم داره، مثل شکل لباس یا معماری، وجدان کاری یا احترام به بزرگترها. پشت فرهنگ عمومی هیچ اجبار یا قانونی نیست و پایه و اساس اون پذیرش عموم مردم جامعه است. باید توجه داشته باشیم که فرهنگ عمومی تأثیرش بر عامه مردم هست و عموم مردم نسبت به اون شناخت و حساسیت دارن.

قبول فرهنگ پیشینیان یک جامعه صرفاً به خاطر جا افتادن این فرهنگ و بدون هیچ استنباط منطقی، برای نسل جدید اون جامعه پذیرفته‌شده نیست و اصولاً طبیعت انسان با توجه به تغییرات شکل فکری نسل‌ها، این و قبول نمی کنه. باید این و در نظر بگیریم که یک جاهایی بنا به ضرورت و نیاز باید این فرهنگ تغییر کنه. تغییر فرهنگ کار ساده‌ای نیست و نیاز به تحقیق و تحلیل‌های تخصصی داره، اما اگه فرد از خودش شروع کنه میتونه یک گام بزرگ در اصلاح تغییر یک فرهنگ غلط برداره.

بزارید براتون یک مثال بزنم؛ شمایی که بنا به نیازتون دارید وقت زیادی رو در فضای مجازی و اینترنت می گذرونید، حتماً با موارد این‌چنینی زیاد برخورد کردید: دانلود رایگان آهنگِ ...، دانلود رایگان کتابِ ...، دانلود رایگان نرم‌افزار ...، دانلود رایگان فیلمِ...، دانلود رایگانِ...! نکته ابهام برانگیز اینجاست که ممکنه در همین منابع با جمله: حق قانونی برای شخص یا اشخاص حقیقی یا حقوقی محفوظ است، روبرو بشید!

«حق نشر، تکثیر یا کپی‌رایت» مجموعه‌ای از حقوق انحصاری مادی و معنوی است که به ناشر یا پدیدآورنده یک اثر اصل و منحصربه‌فرد تعلق می گیره. اگر کسی قانون کپی‌رایت رو در مورد اثر دیگران رعایت نکنه، صاحب اثر میتونه به صورت قانونی شکایت و اون شخص و مورد پیگرد قانونی قرار بده.

متأسفانه الان می‌بینیم، اکثر افراد جامعه ما، این مساله براشون فرهنگ شده که میتونن حق کپی‌رایت یک آهنگ، کتاب، فیلم و یا ... نقص کنن؛ فقط چون امکان تهیه اون به صورت اورجینال و ندارن مثل خیلی از نرم‌افزارها، یا به‌راحتی و فراوانی در منابع مختلف و اینترنت قرارگرفته و در دسترسه پس چه فرقی می کنه من یک نفر بخوام اون و به صورت اورجینال تهیه کنم یا به نظر شخصیشون قیمت بالایی داره، بدون اینکه از پشت پرده‌های هزینه‌های مادی و معنوی که صرف تهیه این اثر شده اطلاعی داشته باشن. اصلاً ما حقی برای قضاوت درباره درآمد حاصل از این اثر و داریم؟

علاوه بر خسارات مالی که با نقص قانونی کپی‌رایت به صاحب اثر وارد میشه، خسارات معنوی این عمل گاهی جبران ناپذیره. احترام نداشتن به مالکیت ایده افراد، یک حفره فرهنگی بزرگه

SoftGozar.com

و باید بدونیم که مالکیت یک اثر به اندازه مالکیت اموال فیزیکی و دارایی‌های مالی اهمیت داره. شاید صاحب اثر بتونه با پیگیری قانونی که زمان‌بر و پرهزینه است خسارت مادی این نقض قانون و جبران کنه اما خسارت معنوی اون چطور قابل جبرانه؟ حالا این و در نظر بگیرید که صاحب اثر شاید بارها مجبور باشه این شکایت و پیگیری کنه. حتی فکر می‌کنم گاهی این نقض قانون به دلیل ضعف قانون و برخوردهای قانونیه. افراد وقتی این ضعف و می بینن با خاطری آسوده قانون کپی‌رایت و نقض می کنن.

شورای فرهنگ عمومی، ۱۴ آبان رو در تقویم به نام « روز فرهنگ عمومی» نام‌گذاری کرده. بیاین برای تغییر یک فرهنگ غلط، از همین امروز شروع کنیم. بذاریم افراد فعال و خلاق برای پیشرفت و خلق ایده‌های نو در زمینه‌های مختلف با خاطری آسوده کار کنن و انگیزه و امید حمایت داشته باشن. با حمایت از اونها درصدی هرچند ناچیز در پیشرفت جامعه سهم داشته باشیم. حقوق مادی و معنوی یک اثر و رعایت کنیم، نه برای ترس از قانون، نه برای تظاهر به باکلاس بودن یا هر دلیل غیرموجه دیگه. به خودتون این اجازه رو بدید که مروج یک فرهنگ اخلاقیِ درست یا همون فرهنگ احترام به حقوق دیگران باشید. بیاین کاری کنیم حق کپی‌رایت بجای قانون به فرهنگ عمومی تبدیل بشه...بخاطر خودمون، صاحب اثر، جامعه و نسل بعد.

۱. دانشنامه آزاد ویکی‌پدیا
۲. سایت موسسه فرهنگی و اطلاع‌رسانی تبیان
۳. نقض مالکیت معنوی: بردی کوچک، باختی بزرگ؛ محمدرضا شعبانعلی
۴. قانون کپی‌رایت و فرهنگ رعایت آن؛ سالار کابلی

SoftGozar.com

نظرات، انتقادات و پیشنهادات خود را
جهت هرچه بهتر شدن کیفیت مجله
با ما در میان بگذارید.

شماره پیامک: ۳۰۰۰۲۲۲۳۳۲۱۱۵

آی دی تلگرام: @daneshjooyar_admin

همچنین می توانید با استفاده از این راههای ارتباطی سوالات خود را در زمینه های
مختلف علوم کامپیوتر مطرح کنید تا ما در بخش بپرس بدون مجله به سوالات شما
به طور کامل پاسخ دهیم .

کانال دانشجویار را دنبال کنید

جدیدترین اخبار سایت ،مطالب کاربردی ، آموزش های پروژه محور و ...

@daneshjooyar

SoftGozar.com

برگزاری رویداد

«ارائه استارتاپ های حوزه فناوری اطلاعات به سرمایه گذاران»

در پارک فناوری پردیس

با توجه به چشم اندازهای معاونت علمی ریاست جمهوری و اهداف پارک فناوری پردیس، در جهت حمایت از کسب و کارهای نوظهور و خصوصا دانش بنیان، نشست تخصصی ارائه استارتاپ های حوزه فناوری اطلاعات، ۵ آبان ماه در پارک فناوری پردیس برگزار خواهد شد.

این رویداد در قالب ارائه استارتاپ ها به سرمایه گذاران است، که در ساختمان سراج پارک فناوری پردیس برگزار خواهد شد. در این رویداد سرمایه‌گذاران برتر این حوزه از جمله شرکت خدمات اول مخابرات، موسسه مبنا و همچنین ۱۲ استارتاپ منتخب حضور خواهند داشت. این ارائه دهندگان از بین حدود ۷۰ استارتاپ و فعال حوزه فناوری اطلاعات انتخاب شده اند.

حاصل رویداد هایی به این سبک، عقد قرارداد و ایجاد بستر مناسب ارائه و اتصال سرمایه به مولدین بالقوه بازار فناوری اطلاعات کشور است.

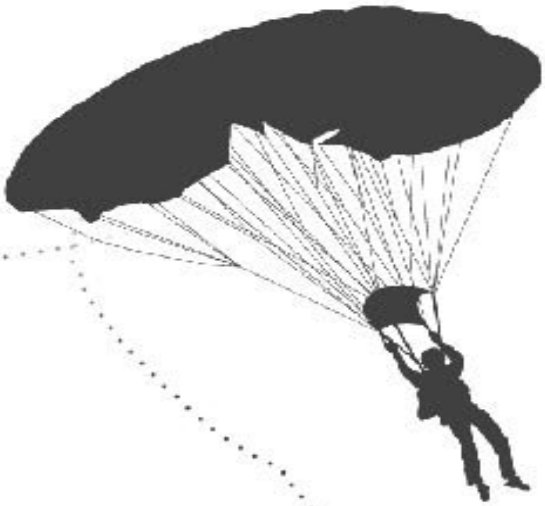
این رویداد ساعت ۹ صبح ۵ آبان سال جاری در در محل ساختمان سراج پارک فناوری پردیس برگزار خواهد شد.

SoftGozar.com

آیا کلمه عبور شما واقعا از شما محافظت می کند؟

پسوردها به عنوان استراتژی نظامی پدیدار شدند

قبل از کامپیوترها، پسوردها توسط سربازان در جنگ جهانی دوم استفاده می شدند.



چتربازان آمریکایی از پسوردها و ضد پسوردها به عنوان روشی برای شناسایی در نبرد نرماندی در سال ۱۹۹٤ استفاده کردند.

ضد پسورد به صورت پرسش و پاسخ استفاده می شد. (مثال: فرمانده میگفت برق و سربازان باید میگفتند رعد.)

در طول جنگ جهانی پسوردها و ضد پسوردها هر ۳ روز تغییر می کردند.

SoftGozar.com

ابداع شده بوسینه
رابرت هوریس

پسوردها به آن شکل که ما امروز آنها را می شناسیم تا سال ۱۹۷۲ ابداع نشده بودند و تا سال ۱۹۷۴ به کار گرفته نشدند.

حریم خصوصی شما به شدت بر محافظت با استفاده از کلمات عبور وابسته است

- رمز خودپرداز بانک
- رمز سیم کارت تلفن همراه
- دسترسی به کامپیوتر
- حساب ایمیل
- بانکداری الکترونیکی
- پسورد شبکه WiFi
- حساب شبکه‌های اجتماعی
- رمز سیستم امنیتی
- تمامی وب سایت‌های محافظت شده با پسورد

استفاده از پسوردهای مختلف یک الزام است

SoftGozar.com

یک فرد معمولی به طور متوسط ۲۵ وب سایت محافظت شده با پسورد را مشاهده می‌کند
ولی تنها از ۶ پسورد متفاوت استفاده می‌کند

۷۳٪

از مردم از پسورد مشابه برای سایت‌های
مختلف استفاده می‌کنند

۳۳٪

از مردم از یک پسورد برای هر وب سایتی
استفاده می‌کنند

۳۲٪

از مردم پسورد و سایر اطلاعات ورود
به حساب‌های کاربری را در
گوشی همراه خود ذخیره می‌کنند

۶۲٪

از صاحبان گوشی‌های هوشمند
از رمز عبور برای محافظت از
گوشی خود استفاده نمی‌کنند

اغلب مردم از پسوردهای ضعیف استفاده می کنند

کلمات عبور پیچیده کلید امنیت هستند
و بسیار سخت تر شکسته می شوند

SoftGozar.com

٤٪

از مردم عبارت password را به عنوان کلمه عبور خود استفاده می‌کنند

۲۵٪

از ۲۰ پسورد متداول برتر، اسامی کوچک است

۳ دقیقه

یک هکر حرفه‌ای می‌تواند پسوردهای معمولی را در کمتر از ۳ دقیقه بشکند

۵٪

از مردان نام شریک زندگی خود را در کلمات عبور استفاده می‌کنند

۳۰٪

از زنان نام شریک زندگی خود را در کلمات عبور استفاده می‌کنند

۶

میانگین طول پسوردها ۶ حرف است که همگی حروف کوچک هستند

۱۰ پسورد ضعیف سال ۲۰۱٤

۱. ۱۲۳٤٥٦
۲. password
۳. ۱۲۳٤٥
٤. ۱۲۳٤٥٦۷۸
٥. qwerty
٦. ۱۲۳٤٥٦۷۸۹۰
۷. ۱۲۳٤
۸. baseball
۹. dragon
۱۰. football

SoftGozar.com

بایدها و نبایدها در ساختن یک کلمه عبور

بایدها ۷

۱

****

طول کلمه‌عبور خود را ۸ حرف و یا بیشتر کنید

هر طولی کمتر از این ضعیف تلقی می‌شود

۲

ABC abc 123 @$&

از ترکیبی از تمام ٤ نوع حروف استفاده کنید

حروف کوچک، حروف بزرگ، اعداد و کاراکترهای خاص

۳

مثلا: ToBeMan۵$Bedehkari

پسوردی انتخاب کنید که به خاطر می‌سپارید

پسورد مستحکمی که اغلب فراموش می‌کنید به کار شما نمی‌آید

٤

خیلی مستحکم ★★★★★

پسورد خود را تست کنید

سایت‌های ایمن زیادی هستند که استحکام پسورد شما را بررسی می‌کنند
و پیشنهادهایی به شما می‌دهند تا پسورد خود را قوی‌تر کنید

۵

۰۹۳۵۲۲۲۳۳٤٤

یک روش بازیابی کلمه عبور تنظیم کنید

روش بازیابی با موبایل مناسب است چرا که گوشی تلفن همراه
شما به صورت فیزیکی در اختیار شما قرار دارد

۶

سال/۲بار

کلمه عبور خود را ۲ بار در سال تغییر دهید

SoftGozar.com

نبایدها

استفاده از اطلاعات عمومی

نام شما، تاریخ تولد، نام فرزندان، نام همسر و غیره
به صورت عمومی در دسترس هستند
و هکرها از آنها برای حدس زدن پسورد شما استفاده می‌کنند

استفاده از کلمات کامل

پسوردهایی که از کلمات کامل استفاده می‌کنند، به شکل قابل ملاحظه‌ای راحت‌تر شکسته می‌شوند

نوشتن پسورد در جایی

از نوشتن پسورد خود روی کاغذ خودداری کنید. مخصوصا بر روی کاغذ یادداشت‌های چسبان
اگر مجبور شدید پسورد خود را بنویسید به جای پسورد یک یادآوری بنویسید

استفاده از یک پسورد برای چندین حساب

این کار باعث می‌شود همه چیز یکجا برای مجرمان اینترنتی فراهم شود

لاگین کردن به حساب‌های شخصی از کامپیوترهای عمومی

اطلاعات شما ممکن است ثبت شوند و یا فراموش کنید از حسابتان خارج شوید

گفتن پسورد خود به کسی

شما و فقط شما تنها کسی هستید که باید پسوردتان را بداند

برای محافظت در مقابل مجرمان فضای مجازی همیشه از کلمات عبور مستحکم استفاده کنید.
برای نکات امنیتی بیشتر لطفا سایت جاکلید را مرور کنید.

www.infograph.ir
نخستین مرجع تخصصی اینفوگرافیک به زبان فارسی
SoftGozar.com

جامع ترین آموزش

صفر تا صد

افزونه نویسی وردپرس

را از دانشجویار بخواهید...

daneshjooyar.com
nikandroid.com
matlabyar.com

SoftGozar.com