کامپیوتر کاغذی

ماهنامهٔ علمی_اطلاع رسانی انجمن علمی کامپیوتر
دانشگاه الزهرا(س) مشهد_سال اول_خردادماه ۱۴۰۱

۱

در اولین شماره می‌خوانیم:

وی.پی.اس و وی.پی.ان

وی‌پی‌اس همانند کامپیوتری است که کیس آن در مکانی با زیرساخت‌های استاندارد و قدرتمند و مانیتور و کیبورد و موس آن در منزل شما قرار گرفته است و آن را از راه دور...

احراز هویت بیومتریک

در دنیای کنونی و پیشرفت چشمگیر تکنولوژی مسئله امنیت و حریم خصوصی برای همه افراد اهمیت بسیار زیادی دارد. با افزایش جرایم اینترنتی، کلاهبرداری و ...

استارلینک

بسم الله الرحمن الرحیم

نشریهٔ انجمن علمی کامپیوتر دانشگاه الزهرا مشهد

@ALZAHRA_CLUB_COMPUTER

دانشکده فنی و حرفه‌ای الزهرا مشهد

@ALZAHRA_CLUB_COMPUTER

کامپیوتر کاغذی

انجمن علمی کامپیوتر دانشکده‌ی الزهرا مشهد
صاحب امتیاز نشریه


فاطمه (شهرزاد) هاشم‌زاده نافجی
مدیر مسئول (مدیر سامانه)


زهرا تاتار
سردبیر نشریه و ویراستار ارشد


سیده‌صالحه مدنی
گرافیست و صفحه‌آرا

الیا کاری علی‌آبادی
طراح مسکات

معصومه متقی
ویراستار و نویسنده‌ی نشریه

زینب عرفانیان
نویسنده


یاسمن خسروی
نویسنده

ریحانه قائمی
نویسنده

زینب ابراهیمیان
نویسنده

سخن سردبیر

امروزه علم رایانه، ثانیه به ثانیه در حال پیشرفت است. رایانه‌ها هر چه بیشتر به ما کمک کنند، چالش‌ها و مشکلات آن‌ها هم بیشتر می‌شود. این چالش‌ها از همان لحظه‌ای که شما تصمیم به خرید یک رایانه می‌گیرید شروع می‌شوند و تا جایی که کار شما با آن رایانه گره خورده است، ادامه دارند.

ما دور هم جمع شدیم تا قدمی کوچک برای حل این مشکلات برداشته باشیم. نتیجه آن شد یک نشریه که با زبانی ساده و قابل فهم راه حل این مشکلات را در دسترس‌تان قرار دهد.

این اولین شماره از اولین فعالیت نشریه انجمن علمی ماست.

قرار است در این ماهنامه‌ها، به دنیای امنیت، نرم‌افزارها، فناوری‌های جدید و اخبار روز حول رایانه سفر کنیم.

امیدواریم در این راه مفید و موثر باشیم. منتظر شنیدن پیشنهادات و انتقادات شما برای بهبود و رشد محتوای نشریه **کامپیوتر کاغذی** هستیم.

سردبیر نشریه : زهرا تاتار

راه ارتباطی: **computerkagazi.mag@gmail.com**

امنیت : VPN و VPS

نویسنده: معصومه متقی

VPS و VPN ازنظر کاربرد و عملکرد کاملاً متفاوت‌اند!

وی‌پی‌اس همانند کامپیوتری است که کیس آن در مکانی با زیرساخت‌های استاندارد و قدرتمند و مانیتور و کیبورد و موس آن در منزل شما قرار گرفته است و آن را از راه دور مدیریت می‌کنید.

وی‌پی‌ان نیز ابزاری است که ازطریق آن با آی‌پی یا آدرس اینترنتی متفاوتی با آدرس خودتان به اینترنت متصل می شوید. اتصال به وی‌پی‌ان همانند تغییر پلاک خودرو و تردد در شهر است. در این مقاله، تفاوت‌های **VPN** و **VPS** را بررسی خواهیم کرد.

VPS یا **Virtual Private Server** به‌معنای «سرور مجازی شخصی» است. این کامپیوتر مجازی همانند کامپیوتر خانگی شما، از بخش‌های مختلفی مثل رم و هارد و پردازنده تشکیل شده است که قدرت خود را از کامپیوتر بزرگ‌تر یا همان سرور می‌گیرد و دراختیار شما می‌گذارد.

این سرورها در ساختمانی با نام مرکز داده (دیتاسنتر) قرار گرفته‌اند که تمام استانداردهای نگه‌داری در آن رعایت و با استفاده از نرم‌افزارهای مجازی‌ساز، منابع سخت‌افزاری آن بین چند کاربر **VPS** تقسیم می‌شود. این یعنی مثلاً به شما بیشتر از **2** گیگابایت حافظه رم و **10** گیگابایت فضای ذخیره‌سازی اختصاص داده نمی‌شود.

امنیت : VPN و VPS

نویسنده: معصومه متقی

مزایای مهم خریدVPS

- داشتن آی پی ثابت و اختصاصی از کشور و منطقه دلخواه
- امکان اتصال با تلفن‌همراه هوشمند و تبلت
- دسترسی ادمین و روت در سیستم‌عامل ویندوز و لینوکس
- نصب نرم‌افزارهای دلخواه روی آن
- قابلیت ارتقای منابع سخت‌افزاری
- پشتیبانی ۲۴ساعته
- میزبانی از چندین وبسایت
- سرعت بیشتر و کیفیت بهتر درمقایسه‌با هاست‌های اشتراکی

امنیت : VPN و VPS

نویسنده: معصومه متقی

مزایای مهم خرید VPN و خطرات استفاده از VPN

مزایای خرید VPN

- تغییر آی‌پی و نمایش محتوای مسدودشده برای مثال، وب‌سایت نتفلیکسNetflix برای تماشای فیلم در کشور خاصی محدود شده است؛ اما با استفاده از وی‌پی‌ان می‌توان از امکانات آن استفاده کرد.
- حفظ امنیت اطلاعات ارسالی در محیط اینترنت با رمزگذاری‌های خاص
- زمانی که به مودم و شبکه اینترنت نامطمئن مثل رستوران‌ها و فرودگاه‌ها و کافه‌ها متصل شده اید و از امنیت آن شبکه اطلاعی ندارید، با کمک وی‌پی‌ان‌ها می توانید از ایمن‌بودن اتصال خود مطمئن شوید.

خطرات VPN

- امکان قطع و وصل‌شدن و عملکرد ناصحیح
- مسدودبودن فهرستی از IP وی‌پی‌ان ها برای وب‌سایت‌های خاص
- مصرف زیاد باتری برای گوشی‌های تلفن‌همراه
- کاهش سرعت اینترنت
- امکان نفوذ تروجان‌ها یا KeyLogger به سیستم‌عامل

امنیت : VPN و VPS

نویسنده: معصومه متقی

سوالات متداول

۱. VPS یا VPN کدامیک بهتر است؟

VPS یک سرویس میزبانی مجازی است که اگر دیتاسنتر آن در داخل باشد IP| ثابت و اختصاصی ایران را دارد، اما اگر دیتاسنتر آن در خارج از کشور باشد، IP اختصاصی و ثابت خارج از کشور را خواهد داشت. برای همین شبیه به یک کامپیوتر در موقعیت یک کشور خارجی برای شما عمل می‌کند. اما VPN یک سیستم برای تغییر موقت IP است و به شما IP خارج اما موقت ارائه می‌کند که با هر باز قطع و وصل شدن، IP تغییر خواهد کرد.

۲. VPS به چه منظوری مورد استفاده قرار می‌گیرد؟

VPS یا سرور خصوصی مجازی، یک سیستم عامل مجازی است که در یک سرور والد قرار دارد و از فناوری مجازی‌سازی برای ارائه منابع اختصاصی (خصوصی) به سرورهای مجازی دیگر استفاده می کند.

۳. برایِ ترید و خرید و فروش ارز دیجیتال، VPS بهتر است یا VPN؟

مطمئنا VPS انتخاب مطمئن‌تری است، چرا که کاملا مانند یک سیستم همیشه روشن در کشور خارجی عمل می‌کند و با قطع اتصال شما، IP تغییر نمی‌کند. اما VPN ممکن است IP شما را تغییر دهد یا امکان قطع و وصل‌های زیادی دارد.

نویسنده: معصومه متقی

احراز هویت بیومتریک

در دنیای کنونی و پیشرفت چشمگیر تکنولوژی مسئله امنیت و حریم خصوصی برای همه افراد اهمیت بسیار زیادی دارد. با افزایش جرایم اینترنتی، کلاهبرداری و سرقت هویت، بیشتر از هر زمان برای کسب و کارها به معضلی تبدیل شده . احراز هویت بیومتریک یکی از معتبرترین روش ها برای حل این مسئله است.

اما این سیستم ها چطور کار میکنند و از طریق شناسه های منحصربفرد هرکس اورا شناسایی میکنند؟

در این روش احراز هویت اسکنر ویژگی های فیزیکی منحصر به فرد هرفرد مثل(اثر انگشت- عنبیه- چهره و ...) را می خواند، که سپس به یک (بارکد) رمزگذاری شده تبدیل می شود. این بارکد وارد سیستم شده و در صورت مطابقت اجازه دسترسی به سامانه ها، برنامه ها و موارد دیگر را می دهد.

در ادامه به چند نمونه از هر کدام می پردازیم:

تشخیص اثر انگشت

یک سیستم شناسایی مبتنی بر تشخیص اثر انگشت به دنبال ویژگی های خاص در الگوی خط روی سطح انگشت است. دوشاخه ها، انتهای خط الراس و جزایری که این الگوی خط را تشکیل می دهند در قالب یک تصویر ذخیره می شوند.

شناسایی اثر انگشت در حال حاضر برای بسیاری از مردم آشنا است و بنابراین توسط تعداد زیادی از کاربران برای استفاده به عنوان امنیت بیومتریک پذیرفته شده است. این فناوری همچنین نسبتاً ارزان و آسان برای استفاده است.

اما مشکل این روش این است که تصویر از یک مشخصه خارجی این است که می توان این تصویر را تکرار کرد. بنابراین می توان آن را مقایسه کرد. در اصل، پس از آن می توانید همان کد را ایجاد کنید. با استفاده از فناوری نسبتا در دسترس می‌توان اثر انگشت را جعل کرد.

نویسنده: معصومه متقی

احراز هویت بیومتریک

نکته دیگری که به هیچ وجه بی اهمیت نیست این است که انگشتی که برای شناسایی ارائه می شود لزوماً نیازی به اتصال به بدن ندارد... علاوه براین نرخ پذیرش نادرست و خطا وجود دارد و برخی افراد به که صورت ارثی اثر انگشت ندارند نمیتوانند از آن استفاده کنند.

تشخیص چهره

یک سیستم تشخیص چهره شکل و موقعیت قسمت‌های مختلف صورت را برای تعیین یک تطابق تجزیه و تحلیل می‌کند. ویژگی های سطحی مانند پوست نیز گاهی اوقات در نظر گرفته می شود.تشخیص چهره برای اهداف امنیتی بیومتریک شاخه‌ای از فناوری تشخیص چهره است که برای شناسایی چهره‌ها در تصاویر پیچیده که ممکن است تعدادی چهره در آن ها وجود داشته باشد، استفاده می شود.

این فناوری در سال های اخیر به سرعت توسعه یافته است و بنابراین در صورت نیاز به سیستمی برای شناسایی از راه دور، یک نامزد عالی به عنوان امنیت بیومتریک است. مزیت دیگر این است که این فناوری "شناسایی منفی" یا حذف چهره ها را امکان پذیر می کند و اسکن جمعیت برای افراد مشکوک را بسیار آسان تر می کند.

با این حال، تشخیص چهره دارای تعدادی نقاط ضعف قابل توجه است. به عنوان مثال، این فناوری عمدتا بر روی خود صورت تمرکز می کند، یعنی از خط مو به پایین. در نتیجه، معمولاً یک فرد باید مستقیماً به دوربین نگاه کند تا تشخیص آن ممکن شود. و حتی با وجود اینکه این فناوری هنوز با سرعتی سریع در حال توسعه است، سطح امنیتی ای که در حال حاضر ارائه می دهد هنوز با اسکن عنبیه یا تشخیص الگوی رگ برابری نمی کند.

این فناوری در سال های اخیر به سرعت توسعه یافته است و بنابراین

نویسنده: معصومه متقی

احراز هویت بیومتریک

تشخیص عنبیه

هنگامی که یک اسکن عنبیه انجام می شود، یک اسکنر ویژگی های منحصر به فرد یک عنبیه را می خواند، که سپس به یک (بارکد) رمزگذاری شده تبدیل می شود. اسکن عنبیه به عنوان یک تکنیک امنیتی بیومتریک عالی شناخته میشود ، به خصوص اگر با استفاده از نور مادون قرمز انجام شود.

- در این روش خطا و جعل هویت دیگران امکان پذیر نیست و روش بسیار مطمئن است.
- با این حال، یکی از نقاط ضعف که اغلب هنگام معرفی این فناوری با آن مواجه می‌شود، مقاومت کاربران است. تعداد کمی از افراد اسکن چشمان خود را تجربه نسبتاً ناخوشایندی می دانند. همچنین باید موقعیت خاصی را در نظر بگیرید تا اسکنر بتواند عنبیه شما را بخواند که می تواند باعث ناراحتی شود. بهداشت یکی دیگر از اشکالاتی است که اغلب ذکر می شود، زیرا بسیاری از سیستم ها از کاربران می خواهند که چانه خود را روی یک تکیه گاه چانه قرار دهند که توسط افراد بی شماری قبل از آنها استفاده شده است.

در نهایت، مهم است که به خاطر داشته باشید که اگرچه اسکن عنبیه سطح بالایی از امنیت بیومتریک را ارائه می دهد، اما ممکن است به قیمت از دست دادن سرعت تمام شود.

تشخیص الگوی رگ انگشت

در مورد تشخیص الگوی رگ، نقاط انتهایی و دوشاخه‌های وریدهای انگشت به شکل یک تصویر گرفته می‌شوند، دیجیتالی می‌شوند و به یک کد رمزگذاری شده تبدیل می شوند. این روش، همراه با این واقعیت که رگ‌ها به جای روی سطح پوست یافت می‌شوند، این فناوری را به طور قابل توجهی ایمن‌تر از شناسایی مبتنی بر اثر انگشت و همچنین سریع‌تر و راحت‌تر برای

نویسنده: معصومه متقی

احراز هویت بیومتریک

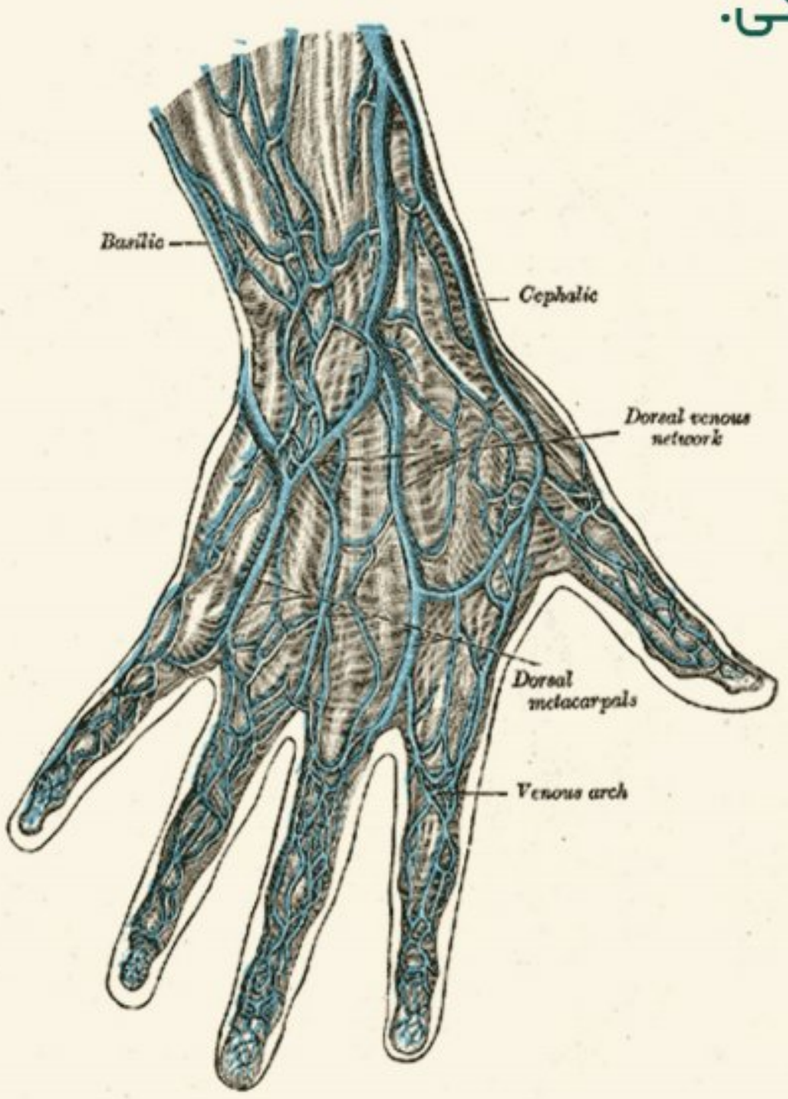
کاربر می‌کند. با این حال، روش گران‌تری است.

• نکته دیگری که باید در نظر داشت این است که انگشتان بسیار سرد و انگشتان مرده (مانند افرادی که از سندرم رینود رنج می برند) با استفاده از تشخیص الگوی رگ انگشت خواندن غیرممکن یا دشوار است. با این حال، شاید بزرگترین نقطه ضعف این باشد که این نوع امنیت بیومتریک هنوز نسبتا ناشناخته است.

تشخیص الگوی رگ کف دست

این تکنیک همچنین بر اساس شناخت الگوهای رگه منحصر به فرد است. با این حال، از آنجایی که نقاط مرجع بیشتری نسبت به تشخیص الگوی رگ انگشت استفاده می شود، این روش شناسایی ساده تر و مطمئن تر است.

این فناوری که نمی توان آن را کپی کرد در حال حاضر به عنوان بهترین روش موجود در زمینه امنیت بیومتریک در کنار اسکن عنبیه در نظر گرفته می شود. اسکن کف دست سریع و دقیق است و سطح بالایی از راحتی کاربر را ارائه می دهد. سیستم های کنترل دسترسی مبتنی بر تشخیص الگوی ورید کف دست نسبتاً گران هستند. به همین دلیل، چنین سیستم‌هایی عمدتاً در بخش‌هایی استفاده می‌شوند که در مورد امنیت، تقاضاهای دقیقی دارند، مانند دولت، سیستم قضایی و بخش بانکی.



نویسنده: معصومه متقی

احراز هویت بیومتریک

قوی ترین مثال در شناسه منحصربفرد DNA است که نه تنها یک فرد را شناسایی می کند، بلکه طیف گسترده ای از اطلاعات سلامتی را نیز نشان می دهد.
سیستم‌های بیومتریک مورد استفاده برای مدیریت دسترسی به یک برنامه یا خدمات ممکن است شامل محدود کردن گزینه‌ها و در نتیجه فرسایش کنترل باشد. به عنوان مثال، برای حفظ پاسپورت، شخص باید با استفاده از تصویر صورت موافقت کند.
استفاده دولت از سیستم های بیومتریک ابعاد بیشتری به این فرسایش کنترل می بخشد. در بسیاری از انواع تعاملات با دولت، افراد چاره ای جز صرف نظر کردن از اطلاعات شخصی ندارند – اغلب اطلاعات حساس. در واقع، داده های شخصی معمولاً ارز مبادله شده برای برنامه ها، خدمات یا حقوق دولتی است.

اخبار: استارلینک

از استارلینک چه خبر؟

نویسندگان:
یاسمن خسروی،
زینب ابراهیمیان،
معصومه متقی

واژه استارلینک Starlink که از شرکت اسپیس ایکس space X و شبکه فضایی هم‌نام آن گرفته شده است، به مجموعه‌ای از ماهواره‌های مبتنی بر شبکه دلالت دارد.

شبکه های ماهواره ای شامل ۳۰۰۰ ماهواره کوچک است که در مدار کره زمین حرکت می‌کنند.البته بدون استفاده از امکانات نرم افزاری نیز امکان استفاده از خدمات اینترنت ماهواره‌ای این پروژه وجود ندارد. باید علاوه بر دیش‌ها و ریسیورهای مخصوص از برنامه‌های خاصی جهت دریافت و ارسال سیگنال بهره گرفته شود.

به احتمال زیاد این روزها، خبر رسیدن اینترنت ماهواره‌ای استارلینک به ایران را شنیده اید حال به این میپردازیم که اینترنت ماهواره ای استارلینک چیست؟

جدیدترین اخبار تکنولوژی و فناوری های نوین

۱.مایکروسافت به متاورس می پیوندد

مایکروسافت با امضای قرارداد جدیدی، در مسیر توسعه نرم‌افزارهای خود در دنیای متاورس، به شرکت متا (فیسبوک) پیوسته است. با شروع این همکاری، استفاده از امکانات نرم‌افزاری مایکروسافت به کمک هدست‌های واقعیت مجازی متا ممکن خواهد شد.

۲.اپل سر خم کرد

شرکت اپل رسما اعلام کرد که باید از قانون جدید اروپا یعنی استفاده از پورت USB-C تبعیت کند؛ این درحالی است که قول تکنولوژی جهان با این ایده مخالف بود.

۳.استارینک برای ماشینها

اینترنت استارلینک در مسیر پیشرفت خود امکان نصب بر روی خودروهای در حال حرکت را پیدا می کند.

۴.غول های تکنولوژی زیر بار رکود

هلدینگ گوگل و مایکروسافت درآمد خود را اعلام کردند. هر دو غول فناوری در طول همه‌گیری ویروس کرونا از درآمدهای قوی برخوردار بودند، اما اکنون رکود اقتصاد بر سود آنها تأثیر گذاشته است.

۱۰ کامپیوتر کاغذی

اخبار: استارلینک

نو یسند گـــــــا ن :
یاســمن خســـروی،
زینــب ابراهیمیــان،
معصومــه متقــی

تفاوت اینترنت زمینی و ماهواره‌ای

در حالت عادی شما برای دسترسی به دیتای اینترنت به یک ISP یا تامین کننده خدمات اینترنت متصل هستید. این اتصال از طریق سیم (سیم تلفن در ADSL) و یا از طریق امواج وای فای یا دیتای گوشی امواجی که از دکل ها و یا آنتن های نصب شده در زمین منتشر می شوند صورت می پذیرد

. اما در اینترنت ماهواره ای شما با استفاده از یک دیش، مستقیماً به ماهواره یا ماهواره های موجود در مدار زمین متصل می شوید و دریافت و انتقال دیتا از طریق دیش و این اتصال برقرار می شود. وقتی اطلاعات موجود در اینترنت را از طریق اتصال مستقیم به یک ماهواره دریافت می کنید، شما در حال استفاده از اینترنت ماهواره ای هستید.

اینترنت ماهواره‌ای استارلینک نیز خدماتی مشابه این ارائه می دهد.

اخبار: استارلینک

نویسندگان:
یاسمن خسروی،
زینب ابراهیمیان،
معصومه متقی

آیا استارلینک، اولین ارائه دهنده اینترنت ماهواره ای است؟

دیگر شرکت های ارائه دهنده اینترنت ماهواره ای:

ویاست Viasat / هیوزنت Hughes Network Systems / استار لینک starlink

معایب و مزایای اینترنت ماهواره ای استارلینک:

* جهانی بودن اینترنت ماهواره ای استارلینک

* استارلینک خدمات خود را به همه جهان ارائه خواهد داد که کمک بزرگی به بیش از ۳ میلیارد نفری است که در حال حاضر به اینترنت دسترسی ندارند.اما دیگر شرکت ها ارائه دهنده این خدمات، تنها بر روی کشورهایی مانند آمریکا متمرکز هستند.

* سرعت رو به افزایش و تاخیر رو به کاهش اینترنت استارلینک در مقایسه با دیگر شرکت های ماهواره ای مثال زدنی است و نوید اینترنتی پر سرعت با تعداد کاربران زیاد را می دهد.

بنا به ادعای اسپیس ایکس، شرکت ارائه دهنده اینترنت ماهواره ای استارلینک، در فاز نهایی تعداد ماهواره های در حال گردش به دور زمین به بیش از ۴۰ هزار ماهواره می رسد. که عدد ترسناکی است. زیرا بسیاری از کارشناسان معتقد هستند که تعداد بالای ماهواره های استارلینک در مدار پایینی زمین، به معنی انباشتی از زباله های فضایی و ایجاد سندروم کسلر است. البته شرکت اسپیس ایکس در پاسخ به این انتقادات، بیان کرده است که حتی در صورت برخورد ماهواره ها با هم و یا خرابی هر یک، این ماهواره ها طی چند سال در جو زمین خواهند سوخت و هیچ خطری زمین را تهدید نمیکند.

نویسنده: ریحانه قائمی

امنیت در گوشی‌های هوشمند

امنیت اطلاعات؛ چیزی که این روزها زیاد شنیده‌ایم و شاید از ندانستن ضروریت‌های آن ضربه‌هایی هم خورده باشیم.
اول از همه باید بدانیم امنیت اطلاعات اصلا چیست ؟ امنیت اطلاعات یعنی تمام فرآیند محافظت از اطلاعات در مقابل حملات هکرها. این حملات می‌تواند عمد یا غیر عمد و یا حتی فعالیت‌های غیرمجازی مانند دسترسی، استفاده، افشاء، تغییر، تخریب و یا اختلال باشد.
افراد برای ادامه حیات خود نیاز به حفاظت از اطلاعات و دارایی های خود دارند. و برای این حفاظت نیاز است تا دانش و علم خود را افزایش دهند. پس امنیت اطلاعات نیازمند دانش تخصصی است.

بعد از محبوب شدن تلفن‌های هوشمند، به امنیت تلفن‌های همراه اهمیت چندانی داده نمی‌شد. واقعا چه چیزی در گوشی‌های قدیمی ما ذخیره شده بود؟ تعدادی مخاطب، بازی‌های کلاسیک، و چند تصویر تار برای پس‌زمینه. با این حال امروزه همه چیز تغییر کرده، تعداد زیادی از مردم برای اجرای بسیاری از امور، از گوشی‌های هوشمند استفاده می‌کنند از ورود به حساب بانکی تا داشبورد شرکت برای انجام کارهایی که به آنان واگذار شده، بنابراین اهمیت امنیت گوشی های هوشمند بیشتر از قبل شده است.
ما همه چیز را در تلفن همراه‌مان ذخیره می‌کنیم تا در مواقعی که به آن احتیاج داشتیم کاملا در دسترس‌مان باشد. اما این کار بسیار نگران کننده است. این روزها هکرها برای ورود به گوشی تلفن ما بسیار زیرک، قدرتمند، و سریع عمل می‌کنند.

نویسنده: ریحانه قائمی

امنیت در گوشی‌های هوشمند

هنگامی که صحبت از امنیت تلفن همراه می شود، بسیاری از مردم تصور می کنند که منظور از امنیت، همان امنیت فیزیکی گوشی و گذاشتن رمزهای پیچیده یا قفل کردن دستگاه پس از مکالمه است. اگرچه این موضوع هم از اهمیت ویژه ای برخوردار است اما تنها بخش کوچکی از امنیت تلفن همراه را شامل می شود و بخش مهمتر، مربوط به پلت فرم آن است.

هم اکنون سه پلت فرم اندروید گوگل، ویندوز فون ۷ و iOS از مهمترین پلت فرم های تلفن همراه به شمار می روند که هر کدام با مشکلات امنیتی خاصی روبرو هستند. اگرچه نگرانی های امنیتی که کارشناسان امنیت دارند، عمدتاً نظری بوده و تهدیدها نیز جزء جدایی ناپذیر هر سیستم عامل به شمار می رود ولی شناخت این تهدیدات، آگاهی ما را در مواجه با خطرات بیشتر می سازد.

نویسنده: ریحانه قائمی

مشکلات امنیتی اندروید

این روزها گرایش به سیستم عامل اندروید هر لحظه در حال افزایش است، اما مشکلات امنیتی آن باعث نگرانی و هشدار کارشناسان شده است. کارشناسان امنیتی اعتقاد دارند به علت متن باز بودن اندروید که اجازه دسترسی به معماری و اصول اولیه طراحی آن را می دهد، از سایر سیستم عامل ها در برابر حملات هکرها و ویروس نویسان آسیب پذیرتر است. اگرچه گوگل هدف از متن باز بودن اندروید را ارایه برنامه های کاربردی بیشتر برای تلفن همراه می داند، اما این قابلیت، تولید برنامه های مخرب فراوان را نیز برای آن در پی داشته است.

تا مدتی پیش، دو آسیب پذیری مهم در سیستم عامل اندروید وجود داشت که مهاجمان را قادر به دور زدن تأییدیه کاربر برای نصب برنامه های مخرب روی گوشی می نمود. یکی از این آسیب پذیری ها به این صورت عمل می کرد که توسط یک افزونه ساختگی برای بازی معروف Angry Birds و با فریب کاربر به مراحل اضافی و دریافت جایزه بازی، به صورت مخفیانه سه برنامه مخرب که امکان پرداخت آنلاین جعلی، سرقت اطلاعات مخاطبین از دفترچه تلفن همراه و ردگیری مکان کاربر را داشت، بر روی گوشی نصب می کرد. مدتی پس از انتشار خبر جنجالی این آسیب پذیری، گوگل توانست با انتشار وصله ای، آن را رفع نموده و از حملاتی که به فضای کاربری گوشی های هوشمند اندرویدی می شود، جلوگیری نماید.

گوگل که اندروید را با اندیشه فتح دنیای گوشی های همراه هوشمند و لوح-رایانه ها عرضه نموده، تلاش کرده است تا در نسخه های خود علاوه بر ارتقاء بهتر رابط کاربری سیستم عامل و همچنین رفع برخی از مهمترین مشکلات امنیتی آن، با ایجاد ابزارک هایی برای امکانات مورد نیاز کاربران بر روی نمایشگر، همچون تسریع دسترسی به سرویس های جیمیل، نقشه، تقویم، چند سایت پرطرفدار اینترنتی و نسخه به روز شده مرورگر کروم خود، توجه کاربران را بیشتر جلب نماید. این غول جستجوگر اینترنتی با اعطای جوایز بسیار ارزشمند برای کشف و گزارش حفره های امنیتی سیستم عامل خود، به شدت در تلاش است تا اعتماد کاربران را همچنان حفظ کند.

نویسنده: ریحانه قائمی

امنیت اطلاعات در گوشی های هوشمند

مشکلات امنیتی IOS

در این میان سیستم عامل iOS اپل نیز به دلیل استفاده در تلفن های لوکس هوشمند، هر روز مورد هجوم گسترده تری قرار می گیرد؛ ویروس هایی که اختصاص به iOS داشته و سعی دارندکه خودشان را به صورت های مختلف، تکرار کرده یا با تجزیه نمودن و دوباره نویسی خود، در نبرد با آنتی ویروس ها پیروز شوند.

اپل در سیستم عامل تلفن همراه هوشمند آیفون خود می کوشد تا امنیت را با کنترل امضاء امنیتی برنامه ها برقرار نموده و از نصب برنامه های کاربردی غیر مجاز یا مخرب بر روی گوشی جلوگیری کند. اپل نکات امنیتی را هم در iOS دقیق تر از اندروید رعایت می نماید، در نتیجه ویروس ها نمی توانند به راحتی در این سیستم عامل نفوذ کنند.

در ادامه در خصوص اهمیت امنیت گوشی های هوشمند، لیستی از کارهایی که شما به منظور محافظت از تلفن همراهتان در برابر مجرمان سایبری می‌توانید انجام دهید ارائه گردیده:

آن دسته از کاربرانی که به اهمیت امنیت گوشی های هوشمند پی نبرده اند، با نداشتن رمز عبور برای موبایل، خود را در درد سر بزرگی می اندازند. آن‌ها با وارد شدن به حساب‌های کاربری شخصی هنگام استفاده از wifi عمومی مرتکب اشتباه دیگری می‌شوند. استفاده از این سایت‌ها هنگام اتصال به wifi عمومی به هیچ وجه امن نیست چرا که اطلاعات شما می‌تواند به سرقت برود. بهتر است برای این کار از یک VPN استفاده کنید. با این کار می‌توان مطمئن شد که هویت شما مخفی و امن است.

دیگر راهکارهای حفظ امنیت

سعی کنید در حد امکان از WIFI عمومی استفاده نکنید.
استفاده از wifi عمومی بسیار مفید است اما با این کار دسترسی و دزدی اطلاعات شخصی شما برای هکرها بسیار آسان خواهد بود. اگر مجبور به استفاده از wifi عمومی هستید، حتما از یک VPN استفاده کنید یا از ورود به حساب‌های شخصی خودداری کنید. همان طور که می‌دانید wifi های عمومی شبکه‌هایی با امنیت پایین هستند و تلفن شما می‌تواند طعمه آسانی برای هکرهای سایبری به منظور دزدیدن اطلاعات و هویت شما باشد.

برای تلفن خود رمز عبور بگذارید.
در بحث اهمیت امنیت گوشی های هوشمند، قرار ندادن رمز عبور برای موبایل یک اصل مهم به شمار می رود که اشتباه اصلی بیشتر کاربران تلفن همراه است. این کار می‌تواند در هنگام سرقت تلفن بسیار خطرناک باشد.
آپدیت‌های جدید امنیتی را به طور مداوم دریافت نمایید خیلی‌ها از این موضوع با خبر نیستند، اما بیشتر آپدیت‌های نرم‌افزارها شامل آپدیت‌های امنیتی مهم نیز می‌باشد. آپدیت کردن به آخرین نرم‌افزار می‌تواند تلفن شما را کارآمدتر کند همچنین تهدیدات سایبری کمتری تلفن همراه شما را تهدید می‌کند.

برنامه‌های ردیابی موبایل را فعال کنید.
داشتن برنامه‌های ردیابی در گوشی تلفن بسیار ضروری است. بنابراین، شما قادرید تا در هنگام گم شدن تلفن خود را به راحتی ردیابی کنید. بدین منظور می‌توانید از برنامه Find My iPhone در گوشی‌های آیفون و Find My Device در گوشی های اندرویدی استفاده نمایید.

نویسنده: ریحانه قائمی

دیگر راهکارهای حفظ امنیت

حواستان به شماره‌های ناشناس باشد.
هر روزه ما تعداد زیادی تماس و پیغام از شماره‌های ناشناس دریافت می‌کنیم. بیشتر آن‌ها تماس‌های اسپمی می‌باشند که تلاش می‌کنند تا اطلاعات شما را سرقت کنند.

همیشه از تلفن خود نسخه پشتیبان تهیه کنید.
تهیه نسخه پشتیبان از تلفن همراه علاوه بر اهداف امنیتی مزایای زیاد دیگری نیز دارد. اگر موبایل شما با یک ویروس آلوده شد، ویروس می‌تواند به داخل موبایل شما نفوذ کرده و به هرچیزی را که ذخیره کرده‌اید آسیب برساند.

حال با توجه به مواردی که مطرح شد، توصیه ای که ما به کاربران تلفن همراه داریم این است که تنها برنامه های کاربردی را روی گوشی خود نصب کنند که به شرکت تولیدکننده آن نرم افزار اعتماد کامل دارند. همچنین پیشنهاد می کنیم که برای حفاظت از اطلاعات شخصی خودتان، همواره از آنتی ویروسی که شما را در برابر حملات و نرم افزارهای مخرب محافظت نموده و قابلیت فیلتر کردن پیام های متنی آلوده را دارد، استفاده نمایید.

و در آخر:
اهمیت امنیت گوشی های هوشمند بر هیچ گس پوشیده نیست؛ پس همیشه به یاد داشته باشید که هنگام استفاده از حساب بانکی، و سایت‌هایی که باید به طور کامل از آن محافظت کنید این نکات را رعایت کنید.
هرچند هکرها از چگونگی عملکرد این نکات بیشتر از ما اطلاع دارند، اما به موقعیتی فکر کنید که هکر می‌تواند به حساب کاربری یا اطلاعات شخصی شما دسترسی پیدا کند. بنابراین به شما پیشنهاد می‌کنیم که موکدا نکات بالا را به منظور جلوگیری از یک موقعیت ناخوشایند رعایت کنید.

فناوری های روز: شبکه حسگر بیسیم

نویسنده: زهرا تاتار

حسگرهای حساس!

اول از همه باید بدانیم شبکه حسگر بیسیم یعنی چه؟

پیشرفت ارتباطات و مخابرات باعث شد حسگرهای کوچک با کاربردهای وسیع روی کار بیایند.حسگرها می‌توانندکارهایی مانند دریافت اطلاعات از محیط و پردازش و ارسال آن‌ها را انجام بدهند. حسگرهای بیسیم در محیطهای خاص به صورت گسترده یا محدود نصب میشوند تا داده ها را جمع‌آوری کنند.

نحوه ارتباط برقرار کردن حسگرها

بدین گونه است که آن‌ها در مناطق مختلف و دور و نزدیک نصب میشوند و از طریق امواج رادیویی ارتباط برقرار میکنند. یک شبکه‌ی حسگر بیسیم، متشکل از گیرنده رادیویی برای دریافت اطلاعات از محیط، فرستنده رادیویی، برای ارسال اطلاعات به مرکز، آنتن داخلی و خارجی، باتری و ریزکنترلر است. ریز کنترلر مداری الکترونیکی است که وظیفه برقراری ارتباط با حس‌گرها و منابع تامین انرژی را دارد.

کاربرد حسگرها

کاربردهای حسگرها در حوزه‌های نظامی، نظارت از راه دور، کشاورزی و محیط زیست و پزشکی است. مثلا در نظارت از راه دور میتوان تشخیص نشتی گاز را مثال زد. حسگرها نشتی گاز یک محیط را تشخیص می‌دهند و برای مرکز مدیریت، هشدار ارسال میکنند.و این‌گونه بدون تلفات جانی میتوان این مشکل را حل کرد. باید در نظر داشت که این حس‌گرها در مقابل بعضی تهدیدات آسیب پذیر هستند.مثلا استراق سمع پیغام ها ، تزریق پیام های جعلی ،اتلاف منابع شبکه برای اعمال امنیت حداکثری و محدودیت هایی مانند محدود بودن فضای ذخیره سازی و ارتباطات.

مزایای حسگرها

از مزایای این حسگرها هم میتوان به موارد زیر اشاره کرد: جلوگیری از سیم کشی اضافی ، مناسب مکان هایی با دسترسی سخت ،کم هزینه و مقاوم در برابر شرایط سخت محیطی.

مشاغل: مشاغل در حوزه‌ی امنیت

نویسنده: زهرا تاتار

کار و بار

در دنیای امنیت فناوری‌اطلاعات چهار گرایش اصلی وجود دارد:

Security Architect (معمار امنیت)

Security Consultan (مشاور امنیت)

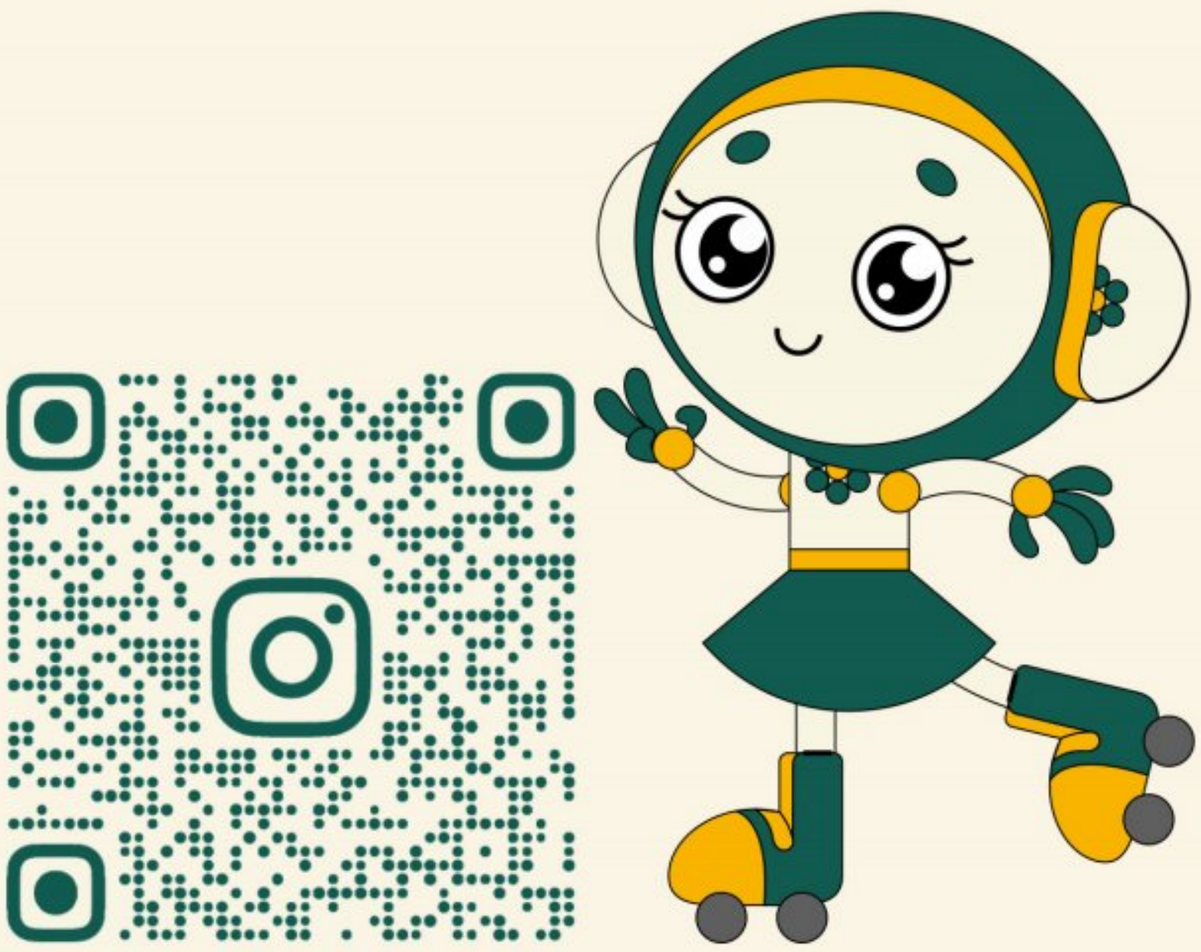
Penetration Tester/Ethical Hacke (کارشناس تست نفوذ/ هکر اخلاق مدار)

Chief Information Security Officer (CISO) (مدیر ارشد امنیت اطلاعات)

همراهان گرامی؛

ما مشتاقانه در انتظار شنیدن پیشنهادات و انتقادات شما در خصوص نشریه‌ی **کامپیوتر کاغذی** هستیم.
می‌توانید نظرات خود را به ایمیل زیر ارسال کنید.

Computerkagazi.mag@gmail.com



صفحه‌ی رسمی انجمن علمی کامپیوتر دانشکده‌ی الزهرا مشهد