شرکت مخابرات ایران

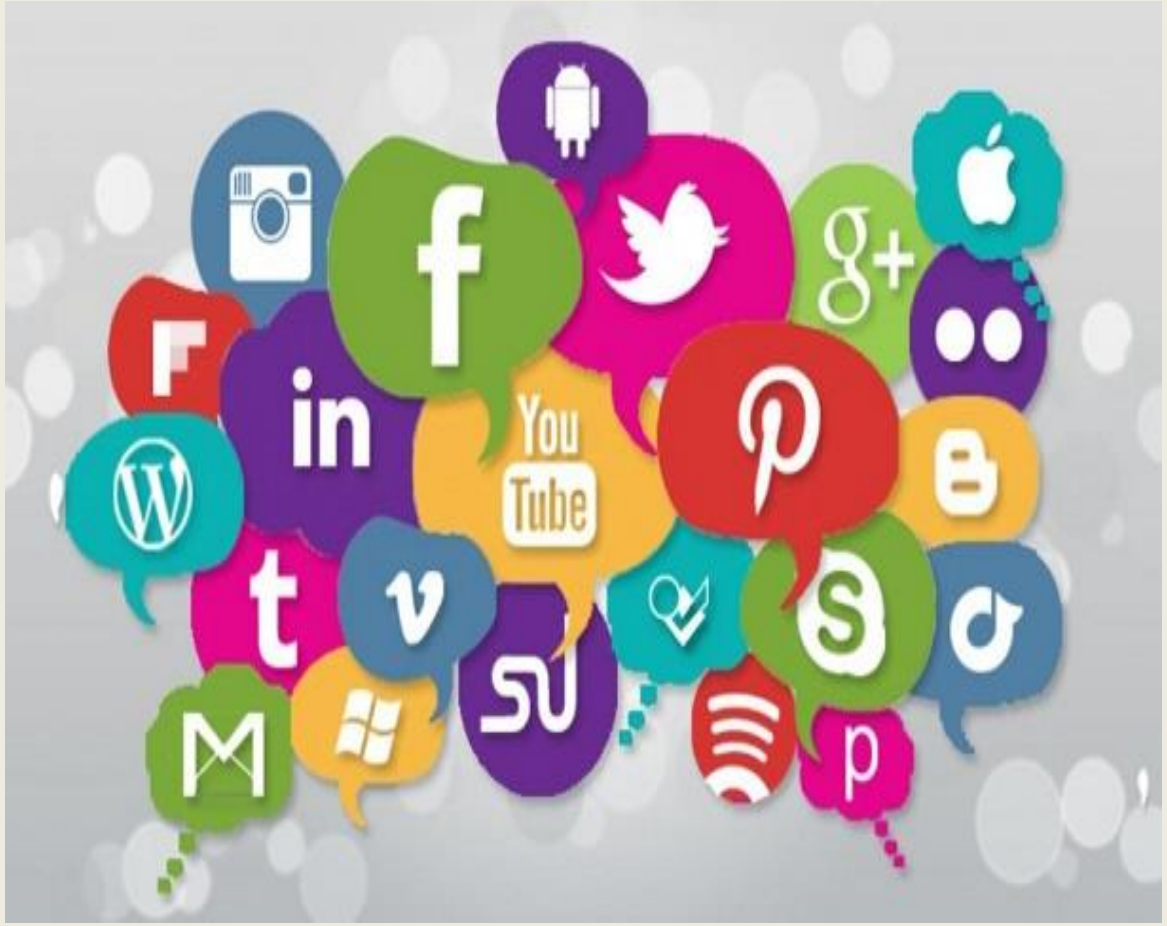
همیشه آشنا

آشنای اول

هشدارهای امنیتی استفاده از اینترنت

شبکه های اجتماعی

www.tci.ir



- به مجموعه ای از افراد که به صورت گروهی با یکدیگر ارتباط داشته و مواردی مانند: اطلاعات، نیازمندی ها، فعالیت ها و افکار خود را به اشتراک بگذارند، شبکه های اجتماعی گویند.

- شبکه های اجتماعی را می توان به دو دسته شبکه های مجازی و شبکه های غیر مجازی تقسیم کرد. شبکه های غیرمجازی که بحث این نوشتار است، در واقع شبکه هایی هستند که توسط مجموعه ای از افراد و گروه های به هم پیوسته، در محیط اجتماعی عمل می کنند. شبکه اجتماعی مجازی یا شبکه اجتماعی اینترنتی، وب سایت یا مجموعه ای از وب سایت هایی است که به کاربران امکان می دهد، علاقه مندی ها، افکار و فعالیت های خود را با یکدیگر به اشتراک بگذارند؛ به عبارت دیگر، شبکه های اجتماعی پایگاه هایی هستند که با استفاده از یک موتور جستجوگر و افزودن امکاناتی مانند: چت، پیام رسانی الکترونیک، انتقال تصویر و صدا و...، امکان ارتباط بیشتر کاربران را در قالب شبکه ای از روابط فردی و گروهی فراهم می آورند. وبلاگ ها، فیس بوک، توییتر، یتویب و پادکست از جمله شبکه ها ی اجتماعی مجازی هستند.

۵ سؤال امنیتی که باید پیش از کلیک‌کردن روی یک لینک از خود بپرسید

www.tci.ir

- **آیا به کسی که پیوند را برای شما ارسال کرده اعتماد دارید؟**

اگر فرستنده، یا آدرس رایانامه و یا محتوای رایانامه را نمی‌شناسید بهترین گزینه این است که آن را باز نکنید. به خصوص باید در مواردی که در عنوان رایانامه نام شما ذکر شده یا مدعی شده است که از طرف بانک شما است جوانب احتیاط را رعایت کنید.

- **آیا به بستر نرم‌افزاری مورد علاقه‌تان اعتماد دارید؟**

اگر پیوندی از طریق شبکه‌ی داخلی کاری‌تان و یا گروه خصوصی واتس‌اپ به اشتراک گذاشته شده است جای نگرانی وجود ندارد، اما اگر پیوندی در هرزنامه باشد یا از سوی حساب کاربری ناشناسی در توئیتر فرستاده شده باشد، باید قبل از کلیک کردن روی آن بیشتر فکر کنید. درمورد توئیتر و فیس‌بوک بیشتر مراقب باشید. در هردوی آن‌ها هرزنامه‌هایی گزارش شده است که حاوی پیوندهایی بوده‌اند که مستقیماً شما را به وب‌گاه‌های مخرب هدایت می‌کنند.

- **آیا به مقصدی که پیوند شما را هدایت خواهد کرد اعتماد دارید؟**

اگر به مقصد آن اعتماد ندارید یا آن را نمی‌شناسید نباید روی آن کلیک کنید .به‌جای آن، خودتان به طورمستقیم آدرس مقصد اینترنتی مدنظرتان را جست‌وجو کنید.

- **آیا این پیوند متقارن با زمان وقوع رویدادی جهانی است؟**

مجرمان اینترنتی بسیار فرصت طلب‌اند. اگر پیوندی دیدید، مثلاً درباره‌ی زلزله‌ی نپال، درباره‌ی آن خوب فکر کنید تا بتوانید به سؤال‌های قبل پاسخ دهید، این که چه کسی آن را به اشتراک گذاشته است، منبع آن کجاست و به چه مقصدی شما را هدایت خواهد کرد.

- **آیا پیوند دریافتی، یک پیوند کوتاه شده است؟**

گسترش شبکه‌های اجتماعی هم‌چون فیس‌بوک، توئیتر و اینستاگرام نیاز را به پیوندهای کوتاه‌شده افزایش داده‌اند. برای پیوندهای کوتاه شده، ابتدا پاسخ سؤال‌های قبلی را برای خود بیابید .هم‌چنین می‌توانید از ابزارهایی مانند LongURL و یا CheckShortURL برای بازگرداندن پیوند کوتاه‌شده به حالت معمولی استفاده کنید.

راهنمایی های ضروری برای امنیت پست الکترونیکی

www.tci.ir

سرویس گیرنده امنیتی(Client Security)

به تازگی ابزارهای ضد–هرزنامه، فیلترینگ فیشینگ ها و سایر ویژگی هایی که برای به دام انداختن و جداسازی پیام های پر مخاطره قبل از اینکه اثرات مخربی بر روی سیستم بگذارند، طراحی شده اند. کاربران بایستی در مورد این ویژگی ها بررسی های لازم را صورت دهند و از آنها بعنوان اولین سد دفاعی استفاده کنند.

دیواره ی آتشین : (Firewall)

دیواره آتشین می تواند امنیت پست الکترونیکی را از طریق فیلتر کردن فایل ضمیمه حاوی تروجان و نیز دیگر پست الکترونیکی های ناخواسته که تنظیمات از پیش تعیین شده آن ها را برآورده نمی کند، تقویت کند.

ابزارهای آنتی ویروس

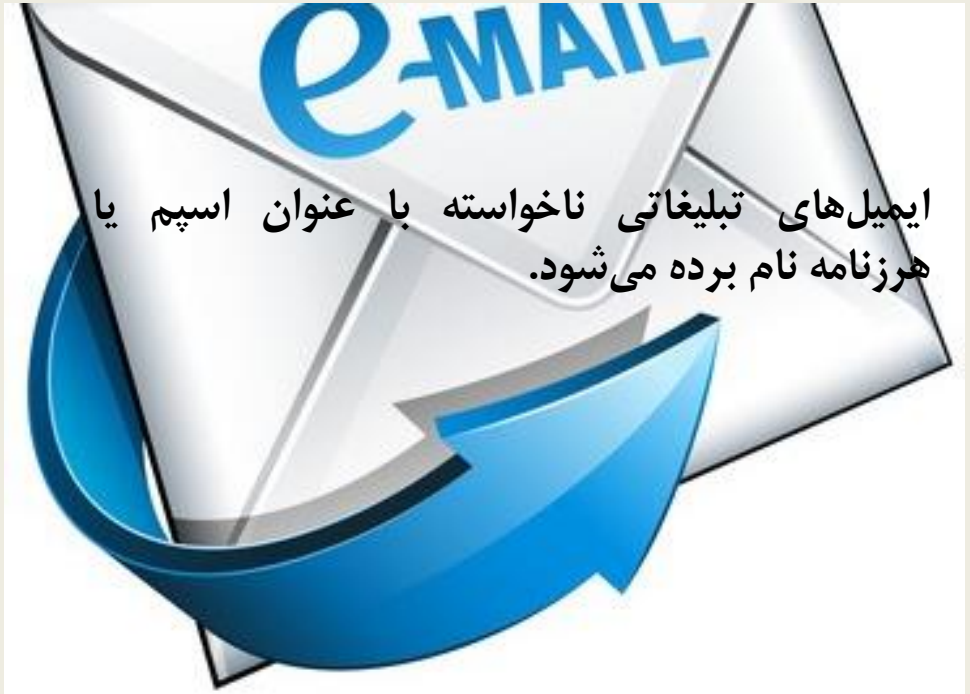
محصولات و خدمات آنتی ویروس ها عمدتا کارشان را برای شناسایی و حذف ویروس ها، تروجان ها و کرم ها به خوبی انجام می دهند.

فیلتر هرزنامه

یک فیلتر هرزنامه ی خوب می تواند به خوبی تفاوت پست الکترونیکی های عادی را از هرزنامه ها تشخیص دهد، و صندوق پستی شما را از مقدار بسیار زیادی از هرزنامه ها پاک کند.

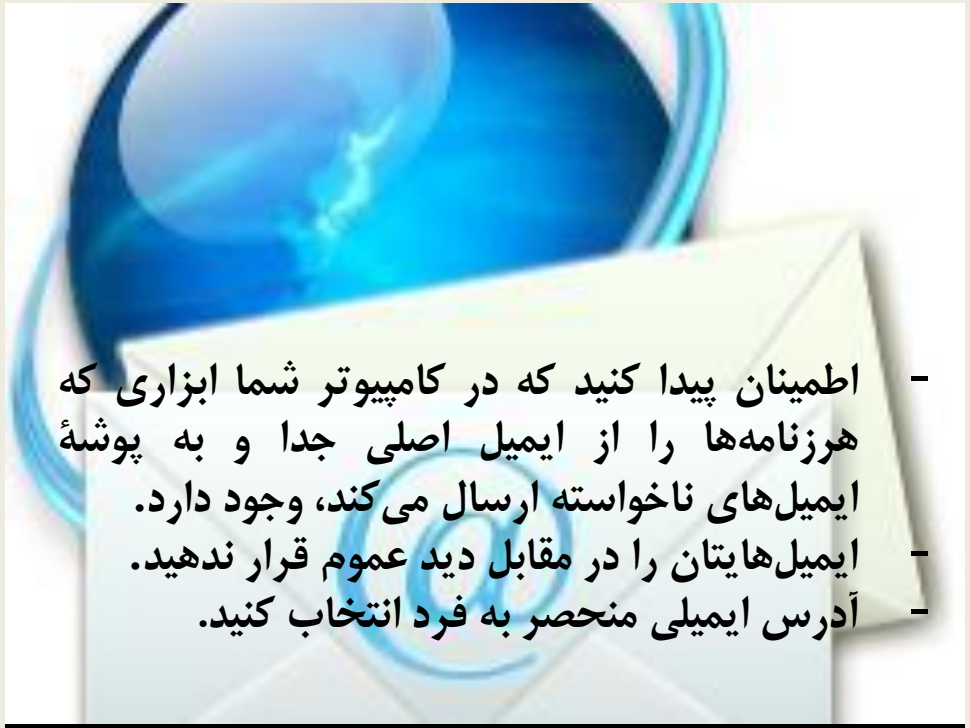
هرزنامه

www.tci.ir



ایمیل‌های تبلیغاتی ناخواسته با عنوان اسپم یا هرزنامه نام برده می‌شود.

هرزنامه(اسپم) چیست؟



- اطمینان پیدا کنید که در کامپیوتر شما ابزاری که هرزنامه‌ها را از ایمیل اصلی جدا و به پوشهٔ ایمیل‌های ناخواسته ارسال می‌کند، وجود دارد.
- ایمیل‌هایتان را در مقابل دید عموم قرار ندهید.
- آدرس ایمیلی منحصر به فرد انتخاب کنید.

چگونه می‌توانیم تعداد ایمیل‌هایی را که به صورت اسپم دریافت می‌کنیم، کاهش دهیم؟

حفظ امنیت کودکان در اینترنت

www.tci.ir

- کودکانتان را تشویق کنید که تجارب اینترنتی خود را با شما سهیم شوند. همراه با کودکانتان از اینترنت لذت ببرید.

- اگر فرزندانتان به اتاق های گفتگو سر می زنند، از برنامه های پیام رسان فوری و بازی های ویدویی آنلاین استفاده می کنند، یا فعالیت های دیگری که به نامی برای مشخص کردن خودشان نیاز است، انجام می دهند، به آنها در انتخاب این نام کمک کنید و مطمئن شوید که این نام باعث افشاء هیچ اطلاعات شخصی در موردشان نمی شود.

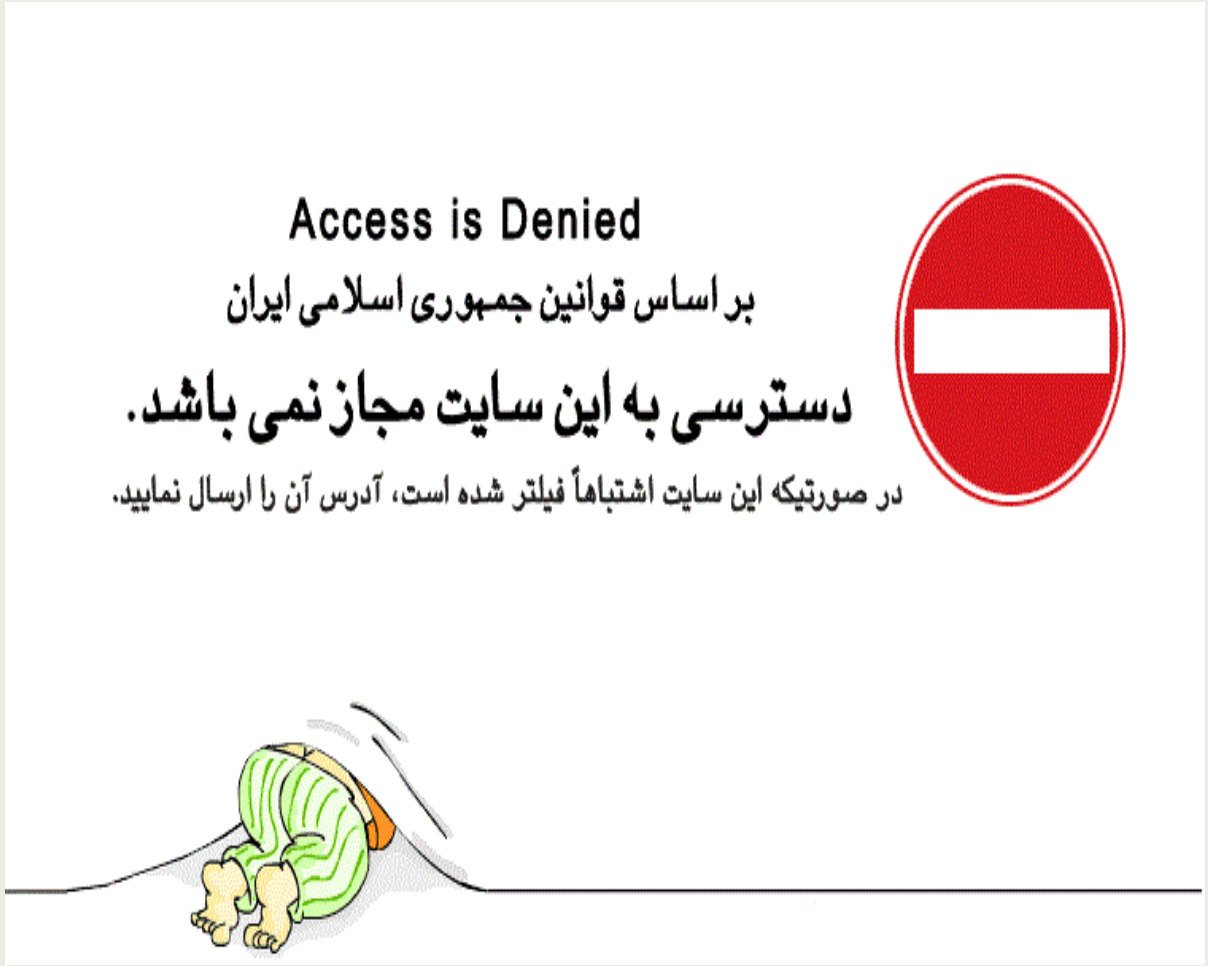
- به فرزندانتان تأکید کنید که هرگز آدرستان، شماره تلفن یا سایر اطلاعات شخصی شامل جایی که به مدرسه می روند یا جایی که دوست دارند بازی کنند را ارسال نکنند.

- به کودکان بیاموزید که چگونه به دیگر استفاده کنندگان از اینترنت، احترام بگذارند. مطمئن شوید که آنها می دانند قواعد رفتار خوب فقط به دلیل اینکه پشت کامپیوتر هستند، تغییر نمی کند.

- چندین ایده در مورد چیزهایی که باید با کودکانتان بحث کنید تا به آنها در مورد استفاده ایمن تر از اینترنت بیاموزید.

نرم‌افزارهای فیلترینگ خانگی برای مراقبت از فرزندانتان در فضای‌مجازی

www.tci.ir



کید لاگر

با استفاده از این نرم افزار می‌توان فهمید کاربر (فرزند و یا پرسنل تحت نظر) چقدر با کامپیوتر کار می‌کنند.

آی نت

نرم افزار دیگر «I net» می‌باشد که امکانات کنترل فرزندان از راه دور را داراست. با استفاده از این نرم افزار می‌توان از تمامی فعالیت‌های فرزندان در هنگام استفاده از رایانه و اینترنت مطلع شد و حتی میزان دسترسی را برای فرزندان مشخص کرد و این دسترسی‌ها را محدود نمود.

چایلد کنترل

توسط این نرم افزار می‌توانید محدودیت‌های مورد نظر خود را ایجاد کنید. فقط در ساعت‌های خاصی اجازه کار با کامپیوتر را بدهید. بعضی از سایت‌ها را فیلتر کنید. و یا فقط اجاره دسترسی به چند سایت خاص را بدهید.

مراقب این ۵ نقطه خطرناک در اینترنت باشید

کاربران اینترنت معمولاً برای یافتن عکس‌ها، ویدئوهای خنده دار، مقالات علمی و... خود در گوگل جستجو می‌کنند اما ممکن است در خلال همین جستجوها به یکباره سیستم آن‌ها با مشکلات جدی روبرو شود

وب سایت‌های حاوی فایل‌های فلش

شامل وب سایت‌هایی است که کاملاً امن بوده و امکان وجود هیچ گونه خطر امنیتی در آن‌ها وجود ندارد

توییتر

اگر کاربری به دنبال ریسک‌های امنیتی باشد، شاید بتواند نوع خفیفی از آن را پیدا کند اما به هیچ عنوان آسیب جدی به حساب نمی‌آید

ایمیل شما

وب سایت‌های خطرناکی را در بر می‌گیرد که به خودی خود آلوده نیستند اما لینک‌های رد و بدل شده در آنها می‌تواند آلوده باشد و یک کلیک کاربر می‌تواند او را با مشکلات جدی روبرو کند

وب سایت‌های دریافت موزیک، ویدئو و نرم افزار

وب سایت‌های خطرناک را در بر می‌گیرد. در این وب سایت‌ها آلودگی به کاربر بسیار نزدیک بوده و بهتر است کاربر اصلاً به آن‌ها مراجعه نکند

وب سایت‌های نامشروع

سایت‌های بسیار خطرناک و آلوده را شامل می‌شود که کاربر به محض بازدید از آن‌ها قطعاً آلوده خواهد شد

امنیت در فضای مجازی

www.tci.ir

برخی نکات مهم در رابطه با تامین امنیت در فضای شبکه‌های اجتماعی

۱. مراقب جعل هویت باشید.
۲. اسرار ملّی و سازمانی را افشاء نکنید.
۳. مراقب کرم‌های رایانه‌ای و تروجان‌ها باشید.
۴. افق‌نامه‌ی محرمانگی اطّلاعات را مطالعه کنید.
۵. به هر ناشناسی اعتماد نکنید.
۶. تنظیمات حریم خصوصی را انجام دهید.
۷. جهت کسب اطلاعات بیشتر در این خصوص می توانید به وب سایت پلیس فتا به آدرس www.cyberpolice.ir مراجعه نمائید.