فصل ۷ ارتباط امن

هدف های رفتاری

پس از آموزش این فصل، هنرجو می تواند

۱-خطرات و مشکلات پیام های ناشناس را شناسایی کند.

۲-هویت مجازی را توضیح دهد.

۳-جرائم مختلف در فضای اینترنت را بیان کند.

۴-با ویروس های اینترنتی مقابله نماید.

۵-انواع برنامه های مخرب را بشناسد.

۶-با برنامه های ضد ویروس کار کند.

۷-ملزومات امنیتی در اینترنت را بشناسد.

۸-به شکل امن در تجارت الکترونیک شرکت نماید.

۹-حقوق مصرف کنندگان در اینترنت را توضیح دهد.

۱۰-دلایل کنترل والدین را توضیح دهد.

۱-۷- مقدمه

اینترنت، یک شبکه عظیم اطلاع رسانی و یک بانک وسیع اطلاعاتی است که در آینده نزدیک دسترسی به آن برای تک تک افراد ممکن خواهد شد.کارشناسان ارتباطات، بهره گیری از این شبکه را یک ضرورت در عصر اطلاعات می دانند .این شبکه که از هزاران شبکه کوچکتر تشکیل شده، فارغ از مرزهای جغرافیایی، سراسر جهان را به هم مرتبط ساخته است. طبق آخرین آمار بیش از شصت میلیون رایانه از تمام نقاط جهان در این شبکه گسترده به یکدیگر متصل شده اند که اطلاعات بی شماری را در تمامی زمینه ها از هر سنخ و نوعی به اشتراک گذاشته اند. گفته می شود نزدیک به یک میلیارد صفحه اطلاعات با موضوعات گوناگون از سوی افراد حقیقی و حقوقی روی این شبکه قرار داده شده است. این اطلاعات با سرعت تمام در بزرگراه های اطلاعاتی بین کاربران رد و بدل می شود و تقریباً هیچ گونه محدودیت و کنترلی بر وارد کردن یا دریافت کردن داده ها اعمال نمی شود. حمایت از جریان آزاد اطلاعات، گسترش روزافزون فنآوری اطلاعات و بسترسازی برای اتصال به شبکه های اطلاع رسانی، شعار دولتهاست. این در حالی است که گستردگی و تنوع اطلاعات آلوده روی اینترنت، موجب بروز نگرانی در بین کشورهای مختلف شده است. انتشار تصاویر مستهجن، ایجاد پایگاه هایی با مضامین پورنوگرافی و سایتهای سوءاستفاده از کودکان و انواع قاچاق در کشورهای پیشرفته صنعتی، بخصوص در خاستگاه این شبکه جهانی یعنی آمریکا، کارشناسان اجتماعی را بشدت نگران کرده، به گونه ای که هیأت حاکمه را مجبور به تصویب قوانینی مبنی بر کنترل این شبکه در سطح آمریکا نموده است. هشدار، جریمه و بازداشت برای برپاکنندگان پایگاههای مخرب و فسادانگیز تدابیری است که کشورهای مختلف جهان برای مقابله با آثار سوء اینترنت اتخاذ کرده اند. ترس و بیم از تخریب مبانی اخلاقی و اجتماعی، ناشی از هجوم اطلاعات آلوده و مخرب از طریق اینترنت، واکنشی منطقی است، زیرا هر جامعه ای چارچوب های اطلاعاتی خاص خود را دارد و طبیعی است که هر نوع اطلاعاتی که این حد و مرزها را بشکند می تواند سلامت و امنیت جامعه را به خطر اندازد. علی رغم وجود جنبه ی مثبت شبکه های جهانی، سوء استفاده از این شبکه های رایانه ای توسط افراد بزهکار، امنیت ملی را در

کشورهای مختلف با خطر روبرو ساخته است. از این رو بکارگیری فیلترها و فایروال های مختلف برای پیشگیری از نفوذ داده های مخرب و مضر و گزینش اطلاعات سالم در این شبکه ها رو به افزایش است. خوشبختانه با وجود هیاهوی بسیاری که شبکه اینترنت را غیرقابل کنترل معرفی می کند، فناوری لازم برای کنترل این شبکه و انتخاب اطلاعات سالم روبه گسترش و تکامل می باشد.

۷-۲

خطرات و مشکلات پیغام های ناشناس

پیام های 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 ضربه ای سنگین بر سیستم و یا به اطلاعات موجود در آن می شود که در واقع می توان گفت رویکرد دیرهنگامی است. اینترنت همواره از جهت های گوناگون مورد نقد و ارزیابی قرار می گیرد، اما واقعیت این است که این شبکه عظیم مانند هر اجتماع عادی انسانی دیگر در معرض تهدیدها و خطرات قرار دارد. از نفوذ داده های مخرب گرفته تا تخریب داده های سالم و برهم زدن نظم شبکه همه و همه تنها به یک مورد بستگی دارد و آن بحث امنیت اطلاعات در محیط اینترنت است. امروزه امنیت اطلاعات در زمینه اینترنت از یک بحث حاشیه ای به یک بحث ضروری تغییر جهت داده است. هرگونه خرید و فروش روی اینترنت و یا انتقال داده ها باید تحت یک کنترل امنیتی صورت گیرد. اگر امنیت شبکه برقرار نگردد، مزیت های فراوان آن نیز به خوبی حاصل نخواهد شد و پول و تجارت الکترونیک، خدمات به کاربران خاص، اطلاعات شخصی، اطلاعاتی عمومی و نشریات الکترونیک همه و همه در معرض دستکاری و سوءاستفاده های مادی و معنوی قرار می گیرند. همچنین دستکاری اطلاعات- به عنوان زیربنای فکری ملت ها - توسط گروه های سازماندهی شده بین المللی، به نوعی مختل ساختن امنیت ملی و تهاجم علیه دولت ها و تهدیدی ملی محسوب می شود. در ایران که بسیاری از نرم افزارهای پایه از قبیل سیستم عامل و نرم افزارهای کاربردی و اینترنتی، از طریق واسطه ها و شرکت های خارجی تهیه می شود، بیم نفوذ از طریق راه های مخفی وجود دارد. هم اکنون نیز بانک ها و بسیاری از نهادها و دستگاه های دیگر از طریق شبکه به فعالیت می پردازند، به همین دلیل جلوگیری از نفوذ عوامل

مخرب در شبکه به صورت مسئله ای استراتژیک درآمده که نپرداختن به آن باعث ایراد خساراتی خواهد شد. تجربیاتی نیز در همین زمینه وجود دارد که این موضوع را کاملاً ثابت کرده است.

هویت مجازی

به رغم معرفی سرویس های متعدد روی شبکه، تاکنون مهمترین سرویس از میان سرویس های 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 پیام های رد و بدل شده بین کاربران حاوی یادداشت های شخصی است. گرچه اغلب پیام ها از متن ساده تشکیل شده اند، اما امکان پست الکترونیکی تمام انواع داده ها، مثل تصاویر، برنامه های 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 و در واقع، فردی با فرد دیگری که هزاران کیلومتر از او دور است و هیچ وقت او را ندیده است، می تواند ارتباط داشته باشد. پست الکترونیکی امروزه در تجارت و بانکداری الکترونیکی هم کاربرد فراوانی دارد و بسیاری از تعیین هویت های مجازی امروزه توسط پست الکترونیک صورت می گیرد. در همین رابطه برای استفاده امن از پست الکترونیکی تذکراتی وجود دارد. درک تفاوت های پست الکترونیکی با پست عادی و یا گفت وگوی تلفنی کمی دشوار است، ولی به کار بستن برخی نکات ساده می تواند در بالا بردن امنیت هنگام به کارگیری این سرویس مؤثر باشد از جمله این موارد می توان از موارد زیر را نام برد:

بایستی همواره تصور شود که هیچ گونه اختفایی وجود ندارد. پیام هایی که به دلایلی نباید همه ببینند نباید از این طریق ارسال شود، بنابراین از ارسال نامه های بسیار خصوصی، سخنرانی های تند، بی احترامی های منظوردار و... باید احتراز شود. نباید فرض شود که پیام های حذف شده قابل بازیابی نیستند. چنانچه پیامی حذف شود، احتمالاً در نسخه های پشتیبان که شب یا روز قبل تهیه شده است موجود است. در این سیستم ابزار مشابه کاغذ خردکن وجود ندارد. در متن های ارسالی باید محتاط بود. این طبیعت پست الکترونیکی است که مردم پیام های دریافتی خود را بیشتر از پیام های ارسالی جدی می گیرند. ضمن اینکه ارسال یادداشت سریع به هر جایی از جهان بسیار ساده است.

نگاهی به کشور ایران

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

عناوینی مانند :

❊ کنجکاوی کنید!

❊ سلام من منتظرم !

❊ شما برنده شده اید!

❊ این ایمیل را ببین!

❊ آیا می خواهید 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!

موضوعات دسته دیگری از ایمیل های مزاحم نیز کم اهمیت و نامناسب است :

❊ پر فروش ترین فیلم سال

❊ فروش ویژه اقساطی !

❊ ارزان سرای ما!

❊ فرصت رو از دست نده

❊ بشتابید !

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

در تعالیم دینی ما مسلمانان، ایجاد مزاحمت با هر روشی، امری ناپسند است. مضافاً اینکه فریبکاری و دروغ به بهانه تبلیغ، توجیهی ندارد. باید دانست که ارسال هزاران ایمیل با عبارات و محتوای نامناسب که مشخص نیست رویت کننده آن در چه سنی، با چه جنسیتی و با کدام فرهنگ و تحصیلات می باشد، صحیح نمی باشد. اگر این نوع ایمیل ها به عنوان مثال توسط یک دانش آموز باز شده و موجب ایجاد سوال و تعجب برای او گردد، ممکن است وی برای یافتن پاسخ سئوال

خود، که امری ضروری نیست، به دوستان، وبلاگ ها 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 پیام ها امری ناپسند می باشد. اما لینک های فریبنده در برخی وبلاگ هایی که از سوی فارسی زبانان داخل کشور معمولاً با مقاصد مادی ساخته می شود، مشکلات و خطراتی را مخصوصاً برای خانواده ها که دارای فرزندان دوره های ابتدایی تا دبیرستان می باشند، به وجود آورده است. در این رابطه هشدار معلمان و اولیای آموزشی نیز به گوش می رسدکه مراقب استفاده کودکان و نوجوانان خود از اینترنت باشید.

اما کاربران آگاه اینترنت می دانند که معمولاً سایتهایی معتبر هستند که دارای Domain رسمی با درج شماره های تماس مدیر و توضیحاتی در مورد موسسان سایت، صفحات درباره ما ، تماس با ما و غیره هستند. به عبارت دیگر، آنها سایت هایی بسیار معتبر هستند که به صورت زیر زمینی به فعالیت نپرداخته و دارای مطالبی هستند که تمام جوانب احتیاط برای بازدید کننده ها اعم از کودک و نوجوان تا بزرگسال را در نظر گرفته و مطالب نامناسب ندارند. با این توصیف برخی افراد سود جو از راه زیرکانه ای وارد شده و می خواهند طی چند مرحله و چندین کلیک، بازدید کننده بیشتری را به داخل سایت مورد نظر خود بکشانند و معمولاً از روشهای فریبکارانه برای مقاصد خود استفاده می کنند، این دسته سایت ها به نوعی با منافع مالی و فروش اجناس سروکار دارند. سیستم کلیک پولی هم بر این مشکل می افزاید. اما سایتهای معتبر از این نوع تبلیغات فریبکارانه(تکدی گری اینترنتی!) بی نیاز هستند و معمولاً با صداقت در موتورهای جستجو جایی برای خود باز کرده و بازدید کننده به صورت آگاهانه به سایتشان وارد می شود.

در برخی وبلاگ ها 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 می یابد تا بلکه بار دیگر وارد آن آدرس شده و شاید خرید داشته باشید و معمولاً این نوع کارها در سایتهای معتبر و مفید، رخ نمی دهد و این اعمال بدون اجازه شما، توسط وبلاگ های وابسته بدون نام و نشان سازنده ، به سایت اصلی انجام می شود.

از دیگر اعمال ناپسند در اینترنت و در سایت و وبلاگهای فارسی ، که گاهاً موتور های جستجو و بازدیدکنندگان را فریب می دهند، 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 می کنند!

آسیب دیگر اینترنت در کشور، کپی برداری وبلاگ ها و برخی سایت ها 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 کپی برداری کرده و به نام خود در وبلاگ یا سایتش استفاده کرده و امانت داری را رعایت نمی کنند.

در مواجهه با موارد بالا یا نظایر آن پیشنهاد می گردد:

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

۲–از ثبت ایمیل خود در صفحات غیر ضروری وبلاگ و سایتها خود داری نمایید.

۳–اگر مجبورید ایمیل خود را در یک صفحه اینترنتی ثبت نمایید، پیشنهاد می گردد در صورت امکان آن را به صورت یک عکس کم حجم در معرض دید دیگران قرار دهید .

۴–به هیچ وجه روی لینکها و ایمیل ها با عناوین فریبنده و غیر واقعی و ناشناس کلیک نکنید.

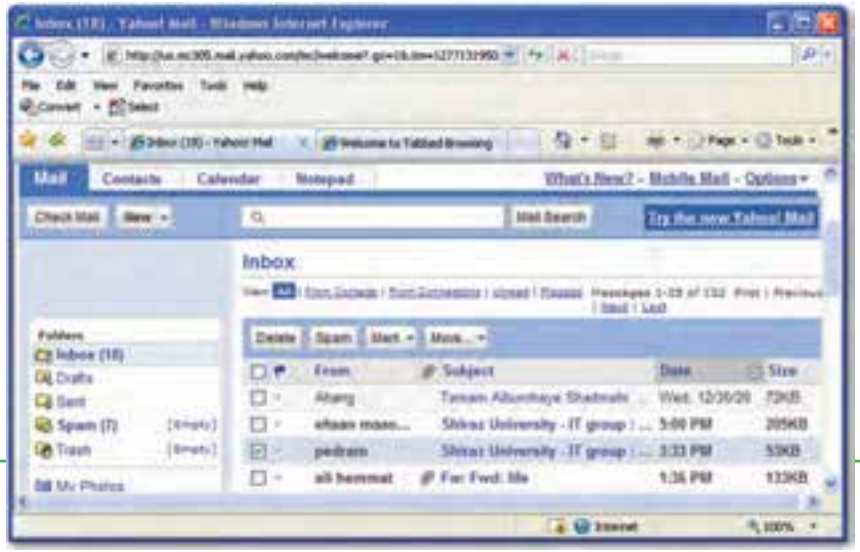
۵–هرگز به یک ایمیل ناخواسته و مشکوک پاسخ ندهید، زیرا اینکار باعث خواهد شد که در آینده پیام های ناخواسته بیشتری برای شما ارسال شود.

۶–در خیلی از موارد لازم است والدین و بزرگترها برگشت و گذار کودکان و نوجوانان در اینترنت نظارت داشته باشند، توصیه می شود علی الخصوص کودکان را در استفاده بی قید و بند از اینترنت، آزاد نگذارید .

۷–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.

۸–و مهمتر از همه : «روی هر لینکی کلیک نکنید».

۹–با تعیین یک آدرس یا ایمیل دریافتی به عنوان هرزنامه، می توانید سرویس دهنده ی پست الکترونیکی خود را برای موارد بعدی آگاه نمایید. (شکل ۱–۷)



شکل ۱–۷ تعیین آدرس یا یک ایمیل دریافتی به عنوان هرزنامه

برخی جرائم در فضای اینترنت

در گفتگو های 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!(در حالی که آن یک Spam بوده و برای هزاران نفر ارسال شده است)

❊ فردی چون ساعتهای 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:

«من یک سرمایه دار گینه ای هستم. در کشور من به خاطر جنگ هایی که در جریان است سرمایه گذاری ممکن نیست. به همین خاطر دنبال کسی می گردم که سرمایه ام را که ۲۰ میلیون دلار است به دست او بسپارم تا در کشورش سرمایه گذاری کند. در صورتی که مایلید این پول را دریافت کنید با من تماس بگیرید».

این متن به طور خلاصه محتوای ایمیلی است که یک شهروند دریافت کرد. او به شدت تحت تاثیر این ایمیل قرار گرفت. به ویژه این که نامه و سرگذشت «مرد گینه ای»کاملاً واقعی به نظر می رسید. او فکر می کرد که با ۲۰ میلیون دلار قادر است سرمایه گذاری های بزرگی انجام دهد. اما از طرفی به صحت این ادعا شک داشت. بنابراین از طریق ایمیل با کسی که نامه الکترونیکی را فرستاده بود تماس گرفت و از او خواست اطلاعات بیشتری در اختیارش قرار دهد. جواب تقریباً تکرار همان حرف ها بود. تنها چیزی که اضافه شده بود درباره نحوه انتقال پول بود. مردی که ادعا می کرد یک سرمایه دار گینه ای است می خواست که این شهروند مشخصات و شماره حسابی در اختیارش قرار دهد و خودش نیز شماره تلفنی در اختیارش قرار داده بود. به نظر این شهروند، دادن شماره حساب اندکی بی احتیاطی بود، ضمن این که چند نفر به او گفتند که این قبیل افراد کلاهبردارند. وقتی این شهروند بیشتر تحقیق کرد متوجه شد که این یک روش کلاهبرداری است که اینک شهروندان غربی که دسترسی زیادی به اینترنت دارند کاملاً با آن آشنا هستند و در نتیجه کلاهبرداران پیکان خود را به سوی کشورهای کمتر توسعه یافته برگردانده اند.

مثال دیگر: 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 آن جایی 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 ازایش 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 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 می کند و فرستندگان پیام نیز به محض دریافت پاسخ مثبت از سوی کاربر با ارسال مدارکی جعلی در پی القای این موضوع برمی آیند که گیرنده پیام دریکی از بانک های معتبر بین المللی برنده شده است. در مرحله بعدی از کاربران درخواست افتتاح حساب و واریز مبالغی به آن حساب ها به عنوان هزینه جابه جایی مبالغ برنده شده می شود و از سوی ارسال کنندگان پیام اعلام می گردد که هزینه جابه جایی پول برعهده فرد برنده شده بوده و شرکت در این مورد هزینه ای را متقبل نمی شود.

به عنوان نمونه دیگر، برخی از کلاهبرداران از طریق ارتباط با افراد ابراز می کنند وارث پدری هستند که پول زیادی در حساب وی وجود دارد و از فرد می خواهند با ادعای شراکت با پدر فوت شده، اقدام به دریافت پول از بانک کرده و بخشی از این پول را به عنوان حق الزحمه دریافت نماید. در نوع دیگری از این کلاهبرداری ها، افراد ازکاربران درخواست حمل پول به کشوری ثالث به قصد پولشویی و دریافت حق الزحمه می کنند. پس از پیگیری های پلیس به دلیل جعلی بودن آدرس ها و مدارک و همچنین اجاره ای بودن خطوط تلفن امکان ردیابی بسیار سخت می شود.

البته جرائم اینترنتی تنها محدود به کلاهبرداری نمی شوند. انتشار اخبار کذب، افترا، آزار و اذیت، سوء استفاده از پست الکترونیک، ارسال مطالب و تصاویر و فیلم های 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 سایت ها از جمله جرائم دیگر اینترنتی محسوب می شوند. ظاهراً هنوز آمار دقیقی در زمینه میزان جرائم اینترنتی در کشور وجود ندارد. اما گفته می شود 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 فناوری هایی 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 می کنند 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 اطلاع رسانی کنیم و بویژه در این زمینه قوانین محکمی تدوین کنیم. طبیعی است که کلاهبرداری اینترنتی با کلاهبرداری سنتی متفاوت است و قوانین مناسب خود را می خواهد 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 می شود، لازم است حفظ احترام افراد و اعاده حیثیت آنها و مجازات مجرمان را دنبال کند. طبیعی است که هرقدر فناوری توسعه می یابد هم امکان به وجود آمدن جرائم بیشتر می شود و هم امکان کنترل همان جرائم به وجود می آید. مانند تلفن که عده ای برای مزاحمت و تهدید دیگران نیز از آن استفاده می کردند، 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.

۷-۳

مقابله با ویروس ها

چگونه می توانم رایانه ام را در مقابل ویروس های اینترنتی ایمن نمایم؟

ویروسهای رایانه‌ای برنامه هایی هستند که مشابه ویروسهای بیولوژیک گسترش یافته و پس از وارد شدن به رایانه اقدامات غیرمنتظره ای را انجام می دهند. با وجودی که همه ویروسها خطرناک نیستند، ولی جزئی از برنامه های مخرب هستند که در بیشتر موارد برای تخریب یا تغییر انواع مشخصی از پرونده‌ها، برنامه های کاربردی ، سیستمهای عامل یا سوء استفاده از آنها نوشته می شوند. ویروسها هم مشابه همه برنامه های دیگر از منابع سیستم مانند حافظه و فضای دیسک سخت، توان پردازنده و سایر منابع بهره می گیرند و می‌توانند اعمال خطرناکی را انجام دهند. در این بخش

انواع برنامه های مخرب شامل ویروس، کرم، تروجان و کدهای مخرب مورد بررسی قرار خواهد گرفت.

عملکرد ویروسها

تخریب : ویروس ها در ابتدا با همین هدف نوشته و توزیع می شد 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 پرونده ها 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 ویروس های مخرب، ویروس هایی شیوع پیدا کرد که به شبکه ها و اطلاعات ارزشمند و یا غیر ارزشمند دسترسی پیدا می کردند. فرض کنید فردی به شبکه بانک های شهر ویروس ارسال می‌کند و میخواهد اطلاعات حساب های بانکی را دریافت کرده و دست کاری یا از آنها سوء استفاده کند.

کسب درآمد: می توان مواردی را مشخص کرد که فردی ویروسی را آماده می‌کند، پس از توزیع در شبکه ها، به شرکتهایی که نرم افزار ضدویروس را مینویسند، میفروشد و یا اینکه شرکت ها راساً 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 ویروس ها برای اعمال مجرمانه، جرم محسوب می‌شود و مورد پیگرد قانونی قرار می گیرد.

انواع برنامه های مخرب

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

کرم : یک کرم، برنامه نرم افزاری کوچکی است که با استفاده از شبکه های رایانه‌ی و اشکالات برنامه ای (حفره های امنیتی موجود)، اقدام به تکثیر خود می‌کنند و با تکثیر بیش از حد خود، عملاً سیستم‌ها را از کار می‌اندازند. نسخه ای از «کرم»، شبکه را پیمایش تا ماشینهای دیگر موجود در شبکه را که دارای حفره های امنیتی هستند، تشخیص و نسخهای از خود را تکثیر کنند. کرمها با استفاده از حفره های امنیتی موجود، نسخهای از خود را بر روی ماشینهای جدید تکثیر می‌کنند.

با استفاده از شبکه های رایانه‌ای، کرمها قادر به تکثیر باورنکردنی خود در اسرع زمان می‌باشند. مثلا کرم «Code Red»، که در سال ۲۰۰۱ مطرح گردید، قادر به تکثیر خود به میزان ۲۵۰۰۰۰ مرتبه در مدت زمان ۹ ساعت بود. کرمها می توانند منابع رایانه ای و شبکه ای مانند زمان پردازنده، حافظه یا تمام یا قسمتی از امکانات شبکه را در اختیار خود بگیرند.

تروجان : تروجان یا اسب تراوا، نوع خاصی از برنامه های مخرب هستند. برنامه های 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 می کنند. اسبهای تراوا دارای روشی برای تکثیر خود نمی‌باشند.

کدهای جاسوس : برنامه هایی 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 جمع آوری کرده و برای مرکز کنترل خود ارسال می‌کنند.

نحوه گسترش ویروس

روش‌های زیر از مهم ترین 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 برنامه های خاص.
- کند شدن سرعت دریافت و ارسالهای اینترنتی.
- افزایش حجم اطلاعات.
- ناپدید و گم شدن اطلاعات.
- تخریب پرونده ها و اطلاعات.
- کار نکردن برخی از قطعات سخت افزاری.

نحوه مقابله با ویروسها

یکی از مهم ترین روش های مقابله با برنامه های مخرب پیشگیری از انتقال آن به رایانه است لذا باید روش های انتقال آنها را فرا گرفت و اقدامات پیشگیرانه ای لازم را انجام داد.

❊ استفاده از یک دیواره آتش[1] : دیواره آتش، یک برنامه امنیتی است که از نفوذ انواع نرم افزارهای مخرب جلوگیری می‌کند.

❊ از نرم افزارهائی که توسط منابع غیر مطمئن توزیع و ارائه میگردند، اجتناب و نرم افزارهای مربوطه را از منابع مطمئن تهیه و نصب کنید.

❊ امکان راه اندازی 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 بصورت تصادفی در درایو مربوطه قرار گرفته شده است، اجتناب شود.

❊ امکان «حفاظت ماکرو در مقابل ویروس» را در تمام برنامه های 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 پیوست های یک نامه الکترونیکی ارسال شده که می تواند شامل کدهای اجرائی باشند، آنها را باز نکنید. در رابطه با پرونده‌های word و Excel، پیوست هایی 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 می شناسید معمولاً خیلی بیشتر از غریبه هاست. بسیاری از کارشناسان امنیتی عقیده دارند که حتی اگر با اطلاع قبلی نیز پیامی دریافت می کنید که فایلی به آن ضمیمه شده است، باز هم باید مراقب باشید، زیرا ممکن است فرستنده به طور ناخواسته فایل آلوده ای را ارسال کرده باشد. برخی از ویروس ها نیز می توانند از طریق اتصال به آدرس دفترچه آدرس شما خود را تکثیر کنند.

❊ معمولاً پیام های متنی ساده نمی توانند ویروسی باشند اما به عنوان مثال، پیام هایی که قالب آنها HTML است، می توانند حامل یک ویروس بسیار خطرناک باشند.

❊ پرونده‌های با پسوند EXE، COM و یا VBS اجرائی 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 اجرائی که بهمراه 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.

۱- Firewall

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

❊استفاده از برنامه های ضد Pop Up.

❊عدم استفاده از برنامه های به اشتراک گذاری پرونده از جمله Kazza.

❊عدم استفاده ارتباط شبکه ای با پایگاه‌های ناشناخته و نامعتبر.

برنامه های ضد ویروس

ضد ویروس (آنتی ویروس) اصطلاحی است که به برنامه یا مجموعهای از برنامه ها 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 می نماید. در بیشتر موارد درصورتی 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

چند نمونه از نرم‌افزارهای ضد جاسوسی رایج نیز عبارتند از:

❊نرم افزار ضد جاسوسی مایکروسافت

❊Ad_ aware Standard Edition

نکات مهم در انتخاب ضدویروس

برخی از نکات که لازم است در انتخاب ضدویروس، مورد توجه قرار گیرند، در این قسمت بیان شده است. توجه به این نکات سبب می‌شود تا احتمال آلوده شدن رایانه به ویروس به کمترین حد ممکن برسد.

❊ضدویروس معروف و مطمئن انتخاب کنید.

❊ضدویروس 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 بطور متوسط در هر هفته صدها ویروس جدید تولید شده و در شبکه ها توزیع میشوند.)

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

❊ دارای دیواره آتش قدرتمند باشد.

کاربرد ضدویروس NOD ۳۲

در این بخش عملکرد ضد ویروس NOD۳۲ 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

همانطورکه 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 المعل مناسب نشان دهد. به روز رسانی ضد ویروس به دو صورت آنلاین(Online) و آفلاین (Offline) 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 (شکل۲-۷) 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 ۲-۷ به روزرسانی ضد ویروس NOD۳۲

اگر رایانه ای را که نرم افزار ضد ویروس NOD۳۲ روی آن نصب شده است، به شبکه اینترنت با سرعت مناسب متصل است، می توانید مستقیماً به روز رسانی را انجام دهید. برای این کار در پنجره اصلی نرم افزار روی بخش Update (شکل ۳-۷) کلیک کرده و گزینه Update virus signature database را انتخاب نمائید. نرم افزار به صورت خودکار به پایگاه مربوط متصل شده، پرونده های لازم برای به روز رسانی را دریافت و بروز رسانی را انجام می دهد.

شکل ۳-۷ بروز رسانی نرم افزار

زمانبندی اجرا

این نرم افزار قابلیت زمانبندی برای کارهای مختلف مانند بررسی ویروس و بروزرسانی را دارد. برای تنظیم این زمانبندی می توانید در بخشTools گزینهScheduler را انتخاب و تنظیمات مربوط را انجام دهید(شکل ۴-۷).

شکل ۴-۷ زمانبندی 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 ۵-۷

۷-۴

اطلاعات محرمانه، ریسک های امنیتی

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

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

البته برخلاف بزرگنمایی های رسانه ای و تحلیل های غیرواقعی بسیاری از کارشناسان، تهدیدهای امنیتی معاملات الکترونیک به هیچ وجه فلج کننده و غیرقابل کنترل نیستند؛ چرا که حتی در بدبینانه ترین بررسی ها، از ابتدای تولد جرایم دنیای مجازی، مجموع درآمد سالانه 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، بی انصافی ست. نباید این گونه فکر کرد که تک تک اعمال، رفتار و فعالیت های ما در اینترنت تحت کنترل تبه کاران و ابزار مخرب آن ها 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 می باشند و درست به همین دلیل تنها درصد محدودی از اقدامات خرابکارانه با هدف سرقت مستقیم یا غیرمستقیم پول به ثمر می نشینند و اغلب آنها به نحوی خنثی شده و ماهیت مجرمانه خود را از دست می دهند.

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 اعتباری تان را یادداشت کند و یا حتی خود آن را برداشته و پا به فرار بگذارد...؛ نه بیشتر. تنها تفاوت موجود، محیط انجام معامله است و عدم حضور تهدیدهای فیزیکی و قابل مشاهده .

در مبادلات و معاملات آنلاین احتمال نادیده انگاشتن جوانب امنیتی و عدم رعایت آن، فقط کمی بیشتر از داد و ستدهای حضوری ست. در حقیقت مجرمان اینترنتی معمولاً به صورت مستقیم به شبکه های سازمانی و سرورهای اطلاعاتی حمله نمی کنند؛ بلکه تمام تمام تلاش خود را بر روی آسیب پذیرترین حلقه زنجیر متمرکز می کنند... و این حلقه شکنده چیزی و یا بهتر بگوییم کسی نیست به جز کاربر نهایی. دسترسی به اطلاعات حساس و با ارزش سازمانی از طریق کاربران خانگی بسیار آسان تر از شکستن لایه های مختلف امنیتی، نفوذ به یک پایگاه اطلاعاتی و دسترسی به اطلاعات رمزگذاری شده است.

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

صفحات اینترنتی که در آن ها مبادلات آنلاین و خدمات حساس مالی یا تجاری انجام می شود، باید دارای ملزومات زیر باشند:

❊ تضمین این مسئله که داده های وارد شده برای انجام مبادلات و یا معاملات الکترونیک، تنها توسط بخش ها یا افراد معینی قابل دسترسی ست. این مسئله از طریق رمزگذاری انجام می شود.

❊ صحت، درستی و عدم نقص اطلاعات درطول عملیات نقل و انتقال؛ به منظور اطمینان از عدم سوء استفاده از اطلاعات حساس. این مسئله از طریق استفاده از امضای دیجیتال انجام می شود.

❊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 نگرانی های موجود در این رابطه مورد استفاده قرار می گیرند.

برای دسترسی به این ملزومات کلی، روش های ارتباطی استانداردی طراحی شده است که هر کدام وظایف خاصی را بر عهده دارند.

پروتکل های امنیتی

پروتکل های امنیتی قوانین و استانداردهایی هستند که برای محافظت از مبادلات و معاملات اینترنتی در برابر تهدیدهای آنلاین، وضع شده اند و دسترسی های غیرمجاز به اطلاعات تبادل شده را محدود می کنند. به این ترتیب این پروتکل ها، نقش مهمی در محافظت از کاربران خانگی، شبکه های محلی، فروشگاه ها، سازمان ها و مؤسسات مالی تجاری دارند. تهدیدهایی چون سرقت اطلاعات، سرقت مستقیم و یا غیر مستقیم پول، ایجاد توقف و اختلال در فرآیندهای تجاری، کلاهبرداری های آنلاین و غیره تهدیدهایی هستند که از کوچکترین نقص و اشتباه در کاربرد این پروتکل ها سود می برند.

مهمترین و پرکاربردترین این استانداردهای ارتباطی، برای حفاظت از فعالیت های تجاری آنلاین، پروتکل مشهوری با عنوان SSL[1] است. این پروتکل می تواند هرگونه داده و اطلاعات ورودی به سیستم یا شبکه را رمزگذاری کرده و سپس آن ها را در مقصد و برای تحویل گیرنده مجاز، رمز گشایی نماید. این بدان معناست که اگر شخص سومی بخواهد به داده های مبادله شده از طریق SSL، دسترسی پیدا کند، بدون در اختیار داشتن کلید رمزگشایی مربوطه کاملاً ناموفق خواهد بود.

در این پروتکل، تنها فروشنده و ارائه کننده خدمات آنلاین، نیاز به مدارک و معرفی نامه های دیجیتال دارد تا هویت و اعتبار امنیتی وی مورد تأیید قرار بگیرد. در این صورت خریدار و دریافت کننده خدمات اینترنتی، هیچ نیازی به ارائه معرفی نامه و هویت سنجی امنیتی نخواهد داشت.

اعتبار بخشی امنیتی

علاوه بر استفاده از پروتکل های امنیتی و ابزار حفاظت از اطلاعات رایانه ای مانند نرم افزارهای ضد ویروس، هرکدام از طرف های 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،کارت های هوشمند، امضای دیجیتال،

۱- Secure Socket Layer

شماره های IP ، آدرس های MAC و حتی خصوصیات منحصر بفرد بیومتریک (اثر انگشت، ...) همگی ابزاری هستند که به اعتبار سنجی امنیتی طرف های یک معامله اینترنتی کمک می کنند. اعتبار و هویت امن کاربرهای خانگی اینترنت معمولاً با رمزهای عبور، شماره کارت هوشمند، امضای دیجیتال و ... تأیید می شود اما برای بانک ها، مراکز فروشگاهی بزرگ و سازمان های تجاری، دارا بودن مدارک امنیتی ویژه ضروری ست. شاید بتوان گواهی نامه های دیجیتال را مهمترین ابزار شناسایی و تأیید اعتبار مراکز بزرگ مالی تجاری دانست. بدان معنی که اگر یک پایگاه اینترنتی دارای این گواهی نامه امنیتی نباشد، نباید به خیلی به آن اعتماد کرد و اطلاعات حساس و محرمانه خود را در آن وارد کرد.

امنیت تجارت الکترونیک؛ قابل دسترس، قابل اجرا

نکته بسیار مهم در اینجاست که روش های خاص امنیتی برای محافظت از معاملات اینترنتی چنان سخت گیرانه طراحی شده اند که می توان 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 فروشنده ای قرار نمی دهد و جوانب امنیتی را به طور کامل حفظ میکند، در حوزه مبادلات آنلاین نیز نباید این اطلاعات را در صفحات، پایگاه ها و نیز سرورهایی که فاقد مدارک و گواهی نامه های خاص امنیتی هستند، وارد کند .

علاوه بر این، در لایه های ارتباطی بالاتر، مدیر شبکه خدمات دهنده باید نهایت دقت و احتیاط را در اطمینان از عدم وجود هر گونه کد یا ابزار مخرب (ویروس، تروجان، ابزار هک و ...) و نیز هرگونه آسیب پذیری (حفره ها و نقص های امنیتی) به کار گیرد تا امنیت داده ها و اطلاعات ذخیره شده در سرور مورد تهدید قرار نگیرند. همان طور که بیان شد، بسیاری از نرم افزارهای مخرب مانند تروجان ها با هدف ایجاد آسیب پذیری در سرورها و یا سیستم های متصل به آن، تنها از طریق کاربران خانگی و یا سایر شبکه های خدمات گیرنده، سازمان های ارائه دهنده خدمات آنلاین را تهدید می کنند. دسترسی های غیر مجاز در سطوح بالا، سرقت داده های حساس و محرمانه و ایجاد خسارت های قابل توجه و ... تهدیدهای دائم و شایعی هستند که از کوچکترین فرصت و باریکترین روزنه استفاده مطلوب می کنند.

از طرف دیگر، مراجع صدور گواهی نامه های دیجیتال، مسئول صدور تأییدیه های امنیتی برای سرورها و شبکه ها بر اساس پروتکل های امنیتی هستند. این مراکز تصمیم گیری می توانند برای شرکت های ارائه کننده خدمات الکترونیک، مشتری ها و حتی کاربران عادی اینترنت نیز گواهی نامه های دیجیتال صادر کنند.

به عنوان نمونه ای از این مراجع معتبر می توان به گروه VeriSign اشاره کرد که عمده فعالیت های امنیتی زیرساخت در اینترنت را به عهده دارد.

توصیه های مهم به کاربران خدمات بانکی و تجاری آنلاین

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

❊ ۱.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 خطرناک ترین و در عین حال شایع ترین تهدید علیه فعالیت های مالی اعتباری در اینترنت، نوعی کد مخرب از خانواده تروجان های Banker می باشد. 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 وفروش اینترنتی و ... اطلاعات حساس مبادله شده را پس از سرقت، به مجرمان اینترنتی ارسال می کنند.

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 آن ها به پول های باد آورده ای ست 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 آن ها، به تناسب امنیت مورد نیازتان، مهمترین و ضروری ترین ابزار دفاعی شما می باشد.

متأسفانه آمار و ارقام مربوط به خسارت های مالی، اعتباری و اطلاعاتی شرکت های بزرگ و نیز کاربران خانگی اینترنت و روزهای سخت و پر مشقت شرکت های امنیتی، نشان میدهد که تنها استفاده از نرم افزارهای حفاظتی به روز شده، درمان قطعی درد کهنه ناامنی در فضای آنلاین نیست. مجرمان اینترنتی با بهره گیری از فن آوری های روز و ابزار مدرن خرابکاری و نیز آگاهی از نحوه عملکرد نرم افزارهای سنتی ضدویروس، به انتشار هر چه بیشتر کدهای مخرب مشغول هستند. کمیت بدافزارهای رایانه ای به شکل سرسام آوری رشد داشته و به موازات آن، کیفیت عملکرد تخریبی آن ها نیز ارتقاء چشمگیری یافته است.

به احتمال قوی دلیل اصلی این موضوع، سردرگم کردن شرکت های امنیتی از طریق بمباران بی وقفه لابراتوارهای کشف و تحلیل کدهای مخرب و منحرف کردن آن ها از ردیابی حملات اصلی و اساسی خرابکاران، علیه اهداف بزرگتر است. برای مثال PandaLabs، لابراتوارهای ردیابی و کشف کدهای مخرب در شرکت پاندا، در گزارش های جدید خود به این نکته اشاره کرده است که در برخی از روزها حتی تا ۳۰۰۰ کد مخرب جدیدالانتشار را کشف و در بانک اطلاعات نرم افزارهای مخرب ثبت نموده است. شک نکنید که حداقل ۸۰ درصد از این ویروس ها، کدهای بی مصرف و بی

آزاری هستند که تنها هدف آن ها سردرگم کردن شرکت های امنیتی و نیز مشغول نگاه داشتن آن ها به ردیابی ویروس های ساده و در پشت پرده فراهم آوردن شرایط مناسب برای انتشار کدهای مخرب هدفدار و قدرتمند است.

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 فن آوری های پیشرفته و یا استفاده از روش های هوشمند در تشخیص ویروس های مخرب و ... ایده های خوبی باشند.

❊ ۲.تقریباً همه کارشناسان امنیتی عقیده دارند که اکنون مؤثرترین ابزار دفاعی در رایانه ها، بهره گیری از روش های پیشگیرانه[1] است. در این روش رفتار خاص کدها و نرم افزارهای فعال درموقعیت های مختلف، مهمترین 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.

❊ ۳.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 TruPrevent™، ابزار قدرتمندی برای پیشگیری از نفوذهای غیرمجاز و نیز افزایش توان بازدارندگی سیستم امنیتی نصب شده در رایانه است.

با توجه به حجم عظیم تولید و انتشار کدهای مخرب در شبکه جهانی وب، بدیهی و منطقی ست که اغلب شرکت های امنیتی نتوانند در ردیابی، کشف و تولید کد ضد ویروس همه بدافزارهای پراکنده در اینترنت، موفق باشند. بنابر این می توان تصور کرد که شرکت های مختلف قادرند به نحوی همپوشانی امنیتی داشته باشند و با همکاری یکدیگر و بهره گیری از کمک کاربران، تهدیدهای رایانه ای را به نحو مؤثری کنترل کنند؛ به این ترتیب حداقل کاری که می توان کرد، استفاده از ابزار مکملی ست که بیشترین سطح و بالاترین نرخ ردیابی،کشف و پاکسازی کدهای مخرب را در اختیار داشته و به محیط داخلی سیستم عامل وابسته نباشد. به عنوان نمونه ای از این ابزار مکمل نیز می توان به برنامه مشهور ActiveScan اشاره نمود که از طریق پایگاه اینترنتی www.infectedornot.com قابل دسترسی ست.

❊ ۴.به هیچ وجه هرزنامه های موجود در صندوق پستی خود را جدی نگیرید و به آن ها اعتماد نکنید؛ هرچند اگر بسیار جذاب و قابل توجه جلوه کنند. هرزنامه هایی که از طرف فرستنده ها یا منابع کاملاً نامشخص و مبهم ارسال می شوند، ریسک تخریبی بسیار بالاتری دارند. در خصوص هرزنامه های مربوط به تجارت یا خرید و فروش الکترونیک نیز باید گفت که اغلب آن ها از منابع مطمئن و امن ارسال نمی شوند و به احتمال قوی ممکن است تنها، ابزاری برای

۱- Proactive

فریبکاری خرابکاران و نیز سرقت اطلاعات حساس و ارزشمند شما باشند. هرزنامه ها سهم مهمی در اجرای حملات Phishing (ابزار کلاهبرداری آنلاین) دارند. Phishing، تکنیک بسیار حرفه ایست که اغلب کاربران غیرحرفه ای خدمات آنلاین را هدف می گیرد. خرابکاران با استفاده از این روش پیغام ها و صفحات به ظاهر امن و غیرواقعی را برای کاربر نمایش می دهند و وی را به ارسال اطلاعات محرمانه و بسیار حساس تحریک می کنند. این صفحات ممکن است شامل یک اطلاعیه و یا اعلام مشکل فنی از طرف بانک و یا سیستم پرداخت آنلاین باشد. طبق بررسی های انجام شده توسط مراکز امنیتی معتبر، تعداد کلاهبرداری هایی که فقط از طریق حملات Phishing انجام می شوند، سالیانه ۱۰ الی ۲۰ درصد رشد را نشان می هد که این میزان شامل موارد نامحسوس و کشف نشده نمی باشد.

مهمترین چیزی که از یک کاربر خدمات بانکی آنلاین و یا یک خرید و فروش کننده اینترنتی انتظار می رود این است که بداند هیچ مؤسسه مالی و یا هیچ بانکی با او در خصوص دریافت و یا تأیید اطلاعات فوق محرمانه و شخصی وی مکاتبه نمی کند. در هر حال اگر باز هم گمان می کنید که نامه مورد نظر شما که اطلاعات محرمانه تان را درخواست کرده، از طرف بانک یا بخش فروش یک سازمان بزرگ تجاری برای شما ارسال شده است، قبل از انجام هرکاری در صفحه مقابل خود، با بخش ارسال کننده نامه شخصاً تماس بگیرید و در خصوص صحت و امنیت نامه مورد نظر، اطمینان حاصل کنید. در خاطر داشته باشید که در خصوص داده های حساس و ارزشمند هیچ گونه سهل انگاری پذیرفته نیست.

علاوه بر این، لینک های موجود در هرزنامه ها نیز می توانند بسیار خطرناک باشند؛ زیرا قادرند براحتی شما را به صفحات مخرب و غیرواقعی در وب هدایت کنند که هدف آن ها ایجاد تخریب و اختلال در سیستم و نیز دسترسی غیرقانونی به اطلاعات و داده های مهم شماست. بنابراین به شما توصیه می شود 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 فعالیت های بانکی آنلاین را دارید، موارد زیر را فراموش نکنید:

❊ قبل از انجام خرید از فروشگاه های آنلاین و یا از طریق پایگاه های 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 ست. یک جستجوی ساده در اینترنت، شاید راهنمای خوبی در این زمینه باشد.

❊ سیستم های رایانه ای خود را همواره به روز نگاه دارید. سیستم های عامل و نیز بسیاری از برنامه های کاربردی نصب شده در رایانه شما یقیناً دارای نقص ها و حفره های امنیتی بی شماری هستند که می توانند توسط خرابکاران اینترنتی برای نفوذهای نامحسوس و انجام فعالیت های غیرقانونی مورد استفاده قرار بگیرند. تنها یک اشکال کوچک امنیتی در برنامه های به ظاهر ساده و پرکاربرد مانند Media Player، Yahoo Messenger و یا ACDSee، نقش خود را به نحو احسن ایفا می کند.

❊هیچ گاه فایل ها و نرم افزارهای نامطمئن را بارگذاری و اجرا نکنید؛ به خصوص اگر آن ها در منابع و پایگاه های اینترنتی نامشخص و بی نام و نشان وجود داشته باشند. این فایل ها می توانند ضمیمه نامه های الکترونیک و یا برگرفته از صفحات اینترنتی مشکوک باشند. به خاطر داشته باشید که احتمال آلوده بودن این فایل ها آنقدر زیاد است که با اجرای آن، بطور مستقیم کدهای مخرب را در رایانه خود نصب می کنید.

❊هیچ گاه 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 می دهید). به خاطر داشته باشید که احتمال کلاهبرداری و فعالیت غیرقانونی در اینترنت همیشه بیش از آن است که فکر می کنید. شما نخستین فردی نیستید که شاید در ازای سفارش آخرین و مدرن ترین نسل تلفن های همراه، جعبه ای پر از سنگ و ماسه دریافت کرده باشد.

❊امروزه انجام مزایده های 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 تکنیک های حرفه ای فروش وی را نخورید.

❊هیچ گاه اطلاعات حساس و محرمانه خود را از طریق نامه های الکترونیک ارسال نکنید. کاربران عادی و حتی برخی از کاربران حرفه ای اینترنت گمان می کنند که این روش بسیار امن تر از پرکردن فرم های الکترونیکی ست. اما متاسفانه این حقیقت ندارد. نامه های الکترونیک از لحاظ امنیتی بسیار آسیب پذیرند.

❊از تیزهوشی و حس شک خود بهره بگیرید. ظاهر و ساختار یک صفحه وب اغلب می تواند نشان دهنده غیرواقعی بودن و یا امن نبودن آن باشد. به خاطر داشته باشید که در بسیاری از موارد خرابکاران اینترنتی صفحات موقتی در اینترنت ایجاد می کنند که تنها کاربرد آن ها، 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 ست که مجرمان از شما انتظار دارند. یک خرابکار اینترنتی تنها با اعداد، ارقام و شماره های IP شما سروکار دارند 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 باشم؟

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 می کنید، به طور حتم ملاحظاتی

را در نظر می گیرید (به عنوان مثال خرید از یک مکان معتبر). خرید اینترنتی شاید ساده ترین و لذت بخش ترین کاری باشد که شما در اینترنت می توانید انجام دهید به شرطی که به یک سری نکات مهم توجه داشته باشید.

خرید اینترنتی از فروشگاه های معتبر

قبل از خرید اینترنتی، ابتدا در مورد فروشگاهی که می خواهید از آن خرید کنید تحقیق نمایید. فروشگاه های معتبر عموماً آدرس پستی، تلفن و مشخصات خود را به طور دقیق در وب سایت شان درج می کنند. 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 سرویس دهی می کرده اند، اما اکنون به علل مختلف بی استفاده مانده اند. اگر از طریق تبلیغات با فروشگاه آشنا شده اید، تقریباً می توان اطمینان داشت که فروشگاه مورد نظر فعال است، اما اگر به طور اتفاقی وارد فروشگاه شدید، باید بررسی بیشتر نمایید. معمولاً در وب سایت های فعال، بخش اخبار به روز است و این را به عنوان یکی از نشانه های به روز بودن فروشگاه می توان در نظر گرفت. نکته دیگر این است که می توان بررسی نمود که اطلاعات تکمیلی در مورد کالا به همراه قیمت و شرایط و هزینه های ارسال درج شده باشد. معمولاً فروشگاه هایی که یک شعبه ی فیزیکی دارند، بسیار مطمئن تر از فروشگاه هایی هستند که فقط به صورت مجازی پایه گذاری شده اند و آمارها نیز نشان می دهد اعتماد افراد به فروشگاه هایی که شعبه ی 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، می توانید به آدرس فروشگاه مربوطه مراجعه کنید.

شکل ۶-۷ انتشارات مدرسه

انتخاب روش خرید مناسب

وقتی از یک فروشگاه مجازی معتبر خرید می کنید، معمولاً انتخاب های 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 ریسک پذیری را داشته باشد.

خرید به صورت آنلاین

معمولاً فروشگاه هایی که ارائه دهنده سرویس های آنلاین هستند، خدمات پرداخت اینترنتی خود را از یکی از بانکهای کشور دریافت می کنند و بانک ها نیز معمولاً بابت ارائه این نوع سرویس، از فروشگاه ها مبالغی بابت ضمانت دریافت می کنند. 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 می خواهید به صورت الکترونیکی دریافت کنید، مانند خرید کارت اینترنت و موارد شبیه آن. در پرداخت های آنلاین همیشه وقتی می خواهید مرحله پرداخت وجه را از طریق کارت انجام دهید، وارد سایت دومی خواهید شد که سایت بانک دریافت کننده وجه است. دقت کنید بسیاری از سارقان اینترنتی با راه اندازی سایت هایی شبیه به سایت های بانکها و آدرس های شبیه به آنها، اقدام به کلاهبرداری نموده اند. اگر از مرورگر IE استفاده می کنید، بعد از ورود به صفحه پرداخت بانک، تصویر یک قفل زرد رنگ پایین صفحه مشاهده می شود. 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 نبود، شماره کارت رمز خود را وارد نکنید، چون نشان دهنده ی این است که این سایت از نظر امنیتی تایید نشده است و یا اصلاً سایت بانک نمی باشد و اطلاعات شما در اختیار افراد دیگری قرارخواهد گرفت.

شیوه خرید از طریق واریز به حساب

در این روش برای خرید اینترنتی یک کالا باید (احتمالاً ساعت ها!) 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 نامناسب ترین شیوه های 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 پرداخت

های الکترونیکی تمام سوابق تراکنش های مالی شما در سیستم ثبت می شود و حتی مشخص است که این کالا در چه تاریخی و از چه فروشگاهی و با چه قیمتی خریداری شده است. اما در حالتی که شما به حساب فردی مبلغی واریز می کنید، ممکن است هیچ وقت چیزی به دست شما نرسد و چون شما مبلغ را در بانک واریز کرده اید 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 کرده اید مشکل تر است و ردیابی آن سخت تر و یا اگر بر فرض فیش بانکی گم شود، که اوضاع وخیم تر خواهد شد. بسیاری از سارقان از این روش نیز برای کلاهبرداری های اینترنتی خود استفاده می کنند و با راه اندازی یک سایت و ارائه یک محصول با قیمت وسوسه انگیز و ارائه شماره حساب از مشتریان، می خواهند مبالغ را واریز کنند. معمولاً این افراد درخواست مبالغ اندکی از مشتریان دارند، به طور مثال ۳ تا ۵ هزار تومان. به همین خاطر بیشتر افراد وقتی چیزی به دستشان نمی رسد در پی شکایت نمی روند، اما در نظر بگیرید این افراد از هزاران نفر به این شیوه کلاهبرداری می کنند و مبالغ کلانی به جیب می زنند.

خرید پستی

شاید بتوان امن ترین روش برای خرید اینترنتی استفاده از سیستم خرید پستی باشد که امروزه اغلب فروشگاه ها نیز از این سرویس استفاده می کنند. شما با استفاده از این روش می توانید محصول مورد نظر را سفارش دهید و محصول موردنظر توسط شرکت پست برای شما ارسال شده و سپس مبلغ کالا را به مامور پست تحویل می دهید. می بینید که در این روش شما با اطمینان خاطر و بدون اینکه پولی را از پیش پرداخت کرده باشید، می توانید محصول خود را خریداری نمایید. استفاده از این روش برای کالاهایی که ماهیت فیزیکی دارند، بسیار مناسب است. همیشه سعی کنید در فروشگاهی که امکان خرید پستی وجود دارد، از این روش استفاده کنید. البته از این شیوه در محصولاتی که ماهیت فیزیکی ندارند مانند کارت اینترنتی و اطلاعات و حق عضویت و .... نمی توان استفاده کرد و باید شیوه پرداخت آنلاین استفاده شود.

شکل۶-۷ انتشارات مدرسه

خدمات بانک‌داری الکترونیکی (بانکداری اینترنتی)

بانکداری الکترونیک شامل سیستم‌هایی است که مشتریان موسسات مالی را قادر می سازد تا در سه سطح اطلاع رسانی، ارتباط و تراکنش از خدمات و سرویس های بانکی استفاده کنند:

الف ـ 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 ـ 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 سیستم های رایانه‌ای نیاز دارد.

ج ـ تراکنش : 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 ویژگی های بانکداری اینترنتی

بانک های صددرصد اینترنتی با هدف اصلی قبول سپرده، به عنوان بانک های بدون شعبه یا دستگاه خودپرداز می باشند که با استفاده از وب سایت، مشتریان را جذب و خدمات خود را ارائه می دهند(در حقیقت این بانک ها شعبه فیزیکی و واقعی ندارند). زمانی که بانک SFNB آمریکا برای اولین بار ارائه حساب های سپرده و قبول پرداخت قبوض، خدمات خود را آغاز نمود، ایده بانکداری با استفاده از Web، اقدام و حرکت جدیدی بود. در حقیقت، بانک SFNB هرگز شعبه ای به صورت فیزیکی ایجاد ننمود و به جای آن، با استفاده از وب سایت به پذیرش حساب های جدید دست زد. در آن زمان، اندک بانک های عادی در آمریکا امکان بررسی مانده های حساب را از طریق شبکه اینترنت به مشتریان می داد و هیچکدام از خدمات پرداخت قبوض را هنوز ارائه نمی نمودند.

در این سال ها، بانکداری از طریق شبکه، همزمان با بانکهای عادی رشد کرد. از آنجایی که بانک های اینترنتی اقدام به تاسیس شعبه و خودپرداز نمی نمایند و بانک های عادی به طور مرتب بر شعبه ها و دستگاه‌های خودپرداز خود می افزایند، بعضی ممکن است که فکر کنند، بانک های عادی تمامی فعالیت ها و خدماتی که بانکهای اینترنتی ارائه می دهند را نیز انجام می دهند. اما وظیفه اصلی بانک های اینترنتی ارائه خدمات به مشتریان با بهترین برنامه برای انجام تراکنش بر روی خط اینترنت می باشد. با اینکه 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. تایید اینگونه بانک ها نیز همچون بانکهای عادی، با دریافت معیارها و شرایط قانونی لازم و کسب مجوز از بانک مرکزی انجام می شود.

مزایای بانک های صددرصد اینترنتی

همانند هرگونه تجارت الکترونیکی، مزایا و معایبی برای کار با این نوع بانک ها وجود دارد که در این بخش به طور خلاصه به آن می پردازیم.

در صورتی که شما تصمیم به کنار گذاشتن بانک خود و حرکت به سمت دنیای جدید بانک صد درصد اینترنتی گرفته‌اید، چه انتظاری از این تجربه جدید می توانید داشته باشید؟

با توجه به قابلیت آن در ارائه خدمات در وب سایت، این نوع بانک ها 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 : بانک های صددرصد اینترنتی نه تنها برای گشایش حساب، امکان انجام کلیه مراحل از طریق خط اینترنت را می دهند، بلکه واریز وجه برای گشایش حساب نیز می تواند انجام شود.

❊وب سایت هایی که دارای ویژگی های سهولت در استفاده و قدرت عملیاتی بیشتری می باشند: اینترنت تنها شعبه برای بانک های اینترنتی محسوب می شود. این گونه بانک ها 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 بانک های عادی– به ارمغان می آورد.

❊پیشنهاد بهتر: با کاهش هزینه های کلی، بانکهای صددرصد اینترنتی قادر هستند که سود خود را به مشتریان انتقال دهند. برای مشتریانی که مبالغ زیادی در این بانکها سپرده گذاری می نمایند، امکان کاهش و یا حذف کارمزدها وجود دارد.

❊سهولت در پرداخت قبوض : بانک های اینترنتی در ساده نمودن مراحل پرداخت قبوض – چه نمایش قبوض بر روی صفحه کامپیوتر و چه پرداخت قبوض – تا حد امکان تلاش نموده اند. با تشویق مشتریان در تجهیز این گونه خدمات، بانک های صددرصد اینترنتی تلاش در جهت کاهش هزینه ها می نمایند.

معایب بانک های صددرصد اینترنتی

توصیه می شود قبل از تصمیم به تثبیت وضعیت حساب های خود (جاری و پس انداز) در یک بانک اینترنتی، به موارد زیر نیز توجه فرمائید:

❊ملاقات حضوری در بانک را فراموش نکنید: اگر نزدیک دفتر مرکزی آن،زندگی می کنید، این تنها راهی است که از وجود بانک اطمینان حاصل نمایید.

❊واریز نمودن پول نقد در حساب ها را فراموش کنید: در صورتی که پول نقد دارید، با استفاده از چک و از طریق پست به دفتر مرکزی آن ارسال دارید.

❊نبودن بعضی از خدمات ویژه: اینترنت موقعیت های بسیاری را در مقابل شما قرار میدهد، اما نمی تواند کلیه خدماتی که در بانک های عادی عرضه می شود – همچون: چک مسافرتی و بانکی و غیره – را در اختیار شما قرار دهد. ارائه این گونه خدمات بر روی خط اینترنت غیر ممکن است.

❊مشاور مالی : اینترنت هنوز به عنوان یک ابزار موثر در جهت امور مشاوره ای قرار نگرفته است. ارتباط از طریق پست الکترونیک یا تلفن نیز در حدی نیست که بتوان از آن برای سوالات پیچیده مالی استفاده نمود.

❊مواظب هیولای کارمزد باشید: در حالی که بسیاری از بانک های صددرصد اینترنتی، بخشی ازکارمزدهای استفاده از خودپرداز بانک های دیگر را حذف می نماید، این به آن معنی نیست که این بانک ها برای عملیات خودشان هیچگونه کارمزدی دریافت نمی کنند. افرادی که تراکنش های بسیاری را انجام می دهند و مانده اندکی در حساب خود دارند، باید به کارمزدها توجه کافی داشته باشند. کارمزدها بخشی از زندگی روزانه بانکی ما را تشکیل می دهد و بانک اینترنتی نیز از این قاعده مستثنی نیست.

❊ضرورت آشنایی با فناوری : آشنایی و تسلط کافی به رایانه، از جمله ضرورت های استفاده از بانکهای صددرصد اینترنتی می باشد.

هنگامی که تصمیم به انتخاب بانک اینترنتی می گیرید، مطمئن باشید که نرخ بالای بازار پول آنها، تنها دلیل تصمیم شما نباشد.

کاربری بانکداری اینترنتی

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

۱.معامله کنندگان اینترنتی : این گروه مشتری مایل به اتوماسیون و ساده نمودن احتیاجات تراکنشی خود، تا حد امکان می باشد. دستیابی به حساب های چک (جاری) و کارت های اعتباری از طریق خط اینترنت، به عنوان مزیتی برای این گروه مشتریان محسوب می شود. 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 حساب های خود هستند که اقدام به نگاه داری 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، کارت های اعتباری، وام ها و پرداخت قبوض به طور یکپارچه می باشند. سهولت در استفاده و گستردگی این خدمات، مهمترین عامل برای این گروه از مشتریان می باشد.

۴.وام گیرندگان: این گروه از مشتریان خواهان دریافت وام با مبالغ دلخواه و باسود کم و امکان وثیقه گذاری پایین می باشند.

کارمزد در بانک های اینترنتی

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

❊ پرداخت قبوض: در حالی که پرداخت قبوض به عنوان ذخیره ای برای بانک محسوب می شود، بیشتر بانکها برای این گونه خدمات، وجهی به صورت ماهانه در یافت می نمایند. در بعضی موارد نیز این خدمات رایگان انجام می شود.

❊ کارمزد دستگاه های خودپرداز :بیشتر بانک های اینترنتی برای استفاده از خودپرداز بانکهای دیگر، کارمزد دریافت می نمایند. البته حداکثر تا یک مبلغ معین در روز امکان استفاده از این خدمات وجود دارد.

❊ کشیدن چک و درخواست دسته چک :همانند شیوه های مرسوم بانکی در بانکداری اینترنتی، برای کشیدن هر چک یا درخواست دسته چک، ممکن است هزینه ای دریافت شود.

❊ کارت های اعتباری: در رابطه با کارت های اعتباری، انتظار نداشته باشید که کارتی با کارمزد سالیانه یا نرخ بهره خوبی را به دست آورید.

❊ سایر کارمزدها: همانند بانک های سنتی، انتظار کارمزد برای انتقال وجه از طریق سیم، چک های برگشتی چک بی محل را داشته باشید. در این نوع موارد، تفاوتی میان بانک های اینترنتی و بانک های عادی وجود ندارد.

یکی از مزایای بانک اینترنتی در این است که بسیاری از بانکهای اینترنتی اهمیت رابطه مشتری را درک می‌کنند. اگر شما حساب بانکی با مانده قابل توجه داشته باشید، بعضی یا تمام کارمزدها در رابطه با بانکداری روی خط، حذف می شوند.

راه حلی برای برتری در بانکداری: شعبه اینترنتی

بر اساس آخرین تحقیقات به عمل آمده، استفاده از اینترنت ظرف چند سال آینده، بطور قابل ملاحظه ای افزایش می‌یابد که از جمله دلایل این افزایش فوق العاده، می توان به: پایین بودن قیمت کامپیوترهای شخصی، آسودگی بیشتر و ایمنی

اشاره کرد. فراهم کردن فرصتی برای بازاریابی بی واسطه و مستقیم، کارآیی موثر، مطمئن و با ایمنی بالا، از مزایای ایجاد سیستم الکترونیک بانکداری است.بانک های نیز واقعی تلاش کرده اند که بخشی از خدمات خود را به صورت اینترنتی به مشتریان خود ارایه دهند.

البته اخیراً، بسیاری از بانک هایی که به این کانال جدید توزیع و تبلیغ، به عنوان ترفندی برای حفظ مشتریان و افزایش تعداد آنان می نگریستند، از ادامه کار ناامید شده اند. چرا که افزایش بی سابقه عرضه خدمات بانکی لحظه ای توسط بانک های مختلف، عرصه کار و رقابت را برای آنان تنگ تر کرده است و شاید هم حق با آنان باشد. ایجاد یک شعبه اینترنتی، دقیقاً به سختی احداث یک شعبه بانکی در مرکز شهر و تامین کلیه نیازهای آن می‌باشد. مطالعه عمیق بروشورهای تجاری، شرکت در کنفرانس های فناوری بانکی و آگاه بودن از طرح های مختلف تجاری، مانند: ادغام شرکت ها و تجارت خانه ها و یا حتی پیمانکاری برای ایجاد شعبه اینترنتی از میان پایین ترین قیمت های پیشنهادی، از جمله موارد حائز توجه و اهمیت می باشد. اما این موارد نه تنها ممکن است تضمین کننده موفقیت نباشد، بلکه احتمالاً باعث افزایش هزینه ها در درازمدت خواهد شد. گرچه، بسیاری از بانکهای بزرگ و سابقه دار جایگاه خاصی در عرصه تجارت الکترونیک یافته‌اند، اما بسیاری از اطلاعات تکنولوژیک و ماشینی برای آنها، همچنان تعریف نشده باقی مانده است.

۷-۶

هوشیاری در اینترنت

چرا باید در دسترسی به خدمات اینترنتی بانک ها، به مساله 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 بانک ها است که کمابیش توجه کاربران ایرانی را نیز به خود جلب کرده است.

حتی از طریق یک اتصال معمولی به اینترنت، می توانیم بسیاری از فعالیت های 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 بانک ها، بسیار مناسب، خیلی سریع و کاملاً ساده هستند؛ اما آیا می توانیم عبارت «خیلی امن» را هم قاطعانه به این فهرست اضافه کنیم؟ چند درصد از افرادی که از خدمات «اینترنت بانک» استفاده می کنند، بویژه آن هایی که مشتری دائم این خدمات محسوب نمی شوند، از امنیت کامل در هنگام فعالیت های

مالی و اعتباری برخوردارند؟ آیا صرف اینکه مبلغ زیادی را جابجا نمی کنیم و یا تنها برای پرداخت قبوض یا اطلاع از موجودی حساب از اینترنت استفاده می کنیم، می توانیم احساس امنیت کامل داشته باشیم؟ آیا به صرف این که امنیت مؤثر فرآیندهای مالی، از طرف بانک خدمات دهنده تأمین شده باشد، کاربران خدمات «اینترنت بانک» به طور کامل از تهدیدهای امنیتی مصون خواهند بود؟

امنیت، حقیقت فراموش شده

واقعیت این است که اغلب بانک ها، سازمان ها و مراکز تصمیم گیری، کابران خدمات بانکی را با انواع تبلیغات، اطلاعیه ها و تشویق ها بمباران می کنند تا علی رغم تمام محدودیت های موجود در خصوص دسترسی افراد به اینترنت، آن ها را به سمت استفاده از خدمات اینترنتی سوق دهند، فارغ از این که اطلاع رسانی همین دستگاه ها در خصوص امنیت «اینترنت بانک» تقریباً صفر است. البته این مساله کاربران خانگی و شخصی را از بی توجهی به تأمین امنیت اینترنت در رایانه های خود مبرا نمی کند؛ اما مراکز و رسانه های تأثیر گذار 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 خدمات دهنده[1] و هم در طرف خدمات گیرنده[2]، 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.

این روزها، خرابکاران و تبهکاران اینترنتی، به دنبال فتح پایگاه های مهم اطلاعاتی و نفوذ در مراکز نظامی و دولتی، تنها با هدف کسب شهرت و خودنمایی در برابر هم قطارانشان نیستند. آن ها اکنون یک انگیزه قوی تر دارند: «پول». سرقت مستقیم پول و یا هرنوع فعالیت خرابکارانه ای که به کسب درآمدهای کلان منجر شود، اکنون به محور فعالیت های مجرمانه در اینترنت تبدیل شده است.

درست به همین دلیل، بسیاری از کدهای مخرب و ویروس های رایانه ای، با هدف سرقت اطلاعات ارزشمند وحساس کاربران، طراحی و در شبکه جهانی اینترنت منتشر می شوند. بر اساس اعلام شرکت امنیتی پاندا، هم اکنون ویروس های سارق اطلاعات مالی، بیش از دو سوم کدهای مخرب پراکنده در اینترنت را به خود اختصاص داده اند. این بدافزارها اغلب به دنبال ایجاد اختلال در فرآیندهای عملیاتی رایانه شما نیستند و شما هیچ وقت از حضور و فعالیت مخرب آن ها آگاه نخواهید شد. به بیانی دیگر چون این ویروس ها نشانه خاصی ندارند و عملکردهای سیستم را تحت تأثیر قرار

۱- Server-Side ۲- Client-Side

نمی دهند، توجه شما را به هیچ وجه جلب نمی کنند. وظایف اصلی آن ها، جمع آوری اطلاعات محرمانه و ارسال رونوشتی از آن ها به خرابکاران و مجرمان اینترنتی ست. بسیاری از آن ها فعالیت های مالی اعتباری شما را رصد می کنند؛ برخی دیگر رایانه شما را در برابر سایر تهدیدهای خطرناک آسیب پذیر می کنند و بعضی دیگر نیز مانند کدهای مخرب Bot، می توانند رایانه ها را به طور کامل در اختیار گروه های تبهکاری قرار دهند، به نحوی که از آن ها در تخریب وسیع و یا سرقت گسترده اطلاعات استفاده شود.

نکته دیگر این که بسیاری از کاربران تصور می کنند، چون پول زیادی در کارت های اعتباری و حساب های بانکی خود ندارند و یا تنها برای پرداخت قبوض خدماتی خود از اینترنت استفاده می کنند، هدف مناسب و مهمی برای هکرها و مجرمان اینترنتی محسوب نمی شوند. اما درست برعکس، تمام کاربران متصل به اینترنت، همگی به یک میزان در معرض حملات اینترنتی قرار دارند. چون همه آنها تنها یک مشخصه مجازی واضح دارند و آن هم همان «آدرس های اینترنتی» یا آدرس های IP رایانه های متصل به اینترنت است. برای اجرای حملات مخرب و نفوذهای غیرمجاز در اینترنت تنها آدرس های IP اهمیت دارند و نه چیز دیگر.

متأسفانه هر چقدر تعداد کدهای مخرب رایانه ای و ویروس های سارق اطلاعات افزایش می یابد، توجه امنیتی کاربران اینترنت نیز به دلایلی که ذکر شد، کاهش می یابد. فراموش نکنیم که مهمترین این دلایل، احساس کاذب امنیتی ست که به علت اطمینان از عدم وجود ویروس یا نقص های امنیتی در رایانه های شخصی و خانگی ست. کاربران خانگی، کلمه «ویروس» را مترادف با اختلال، ناهماهنگی، تخریب و یا کندی عملکرد در رایانه ها می دانند و احتمال نمی دهند که بسیاری از بدافزارها دارای عملکرد کاملاً نامحسوس و پنهان هستند.

چگونه، دسترسی به خدمات اینترنتی بانک ها را امن کنیم؟

بانک ها و مؤسسات مالی اعتباری، به شما خدمات امن ارائه می کنند. این مساله نباید موجب نگرانی شما باشد که ممکن است بانک ها ناامن باشند. البته در مواردی نادر، خرابکارهای حرفه ای با حمله به پایگاه های اطلاعاتی مؤسسات مالی، موفق شده اند تا علاوه بر سرقت مستقیم پول، اطلاعات ارزشمند و حساس مشتریان آن ها را نیز به سرقت ببرند (نظیر آنچه که در سال ۲۰۰۸ میلادی برای بانک سوئدی نوردآ اتفاق افتاد). اغلب مجرمان اینترنتی ترجیح می دهند 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 عمده ای متوجه شما و اطلاعات شما نخواهد بود.

مهمترین نکته ای که باید به آن توجه کنید این است که همانقدر که در دنیای واقعیت مراقب اطلاعات مالی، کارت

های 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 دسته ای پول نقد که حتی در کیف دستی خود قرار داده اید، کمتر نیست. پس بنابراین، برای امنیت فعالیت های 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 فن آوری های حفاظتی برای پیشگیری از نفوذ برخوردار بوده و فایل ضدویروس آن بروز باشد. به عنوان پیشنهاد می توانید از ضدویروس رایگان و قدرتمند Panda Cloud Antivirus، استفاده کنید.

❊هر از چندگاهی، رایانه خود را برای کشف و پاکسازی ویروس های احتمالی اسکن کنید. برخی از ویروس ها، به هر دلیل می توانند از لایه های حفاظتی رایانه شما عبور کرده باشند. برای پاکسازی این نوع ویروس ها، اسکن دستی رایانه ها به صورت دوره ای ضروری ست.

❊هرزنامه ها و یا پیغام های مشکوک با فرستنده های ناشناس را به هیچ وجه جدی نگیرید. هرچند اگر جذاب یا قابل توجه جلوه کنند. این نامه ها می توانند حاوی لینک های مخرب و یا ابزار کلاهبرداری آنلاین باشند.

❊از هر فروشگاهی 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 فروشگاهی اطمینان حاصل نمایید.

❊علاوه بر نرم افزارهای ضدویروس، سیستم های عامل و برنامه های کاربردی مهم خود را نیز به روز نگاه دارید. دانلود و نصب اصلاحیه های مهم نرم افزاری و بروزرسانی خودکار سیستم های عامل، راهکارهای مناسبی محسوب می شوند.

❊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 استفادهٔ روزافزون و همگانی از پدیده‌های فناوری اطلاعات و ارتباطات، به خصوص در دسترس بودن این ابزار و امکانات برای کودکان و نوجوانان، خطرات و آسیب‌های بکارگیری آن‌ها، ضروری است مطالبی، در بارهٔ نظارت والدین بر استفاده این گروه آسیب‌پذیر ارائه شود.

در چنین عصری که جهان بر محور فناوری اطلاعات و ارتباطات می‌چرخد و همه شئون اجتماعی را تحت تأثیر قرار داده و همهٔ گروه‌های سنی را مجذوب خود کرده است، و انواع جرائم وآسیب‌های اجتماعی را نه تنها مضاعف، که متحول و دگرگون ساخته است، باید در اندیشهٔ طرح و روشی دیگر برای هدایت، راهنمایی و حفاظت از نوجوانان بود. برای مثال امروزه کامپیوتر در زندگی کودکان نقش مهمی ایفا میکند و این نقش، به سرعت در حال افزایش است. برای نمونه، تعداد کودکان ۲ تا ۷ سال که در منزل از کامپیوتر استفاده می کنند، از میزان ۴۸ درصد در سال ۱۹۹۶ به ۷۰ درصد در سال ۲۰۰۸ رسید. استفاده از اینترنت نیز از ۱۵ درصد به ۵۲ درصد، در یک دورهٔ پنج ساله افزایش یافته است. تحقیقات نشان داده است که ۱۴۹ میلیون نفر در سراسر دنیا به شبکه اینترنت متصل هستند که این رقم، به میزان ۱۲ درصد در هر ماه افزایش می‌یابد. بررسیهای آماری در سال ۲۰۰۸ بیانگر این مطلب است که کودکان ۲ تا ۷ ساله، به صورت متوسط ۳۴ دقیقه در روز از کامپیوتر استفاده میکنند که این زمان، با افزایش سن، بیشتر میشود. این افراد آسیب پذیرترین و تأثیرپذیرترین قشر جامعه هستند و بیشترین خطرات پدیدار شده، ناشی از به‌کارگیری فناوری اطلاعات متوجه آن‌هاست. اهمیت این مسئله به اندازه‌ای است که امکان دارد، ضربه‌ای جبران ناپذیر بر جامعه و خانواده‌ها وارد آورد. استفادهٔ کودکان و نوجوانان از فناوری اطلاعات، در صورت نداشتن علم استفاده از آن یا غفلت والدین، میتواند نگران کننده باشد. نقش پدر و مادر در این زمینه، بسیار پررنگ است و میتواند با یک برنامه‌ریزی دقیق و نظارت درست بر استفادهٔ فرزندان، از این معضل پیشگیری کند. در این عصر، فرزندان از سنین کم به سوی رایانه و به طور کلی، فناوری اطلاعات کشیده شده اند و نمیتوان از استفادهٔ آن‌ها از این فناوری جلوگیری به عمل آورد. پدر و مادر باید سعی کنند، بر عملکرد فرزندان‌شان نظارت و کنترل مناسب داشته باشند. فناوری اطلاعات، هم میتواند خطرآفرین و هم سودمند باشد، زیرا در صورت نبودن نظارت، فرزندان به مشکلاتی از لحاظ جسمی و روحی دچار میشوند 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، میتوانیم 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 میخواهند از این فناوری استفاده کنند؛ مانند کسانی هستند که میخواهند، به فضا یا جهانی تخیلی سفر کنند و از دامها، دره‌ها، سیاه چال‌ها و حتی مناظر زیبایی که در این سفر با آن‌ها روبه‌رو می‌شوند، اطلاعی ندارند.

اگر کسی میخواهد به این سفر برود، باید خود را به وسایل گوناگون تجهیز کند و برای مقابله و پیشگیری از هرگونه خطر آماده باشد. یکی از این وسایل، نقشهٔ راه است، بنابراین، والدین باید نقشهٔ راه را به فرزندان نشان دهند و آن‌ها را از خطرها آگاه سازند. زمانی که فرزند این نقشه را به هر دلیلی در اختیار نداشته باشد، بی‌تردید در دامهایی که برای او گسترانیده شده، گرفتار خواهد شد. همان‌گونه که نقش والدین در هدایت و راهنمایی فرزندان بسیار مؤثر است، تأثیرپذیری فرزندان نیز تا حدود بسیاری در دستان والدین است، والدین باید بکوشند، فرزندان را به خود نزدیک سازند و نگذارند که آن‌ها نیاز عاطفی خود را از راه‌های نادرست برطرف سازند؛ ارتباط صمیمی و گرم والدین با فرزندان موجب می‌شود که کودکان و نوجوانان در مقابل چالش‌ها و تهدیدها به دامان والدین پناهنده شوند. در غیر از این صورت، فرزندان ما با مشکلات زیادی روبه رو خواهند شد. ابزارهای فناوری جدید که ممکن است، فرزندان ما را تهدید کند، عبارت است از: اینترنت، بازیهای رایانه‌ای و تلفن همراه.

اینترنت

اینترنت فضایی وسیع و اقیانوسی از اطلاعات است که هم اکنون با شکل گرفتن جامعهٔ اطلاعاتی و فضای شبکه‌ای، نمودی از دهکدهٔ جهانی را به نمایش گذاشته است. این فضا روزانه در حال گسترش و افزایش است و محدودیتی برای آن متصور نیست. شبکهٔ 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 دستیابی به آن‌هاست که اینترنت، اینگونه جایگاه ویژه ای نزد اقشار مختلف مردم یافته و روزبه روز، هم به جمع علاقه مندان این فناوری در جهان افزوده میشود.

تحقیقات صورت گرفته در این زمینه نشان میدهد، سرعت انتشار اینترنت ۹ برابر سریعتر از رادیو، ۴ برابر سریعتر از رایانه های شخصی و ۳ برابر سریعتر از تلویزیون بوده است. فرزندان ما به دلیل دستیابی هرچه سریع‌تر به علایق خود، به سمت اینترنت کشیده شده و ساعت‌ها در اقیانوسی مواج از زشت و زیبا، و خوب و بد غوطه‌ور می‌شوند. این والدین هستند که باید آن‌ها را از رسیدن به گرداب‌های بیهوده، هرزه و ضداخلاقی باز دارند.

بر اساس اعلام مراکز گوناگون جهانی، دو سوم والدین، از نحوهٔ آگاهی یافتن استفاده فرزندان شان از اینترنت ناتوان

هستند. در حقیقت آن‌ها به هیچ وجه نمی توانند، ارتباطات اینترنتی فرزندانشان را کنترل کنند و این به نگرانی عمیق در میان والدین تبدیل شده است. از سوی دیگر، از هر صد پدر و مادر، یک نفر از نحوهٔ استفاده فرزندش از اینترنت نگران بوده، این نگرانی را به شکلهای مختلف، اعم از منع استفاده از اینترنت، تنبیه بدنی یا لفظی بروز میدهد. آمار نشان میدهد که بسیاری پایگاه‌های اینترنتی به کاربران اجازه میدهند، تا هر گونه پیام و تصویر، حتی تصاویر و پیامهای غیراخلاقی را به دیگران ارسال کنند که بر همین اساس، شاخص‌ترین سنینی که این پیامها را ارسال میکنند، ردهٔ سنی ۱۵ تا ۲۵ سال هستند.

از طرفی یک سوم کودکان زیر یازده سال (عمدتاً پسر)، به دلیل کنجکاوی بیش از اندازه، حداقل دو تا سه بار در هفته، از پایگاه‌های غیراخلاقی دیدن کرده، تصاویر و پیامهای نامناسب و غیراخلاقی دریافت یا ارسال میکنند. این در حالی است که اغلب والدین این کودکان، از این موضوع بی اطلاع بوده و گمان میکنند، فرزندانشان برای آگاهی از جدیدترین بازیهای کامپیوتری، کارتون یا کتاب به اینترنت مراجعه می کنند. بررسی نتایج پژوهشهای روانشناسان دانشگاه تورنتو نشان می‌دهد، کودکان بیشتر بعد از ظهرها، و نوجوانان و جوانان ساعتهای پایانی شب را برای مراجعه به اینترنت انتخاب میکنند. در این پژوهش آمده است که هر چه اشتیاق به بازدید از پایگاه‌های غیراخلاقی بیشتر باشد، زمان استفاده از اینترنت به سمت ساعتهای پس از نیمه شب گرایش می یابد.

این اطلاعات و آمار، نشان دهندهٔ اهمیت موضوع اینترنت و استفادهٔ فرزندان از آن است. از دیگر مسائلی که میتواند، در رابطهٔ میان فرزندان و اینترنت مشکل آفرین باشد، استفاده از اطاق 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 نمی شناسند، 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.

همچنین 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 کلمهٔ کاربری آن اطلاع یابند.

اینترنت جدا از مضراتش، منافعی هم برای رشد علمی و خلاقیت فرزندان دارد. با اتصال به شبکهٔ 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.

بازیهای رایانه‌ای

مبحث دیگری که باید بدان پرداخت، مسئلهٔ بازیهای رایانه‌ای است. با این‌که برخی از این بازی‌ها می‌تواند سازنده باشد، برخی دیگر میتواند، آثار مخربی بر روح و جسم فرزندان داشته باشد. بسیاری متخصصان معتقدند که بهتر است، کودکان زیر سه سال، اصلاً با کامپیوتر و بازیهای ویدیویی آشنا نشوند و تا حدّ ممکن، با اسباب بازیهای قابل لمس و واقعی، مثل لگو، خانه سازی و ... سرگرم شوند.در این مورد نتایج تحقیقات نشان میدهد که هیجان‌های رایانه‌ای می تواند، به تخریب یا کندی عملکرد ذهنی کاربر منجر شود. اعتیاد به بازیها، پرخاش‌گری، شرط بندی، کم شدن علاقه به فعالیتهای بدنی، فرار از مدرسه، دزدی برای تهیه پول‌بازی، صرف پول تغذیه برای بازی، گوشه گیری، آسیب بینایی و ده‌ها تأثیر مخرب دیگر، از عوامل اعتیاد به بازیهای رایانه‌ای است.

روانشناسان اعتقاد دارند بازیهای رایانه‌ای در جریان ارائه مضامین جذاب و گیرای خود، با ارائه صحنه‌های پرخشونت و خشن، طرح اسلحه‌های مختلف، تأکید بر سرعت بیشتر، به نمایش گذاشتن برهنگی و ... زمینهٔ ارائهٔ فرهنگی خاص را که بازیهای رایانه‌ای مبلغ آن‌ها هستند، برای جوانان فراهم می‌آورند.

در بسیاری از این بازیها، به هیچ عنوان بر محتوا و آثاری که میتواند، در کودک و نوجوان اثر بگذارد، فکر نشده و پشتوانهٔ علمی و روان‌شناسانه‌ای ندارد، بلکه برخی از این بازی‌ها، برخلاف آنچه ما تصور می‌کنیم، بسیار مخرب و مضرند. بیشتر بازی‌ها تنها به دلیل درآمد مالی برای صاحبان شرکتهای تولید کننده، به بازار عرضه میشوند و می‌توانند خسارات زیادی را به فرزندان ما و به موازات آن، به جامعه وارد سازند. بیشتر بازی‌های رایانه‌ای، رهاوردی جز خشونت، اشاعهٔ برهنگی، اضطراب، هیجان کاذب و سپس افسردگی در مقابل شکست از رایانه و آثار مخرب دیگر بر روح و روان فرزندان، چیز دیگری به ارمغان نمی آورد.

یکی از مضرات ثابت شده بازیهای رایانه‌ای، ایجاد روحیه خشونت و پرخاش‌گری در نوجوانان است، زیرا کودکان و نوجوانان در سنی هستند که زود تأثیر میپذیرند. امروزه با افزایش ضریب نفوذ رایانه در میان مردم، این دو قشر، بیشتر وقت خود را به بازیهای مختلف رایانه‌ای که معمولاً محتوای آن‌ها خشونت است، سپری میکنند. آن‌ها از این روحیه الگو گرفته، با والدین و هم سن و سالهای خود نیز اینگونه رفتار میکنند. حتی ممکن است کار به جایی برسد که شخصیت آن‌ها همینگونه شکل گرفته، صحبت کردن و ارتباط عادی خود را فراموش کنند و تنها با حرکات فیزیکی

ارتباط برقرار سازند و در خواستهای خود را متأثر از شخصیت‌های رایانه‌ای، در قالب مکالمه‌های 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 پیچیده‌ای مواجه خواهند شد که به‌راحتی قابل حل نخواهد بود.

همانگونه که بیان شد، وظیفهٔ والدین نظارت است. پدر و مادر باید بکوشند که خود بازیها را خریداری کرده، نخست خود از محتوای بازی آگاهی بیابند، در غیر اینصورت، اگر فرزند خود به تنهایی به خرید بازی اقدام کرد، از او بخواهند که بازی را در اختیار ایشان قرار دهد، تا آن را بررسی کرده، سپس در اختیار آنان قرار دهند و در صورت مشاهدهٔ محتوای نامناسب، او را از این موضوع آگاه کرده، از بازی او با این نرم افزار جلوگیری کنند.

برای بازی فرزندان، باید زمان تعیین کرد و این زمان، به تکالیف، روحیه، نوبتی که به مدرسه میرود، خانواده، مسائل جسمی و روانی کودک بستگی دارد. نظر روانشناسان این است که زمان برای بازی کودکان، روزانه باید بین ۱ تا ۲ ساعت باشد و روزهای تعطیل هم میتوان، کمی مدت آن را افزایش داد. والدین میتوانند این ساعات را طبق نظم و شرایط خانه تقسیم کنند. استفاده از فناوری رایانه، چه در بحث اینترنت و چه در بحث بازیها، به صورت عمومی مضراتی را در بر دارد که به برخی از مهم‌ترین آن‌ها پرداخته، راهکارهای مقابله با آن را به صورت مختصر بیان میکنیم.

الف. معایب:

۱-اختلال در بینایی: فرزندان ما برای استفاده از رایانه به صورت مستمر به صفحهٔ نمایش‌گر نگاه می‌کنند. این امر آسیب هایی را به چشم آن‌ها وارد خواهد کرد؛ از جمله این آسیب ها عبارت است از:

- نگاه مداوم به صفحه نمایش‌گر موجب جلوگیری از پلک زدن چشم ها میشود که به کم شدن اشک چشم منجر شده و ناراحتیهای چشمی را موجب میشود.
- معمولاً کامپیوترها، در مقایسه با کارهای دفتری، در مکان بالاتری از افق دید قراردارند، بنابراین پلک‌های بالا تا اندازهٔ زیادتری جمع می شوند و در نتیجه، تبخیر اشک چشم‌ها بیش از حد معمول است و این امر موجب ایجاد خستگی و ناراحتی چشمها می‌گردد. به همین دلیل پیشنهاد می‌شود، پس از هر ۲۰ دقیقه کار با رایانه، چند دقیقه چشم به جای دیگری دوخته شود.
- کودکان به راحتی، تاری دید ناشی از نزدیک بینی، دوربینی یا آستیگماتیسم را می‌پذیرند، چون می پندارند سایر افراد نیز مانند آنان می بینند، از این‌رو در مقابل آسیب‌های چشمی به موقع واکنش نشان نمی‌دهند.

۲-بلوغ جنسی زودرس : به علت متصل شدن به پایگاه‌های غیراخلاقی در اینترنت و نیز سرگرم شدن با بازیهای رایانه‌ای که با هدف اشاعهٔ فرهنگ برهنگی طراحی شده‌اند، یا اصولاً با فرهنگ عفاف و حیای اسلامی منافات دارند، نوجوان بلوغ جنسی زودرس پیدا خواهد کرد که می‌تواند برای او خطرآفرین باشد.

۳-اختلال در رشد جسمی : به طور کلی، پایه‌های اولیه رشد و تکامل آدمی در کودکی، تعیین کنندهٔ کم و کیف رشد و تکامل بعدی وی در بزرگسالی به شمار میرود و این پایه‌ها، عمدتاً تحت تأثیر یادگیری و تجربه قرار میگیرند. حال اگر این پایه‌ها برای سازگاریهای شخصی و اجتماعی کودک مضر باشند، میتوان به سرعت و به موقع آن‌ها را تغییر داد و از عواقب ناگوار احتمالی جلوگیری کرد.

کودک و نوجوان به دلیل نشستن بیش از اندازه، در مقابل رایانه و نداشتن تحرک در چنین سنی که سن رشد و نمو اوست، اجازه رشد اعضا و جوارح خود را در اندازهٔ نرمال به بدن نمی دهد و آن‌ها به اندازهای طبیعی رشد نمی کنند. همچنین ممکن است مشکلاتی هم در ستون فقرات و مهره‌های گردن و نیز مچ دستها پدید آید که موجب ناراحتیها و دردهای بعدی مفاصل گردد.

۴-اختلال در روابط و تربیت اجتماعی : کودکان و نوجوانان به دلیل پرداختن به رایانه و ماندن در خانه، فرصت ارتباط و معاشرت با خانواده و افراد جامعه را از دست می‌دهند. و از مسائل جامعه و مباحث اجتماعی پیرامون خود دور می‌مانند. کودک بر اثر ارتباط با کودکان و بزرگسالان، دارای رفتار اجتماعی میشود که در دوره‌های پس از کودکی، همچون دورهٔ نضج، ارزشمند است؛ برای مثال بازی با دیگران، درس سازگاری با زندگی گروهی را به او میدهد و شعور و درک اجتماعی او رشد می‌کند.

۵-عدم کشف و رشد استعدادها و خلاقیت فرزندان: اگر مبانی خلاقیت را هم نیز همهٔ تواناییهای ذاتی، فطری بدانیم تأثیر محیط را در تحریک آن نمیتوانیم انکار کنیم و هر عاملی که مانع این تحریک باشد، طبعاً از رشد خلاقیت و کشف استعدادها جلوگیری خواهد کرد. از شواهد چنین برمیآید که خلاقیت در نخستین سالهای زندگی، در شیوه‌های بازی بچه‌ها ظاهر میشود. در همین موقع، هر عاملی که مانع رشد، آن باشد، خلاقیت را خفه خواهد کرد، پس از جمله موانع بسیار همگانی فقدان محرک است. اگر فرزندان تمام یا بیشتر وقت خود را در مقابل رایانه سپری کرده، استعدادهای خود را در مسائل پیرامون زندگی خود پرورش ندهند و به کارها و بازیهای مختلف نپردازند، نمیتوان خلاقیت و استعدادی را که در آن‌ها وجود دارد شناسایی و پرورش داد.

۶-گوشه گیری و کمرویی : اگر فرزندان با همسن و سالهای خود بازی نکنند و در کنار گروه دوستان خود قرار نگیرند، در آینده نمیتوانند، با آن‌ها ارتباط برقرار کنند و در نتیجه احساس خجالت کرده، در هیچ جمعی شرکت نمیکنند و گوشه گیر و کمرو میشوند.

۷-کم خوابی و دیدن خواب های پریشان: کودکان و نوجوانان، به دلیل وجود صحنه‌های عجیب و وحشت انگیر در بازیها و فضای اینترنت و نیز نوشته‌های نامفهومی که بر صفحه نمایش‌گر ظاهر میشود و فرزندان از مفهوم آن چیزی متوجه نمی شوند و تخیلاتی که در ذهن خود می پرورانند و نیز صحنه‌های خشونت‌آمیز، دچار آشفتگی خواهند شد و آن مسائل را در ساعات آخر شب، در بستر در ذهن خود مرور میکنند؛ همین تفکرات موجب میشود که آن‌ها در خواب، رؤیاهای آشفته دیده، دچار ناراحتیهای روحی شوند.

۸-افت تحصیلی: فرزندان هنگامی که به بازی و کار با کامپیوتر مشغول میشوند، گذر زمان را متوجه نشده، رسیدگی به تکالیف و خواندن درس را فراموش می کنند. وقتی میخواهند به آن‌ها بپردازند، آنقدر خسته‌اند که دقت لازم و کافی را در تکالیف خود نداشته، آن‌ها را به صورت نامطلوبی انجام میدهند. همین امر موجب میشود که کودکان و نوجوانان، به صورت محسوس افت تحصیلی پیدا کرده، از همکلاسیهای خود عقب بیفتند و این عقب افتادگی از همکلاسیها، موجب ناامید شدن از تحصیل یا حتی منجر به ترک تحصیل میشود.

ب. راهکارها

۱- والدین باید سعی کنند، اطلاعات خود را در مورد فناوری اطلاعات و کاربردهای آن افزایش داده، بتوانند در مواقع لزوم، از تواناییهای خویش برای کنترل و نظارت بر کار فرزندانشان استفاده کنند.

۲- باید مقررات ویژه ای برای استفاده از رایانه برای فرزندشان وضع کرده و فرزندان را به اجرای آن ملزم سازند. حتی‌الامکان سعی کنید، قوانین را به همراه فرزندتان وضع کنید و از آن‌ها نظر خواهی کنید؛ ولی حرف آخر را خود بزنید و بر اجرا وحسن انجام قوانین نظارت داشته باشید.

۳- از دوستان فرزندتان اطلاعات کافی پیدا کرده، نگذارید با هر کسی رابطهٔ دوستی برقرار کنند.

۴- نرم افزارهای بازی که فرزندان به خانه میآورند، را در زمان نبودشان بررسی کنید. همچنین می‌توانید از طریق قابلیت History، از پایگاه‌هایی که فرزندتان از آن‌ها دیدن کرده‌اند، مطلع شوید و در صورت لزوم آن‌ها را مطالعه کرده، محتوای آن را بررسی کنید.

۵- برای استفاده فرزندتان از رایانه، زمان تعیین کرده، آن را به دلخواه خود، در طول شبانه روز تقسیم کنید.

۶- تا حد امکان سعی کنید، دستگاه کامپیوتر فرزندتان را در جایی قرار دهید که در معرض دید پدر و مادر قرار داشته باشد و از قرار دادن کامپیوتر در اتاق خواب یا اتاقهایی که امکان نظارت مستقیم بر روی آن ندارید، خودداری کنید.

۷- سعی کنید گاهی اوقات، در زمان استفاده از رایانه، خود در کنار فرزندتان حضور بیابید و با او در استفاده از سیستم همراه شوید.

۸- از استفادهٔ فرزندتان از کامپیوتر در ساعات آخر شب خودداری کنید.

۹- از نرم افزارهای فیلتر کننده، مخصوص والدین استفاده کنید.

۱۰- فرزندان را با نرم افزارها و پایگاه‌های مخصوص خودشان آشنا کنید و طریقهٔ استفاده از آن‌ها را آموزش دهید.

۱۱- از دیدن پایگاه‌ها و نرم افزارهایی که مخصوص فرزندان نیست، در مقابل آن‌ها خودداری کنید.

۱۲- جایگاه دستگاه را طوری طراحی کنید که به بینایی و ستون فقرات او آسیب نرساند.

۱۳- در زمان استفاده از رایانه، از فرزند خود بخواهید، چند دقیقه از صندلی پایین بیاید و کمی تحرک داشته باشند.

۱۴- اگر پدر یا مادر هم از کامپیوتر استفاده می کنند، باید برای فرزند خود یک کاربری جدا ایجاد کرده، محدودهٔ کار او را مشخص کنند و نیز والدین باید برای صفحهٔ کاربری خود رمز گذاشته، فایلهای محرمانه را نیز رمزگذاری کنند تا فرزندان نتوانند به پوشه‌های مخصوص والدین دسترسی بیابند.

۱۵- تا حد امکان فرزند خود را در خانه تنها نگذارید.

۱۶- تا سن دوم دبستان، کودک خود را با بازی‌های رایانه‌ای و اینترنت آشنا نکنید و بگذارید، زندگی عادی غیر الکترونیکی را پشت سر بگذارد و همان بازیهای مخصوص کودکی را انجام دهد.

در کنار زیان‌های بازیهای رایانه‌ای میتوان به فواید آن نیز اشاره کرد. چنان که گفته شد، اگر این بازی‌ها را مخصوص سن فرزندان و با شناخت و زمانبندی به آنان ارائه کنیم، میتواند سرعت عمل، دقت، مهارت و قدرت تحلیل او را بالا ببرد. همچنین اگر نهادهای آموزشی، به علت علاقهٔ فرزندان به بازیهای رایانه‌ای، بتوانند نرم افزارهایی تولید کنند و محتواهای آموزشی و کتابهای درسی را با همان جذابیت و گیرایی ارائه دهد، بسیار مفید و سازنده خواهد بود. به این ترتیب با استفاده از اوقات تفریح و بازی در فرا گرفتن دروس مدرسه و افزایش اطلاعات علمی، به دانش آموزان کمک وافری خواهیم کرد.

تلفن همراه

این فناوری با قابلیتهای فراوانی، چون فیلمبرداری، عکاسی، بلوتوث، اتصال به اینترنت، پیام چندرسانه‌ای، موقعیت یاب و چندین قابلیت دیگر، جایگاه ویژه ای نزد کودکان و نوجوانان یافته است. این فناوری نیز مانند دیگر فناوری ها، معایب ومحاسنی 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 مدّنظر هستند، اپراتورهای تلفن همراه و تولید کنندگان مسئلهٔ سلامت

و بهداشت را فراموش میکنند و بیشتر سعی در تحریک و به هیجان آوردن آن‌ها، باموادّ، 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 جبران ناپذیری را به دنبال دارد. در اروپا دانشمندان حدود هفت سال در ۱۳ کشور، بر روی کودکان و تلفن همراه تحقیق کرده اند. این تحقیقات تحت عنوان «اینترفون»، بر روی بیش از ۶ هزار نفر از افرادی که به انواع سرطان و تومور مغزی مبتلا بودند، صورت گرفت و در نهایت آن‌ها این بیماریها را به تلفن همراه ربط دادند؛ به این ترتیب ثابت شد که در این زمینه باید به کاربران هشدار داده شود.

نوجوانان و کودکان کشور ما هم از این قضایا مستثنی نبوده، این ابزار در میان فرزندان این مرز و بوم نیز نفوذ و جذابیتی فراوان یافته است. به گزارش بخش شبکهٔ فناوری اطلاعات ایران، یکی از علل افسردگی و اضطراب در بین نوجوانان و جوانان، استفاده بیش از حد و غیر منطقی از تلفن همراه و علاقهٔ بسیار زیاد آن‌ها به سرویس پیام کوتاه، دانلود انواع آهنگهای ویژه تلفن همراه و تبادل اطلاعات بیهوده است. تحقیقات صورت گرفته بین ۵۷۵ دانش آموز مدارس دورهٔ متوسطه نشان میدهد، یک سوم کاربران تلفن همراه، علاقهٔ بسیاری به تلفن همراه خود دارند و روزانه بیش از ۹۰ بار به سوی تلفن خود می‌روند. این افراد در کوتاه مدت، از نظر روانی با مشکل روبه‌رو شده، دچار افسردگی می شوند. این نوجوانان در مقایسه با کاربرانی که ۷۰ بار در روز به سمت گوشیهای خود میروند و به نوعی از آن استفاده میکنند، از افسردگی و ناراحتیهای بیشتری برخوردارند.

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. در بیشتر گوشی هایی که کودکان و نوجوانان از آن‌ها استفاده میکنند، فیلمها و تصاویر مستهجن و غیراخلاقی وجود دارد که آن‌ها را از طریق بلوتوث و نیز پایگاه‌های مختلف اینترنت دریافت کرده، در گوشی خود ذخیره میکنند و دور از چشم والدین، به تماشای آن‌ها میپردازند. این مسئله همانند استفاده از فناوری‌های رایانه‌ای، بلوغ جنسی زودرس را به همراه دارد و عوارض خطرناکی برای خانواده‌ها به دنبال خواهد داشت.

والدین تا حد مقدور سعی کنند، تا ۱۸ سالگی برای فرزندشان گوشی تهیه نکنند؛ اگر هم تهیه کردند، باید مقرراتی را برای استفاده از آن وضع کنند. بهتر است والدین گوشی‌هایی را خریداری کنند که دارای قابلیت نظارت و کنترل باشد، تا فرزندان نتوانند، به هرچیزی که خواستند دست بیابند. و با هر کس تماس برقرار کنند. همچنین باید سعی شود، زمان مکالمه آنان محدود شود

هشدارهایی که داده شد، هم برای والدین و هم برای مسئولان امر کاملاً جدی و حائز اهمیت است. مسئولان امر نیز با نظارت بر بازیهایی که در بازار موجود است و همچنین فیلتر شدید پایگاه‌ها و وبلاگهای غیراخلاقی، میتوانند از بروز

بسیاری مشکلات فرهنگی واجتماعی جلوگیری به عمل آورند. والدین در این زمینه بیشترین نقش را دارند و با جدی گرفتن این مسئله و قرار دادن آن در برنامه ریزی های زندگی خانوادگی خود، به فرزندان خود و نیز جامعه کمک شایانی برسانند. تنها مسئلهٔ 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.kanoonParvaresh.com

www.Hod hod.ir

www.Intizarmag.ir

www.Roshd.Ir

مطالعه آزاد – راهنمایی هایی برای مقابله با Spam ها

در زیر راهنمایی هایی برای مبارزه با Spam ها آورده شده است:

بدون باز کردن پیام آن را پاک کنید: باز کردن پیام Spam می تواند 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 Spam های بیشتری دریافت خواهید کرد).

اگر شما نام فرستنده درون صندوق پستی تان یا موضوع بخش عنوان ایمیل را نمی شناسید، می توانید به سادگی بدون خواندن پیام، آن را پاک کنید. یا می توانید از قابلیت پیش نمایش در برنامه ایمیلتان استفاده کنید، یعنی بدون اینکه واقعاً آن را باز کنید، بدانید در چه رابطه ای است و سپس آن را پاک نمایید.(تذکر: مطمئن شوید که لحظه به لحظه از شر پیام های پاک شده خلاص می شوید وگرنه آنها دوباره در ناحیه سطل آشغال ساخته می شوند).

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 می گویند اگر می خواهید از فهرست ایمیل آنها حذف شوید، با یک کلمهRemove 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 گونه ای تنظیم می کنند که در نهایت، بیشتر پیام های ناخواسته دریافت نمایید.

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

از فیلتر Spam استفاده نمایید. سرویس دهنده اینترنت شما ممکن است یک فیلترspam رایگان (برای مثال Earth linki Spominator)برای توقف انباشته شدن spamها، قبل از آنکه آنها را ببینید، ارایه کند. اگر این گونه نبود، شما میتوانید برای یک سرویس فیلتر، مثلmail wise با پرداخت شارژ ماهیانه ثبت نام کنید. البته برنامه های خودکار توقف spamها نظیرmcaffe spam killer, barracuda, mail washer,choicemail نیز وجود دارند. همچنین بسته های مسدود کننده پیچیده تر spam، برای کاربردهای تجاری وجود دارند. سرانجام، می توانید در سرویس ارسال ایمیل مانندmail addresses که به آن می گویید فقط ایمیل هایی که برای شما مزیت دارد را دریافت کنید، مشترک شوید.

مراقب باشید: حتی به اصطلاح،اسپم کش ها نیز همیشه درست کار نمی کنند.یک اپراتور سرویس آنلاین به نام spamcop،می گوید « هیچ چیزی ۱۰۰٪ کار نمی کند،به جز عوض کردن آدرس ایمیل تان». صرف نظر از اینکه شما چگونه،برای فیلتر کردن یک spam تلاش می کنید،آنها همیشه برای شکست دادن فیلترها،کار می کنند.

مبارزه کنید: اگر شما می خواهید بر spamها(و سایر متجاوزین اینترنت) پیروز شوید، سایت هایabuse.net یا صفحه ردیاب ed falk را بررسی کنید. spamhaus، بدترین اسپمه های اینترنت را ردیابی میکند و با ispها و سازمان های مجری قانون، و پاک کردن spam های مقاوم و سمج از اینترنت، همکاری می کند.این سایت همچنین، یک پایگاه داده رایگان از آدرس های ip وspam های تایید شده را فراهم می کند. این گروه ها،این که کجا، spamها را گزارش دهید، افراد مناسب برای شکایت کردن نزد آنها و دیگر راه های مبارزه با spamها را به شما خواهند گفت.

محافظت کودکان در اینترنت

محافظت کودکان از سوء استفاده اینترنت Protecting Children from Internet Abuse عنوان کتاب ۱۲ صفحه ای 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 اطلاع رسانی برای والدین، سرپرستان، معلمان و نوجوانان نگاشته شده است. نکات، قوانین و مقراراتی که در این کتاب جمع آوری و ارائه شده است، تدبیری برای آگاهی و حفظ سلامت جامعه و فرزندان آن است.

خطراتی که کودکان آنلاین با آن روبرو هستند

خطراتی که کودکان ممکن است در دسترسی آزاد به اطلاعات و منابع اینترنتی با آن مواجه شوند، منابع اینترنتی غیر قانونی هستند که اغلب جنسی، محرک و خشونت آمیز بوده و عامل اصلی ترغیب کودکان به انجام فعالیتهای خطرناک و غیرقانونی هستند. نمونه ایی 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 می زنند. بعضی دیگر نیز روش ساخت بمب و یا دریافت و ارسال کیت‌های کشت ویروس را آموزش می دهند.

❊ باوجود غیرقانونی بودن بازیهای قمار، سایتهای قماربازی اینترنت را تسخیرکرده اند. 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 سایت ها تهدید بالقوه ای برای خانواده هایی که رفاه مالی خوبی دارند، محسوب می شود.

❊ با دسترسی کودکان به شماره کارت اعتباری والدین، خطر ارتکاب جرم اینترنتی وجود دارد، که در نهایت منجر به پیگرد های قانونی و عواقب مالی جبران ناپذیر می شود. باید Netiquette یعنی قوانین و آداب استفاده صحیح از اینترنت را به کودکان آموزش داد و از بی‌پروایی کودکان در سرکشی به چنین سایت هایی در زمان کار با اینترنت جلوگیری و کنترل کرد.

❊ خطر دیگر کودک آزاران هستند. افرادی که به هدف اغفال کودکان و سوءاستفاده جنسی در سایت های مختلف پرسه می زنند، و مانند شکارچیان موذی برای کودکان معصوم و ناآگاه دام های رنگین می گسترانند. آنها از پست الکترونیک و اتاق‌های گفتگو (Chat Rooms) به منظور جلب اعتماد کودکان و ترغیب آنها برای شرکت در جلسات رودررو استفاده می کنند. و با جلب اعتماد کودک، جلسه ملاقاتی را با او می گذارند. در این زمان است که کودک در دام این شیادان اسیر شده و با خطراتی چون تحلیل جسمی، بحران های روحی و دائمی روبرو خواهد شد.

❊ در بعضی موارد هم کودکان پیام‌های الکترونیکی دریافت می کنند که آزار دهنده و خصمانه است یا اینکه حاوی

اطلاعاتی هستند که تأثیرات منفی از لحاظ روحی و روانی برای آنها بوجود می آورند. تاثیراتی که سرنوشت و آینده این کودکان را تحت شعاع خود قرار می دهند.

❊ حفاظت ازحریم خصوصی کودکان امری حیاتی است. چرا که چنین حریمی در اینترنت با درجه آسیب‌پذیری بالایی روبرو است. هیچ فردی حق ندارد، مگر با کسب اجازه اولیا یا سرپرست کودک، به اطلاعات شخصی کودکی سرکشی کند. این اطلاعات شامل؛ نام، تاریخ تولد، نام مدرسه، اطلاعات خانوادگی، اطلاعاتی درخصوص دوستان، اماکن مورد علاقه، علائق و سرگرمیهای کودکانه 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 می کند اتصال نامحدود به اینترنت بدون برنامه ریزی و کنترل است. این روند استفاده، زمان با ارزش کودکان را به هدر می دهد. زمانی که می بایست صرف انجام تکالیف مدرسه یا آموزش کارهای هنری، ورزشی و یا صرف سایر موارد ارزشمند آموزشی شود. مواردی که می تواند تضمینی برای رشد سازنده و موفقیت های آینده کودک در جامعه انسانی باشد. در غیر اینصورت آینده او به مخاطره خواهد افتاد.

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

❊ زمانیکه 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، می بایست با رفتاری کاملا شایسته وی را از خطرات ادامه این کار آگاه ساخته و بصورت صریح از او بخواهید که از انجام آن خوداری کند.

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

❊ تماس های تلفنی افراد غریبه و مشکوک با کودک خود را می توانید از طریق نمایشگر شماره تلفن (Caller ID) بر روی دستگاه تلفن منزل کنترل و شناسایی کنید. از کودک خود بخواهید در خصوص شماره های ناشناس به شما توضیح دهد.

❊ زمانیکه کودک در نیمه‌های شب از جا برخاسته و پشت کامپیوتر خود اقدام به چت (گفتگوی اینترنتی) می کند،

می بایست صریحا به او گوش زد 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 سایت های مورد استفاده کودکان را هوشیارانه زیر نظر داشته و کنترل کنند.

❊ اگر احساس می کنید که کار های 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 زیادروی 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 منجرخواهد شد. در صورتیکه باید به حریم خصوصی کودکان احترام گذارده و هوشیارانه و با درایت کار های او را نظارت وکنترل 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 تنهاکمکی 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 وراه حل آن باشید.

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

۱-اگر کودک شما لباس نامتعارفی به تن می کند یا اینکه پول و هدایای دریافت می کند که توجیهی ندارد، این امر باید والدین را نگران کند. زیرا افرادی که اغلب به دنبال آزار و سوءاستفاده جنسی از کودکان می‌باشند، مبالغ هنگفتی را برای برقراری رابطه دوستی با کودکان و جلب اعتماد و اطمینان آنان صرف می کنند. استفاده نامحدود کودک یا نوجوان از خدمات اینترنتی بویژه 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، بویژه در مدت زمانی که از اینترنت استفاده می کند، منزوی شده است، باید توجه بیشتری به او و کارهایش نشان دهید.

۳-کودک آزاران و افراد متجاوز که کودکان را هدف قرار می دهند به شدت به دنبال ایجاد اختلاف و شکاف میان کودک و حامیان آنان(والدین یا سرپرستان) هستند. بزرگترین شکاف میان کودکان و خانوادها، در زمان برقراری رابطه آنان با این افراد متجاوز بروز می کند.

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 می توان 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 می کنند. برنامه‌های دیگری هم برای جلوگیری از ورود کودکان به اتاقهای چت (گفتگوی اینترنتی) و یا ارسال یا خواندن نامه های الکترونیکی طراحی شده اند. باید خاطر نشان کرد که نصب برنامه‌های فیلترینگ و بلوکه کردن تنها بخشی از طرح امنیتی اینترنت در خانه شما محسوب می شود. وجود آنها نباید باعث شود تا شما نگران و مراقب کودک خود نباشید.

۵-والدین باید به فایلهای گرافیکی که کودکشان ذخیره می کند، توجه کنند. ممکن است بعضی از آنها حاوی مطالب و عکس های نامناسبی باشند(فایلهایی که با فرمت tif ، gif،bmp ، 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، برنامه ریزی کنید. زمانی را به گفتگو و تبادل تجربه ها با سایر والدین درخصوص طرز رفتار با کودکان اختصاص دهید.

۸-شیوه هایی 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 گفتگو با کودک خود بی حوصله و عجله نداشته باشید.

۹-با کودکانتان همراه شوید. همراه کودکتان از خدمات اینترنتی و برنامه‌هایی که کودکتان از آنها استفاده می‌کنند، آشنا شوید. از آنها بخواهید تا طرز کار خود را در اتاقهای گفتگوی اینترنتی و یا روشهای بازی های آنلاین را برای شما توضیح دهند. ساعتی را کنار کودکانتان و فعالیت های اینترنتی آنها بگذرانید.

۱۰-با کودک خود درخصوص مسائلی که ممکن است در اینترنت با آن مواجه شوند، 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 می شود، بسیار متفاوت است.

۱۱-استفاده بیش از حد از اینترنت روند سلامت کودکان را به خطر می اندازد. بهتر است کودکان را به انجام فعالیت های نظیر تمرینات ورزشی، کار های 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 کودکتان باید مجاز به استفاده از اینترنت باشد.

۱۳-برای وجود کامپیوتر یا اینترنت در منزل خود متأسف نباشید چراکه کامپیوتر و اینترنت ابزار خارق‌العاده‌ایی هستند که قادرند زندگی افراد را متحول سازند. به حس درونی خود اعتماد کرده و مطابق آن رفتار کنید. بهترین کاری که شما می توانید انجام دهید محافظت از خانواده تان در مقابل استفاده بی رویه و غلط آنها از اینترنت و کامپیوتر است. با قبول مسؤولیت آن می‌توانید خطرات ناشی از این استفاده را به حداقل برسانید.

۱۴-شما باید الگوی کودکان خود باشید. اگر شما از سایت های نامناسب یا نرم افزارهای غیر مجاز یا منابع کپی رایت شده استفاده کنید، چگونه می توانید کودکان خود را از انجام چنین کارهای اشتباهی منع کنید.

۱۵-برای استفاده صحیح از این تکنولوژی بهتر است راه کارهایی را کارشناسان پیشنهاد می کنند به اجرا درآورید.

رهنمود هایی برای والدین

در این قسمت نکات مهمی را برای والدین و سرپرستان کودک ذکر کرده ایم که با رعایت آنها می توانند درصد آسیب پذیری 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 کودکتان از آنها استفاده می کنند، اطلاع حاصل کنید.

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

۴-طریقه بلوکه نمودن منابع نامناسب اینترنتی و اطلاعات ارائه شده 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 یابید.

۶-هرگز به پیغام‌های افراد ناشناس پاسخ ندهید.

۷-در برخورد با منابع اینترنتی وسوسه‌آمیز، مستهجن، خشونت آمیز، تهدیدآمیز و مطالبی که موجبات ناراحتی شما را فراهم می آوردند، پاسخی ندهید.

۸-کودکان خود را تشویق کنید در صورت برخورد با چنین مطالبی به شما اطلاع دهند. شما می توانید پیام دریافتی را فورا 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 غالبا از هویتی نامشخص برخوردارند. یک کاربر اینترنتی می تواند خود را دختری ۱۲ساله 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 بنظر حقیقی می رسد، می تواند کذب باشد. در نتیجه در برخورد و پذیرش هرگونه پیشنهادی برای قرار ملاقات با فردی، بسیار محتاط و هوشیار عمل کنید.

۱۰-قوانین و راه کارهای 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 اینکه 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 فن آوری 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. افشاء کلمهٔ رمز به افراد بیگانه، می‌تواند دردسر ساز یا خطرناک باشد. در صورتیکه شخصی تماس بگیرد و عنوان نماید که کارمند شرکت ارائه کننده خدمات اینترنتی می‌باشد و به کلمهٔ 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 می‌خواهند 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 سریعا پاک کنید. این نامه‌ها می‌توانند حاوی کدها ، ویروس‌ها وکرم‌های 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 مشی‌ها مربوط به کاربران سایتهای اینترنتی است که توصیه‌های ویژه 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 والدینتان 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 برقرارکرده اید، قرار ملاقات نگذارید. اگر قصد ملاقات باآنها را دارید در یک محل عمومی و همراه با والدین خود بر سر قرار حاضر شوید.

۹-زمانی را برای آموزش والدین خود درخصوص 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 می دهد.

۱۰-مراقب کامپیوتر خود باشید. بعضی از سایتها که کیتهای ویروس را ارائه می‌کنند. می توانند با ارسال یک ویروس کامپیوترشما 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 مقرارت 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 مقراراتی وضع شده که با رعایت و توجه به آن تا حدودی مسائل و مشکلات کاربران کاهش می یابد. قوانینی که شما را در موارد زیر متعهد می سازد:

❊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 مدرسه ام 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 کرده ام.

❊هرگز با شخصی که در اینترنت با او آشنا شده ام، بدون آگاهی و تحقیق والدینم با او ملاقات نخواهم کرد. در

صورت موافقت و همراهی آنها بر سر قرار حاضر خواهم شد.

با والدینم درخصوص وضع قوانینی برای استفاده از اینترنت صحبت خواهم کرد. تعیین مدت زمانی که می توانم در طول روز از اینترنت استفاده کنم و نیز در مورد سایتهای مناسب و سالم که می توانم مشاهده کنم، تصمیم گیری 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 می دانند، اما موضوع امنیت در تبادل اطلاعات همواره به عنوان یکی از اصول غافل مانده به شکل یک معضل پنهان باقی می ماند. تاکنون مهمترین سرویس از میان سرویس های گوناگون اینترنت، سیستم پست الکترونیکی بوده است. پست الکترونیکی امروزه در تجارت و بانکداری الکترونیکی هم کاربرد فراوانی دارد و بسیاری از تعیین هویت های مجازی امروزه توسط پست الکترونیک صورت می گیرد.

کاربران آگاه اینترنت می دانند که معمولاً سایتهایی معتبر هستند که دارای Domain رسمی با درج شماره های تماس مدیر و توضیحاتی در مورد موسسان سایت، صفحات درباره ما ، تماس با ما و غیره هستند. 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.

جرائم اینترنتی تنها محدود به کلاهبرداری نمی شوند. انتشار اخبار کذب، افترا، آزار و اذیت، سوء استفاده از پست الکترونیک، ارسال مطالب و تصاویر و فیلم های 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 سایت ها از جمله جرائم دیگر اینترنتی محسوب می شوند.

ویروسهای رایانه‌ای برنامههایی هستند که مشابه ویروسهای بیولوژیک گسترش یافته و پس از وارد شدن به رایانه اقدامات غیرمنتظرهای را انجام میدهند. انواع برنامه های مخرب عبارتند از ویروس، کرم، تروجان و کدهای جاسوس.

یکی از مهم ترین روش های مقابله با برنامه های مخرب پیشگیری از انتقال آن به رایانه است لذا باید روش های انتقال آنها را فرا گرفت و اقدامات پیشگیرانه ای 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. پروتکل های امنیتی قوانین و استانداردهایی هستند که برای محافظت از مبادلات و معاملات اینترنتی در برابر تهدیدهای آنلاین، وضع شده اند و دسترسی های غیرمجاز به اطلاعات تبادل شده را محدود می کنند.

بانکداری الکترونیک شامل سیستم‌هایی است که مشتریان موسسات مالی را قادر می سازد تا در سه سطح اطلاع رسانی، ارتباط و تراکنش از خدمات و سرویس های 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، بازیهای رایانه‌ای و تلفن همراه.

فعالیت کارگاهی

۱–از طریق اینترنت تحقیق کنید آیا بانک صددرصد اینترنتی در ایران وجود دارد یا خیر؟

۲–یک بانک صددرصد اینترنتی در شبکه اینترنت پیدا کنید و خدمات آنرا بررسی نمایید.

۳–چه بانک هایی در ایران خدمات اینترنتی ارایه 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 آنرا 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 آنرا بروز نمایید؟

خودآزمایی

۱-سایت های معتبر چه مشخصه هایی دارند؟

۲-ویروس چیست و چه تفاوتی با کرم و تروجان دارد؟

۳-عملکرد ویروس ها در رایانه بر چه اهدافی استوار است؟

۴-علایم وجود ویروس در رایانه چیست؟

۵-سه مورد از نحوه مقابله با ویروس ها را توضیح دهید.

۶-چرا هدف اصلی تبهکاران آنلاین کاربر نهایی می باشد؟

۷-پروتکل امنیتی SSL چیست؟

۸-چه روش های خریدی برای خرید اینترنتی وجود دارد؟ کدام مناسب تر است؟

۹-مزایای بانک های صددرصد اینترنتی چیست؟

۱۰-ابزارهای فناوری های جدید چگونه فرزندان ما را تهدید می کنند؟