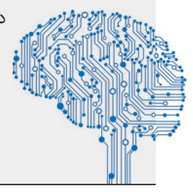
مغز انسان در آینده نزدیک به اینترنت متصل می‌شود



در گزارشی که به‌تازگی در نشریه پیشگامان علوم عصبی (Frontiers in Neuroscience) منتشر شده، گروهی از دانشمندان بین‌المللی پیش‌بینی می‌کنند طی دهه‌های آتی پیشرفت‌های بنیادینی در بخش «اتصال مغز به ابر حسابرسی» وجود دارد. آنها معتقدند انسان با استفاده از ترکیب فناوری‌های نانو، هوش مصنوعی و علم رایانه می‌توانند به طور نامحسوسی مغز افراد را به ابر حسابرسی رایانه‌ها متصل کند. / مهر

تلویزیون شفاف، تازه‌ترین اختراع ژاپنی‌ها

یك شرکت ژاپنی در جدیدترین ابتکار خود نوعی تلویزیون اولد (OLED) شیشه‌ای و شفاف طراحی کرده که به‌راحتی می‌توان پشت آن را دید. این شرکت طرحی مفهومی از این صفحه نمایشگر شفاف منتشر و آن را به عنوان وسیله‌ای برای زیباسازی طراحی دکور خانه معرفی کرده است. هنگامی که این تلویزیون خاموش باشد، صفحه نمایش ظاهری شبیه یك آکواریوم با قاب چوبی پیدا می‌کند و هنگامی که روشن شود افراد خانواده می‌توانند به تماشای برنامه دلخواهشان بپردازند. / ایسنا

اگر از گوشی هوشمند استفاده می‌کنید حتما این مطلب را بخوانید

۷ شگرد پیشگیری از سرقت اطلاعات گوشی

یاسمین مشرف

دانش

حتما شما هم خبرهای زیادی در مورد سرقت اطلاعات شخصی افراد و روش‌هایی که این سرقت‌ها از طریق آنها صورت می‌گیرند شنیده‌اید. برخی نرم‌افزارها (اپلیکیشن‌ها) که در سال‌های اخیر به عنوان بدافزار شناخته شده‌اند و برای کلیك‌های تقلبی یا فروش اطلاعات به شخص ثالث مورد استفاده قرار می‌گیرند معمولا بخشی از ماجرا هستند، اما چگونه می‌توانید وقتی یك نرم‌افزار جدید دانلود می‌کنید، مطمئن باشید اطلاعات شما را سرقت نمی‌کند؟ متاسفانه هیچ راه قابل استنادی که بگوید یك نرم‌افزار دارای جنبه‌های منفی است وجود ندارد.

همین طور هیچ راه محافظت‌کننده خطاناپذیری هم برای مقابله با این انگیزه‌ها در دنیای پیوسته درحال پیشرفت فناوری وجود ندارد. نرم‌افزاری که امروز عملکرد خوبی دارد اگر شرکت سازنده آن فروخته شود یا سیاست جدیدی اتخاذ کند ممکن است فردا به بدافزار تبدیل شود. با این حال، رای والش و استفان هارت، کارشناسان امنیت و حفظ حریم شخصی راهکارهایی برای حفاظت از اطلاعات شخصی شما هنگام استفاده از نرم‌افزارها ارائه کرده‌اند که در ادامه با آنها آشنا می‌شوید.

منبع: MSN

مدیریت گذرواژه

شاید کلیشه‌ای به نظر برسد، اما داشتن یك گذرواژه (Password) خوب، گام اول در حفظ امنیت اطلاعات شخصی است. جالب است بدانید که دو گذرواژه «Password» و «۱۲۳۴۵۶» همچنان در صدر فهرست بدترین پسوردهای سال ۲۰۱۸ قرار داشتند. شاید فکر کنید جایگزینی حروف با اعداد یا علائم، کار زیرکانه‌ای است. اما این جایگزینی هم کار زیادی برای قوی‌تر شدن گذرواژه شما انجام نمی‌دهد. واقعیت این است که قدرتمند بودن یك گذرواژه براساس میزان مقاومت آن در برابر یك «حمله جست‌وجوی فراگیر» و یورش سیستماتیك حدس و گمان‌های یك هکر سنجیده می‌شود. قوی‌ترین گذرواژه‌ها شامل توالی‌های تصادفی از نویسه‌ها هستند؛ احتمال این‌که مجموعه‌ای از حروف، اعداد و علائم را که هیچ‌گونه ترتیب خاصی ندارند بتوان در فرهنگ لغات یافت یا با جست‌وجوی فراگیر به آن رخنه کرد بسیار کم است. اما اشکال این گذرواژه‌ها این است که به سختی می‌توان آنها را به خاطر سپرد. کارشناسان همچنین توصیه می‌کنند از به کار بردن یك گذرواژه برای چند حساب کاربری پرهیز کنید. استفاده از یك گذرواژه برای چند حساب باعث می‌شود با مورد دستبرد قرار گرفتن یك حساب، همه حساب‌ها به خطر بیفتند. اگر مدیریت گذرواژه داشته باشید هرکدام از حساب‌هایتان می‌توانند پسوردهای متفاوت و پیچیده‌ای داشته باشند که نفوذ به آنها مشکل است.

استفاده از وی‌پی‌ان هنگام کار با وای‌فای عمومی

استفاده از شبکه مجازی خصوصی یا به اختصار (vpn) زمانی که با وای‌فای عمومی کار می‌کنید نکته مهمی در حفظ امنیت اطلاعات شخصی شماست. در این حالت، وی‌پی‌ان‌ها می‌توانند اطلاعات شما را از جست‌وجوی مخفیانه افراد دیگر که از همان شبکه عمومی استفاده می‌کنند، محافظت کنند. صرف نظر از این‌که چقدر از وی‌پی‌ان استفاده می‌کنید خواندن کامل توافق‌نامه سرویس و اطلاع از این‌که چه اطلاعاتی ممکن است گردآوری شود و این اطلاعات در کجا ذخیره خواهد شد اهمیت زیادی دارد.

دانلود نرم‌افزارهای همراه از گوگل و فروشگاه اپل

همه نرم‌افزارهای همراه گوگل‌پلی یا اپل‌استور، صددرصد قابل اعتماد نیستند. با این حال کارشناسان می‌گویند بهتر است برنامه‌هایتان را از این دو فروشگاه آنلاین دانلود کنید.

هارت می‌گوید نرم‌افزارهای همراه این دو پلتفرم از نظر کیفیت‌های استانداردِ حفاظت از داده‌ها مورد بررسی قرار گرفته‌اند. دانلود نرم‌افزار همراه از منابع غیرمعتبر خطر بیشتری برای دستگاه شما و اطلاعات شخصی‌تان دارد. والش نیز هشدار می‌دهد نرم‌افزارهای همراه دانلودشده از وبگاه‌های غیررسمی نسبت به باج‌افزارها، بدافزارها، جاسوس‌افزارها و ویروس‌های تروجان آسیب‌پذیر هستند.

وی می‌افزاید در بدترین موارد، هکرها کنترل کامل ابزار شما ازجمله قسمت‌هایی مثل دوربین و میکروفن آن را در اختیار می‌گیرند. از دیگر توصیه‌های کارشناسان این است که قبل از دانلود یك نرم‌افزار به مدت‌زمان در دسترس بودن آن توجه کنید. بیکر می‌گوید اگر نرم‌افزارهای همراهی که قصد دانلود آن را دارید برای مدتی طولانی در دسترس بوده، می‌توانید با توجه به دیدگاه‌های کاربران تصمیم بهتری بگیرید. توجه داشته باشید دیدگاه‌ها هم می‌توانند جعلی یا ساختگی باشند. این نوع دیدگاه‌ها معمولا شامل الگوهای گفتاری غیر معمول و میزان زیادی از توصیفات و توضیحات است.

به روز نگهداشتن نرم‌افزار

والش معتقد است وقت گذاشتن برای به‌روزرسانی سیستم عامل گوشی هوشمند بسیار حیاتی است. داشتن بالاترین جایگاه در به‌روزرسانی‌های سیستم عامل می‌تواند با یك قدم جلوتر نگهداشتن شما از هکرها و آخرین سوءاستفاده‌هایی که در سراسر اینترنت و وب تاریك (Dark web) صورت می‌دهند، امنیت ابزار و داده‌های شما را حفظ کند.

والش معتقد است: به‌روزرسانی نرم‌افزار درواقع واکسیناسیون گوشی هوشمند شماست. شیوه‌هایی که هکرها برای دسترسی به اطلاعات ما به کار می‌برند پیوسته درحال تحول و تکامل است، بنابراین شیوه‌های محافظت ما از گوشی‌هایمان هم باید در حال تکامل باشد. والش پیشنهاد می‌کند گوشی‌تان را طوری تنظیم کنید که به‌روزرسانی‌هایش به طور خودکار انجام شود و نیازی به انجام آن به صورت دستی نباشد.

توجه به مجوزهایی که نرم‌افزارها درخواست می‌کنند

یکی از راهکارهایی که تقریبا همه کارشناسان آن را توصیه می‌کنند توجه ویژه به مجوزهایی است که نرم‌افزار از شما درخواست می‌کند. رای والش، کارشناس حریم خصوصی دیجیتال در BestVPN.com در این باره می‌گوید: اگر به نرم‌افزار اجازه دسترسی به فهرست مخاطبان، اطلاعات جی‌پی‌اس، عکس‌ها یا هرچیز دیگری را بدهید، نباید تعجب کنید از این‌که از اطلاعات شما سوءاستفاده شود.

والش می‌افزاید هنگام نصب نرم‌افزار، همیشه تمام درخواست‌ها را بررسی و هر تعداد درخواستی را که می‌توانید در بخش تنظیمات ابزارتان لغو کنید. همیشه از خودتان بپرسید آیا معنی دارد یك نرم‌افزار این مجوزها را درخواست کند؟!

استفان هارت، مدیر شرکت Cardswitcher می‌گوید: اگر یك نرم‌افزار تقاضای دسترسی به داده‌هایی را داشته باشد که ارتباطی با عملکرد آن ندارند باید این درخواست مجوز را یك علامت هشدار بدانید.

هارت می‌افزاید: برای مثال اگر برنامه ساده‌ای را برای داشتن یك ماشین‌حساب جیبی دانلود می‌کنید و آن نرم‌افزارها دسترسی به فهرست مخاطبان و موقعیت مکانی شما را درخواست می‌کنند، باید از خودتان بپرسید چرا مثلا یك ماشین‌حساب باید به فهرست مخاطبان و موقعیت مکانی شما نیاز داشته باشد؟ چنین مواردی یك زنگ هشدار جدی است.

علاوه بر توجه به مجوزهایی که نرم‌افزار درخواست می‌کند، توجه به چگونگی عملکرد تلفن همراه بعد از دانلود هم اهمیت زیادی دارد. اشلومی لیبرو، مدیر برنامه‌های فنی و امنیتی در پلتفرم HackerOne می‌گوید: تغییرات زیاد در طول عمر باتری ابزارتان یك علامت هشدار دیگر است.

به گفته لیبرو اگر بعد از نصب یك نرم‌افزار متوجه شدید عمر باتری دستگاه‌تان کوتاه‌تر از حد معمول شده است، احتمالا این علامتی است که می‌گوید برنامه نصب‌شده خیالات بدی دارد و درحال انجام کارهای پشت‌پرده است. لیبرو اضافه می‌کند: اغلب برنامه‌های مخرب، به طور مداوم درحال آپلود اطلاعاتی مانند فهرست مخاطبان تلفن همراه هستند.

> هنگام نصب نرم‌افزار، همیشه تمام درخواست‌ها را بررسی و هر تعداد درخواستی را که می‌توانید در بخش تنظیمات ابزارتان لغو کنید. همیشه از خودتان بپرسید آیا معنی دارد یك نرم‌افزار این مجوزها را درخواست کند؟!

تحقیق درباره نرم‌افزارها یا شرکت ارائه‌کننده آن

هرچند از روی عملکرد ظاهری یك نرم‌افزار نمی‌توان به انگیزه‌های مخرب آن پی برد، یك جست‌وجوی ساده در گوگل می‌تواند به اطمینان بیشتر از امن بودن نرم‌افزار همراه کمك کند.

کارشناسان، تحقیق در مورد نام نرم‌افزار با عبارت data scandal (به معنی رسوایی داده) یا scam (یعنی کلاهبرداری) را پیشنهاد می‌کنند. هارت می‌گوید: نتایج این جست‌وجو به شما خواهد گفت آیا به‌تازگی درز داده یا اطلاعات خصوصی به نام این شرکت به ثبت رسیده است یا خیر.

به گفته هارت درصورتی که درز اطلاعات، اتفاقی معمول در این شرکت باشد این جست‌وجو شما را از آن مطلع خواهد کرد و در جریان نحوه واکنش شرکت به چنین اتفاقاتی نیز قرارتان خواهد داد. اگر شرکت موردنظر چند مورد درز اطلاعات را تجربه کرده و کاری برای حل مشکل انجام نداده باشد، به این معنی است که این موضوع را جدی نگرفته و بهتر است از استفاده از نرم‌افزار موردنظر چشم‌پوشی کنید.

جو بیکر، مدیر سیستم فناوری اطلاعات در شرکت Anderson Technologies می‌گوید: عاقلانه است که از استفاده از نرم‌افزار همراهی که تنها محصول یك توسعه‌دهنده نرم‌افزار است یا دیگر نرم‌افزارهای تولیدشده توسط آن هم موارد مشکوکی هستند، خودداری کنید.

محدود کردن حضور در شبکه‌های اجتماعی

انجام این راهکار شاید مشکل‌تر از دیگر راهکارها باشد؛ زیرا نرم‌افزارهای شبکه‌های اجتماعی از پرکاربردترین‌ها در گوشی‌های همراه هستند. به عنوان مثال اگر در حساب کاربری فیسبوك دوست یا نزدیکان‌تان حضور دارید، درحالت آنلاین قابل مشاهده هستید و این سرویس می‌تواند اطلاعاتی مانند علاقه‌مندی‌ها، جهت‌گیری‌های سیاسی و عقاید مذهبی شما را در یك «پروفایل سایه» گردآوری کند. عاقلانه است که جدا از اطلاعاتی که وبگاه در پروفایل از شما می‌خواهد، سایر اطلاعاتی را که در شبکه‌های مجازی به اشتراك می‌گذارید را محدود کنید.

هرچقدر اطلاعات بیشتری به اشتراك بگذارید، داده‌های بیشتری در اختیار آنها قرار خواهید داد تا برای ارائه تبلیغات به شما از آنها استفاده کنند. بهتر است فقط حداقل اطلاعات لازم را پر کنید و برای «تکمیل» اطلاعات. به صورت داوطلبانه. داده‌های اضافی ارائه نکنید.

بابی کیتل برگر، رئیس Legal Software Help در این زمینه می‌گوید: وقتی صحبت از تبلیغات هدفمند است نرم‌افزارهای همراه در گوشی‌های هوشمند بسیار موشکافانه‌تر عمل می‌کنند.

برخی افراد در مورد انجام تبلیغات هدفمندتر با مورد استفاده قراردادن برنامه‌هایی که به میکروفن تلفن همراه شما دسترسی دارند هم ابراز نگرانی می‌کنند. به خاطر داشته باشید هرچقدر اطلاعات بیشتری در پروفایل‌تان ارائه کنید، درصورت به سرقت رفتن اطلاعات، داده‌های بیشتری به خطر خواهد افتاد.

ماشین زمان

ساخت رگ‌های مصنوعی

زمان احتمالی تحقق این فناوری: سال ۱۴۰۶ هجری شمسی / ۲۰۲۷ میلادی

مترجم: نادیا زکالوند

دانش

خانواده‌ای را تصور کنید که در اتاق انتظار بیمارستانی نشسته است. پای چپ پدر خانواده درد می‌کند و در خطر ابتلا به تصلب شریان است. پزشك هم می‌گوید، مقدار قابل توجهی لخته در پای او جمع شده و جریان خون به پا را محدود کرده است و هر لحظه امکان دارد این لخته‌های خون به نقاطی دیگر از بدن حرکت کنند و موجب سکته قلبی یا مغزی شوند. حتی ممکن است آنها مجبور به قطع پای پدر بشوند!

در این‌گونه مواقع جراحی بای‌پس پیشنهاد می‌شود که البته عواض جانبی زیادی هم دارد. در واقع بدن بیمار ممکن است پیوند را قبول نکند و جراحی باز هم تکرار شود یا بیمار جان خود را از دست بدهد.

حتی در پیشرفت‌های چشمگیر پزشکی مدرن امروز در زمینه جراحی عروق، هنوز تا بدون نقص انجام دادن این جراحی فاصله زیادی داریم. معمولا پیوندهای مصنوعی به دلیل این‌که از سلول‌های بدن بیمار ساخته نشده‌اند مورد حمله سیستم ایمنی بدن قرار می‌گیرند و همچنین از آنجاکه ساختارهای بیولوژیکی ندارند، نمی‌توانند خود را با تغییرات محیط پویای بدن سازگار کنند.

اما اخیرا دانشمندان دانشگاه مینه‌سوتا، فناوری تازه‌ای ایجاد کرده‌اند که می‌تواند نوعی رگ خونی مصنوعی در بدن بیمار رشد دهد و سلول‌های این رگ‌ها با سلول‌های بیمار عجین شوند.

اگر این فناوری که در حال حاضر نتایج شگفت‌انگیزی را نشان داده است موفق شود، دیگر عمل جراحی پیوند رگ‌های خونی جان بیماران را به خطر نمی‌اندازد. حتی این فناوری می‌تواند کودکان مبتلا به بیماری‌های مادرزادی قلبی را از جراحی‌های مکرر نجات دهد، زیرا رگ‌های خونی مصنوعی در بدنشان رشد کرده و به جزئی از بدن آنها تبدیل می‌شوند و این بیماران می‌توانند تا پایان عمر این رگ‌های خونی مصنوعی را داشته باشند.

مهندسان بیوپزشکی دانشگاه مینه‌سوتا، هیجان و امید را به این حوزه از پزشکی آورده و نشان داده‌اند مواد مورد استفاده آنها در تولید رگ‌های خونی مصنوعی بسیار موثر است و در مدت یك یا دو دهه دیگر بیماران مبتلا به مشکلات عروقی می‌توانند بدون نگرانی از جراحی‌های مکرر یا خطر مرگ، از این فناوری بهره‌مند شوند. این پیوند رگ‌های خونی دائمی خواهد بود و نیاز به جراحی‌های متعدد نیست.

منبع: Quantumrun

> اخیرا دانشمندان دانشگاه مینه‌سوتا، فناوری تازه‌ای ایجاد کرده‌اند که می‌تواند نوعی رگ خونی مصنوعی در بدن بیمار رشد دهد و سلول‌های این رگ‌ها با سلول‌های بیمار عجین شوند

تازه‌های فناوری

اینوتکس ۲۰۱۹ استارت خورد

هشتمین نمایشگاه بین‌المللی نوآوری و فناوری با حضور بازیگران این اکوسیستم برگزار می‌شود

معاون توسعه نوآوری پارك فناوری پردیس از برگزاری هشتمین نمایشگاه بین‌المللی نوآوری و فناوری (اینوتکس ۲۰۱۹) با برپایی ۴۰۰ غرفه و حضور همه بازیگران اکوسیستم نوآوری و فناوری کشور در خرداد سال جاری خبر داد.

به گزارش جام‌جم و به نقل از ایرنا، اکبر قنبرپور در نشست خبری اینوتکس ۲۰۱۹ در محل کارخانه نوآوری آزادی اظهارکرد: هشتمین نمایشگاه بین‌المللی نوآوری و فناوری (INOTEX ۲۰۱۹) از ۱۹ تا ۲۲ خردادماه ۱۳۹۸ درفضایی ده هزارمتری و در سالن ۴۰ و ۴۴ نمایشگاه بین‌المللی تهران با شعار «اکوسیستم نوآوری و فناوری زیر یك سقف» برگزار می‌شود.

وی ضمن دعوت از تمام بازیگران اکوسیستم استارت‌آپی و فناور کشور برای حضور در این نمایشگاه خاطر نشان کرد: فرآیند ثبت‌نام در نمایشگاه از ۲۵ اسفند سال گذشته آغاز شده و تا ۵ اردیبهشت سال جاری ادامه خواهد یافت. علاقه‌مندان برای دریافت غرفه می‌توانند به سایت رسمی نمایشگاه به نشانی www.inotex.com مراجعه کنند.

دبیر هشتمین نمایشگاه بین‌المللی نوآوری و فناوری (INOTEX ۲۰۱۹) در ادامه هدف از برگزاری این نمایشگاه را افزایش تعامل بین سرمایه‌گذاران و استارت‌آپ‌ها و شرکت‌های فناور، افزایش میزان مشارکت و همکاری‌های دوجانبه و چندجانبه بین شرکت‌ها و استارت‌آپ‌های داخلی و بین‌المللی با یکدیگر و نیز تولید و ارائه محتوای جدید برای اجزای مختلف اکوسیستم نوآوری و همچنین واکاوی چالش‌های این اکوسیستم عنوان کرد.

وی افزود: به منظور دستیابی به این اهداف، بیش از ۴۰۰ استارت‌آپ، شرکت فناور، شتاب‌دهنده، پارك فناوری، مخترع، مرکز رشد، سرمایه‌گذار خطرپذیر، منتور و مشاور همراه با ارائه‌کنندگان خدمات کسب و کار در غرفه‌های نمایشگاه حضور خواهند داشت.

قنبرپور با بیان این‌که غرفه‌داران نمایشگاه اینوتکس ۲۰۱۹ را ۴۰۰ مجموعه مختلف تشکیل می‌دهند، افزود: ما برای مجموعه‌های کوچك‌تر همچون استارت‌آپ‌ها و مخترعان، فضاهایی کوچك‌تر با هزینه کمتر و برای شرکت‌های فناور، مجموعه‌های سرمایه‌گذاری، پارك‌ها و شتاب‌دهنده‌ها، فضای بزرگ‌تری را در نظر گرفته‌ایم. معاون توسعه نوآوری پارك فناوری پردیس با بیان این‌که در اینوتکس ۲۰۱۹ رویدادها و بخش‌های مختلفی از جمله ۴۰۰ جلسه B2B و همچنین ۳۰ پیش رویداد و رویدادهای جانبی برنامه‌ریزی شده است، افزود: پیش‌بینی می‌شود حدود ۸۰۰۰ نفر از این نمایشگاه بازدید کنند.

وی در ادامه با اشاره به سه نقطه تمایز نمایشگاه اینوتکس با سایر نمایشگاه‌ها اظهارکرد: اینوتکس جنبه بازرگانی ندارد، همه بازیگران اکوسیستم نوآوری و فناوری کشور در آن حضور فعال دارند و همچنین در برگزاری این رویداد بزرگ بازیگران اکوسیستم نوآوری کشور درگیر هستند.

قنبرپور همچنین با اشاره به برگزاری نخستین مجمع نوآوری آسیا و اقیانوسیه با همکاری کمیسیون اقتصادی و اجتماعی سازمان ملل متحد (ESCAP) اظهارکرد: برگزاری این مجمع به میزبانی جمهوری اسلامی ایران در دومین کمیته نوآوری ESCAP به تصویب رسیده که با توافقات شکل گرفته با سازمان ملل متحد، این مجمع میزبان سیاستگذاران عرصه علم و فناوری از ۶۳ کشور جهان همزمان با اینوتکس ۲۰۱۹ در محل نمایشگاه بین‌المللی تهران است. وی همچنین با اشاره به برگزاری اولین مجمع پیشگامان اقتصاد دانش‌بنیان همزمان با نمایشگاه اینوتکس بیان کرد: نمایشگاه اینوتکس در سال آتی، میزبان نخستین گردهمایی بزرگ‌ترین شرکت‌های دانش‌بنیان و سرمایه‌گذاران و عناصر اصلی این اکوسیستم به عنوان هسته اصلی تحول و پیشرفت کشور است.

هشتمین نمایشگاه بین‌المللی نوآوری و فناوری (INOTEX ۲۰۱۹) روزهای یکشنبه تا چهارشنبه ۱۹ الی ۲۲ خرداد ۹۸ در محل دائمی نمایشگاه‌های بین‌المللی تهران با شعار «اکوسیستم نوآوری و فناوری زیر یك سقف» برگزار می‌شود.