خبر

ثبت نام در نمایشگاه الکامپ آغاز شد

بر اساس مسوولیت دبیرخانه شورای عالی اطلاع‌رسانی در برپایی و مدیریت سالن دولت الکترونیکی شانزدهمین نمایشگاه بین‌المللی الکترونیک، کامپیوتر و تجارت الکترونیکی (الکامپ)، کلیه دستگاه‌های دولتی متقاضی برای حضور در نمایشگاه می‌توانند از ۱۷ تا ۲۰ مهرماه با مراجعه به وب‌گاه www.elecomp89.scict.ir نسبت به ثبت‌نام اولیه اقدام کنند. به گزارش شرق سعید سالاریان قائم مقام دبیر شورای عالی اطلاع‌رسانی با اعلام مطلب یاد شده تصریح کرد: ثبت‌نام دستگاه‌های دولتی برای حضور در نمایشگاه، تنها از طریق وب‌گاه اعلام شده توسط دبیرخانه شورای عالی اطلاع‌رسانی و در مدت زمان تعیین شده که تمدید نخواهد شد، صورت خواهد گرفت. دبیر ستاد برگزاری بخش دولتی شانزدهمین نمایشگاه بین‌المللی الکامپ با اشاره به فضای ۲۳۰۰ متری سالن ۴۰ که به بخش دولتی اختصاص پیدا کرده است، ویژگی خاص این سالن را مستقل بودن، حضور منسجم بخش‌های دولتی منتخب و ارائه تخفیف ویژه به سازمان‌های دولتی شرکت‌کننده در این نمایشگاه ذکر کرد. سالاریان همچنین از حضور پررنگ دبیرخانه شورای عالی اطلاع‌رسانی و ارائه دستاوردهای آن در نمایشگاه خبر داد. گفتنی است محور خدمات الکترونیکی شامل خدماتی که قابل ارائه به مردم در محل نمایشگاه باشند، خدماتی که تا پایان سال جاری به صورت کاملاً الکترونیکی و بدون مراجعه حضوری مردم ارائه خواهند شد، خدماتی که هم‌اکنون از طریق دفاتر پیشخوان (یا دفاتر مشابه) ارائه می‌شوند یا تا پایان سال جاری ارائه خواهند شد، خدماتی که در بستر الکترونیکی و در تعامل با سایر دستگاه‌های اجرایی ارائه می‌شوند و معرفی فناوری‌های نوین به کارگرفته شده در ارائه خدمات الکترونیکی تعریف شده است.

ویروس سارق کلمه عبور کاربران کشف شد

یک تروژان فایرفاکس از سوی محققان امنیتی کشف شده که کاربران این مرورگر اینترنتی را وادار می‌کند کلمه عبور خود را ذخیره کرده و سپس از آن برای ایجاد حساب کاربری جدید در رایانه آلوده استفاده می‌کند. به گزارش ایسنا، بیشتر محققان امنیتی به کاربران فایرفاکس توصیه کرده‌اند گزینه «به خاطر سپردن کلمه عبور» را در مرورگر خود انتخاب نکنند زیرا کلمات عبور ذخیره‌شده به سادگی توسط این بدافزار گرفته می‌شوند. بدافزار Trojan-PWS-Nslog که توسط شرکت امنیتی «وب روت» کشف شده، با غیرفعال کردن کد فایرفاکس که از کاربر هنگام ورود به یک سایت معتبر درباره ذخیره کردن کلمه عبور می‌پرسد، ترجیحات کاربری را دور می‌زند. این تروژان با اطلاعاتی که به دست می‌آورد، حساب جدیدی تحت نام Maestro در رایانه آلوده ایجاد می‌کند و سپس اطلاعات را از رجیستری و بخش معروف به ذخیره‌سازی تحت حفاظت که توسط مرورگر اینترنت اکسپلورر برای ذخیره کلمات عبور استفاده می‌شود و همچنین از ذخیره‌سازی کلمه عبور خود فایرفاکس می‌گیرد و تلاش می‌کند اطلاعات مسروقه را ارسال کند. دامنه‌های اینترنتی که به منظور دریافت اطلاعات به سرقت رفته توسط این تروژان درنظر گرفته شده، بسته شده‌اند اما کد داخل بدافزار نام نویسنده و نشانی ای‌میل وی را برملا کرده و وب روت را به صفحه هکری در فیس بوک هدایت می‌کند. این هکر یک ابزار ایجادکننده کی‌لاگر رایگان را ارائه می‌کند که کاربران ویندوز مایکروسافت را هدف می‌گیرد. بر اساس گزارش Net Applications، فایرفاکس موزیلا با ۲۳ درصد سهم در ماه سپتامبر، در بازار مرورگر جهانی در رتبه دوم قرار دارد. به تازگی نخستین نسخه آزمایشی بتا فایرفاکس ۴ برای تلفن‌های آندرویدی منتشر شده است.

دانلود اطلاعات از فیس بوک امکان‌پذیر شد

فیس‌بوک اعلام کرد کاربران از این پس امکان دانلود اطلاعات را از این شبکه اجتماعی دارند. به گزارش موبنا دانلود اطلاعات از فیس‌بوک ویژگی جدیدی است که بزرگ‌ترین شبکه اجتماعی دنیا برای کاربران ارائه کرده و امکان دانلود همه اطلاعات را از پروفایل فیس‌بوک فراهم می‌کند. بر این اساس کاربران می‌توانند اطلاعات فیس‌بوک را همانند یک فایل فشرده دانلود کنند که همه اطلاعات از کانکت‌ها و پیام‌ها را شامل می‌شود. این ویژگی جدید از بخش تنظیمات اکانت کاربران قابل دسترس است و اطلاعات دانلود شده از این وب‌سایت حذف نمی‌شود. بنابراین کاربران می‌توانند نسخه پشتیبانی از اطلاعات فیس‌بوک‌شان بگیرند پیش از اینکه از آن خارج شوند.

ساخت دیسک نوری با ظرفیت ۳۲۰ گیگابایت

شرکت TDK نمونه اولیه از دیسک نوری جدیدی را به نمایش گذاشته است که می‌تواند ۳۲۰ گیگابایت اطلاعات را در خود جا دهد که این میزان شش برابر بیشتر از پرظرفیت‌ترین دیسک‌های کنونی است. به گزارش آی‌تی‌ایران این دیسک نوری ۱۲ سانتی‌متری شامل ۱۰ لایه مجزا برای ذخیره اطلاعات است که هر کدام از این لایه‌ها می‌توانند ۳۲ گیگابایت اطلاعات را در خود جا دهند. دیسک‌های بلو-ری که هم‌اکنون به عنوان پرظرفیت‌ترین دیسک نوری در جهان محسوب می‌شوند، در بیشترین حالت ممکن تنها دو لایه ذخیره‌کننده اطلاعات را در خود جا داده‌اند و در هر لایه تنها ۲۵ گیگابایت از اطلاعات را ذخیره می‌کنند. به طور کلی هر چه تعداد لایه‌های یک دیسک افزایش یابد، خواندن و ذخیره اطلاعات در آن دشوارتر می‌شود. زیرا نور لیزر برای عبور از این لایه‌ها مشکلات بیشتری را پیش‌رو دارد. مهندسان شرکت TDK به منظور حل این مشکل از نوعی پلاستیک شفاف استفاده کرده‌اند که نور لیزر با آسانی بیشتری می‌تواند از لایه‌های آن عبور کند. این دیسک در حالی عرضه شده که شرکت TDK در سال ۲۰۰۶ نمونه دیگری از آن را با حجم ۲۰۰ گیگابایت به نمایش گذاشته بود.

مصلی میزبان چهارمین دوره است

آغاز جشنواره رسانه‌های دیجیتال

حامد شفیعی


عکس: مرضیه موسوی، ایرنا

برپایی جشنواره و نمایشگاه رسانه‌های دیجیتال تهران که برای چهارمین بار و این بار به صورت بین‌الملل در سطحی به وسعت مصلای تهران از ۱۵ مهرماه آغاز به کار کرد، دیدگاه‌های متفاوتی را نسبت به سطح کیفی و کمی به همراه داشت. برخی نمایشگاه امسال را ضعیف‌تر و برخی بهتر از سال قبل می‌دانند. اگر این سوال را که وضعیت نمایشگاه را نسبت به سال قبل چگونه ارزیابی می‌کنید از مسوولان برگزارکننده بپرسید، بی‌شک با این پاسخ مواجه خواهید شد که برپایی چنین نمایشگاهی در سطحی وسیع چه به لحاظ وسعت فیزیکی و چه به لحاظ کمیت محصولات و خدمات ارائه‌شده که در سطح کشور و منطقه بی‌نظیر است، بدون همکاری و هماهنگی بخش‌های دولتی و بخش خصوصی امکان‌پذیر نبوده یا به صورت ایده‌آل انجام نخواهد شد. این همکاری‌ها در بخش‌ها و سطوح مختلف به لحاظ کیفی و کمی متفاوت و قابل توجه است. یکی از مواردی که نیازمند همکاری مستمر و تنگاتنگ این دو قشر است، مبحث نظم و انضباط نمایشگاهی است که ضامن امنیت و فروش و ارائه هرچه بهتر محصولات و در نهایت رضایت دوسویه مسوولان و غرفه‌داران خواهد شد. اما در مقابل برخی غرفه‌داران و بازدیدکنندگان نظری متفاوت از برگزارکنندگان دارند و این‌گونه پاسخ می‌دهند که نمایشگاه امسال دچار ضعف هماهنگی است؛ در عین حال چیز تازه‌ای برای ارائه وجود نداشت. با این حال این جشنواره با اهداف گوناگونی که مسوولانش در ۱۰ بند از جمله جریان‌سازی و بسترسازی برای تولید و توسعه محتوای منطبق بر فرهنگ بومی، ملی و اسلامی در حوزه رسانه‌های دیجیتال و بسترسازی و فراهم کردن زمینه لازم برای تحقق جنبش نرم‌افزاری در حوزه محتوایی فناوری اطلاعات خلاصه کرده‌اند به مدت ۱۰ روز برپا خواهد بود.

از هدف تا آنچه عرضه می‌شود

بازدید از جشنواره و نمایشگاه رسانه‌های دیجیتال فرصتی است تا بتوان آنچه ارائه شده و آنچه به عنوان هدف تعیین شده را تطبیق داد. آنچه در نمایشگاه امسال ارائه شده کمتر به اهداف تعیین‌شده نزدیک است. در عین حال که با وجود عدم مشارکت بنیاد ملی بازی‌های رایانه‌ای، حضور غرفه‌های بازی طیف گسترده‌ای از گروه سنی نوجوانان را که شاید کمتر به مساله رسانه‌های دیجیتال آشنایی دارند، به خود جذب کرده است. از این رو می‌توان استقبال از نمایشگاه را مرهون حضور اپراتورها و بازی‌های رایانه‌ای دانست. هرچند در بندهای گفته شده به عنوان هدف، نامی از ارائه محصولات تلفن همراه و دستاوردهای آن در عرصه رسانه‌های دیجیتال آورده نشده است. از طرفی سنگینی وزنه ترازوی نمایشگاه امسال بیشتر به سمت غرفه‌هایی است که به موضوع جنگ نرم و جنگ سایبری می‌پردازند. البته از حق نگذریم امسال ابتکار خوبی نسبت به سال قبل صورت گرفت و آن اینکه در جشنواره نمایشگاه امسال، محل و موضوع غرفه‌ها را با رنگ‌های متفاوت برای آگاهی مردم در نظر گرفته‌اند. برای نمونه، بخش پایگاه‌های اینترنتی و وبلاگ‌ها با رنگ آبی فیروزه‌ای، بخش پژوهش، فناوری و نوآوری با رنگ نارنجی، بازی‌های رایانه‌ای با رنگ صورتی و نرم‌افزارهای رسانه‌ای با رنگ قرمز مشخص شده است.

اطلاع رسانی، فقط به صورت موردی

اگر شما جزء آن دسته از افرادی هستید که هنگام ورود به نمایشگاه به دنبال جایگاه اطلاع‌رسانی برای به دست آوردن اطلاع در مورد شرکت یا نهادی هستید، امسال مکان‌های متعددی را به این امر اختصاص داده‌اند. اما باید این را در نظر بگیرید که هنگام پرسش از متصدیان اطلاع‌رسانی از آنها نام محصول را نخواهید، زیرا اطلاعی در سیستم‌های رایانه‌ای آنها در این زمینه ثبت نشده و شما تنها می‌توانید نام شرکت را بپرسید. در عین حال آنها نمی‌توانند اسامی شرکت‌کنندگان را به صورت کلی در اختیار بازدیدکنندگان قرار دهند، زیرا چنین چیزی ندارند و فقط به صورت موردی اطلاعات ارائه می‌دهند. همکاران رسانه‌ای نیز اگر به دنبال پاویونی برای فعالیت‌های رسانه‌ای خود هستند، می‌توانند از ستاد خبری نمایشگاه که به فعالیت‌های رسانه‌ای می‌پردازد، بروند و از امکانات آنان استفاده کنند.

نکته

بخش بین‌الملل نمایشگاه از ۱۷ مهرماه افتتاح شده و چنانچه بازدیدی از این محل صورت گیرد، از میان تعداد کشورهای ذکرشده پنج کشور امریکای لاتین، دو کشور امریکای شمالی، یک کشور اروپایی- انگلستان آن هم به صورت نمایندگی که در ایران دارد- و از کشورهای آسیایی نیز مالزی، پاکستان، افغانستان، سریلانکا و روسیه حضور خواهد داشت. کشوری مانند ایتالیا در قالب سخنرانی حضور خواهد داشت.

بخش بین‌الملل و حضور کشورها

بنابر اظهارات مسوولان برگزاری چهارمین جشنواره و نمایشگاه رسانه‌های دیجیتال، امسال ۳۰کشور در نمایشگاه حضور دارند که به ارائه دستاوردهای خود در حوزه رسانه‌های دیجیتال می‌پردازند. بر اساس اعلام آنان کشورهایی مانند ایتالیا، انگلستان، برخی کشورهای آسیایی و ۱۰ کشور امریکای لاتین به همراه امریکای شمالی حضور دارند. بخش بین‌الملل نمایشگاه از ۱۷ مهرماه افتتاح شده و چنانچه بازدیدی از این محل صورت گیرد، از میان تعداد کشورهای ذکرشده پنج کشور امریکای لاتین، دو کشور امریکای شمالی، یک کشور اروپایی- انگلستان آن هم به صورت نمایندگی که در ایران دارد- و از کشورهای آسیایی نیز مالزی، پاکستان، افغانستان، سریلانکا و روسیه حضور دارند. کشوری مانند ایتالیا در قالب سخنرانی حضور خواهد داشت. کشورهایی مانند بولیوی، اکوادور، مالزی، کوبا و نیکاراگوئه نیز حضور دارند و به معرفی کشورهای خود و نشان دادن آداب و سنن، صنایع دستی و تحفه‌هایشان می‌پردازند. البته در همان ابتدای آغاز به کار بخش بین‌الملل، به دلیل علاقه‌ای که جوانان ما به کشورهای خارجی دارند، استقبال قابل توجهی صورت گرفت. طبقه بالای مصلای تهران به این بخش و همچنین بخش خانواده و رسانه و رسانه‌های دیجیتال در آیینه هنر اختصاص دارد.

دستاوردهای نهادها و سازمان‌ها، یکی در میان

با برنامه‌ریزی‌های صورت گرفته، قرار بر این بوده امسال تمامی استان‌های کشور، اداره فرهنگ و ارشاد، به همراه دانشگاه‌ها و نهادهای اجرایی حضور داشته باشند. فضای در نظر گرفته شده برای نهادها با رنگ سبز یشمی مشخص است. نخست آنکه تمامی استان‌ها حضور ندارند و برخی از غرفه‌های مربوط به تعدادی از استان‌ها خالی است که احتمال می‌رود تا هفته آینده پر شود، دوم آنکه دانشگاه‌های حاضر دستاوردهایی را که باید و شاید داشته باشند، ارائه نکرده‌اند و برخی از آنها در مکان‌هایی قرار داده شده‌اند که دور از چشم بازدیدکننده است، سوم آنکه از نهادهای اجرایی تنها وزارت ارشاد، وزارت آموزش و پرورش، وزارت ارتباطات و فناوری اطلاعات، صداوسیما، بنیاد شهید و امور ایثارگران، سازمان ملی جوانان و سازمان بسیج مستضعفین به همراه ارتش حضور دارند. برای تعداد اندکی از بانک‌های کشور نیز به منظور ارائه فناوری‌های بانکداری الکترونیکی خود، و نه در حوزه رسانه‌های دیجیتال غرفه‌هایی در نظر گرفته شده که البته فضای مشخصی ندارند. نکته‌ای که باید یادآوری شود این است که اگر هنگام بازدید به غرفه‌هایی برخوردید که ارتباطی با جشنواره رسانه‌های دیجیتال ندارند، تعجب نکنید، زیرا این نوع غرفه‌ها در اغلب نمایشگاه‌های کشور حضور دارند. با این وجود چهارمین نمایشگاه و جشنواره بین‌الملل رسانه‌های دیجیتال، در قالب رنگ‌ها و موضوعات متنوع که از ۱۵ مهرماه آغاز به کار کرده و تا ۲۴ مهرماه ادامه دارد، فرصت مناسبی برای بازدید نوجوانان، جوانان و حتی خانواده‌هایی است که به همراه فرزندان خردسال خود برای آشنایی بیشتر با رسانه‌های دیجیتال به این نمایشگاه بیایند.

آنلاین

رهایی از چنگال ویروس‌ها

همه ما درباره حضور گسترده بدافزارها در دنیای کامپیوتر و اینترنت آگاهی داریم؛ بدافزارها شامل برنامه‌هایی هستند که جاسوسی کرده، داده‌ها را تخریب می‌کنند، به دیسک سخت صدمه می‌زنند یا اختیار کامپیوتر را در دستان فردی هزاران کیلومتر دورتر از شما قرار می‌دهند اما با تمامی این اوصاف چگونه می‌توان از شر این بدافزارها خلاص شد. به گزارش ایسنا، مهم نیست که بدافزارها چه ظاهری داشته باشند، آنها خرابکار هستند و از آنجا که تعداد بی‌شماری بدافزار در فضای تبادل اطلاعات وجود دارند، بالاخره هر فردی روزی قربانی آنها خواهد شد و فقط مساله زمان مطرح است. مهم‌ترین توصیه برای فردی که گمان می‌کند رایانه وی توسط بدافزارها آلوده شده، عبارت است از اینکه اولاً وحشت‌زده نشود، ثانیاً فرض نکند لازم است تمام اطلاعات دیسک سخت را پاک کرده و از اول شروع کند. اغلب اوقات می‌توان بدافزار را بدون از دست دادن چیزی حذف کرد. گاهی اوقات ممکن است کاربر برخی داده‌ها را از دست بدهد ولی احتمالاً همه چیز را از دست نخواهد داد. در وهله اول لازم است مشخص شود آیا اصلاً کامپیوتر آلوده شده است یا خیر. در صورتی که کامپیوتر به نظر بسیار کند می‌رسد، می‌توان به آن مشکوک شد. یا اگر مرورگر وب تغییر شکل داده و به صورت خودکار به وب‌سایتی می‌رود که برای کاربر ناشناس است، علامت خوبی برای وجود یک بدافزار روی رایانه است. ناپایداری سیستم و از کار افتادن‌های مداوم نیز نشان‌دهنده وجود مشکلی در آن است. یک نشانه دیگر در زمان دسترسی به فایل‌ها یا درایوها رخ می‌دهد که پیغام خرابی آنها نمایش داده می‌شود. در صورتی که فردی فکر می‌کند کامپیوتر او آلوده شده است، لازم است با استفاده از یک برای همه کاربران یک ضرورت محسوب می‌شود. در اینجا سوالی که برای اکثر کاربران مطرح می‌شود این است که آیا نصب دو آنتی‌ویروس به صورت هم‌زمان خطر آلودگی را کاهش می‌دهد. در جواب باید گفت اجرای بیش از دو آنتی‌ویروس سرعت کامپیوتر را بسیار پایین آورده و از طرف دیگر بسیاری از آنتی‌ویروس‌ها با یکدیگر سازگاری نداشته و اجازه نصب یک آنتی‌ویروس دیگر را به شما نمی‌دهند و در صورت نصب نیز ممکن است سیستم شما را بیش از پیش به خطر اندازند. در صورتی که آنتی‌ویروس اعلام کند بدافزار را با موفقیت پاک کرده است، لازم است کامپیوتر راه‌اندازی مجدد شود. بهتر است بعد از دوباره بالا آمدن سیستم، برنامه آنتی‌ویروس یک بار دیگر اجرا شود و در صورتی که لیست بدافزارهای آن خالی باشد، یعنی کار با موفقیت به پایان رسیده است. در نظر داشته باشید اگر بدافزارهای دیگری در لیست مشاهده می‌شوند، لازم است گام‌های قبلی دوباره تکرار شوند. اما در صورتی که آنتی‌ویروس همان بدافزارهای قبلی را پیدا کند، باید روش‌های دیگری را امتحان کرد.

آنتی‌ویروس آنها را از روی سیستم پاکسازی کند. برخی از ویروس‌ها هوشمند بوده و برنامه آنتی‌ویروس را غیرفعال می‌سازد. در صورتی که هیچ‌گونه آنتی‌ویروسی روی کامپیوتر نصب نیست، لازم است حتماً یک نسخه خریداری شده یا به صورت آنلاین دریافت شود. البته تعداد کمی از بدافزارها دسترسی کاربر به وب‌سایت‌های امنیتی را محدود کرده و اجازه دریافت آنتی‌ویروس را به وی نمی‌دهند. در صورت بروز این مشکل باید نرم‌افزارهای مذکور توسط یک سیستم دیگر دریافت شده و سپس از طریق سی‌دی یا حافظه فلش به کامپیوتر آلوده منتقل شود. نصب یک آنتی‌ویروس روی سیستم

دنیای نرم‌افزار

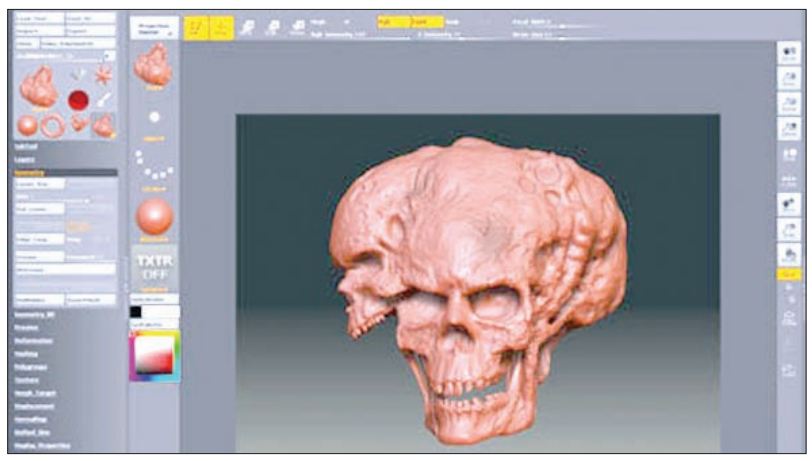
حکاکی سه‌بعدی به کمک نرم‌افزار

شرق: طراحی تصاویر سه‌بعدی امروزه با استفاده از نرم‌افزارهای مختلفی امکان‌پذیر است. ایجاد تصاویر انیمیشن برای کودکان، ساخت تیزرهای تبلیغات سه‌بعدی، ایجاد تصاویر مربوط به فیلم‌ها، ساخت نماهای ثابت سه‌بعدی و... همگی به راحتی و توسط نرم‌افزارهای مختلف ایجاد تصاویر سه‌بعدی امکان‌پذیر است.

کاربرانی که با دنیای نرم‌افزارها آشنایی دارند خصوصاً نرم‌افزارهای خاص طراحی، به نوعی پس از شنیدن اصطلاح سه‌بعدی و نرم‌افزار مربوط به آن در بیشتر موارد نرم‌افزار معروف و حرفه‌ای 3D Max در ذهن آنها نقش می‌بندد. این نرم‌افزار یک برنامه کامل و به صورت کاملاً حرفه‌ای به شمار می‌آید که علاوه بر اینکه هنگام کار با آن باید آشنایی کامل با ابزارها داشت، نیاز به سیستم‌های قدرتمند از نظر سخت‌افزاری و به خصوص کارت‌گرافیک و حافظه دارد. بسیاری از نرم‌افزارهای دیگر را نیز امروزه می‌توان یافت که به کمک آنها می‌توان تصاویر سه‌بعدی حرفه‌ای را ایجاد کرد و استفاده از آنها برای کاربران در مقابل نرم‌افزارهایی همچون 3D Max بسیار آسان‌تر است، به همین علت در این مطلب سعی داریم شما را با نرم‌افزاری قوی آشنا کنیم که کار کردن با آن نیاز به تسلط خاص مانند نرم‌افزار حرفه‌ای 3D Max ندارد. ZBrush نام نرم‌افزاری فوق‌العاده حرفه‌ای برای ساخت و طراحی تصاویر سه‌بعدی Sculp ture یا حکاکی‌مانند طبیعی در اثر سه‌بعدی است که به کمک آن کاربران می‌توانند اقدام به ساخت تصاویر سه‌بعدی حرفه‌ای کنند. در دنیای سینمای مدرن امروزه این نرم‌افزار در ساخت اکثر شخصیت‌ها و هیولاهای مخوف به کار می‌رود. در این نرم‌افزار ابزارهای مختلفی برای ساخت این تصاویر قرار داده شده‌اند که دسترسی به آنها با توجه به نحوه طراحی و قرارگیری ابزارهای در دسترس کاربر بسیار سریع است.

این نرم‌افزار دارای ویژگی‌های بسیاری است که از جمله آن می‌توان به این موارد اشاره داشت:

- ساخت تصاویر سه‌بعدی بدون پشت‌زمینه
- قابلیت وارد کردن (Import) تصاویر مختلف به منظور استفاده در تصویر سه‌بعدی



- قدرت بالا در Render کردن تصاویر
- ارائه پیش‌نمایش‌های Real Time هنگام طراحی
- قابلیت استفاده از ابزارهای Mesh Morphing
- ابزارهای بهینه‌سازی تصویر و حجم آن
- ابزار بازگشتی به آخرین مرحله انجام‌شده
- قابلیت ذخیره‌سازی تصاویر خروجی در فرمت‌های Swf3، ds، html و... و ده‌ها ویژگی برتر دیگر که علاقه‌مندان به کسب اطلاعات بیشتر در خصوص نرم‌افزار یادشده و همچنین بارگذاری رایگان آن می‌توانند به سایت p30world.com مراجعه کنند. گفتنی است این نرم‌افزار قدرتمند در زمینه ساخت تصاویر سه‌بعدی محصولی از شرکت Pixologic به‌شمار می‌آید.

جرائم رایانه‌ای

هکینگ؛ یک دسترسی غیرمجاز

فرزاد تحیری*

دسترسی غیرمجاز از جمله جرائمی محسوب می‌شود که دارای نقشی زاینده در ارتکاب سایر جرائم رایانه‌ای، به خصوص جرائم رایانه‌ای محض است. به همین دلیل در محیط سایبر به عنوان جرمی مادر تلقی می‌شود. در میان متخصصان چه حقوقی و چه فنی نسبت به مفهوم دسترسی غیرمجاز، وحدت نظر وجود ندارد. متخصصان فنی از عبارت «هکینگ» استفاده می‌کنند و منظور از آن را «هر نوع حمله به سیستم‌های ایمن بیان می‌کنند»، برخی دیگر «هکینگ» را در معنی محدودتر، «نفوذیابی» یا «نفوذگری» ترجمه می‌کنند. عده‌ای نیز «هکینگ» را مترادف با دسترسی غیرمجاز می‌دانند. به نظر می‌رسد «هکینگ» را نمی‌توان مترادف با دسترسی غیرمجاز تلقی کرد زیرا «هکینگ» چه در عنوان، چه در آماج، چه در نوع سیستم بر حسب ایمن یا غیرایمن بودن و چه در وسعت شمول افعال مادی، با دسترسی غیرمجاز متفاوت است: نخست آنکه «هکینگ»، عنوانی است اختصاصی که تنها در دانش فنی- مهندسی (علوم رایانه‌ای) به کار می‌رود و در این دانش، معنایی خاص و فنی دارد، دوم آنکه دسترسی غیرمجاز به سیستم‌ها و داده‌های رایانه‌ای مربوط می‌شود در حالی که «هکینگ» تنها راجع به سیستم‌های رایانه‌ای است و سوم آنکه دسترسی غیرمجاز به همه سیستم‌ها حتی «بدون محافظ» نیز گفته می‌شود در حالی که ایمن بودن سیستم‌ها از قیود تفکیک‌ناپذیر در «هکینگ» است و در نهایت اینکه در دسترسی غیرمجاز صرف دسترسی به سیستم‌ها و داده‌های رایانه‌ای جرم است در حالی که در «هکینگ»، علاوه بر دسترسی غیرمجاز اقداماتی دیگر نیز انجام می‌گیرد. متخصصان حقوق کیفری رایانه از عباراتی دیگر مانند نفوذ غیرمجاز، ورود غیرمجاز، دستیابی غیرمجاز استفاده می‌کنند که به زعم ما همه آنها در زیرمجموعه دسترسی غیرمجاز قرار می‌گیرند. به این ترتیب، دسترسی غیرمجاز عبارت است از: « دسترسی بدون مجوز به سیستم‌ها یا داده‌های رایانه‌ای (جزئاً یا کلاً) یا بدون نقض تدابیر ایمنی یا حفاظتی آنها.» دسترسی غیرمجاز، جرمی است که عموماً توسط افراد برنامه‌نویس و متخصص در علوم رایانه‌ای ارتکاب می‌یابد. در تقسیم‌بندی‌های سنتی از جرائم می‌توان آن را از زمره جرائم علیه اموال محسوب داشت. همچنین جرمی است عمدی، آنی، مطلق و غیرمشهود. از آنجایی که دسترسی غیرمجاز، در ارتکاب بسیاری از جرائم رایانه‌ای (خصوصاً جرائم رایانه‌ای محض) دارای تاثیر و نقش است به عنوان جرمی مادر یا زاینده، معروف است. تاکنون از جانب هیچ مرجع رسمی آماری در خصوص میزان دسترسی‌های غیرمجاز منتشر نشده و تنها تا به حال چندین مورد انگشت‌شمار در اخبار منتشر شده است. به نظر می‌رسد رقم سیاه در این خصوص در ایران بالا باشد زیرا سیستم‌ها و شبکه‌های رایانه‌ای به طور مناسب ایمن نشده‌اند و اصولاً به دلیل امکانات کم مادی چنین هزینه‌هایی وجود ندارد. در عین حال بسیاری از مدیران سیستم‌ها فاقد اطلاعات تخصصی و حتی عمومی هستند و گاه از روی بی‌احتیاطی زمینه دسترسی غیرمجاز را فراهم می‌کنند و تا به حال دسترسی غیرمجاز مانند سایر جرائم رایانه‌ای جرم‌انگاری نشده است. دسترسی غیرمجاز بر اساس آماج (شامل دسترسی به سیستم‌ها و دسترسی به داده‌های رایانه‌ای)، محیط وقوع جرم (محل فیزیکی سیستم‌ها، دسترسی در داخل یا خارج از شبکه، دسترسی بر اساس دوری و نزدیکی سیستم‌ها نسبت به مرتکب شامل دسترسی از راه نزدیک و دسترسی از راه دور)، تمهیدات حمایتی و حفاظتی (سیستم‌های محافظت‌شده و بدون محافظ، سیستم‌های حمایت‌شده و بدون حمایت، دسترسی با نقض و بدون نقض تدابیر حفاظتی)، نتیجه ارتکاب (مطلق و مقید) و شیوه ارتکاب (دسترسی ساده یا محض، کسب اطلاع به نحو غیرمجاز، تحصیل اطلاعات به نحو غیرمجاز) قابل تقسیم است. دسترسی غیرمجاز از زمره جرائم عمدی تلقی می‌شود. انگیزه در دسترسی غیرمجاز بدون اینکه تاثیری در ماهیت جرم داشته باشد، مختلف و متنوع است. انگیزه مجرمانه را می‌توان شامل انگیزه‌های شرافتمندانه شامل بالا بردن امنیت سیستم‌ها، مراقبت از سیستم‌ها در برابر آسیب، کمک به پیشرفت دانش فنی و مهندسی و... و غیرشرافتمندانه شامل غرض‌ورزی و انتقام‌جویی، کسب شهرت، انگیزه‌های مالی، حسادت و... دانست. گفتنی است انگیزه‌های یاد شده هیچ تاثیری در ماهیت جرم ندارد و در نهایت ممکن است به عنوان عاملی تخفیف‌دهنده محسوب شود. دسترسی غیرمجاز، «عاملی محرک» در ارتکاب سایر جرائم رایانه‌ای (خصوصاً جرائم رایانه‌ای محض) است. غالب دست‌یابندگان غیرمجاز پس از دسترسی به سیستم به صرف دسترسی بسنده نکرده و اقداماتی دیگر که ممکن است دارای وصف مجرمانه نیز باشد انجام می‌دهند. نسخه‌برداری از داده‌ها، اختلال در سیستم انتشار برنامه‌های مخرب و... از این جمله است. در قوانین جزایی اعم از مجموعه قانون مجازات اسلامی و سایر قوانین جزایی پراکنده دیگر، هیچ ماده قانونی در خصوص دسترسی غیرمجاز به چشم نمی‌خورد زیرا اصولاً در مجموعه قوانین جزایی ایران تاکنون به جرائم رایانه‌ای پرداخته نشده است. در بررسی قوانین جزایی سنتی چنین نتیجه‌گیری می‌شود که در برخی از آنها دسترسی غیرمجاز به عنوان یکی از شیوه‌های ارتکاب و در برخی دیگر به عنوان یک عامل تسهیل‌کننده محسوب می‌شود. با این حال بر اساس ماده ۴ قانون جرائم رایانه‌ای «هر کس عمداً و بدون مجوز با نقض تدابیر حفاظتی سیستم یا داده‌های رایانه‌ای یا مخابراتی به آنها دسترسی یابد به جزای نقدی تا شش میلیون ریال یا به حبس تا یک سال محکوم می‌گردد.» بر اساس این قانون دسترسی غیرمجاز مقید به سیستم‌های ایمن و نیز نقض تدابیر ایمنی شده است، همچنین آماج سیستم و داده قرار داده شده و سیستم‌های غیرایمن و نیز دسترسی بدون نقض تدابیر ایمنی از شمول ماده یادشده خارج است.

*دانشجوی کارشناسی ارشد رشته حقوق جزا و جرم‌شناسی