



فصل ۷ ارتباط امن

هدف‌های رفتاری

پس از آموزش این فصل، هنرجو می‌تواند:

- ۱- خطرات و مشکلات پیام‌های ناشناس را شناسایی کند.
- ۲- هویت مجازی را توضیح دهد.
- ۳- جرائم مختلف در فضای اینترنت را بیان کند.
- ۴- با ویروس‌های اینترنتی مقابله نماید.
- ۵- انواع برنامه‌های مخرب را بشناسد.
- ۶- با برنامه‌های ضد ویروس کار کند.
- ۷- ملزومات امنیتی در اینترنت را بشناسد.
- ۸- به شکل امن در تجارت الکترونیک شرکت نماید.
- ۹- حقوق مصرف‌کنندگان در اینترنت را توضیح دهد.
- ۱۰- دلایل کنترل والدین را توضیح دهد.



۱-۷- مقدمه

اینترنت، یک شبکه عظیم اطلاع‌رسانی و یک بانک وسیع اطلاعاتی است که در آینده نزدیک دسترسی به آن برای تک‌تک افراد ممکن خواهد شد. کارشناسان ارتباطات، بهره‌گیری از این شبکه را یک ضرورت در عصر اطلاعات می‌دانند. این شبکه که از هزاران شبکه کوچک‌تر تشکیل شده، فارغ از مرزهای جغرافیایی، سراسر جهان را به هم مرتبط ساخته است. این اطلاعات با سرعت تمام در بزرگراه‌های اطلاعاتی بین کاربران رد و بدل می‌شود و تقریباً هیچ‌گونه محدودیت و کنترلی بر وارد کردن یا دریافت کردن داده‌ها اعمال نمی‌شود. حمایت از جریان آزاد اطلاعات، گسترش روزافزون فناوری اطلاعات و بسترسازی برای اتصال به شبکه‌های اطلاع‌رسانی، شعار دولت‌هاست. این درحالی است که گستردگی و تنوع اطلاعات آلوده روی اینترنت، موجب بروز نگرانی در بین کشورهای مختلف شده است. هشدار، جریمه و بازداشت برای برپاکنندگان پایگاه‌های مخرب و فسادانگیز تدابیری است که کشورهای مختلف جهان برای مقابله با آثار سوء اینترنت اتخاذ کرده‌اند. ترس و بیم از تخریب مبانی اخلاقی و اجتماعی، ناشی از هجوم اطلاعات آلوده و مخرب از طریق اینترنت، واکنشی منطقی است، زیرا هر جامعه‌ای چارچوب‌های اطلاعاتی خاص خود را دارد و طبیعی است که هر نوع اطلاعاتی که این حد و مرزها را بشکند می‌تواند سلامت و امنیت جامعه را به خطر اندازد. علی‌رغم وجود جنبه مثبت شبکه‌های جهانی، سوء استفاده از این شبکه‌های رایانه‌ای توسط افراد بزهکار، امنیت ملی را در کشورهای مختلف با خطر روبه‌رو ساخته است. از این‌رو به کارگیری فیلترها و فایروال‌های مختلف برای پیشگیری از نفوذ داده‌های مخرب و مضر و گزینش اطلاعات سالم در این شبکه‌ها رو به افزایش است. خوشبختانه با وجود هیاهوی بسیاری که شبکه اینترنت را غیرقابل کنترل معرفی می‌کند، فناوری لازم برای کنترل این شبکه و انتخاب اطلاعات سالم روبه گسترش و تکامل می‌باشد.

خطرات و مشکلات پیغام‌های ناشناس

پیام‌های الکترونیکی ناشناس چه خطرات و مشکلاتی برای من دربردارد؟

در حالی که بسیاری فناوری اطلاعات و ارتباطات را باعث تسهیل در امر انتقال اطلاعات می دانند، اما موضوع امنیت در تبادل اطلاعات همواره به عنوان یکی از اصول غافل مانده به شکل یک معضل پنهان باقی می ماند. امنیت اطلاعات برای بخش مهمی از فعالان بخش فناوری اطلاعات تنها زمانی به عنوان یک موضوع حاد مطرح می شود که مشکلی در سیستم به وجود آید. در اغلب مواقع این مشکلات باعث ضربه‌ای سنگین بر سیستم و یا به اطلاعات موجود در آن می شود که در واقع می توان گفت رویکرد دیر هنگامی است. امروزه امنیت اطلاعات در زمینه اینترنت از یک بحث حاشیه‌ای به یک بحث ضروری تغییر جهت داده است. هرگونه خرید و فروش روی اینترنت و یا انتقال داده‌ها باید تحت یک کنترل امنیتی صورت گیرد. اگر امنیت شبکه برقرار نگردد، مزیت‌های فراوان آن نیز به خوبی حاصل نخواهد شد و پول و تجارت الکترونیک، خدمات به کاربران خاص، اطلاعات شخصی، اطلاعات عمومی و نشریات الکترونیک همه و همه در معرض دستکاری و سوءاستفاده‌های مادی و معنوی قرار می گیرند. در ایران که بسیاری از نرم افزارهای پایه از قبیل سیستم عامل و نرم افزارهای کاربردی و اینترنتی، از طریق واسطه‌ها و شرکت‌های خارجی تهیه می شود، بیم نفوذ از طریق راه‌های مخفی وجود دارد. هم اکنون نیز بانک‌ها و بسیاری از نهادها و دستگاه‌های دیگر از طریق شبکه به فعالیت می پردازند، به همین دلیل جلوگیری از نفوذ عوامل مخرب در شبکه به صورت مسئله‌ای استراتژیک درآمده که نپرداختن به آن باعث ایراد خساراتی خواهد شد.

هویت مجازی

به رغم معرفی سرویس‌های متعدد روی شبکه، تاکنون مهم‌ترین سرویس از میان سرویس‌های گوناگون اینترنت، سیستم پست الکترونیکی بوده است. بسیاری از کاربران اینترنت از این بخش بیشتر از سایر امکانات فراهم آمده توسط این شبکه جهانی استفاده می کنند. امروزه، اقتصاد جهانی به پست الکترونیکی متکی شده است، بسیاری از پیام‌های رد و بدل شده بین کاربران حاوی یادداشت‌های شخصی است. گرچه اغلب پیام‌ها از متن ساده تشکیل شده‌اند، اما امکان پست الکترونیکی تمام انواع داده‌ها، مثل تصاویر، برنامه‌های کامپیوتری، سندهای صفحه گسترده و... نیز وجود دارد. با توجه به این سرویس، اینترنت اجازه می دهد که افرادی که دور از هم هستند با یکدیگر در تعامل و کار باشند. پست

الکترونیکی امروزه در تجارت و بانکداری الکترونیکی هم کاربرد فراوانی دارد و بسیاری از تعیین هویت‌های مجازی امروزه توسط پست الکترونیک صورت می‌گیرد. در همین رابطه برای استفاده امن از پست الکترونیکی تذکراتی وجود دارد. درک تفاوت‌های پست الکترونیکی با پست عادی و یا گفت‌وگوی تلفنی کمی دشوار است، ولی به کار بستن برخی نکات ساده می‌تواند در بالا بردن امنیت هنگام به کارگیری این سرویس مؤثر باشد از جمله این موارد می‌توان موارد زیر را نام برد:

بایستی همواره تصور شود که هیچ‌گونه اختفایی وجود ندارد. پیام‌هایی که به دلایلی نباید همه ببینند نباید از این طریق ارسال شود، بنابراین از ارسال نامه‌های بسیار خصوصی، سخنرانی‌های تند، بی‌احترامی‌های منظوردار و... باید احتراز شود. نباید فرض شود که پیام‌های حذف شده قابل بازیابی نیستند. چنانچه پیامی حذف شود، احتمالاً در نسخه‌های پشتیبان که شب یا روز قبل تهیه شده است موجود است. در این سیستم ابزار مشابه کاغذ خردکن وجود ندارد. در متن‌های ارسالی باید محتاط بود. این طبیعت پست الکترونیکی است که مردم پیام‌های دریافتی خود را بیشتر از پیام‌های ارسالی جدی می‌گیرند. ضمن اینکه ارسال یادداشت سریع به هرجایی از جهان بسیار ساده است.

نگاهی به کشور ایران

بسیاری از اوقات هنگامی که برای چک کردن ایمیل خود به اینترنت وصل می‌شوید، تعداد زیادی ایمیل تبلیغاتی از فرستندگان ناشناس با اسامی غیر واقعی و عجیب و غریب را ملاحظه می‌نمایید که عناوین موضوعات آن نیز تعجب‌آور است.

عناوینی مانند:

- کنجکاو کنید!
- سلام من منتظرم!
- شما برنده شده‌اید!
- این ایمیل را ببین!
- آیا می‌خواهید یک شبه پولدار شوید؟!
- ۲ میلیون تومان درآمد در ماه!
- در مورد فیلتر بیشتر بدانید.
- عضو برترین گروه دنیا شوید!
- کجایی؟
- یک خبر جدید!

● چرا فیلتر؟

● با هر کلیک ۱۰۰ تومان دریافت کنید.

دسته دیگر، موضوعات تبلیغاتی کم اهمیت:

● پر فروش ترین فیلم سال

● فروش ویژه اقساطی!

● ارزان سرای ما!

● فرصت رو از دست نده

● بشتابید!

و هر روز سیل این ایمیل‌های مزاحم، کم اهمیت و فریبنده، کاربران را کلافه کرده و اکثراً از سوی فارسی زبانان داخل کشور ارسال می‌شود. در برخی موارد صاحب ایمیل مجبور است این ایمیل‌ها را در spam و inbox یکجا حذف نماید که ممکن است در بین آنها یک ایمیل مهم از دوست یا شرکتی را نیز، ناخوانده، قربانی مزاحمت دیگران نماید!

اگر این نوع ایمیل‌ها به عنوان مثال توسط یک دانش آموز باز شده و موجب ایجاد سؤال و تعجب برای او گردد، ممکن است وی برای یافتن پاسخ سؤال خود، که امری ضروری نیست، به دوستان، وبلاگ‌ها و سایت‌ها و غیره مراجعه نماید تا اطلاعاتی در مورد آن کسب نماید و موجب بروز مشکلاتی جدی برای نسل نوجوان و جوان بشود. در نتیجه، ارسال این گونه پیام‌ها امری ناپسند می‌باشد. اما لینک‌های فریبنده در برخی وبلاگ‌هایی که از سوی فارسی زبانان داخل کشور معمولاً با مقاصد مادی ساخته می‌شود، مشکلات و خطراتی را مخصوصاً برای خانواده‌هایی که دارای فرزندان دوره‌های ابتدایی تا دبیرستان می‌باشند، به وجود آورده است. در این رابطه هشدار معلمان و اولیای آموزشی نیز به گوش می‌رسد که مراقب استفاده کودکان و نوجوانان خود از اینترنت باشید.

اما کاربران آگاه اینترنت می‌دانند که معمولاً سایت‌هایی معتبر هستند که دارای Domain رسمی با درج شماره‌های تماس مدیر و توضیحاتی در مورد مؤسسان سایت، صفحات درباره ما، تماس با ما و غیره هستند. اما سایت‌های معتبر از این نوع تبلیغات فریبکارانه (تکدی گری اینترنتی!) بی‌نیاز هستند و معمولاً با صداقت در موتورهای جست و جو جایی برای خود باز کرده و بازدید کننده به صورت آگاهانه به سایتشان وارد می‌شود.

در برخی وبلاگ‌ها و سایت‌های فروش، اگر دیواره آتش و ویروس یاب شما فعال نباشد، با ورود به آنها، بدون اجازه شما، آدرس صفحه خانگی مرورگر وب شما به آدرس مورد نظر آنها تغییر می‌یابد تا بلکه بار دیگر وارد آن آدرس شده و شاید خرید داشته باشید و معمولاً این نوع کارها در سایت‌های معتبر و مفید، رخ نمی‌دهد و این اعمال بدون اجازه شما، توسط وبلاگ‌های وابسته بدون نام و نشان سازنده، به سایت اصلی انجام می‌شود.

از دیگر اعمال ناپسند در اینترنت و در سایت و وبلاگ‌های فارسی، که گاهاً موتورهای جست‌وجو و بازدیدکنندگان را فریب می‌دهند، استفاده از تصاویر غیر مرتبط با شرح آن است. به عنوان مثال با درج عبارت: ورزش‌های مفید نوجوانان، تصویری نامناسب و غیر مرتبط با آن را به بیننده معرفی می‌کنند!

آسیب دیگر اینترنت در کشور، کپی‌برداری وبلاگ‌ها و برخی سایت‌ها و اشخاص و عدم درج منبع بوده و جالب اینکه مطلب جالب یک نویسنده در صدها سایت و وبلاگ دیگر به نام فرد دیگر درج شده و هر کسی بدون واهمه مجدداً از آن کپی‌برداری کرده و به نام خود در وبلاگ یا سایتش استفاده کرده و امانت‌داری را رعایت نمی‌کنند.

در مواجهه با موارد بالا یا نظایر آن پیشنهاد می‌گردد:

۱- از ثبت ایمیل خود در وبلاگ و سایت‌های غیر ضروری، جهت عضویت و غیره خودداری نمایید تا از ایمیل‌های مزاحم تا حدودی در امان باشید.

۲- اگر مجبورید ایمیل خود را در یک صفحه اینترنتی ثبت نمایید، پیشنهاد می‌گردد در صورت امکان آن را به صورت یک عکس کم حجم در معرض دید دیگران قرار دهید.

۳- به هیچ وجه روی لینک‌ها و ایمیل‌ها با عناوین فریبنده و غیر واقعی و ناشناس کلیک نکنید.

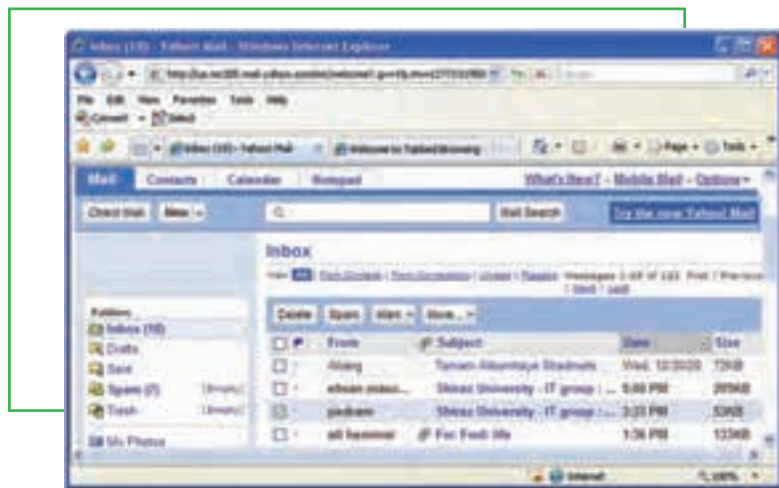
۴- هرگز به یک ایمیل ناخواسته و مشکوک پاسخ ندهید، زیرا اینکار باعث خواهد شد که در آینده پیام‌های ناخواسته بیشتری برای شما ارسال شود.

۵- در خیلی از موارد لازم است والدین و بزرگترها برگشت و گذار کودکان و نوجوانان در اینترنت نظارت داشته باشند، توصیه می‌شود علی‌الخصوص کودکان را در استفاده بی‌قید و بند از اینترنت، آزاد نگذارید.

۶- اگر لازم است فرزندان شما مطالبی را جهت مطالعه از اینترنت دریافت نمایند، با همکاری یکدیگر و در زمان محدود این کار را انجام دهید.

۷- و مهم‌تر از همه: «روی هر لینکی کلیک نکنید».

۸- با تعیین یک آدرس یا ایمیل دریافتی به عنوان هرزنانه، می‌توانید سرویس دهنده پست الکترونیکی خود را برای موارد بعدی آگاه نمایید. (شکل ۱-۷)



شکل ۱-۷ تعیین آدرس یا یک ایمیل دریافتی

به عنوان هرزنانه

برخی جرائم در فضای اینترنت

در گفت وگوهای روزمره، مواردی از این قبیل شنیده می شود:

- برای فردی ایمیلی از یک کشور غربی رسیده که وی را به تحصیل در خارج دعوت کرده اند! (درحالی که آن یک Spam بوده و برای هزاران نفر ارسال شده است)
- فردی چون ساعت های زیادی در اینترنت کار می کند، به تازگی برنده ۱۰۰۰۰ دلار شده اما شرایط دریافت آن کمی مشکل است.

اما کاربران آگاه اینترنتی می دانند چنین مواردی عاری از واقعیت است. به مثال دیگری توجه نمایید:

یک شهروند دیگر از یک بانک نامه ای دریافت کرده بود به این مضمون که «بیمه عمر یک فرد ثروتمند در دست ما است و از آنجایی که او مرده و ورثه ای هم ندارد شما می توانید با ما همکاری کنید تا در استفاده از این پول با ما شریک شوید». وقتی این شهروند با این بانک تماس گرفت، از او خواسته شد که ۲۵ دلار را همراه با اطلاعاتش برای بانک بفرستد تا برای ایجاد پرونده مورد استفاده قرار گیرد.

مثال دیگر: برای شهروند دیگری نیز ایمیلی ارسال شد که از او می خواست که با پرداخت مبلغی در یک کار خیر شریک شود و بعداً در افزایش مبالغی را دریافت کند.

بعضی از افراد کلاهبردار به همین وسیله شماره تلفن افراد را می گیرند و سپس با گرفتن شماره تلفن آنها برای رسیدن به هدفشان بارها با آنها تماس می گیرند و با سماجت و با دروغ های زیاد می کوشند توجه ایشان را به خود جلب کنند.

بنابراین مشخص است که فناوری جدید، جرائم جدید به همراه می آورد. رایانه و اینترنت یک فناوری جدید است. مانند هر فناوری دیگری تا زمانی که استفاده از رایانه و اینترنت عمومیت پیدا نکرده بود، هیچ پیش فرضی درباره مزایا و مخاطرات احتمالی آن وجود نداشت. اما اکنون به تدریج زوایای بسیاری از آن آشکار می شود. در کشورهای پیشرفته که این فناوری گسترش زیادی پیدا کرده است، مردم بیشتر با مزایا و جرائمی که این فناوری با خود آورده آشنا شده اند و به تدریج قوانینی مناسب در حال ایجاد شدن است و این قوانین هر روز نیز در حال تکمیل شدن هستند. اما در کشور ما زوایای مختلف این فناوری و تبعات مثبت و جرائم مربوط به آن به تدریج آشکار می شود.

شهروندان باید درباره کلاهبرداری های مختلف که از طریق اینترنت و پست الکترونیک صورت می پذیرد، آگاه باشند. در پیام هایی که به قصد کلاهبرداری فرستاده می شوند، به مخاطبان خبر برنده شدن در یک قرعه کشی داده می شود و یا از افراد برای شرکت در قرعه کشی و یا شرکت در جابه جایی پولی که منجر به کسب درآمد خواهد شد، دعوت می شود. در این پیام ها به کاربران اعلام می شود که مبالغ بسیار زیادی برنده شده اند و کاربران با درخواست هایی مبنی بر اعلام مشخصات مواجه می شوند. در قدم های بعدی، کاربر با این تصور که ثبت اطلاعات مشکلی را متوجه وی

نخواهد کرد، اقدام به ارسال اطلاعات می‌کند و فرستندگان پیام نیز به محض دریافت پاسخ مثبت از سوی کاربر با ارسال مدارکی جعلی در پی القای این موضوع برمی‌آیند که گیرنده پیام در یکی از بانک‌های معتبر بین‌المللی برنده شده است. در مرحله بعدی از کاربران درخواست افتتاح حساب و واریز مبالغی به آن حساب‌ها به عنوان هزینه جابه‌جایی مبالغ برنده شده می‌شود و از سوی ارسال‌کنندگان پیام اعلام می‌گردد که هزینه جابه‌جایی پول برعهده فرد برنده شده بوده و شرکت در این مورد هزینه‌ای را متقبل نمی‌شود.

البته جرائم اینترنتی تنها محدود به کلاهبرداری نمی‌شوند. انتشار اخبار کذب، افترا، آزار و اذیت، سوء استفاده از پست الکترونیک، ارسال مطالب و تصاویر و فیلم‌های مستهجن، هتک حرمت افراد با پخش مطلب یا تصاویر آنها، تلاش برای به انحراف کشاندن و سوء استفاده از کودکان، نقض حق مالکیت مادی و معنوی افراد، هک کردن و ویروسی کردن سایت‌ها از جمله جرائم دیگر اینترنتی محسوب می‌شوند. ظاهراً هنوز آمار دقیقی در زمینه میزان جرائم اینترنتی در کشور وجود ندارد. اما گفته می‌شود که خلاف‌کاران علاقه زیادی به پیدا کردن اطلاعات شخصی افراد به ویژه برای خالی کردن حساب بانکی آنها و نفوذ به سیستم بانکی دارند.

اینترنت مزایای زیادی دارد و یکی از فناوری‌هایی است که جهان امروز بدون آن قابل تصور نیست. از جمله مزایای اینترنت، گسترش تجارت و در دسترس همگان بودن اطلاعات است. بنابراین برخلاف نظر برخی که فکر می‌کنند برای کنترل برخی از عواقب سوء اینترنت باید از گسترش آن جلوگیری کرد، اما لازم است که به هر وسیله ممکن در صدد گسترش آن به همه نقاط کشور و در بین همه افراد اعم از شهری و روستایی باشیم. بعد هم مانند هر فناوری دیگری لازم است درباره جرائم اینترنتی اطلاع‌رسانی کنیم و به‌ویژه در این زمینه قوانین محکمی تدوین کنیم. طبیعی است که کلاهبرداری اینترنتی با کلاهبرداری سنتی متفاوت است و قوانین مناسب خود را می‌خواهد و یا جرائمی مثل هک کردن وجود دارد که اصولاً مربوط به رایانه و اینترنت است. در بسیاری از کشورهای پیشرفته هم تصحیح یا تغییر قوانین در این زمینه و سایر جرائم اینترنتی فرایندی مداوم است.

قوانینی که در حوزه اینترنت و جرائم اینترنتی تدوین می‌شود، لازم است حفظ احترام افراد و اعاده حیثیت آنها و مجازات مجرمین را دنبال کند. طبیعی است که هر قدر فناوری توسعه می‌یابد هم امکان به وجود آمدن جرائم بیشتر می‌شود و هم امکان کنترل همان جرائم به وجود می‌آید. مانند تلفن که عده‌ای برای مزاحمت و تهدید دیگران نیز از آن استفاده می‌کردند، ولی بعداً هم امکان ردیابی مزاحمان به وجود آمد و حتی اکنون با وجود نمایش شماره تلفن تماس گیرنده، هر کسی شخصاً نیز قادر به پیدا کردن مزاحم است.

مقابله با ویروس‌ها

چگونه می‌توانم رایانه‌ام را در مقابل ویروس‌های اینترنتی ایمن نمایم؟

ویروس‌های رایانه‌ای برنامه‌هایی هستند که مشابه ویروس‌های بیولوژیک گسترش یافته و پس از وارد شدن به رایانه اقدامات غیرمنتظره‌ای را انجام می‌دهند. با وجودی که همه ویروس‌ها خطرناک نیستند، ولی جزئی از برنامه‌های مخرب هستند که در بیشتر موارد برای تخریب یا تغییر انواع مشخصی از پرونده‌ها، برنامه‌های کاربردی، سیستم‌های عامل یا سوء استفاده از آنها نوشته می‌شوند. ویروس‌ها هم مشابه همه برنامه‌های دیگر از منابع سیستم مانند حافظه و فضای دیسک سخت، توان پردازنده و سایر منابع بهره می‌گیرند و می‌توانند اعمال خطرناکی را انجام دهند. در این بخش انواع برنامه‌های مخرب شامل ویروس، کرم، تروجان و کدهای مخرب مورد بررسی قرار خواهد گرفت.

عملکرد ویروس‌ها

تخریب: ویروس‌ها در ابتدا با همین هدف نوشته و توزیع می‌شد که به کل یا قسمتی از اطلاعات آسیب جزیی یا جدی برساند و در مواردی نادر کل اطلاعات را از بین ببرد. فرض کنید یک فرد ناراضی ویروسی را در شبکه پلیس شهر پخش می‌کند تا کلیه پرونده‌ها را نابود سازد. هدف وی از این کار تخریب اطلاعات و احتمالاً از بین بردن اطلاعات مربوط به خود در نزد پلیس است.

جاسوسی: پس از ویروس‌های مخرب، ویروس‌هایی شیوع پیدا کرد که به شبکه‌ها و اطلاعات ارزشمند و یا غیر ارزشمند دسترسی پیدا می‌کردند. فرض کنید فردی به شبکه بانک‌های شهر ویروس ارسال می‌کند و می‌خواهد اطلاعات حساب‌های بانکی را دریافت کرده و دستکاری یا از آنها سوء استفاده کند.

کسب درآمد: می‌توان مواردی را مشخص کرد که فردی ویروسی را آماده می‌کند، پس از توزیع در شبکه‌ها، به شرکت‌هایی که نرم افزار ضدویروس را می‌نویسند، می‌فروشد و یا اینکه شرکت‌ها رأساً نسبت به این کار اقدام می‌کنند. البته در برخی موارد، ویروس نویس به صورت مستقیم با قربانی معامله می‌کند.

نکته

در اغلب کشورهای دنیا نگارش، پخش و هرگونه دخالت در پدید آوردن یا استفاده از ویروس‌ها برای اعمال مجرمانه، جرم محسوب می‌شود و مورد پیگرد قانونی قرار می‌گیرد.

انواع برنامه‌های مخرب

ویروس: ویروس یک قطعه نرم‌افزار کوچک بوده که بر دوش یک برنامه حقیقی حمل می‌گردد. مثلاً یک ویروس می‌تواند خود را به برنامه‌ای نظیر واژه‌پرداز متصل نماید. هر مرتبه که برنامه واژه‌پرداز اجرا شود، ویروس نیز اجرا می‌شود و این فرصت (شانس) را پیدا خواهد کرد که ضمن این که نسخه‌ای از خود را مجدداً تولید (الحاق یک نسخه از خود به سایر برنامه‌ها) کند، فعالیت اصلی خود که ممکن است تغییر اطلاعات، تخریب آن یا جاسوسی را نیز انجام دهد.

کرم: یک کرم، برنامه نرم‌افزاری کوچکی است که با استفاده از شبکه‌های رایانه‌ای و اشکالات برنامه‌ای (حفره‌های امنیتی موجود)، اقدام به تکثیر خود می‌کند و با تکثیر بیش از حد خود، عملاً سیستم‌ها را از کار می‌اندازد. نسخه‌ای از «کرم»، شبکه را پیمایش تا ماشین‌های دیگر موجود در شبکه را که دارای حفره‌های امنیتی هستند، تشخیص و نسخه‌ای از خود را تکثیر کند. کرم‌ها با استفاده از حفره‌های امنیتی موجود، نسخه‌ای از خود را بر روی ماشین‌های جدید تکثیر می‌کنند. با استفاده از شبکه‌های رایانه‌ای، کرم‌ها قادر به تکثیر باورنکردنی خود در اسرع زمان می‌باشند. مثلاً کرم «Code Red»، که در سال ۲۰۰۱ مطرح گردید، قادر به تکثیر خود به میزان ۲۵۰۰۰۰ مرتبه در مدت زمان ۹ ساعت بود. کرم‌ها می‌توانند منابع رایانه‌ای و شبکه‌ای مانند زمان پردازنده، حافظه یا تمام یا قسمتی از امکانات شبکه را در اختیار خود بگیرند.

تروجان: تروجان یا اسب تراوا، نوع خاصی از برنامه‌های مخرب هستند. برنامه‌های فوق در برخی موارد با ادعای کمک به کاربر در زمینه رفع مشکلات رایانه یا تحت عنوان بازی یا برنامه رایگان، کاربر را فریب داده و پس از اینکه توسط کاربر به رایانه او منتقل شد، برخلاف ادعای قبلی، باعث بروز آسیب‌های جدی مانند حذف اطلاعات موجود دیسک سخت می‌کنند. اسب‌های تراوا دارای روشی برای تکثیر خود نمی‌باشند.

کدهای جاسوس: برنامه‌هایی که بعد از قرار گرفتن در رایانه شما شروع به گردآوری اطلاعات کرده و اطلاعات شما را برای مقاصد مختلف از جمله تجاری و سیاسی جمع‌آوری کرده و برای مرکز کنترل خود ارسال می‌کنند.

نحوه گسترش ویروس

روش‌های زیر از مهم‌ترین روش‌های انتقال و گسترش ویروس‌ها است:

- اجرای پرونده‌های ناشناس توسط کاربر روی رایانه.
- انتقال از طریق CD، فلاپی و یا کارت‌های حافظه از یک سیستم آلوده به سیستم دیگر.
- انتقال از طریق شبکه و اینترنت.

علائم وجود ویروس در یک رایانه

چنانچه رایانه ویروسی باشد ممکن است یک یا چند مورد از علائم زیر بروز کند:

- سرعت رایانه به شدت افت می‌کند.
- با پرونده‌هایی مواجه می‌شوید که شما آن را ایجاد نکرده و با آن آشنا نیستید.
- درخواست اتصال به اینترنت از طرف برنامه‌های خاص.
- کند شدن سرعت دریافت و ارسال‌های اینترنتی.
- افزایش حجم اطلاعات.
- ناپدید و گم‌شدن اطلاعات.
- تخریب پرونده‌ها و اطلاعات.
- کار نکردن برخی از قطعات سخت افزاری.

نحوه مقابله با ویروس‌ها

یکی از مهم‌ترین روش‌های مقابله با برنامه‌های مخرب پیشگیری از انتقال آن به رایانه است لذا باید روش‌های انتقال آنها را فرا گرفت و اقدامات پیشگیرانه لازم را انجام داد.

- استفاده از یک دیواره آتش^۱: دیواره آتش، یک برنامه امنیتی است که از نفوذ انواع نرم افزارهای مخرب جلوگیری می‌کند.
- از نرم افزارهایی که توسط منابع غیر مطمئن توزیع و ارائه می‌گردند، اجتناب و نرم افزارهای مربوطه را از منابع مطمئن تهیه و نصب کنید.
- امکان راه‌اندازی شدن از طریق دیسکت را با استفاده از برنامه BIOS، غیر فعال کرده تا بدین طریق امکان آلوده شدن ویروس از طریق یک دیسکت که به صورت تصادفی در درایو مربوطه قرار گرفته شده است، اجتناب شود.
- امکان «حفاظت ماکرو در مقابل ویروس» را در تمام برنامه‌های مایکروسافت فعال کرده و هرگز امکان اجرای ماکروهای موجود در یک سند را تا حصول اطمینان از عملکرد واقعی آنها ندهید.
- هرگز قبل از بررسی نشدن پیوست‌های یک نامه الکترونیکی ارسال شده که می‌توانند شامل کدهای اجرایی باشند، آنها را باز نکنید. در رابطه با پرونده‌های word و Excel، پیوست‌هایی که دارای پسوند DOC (پرونده‌های word)، پسوند XLS (صفحه گسترده)، به مسئله ماکرو و ویروس‌های مربوطه دقت گردد.
- با کمال تعجب، احتمال گرفتن ویروس از افرادی که می‌شناسید معمولاً خیلی بیشتر از غریبه‌هاست. بسیاری از کارشناسان امنیتی عقیده دارند که حتی اگر با اطلاع قبلی نیز پیامی دریافت می‌کنید که فایلی به آن ضمیمه شده است،

باز هم باید مراقب باشید، زیرا ممکن است فرستنده به طور ناخواسته فایل آلوده‌ای را ارسال کرده باشد. برخی از ویروس‌ها نیز می‌توانند از طریق اتصال به آدرس دفترچه آدرس شما را تکثیر کنند.

● معمولاً پیام‌های متنی ساده نمی‌توانند ویروسی باشند اما به عنوان مثال، پیام‌هایی که قالب آنها HTML است، می‌توانند حامل یک ویروس بسیار خطرناک باشند.

● پرونده‌های با پسوند COM، EXE و یا VBS اجرایی بوده و در صورت آلوده بودن به ویروس، با اجرای آنان بر روی سیستم خود زمینه فعال شدن آنها فراهم خواهد شد. بنابراین لازم است از اجرای هرگونه پرونده اجرایی که به همراه پست الکترونیکی برای شما ارسال می‌گردد (خصوصاً مواردی که آدرس فرستنده برای شما گمنام و ناشناخته است)، صرف نظر کنید.

● Service Pack های ویندوز را دانلود کنید و همیشه ویندوز خود را به روز نگه دارید.

● استفاده از برنامه‌های ضدویروس (آنتی ویروس)، ضد جاسوسی و برنامه‌های امنیتی شبکه: این کار از جمله اقدامات لازم برای کاهش اثرات سوء برنامه‌های مخرب است. برای این کار باید برنامه‌های مذکور در سیستم نصب شوند و در وضعیت فعال یا حفاظت قرار بگیرند.

● استفاده از برنامه‌های ضد Pop Up.

● عدم استفاده از برنامه‌های به اشتراک گذاری پرونده از جمله Kazza.

● عدم استفاده ارتباط شبکه‌ای با پایگاه‌های ناشناخته و نامعتبر.

برنامه‌های ضد ویروس

ضد ویروس (آنتی ویروس) اصطلاحی است که به برنامه یا مجموعه‌ای از برنامه‌ها اطلاق می‌شود که برای محافظت از رایانه‌ها در برابر ویروس‌ها استفاده می‌شوند. وظیفه اصلی این برنامه‌ها شناسایی پرونده‌های آلوده به ویروس و پاکسازی آنهاست. ضد ویروس متن پرونده‌های موجود در رایانه را با نشانه‌های ویروس‌های شناخته شده مقایسه می‌نماید. در بیشتر موارد در صورتی که پرونده آلوده باشد، برنامه ضدویروس قادر به پاکسازی آن و از بین بردن ویروس است. در مواردی که این عمل ممکن نباشد، مکانیزمی برای قرنطینه کردن پرونده آلوده وجود دارد و حتی می‌توان تنظیمات ضدویروس‌ها را به گونه‌ای انجام داد که پرونده آلوده حذف شود. چند نمونه از ضد ویروس‌های رایج در ایران عبارتند از:

● مک آفی (MacAfee)

● نورتون (Norton)

● NOD 32

● AVIRA

● Kaspersky

چند نمونه از نرم افزارهای ضد جاسوسی رایج نیز عبارتند از:

● نرم افزار ضد جاسوسی میکروسافت

● Ad_aware Standard Edition

نکات مهم در انتخاب ضد ویروس

برخی از نکات که لازم است در انتخاب ضد ویروس، مورد توجه قرار گیرند، در این قسمت بیان شده است. توجه به

این نکات سبب می شود تا احتمال آلوده شدن رایانه به ویروس به کمترین حد ممکن برسد.

● ضد ویروس معروف و مطمئن انتخاب کنید.

● ضد ویروس باید قابلیت به روز رسانی را داشته باشد و بتواند بانک اطلاعات خود در مورد ویروس ها و امکانات

لازم برای شناسایی و پاک کردن آنها را از پایگاه شرکت تولید کننده به رایانه منتقل کند. (این گزینه اهمیت زیادی دارد

چون به طور متوسط در هر هفته صدها ویروس جدید تولید شده و در شبکه ها توزیع می شوند.)

● دارای امکانات لازم برای بررسی (اسکن) درایوها به صورت کامل و منظم باشد.

● دارای دیواره آتش قدرتمند باشد.

کاربرد ضد ویروس NOD 32

در این بخش عملکرد ضد ویروس NOD32 تشریح می شود و اسکن درایوها، زمانبندی اجرا و به روز رسانی نرم افزار

به صورت مختصر آموزش داده می شود.

نکته

در صورتی که در رایانه شما برنامه ضد ویروس دیگری نصب شده باشد می توانید همین عملیات را با آن نرم افزار انجام دهید.

به روز رسانی

همانطور که قبلاً بیان شد با توجه به تولید روزانه برنامه های مخرب جدید یکی از کارهایی که باید به صورت مرتب

انجام دهید، به روز رسانی نرم افزار ضد ویروس است تا در صورتی که ویروس های جدید رایانه را مورد حمله قرار

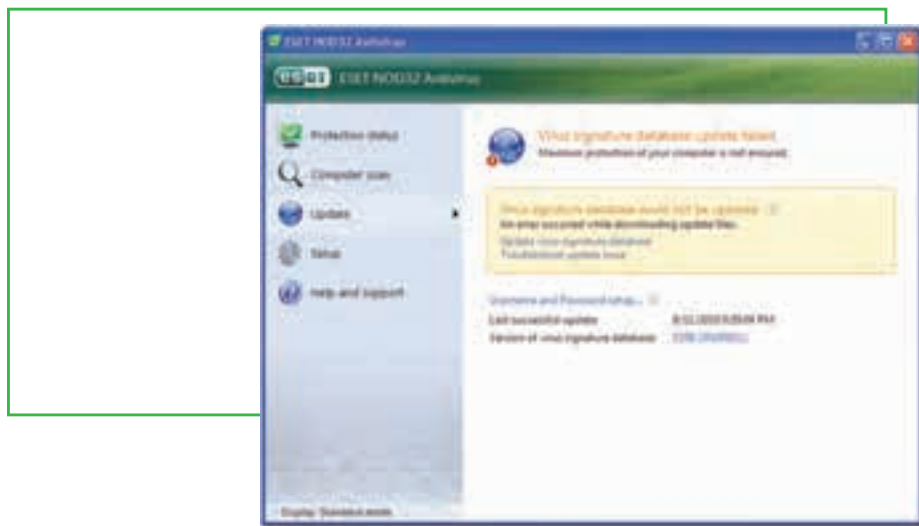
دهد، بتواند نسبت به عملکرد مخرب آنها عکس العمل مناسب نشان دهد. به روز رسانی ضد ویروس به دو صورت

آنلاین (Online) و آفلاین (Off line) قابل انجام است. در حالت آنلاین با برقراری اتصال اینترنتی ضد ویروس با توجه به تنظیم برقرار شده به صورت خودکار شروع به دریافت اطلاعات لازم از پایگاه خود می کند یا می توان به صورت دستی به روز رسانی آنلاین را انجام داد. در روش آفلاین ابتدا باید وارد سایت <http://www.eset.com> شوید در این سایت (شکل ۷-۲) می توانید با توجه به نوع نرم افزار نصب شده پرونده های مورد نظر را دانلود کنید. سپس از آنها برای Update کردن نرم افزار ضد ویروس استفاده نمایید.



شکل ۷-۲ به روز رسانی ضد ویروس NOD32

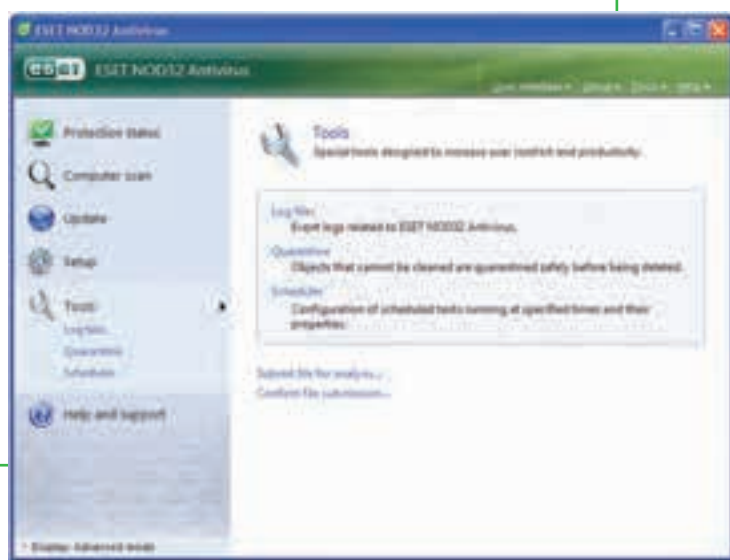
اگر رایانه ای را که نرم افزار ضد ویروس NOD32 روی آن نصب شده است را به شبکه اینترنت با سرعت مناسب متصل نمایید، می توانید مستقیماً به روز رسانی را انجام دهید. برای این کار در پنجره اصلی نرم افزار روی بخش Update (شکل ۷-۳) کلیک کرده و گزینه Update virus signature database را انتخاب نمایید. نرم افزار به صورت خودکار به پایگاه مربوط متصل شده، پرونده های لازم برای به روز رسانی را دریافت و به روز رسانی را انجام می دهد.



شکل ۷-۳ به روز رسانی نرم افزار

زمان بندی اجرا

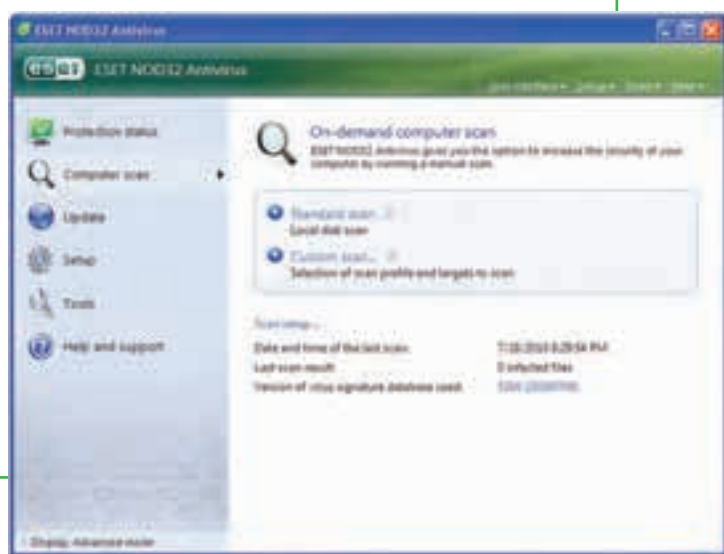
این نرم افزار قابلیت زمان بندی برای کارهای مختلف مانند بررسی ویروس و به روز رسانی را دارد. برای تنظیم این زمان بندی می توانید در بخش Tools گزینه Scheduler را انتخاب و تنظیمات مربوط را انجام دهید (شکل ۷-۴).



شکل ۷-۴ زمان بندی اجرای نرم افزار

تنظیم ویروس یابی

برای تنظیم ویروس یابی در بخش Computer Scan دو گزینه بررسی استاندارد و بررسی سفارشی قابل انتخاب است.



شکل ۷-۵

اطلاعات محرمانه، ریسک‌های امنیتی

ملزومات امنیتی یک صفحه اینترنتی برای ارائه خدمات پولی و تجاری چیست؟

بمباران اخبار، اطلاعیه‌ها و هشدارهای پی در پی در خصوص مشکلات امنیتی موجود در بانکداری و تجارت آنلاین، رسانه‌های گروهی جهان و مخاطبان آنها را بیش از خود تهدیدهای امنیتی با سردرگمی مواجه کرده است! به نظر می‌رسد جنگ بین امنیت و ضد امنیت پایانی نخواهد داشت و کاربران خدمات اینترنتی، تنها قربانیان این نبرد محسوب می‌شوند؛ درست به این دلیل که هم مجرمان اینترنتی تا حد زیادی به اهداف خود می‌رسند و هم شرکت‌های امنیتی، روز به روز بر تجارت و فروش نرم افزارهای امنیتی خود می‌افزایند. شرکت‌های ارائه دهنده خدمات آنلاین نیز آنقدر نقدینگی دارند که حتی ضررهای هنگفت در نظر ما، برای آنها کاملاً قابل اغماض باشد.

البته برخلاف بزرگنمایی‌های رسانه‌ای و تحلیل‌های غیرواقعی بسیاری از کارشناسان، تهدیدهای امنیتی معاملات الکترونیک به هیچ وجه فلج کننده و غیرقابل کنترل نیستند؛ چرا که حتی در بدبینانه‌ترین بررسی‌ها، از ابتدای تولد جرایم مجازی، مجموع درآمد مجرمان اینترنتی از چندین میلیون دلار فراتر نرفته است، که این مبلغ و حتی چند برابر آن نیز، در مقایسه با گردش جهانی پول کاملاً ناچیز است. به هر ترتیب اغراق و بزرگنمایی مشکلات امنیتی موجود، بی‌انصافی است. نباید این گونه فکر کرد که تک تک اعمال، رفتار و فعالیت‌های ما در اینترنت تحت کنترل تبهکاران و ابزار مخرب آنها قرار دارد. علاوه بر این، ابزار و نرم افزارهای امنیتی هم چندان بی کفایت نیستند و قادر به کنترل و انسداد درصد بسیار بالایی از کدهای مخرب و نفوذهای غیرقانونی می‌باشند و درست به همین دلیل تنها درصد محدودی از اقدامات خرابکارانه با هدف سرقت مستقیم یا غیرمستقیم پول به ثمر می‌نشینند و اغلب آنها به نحوی خنثی شده و ماهیت مجرمانه خود را از دست می‌دهند.

آخرین حلقه زنجیر

هیچ دلیلی وجود ندارد که ریسک امنیتی خرید آنلاین از یک فروشگاه معتبر، کمتر از استفاده حضوری از کارت اعتباری و یا وجه نقد در محوطه فیزیکی آن فروشگاه باشد. احتمال اجرای تهدیدهای اینترنتی آنلاین، درست به اندازه این احتمال است که شخصی در محل خرید حضوری شما و بدون این که متوجه شوید، رمز و شماره کارت اعتباری‌تان را یادداشت کند و یا حتی خود آن را برداشته و پا به فرار بگذارد؛ نه بیشتر. تنها تفاوت موجود، محیط انجام معامله و عدم حضور تهدیدهای فیزیکی و قابل مشاهده است.

در مبادلات و معاملات آنلاین احتمال نادیده انگاشتن جوانب امنیتی و عدم رعایت آن، فقط کمی بیشتر از دادوستدهای حضوری است. در حقیقت مجرمان اینترنتی معمولاً به صورت مستقیم به شبکه‌های سازمانی و سرورهای اطلاعاتی حمله نمی‌کنند؛ بلکه تمام تلاش خود را بر روی آسیب‌پذیرترین حلقه زنجیر متمرکز می‌کنند و این حلقه شکننده چیزی و یا بهتر بگوییم کسی نیست به جزء کاربر نهایی. دسترسی به اطلاعات حساس و با ارزش سازمانی از طریق کاربران خانگی بسیار آسان‌تر از شکستن لایه‌های مختلف امنیتی، نفوذ به یک پایگاه اطلاعاتی و دسترسی به اطلاعات رمزگذاری شده است.

در اینجا ملاحظات در رابطه با راهکارها و ملزومات حفاظتی که هر کاربری برای افزایش امنیت اطلاعات و دریافت خدمات مطلوب در اینترنت، باید از آنها آگاه باشد، آورده شده است.

صفحات اینترنتی که در آنها مبادلات آنلاین و خدمات حساس مالی یا تجاری انجام می‌شود، باید دارای ملزومات زیر باشند:

- تضمین این مسئله که داده‌های وارد شده برای انجام مبادلات و یا معاملات الکترونیک، تنها توسط بخش‌ها یا افراد معینی قابل دسترسی است. این مسئله از طریق رمزگذاری انجام می‌شود.
 - صحت، درستی و عدم نقص اطلاعات در طول عملیات نقل و انتقال؛ به منظور اطمینان از عدم سوءاستفاده از اطلاعات حساس. این مسئله از طریق استفاده از امضای دیجیتال انجام می‌شود.
 - در نهایت، هویت هر دو طرف رابطه تجاری، یعنی ارائه دهنده و دریافت کننده خدمات آنلاین، باید کاملاً واضح و مشخص بوده و مورد تأیید و تصدیق قرار گیرد. مدارک هویت دیجیتالی برای رفع نگرانی‌های موجود در این رابطه مورد استفاده قرار می‌گیرند.
- برای دسترسی به این ملزومات کلی، روش‌های ارتباطی استاندارد طراحی شده است که هر کدام وظایف خاصی را بر عهده دارند.

پروتکل‌های امنیتی

پروتکل‌های امنیتی قوانین و استانداردهایی هستند که برای محافظت از مبادلات و معاملات اینترنتی در برابر تهدیدهای آنلاین، وضع شده‌اند و دسترسی‌های غیرمجاز به اطلاعات تبادل شده را محدود می‌کنند. به این ترتیب این پروتکل‌ها، نقش مهمی در محافظت از کاربران خانگی، شبکه‌های محلی، فروشگاه‌ها، سازمان‌ها و مؤسسات مالی تجاری دارند. تهدیدهایی چون سرقت اطلاعات، سرقت مستقیم و یا غیر مستقیم پول، ایجاد توقف و اختلال در فرایندهای تجاری، کلاهبرداری‌های آنلاین و غیره، تهدیدهایی هستند که از کوچک‌ترین نقص و اشتباه در کاربرد این پروتکل‌ها سود می‌برند.

اعتبار بخشی امنیتی

علاوه بر استفاده از پروتکل‌های امنیتی و ابزار حفاظت از اطلاعات رایانه‌ای مانند نرم‌افزارهای ضد ویروس، هرکدام از طرف‌های یک معامله الکترونیک (ارائه کننده و دریافت کننده خدمات)، باید دارای ابزار و مدارک خاص امنیتی برای برقراری ارتباط امن با طرف مقابل خود باشند. رمزهای عبور، مدارک دیجیتال، کارت‌های هوشمند، امضای دیجیتال، شماره‌های IP، آدرس‌های MAC و حتی خصوصیات منحصر بفرد بیومتریک (اثر انگشت، ...) همگی ابزاری هستند که به اعتبار سنجی امنیتی طرف‌های یک معامله اینترنتی کمک می‌کنند. اعتبار و هویت امن کاربرهای خانگی اینترنت معمولاً با رمزهای عبور، شماره کارت هوشمند، امضای دیجیتال و ... تأیید می‌شود اما برای بانک‌ها، مراکز فروشگاهی بزرگ و سازمان‌های تجاری، دارا بودن مدارک امنیتی ویژه ضروری است.

امنیت تجارت الکترونیک؛ قابل دسترس، قابل اجرا

نکته بسیار مهم در اینجا است که روش‌های خاص امنیتی برای محافظت از معاملات اینترنتی چنان سختگیرانه طراحی شده‌اند که می‌توان ادعا کرد «دیگر تفاوت چندانی میان انجام معاملات حضوری و مبادلات الکترونیک باقی نمانده است.»

درست به همان نحو که یک مشتری، اطلاعات شخصی، محرمانه و حساس خود را به صورت رو در رو در اختیار هر فروشنده‌ای قرار نمی‌دهد و جوانب امنیتی را به طور کامل حفظ می‌کند، در حوزه مبادلات آنلاین نیز نباید این اطلاعات را در صفحات، پایگاه‌ها و نیز سرورهایی که فاقد مدارک و گواهی‌نامه‌های خاص امنیتی هستند، وارد کند. علاوه بر این، در لایه‌های ارتباطی بالاتر، مدیر شبکه خدمات دهنده باید نهایت دقت و احتیاط را در اطمینان از عدم وجود هرگونه کد یا ابزار مخرب (ویروس، تروجان، ابزار هک و ...) و نیز هرگونه آسیب پذیری (حفره‌ها و نقص‌های امنیتی) به کار گیرد تا امنیت داده‌ها و اطلاعات ذخیره شده در سرور مورد تهدید قرار نگیرند.

توصیه‌های مهم به کاربران خدمات بانکی و تجاری آنلاین

در هنگام انجام فعالیت‌های بسیار محرمانه مانند خرید و فروش آنلاین و یا انجام امور بانکی باید نکات زیر را همیشه به خاطر داشته باشید:

- از عدم حضور و فعالیت هر نوع کد مخرب در لحظه آغاز و در حین انجام فعالیت تجاری و دریافت هرگونه خدمات اینترنتی حساس، اطمینان حاصل کنید. در این خصوص باید گفت که خطرناک‌ترین و در عین حال شایع‌ترین تهدید علیه فعالیت‌های مالی اعتباری در اینترنت، نوعی کد مخرب از خانواده تروجان‌های Banker می‌باشد. این تروجان

پس از نفوذ در سیستم (اغلب به شکل نامحسوس)، بازدیدهای اینترنتی کاربر را کنترل می کند و به محض ورود وی به پایگاه های مؤسسات مالی اعتباری، سیستم های پرداخت آنلاین، مراکز خرید و فروش اینترنتی و ... اطلاعات حساس مبادله شده را پس از سرقت، به مجرمان اینترنتی ارسال می کند.

تمایل روزافزون کاربران اینترنت به انجام معاملات آنلاین و گسترش زمینه های دسترسی به خدمات الکترونیک نیز دلیل ساده ای برای افزایش تعداد و تنوع تروجان های Banker بوده است. البته دلیل محکم تری نیز وجود دارد و آن انگیزه های مالی خرابکاران اینترنتی و لذت دسترسی آسان و در عین حال غیرقانونی آنها به پول های باد آورده ای است که به علت ناآگاهی و بی احتیاطی بین زمین و هوا معلق مانده است. درست به همین خاطر، استفاده از نرم افزارهای حفاظتی به روز و ایجاد تنظیمات صحیح بر روی آنها، به تناسب امنیت مورد نیازتان، مهم ترین و ضروری ترین ابزار دفاعی شما می باشد.

پس دور از انتظار نیست که در آینده ای بسیار نزدیک، ابزار سنتی ضد ویروس، قدرت مؤثر خود را از دست بدهند. باید اعتراف کرد که آینده ای در کار نیست؛ همین حالا راهکارهای ضد ویروس باید آماده یک پوست اندازی کامل باشند تا بتوانند اقتدار نسبی شرکت های امنیتی را در دنیای فناوری اطلاعات حفظ کنند.

به همین منظور، شاید افزودن یک لایه امنیتی مکمل با فناوری های پیشرفته و یا استفاده از روش های هوشمند در تشخیص ویروس های مخرب و ... ایده های خوبی باشند.

● تقریباً همه کارشناسان امنیتی عقیده دارند که اکنون مؤثرترین ابزار دفاعی در رایانه ها، بهره گیری از روش های پیشگیرانه^۱ است. در این روش رفتار خاص کدها و نرم افزارهای فعال در موقعیت های مختلف، مهم ترین عامل شناسایی و تفکیک کدهای مخرب و مشکوک از کدهای امن و مفید است. در این حالت نیاز چندانی به استفاده از پایگاه های اطلاعات امنیتی ثبت شده و مشخصات ویروس های قدیمی تر (البته تا حدی) نیست.

● راهکار مؤثر دیگر استفاده از یک ابزار مکمل امنیتی در کنار نرم افزارهای حفاظتی نصب شده در سیستم (یا به عبارتی در کنار همان راهکارهای سنتی حفاظت از اطلاعات) برای ترمیم نقاط ضعف آنهاست. یکی از این سیستم های پیشرفته برای ردیابی و کشف ویروس های ثبت نشده با نام TruPreventTM، ابزار قدرتمندی برای پیشگیری از نفوذهای غیرمجاز و نیز افزایش توان بازدارندگی سیستم امنیتی نصب شده در رایانه است.

● به هیچ وجه هزینه های موجود در صندوق پستی خود را جدی نگیرید و به آنها اعتماد نکنید؛ هرچند اگر بسیار جذاب و قابل توجه جلوه کنند. هزینه هایی که از طرف فرستنده ها یا منابع کاملاً نامشخص و مبهم ارسال می شوند، ریسک تخریبی بسیار بالاتری دارند. در خصوص هزینه های مربوط به تجارت یا خرید و فروش الکترونیک نیز باید

گفت که اغلب آنها از منابع مطمئن و امن ارسال نمی‌شوند و به احتمال قوی ممکن است تنها، ابزاری برای فریبکاری خرابکاران و نیز سرقت اطلاعات حساس و ارزشمند شما باشند. هرزنامه‌ها سهم مهمی در اجرای حملات Phishing (ابزار کلاهبرداری آنلاین) دارند. Phishing، تکنیک بسیار حرفه‌ای است که اغلب کاربران غیرحرفه‌ای خدمات آنلاین را هدف می‌گیرد.

علاوه بر این، لینک‌های موجود در هرزنامه‌ها نیز می‌توانند بسیار خطرناک باشند؛ زیرا قادرند به راحتی شما را به صفحات مخرب و غیرواقعی در وب هدایت کنند که هدف آنها ایجاد تخریب و اختلال در سیستم و نیز دسترسی غیرقانونی به اطلاعات و داده‌های مهم شماست. بنابراین به شما توصیه می‌شود که به جای کلیک بر روی هر لینکی، آدرس آن را به طور مستقیم در نوار آدرس مرورگر خود تایپ کرده و کلید جستجو را فشار دهید. اگر «حتی فقط یکبار» قصد تجربه لذت بخش خرید الکترونیک و یا انجام فعالیت‌های بانکی آنلاین را دارید، موارد زیر را فراموش نکنید:

- قبل از انجام خرید از فروشگاه‌های آنلاین و یا از طریق پایگاه‌های الکترونیک، و نیز دریافت هرگونه خدمات اینترنتی، یکی از بهترین تدابیر امنیتی، اطمینان از قانونی بودن، میزان شهرت و سطح اعتبار این مرکز مالی تجاری است. یک جستجوی ساده در اینترنت، شاید راهنمای خوبی در این زمینه باشد.

- سیستم‌های رایانه‌ای خود را همواره به روز نگاه دارید. سیستم‌های عامل و نیز بسیاری از برنامه‌های کاربردی نصب شده در رایانه شما یقیناً دارای نقص‌ها و حفره‌های امنیتی بی‌شماری هستند که می‌توانند توسط خرابکاران اینترنتی برای نفوذهای نامحسوس و انجام فعالیت‌های غیرقانونی مورد استفاده قرار بگیرند. تنها یک اشکال کوچک امنیتی در برنامه‌های به ظاهر ساده و پرکاربرد مانند Media Player، Yahoo Messenger و یا ACDSee، نقش خود را به نحو احسن ایفا می‌کند.

- هیچ‌گاه فایل‌ها و نرم افزارهای نامطمئن را بارگذاری و اجرا نکنید؛ به خصوص اگر آنها در منابع و پایگاه‌های اینترنتی نامشخص و بی نام و نشان وجود داشته باشند. این فایل‌ها می‌توانند ضمیمه نامه‌های الکترونیک و یا برگرفته از صفحات اینترنتی مشکوک باشند. به خاطر داشته باشید که احتمال آلوده بودن این فایل‌ها آنقدر زیاد است که با اجرای آن، بطور مستقیم کدهای مخرب را در رایانه خود نصب می‌کنید.

- هیچ‌گاه قبل از اطمینان کامل از شرایط امنیتی موجود، اقدام به پرداخت و یا نقل و انتقال پول نکنید (درست به همان گونه که معاملات حضوری و فیزیکی را انجام می‌دهید). به خاطر داشته باشید که احتمال کلاهبرداری و فعالیت غیرقانونی در اینترنت همیشه بیش از آن است که فکر می‌کنید. شما نخستین فردی نیستید که شاید در ازای سفارش آخرین و مدرن ترین نسل تلفن‌های همراه، جعبه‌ای پر از سنگ و ماسه دریافت کرده باشد.

- امروزه انجام مزایده‌های آنلاین در اینترنت به طور چشمگیری رواج یافته است. قبل از آغاز پیشنهاد قیمت و شروع مزایده، از

شخصیت حقیقی و حقوقی مسئول مزایده اطلاع کامل پیدا کنید و فریب تکنیک‌های حرفه‌ای فروش وی را نخورید.

● هیچ گاه اطلاعات حساس و محرمانه خود را از طریق نامه‌های الکترونیک ارسال نکنید. کاربران عادی و حتی برخی از کاربران حرفه‌ای اینترنت گمان می‌کنند که این روش بسیار امن‌تر از پرکردن فرم‌های الکترونیکی است. اما متأسفانه این حقیقت ندارد. نامه‌های الکترونیک از لحاظ امنیتی بسیار آسیب پذیرند.

● از تیزهوشی و حس شک خود بهره بگیرید. ظاهر و ساختار یک صفحه وب اغلب می‌تواند نشان‌دهنده غیرواقعی بودن و یا امن نبودن آن باشد. به خاطر داشته باشید که در بسیاری از موارد خرابکاران اینترنتی صفحات موقتی در اینترنت ایجاد می‌کنند که تنها کاربرد آنها، کلاهبرداری از کاربران اینترنت است.

● در نهایت این عبارت را از دایره باورهای خود حذف کنید که «من به هیچ وجه در معرض خطر نیستم، چرا که من تنها یک کاربر معمولی و عادی اینترنت هستم.» به یاد داشته باشید که این همان چیزی است که مجرمان از شما انتظار دارند. یک خرابکار اینترنتی تنها با اعداد، ارقام و شماره‌های IP شما سروکار دارد و نه با شخصیت، شغل، میزان درآمد و یا سطح دسترسی شما به اینترنت.

۷-۵

خرید اینترنتی و حقوق مصرف کنندگان

در یک خرید اینترنتی از چه مواردی باید آگاه باشیم؟

اگر قصد خرید اینترنتی از یک فروشگاه الکترونیکی را دارید، باید با دقت کافی این کار را انجام دهید. خرید اینترنتی یک کار عجیب و سخت نیست، اما به هر حال وقتی شما به صورت فیزیکی هم خرید می‌کنید، به طور حتم ملاحظاتی را در نظر می‌گیرید (به عنوان مثال خرید از یک مکان معتبر). خرید اینترنتی شاید ساده‌ترین و لذت‌بخش‌ترین کاری باشد که شما در اینترنت می‌توانید انجام دهید به شرطی که به یک سری نکات مهم توجه داشته باشید.

خرید اینترنتی از فروشگاه‌های معتبر

قبل از خرید اینترنتی، ابتدا در مورد فروشگاه‌ای که می‌خواهید از آن خرید کنید تحقیق نمایید. فروشگاه‌های معتبر عموماً آدرس پستی، تلفن و مشخصات خود را به طور دقیق در وب سایت‌شان درج می‌کنند. دقت کنید که فروشگاه مورد نظر یک فروشگاه فعال است یا خیر؟ (یا مثلاً یک وب سایت رها شده). در نظر داشته باشید که تعداد زیادی وب سایت رها شده در اینترنت وجود دارند که روزی به مشتریان خود سرویس‌دهی می‌کرده‌اند، اما اکنون به علل مختلف بی‌استفاده مانده‌اند. اگر از طریق تبلیغات با فروشگاه آشنا شده‌اید، تقریباً می‌توان اطمینان داشت که فروشگاه مورد نظر فعال است،

اما اگر به طور اتفاقی وارد فروشگاه شدید، باید بررسی بیشتر نمایید. معمولاً در وب سایت‌های فعال، بخش اخبار به روز است و این را به عنوان یکی از نشانه‌های به روز بودن فروشگاه می‌توان در نظر گرفت. نکته دیگر این است که می‌توان بررسی نمود که اطلاعات تکمیلی در مورد کالا به همراه قیمت و شرایط و هزینه‌های ارسال درج شده باشد. معمولاً فروشگاه‌هایی که یک شعبه فیزیکی دارند، بسیار مطمئن‌تر از فروشگاه‌هایی هستند که فقط به صورت مجازی پایه‌گذاری شده‌اند و آمارها نیز نشان می‌دهد اعتماد افراد به فروشگاه‌هایی که شعبه فیزیکی دارند بیشتر است، زیرا احتمال کلاهبرداری و یا این که کالای خریداری شده به دست شما نرسد، کمتر است و در صورت بروز مشکل، می‌توانید به آدرس فروشگاه مربوطه مراجعه کنید.



شکل ۶-۷ انتشارات مدرسه

انتخاب روش خرید مناسب

وقتی از یک فروشگاه مجازی معتبر خرید می‌کنید، معمولاً انتخاب‌های متعددی برای نحوه خرید و دریافت کالا برای شما وجود خواهد داشت. از جمله پرداخت وجه به صورت آنلاین، خرید به صورت پستی، واریز به حساب و همیشه سعی کنید روشی برای خرید خود انتخاب کنید که کمترین ریسک‌پذیری را داشته باشد.

خرید به صورت آنلاین

معمولاً فروشگاه‌هایی که ارائه‌دهنده سرویس‌های آنلاین هستند، خدمات پرداخت اینترنتی خود را از یکی از بانک‌های کشور دریافت می‌کنند و بانک‌ها نیز معمولاً بابت ارائه این نوع سرویس، از فروشگاه‌ها مبالغی بابت ضمانت دریافت

می‌کنند. اخذ مبالغ ضمانت به این دلیل است که در صورت طرح شکایت از فروشگاه مربوطه، بانک بتواند ضمانت را به اجرا بگذارد. استفاده از این سیستم بیشتر در مواقعی مناسب است که شما محصول خود را می‌خواهید به صورت الکترونیکی دریافت کنید، مانند خرید کارت اینترنت و موارد شبیه آن، در پرداخت‌های آنلاین همیشه وقتی می‌خواهید مرحله پرداخت وجه را از طریق کارت انجام دهید، وارد سایت دومی خواهید شد که سایت بانک دریافت‌کننده وجه است. دقت کنید بسیاری از سارقان اینترنتی با راه اندازی سایت‌هایی شبیه به سایت‌های بانک‌ها و آدرس‌های شبیه به آنها، اقدام به کلاهبرداری نموده‌اند. اگر از مرورگر IE استفاده می‌کنید، بعد از ورود به صفحه پرداخت بانک، تصویر یک قفل زرد رنگ پایین صفحه مشاهده می‌شود. روی آن قفل دو بار کلیک کنید تا گواهینامه سایت باز شود. در قسمت Issuedto آدرس بانک نوشته شده است. (مثلاً اگر وارد سایت بانک پارسیان شده باشید، باید www.pec.ir نوشته شده باشد). ولی اگر وارد قسمت پرداخت شدید و این قفل زرد رنگ را مشاهده نکردید، یا نام داده شده در قسمت Issuedto درست نبوده، شماره کارت رمز خود را وارد نکنید، چون نشان دهنده این است که این سایت از نظر امنیتی تأیید نشده است و یا اصلاً سایت بانک نمی‌باشد و اطلاعات شما در اختیار افراد دیگری قرار خواهد گرفت.

شیوه خرید از طریق واریز به حساب

در این روش برای خرید اینترنتی یک کالا باید (احتمالاً ساعت‌ها!) در صف بانک بایستید تا مبلغ را به حساب فروشگاه واریز کرده و سپس شماره فیش را در وب سایت وارد کنید تا محصول مورد نظر را برای شما ارسال کنند. این شیوه یکی از نامناسب‌ترین شیوه‌های خرید اینترنتی است و حتی شاید نتوان آن را یک خرید اینترنتی قلمداد کرد. زیرا استفاده از تجارت الکترونیک باید باعث سرعت و سهولت در خرید گردد، اما در این روش شما دردسر بیشتری نسبت به خرید فیزیکی خواهید داشت. از نظر امنیتی هم استفاده از این روش خرید غیر معقولانه است. در پرداخت‌های الکترونیکی تمام سوابق تراکنش‌های مالی شما در سیستم ثبت می‌شود و حتی مشخص است که این کالا در چه تاریخی و از چه فروشگاه‌های و با چه قیمتی خریداری شده است. اما در حالتی که شما به حساب فردی مبلغی واریز می‌کنید، ممکن است هیچ وقت چیزی به دست شما نرسد و چون شما مبلغ را در بانک واریز کرده‌اید و این فروشگاه اینترنتی برای بانک شناخته شده نیست و فروشگاه ضمانتی هم به بانک نداده است. اثبات این که شما مبلغی را بابت خرید محصول خاصی که در اینترنت وجود داشته پرداخت کرده‌اید مشکل‌تر است و ردیابی آن سخت‌تر و یا اگر بر فرض فیش بانکی گم شود که اوضاع وخیم‌تر خواهد شد.

خرید پستی

شاید امن ترین روش برای خرید اینترنتی استفاده از سیستم خرید پستی باشد که امروزه اغلب فروشگاه‌ها نیز از این سرویس استفاده می‌کنند. شما با استفاده از این روش می‌توانید محصول مورد نظر را سفارش دهید و محصول مورد نظر توسط شرکت پست برای شما ارسال شده و سپس مبلغ کالا را به مأمور پست تحویل می‌دهید. می‌بینید که در این روش شما با اطمینان خاطر و بدون اینکه پولی را از پیش پرداخت کرده باشید، می‌توانید محصول خود را خریداری نمایید. استفاده از این روش برای کالاهایی که ماهیت فیزیکی دارند، بسیار مناسب است. همیشه سعی کنید در فروشگاه‌هایی که امکان خرید پستی وجود دارد، از این روش استفاده کنید. البته از این شیوه در محصولاتی که ماهیت فیزیکی ندارند مانند کارت اینترنتی، اطلاعات و حق عضویت و نمی‌توان استفاده کرد و باید شیوه پرداخت آنلاین استفاده شود.



شکل ۶-۷ انتشارات مدرسه

خدمات بانکداری الکترونیکی (بانکداری اینترنتی)

بانکداری الکترونیک شامل سیستم‌هایی است که مشتریان مؤسسات مالی را قادر می‌سازد تا در سه سطح اطلاع رسانی، ارتباط و تراکنش از خدمات و سرویس‌های بانکی استفاده کنند:

الف) اطلاع رسانی: این سطح ابتدایی ترین سطح بانکداری اینترنتی است. بانک اطلاعات مربوط به خدمات و عملیات بانکی خود را از طریق شبکه‌های عمومی یا خصوصی معرفی می‌کند.

ب) ارتباطات: این سطح از بانکداری اینترنتی امکان انجام مبادلات بین سیستم بانکی و مشتری را فراهم می‌آورد. ریسک این سطح در بانکداری الکترونیک بیشتر از شیوه سنتی است و کنترل‌های مناسبی را برای عدم دسترسی به شبکه اینترنت بانک و سیستم‌های رایانه‌ای نیاز دارد.

ج) تراکش: این سیستم متناسب با نوع اطلاعات و ارتباطات خود از بالاترین سطح ریسک برخوردار است و با یک سیستم امنیتی کنترل شده قادر است، صدور چک، انتقال وجه، پرداخت قبوض و افتتاح حساب را انجام دهد.

مروری بر ویژگی‌های بانکداری اینترنتی

بانک‌های صددرد ایتترنتی با هدف اصلی قبول سپرده، به عنوان بانک‌های بدون شعبه یا دستگاه خودپرداز می‌باشند که با استفاده از وب سایت، مشتریان را جذب و خدمات خود را ارائه می‌دهند (در حقیقت این بانک‌ها شعبه فیزیکی و واقعی ندارند). وظیفه اصلی این بانک‌ها ارائه خدمات از طریق اینترنت است، مشتریان محدود، به این شیوه از ارتباط نیستند، بلکه از طریق تلفن و پست نیز می‌توانند تماس برقرار کنند. تأیید اینگونه بانک‌ها نیز همچون بانک‌های عادی، با دریافت معیارها و شرایط قانونی لازم و کسب مجوز از بانک مرکزی انجام می‌شود.

مزایای بانک‌های صددرد ایتترنتی

همانند هرگونه تجارت الکترونیکی، مزایا و معایبی برای کار با این نوع بانک‌ها وجود دارد که در این بخش به طور خلاصه به آن می‌پردازیم.

در صورتی که شما تصمیم به کنار گذاشتن بانک خود و حرکت به سمت دنیای جدید بانک صددرد ایتترنتی گرفته‌اید، چه انتظاری از این تجربه جدید می‌توانید داشته باشید؟

با توجه به قابلیت آن در ارائه خدمات در وب سایت، این نوع بانک‌ها مزایای مهمی را در بردارند:

- دستیابی در هر مکان و هر زمان: تا زمانی که شما یک کامپیوتر و امکان اتصال به اینترنت را دارید، بدون در نظر گرفتن ساعات بانکی و تعطیلات، می‌توانید به آن دسترسی داشته باشید.
- عدم هرگونه دردسر برای گشایش حساب: بانک‌های صددرد ایتترنتی نه تنها برای گشایش حساب، امکان انجام کلیه مراحل از طریق خط اینترنت را می‌دهند، بلکه واریز وجه برای گشایش حساب نیز می‌تواند انجام شود.
- وب سایت‌هایی که دارای ویژگی‌های سهولت در استفاده و قدرت عملیاتی بیشتری می‌باشند: اینترنت تنها شعبه برای بانک‌های ایتترنتی محسوب می‌شود. اینگونه بانک‌ها با جهت گیری بهتر به طرف مشتری و با ایجاد یک ارتباط از طریق شبکه، تجارت بسیار بهتری را برای کاربران آن - در مقایسه با بانک‌های عادی - به ارمغان می‌آورند.
- پیشنهاد بهتر: با کاهش هزینه‌های کلی، بانک‌های صددرد ایتترنتی قادر هستند که سود خود را به مشتریان انتقال دهند. برای مشتریانی که مبالغ زیادی در این بانک‌ها سپرده گذاری می‌نمایند، امکان کاهش و یا حذف کارمزدها وجود دارد.
- سهولت در پرداخت قبوض: بانک‌های ایتترنتی در ساده نمودن مراحل پرداخت قبوض - چه نمایش قبوض بر روی صفحه کامپیوتر و چه پرداخت قبوض - تا حد امکان تلاش نموده‌اند.

معایب بانک‌های صددرد ایتترنتی

توصیه می‌شود قبل از تصمیم به تثبیت وضعیت حساب‌های خود (جاری و پس انداز) در یک بانک ایتترنتی، به موارد زیر نیز توجه فرمایید:

- ملاقات حضوری در بانک را فراموش نکنید.
- واریز نمودن پول نقد در حساب‌ها را فراموش کنید.
- نبودن بعضی از خدمات ویژه
- مشاور مالی
- مواظب هیولای کارمزد باشید.
- ضرورت آشنایی با فناوری

کاربری بانکداری ایتترنتی

بانکداری ایتترنتی برای همه افراد از یک درجه اهمیت برخوردار نیست. مشاورین، مشتریان بانک‌های ایتترنتی را به چهار گروه تقسیم نموده‌اند. شما با تطبیق خود به گروهی که با شرایط شما سازگاری دارد، می‌توانید در جهت مناسب گام بردارید:

۱- معامله کنندگان ایتترنتی: این گروه مشتری مایل به اتوماسیون و ساده نمودن احتیاجات تراکنشی خود، تا حد امکان می‌باشد. دستیابی به حساب‌های چک (جاری) و کارت‌های اعتباری از طریق خط ایتترنت، به عنوان مزیتی برای این گروه مشتریان محسوب می‌شود. در این نوع حساب‌ها، پرداخت قبوض با کارمزد کم با ابزاری برای اتوماتیک نمودن عملیات، از اهمیت خاصی برخوردار است.

۲- پس انداز کنندگان: این دسته از مشتریان به دنبال نتیجه و بازدهی بالا از حساب‌های خود هستند که اقدام به نگهداری وجوه و مبالغ بالا می‌نمایند و همچنین انتظار کارمزد پایین را دارند. انتقال راحت وجوه بین حساب‌ها برای این افراد اهمیت دارد.

۳- خریداران فوری: این گروه از مشتریان بدون دغدغه فکری خواهان خدمات مالی جامع، کارت‌های اعتباری، وام‌ها و پرداخت قبوض به طور یکپارچه می‌باشند. سهولت در استفاده و گستردگی این خدمات، مهم‌ترین عامل برای این گروه از مشتریان می‌باشد.

۴- وام گیرندگان: این گروه از مشتریان خواهان دریافت وام با مبالغ دلخواه و با سود کم و امکان وثیقه‌گذاری پایین می‌باشند.

کارمزد در بانک‌های اینترنتی

در حالی که همه بانک‌های اینترنتی برای ارائه خدمات کارمزد دریافت نمی‌کنند و بعضی نیز بر اساس وضعیت حساب، بخشی از کارمزدها را حذف می‌نمایند، لیکن به هر نحو، باید انتظار کارمزد را برای حداقل برخی از موارد ذکر شده در زیر داشت:

- پرداخت قبوض
- کارمزد دستگاه‌های خودپرداز
- کشیدن چک و درخواست دسته چک
- کارت‌های اعتباری
- سایر کارمزدها

راه حلی برای برتری در بانکداری: شعبه اینترنتی

بر اساس آخرین تحقیقات به عمل آمده، استفاده از اینترنت ظرف چند سال آینده، به طور قابل ملاحظه‌ای افزایش می‌یابد که از جمله دلایل این افزایش فوق العاده، پایین بودن قیمت کامپیوترهای شخصی، آسودگی بیشتر و ایمنی اشاره کرد. فراهم کردن فرصتی برای بازاریابی بی واسطه و مستقیم، کارایی مؤثر، مطمئن و با ایمنی بالا، از مزایای ایجاد سیستم الکترونیک بانکداری است. بانک‌ها نیز، واقعی تلاش کرده‌اند که بخشی از خدمات خود را به صورت اینترنتی به مشتریان خود ارائه دهند.

۶-۷

هوشیاری در اینترنت

چرا باید در دسترسی به خدمات اینترنتی بانک‌ها، به مسئله امنیت دقت کنم؟

اینترنت، زندگی همه ما را به نحو مطلوبی دگرگون کرده و این تحول البته در حوزه پول و اعتبار، مورد اقبال عمومی واقع شده است. افزایش سرعت خدمات بانکی، کارآمدی مؤسسات مالی اعتباری، صرفه جویی در زمان و حتی کاهش ترافیک شهری، کمترین مزایای استفاده از خدمات اینترنتی بانک‌ها است که کمابیش توجه کاربران ایرانی را نیز به خود جلب کرده است.

حتی از طریق یک اتصال معمولی به اینترنت، می‌توانیم بسیاری از فعالیت‌های بانکی وقت گیر و مهم خود مانند انتقال وجه، دریافت صورت وضعیت، اطلاع از آخرین رقم موجودی، پرداخت قبوض، خرید کالا و ... را آن هم به صورت موفقیت آمیز انجام دهیم. خدمات اینترنتی بانک‌ها، بسیار مناسب، خیلی سریع و کاملاً ساده هستند؛ اما آیا می‌توانیم عبارت «خیلی امن» را هم قاطعانه به این فهرست اضافه کنیم؟

امنیت، حقیقت فراموش شده

واقعیت این است که اغلب بانک‌ها، سازمان‌ها و مراکز تصمیم‌گیری، کاربران خدمات بانکی را با انواع تبلیغات، اطلاعیه‌ها و تشویق‌ها بمباران می‌کنند تا علی‌رغم تمام محدودیت‌های موجود در خصوص دسترسی افراد به اینترنت، آنها را به سمت استفاده از خدمات اینترنتی سوق دهند، فارغ از این که اطلاع‌رسانی همین دستگاه‌ها در خصوص امنیت «اینترنت بانک» تقریباً صفر است. البته این مسئله کاربران خانگی و شخصی را از بی‌توجهی به تأمین امنیت اینترنت در رایانه‌های خود مبرا نمی‌کند؛ اما مراکز و رسانه‌های تأثیرگذار بر جامعه باید به تناسب تبلیغات پی در پی در خصوص استفاده از «اینترنت بانک»، به امنیت این خدمات مهم و ارزشمند نیز توجه کافی داشته باشند.

از سویی دیگر، کاربران خدمات اینترنتی باید بدانند که امنیت اطلاعات هم در طرف خدمات‌دهنده^۱ و هم در طرف خدمات‌گیرنده^۲، باید به طور کامل تأمین باشد و صرف ارائه خدمات امن از طرف بانک، امنیت اطلاعات مالی اعتباری کاربر یا خدمات‌گیرنده را تضمین نمی‌کند و محیط عملیاتی او نیز باید کاملاً حفاظت شده و عاری از تهدیدهای رایانه‌ای باشد.

بسیاری از کدهای مخرب و ویروس‌های رایانه‌ای، با هدف سرقت اطلاعات ارزشمند و حساس کاربران، طراحی و در شبکه جهانی اینترنت منتشر می‌شوند. این بدافزارها اغلب به دنبال ایجاد اختلال در فرایندهای عملیاتی رایانه شما نیستند و شما هیچ وقت از حضور و فعالیت مخرب آنها آگاه نخواهید شد. به بیانی دیگر چون این ویروس‌ها نشانه خاصی ندارند و عملکردهای سیستم را تحت تأثیر قرار نمی‌دهند، توجه شما را به هیچ وجه جلب نمی‌کنند. وظایف اصلی آنها، جمع‌آوری اطلاعات محرمانه و ارسال رونوشتی از آنها به خرابکاران و مجرمان اینترنتی است. بسیاری از آنها فعالیت‌های مالی اعتباری شما را رصد می‌کنند؛ برخی دیگر رایانه شما را در برابر سایر تهدیدهای خطرناک آسیب‌پذیر می‌کنند و بعضی دیگر نیز مانند کدهای مخرب Bot، می‌توانند رایانه‌ها را به طور کامل در اختیار گروه‌های تبهکاری قرار دهند، به نحوی که از آنها در تخریب وسیع و یا سرقت گسترده اطلاعات استفاده شود.

۱- Server - Side

۲- Client - Side

چگونه، دسترسی به خدمات اینترنتی بانک‌ها را امن کنیم؟

بانک‌ها و مؤسسات مالی اعتباری، به شما خدمات امن ارائه می‌کنند. این مسئله نباید موجب نگرانی شما باشد که ممکن است بانک‌ها ناامن باشند. البته در مواردی نادر، خرابکارهای حرفه‌ای با حمله به پایگاه‌های اطلاعاتی مؤسسات مالی، موفق شده‌اند تا علاوه بر سرقت مستقیم پول، اطلاعات ارزشمند و حساس مشتریان آنها را نیز به سرقت ببرند (نظیر آنچه که در سال ۲۰۰۸ میلادی برای بانک سوئدی نوردآ اتفاق افتاد). اغلب مجرمان اینترنتی ترجیح می‌دهند به علت سطح بالای امنیت و مدیریت ریسک در مراکز مالی، به مشتریان یا دریافت کنندگان خدمات بانکی حمله کنند. بنابراین اگر شما رایانه خود را به یک محیط امن برای دریافت خدمات مالی تبدیل کنید، تهدید عمده‌ای متوجه شما و اطلاعات شما نخواهد بود.

مهم‌ترین نکته‌ای که باید به آن توجه کنید این است که همانقدر که در دنیای واقعی مراقب اطلاعات مالی، کارت‌های اعتباری و وجوه نقد یا غیر نقد خود هستید، در فضای اینترنت نیز باید تمام جوانب و ملزومات امنیتی را رعایت کنید. مطمئن باشید که احتمال سرقت شماره کارت اعتباری و اطلاعات مالی شما از طریق اینترنت، از احتمال سرقت عمدی کارت اعتباری شما، به همراه رمز عبور مربوط به آن و یا دسته‌ای پول نقد که حتی در کیف دستی خود قرار داده‌اید، کمتر نیست. پس بنابراین، برای امنیت فعالیت‌های بانکی خود در اینترنت:

● رایانه خود را به یک نرم افزار امنیتی پیشرفته با حداکثر امکانات حفاظتی مجهز کنید. این نرم افزار باید از جدیدترین فناوری‌های حفاظتی برای پیشگیری از نفوذ برخوردار بوده و فایل ضدویروس آن بروز باشد. به عنوان پیشنهاد می‌توانید از ضدویروس رایگان و قدرتمند Panda Cloud Antivirus، استفاده کنید.

● هر از چندگاهی، رایانه خود را برای کشف و پاکسازی ویروس‌های احتمالی اسکن کنید. برخی از ویروس‌ها، به هر دلیل می‌توانند از لایه‌های حفاظتی رایانه شما عبور کرده باشند. برای پاکسازی این نوع ویروس‌ها، اسکن دستی رایانه‌ها به صورت دوره‌ای ضروری است.

● هرزنامه‌ها و یا پیغام‌های مشکوک با فرستنده‌های ناشناس را به هیچ وجه جدی نگیرید. هرچند اگر جذاب یا قابل توجه جلوه کنند. این نامه‌ها می‌توانند حاوی لینک‌های مخرب و یا ابزار کلاهبرداری آنلاین باشند.

● از هر فروشگاه‌ای خرید نکنید. حتی اگر شما را به صفحه پرداخت اینترنتی مربوط به بانک خودتان هدایت کنند. حتماً قبل از خریدهای اینترنتی از میزان شهرت، قانونی بودن، سطح اعتبار و قابلیت ارائه خدمات امن توسط مراکز فروشگاه‌ای اطمینان حاصل نمایید.

● علاوه بر نرم افزارهای ضدویروس، سیستم‌های عامل و برنامه‌های کاربردی مهم خود را نیز به روز نگاه دارید. دانلود و نصب اصلاحیه‌های مهم نرم افزاری و به‌روزرسانی خودکار سیستم‌های عامل، راهکارهای مناسبی محسوب می‌شوند.

- هیچ فایل یا نرم افزار نامطمئنی را دانلود و بر روی سیستم خود اجرا نکنید. البته دانلود فایل ها و نرم افزارهای کاربردی به ظاهر امن از پایگاه های نامشخص و بی نام و نشان اینترنتی، به هیچ وجه توصیه نمی شود. در این شرایط احتمال دانلود یک کد مخرب و سپس اجرای مستقیم آن در رایانه توسط خود شما بسیار بالاست.
- در نهایت، هیچ گاه اطلاعات حساس و بسیار محرمانه خود را از طریق نامه های الکترونیک ارسال نکنید. بر خلاف تصور عموم، نامه های الکترونیک از لحاظ امنیتی بسیار آسیب پذیرند.
- این دستورالعمل های ساده، تقریباً امنیت کامل فعالیت های بانکی شما در اینترنت را تضمین می کنند.

۷-۷

کنترل و نظارت والدین

دلایل کنترل و نظارت نوجوانان در اینترنت به وسیله والدین چیست؟

به دلیل استفاده روزافزون و همگانی از پدیده های فناوری اطلاعات و ارتباطات، به خصوص در دسترس بودن این ابزار و امکانات برای کودکان و نوجوانان، خطرات و آسیب های به کارگیری آنها، ضروری است مطالبی، درباره نظارت والدین بر استفاده این گروه آسیب پذیر ارائه شود.

در چنین عصری که جهان بر محور فناوری اطلاعات و ارتباطات می چرخد و همه شئون اجتماعی را تحت تأثیر قرار داده و همه گروه های سنی را مجذوب خود کرده است، و انواع جرائم و آسیب های اجتماعی را نه تنها مضاعف، که متحول و دگرگون ساخته است، باید در اندیشه طرح و روشی دیگر برای هدایت، راهنمایی و حفاظت از نوجوانان بود. برای مثال امروزه کامپیوتر در زندگی کودکان نقش مهمی ایفا می کند و این نقش، به سرعت در حال افزایش است. در این عصر، فرزندان از سنین کم به سوی رایانه و به طور کلی، فناوری اطلاعات کشیده شده اند و نمی توان از استفاده آنها از این فناوری جلوگیری به عمل آورد. پدر و مادر باید سعی کنند، بر عملکرد فرزندان شان نظارت و کنترل مناسب داشته باشند. فناوری اطلاعات، هم می تواند خطرآفرین و هم سودمند باشد، زیرا در صورت نبودن نظارت، فرزندان به مشکلاتی از لحاظ جسمی و روحی دچار می شوند که ممکن است، دیگر راه علاجی برای این مشکلات وجود نداشته باشد؛ ولی اگر از دریچه ای دیگر به این فناوری بنگریم و امکانات مفید آن را به فرزندان آموزش دهیم، می توانیم آینده ای روشن و پربار را برای آنها رقم بزنیم. ابزار و دانش فناوری اطلاعات و ارتباطات جهانی، نوظهور و بسیار پر پیچ و خم است. وقتی فرزندان ما می خواهند از این فناوری استفاده کنند؛ مانند کسانی هستند که می خواهند، به فضا یا جهانی تخیلی سفر کنند و از دام ها، دره ها، سیاه چال ها و حتی مناظر زیبایی که در این سفر با آنها روبه رو می شوند، اطلاعی ندارند.

اینترنت

اینترنت فضایی وسیع و اقیانوسی از اطلاعات است که هم اکنون با شکل گرفتن جامعه اطلاعاتی و فضای شبکه‌ای، نمودی از دهکده جهانی را به نمایش گذاشته است. این فضا روزانه در حال گسترش و افزایش است و محدودیتی برای آن متصور نیست. شبکه اینترنت، هم اطلاعات مفید و قابل استفاده را در خود جای می‌دهد و هم اطلاعات فاسد، ناسالم و گمراه کننده را؛ محیطی که سرگرمی‌ها، بازی‌ها و بسترهای ارتباطی جذابی را متناسب با هر گروه سنی در دل خود دارد، به دلیل همین تنوع و وسعت اطلاعات، و از سویی سرعت و آسانی دسترسی به آنهاست که اینترنت، اینگونه جایگاه ویژه‌ای نزد اقشار مختلف مردم یافته و روزه روز، هم به جمع علاقه مندان این فناوری در جهان افزوده می‌شود. بر اساس اعلام مراکز گوناگون جهانی، دو سوم والدین، از نحوه آگاهی یافتن استفاده فرزندان‌شان از اینترنت ناتوان هستند. در حقیقت آنها به هیچ وجه نمی‌توانند، ارتباطات اینترنتی فرزندان‌شان را کنترل کنند و این به نگرانی عمیق در میان والدین تبدیل شده است.

اطلاعات و آمار، نشان‌دهنده اهمیت موضوع اینترنت و استفاده فرزندان از آن است. از دیگر مسائلی که می‌تواند، در رابطه میان فرزندان و اینترنت مشکل‌آفرین باشد، استفاده از اتاق گفت‌وگو یا همان چت کردن و نیز پست‌های الکترونیکی فرزندان است. باید توجه داشت که این امکان وجود دارد که فرزند ما با کسانی که اصلاً آنها را نمی‌شناسد، به چت مشغول شوند؛ در حالی که نمی‌داند، این شخص چه خطراتی می‌تواند برای آنها در پی داشته باشد. افراد مختلف می‌توانند، در چت مشکلات زیادی را برای فرزندان شما ایجاد کنند و آنها را مورد انواع سوء استفاده قرار دهند. پدر و مادر، با نظارت نامحسوس با آگاهی از اینکه فرزند آنها با چه کسی مشغول گفت‌وگوست، می‌توانند از بروز چنین مشکلاتی جلوگیری کرده، از عدم وقوع خطرات، اطمینان حاصل کنند.

هم چنین والدین باید بر پست الکترونیکی‌ای که برای فرزندان فرستاده می‌شود، کنترل داشته باشند و از مطالب، تصاویر و فیلم‌هایی که برای آنها ارسال می‌شود، آگاهی یابند. پدر و مادر باید بکوشند، خودشان برای فرزندشان ایمیل ایجاد کنند، تا بتوانند از رمز ورود آن اطلاع یابند و پیش از فرزندشان، از موارد ارسالی آگاهی یابند، در غیر این صورت باید سعی کنند به هر طریقی، از رمز ورود و کلمه کاربری آن اطلاع یابند.

اینترنت جدا از مضراتش، منافع هم برای رشد علمی و خلاقیت فرزندان دارد. با اتصال به شبکه جهانی اینترنت، کودکان و نوجوانان ما می‌توانند، با مراجعه با پایگاه‌های مخصوص سن خود، به اطلاعات گسترده و مفیدی دست یابند و قدرت پرسش‌گری و پژوهشگری خود را بالا برده، با جست‌وجو، پاسخ پرسش‌های خود را یافته، اطلاعات عمومی خود را افزایش دهند. آنها می‌توانند، این مطالب سودمند را در مدرسه، زندگی روزمره و برخوردهای اجتماعی به کار برده، به روز فکر کنند.

بازی های رایانه ای

مبحث دیگری که باید بدان پرداخت، مسئله بازی های رایانه ای است. با این که برخی از این بازی ها می تواند سازنده باشد، برخی دیگر می تواند، آثار مخربی بر روح و جسم فرزندان داشته باشد. بسیاری متخصصان معتقدند که بهتر است، کودکان زیر سه سال، اصلاً با کامپیوتر و بازی های ویدیویی آشنا نشوند و تا حد امکان، با اسباب بازی های قابل لمس و واقعی، مثل لگو، خانه سازی و ... سرگرم شوند. در این مورد نتایج تحقیقات نشان می دهد که هیجان های رایانه ای می تواند به تخریب یا کندی عملکرد ذهنی کاربر منجر شود.

روانشناسان اعتقاد دارند بازی های رایانه ای در جریان ارائه مضامین جذاب و گیرای خود، با ارائه صحنه های پرخشونت و خشن، طرح اسلحه های مختلف، تأکید بر سرعت بیشتر، به نمایش گذاشتن برهنگی و ... زمینه ارائه فرهنگی خاص را که بازی های رایانه ای مبلغ آنها هستند، برای جوانان فراهم می آورند.

در بسیاری از این بازی ها، به هیچ عنوان بر محتوا و آثاری که می تواند، در کودک و نوجوان اثر بگذارد، فکر نشده و پشتوانه علمی و روانشناسانه ای ندارد، بلکه برخی از این بازی ها، برخلاف آنچه ما تصور می کنیم، بسیار مخرب و مضرند. یکی از مضرات ثابت شده بازی های رایانه ای، ایجاد روحیه خشونت و پرخاشگری در نوجوانان است، زیرا کودکان و نوجوانان در سنی هستند که زود تأثیر می پذیرند. امروزه با افزایش ضریب نفوذ رایانه در میان مردم، این دو قشر، بیشتر وقت خود را به بازی های مختلف رایانه ای که معمولاً محتوای آنها خشونت است، سپری می کنند. آنها از این روحیه الگو گرفته، با والدین و هم سن و سال های خود نیز اینگونه رفتار می کنند. حتی ممکن است کار به جایی برسد که شخصیت آنها همین گونه شکل گرفته، صحبت کردن و ارتباط عادی خود را فراموش کنند و تنها با حرکات فیزیکی ارتباط برقرار سازند و در خواست های خود را متأثر از شخصیت های رایانه ای، در قالب مکالمه های آنان بیان کنند. در صورت عدم اعتنا به این معضل، خانواده در آینده با مشکلات فراوانی روبه رو خواهد شد. هشدارها و مضرات بیان شده در مسیر رشد و بالندگی نسل امروز، کاملاً حیاتی بوده و اگر والدین، این مسائل را جدی نگرفته و نظارت بر تعامل فرزندان و رایانه را ساده انگاشته، جدی نگیرند و تنها نوعی سرگرمی کودکانه بپندارند، در آینده در ارتباط با فرزندان، با معضلات پیچیده ای مواجه خواهند شد که به راحتی قابل حل نخواهد بود.

تلفن همراه

این فناوری با قابلیت های فراوانی، چون فیلمبرداری، عکاسی، بلوتوث، اتصال به اینترنت، پیام چندرسانه ای، موقعیت یاب و چندین قابلیت دیگر، جایگاه ویژه ای نزد کودکان و نوجوانان یافته است. این فناوری نیز مانند دیگر فناوری ها، معایب و محاسنی دارد که والدین باید از آنها آگاهی یابند و از بروز مشکلات جلوگیری به عمل آورند.

روانشناسان اعتقاد دارند که اعتیاد به تلفن‌های همراه در جوانان و نوجوانان به شدت افزایش یافته و همین موضوع، مشکلات روحی و روانی بسیاری را برای آنان به همراه دارد که آنها باید از این ضررها آگاه باشند. هنگامی که این دستگاه‌ها برای کودکان ساخته می‌شود و کودکان مدّ نظر هستند، اپراتورهای تلفن همراه و تولید کنندگان مسئله سلامت و بهداشت را فراموش می‌کنند و بیشتر سعی در تحریک و به هیجان آوردن آنها، بامواد، ترکیبات و کاربردهای گوشی دارند و می‌کوشند، کاربران را هر چه بیشتر تحت تأثیر قرار دهند.

استفاده بیش از حد از تلفن همراه در میان کودکان و نوجوانان، عواقب جسمی جبران‌ناپذیری را به دنبال دارد. به گزارش بخش شبکه فناوری اطلاعات ایران، یکی از علل افسردگی و اضطراب در بین نوجوانان و جوانان، استفاده بیش از حد و غیرمنطقی از تلفن همراه و علاقه بسیار زیاد آنها به سرویس پیام کوتاه، دانلود انواع آهنگ‌های ویژه تلفن همراه و تبادل اطلاعات بیهوده است.

از دیگر ویژگی‌های تلفن همراه، بلوتوث، فیلم برداری و تصویربرداری، ضبط و پخش صوت و امکان نصب و استفاده از انواع بازی‌های رایانه‌ای ویژه تلفن همراه است. والدین در این زمینه بیشترین نقش را دارند و با جدی گرفتن این مسئله و قرار دادن آن در برنامه‌ریزی‌های زندگی خانوادگی خود، به فرزندان خود و نیز جامعه کمک شایانی برسانند. تنها مسئله نگران کننده که کنترل آن کمی مشکل به نظر می‌رسد، فناوری‌های تلفن همراه است که اگر مسئولان و والدین، دست به دست هم دهند، ممکن است این مشکل را هم تا اندازه‌ای مرتفع سازند و با فرهنگ سازی، آگاهی بخشی برای کاربری صحیح، بهره‌گیری از نرم افزارهای مفید و جذاب برای تلفن همراه و ایجاد پایگاه‌های مناسب با گرافیک زیبا و قابلیت‌های متنوع، کودکان و نوجوانان را به سمت استفاده مثبت از این ابزار راهنمایی کرد و نیاز آنها را برآورده ساخت. در پایان تعدادی از پایگاه‌ها و نرم افزارهایی را که مخصوص کودکان و نوجوانان است، معرفی می‌کنیم.

پایگاه‌ها:

www.Poopakmag.com

www.Melikamag.com

www.Darasara.kanoonParvareh.com

www.Hod.hod.ir

www.Intizarmag.ir

www.Roshd.ir

مطالعه آزاد - راهنمایی‌هایی برای مقابله با Spamها

در زیر راهنمایی‌هایی برای مبارزه با Spamها آورده شده است:

بدون باز کردن پیام آن را پاک کنید: باز کردن پیام Spam می‌تواند یک سیگنال به فرستنده Spam بفرستد که فردی پیام روی صفحه را مشاهده کرده و از این رو آدرس ایمیل معتبر است. (و این بدین معنی است که شما در آینده Spamهای بیشتری دریافت خواهید کرد.)

اگر شما نام فرستنده درون صندوق پستی تان یا موضوع بخش عنوان ایمیل را نمی‌شناسید، می‌توانید به سادگی بدون خواندن پیام، آن را پاک کنید. یا می‌توانید از قابلیت پیش نمایش در برنامه ایمیل تان استفاده کنید، یعنی بدون این که واقعاً آن را باز کنید، بدانید در چه رابطه‌ای است و سپس آن را پاک نمایید. (تذکر: مطمئن شوید که لحظه به لحظه از شر پیام‌های پاک شده خلاص می‌شوید وگرنه آنها دوباره در ناحیه سطل آشغال ساخته می‌شوند.)

هیچگاه به پیام‌های Spam، پاسخ ندهید: به هیچ طریقی، به یک پیام Spam پاسخ ندهید. پاسخ دادن به فرستنده Spam اطمینان می‌دهد که این یک آدرس ایمیل فعال است. برخی فرستندگان Spamها، به شما می‌گویند اگر می‌خواهید از فهرست ایمیل آنها حذف شوید، با یک کلمه Remove یا unsubscribe را در بخش عنوان ایمیل، تایپ کنید و از دستور پاسخ برای بازگرداندن پیام به آنها استفاده نمایید. ولی همواره، این کارها به فرستنده Spam نشان می‌دهد که آدرس شما معتبر است و آن را به گونه‌ای تنظیم می‌کنند که در نهایت، بیشتر پیام‌های ناخواسته دریافت نمایید.

انتخاب کردن: وقتی برای خرید آنلاین چیزی ثبت نام می‌کنید و آنها از شما یک آدرس ایمیل درخواست می‌کنند، یادتان باشد، چیزهایی را که نمی‌خواهید دریافت کنید را حتماً انتخاب نمایید. وقتی شما در یک سایت، ثبت نام می‌کنید، قسمت مربوط به محرمانگی آنها را بخوانید تا بفهمید چگونه از آدرس‌های ایمیل استفاده می‌کنند و به سایت اجازه ندهید ایمیل شما را ذخیره کند.

از فیلتر Spam استفاده نمایید: سرویس دهنده اینترنت شما ممکن است یک فیلتر spam رایگان (برای مثال Earth linki Spominator) برای توقف انباشته شدن spamها، قبل از آنکه آنها را ببینید، ارایه کند. اگر اینگونه نبود، شما می‌توانید برای یک سرویس فیلتر، مثل mail wise با پرداخت شارژ ماهیانه ثبت نام کنید. البته برنامه‌های خودکار توقف spamها نظیر، mcafee spam killer، barracuda، mail washer choicemail، همچنین بسته‌های مسدود کننده پیچیده تر spam، برای کاربردهای تجاری وجود دارند. سرانجام، می‌توانید در سرویس ارسال ایمیل مانند mail addresses که به آن می‌گویید فقط ایمیل‌هایی که برای شما مزیت دارد را دریافت کنید، مشترک شوید.

مراقب باشید: حتی به اصطلاح، اسپم‌کش‌ها نیز همیشه درست کار نمی‌کنند. یک اپراتور سرویس آنلاین به نام spamcop، می‌گوید «هیچ چیزی ۱۰۰٪ کار نمی‌کند، به جز عوض کردن آدرس ایمیل تان». صرف نظر از اینکه شما چگونه، برای فیلتر کردن یک spam تلاش می‌کنید، آنها همیشه برای شکست دادن فیلترها، کار می‌کنند.

مبارزه کنید: اگر شما می‌خواهید بر spamها (و سایر متجاوزین اینترنت) پیروز شوید، سایت‌های abuse.net یا صفحه ردیاب ed falk را بررسی کنید. spamhaus، بدترین اسپم‌های اینترنت را ردیابی می‌کند و با ispها و سازمان‌های مجری قانون، و پاک کردن spamهای مقاوم و سمج از اینترنت، همکاری می‌کند. این سایت همچنین، یک پایگاه داده رایگان از آدرس‌های ip و spamهای تأیید شده را فراهم می‌کند. این گروه‌ها، اینکه کجا، spamها را گزارش دهید، افراد مناسب برای شکایت کردن نزد آنها و دیگر راه‌های مبارزه با spamها را به شما خواهند گفت.

محافظت کودکان در اینترنت

محافظت کودکان از سوءاستفاده اینترنت Protecting Children from Internet Abuse عنوان کتاب ۱۲ صفحه‌ای است که توسط Asian School of cyber Laws در سال ۲۰۰۳ منتشر شده است. این کتاب دارای ۵ فصل و حاوی اطلاعات و نکات مفید در زمینه استفاده صحیح از تکنولوژی اینترنت است. مطالب این کتاب به هدف اطلاع‌رسانی برای والدین، سرپرستان، معلمان و نوجوانان نگاشته شده است. نکات، قوانین و مقرراتی که در این کتاب جمع‌آوری و ارائه شده است، تدبیری برای آگاهی و حفظ سلامت جامعه و فرزندان آن است.

خطراتی که کودکان آنلاین با آن روبه‌رو هستند

خطراتی که کودکان ممکن است در دسترسی آزاد به اطلاعات و منابع اینترنتی با آن مواجه شوند، منابع اینترنتی غیرقانونی هستند که اغلب جنسی، محرک و خشونت‌آمیز بوده و عامل اصلی ترغیب کودکان به انجام فعالیت‌های خطرناک و غیرقانونی هستند. نمونه‌ای از خطرات موجود در زیر آورده شده است:

- برخی از این سایت‌ها و گروه‌های خبری به تشویق و تبلیغ استفاده از مواد مخدر، سیگار یا الکل دست می‌زنند. بعضی دیگر نیز روش ساخت بمب و یا دریافت و ارسال کیت‌های کشت ویروس را آموزش می‌دهند.
- با وجود غیرقانونی بودن بازی‌های قمار، سایت‌های قماربازی اینترنت را تسخیر کرده‌اند. مشاهده یا مشارکت در سایت‌های قماربازی برای کودکان نامناسب و خطرناک است. زیرا شرط لازم جهت ورود به سایت‌های قماربازی آنلاین داشتن کارت اعتباری است. از این رو، مشاهده و مشارکت در این سایت‌ها تهدید بالقوه‌ای برای خانواده‌هایی که رفاه مالی خوبی دارند، محسوب می‌شود.
- با دسترسی کودکان به شماره کارت اعتباری والدین، خطر ارتکاب جرم اینترنتی وجود دارد، که در نهایت منجر به پیگردهای قانونی و عواقب مالی جبران‌ناپذیر می‌شود. باید Netiquette یعنی قوانین و آداب استفاده صحیح از اینترنت را به کودکان آموزش داد و از بی‌پروایی کودکان در سرکشی به چنین سایت‌هایی در زمان کار با اینترنت جلوگیری و کنترل کرد.
- خطر دیگر کودک‌آزاران هستند. افرادی که به هدف اغفال کودکان و سوءاستفاده جنسی در سایت‌های مختلف پرسه می‌زنند، و مانند شکارچیان موزی برای کودکان معصوم و ناآگاه دام‌های رنگین می‌گسترانند. آنها از پست الکترونیک و

اتاق‌های گفت‌وگو (Chat Rooms) به منظور جلب اعتماد کودکان و ترغیب آنها برای شرکت در جلسات رودرو استفاده می‌کنند. و با جلب اعتماد کودک، جلسه ملاقاتی را با او می‌گذارند. در این زمان است که کودک در دام این شیادان اسیر شده و با خطراتی چون تحلیل جسمی، بحران‌های روحی و دائمی روبه‌رو خواهد شد.

● در بعضی موارد هم کودکان پیام‌های الکترونیکی دریافت می‌کنند که آزار دهنده و خصمانه است یا اینکه حاوی اطلاعاتی هستند که تأثیرات منفی از لحاظ روحی و روانی برای آنها به وجود می‌آورند. تأثیراتی که سرنوشت و آینده این کودکان را تحت شعاع خود قرار می‌دهند.

● حفاظت از حریم خصوصی کودکان امری حیاتی است. چرا که چنین حریمی در اینترنت با درجه آسیب‌پذیری بالایی روبه‌رو است. هیچ فردی حق ندارد، مگر با کسب اجازه اولیا یا سرپرست کودک، به اطلاعات شخصی کودک سرکشی کند. این اطلاعات شامل؛ نام، تاریخ تولد، نام مدرسه، اطلاعات خانوادگی، اطلاعاتی درخصوص دوستان، اماکن مورد علاقه، علائق و سرگرمی‌های کودکان و اطلاعاتی از این قبیل. زیرا افشا ساختن و علنی نمودن چنین اطلاعاتی در اینترنت، کودک را در معرض تهدید و خطرات بسیاری قرار خواهد داد.

● خطری که بالاتر از همه کودک را تهدید می‌کند اتصال نامحدود به اینترنت بدون برنامه‌ریزی و کنترل است. این روند استفاده، زمان با ارزش کودکان را به هدر می‌دهد. زمانی که می‌بایست صرف انجام تکالیف مدرسه یا آموزش کارهای هنری، ورزشی و یا صرف سایر موارد ارزشمند آموزشی شود. مواردی که می‌تواند تضمینی برای رشد سازنده و موفقیت‌های آینده کودک در جامعه انسانی باشد. در غیر این صورت آینده او به مخاطره خواهد افتاد.

به همین منظور والدین باید به نظارت کامل کودکان خود که بی رویه از اینترنت استفاده می‌کنند، اقدام کنند. از آنجایی که والدین بهتر از هرکسی با خصوصیات اخلاقی و روحی کودکان خود آشنایی دارند. می‌بایست با رفتاری شایسته، سنجیده و حساب شده به گونه‌ای عمل کنند که احساسات آنان را جریحه‌دار نکرده و دوم اینکه باعث تحریک و کشش پنهانی آنها به سوی این کار نشوند.

● زمانی که کودک شما به سرعت صفحات اینترنتی را تغییر داده یا به هنگام ورود شما به اتاق، مانیتور کامپیوتر را خاموش می‌کند، احتمالاً درحال مشاهده تصویر یا مطلبی است که تمایل ندارد شما از آن آگاهی یابید. در این زمان شما باید درکمال خونسردی از او بخواهید تا شما را در تماشای مانیتور کامپیوتر خود شریک کند. و پس از تماشای صفحه مانیتور او اگر چنانچه با محتوا و مضمون نامناسبی برخورد کردید، می‌بایست با رفتاری کاملاً شایسته وی را از خطرات ادامه این کار آگاه ساخته و به صورت صریح از او بخواهید که از انجام آن خودداری کند.

● هیچ‌گاه بدون دادن آگاهی و توضیح لازم در مورد کار اشتباه کودک، او را از انجام آن (تماشا یا مشارکت در سایت‌های نامناسب) سرزنش و منع نکنید. زیرا نتیجه مطلوبی به دست نخواهید آورد.

● تماس‌های تلفنی افراد غریبه و مشکوک با کودک خود را می‌توانید از طریق نمایشگر شماره تلفن (ID Caller) بر روی

دستگاه تلفن منزل کنترل و شناسایی کنید. از کودک خود بخواهید در خصوص شماره‌های ناشناس به شما توضیح دهد.

- زمانی که کودک در نیمه‌های شب از جا برخاسته و پشت کامپیوتر خود اقدام به چت (گفت و گوی اینترنتی) می‌کند، می‌بایست صریحاً به او گوشزد کنید که هر کاری زمان خود را دارد.
- والدین و سرپرستان وظیفه دارند هنگام کار کودک با کامپیوتر بر آنها نظارت و کنترل کامل داشته باشند. آنها باید زمان‌ها و سایت‌های مورد استفاده کودکان را هوشیارانه زیر نظر داشته و کنترل کنند.
- اگر احساس می‌کنید که کارهای کودک شما غیرعادی شده و یا با دوستانش قطع ارتباط کرده است. باید سعی کنید تا با دوستان او صحبت کرده و علت آن را جویا شوید. یا اگر بر عکس، دیدار دوستان کودک شما تنها به دلیل تجمع برای مشاهده منابع نامناسب اینترنتی است، باید در این صورت مراقب باشید. البته در این مراقبت نباید زیاده‌روی کنید. چرا که افراط در این کار نوعی محدودیت و دخالت در حریم خصوصی کودک است که به احساس عدم اعتماد و تیره شدن روابط با کودک منجر خواهد شد. در صورتی که باید به حریم خصوصی کودکان احترام گذارده و هوشیارانه و با درایت کارهای او را نظارت و کنترل کرد.

دلایلی برای نگرانی والدین

نشانه‌های بسیاری در خصوص تغییر رفتار کودک وجود دارد که شما به عنوان والدین باید از آنها آگاه باشید. عصبانی نشوید و بدون تحقیق تهمت نزنید. زیرا این رفتارها نه تنها کمکی به رفع مشکل شما نخواهد کرد، بلکه آن را بدتر هم خواهد کرد. به عنوان والدین و سرپرست کودک وظیفه شماست که خونسردی خود را حفظ کرده و مدبرانه درصدد شناسایی مشکل و راه‌حل آن باشید.

مواردی که باید والدین و سرپرستان کودک را نگران و هوشیار کند، شامل:

- ۱- اگر کودک شما لباس نامتعارفی به تن می‌کند یا اینکه پول و هدایایی دریافت می‌کند که توجیهی ندارد، این امر باید والدین را نگران کند. زیرا افرادی که اغلب به دنبال آزار و سوءاستفاده جنسی از کودکان می‌باشند، مبالغه‌گفتی را برای برقراری رابطه دوستی با کودکان و جلب اعتماد و اطمینان آنان صرف می‌کنند. استفاده نامحدود کودک یا نوجوان از خدمات اینترنتی به‌ویژه در نیمه‌های شب، دلیل دیگری برای نگرانی و هوشیاری والدین است.
- ۲- اگر کودک شما به مدت طولانی از دوستان و خانواده خود کناره گرفته، به‌ویژه در مدت زمانی که از اینترنت استفاده می‌کند، منزوی شده است، باید توجه بیشتری به او و کارهایش نشان دهید.
- ۳- کودک آزاران و افراد متجاوز که کودکان را هدف قرار می‌دهند به شدت به دنبال ایجاد اختلاف و شکاف میان کودک و حامیان آنان (والدین یا سرپرستان) هستند. بزرگ‌ترین شکاف میان کودکان و خانواده‌ها، در زمان برقراری رابطه آنان با این افراد متجاوز بروز می‌کند.

- ۴- در حال حاضر خدماتی نظیر برنامه‌های فیلترینگ و مرورگرهایی که با قابلیت بلوکه کردن انواع سایت‌های نامناسب اینترنتی است، وجود دارند. با کمک آنها می‌توان محتوای سایت‌ها را ارزیابی و یا مسدود کرد. این برنامه‌ها به شیوه‌های مختلفی عمل می‌کنند. بعضی از آنها سایت‌هایی را که از منابع نامناسب برخوردار هستند، بلوکه می‌کنند. بعضی دیگر از ورود و دسترسی کاربران به اطلاعات شخصی نظیر اسم و آدرس، پست الکترونیکی، شماره تلفن و... جلوگیری می‌کنند. برنامه‌های دیگری هم برای جلوگیری از ورود کودکان به اتاق‌های چت (گفت و گوی اینترنتی) و یا ارسال یا خواندن نامه‌های الکترونیکی طراحی شده‌اند. باید خاطر نشان کرد که نصب برنامه‌های فیلترینگ و بلوکه کردن تنها بخشی از طرح امنیتی اینترنت در خانه شما محسوب می‌شود. وجود آنها نباید باعث شود تا شما نگران و مراقب کودک خود نباشید.
- ۵- والدین باید به فایل‌های گرافیکی که کودکان ذخیره می‌کنند، توجه کنند. ممکن است بعضی از آنها حاوی مطالب و عکس‌های نامناسبی باشند (فایل‌هایی که با فرمت tif، bmp، gif، jpg و pcx هستند).
- ۶- در صورت نیاز، باید مطالب، موارد تحریک کننده یا هرگونه فعالیت و اقدامات غیر قانونی که به نحوی سلامت جسمی و روانی کودک شما را تهدید می‌کند را به پلیس گزارش دهید.
- ۷- خلاق باشید، برنامه‌ریزی کنید. زمانی را به گفت و گو و تبادل تجربه‌ها با سایر والدین درخصوص طرز رفتار با کودکان اختصاص دهید.
- ۸- شیوه‌هایی را برای برقراری ارتباط با کودک خود انتخاب کنید که با شناخت از روحیات آنها انتخاب شده باشند. و نیز صبورانه و درایت آنها را اعمال کنید. کودکان و نوجوانان خود را با خطرات اینترنت آگاه و آشنا سازید. هرگز در گفت و گو با کودک خود بی حوصله نباشید و عجله نداشته باشید.
- ۹- با کودکانتان همراه شوید. همراه کودکان از خدمات اینترنتی و برنامه‌هایی که کودکان از آنها استفاده می‌کنند، آشنا شوید. از آنها بخواهید تا طرز کار خود را در اتاق‌های گفت و گوی اینترنتی و یا روش‌های بازی‌های آنلاین را برای شما توضیح دهند. ساعتی را کنار کودکان و فعالیت‌های اینترنتی آنها بگذرانید.
- ۱۰- با کودک خود درخصوص مسائلی که ممکن است در اینترنت با آن مواجه شود، گفتگو کنید. به جای سرزنش کودک به او بیاموزید که ارزش‌های واقعی زندگی در خارج از اینترنت با آنچه که در اینترنت به عنوان ارزش ارائه می‌شود، بسیار متفاوت است.
- ۱۱- استفاده بیش از حد از اینترنت، روند سلامت کودکان را به خطر می‌اندازد. بهتر است کودکان را به انجام فعالیت‌هایی نظیر تمرینات ورزشی، کارهای هنری، موسیقی و... در محیطی خارج از خانه ترغیب و تشویق کنید.
- ۱۲- کامپیوتر را در اتاقی همگانی یعنی اتاقی که می‌توانید ناظر آن باشید، قرار دهید. افراد غریبه را از ورود به اتاق خواب کودک منع نموده و حتی اجازه استفاده آنان از کامپیوتر را ندهید. تنها زمانی که خود در خانه هستید کودکان باید مجاز به استفاده از اینترنت باشد.

۱۳- برای وجود کامپیوتر یا اینترنت در منزل خود متأسف نباشید چراکه کامپیوتر و اینترنت ابزار خارق‌العاده‌ای هستند که قادراند زندگی افراد را متحول سازند. به حس درونی خود اعتماد کرده و مطابق آن رفتار کنید. بهترین کاری که شما می‌توانید انجام دهید محافظت از خانواده‌تان در مقابل استفاده بی‌رویه و غلط آنها از اینترنت و کامپیوتر است. با قبول مسئولیت آن می‌توانید خطرات ناشی از این استفاده را به حداقل برسانید.

۱۴- شما باید الگوی کودکان خود باشید. اگر شما از سایت‌های نامناسب یا نرم‌افزارهای غیر مجاز یا منابع کپی‌رایت شده استفاده کنید، چگونه می‌توانید کودکان خود را از انجام چنین کارهای اشتباهی منع کنید.

۱۵- برای استفاده صحیح از این تکنولوژی بهتر است راهکارهایی را که کارشناسان پیشنهاد می‌کنند، به اجرا درآورید.

رهنمودهایی برای والدین

در این قسمت نکات مهمی را برای والدین و سرپرستان کودک ذکر کرده ایم که با رعایت آنها می‌توانند درصد آسیب‌پذیری کودکان را در این دنیای تکنولوژی مدرن کاهش دهند.

۱- هرگز اطلاعات شناسایی شخصی مانند؛ آدرس محل زندگی، نام مدرسه یا شماره تلفن خود را به افراد غریبه ارائه نکنید.

۲- از خدماتی اینترنتی که کودکان از آنها استفاده می‌کنند، اطلاع حاصل کنید.

۳- نحوه ورود به سیستم کامپیوتر یا شبکه را به‌طور کامل بیاموزید.

۴- از طریقه بلوکه نمودن منابع نامناسب اینترنتی و اطلاعات ارائه‌شده در اینترنت، آگاهی یابید.

۵- هرگز به کودک خود اجازه ترتیب ملاقات اینترنتی را ندهید. اگر ملاقاتی از سوی کودک شما یا دیگر کاربران ترتیب داده شد، باید خود یا فردی برای همراهی کودک در محل ملاقات حضور یابد.

۶- هرگز به پیغام‌های افراد ناشناس پاسخ ندهید.

۷- در برخورد با منابع اینترنتی وسوسه‌آمیز، مستهجن، خشونت‌آمیز، تهدیدآمیز و مطالبی که موجبات ناراحتی شما را فراهم می‌آورند، پاسخی ندهید.

۸- کودکان خود را تشویق کنید در صورت برخورد با چنین مطالبی به شما اطلاع دهند. شما می‌توانید پیام دریافتی را فوراً به نزدیکترین پلیس محل سکونتتان گزارش کرده و از آنها کمک بخواهید.

۹- به وجود افرادی با هویت ناشناس در اینترنت باید توجه کرد. چرا که کاربران اینترنتی غالباً از هویتی نامشخص برخوردارند. یک کاربر اینترنتی می‌تواند خود را دختری ۱۲ ساله معرفی کند در صورتی که یک مرد ۴۰ ساله است.

شما قادر به شناسایی و کسب اطلاعات صحیح از او نخواهید بود. باید بدانید که محتوای مطالب اینترنتی ممکن است، حقیقت نداشته باشند. در چنین محیطی، هرگونه پیشنهادی که به نظر حقیقی می‌رسد، می‌تواند کذب باشد. در نتیجه در

برخورد و پذیرش هرگونه پیشنهادی برای قرار ملاقات با فردی، بسیار محتاط و هوشیار عمل کنید.

۱۰- قوانین و راهکارهای منطقی برای استفاده کودک خود از کامپیوتر وضع کنید. درباره این قوانین با کودک خود وارد بحث و گفتگو شوید. نتیجه گفتگو را در قالب دستورالعملی در محلی نزدیک به کامپیوتر جهت یادآوری بچسبانید. کنترل و نظارت این که آیا کودک شما از قوانین وضع شده هنگام فعالیت با کامپیوتر پیروی می کند یا نه، بسیار ضروری است. تنها وضع کردن قوانین مهم نیست.

نکاتی برای کودکان آنلاین

کودکان و نوجوانان عصر اینترنت هم باید در برخورد با مسائل و مشکلات زندگی در هر کجای دنیا که باشند، بسیار هوشیارانه و قاطعانه عمل کنند. آنها باید از همفکری و همدلی والدین، معلمان و سرپرستان خود بهره جسته تا مسائل و مشکلات روزمره ناشی از این تکنولوژی ارتباطی را به راحتی رفع کنند. از این رو نکاتی برای پیشگیری و آگاهی از مسائل و نحوه استفاده صحیح از این فناوری را ذکر می کنیم.

۱- کلمه رمز استفاده از کامپیوتر و اینترنت، را باید مخفی نگه دارید. از گفتن کلمه رمز به دیگران به جز والدین خود اجتناب ورزید. افشای کلمه رمز به افراد بیگانه، می تواند دردسرساز یا خطرناک باشد. در صورتی که شخصی تماس بگیرد و عنوان نماید که کارمند شرکت ارائه کننده خدمات اینترنتی می باشد و به کلمه عبور شما نیاز دارد. شما باید اول نام، شماره تلفن و آدرس شرکت او را بخواهید و بعد با آن شرکت تماس گرفته و تحقیق کنید که آیا چنین شخصی در آن جا مشغول به کار است؟ و آیا این کارمند اجازه دارد تا کلمات عبور را بخواهد یا خیر؟

۲- با کاربران شبکه اینترنتی همانند افراد خارج از اینترنت مؤدب و با نزاکت رفتار کنید. اگر شخصی گستاخانه یا به منظور خاصی شما را مورد تهدید قرارداد، از پاسخ به او اجتناب کنید. کاربران تهدید کننده در شبکه اینترنتی، درست شبیه به تهدیدکنندگان خارج از اینترنت می خواهند که شما پاسخ آنها را بدهید. شما با عدم پاسخ به آنها می توانید جلوی مقاصد شوم آنها را بگیرید.

۳- هرگز نامه های الکترونیکی افراد ناشناس، غیرعادی و مشکوک را باز نکنید. و آنها را سریعاً پاک کنید. این نامه ها می توانند حاوی کدها، ویروس ها و کرم هایی که بسیار برای سیستم کامپیوتر شما خطرناک است، باشند. اگر به نامه ای مشکوک هستید از والدین یا افراد متخصص بخواهید تا به شما کمک کنند.

۴- هنگام استفاده از اینترنت، اگر با چیزی مواجه شدید که به آن تمایل و رغبتی نداشتید و یا با مطالعه آن احساس ترس و ناراحتی به شما دست می دهد، کامپیوتر را خاموش کرده و درخصوص آن با والدین خود گفتگو کنید.

۵- زمانی را برای استراحت به خود اختصاص دهید. به مدت طولانی از اینترنت استفاده نکنید. زمان خود را بین خانواده، دوستان خارج از اینترنت و سایر فعالیت های مفید تقسیم کنید.

۶- قوانین مربوط به وب سایت های اینترنتی را مطالعه کنید. این قوانین و خط مشی ها مربوط به کاربران سایت های اینترنتی است که توصیه های ویژه ای برای استفاده از سایت ها در آن ارائه شده است. این قوانین را به همراه والدین خود

مطالعه کرده و از آنها بخواهید تا مفاهیم و مضامین قراردادها را برای شما توضیح دهند. این روند به شما و والدیتان برای درک اطلاعاتی در خصوص امنیت اینترنت کمک می‌کند.

۷- از کپی کردن غیر مجاز اجتناب کنید. کپی کردن برای استفاده از سایت‌های اینترنتی زمانی مجاز است که از سوی مدیر شبکه مجوز این کار را داشته باشید.

۸- از خود محافظت کنید. هرگز با شخصی که در اینترنت ارتباط برقرار کرده‌اید، قرار ملاقات نگذارید. اگر قصد ملاقات با آنها را دارید، در یک محل عمومی و همراه با والدین خود بر سر قرار حاضر شوید.

۹- زمانی را برای آموزش والدین خود در خصوص فعالیت‌های شبکه اینترنتی اختصاص دهید. به آنها سایت‌های مورد علاقه خود را نشان دهید و اجازه دهید تا در لحظه استفاده از اینترنت در کنار شما باشند. آنها را در فعالیت‌های اینترنتی خود شرکت دهید. این کار به آنها احساس رضایت و اطمینان از امنیت شما می‌دهد.

۱۰- مراقب کامپیوتر خود باشید. بعضی از سایت‌ها که کیت‌های ویروس را ارائه می‌کنند، می‌توانند با ارسال یک ویروس کامپیوتر شما را مختل کنند. هرگز از این سایت‌ها بازدید نکنید. دوستان خود را نیز از انجام چنین کاری آگاه سازید.

حفظ امنیت اینترنتی با رعایت قوانین

قوانین و مقررات در همه جای دنیا برای حفظ امنیت و آرامش حافظان آن وضع شده است. از این رو، برای حفظ امنیت و آرامش کاربران اینترنت هم قوانین و مقرراتی وضع شده که با رعایت و توجه به آن تا حدودی مسائل و مشکلات کاربران کاهش می‌یابد. قوانینی که شما را در موارد زیر متعهد می‌سازد:

● من هرگز بدون اجازه اطلاعات شخصی خود را از قبیل آدرس، شماره تلفن، آدرس محل کار والدین و شماره تلفن محل کار، عکس، اسم و آدرس مدرسه‌ام را در دسترس دیگران قرار نخواهم داد.

● اگر با اطلاعاتی روبرو شدم که موجب آزار من شود، بلافاصله به والدینم اطلاع خواهم داد. تقصیر من نیست که چنین اطلاعاتی دریافت کرده‌ام.

● هرگز با شخصی که در اینترنت با او آشنا شده‌ام، بدون آگاهی و تحقیق والدینم ملاقات نخواهم کرد. در صورت موافقت و همراهی آنها بر سر قرار حاضر خواهم شد.

با والدینم در خصوص وضع قوانینی برای استفاده از اینترنت صحبت خواهم کرد. تعیین مدت زمانی که می‌توانم در طول روز از اینترنت استفاده کنم و نیز در مورد سایت‌های مناسب و سالم که می‌توانم مشاهده کنم، تصمیم‌گیری خواهیم کرد.

منبع:

:Protecting Children from internet By Asian School of cyber Laws

<http://www.asianlaws.org/fact>

خلاصه فصل

در حالی که بسیاری فناوری اطلاعات و ارتباطات را باعث تسهیل در امر انتقال اطلاعات می‌دانند، اما موضوع امنیت در تبادل اطلاعات همواره به عنوان یکی از اصول غافل مانده به شکل یک معضل پنهان باقی می‌ماند. تاکنون مهم ترین سرویس از میان سرویس‌های گوناگون اینترنت، سیستم پست الکترونیکی بوده است. پست الکترونیکی امروزه در تجارت و بانکداری الکترونیکی هم کاربرد فراوانی دارد و بسیاری از تعیین هویت‌های مجازی امروزه توسط پست الکترونیک صورت می‌گیرد. کاربران آگاه اینترنت می‌دانند که معمولاً سایت‌هایی معتبر هستند که دارای Domain رسمی با درج شماره‌های تماس مدیر و توضیحاتی در مورد مؤسسان سایت، صفحات درباره ما، تماس با ما و غیره هستند. فناوری‌های جدید، جرائم جدید به همراه می‌آورد. رایانه و اینترنت یک فناوری جدید است. مانند هر فناوری دیگری تا زمانی که استفاده از رایانه و اینترنت عمومیت پیدا نکرده بود، هیچ پیش فرضی درباره مزایا و مخاطرات احتمالی آن وجود نداشت.

جرائم اینترنتی تنها محدود به کلاهبرداری نمی‌شوند. انتشار اخبار کذب، افترا، آزار و اذیت، سوء استفاده از پست الکترونیک، ارسال مطالب و تصاویر و فیلم‌های مستهجن، هتک حرمت افراد با پخش مطلب یا تصاویر آنها، تلاش برای به انحراف کشاندن و سوء استفاده از کودکان، نقض حق مالکیت مادی و معنوی افراد، هک کردن و ویروسی کردن سایت‌ها از جمله جرائم دیگر اینترنتی محسوب می‌شوند.

ویروس‌های رایانه‌ای برنامه‌هایی هستند که مشابه ویروس‌های بیولوژیک گسترش یافته و پس از وارد شدن به رایانه اقدامات غیرمنتظره‌ای را انجام می‌دهند. انواع برنامه‌های مخرب عبارتند از ویروس، کرم، تروجان و کدهای جاسوس. یکی از مهم ترین روش‌های مقابله با برنامه‌های مخرب پیشگیری از انتقال آن به رایانه است، لذا باید روش‌های انتقال آنها را فرا گرفت و اقدامات پیشگیرانه لازم را انجام داد. ضد ویروس (آنتی ویروس) اصطلاحی است که به برنامه یا مجموعه‌ای از برنامه‌ها اطلاق می‌شود که برای محافظت از رایانه‌ها در برابر ویروس‌ها استفاده می‌شوند. وظیفه اصلی این برنامه‌ها شناسایی پرونده‌های آلوده به ویروس و پاک‌سازی آنهاست.

در مبادلات و معاملات آنلاین احتمال نادیده انگاشتن جوانب امنیتی و عدم رعایت آن، فقط کمی بیشتر از داد و ستدهای حضوری ست. پروتکل‌های امنیتی قوانین و استانداردهایی هستند که برای محافظت از مبادلات و معاملات اینترنتی در برابر تهدیدهای آنلاین، وضع شده‌اند و دسترسی‌های غیرمجاز به اطلاعات تبادل شده را محدود می‌کنند.

بانکداری الکترونیک شامل سیستم‌هایی است که مشتریان مؤسسات مالی را قادر می‌سازد تا در سه سطح اطلاع رسانی، ارتباط و تراکنش از خدمات و سرویس‌های بانکی استفاده کنند. کاربران خدمات اینترنتی باید بدانند که امنیت اطلاعات هم در طرف خدمات دهنده و هم در طرف خدمات گیرنده، باید به طور کامل تأمین باشد و صرف ارائه خدمات امن

از طرف بانک، امنیت اطلاعات مالی اعتباری کاربر یا خدمات گیرنده را تضمین نمی کند و محیط عملیاتی او نیز باید کاملاً حفاظت شده و عاری از تهدیدهای رایانه ای باشد.

ابزارهای فناوری جدید که ممکن است، فرزندان ما را تهدید کند، عبارت است از: اینترنت، بازی های رایانه ای و تلفن همراه.

فعالیت کارگاهی

- ۱- از طریق اینترنت تحقیق کنید آیا بانک صددردصد اینترنتی در ایران وجود دارد یا خیر؟
- ۲- یک بانک صددردصد اینترنتی در شبکه اینترنت پیدا کنید و خدمات آن را بررسی نمایید.
- ۳- چه بانک هایی در ایران خدمات اینترنتی ارائه می دهند؟ این خدمات شامل چه فعالیت هایی می باشند؟ سه نمونه را بیان نمایید.
- ۴- به سایت کتابفروشی «انتشارات نص» مراجعه کنید و روش های خرید اینترنتی آن را بررسی نمایید.
- ۵- به پوشه Spam حساب پست الکترونیکی خود بروید و کاری کنید که دیگر از آن آدرس های فرستنده، برای شما ایمیلی ارسال نشود.
- ۶- چند نرم افزار در رابطه با کنترل والدین در اینترنت پیدا کرده و خصوصیات آنها را با یکدیگر مقایسه کنید.
- ۷- چه راهکارهای عملی بر روی رایانه برای کنترل و نظارت والدین وجود دارد؟ آنها را بررسی نمایید.
- ۸- نرم افزار ضدویروس رایانه خود را بررسی نمایید. آیا می توانید از طریق اینترنت آن را به روز نمایید؟

خودآزمایی

- ۱- سایت‌های معتبر چه مشخصه‌هایی دارند؟
- ۲- ویروس چیست و چه تفاوتی با کرم و تروجان دارد؟
- ۳- عملکرد ویروس‌ها در رایانه بر چه اهدافی استوار است؟
- ۴- علائم وجود ویروس در رایانه چیست؟
- ۵- سه مورد از نحوه مقابله با ویروس‌ها را توضیح دهید.
- ۶- چرا هدف اصلی تبهکاران آنلاین کاربر نهایی می‌باشد؟
- ۷- پروتکل امنیتی SSL چیست؟
- ۸- چه روش‌های خریدی برای خرید اینترنتی وجود دارد؟ کدام مناسب‌تر است؟
- ۹- مزایای بانک‌های صدورصد اینترنتی چیست؟
- ۱۰- ابزارهای فناوری‌های جدید چگونه فرزندان ما را تهدید می‌کنند؟