رویداد

حرکت لاک‌پشتی در فضای مجازی، ما را به مقصد نمی‌رساند

■ **ایسنا:** به گفته وزیر فرهنگ و ارشاد اسلامی با توجه به لزوم راه‌اندازی نهضت نرم‌افزاری دینی، حرکت لاک‌پشتی در فضای مجازی ما را به مقصد نمی‌رساند. محمد حسینی با بیان مطلب فوق افزود: امروزه سرمایه‌گذاری زیادی از سوی آمریکا و غرب در مقوله فضای مجازی انجام می‌شود و ما هم قطعا باید سرمایه‌گذاری بیشتری داشته باشیم. وی ادامه داد: آمریکا می‌خواهد سفارتخانه مجازی ایجاد کند و دشمنان در بسیاری از موارد از نیروهای بی‌جیره و مواجب استفاده و یارگیری می‌کنند. در فضای مجازی نیز می‌خواهند از نیروهای کشورهای دیگر به خصوص کشور ما استفاده کنند تا به اهداف خود برسند که ما هم در مقابل باید همه جوانان را در این حوزه بر ضد آنان بسیج کنیم.

ضریب نفوذ اینترنت شهری در مرز ۱۹درصد

■ **شرق:** بر اساس گزارش مرکز آمار ایران ضریب نفوذ اینترنت کل شهرهای کشور در سال ۸۹ معادل ۱۸/۹ و روستاها چهاردرصد اعلام شد. طبق این گزارش جمعیت روستایی در سال ۸۸ با داشتن جمعیتی معادل با ۲۳میلیون و ۴۳۰هزار و ۹۷۵نفری، جمعیت ۷۰۷هزار و ۷۴۱ نفری از کاربران اینترنت داشت که ضریب نفوذی برابر با سه‌درصد را به خود اختصاص داد. در سال گذشته و با توجه به جمعیت ۵۳ میلیون و ۸۹۱هزار و ۴۸۱نفری شهری، ۱۰ میلیون و ۱۵۹هزار و ۵۰۴ نفر کاربر اینترنت در شهرها بوده‌اند که ضریب نفوذ آن ۱۸/۹درصد می‌شود و همین آمار به نسبت جمعیت کل ۲۰ میلیون و ۹۴۶هزار و ۳۱۱ روستایی عدد ۸۴۲هزار و ۷۴۴ نفری را کاربر اینترنت عنوان می‌کند که ضریب نفوذ آن چهاردرصد می‌شود.

تکلیف دستگاه‌ها برای تجهیز سیستم‌های امنیتی

■ **ایسنا:** معاون گسترش فناوری اطلاعات سازمان فناوری اطلاعات از تکلیف دستگاه‌ها برای تجهیز به سیستم‌های مدیریت امنیت اطلاعات خبر داد. اسماعیل اردکانی با اعلام این خبر گفت: در برنامه پنجم به تمامی دستگاه‌ها تکلیف و گفته شده است که همه آنها باید تا پایان سال دوم برنامه به سیستم‌های مدیریت امنیت اطلاعات مجهز شوند. به گفته وی خرید کلیه محصولات امنیتی برای محصولات خارجی ممنوع است اما متقاضیان در شرایط خاص می‌توانند از سازمان فناوری اطلاعات تاییدیه بگیرند. وی ادامه داد: بررسی و احراز صلاحیت برای فعالیت این شرکت‌ها که باید در دستگاه‌ها ذیل ماده پنج قانون خدمات کشوری فعالیت کنند، بر عهده سازمان فناوری اطلاعات است تا پروانه‌هایشان را صادر کند. وی افزود: بخشنامه‌ای در اردیبهشت‌ماه به تمامی دستگاه‌های دولتی ابلاغ شد تا خرید کلیه محصولات امنیتی به واسطه آن ممنوع شود، مگر آنکه در موارد خاصی باشد و در آن شرایط باید از سازمان فناوری اطلاعات تاییدیه بگیرند.

ممنوعیت ایجاد شبکه اختصاصی توسط دستگاه‌ها

■ **فارس:** وزیر ارتباطات و فناوری اطلاعات، در نامه‌ای خطاب به تمام دستگاه‌های اجرایی، ایجاد هرگونه شبکه اختصاصی توسط دستگاه‌ها را بدون هماهنگی با وزارت ارتباطات و فناوری اطلاعات، ممنوع اعلام کرد. رضا تقی‌پور ماه گذشته در نامه‌ای خطاب به تمام دستگاه‌های اجرایی، ایجاد هرگونه شبکه اختصاصی توسط دستگاه‌ها را بدون هماهنگی با وزارت ارتباطات و فناوری اطلاعات، ممنوع اعلام کرده است. بر اساس این گزارش، در این نامه آمده است: با استناد به ماده ۴۶ قانون برنامه پنجم توسعه، این وزارت مکلف به ایجاد و توسعه شبکه ملی اطلاعات است و از آنجا که شبکه‌های اختصاصی (WAN) بین واحدهای سازمانی دستگاه‌ها در کشور، جزو زیرشاخه‌های این شبکه محسوب می‌شود، از تاریخ صدور این بخشنامه ایجاد هرگونه شبکه اختصاصی توسط دستگاه‌ها بدون هماهنگی با این وزارت ممنوع است و تمامی دستگاه‌ها موظفند هم بند (توپولوژی) و روش‌های اجرای شبکه‌های اختصاصی خود را با وزارت ارتباطات و فناوری اطلاعات (سازمان فناوری اطلاعات ایران) نهایی و تاییدیه سازمان یادشده را دریافت کنند.

واکنش «سامسونگ» به پخش تیزر تبلیغاتی صهیونیستی علیه ایران

■ **بیانیه «سامسونگ»: هیچ نقشی در تولید این کلیپ نداشتیم**

شرق: رسانه‌های صهیونیستی از طرح محرمانه واحدهایی از موساد برای تخریب روابط ایران و شرکت‌های کشور کره‌جنوبی که هنوز موفق به همراهی با تحریم‌های ایران نشده‌اند، خبر داد. در این راستا نیز رژیم صهیونیستی با استفاده از یکی از بزرگ‌ترین شرکت‌های تولیدات فناوری اطلاعات در دنیا که سهم قابل توجهی نیز در بازار ایران دارد، اقدام به پخش تیزر تبلیغاتی کرده که در آن به برندگان تبلت سامسونگ هدیه داده می‌شود. این عمل موجب بروز واکنش‌های رسانه‌ای و حتی عکس‌العمل شدید دفتر مرکزی سامسونگ در کره جنوبی شد، به‌نحوی که این شرکت در بیانه خود ضمن عذرخواهی نماینده خود در رژیم صهیونیستی را برکنار کرد. واحد جنگ روانی سازمان‌های اطلاعاتی رژیم صهیونیستی در راستای راهبرد این رژیم برای افزایش تحریم‌ها و فشار بر ایران، طرح‌های ویژه‌ای را تدارک دیده است که از آن جمله می‌توان به جنگ روانی علیه کشورها و شرکت‌هایی که هنوز حاضر به همراهی با پروژه تحریم ایران نشده‌اند، اشاره کرد. بر اساس این طرح، با ساخت تیزرهای ضدایرانی توسط نمایندگی‌های این شرکت‌های بین‌المللی- که بر اساس قوانین می‌توانند بدون اطلاع شرکت اصلی اقدام کنند- اقدام به جنگ روانی علیه این شرکت‌ها می‌کنند. کارشناسان معتقدند پروژه اخیر شرکت سامسونگ هم توسط نمایندگی این شرکت کره‌ای در سرزمین‌های اشغالی و بدون اطلاع شرکت اصلی سامسونگ کلید خورده و هدف نهایی آن خارج کردن این شرکت از ایران و همراه کردن اجباری آن با تحریم‌های غربی است. کارشناسان مسایل اقتصادی اقدام اخیر نمایندگی سامسونگ در سرزمین‌های اشغالی در تهیه تیزر تبلیغاتی ضد ایرانی را طراحی اسراییل برای انتقام از شرکت سامسونگ و کره جنوبی می‌دانند. گفته شده چندی پیش سفارت اسراییل در سئول دیدارهای گسترده‌ای با مسوولان اداره بازرگانی کره جنوبی و شرکت سامسونگ برای خروج این شرکت کره‌ای از ایران داشت که با مخالفت شدید این شرکت کره‌ای مواجه شد. سامسونگ پس از برندهایی مانند نوکیا و سونی اریکسون بیشترین سهم را در بازار ایران داراست؛ این در حالی است که ورود سامسونگ به حوزه تبلت‌ها توانسته گوی سبقت را از برخی برندهای مشابه برباید و این برند توانسته سهم بیش از ۵۰درصدی از بازار ایران را به خود اختصاص دهد.

توطئه صهیونیستی؟

در کلیپ منتشر شده ایران به مثابه بیابانی به تصویر کشیده شده که مملو از گرد و غبار است و مردم آن به دور از هرگونه تمدن و به صورت عصر حجری زندگی می‌کنند؛ چهار مرد با پوشیدن مانتو و در عین حال داشتن سبیل و با راه رفتن نامناسب خود، چهره ناشایست و عقب‌افتاده‌ای از زن ایرانی نشان می‌دهند. در این کلیپ، یک جاسوس موساد در ایران، تبلتی از سامسونگ دارد که با آن تمام فعالیت‌های نیروگاه هسته‌ای را رصد می‌کند. یکی از این چهار نفر، از روی کنجکاوی، دکمه‌ای را روی تبلت لمس می‌کند که به محض لمس دکمه، نیروگاه هسته‌ای ایران که پشت سر آنهاست، منفجر می‌شود! دفتر سامسونگ در ایران نیز ضمن رد هرگونه وابستگی سامسونگ به تولید این کلیپ تبلیغاتی اعلام کرده است تهیه این تبلیغ ارتباطی با شرکت سامسونگ کره ندارد. الهه طاهری مسوول روابط عمومی دفتر سامسونگ در گفت‌وگو با شرق می‌گوید: دفتر سامسونگ کره و دوبی خطاب به دفتر سامسونگ اسراییل، بیانیه‌ای در محکومیت ساخت این تبلیغ صادر کرده است. برخی کارشناسان طراحی این تیزر تبلیغاتی را به سازمان‌های امنیتی اسراییل برای برهم زدن مراودات بازرگانی ایران و کره‌جنوبی نسبت داده‌اند.

بیانیه سامسونگ

«اهداف و سیاست کلی شرکت سامسونگ در تمام دنیا و خصوصا در کشور بزرگ جمهوری اسلامی ایران بر مبنای گسترش و اشاعه صلح و دوستی بین مردم تمامی جهان پایه‌گذاری شده است. متاسفه اخیرا در کلیپی که بدون اطلاع شرکت سامسونگ، توسط یک شرکت اسراییلی با نام شبکه کابلی HOT تولید شده است بی‌محابا و بدون هیچ‌گونه پایه و اساسی به مردم شریف ایران اهانت شده است. اصولا انتساب این کلیپ به شرکت سامسونگ یک سوءتفاهم بوده و شرکت سامسونگ ضمن محکومیت این عمل، همسو با سایر نهادهای مردمی انزجار خود را از این‌گونه اقدامات اعلام می‌کند. بدیهی است شرکت سامسونگ هیچ‌گونه نقشی در تولید این کلیپ نداشته است و شبکه کابلی HOT صرفا در این کلیپ از تبلت سامسونگ به عنوان جایزه برای بینندگان خود استفاده کرده است.»

احتمال ارایه طرحی دوفوریتی تحریم سامسونگ

اقدام رژیم صهیونیستی واکنش نمایندگان مجلس را نیز به همراه داشت به نحوی که رییس کمیسیون اقتصادی مجلس با پشیمان‌کننده خواندن واکنش مجلس به تیزر ضدایرانی سامسونگ، افزود: «عذرخواهی شرکت سامسونگ از ملت ایران گرچه لازم اما کفایت نمی‌کند.» ارسلان فتحی‌پور از تلاش مجلس برای تجدیدنظر در ارتباط با شرکت سامسونگ که اخیرا تیزر ضدایرانی پخش کرده است، خبر داد. به گفته او شرکت سامسونگ در اکثر خانه‌های ایرانی، کالا دارد و شرکت سامسونگ برای خرسندی صهیونیست‌ها اقدام به تولید تیزر تبلیغی ضدایرانی کرده در حالی که فراموش کرده است با ایران بیشترین مراوده اقتصادی را دارد. در این راستا کمیسیون اقتصادی مجلس به زودی در این‌باره بیانیه‌ای صادر خواهد کرد. او همچنین از احتمال مطرح شدن طرح دوفوریتی در مجلس خبر داد و درگفت‌وگو با فارس بیان کرد این طرح تمامی خریدها از شرکت سامسونگ را ممنوع خواهد کرد. همچنین علی موسوی نماینده آبادان در مجلس شورای اسلامی در این‌باره بیان کرد این شرکت در مستندی تبلیغی برای خشنود کردن صهیونیست‌ها به ملت ایران اهانت کرده است و این اهانت برای این شرکت گران تمام خواهد شد. قرار است بحث تیزر تبلیغاتی و ضدایرانی شرکت سامسونگ در دستور جلسه یکشنبه هفته آینده کمیسیون اقتصادی مجلس قرار گیرد و در این جلسه درباره نحوه برخورد با این شرکت تصمیم‌گیری خواهد شد.

همگامی اندونزی برای اجرای «اینترنت پاک» با ایران

شرق: بنا بر اظهارات وزیر ارتباطات و فناوری اطلاعات پیاده‌سازی اینترنت پاک از ایران شروع می‌شود اما موفقیت آن در گرو این است که دیگران هم به این طرح بپیوندند تا این ایده بتواند یک جریان کامل منطقه‌ای و بین‌المللی را شکل دهد. رضا تقی‌پور به تشریح ابعاد مختلف ایده اینترنت پاک و برنامه‌های ایران در همراه کردن مجامع بین‌المللی برای اجرای این طرح پرداخته و بیان کرد برای اجرای اینترنت پاک مجامع بین‌المللی را با خود همراه می‌کنیم. او پیش از این از کنار گذاشتن کسب و کار کثیف در اینترنت و پاک کردن آن سخن گفته و ادامه داد بود هدف اینترنت پاک ارایه شبکه‌ای عاری از این آسیب‌ها برای مردم دنیاست. او حتی از همگام شدن کشور اندونزی در پیاده‌سازی شبکه اینترنت پاک خبر داده و می‌گوید: اندونزی بعد از ایران اولین کشوری خواهد بود که «اینترنت پاک» را عملیاتی می‌کند. او در گفت‌وگو با مهر نیز گفته است بنا داریم که در نشست‌های آتی این موضوع را در دستور کار قرار دهیم و اقدامات عملیاتی آن را هم انجام داده‌ایم؛ در عین حال از نظر تبدیل این ایده به برنامه‌های اجرایی فعالیت‌های زیادی صورت گرفته و جلسات کارشناسی و اتاق فکرها تا به حال تشکیل شده و کار از نظر تئوری در مرحله خوبی پیش رفته که امید می‌رود بتوان بخش‌های زیادی از آن را هم در عمل در ایران و اندونزی پیاده کرد. پروژه اینترنت پاک یا همان شبکه ملی اطلاعات قرار است در ۲۲ بهمن امسال اجرایی شود و فاز نخست آن در خرداد سال آینده به اتمام برسد.

اینترنت پاک برای مجامعی که به ارزش‌ها بها می‌دهند

وزیر ارتباطات و فناوری اطلاعات بر این عقیده است که ایده اینترنت پاک در مجامعی که به ارزش‌ها بها می‌دهند و می‌خواهند ارزش‌های ملی خود را در مقابل آنچه که کسب و کارهای کثیف هدف گرفته‌اند، حفظ کنند، مورد استقبال قرار گرفته و به طور قطع در این رابطه، روزی اجماع جهانی صورت خواهد گرفت. رضا تقی‌پور در گفت‌وگو با مهر بیان می‌کند تعیین زمان عملیاتی کردن اینترنت پاک بستگی دارد به اینکه چقدر بتوانیم مجامع بین‌المللی و منطقه‌ای را در این ایده با خودمان همراه کنیم بنابراین الان یک زمان مشخصی را برای این موضوع پیش‌بینی نمی‌کنیم و این بستگی دارد که این نشست‌ها چه زمانی به نتیجه برسد. به باور تقی‌پور شبکه جهانی اینترنت با وضعیت کنونی دارای حجم وسیعی از اطلاعات است که قابلیت پاسخگویی به هر نوع نیازی را دارد؛ هرچند روی آن اطلاعات زاید و نامناسب بسیاری نیز وجود دارد که از آنها به عنوان ناپاکی یاد می‌شود اما شبکه ملی اطلاعات برای مبارزه با این ناپاکی‌ها آستین‌ها را بالا زده و درصدد است تا اینترنت پاک را نه تنها به ارمغان آورد بلکه به جهانیان عرضه کند. حال این ناپاکی‌ها با چه صافی پاک می‌شوند و چند درصد از اطلاعات اینترنت کنونی مفید واقع خواهد شد، هنوز مشخص نیست

امنیت

پرسش‌هایی از یک محقق امنیتی

شاید برای شما هم پیش آمده که هرگاه با یک محقق امنیت شبکه روبه‌رو شدید، پرسش‌های ذهن خود را از او پرسیده و پاسخ‌های مناسب را دریافت کرده باشید. از این رو قرار است بخشی از این پرسش‌ها که شاید در ذهن همه ما شکل گرفته باشد، بیاید؛ اینها پرسش‌هایی است که از میتجاکلوسک، مدیرکل شرکت امنیتی ACROS و یک محقق سرشناس آسیب‌های امنیتی پرسیده شده و او نیز آنها را پاسخ داده است.

■■■

چه نوع تجهیزاتی را به افرادی که به طور جدی می‌خواهند وارد حوزه آسیب‌شناسی امنیتی بشوند، توصیه و پیشنهاد می‌کنید؟

برای آسیب‌شناسی نرم‌افزاری، نیازی به داشتن ابزار گران‌قیمت و غیرمعمول نیست. با یک کامپیوتر رومیزی کارآمد و چند ابزار و نرم‌افزار رایگان می‌توانید یک کار تحقیقاتی را شروع کنید. من بر استفاده از VMware تاکید بسیاری دارم. به دلیل اینکه می‌توان بین سیستم عامل‌های مختلف برای تست به سرعت تغییر موقعیت داد. آسیب‌شناسی سخت‌افزاری درست برخلاف نرم‌افزار، به ابزار گران‌قیمت و دستگاه‌های خطرناک نیاز دارد. اصولا این دستگاه‌ها در دسترس همه نیست و برای تحقیقات غیرضروری و از روی سرگرمی مورد استفاده قرار نمی‌گیرد. البته باید اشاره کنم، تجهیزات هک کردن سخت‌افزاری در حال حاضر قیمت‌های چندان گرانی ندارند. به طور مثال، تجهیزاتی را که برای تحقیقات GSM مورد نیاز است، می‌توان با چند هزار دلار خریداری کرد. در صورتی‌که همین وسایل درست تا دو سال پیش بسیار گران و غیرقابل خریداری بودند.

روزهای زندگی یک محقق آسیب‌های امنیتی به چه شکلی می‌گذرند؟

روزهای زندگی ما بسیار معمولی و ساده است و چیزی برای گفتن ندارد. شما تمام روز را پشت کامپیوتر می‌نشینید، درباره راه‌های مختلف حمله به یک محصول و هک کردن آن فکر می‌کنید، ابزار مورد نیاز برای نفوذ را یادداشت می‌کنید، برگه‌های راهنمای محصول را که در دست‌تان است، مطالعه می‌کنید، هنگامی که راهی برای نفوذ بی‌عیب و نقص پیدا نمی‌کنید سر خود را می‌خارانید و در آخر، وقتی موفق به یافتن آنچه می‌خواستید شدید، یک لبخند پیروزمندانه می‌زنید. این می‌تواند یک روز کاری یک آسیب‌شناس امنیتی را تشکیل بدهد. البته تعداد روزهای آن به میزان مقاومت محصول در برابر حمله‌ها نیز بستگی دارد. اگر چندین روز متوالی این کار ادامه داشته باشد، شاید بعد از پیروزی برای تخلیه حس خوشحالی داد بزنید یا حتی برقصید.

نظر شما در مورد کدهای بسته و کدهای باز یک محصول چیست؟

در شرایط ایده‌آل که گروهی از محققان امنیتی باید هر دو کدهای بسته و کدهای باز یک محصول را مورد بازبینی قرار بدهند، فرض قوی ما بر این است که تعداد کمی از آسیب‌ها و باگ‌ها در محصولات کد باز غیرقابل کشف شدن باقی می‌مانند. اما ممکن است در محصولاتی که کدهای بسته دارند، این رقم بالاتر باشد. اما در شرایط واقعی چنین اتفاقی نمی‌افتد. تجربه ثابت کرده است که باز یا بسته بودن کدهای منبع یک محصول ارتباط چندانی به قابلیت هک شدن و نفوذ به آن ندارد و چیزی که در این میان حرف اول را می‌زند، برنامه‌نویس‌های آن محصول هستند. هرچقدر برنامه‌نویس قوی‌تر و حرفه‌ای‌تر باشد، کدها امن‌تر نوشته می‌شوند و نفوذ به آنها دشوارتر می‌شود.

نظر شما در مورد مبلغ پیشنهادی شرکت‌های کامپیوتری به محققان امنیتی چیست؟

به عنوان یک محقق امنیتی حرفه‌ای، ما همیشه دستمزد خود را از مشتری‌هایمان برای یافتن اشکالات و باگ‌های آنها دریافت کرده‌ایم. همچنین، برنامه‌های اهدای جوایز به محققان امنیتی که بیشتر شرکت‌ها اجرا می‌کنند نیز روش تجاری دیگری برای این کار محسوب می‌شود. در مورد کارهای کوچک و کم‌هزینه، اصولا این شرکت‌های کامپیوتری و مشتری‌ها هستند که سود می‌برند زیرا محققانی که روی پروژه‌های کوچک تحقیق می‌کنند، اصولا دستمزدی دریافت نمی‌کنند. تنها دریافتی آنها جایزه‌ای برای موفقیت‌شان است. بنابراین، محققان نیز راهی پیدا می‌کنند تا دستمزد یا مبلغ جایزه را افزایش بدهند. به این ترتیب که سوراخ‌ها و باگ‌های امنیتی بزرگ را پیدا نکنند تا شرکت‌ها مجبور بشوند مبلغ پرداختی را افزایش بدهند. اگر تمایلی به افزایش مبلغ نداشتند نیز باید شاهد ترک کردن پروژه توسط محقق باشند. در بیشتر مواقع، شرکت‌های بونتی این کار را می‌کنند و بسیار مایه خوشحالی است که شرکت‌ها و مشتری‌ها، خودشان را با این مساله وفق داده‌اند.

گذرگاه

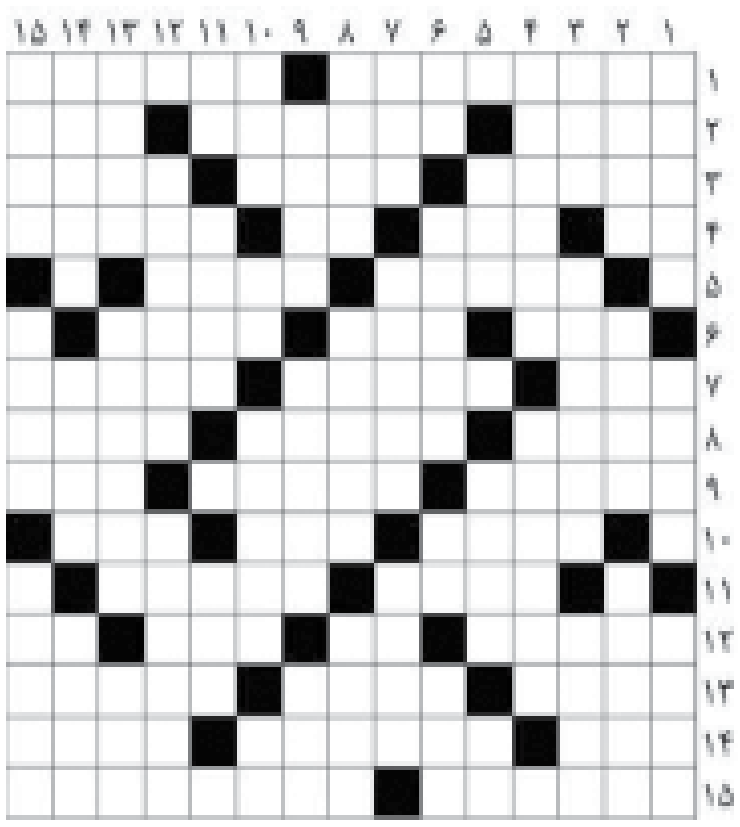
کاربرد اینترنت و فاصله جنسیتی

■ **شرق:** داده‌های به‌دست‌آمده از سنجش کاربران اینترنت نشان می‌دهد هنوز هم در کشورهای در حال‌توسعه و هم در کشورهای توسعه‌یافته درصد مردانی که از اینترنت استفاده می‌کنند، از زنان بیشتر است. در میان تمام کشورهایی که داده‌هایشان موجود است، تنها در نیوزیلند و تایلند نسبت تعداد زنان کاربر اینترنت از مردان بیشتر است و البته این تفاوت اندک است. به نظر نمی‌رسد که تفاوت در کاربری اینترنت میان زنان و مردان با سطح توسعه پیوند داشته باشد، تا جایی که در این زمینه نیز تفاوت‌های زیادی وجود دارد؛ شاید یکی از دلایل این وضعیت این باشد که در بسیاری از کشورها زنان کمتر از مردان درآمد دارند و از امکانات برابر برای تحصیلات برخوردار نیستند. در واقع بعضی از تحقیقات ثابت می‌کنند حتی وقتی که توانایی‌ها و تجربه کار زنان با مردان برابر است، باز هم اغلب کمتر از مردان درآمد دارند. سطوح پایین‌تر درآمد باعث می‌شود دسترسی به اینترنت از نظر مالی برای زنان دشوارتر باشد. به علاوه، سطح تحصیلات پایین‌تر در میان زنان نیز به تفاوت میزان درآمد میان زنان و مردان می‌انجامد. نمونه‌ای از آفریقا نشان می‌دهد مانع عمده بر سر دسترسی اغلب افراد به اینترنت فقدان آگاهی درباره وجود اینترنت است و در آفریقا تعداد زنانی که از وجود اینترنت مطلع‌اند کمتر از مردان است. برای مثال، داده‌های سال ۲۰۰۷ درباره بوتسوانا و سنگال نشان می‌دهد مردان در مورد اینترنت اطلاعات بسیار بیشتری داشتند و این موضوع با بالاتر بودن میزان نفوذ کاربری اینترنت رابطه داشت. در کامرون که میزان آگاهی زنان درباره اینترنت به اندازه مردان و حتی بیشتر از آنان بود، تفاوت کاربرد اینترنت در میان این دو گروه اندک بود؛ در حالی که فقدان آگاهی به واقع می‌تواند مانعی مهم در کاربرد اینترنت باشد، عوامل دیگر شامل درآمد کمتر و سطح تحصیلات نیز احتمالا نقش مهمی ایفا می‌کنند. به نظر نمی‌رسد این واقعیت که زنان کمتر از مردان به کاربرد اینترنت تمایل دارند ربطی به فناوری‌های ارتباطات و اطلاعات داشته باشد. تجارب عملی نشان داده است که در شرایط برابر تحصیلی یا شغلی، تفاوت کمی میان زنان و مردان از نظر کاربرد فناوری‌ها وجود دارد. بنابراین، تفاوت زنان و مردان در زمینه‌هایی چون درآمد و تحصیلات است که تفاوت سطح دسترسی به فناوری‌های اطلاعات و ارتباطات و کاربرد آنها را توضیح می‌دهد. با دقیق‌تر شدن و گران‌تر شدن فناوری‌ها و خدمات که دسترسی و کاربرد آنها را منوط به سطح درآمد و تحصیلات بیشتر می‌کند، تفاوت میان این دو گروه بیشتر می‌شود.

جدول ۱۴۳۳

افقی:
۱- نویسنده «زن ستوان فرانسوی»- شش‌دهم مقدار خون ۲- درختکاری شده- قسمتی از یک سریال داستان یا فیلم- بیم و وحشت ۳- چیز داغ- انتظار و چشمداشت- کفش چوبی ۴- مخفف گاه- خشن- چه وقت؟- ماست آبکی ۵- کفش روستایی- اخبار فرنگی ۶- ماه بیگانه- معشوقه رامین- تابناک ۷- سبزی خوردنی- بازگردانیدن- بندری در بو شهر ۸- از ادعیه معروف مفتاح‌الجنان- نویسنده کمدی الهی- پیشکش ۹- ورم کرده- ریاضیدان فرانسوی قرن هفده- سنگ سبز قیمتی ۱۰- بادها- بیماری مسری- لوله تنفسی ۱۱- چشم سیاه- بیماری زردی ۱۲- نیازمندی- نتی در موسیقی- میوه تابستانی- نت ششم موسیقی ۱۳- زعفران- زیاده‌گو- وزیر فرعون ۱۴- مار بزرگ- کوهی در خراسان- جمع رند ۱۵- مشارکت- کمک‌رسانی

عمودی:
۱- همه و سراسر- دوال چرمی- دشمن موش ۲- شبیه‌تر- تعمیر- ادامه‌دهنده ۳- ناپاک- از شهرهای بندری فرانسه- جزیره ۴- روشن و درخشنده- کرم گوشت خوک ۵- زرنگ- آبزی مفید- صد متر مربع ۶- حرف تعجب- شکستنی ورزشی- گشودن معما- اما ۷- اشتباه معروف- به وجود آوردن- سوره هفدهم قرآن ۸- محل نمایش حیوانات- دستیار دن کیشوت- خودرو روسی ۹- کره خاکی- نوعی پارچه درشت- ساغر ۱۰- پسر- دریا- پایتخت کشور زیمبابوه- خودرأی ۱۱- دشمن سرسخت- پاندول ساعت- بالای کوه ۱۲- کلرو فیل- بی‌تجربه ۱۳- الک- واحد اندازه‌گیری زاویه- گیج و سرگشته ۱۴- نابود شده- مقر حکومت مارشال پتن- موزه پاریس ۱۵- رساتر- با هم- موجد استقلال هند



حل جدول ۱۴۳۲

سودوکو

سودوکو Sudoku یک واژه ترکیبی ژاپنی به معنای عددهای بی‌تکرار است و امروزه به جدولی از اعداد گفته می‌شود که به عنوان یک سرگرمی رایج در نشریات کشورهای مختلف به چاپ می‌رسد.

قانون‌های حل جدول سودوکو:

۱- در هر سطر و ستون باید اعداد یک تا ۹ نوشته شود. بدیهی است که هیچ عددی نباید تکرار شود.

۲- در هر مربع ۳×۳ اعداد یک تا ۹ باید نوشته شود و در نتیجه هیچ عددی نباید تکرار شود.

سودوکو ۴۳۶

۶		۲	۴	۸			۳	۱
	۳	۸			۶	۷	۴	۹
۴		۹		۳		۲		
		۳	۶		۵			۴
۷	۶		۸		۱			
			۳					۷
۳	۲	۱			۸	۶		
۵	۴		۹					۸
۹			۵			۴		۲

حل سودوکو ۴۳۵

۱	۸	۹	۳	۲	۷	۴	۶	۵
۶	۵	۲	۹	۸	۴	۷	۱	۳
۷	۴	۳	۱	۵	۶	۸	۲	۹
۸	۹	۱	۲	۶	۳	۵	۴	۷
۵	۳	۴	۷	۹	۱	۶	۸	۲
۲	۷	۶	۸	۴	۵	۳	۹	۱
۹	۱	۵	۶	۳	۸	۲	۷	۴
۳	۲	۸	۴	۷	۹	۱	۵	۶
۴	۶	۷	۵	۱	۲	۹	۳	۸

سودوکو سخت ۸۴

۹							۳	۶
			۲	۹		۴		
		۸				۵	۲	
	۴	۹	۵					۷
		۵	۷	۳	۶			
۳		۷	۹		۸			
		۱	۶				۷	۴
۶				۵			۱	
			۴		۱			

حل سودوکو سخت

۲	۶	۹	۱	۸	۴	۵	۷	۳
۵	۱	۳	۶	۲	۷	۸	۴	۹
۴	۸	۷	۵	۳	۹	۱	۶	۲
۵	۴	۲	۷	۱	۶	۳	۹	۸
۶	۹	۱	۳	۸	۲	۷	۵	۴
۳	۷	۸	۹	۴	۵	۶	۲	۱
۸	۲	۴	۷	۶	۱	۹	۳	۵
۹	۳	۶	۴	۵	۸	۲	۱	۷
۷	۵	۱	۲	۹	۳	۴	۸	۶