اعتبار بخشی امنیتی

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

امنیت تجارت الکترونیک؛ قابل دسترس، قابل اجرا

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

درست به همان نحو که یک مشتری، اطلاعات شخصی، محرمانه و حساس خود را به صورت رو در رو در اختیار هر فروشنده‌ای قرار نمی دهد و جوانب امنیتی را به طور کامل حفظ می‌کند، در حوزه مبادلات آنلاین نیز نباید این اطلاعات را در صفحات، پایگاه‌ها و نیز سرورهایی که فاقد مدارک و گواهی‌نامه‌های خاص امنیتی هستند، وارد کند.

علاوه بر این، در لایه‌های ارتباطی بالاتر، مدیر شبکه خدمات دهنده باید نهایت دقت و احتیاط را در اطمینان از عدم وجود هرگونه کد یا ابزار مخرب (ویروس، تروجان، ابزار هک و ...) و نیز هرگونه آسیب پذیری (حفره‌ها و نقص‌های امنیتی) به کار گیرد تا امنیت داده‌ها و اطلاعات ذخیره شده در سرور مورد تهدید قرار نگیرند.

توصیه‌های مهم به کاربران خدمات بانکی و تجاری آنلاین

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

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

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

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

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

به همین منظور، شاید افزودن یک لایه امنیتی مکمل با فناوری‌های پیشرفته و یا استفاده از روش‌های هوشمند در تشخیص ویروس‌های مخرب و ... ایده‌های خوبی باشند.

- تقریباً همه کارشناسان امنیتی عقیده دارند که اکنون مؤثرترین ابزار دفاعی در رایانه‌ها، بهره‌گیری از روش‌های پیشگیرانه[1] است. در این روش رفتار خاص کدها و نرم افزارهای فعال درموقعیت‌های مختلف، مهم‌ترین عامل شناسایی و تفکیک کدهای مخرب و مشکوک از کدهای امن و مفید است. در این حالت نیاز چندانی به استفاده از پایگاه‌های اطلاعات امنیتی ثبت شده و مشخصات ویروس‌های قدیمی تر (البته تا حدی) نیست.
- راهکار مؤثر دیگر استفاده از یک ابزار مکمل امنیتی در کنار نرم افزارهای حفاظتی نصب شده در سیستم (یا به عبارتی در کنار همان راهکارهای سنتی حفاظت از اطلاعات) برای ترمیم نقاط ضعف آنهاست. یکی از این سیستم‌های پیشرفته برای ردیابی و کشف ویروس‌های ثبت نشده با نام TruPrevent™، ابزار قدرتمندی برای پیشگیری از نفوذهای غیرمجاز و نیز افزایش توان بازدارندگی سیستم امنیتی نصب شده در رایانه است.
- به هیچ وجه هرزنامه‌های موجود در صندوق پستی خود را جدی نگیرید و به آنها اعتماد نکنید؛ هرچند اگر بسیار جذاب و قابل توجه جلوه کنند. هرزنامه‌هایی که از طرف فرستنده‌ها یا منابع کاملاً نامشخص و مبهم ارسال می‌شوند، ریسک تخریبی بسیار بالاتری دارند. در خصوص هرزنامه‌های مربوط به تجارت یا خرید و فروش الکترونیک نیز باید

۱- Proactive

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

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

- قبل از انجام خرید از فروشگاه‌های آنلاین و یا از طریق پایگاه‌های الکترونیک، و نیز دریافت هرگونه خدمات اینترنتی، یکی از بهترین تدابیر امنیتی، اطمینان از قانونی‌بودن، میزان شهرت و سطح اعتبار این مرکز مالی تجاری است. یک جستجوی ساده در اینترنت، شاید راهنمای خوبی در این زمینه باشد.
- سیستم‌های رایانه‌ای خود را همواره به روز نگاه دارید. سیستم‌های عامل و نیز بسیاری از برنامه‌های کاربردی نصب شده در رایانه شما یقیناً دارای نقص‌ها و حفره‌های امنیتی بی‌شماری هستند که می‌توانند توسط خرابکاران اینترنتی برای نفوذهای نامحسوس و انجام فعالیت‌های غیرقانونی مورد استفاده قرار بگیرند. تنها یک اشکال کوچک امنیتی در برنامه‌های به ظاهر ساده و پرکاربرد مانند Media Player، Yahoo Messenger و یا ACDSee، نقش خود را به نحو احسن ایفا می‌کند.
- هیچ‌گاه فایل‌ها و نرم افزارهای نامطمئن را بارگذاری و اجرا نکنید؛ به خصوص اگر آنها در منابع و پایگاه‌های اینترنتی نامشخص و بی نام و نشان وجود داشته باشند. این فایل‌ها می‌توانند ضمیمه نامه‌های الکترونیک و یا برگرفته از صفحات اینترنتی مشکوک باشند. به خاطر داشته باشید که احتمال آلوده‌بودن این فایل‌ها آنقدر زیاد است که با اجرای آن، بطور مستقیم کدهای مخرب را در رایانه خود نصب می‌کنید.
- هیچ‌گاه قبل از اطمینان کامل از شرایط امنیتی موجود، اقدام به پرداخت و یا نقل و انتقال پول نکنید (درست به همان‌گونه که معاملات حضوری و فیزیکی را انجام می‌دهید). به خاطر داشته باشید که احتمال کلاهبرداری و فعالیت غیرقانونی در اینترنت همیشه بیش از آن است که فکر می‌کنید. شما نخستین فردی نیستید که شاید در ازای سفارش آخرین و مدرن ترین نسل تلفن‌های همراه، جعبه‌ای پر از سنگ و ماسه دریافت کرده باشد.
- امروزه انجام مزایده‌های آنلاین در اینترنت به طور چشمگیری رواج یافته است. قبل از آغاز پیشنهاد قیمت و شروع مزایده، از

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

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

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

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

۷_۵

خرید اینترنتی و حقوق مصرف کنندگان

در یک خرید اینترنتی از چه مواردی باید آگاه 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 می‌کنید، به طور حتم ملاحظاتی را در نظر می‌گیرید (به عنوان مثال خرید از یک مکان معتبر). خرید اینترنتی شاید ساده‌ترین و لذت‌بخش‌ترین کاری باشد که شما در اینترنت می‌توانید انجام دهید به شرطی که به یک سری نکات مهم توجه داشته باشید.

خرید اینترنتی از فروشگاه‌های معتبر

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

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

شکل ۶ـ۷ انتشارات مدرسه

انتخاب روش خرید مناسب

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

خرید به صورت آنلاین

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

می‌کنند. اخذ مبالغ ضمانت به این دلیل است که در صورت طرح شکایت از فروشگاه مربوطه، بانک بتواند ضمانت را به اجرا بگذارد. استفاده از این سیستم بیشتر در مواقعی مناسب است که شما محصول خود را می‌خواهید به صورت الکترونیکی دریافت کنید، مانند خرید کارت اینترنت و موارد شبیه آن، در پرداخت‌های آنلاین همیشه وقتی می‌خواهید مرحله پرداخت وجه را از طریق کارت انجام دهید، وارد سایت دومی خواهید شد که سایت بانک دریافت کننده وجه است. دقت کنید بسیاری از سارقان اینترنتی با راه اندازی سایت‌هایی شبیه به سایت‌های بانک‌ها و آدرس‌های شبیه به آنها، اقدام به کلاهبرداری نموده اند. اگر از مرورگر IE استفاده می‌کنید، بعد از ورود به صفحه پرداخت بانک، تصویر یک قفل زرد رنگ پایین صفحه مشاهده می‌شود. روی آن قفل دو بار کلیک کنید تا گواهینامه سایت باز شود. در قسمت Issuedto آدرس بانک نوشته شده است. (مثلاً اگر وارد سایت بانک پارسیان شده باشید، باید www.pec. ir نوشته شده باشد.) ولی اگر وارد قسمت پرداخت شدید و این قفل زرد رنگ را مشاهده نکردید، یا نام داده شده در قسمت Issuedto درست نبوده، شماره کارت رمز خود را وارد نکنید، چون نشان دهندهٔ این است که این سایت از نظر امنیتی تأیید نشده است و یا اصلاً سایت بانک نمی‌باشد 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 ساعت‌ها!) در صف بانک بایستید تا مبلغ را به حساب فروشگاه واریز کرده و سپس شماره فیش را در وب سایت وارد کنید تا محصول مورد نظر را برای شما ارسال کنند. این شیوه یکی از نامناسب‌ترین شیوه‌های خرید اینترنتی است و حتی شاید نتوان آن را یک خرید اینترنتی قلمداد کرد. زیرا استفاده از تجارت الکترونیک باید باعث سرعت و سهولت در خرید گردد، اما در این روش شما دردسر بیشتری نسبت به خرید فیزیکی خواهید داشت. از نظر امنیتی هم استفاده از این روش خرید غیر معقولانه است. در پرداخت‌های الکترونیکی تمام سوابق تراکنش‌های مالی شما در سیستم ثبت می‌شود و حتی مشخص است که این کالا در چه تاریخی و از چه فروشگاهی و با چه قیمتی خریداری شده است. اما در حالتی که شما به حساب فردی مبلغی واریز می‌کنید، ممکن است هیچ وقت چیزی به دست شما نرسد و چون شما مبلغ را در بانک واریز کرده‌اید و این فروشگاه اینترنتی برای بانک شناخته شده نیست و فروشگاه ضمانتی هم به بانک نداده است. اثبات این‌که شما مبلغی را بابت خرید محصول خاصی که در اینترنت وجود داشته پرداخت کرده‌اید مشکل‌تر است و ردیابی آن سخت‌تر و یا اگر بر فرض فیش بانکی گم شود که اوضاع وخیم‌تر خواهد شد.

خرید پستی

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

شکل ۶ـ۷ انتشارات مدرسه

خدمات بانک‌داری الکترونیکی (بانکداری اینترنتی)

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

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

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

ج) 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 ویژگی‌های بانکداری اینترنتی

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

مزایای بانک‌های صددرصد اینترنتی

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

در صورتی که شما تصمیم به کنار گذاشتن بانک خود و حرکت به سمت دنیای جدید بانک صددرصد 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 بانک‌ها مزایای مهمی را در بردارند:

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

معایب بانک‌های صددرصد اینترنتی

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

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

کاربری بانکداری اینترنتی

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

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

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

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

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

کارمزد در بانک‌های اینترنتی

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

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

راه حلی برای برتری در بانکداری: شعبه اینترنتی

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

۷_۶

هوشیاری در اینترنت

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

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

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

امنیت، حقیقت فراموش شده

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

از سویی دیگر، کاربران خدمات اینترنتی باید بدانند که امنیت اطلاعات هم در طرف خدمات‌دهنده[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 نمی‌کند و محیط عملیاتی او نیز باید کاملاً حفاظت‌شده و عاری از تهدیدهای رایانه‌ای باشد.

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

۱_ Server – Side

۲_ Client - Side

چگونه، دسترسی به خدمات اینترنتی بانک‌ها را امن کنیم؟

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

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

- رایانه خود را به یک نرم افزار امنیتی پیشرفته با حداکثر امکانات حفاظتی مجهز کنید. این نرم افزار باید از جدیدترین فناوری‌های حفاظتی برای پیشگیری از نفوذ برخوردار بوده و فایل ضدویروس آن بروز باشد. به عنوان پیشنهاد می‌توانید از ضدویروس رایگان و قدرتمند Panda Cloud Antivirus، استفاده کنید.
- هر از چندگاهی، رایانه خود را برای کشف و پاکسازی ویروس‌های احتمالی اسکن کنید. برخی از ویروس‌ها، به هر دلیل می‌توانند از لایه‌های حفاظتی رایانه شما عبور کرده باشند. برای پاکسازی این نوع ویروس‌ها، اسکن دستی رایانه‌ها به صورت دوره‌ای ضروری ست.
- هرزنامه‌ها و یا پیغام‌های مشکوک با فرستنده‌های ناشناس را به هیچ وجه جدی نگیرید. هرچند اگر جذاب یا قابل توجه جلوه کنند. این نامه‌ها می‌توانند حاوی لینک‌های مخرب و یا ابزار کلاهبرداری آنلاین باشند.
- از هر 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، سیستم‌های عامل و برنامه‌های کاربردی مهم خود را نیز به روز نگاه دارید. دانلود و نصب اصلاحیه‌های مهم نرم افزاری و به‌روزرسانی خودکار سیستم‌های عامل، راهکارهای مناسبی محسوب می شوند.

- هیچ فایل یا نرم افزار نامطمئنی را دانلود و بر روی سیستم خود اجرا نکنید. البته دانلود فایل‌ها و نرم‌افزارهای کاربردی به ظاهر امن از پایگاه‌های نامشخص و بی‌نام و نشان اینترنتی، به هیچ وجه توصیه نمی‌شود. 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 نامه‌های الکترونیک ارسال نکنید. بر خلاف تصور عموم، نامه‌های الکترونیک از لحاظ امنیتی بسیار آسیب پذیرند.

این دستورالعمل‌های ساده، تقریباً امنیت کامل فعالیت‌های بانکی شما در اینترنت را تضمین می‌کنند.

۷ـ۷ 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 به‌کارگیری آنها، ضروری است مطالبی، دربارهٔ 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. در این عصر، فرزندان از سنین کم به سوی رایانه و به طور کلی، فناوری اطلاعات کشیده شده‌اند 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 دریچه‌ای دیگر به این فناوری بنگریم و امکانات مفید آن را به فرزندان آموزش دهیم، می‌توانیم آینده‌ای 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.

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 ویژه‌ای نزد اقشار مختلف مردم یافته و روزبه روز، هم به جمع علاقه مندان این فناوری در جهان افزوده می‌شود. بر اساس اعلام مراکز گوناگون جهانی، دو سوم والدین، از نحوهٔ آگاهی یافتن استفاده فرزندان‌شان از اینترنت ناتوان هستند. در حقیقت آنها به هیچ وجه نمی‌توانند، ارتباطات اینترنتی فرزندانشان را کنترل کنند و این به نگرانی عمیق در میان والدین تبدیل شده است.

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

هم چنین والدین باید بر پست الکترونیکی‌ای که برای فرزندان فرستاده می‌شود، کنترل داشته باشند و از مطالب، تصاویر و فیلم‌هایی که برای آنها ارسال می‌شود، آگاهی یابند. پدر و مادر باید بکوشند، خودشان برای فرزندشان ایمیل ایجاد کنند، تا بتوانند از رمز ورود آن اطلاع یابند و پیش از فرزندشان، از موارد ارسالی آگاهی یابند، در غیر این صورت باید سعی کنند به هر طریقی، از رمز ورود و 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 امکان، با اسباب بازی‌های قابل لمس و واقعی، مثل لگو، خانه‌سازی و ... سرگرم شوند. در این مورد نتایج تحقیقات نشان می‌دهد که هیجان‌های رایانه‌ای می‌تواند به تخریب یا کندی عملکرد ذهنی کاربر منجر شود.

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 نمایش‌گذاشتن 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. 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.

تلفن همراه

این فناوری با قابلیت‌های فراوانی، چون فیلمبرداری، عکاسی، بلوتوث، اتصال به اینترنت، پیام چندرسانه‌ای، موقعیت‌یاب و چندین قابلیت دیگر، جایگاه ویژه‌ای نزد کودکان و نوجوانان یافته است. این فناوری نیز مانند دیگر فناوری‌ها، 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 هیجان‌آوردن آنها، بامواد، ترکیبات و کاربردهای گوشی دارند و می‌کوشند، کاربران را هر چه بیشتر تحت تأثیر قرار دهند.

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

از دیگر ویژگی‌های تلفن همراه، بلوتوث، فیلم برداری و تصویربرداری، ضبط و پخش صوت و امکان نصب و استفاده از انواع بازی‌های رایانه‌ای ویژه تلفن همراه است. والدین در این زمینه بیشترین نقش را دارند و با جدی گرفتن این مسئله و قرار دادن آن در برنامه‌ریزی‌های زندگی خانوادگی خود، به فرزندان خود و نیز جامعه کمک شایانی برسانند. تنها 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 فرهنگ‌سازی، 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 ـ راهنمایی‌هایی برای مقابله با Spamها

در زیر راهنمایی‌هایی برای مبارزه با Spamها آورده شده است:

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

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

هیچگاه به پیام‌های Spam، پاسخ ندهید: به هیچ طریقی، به یک پیام Spam پاسخ ندهید. پاسخ دادن به فرستنده Spam اطمینان می‌دهد که این یک آدرس ایمیل فعال است. برخی فرستندگان Spamها، به شما می‌گویند اگر می‌خواهید از فهرست ایمیل آنها حذف شوید، با یک 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 گونه‌ای تنظیم می‌کنند که در نهایت، بیشتر پیام‌های ناخواسته دریافت نمایید.

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

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

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

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

محافظت کودکان در اینترنت

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

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

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

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

- در بعضی موارد هم کودکان پیام‌های الکترونیکی دریافت می‌کنند که آزار دهنده و خصمانه است یا اینکه حاوی اطلاعاتی هستند که تأثیرات منفی از لحاظ روحی و روانی برای آنها به‌وجود می‌آورند. تأثیراتی 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 روبه‌رو 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 می‌کند اتصال نامحدود به اینترنت بدون برنامه‌ریزی و کنترل است. این روند استفاده، زمان با ارزش کودکان را به هدر می‌دهد. زمانی که می‌بایست صرف انجام تکالیف مدرسه یا آموزش کارهای هنری، ورزشی و یا صرف سایر موارد ارزشمند آموزشی شود. مواردی که می تواند تضمینی برای رشد سازنده و موفقیت‌های 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 می‌کنند، اقدام کنند. از آنجایی که والدین بهتر از هرکسی با خصوصیات اخلاقی و روحی کودکان خود آشنایی دارند. می‌بایست با رفتاری شایسته، سنجیده و حساب شده به‌گونه‌ای عمل کنند که احساسات آنان را جریحه‌دار 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، می‌بایست با رفتاری کاملاً شایسته وی را از خطرات ادامه این کار آگاه ساخته و به‌صورت صریح از او بخواهید که از انجام آن خودداری کند.
- هیچ‌گاه بدون دادن آگاهی و توضیح لازم در مورد کار اشتباه کودک، او را از انجام آن (تماشا یا مشارکت در سایت‌های نامناسب) سرزنش و منع نکنید. زیرا نتیجه مطلوبی به‌دست نخواهید آورد.
- تماس‌های تلفنی افراد غریبه و مشکوک با کودک خود را می‌توانید از طریق نمایشگر شماره تلفن (ID Caller) بر روی

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

● زمانی‌که کودک در نیمه‌های شب از جا برخاسته و پشت کامپیوتر خود اقدام به چت (گفت وگوی اینترنتی) می‌کند، می‌بایست صریحاً به او گوشزد کنید که هر کاری زمان خود را دارد.

● والدین و سرپرستان وظیفه دارند هنگام کار کودک با کامپیوتر بر آنها نظارت و کنترل کامل داشته باشند. آنها باید زمان‌ها و سایت‌های مورد استفاده کودکان را هوشیارانه زیر نظر داشته و کنترل کنند.

● اگر احساس می‌کنید که کارهای کودک شما غیرعادی شده و یا با دوستانش قطع ارتباط کرده است. باید سعی کنید تا با دوستان او صحبت کرده و علت آن را جویا شوید. یا اگر بر عکس، دیدار دوستان کودک شما تنها به دلیل تجمع برای مشاهده منابع نامناسب اینترنتی است، باید در این صورت مراقب باشید. البته در این مراقبت نباید زیاده‌روی کنید. چرا که افراط در این کار نوعی محدودیت و دخالت در حریم خصوصی کودک است که به احساس عدم اعتماد و تیره شدن روابط با کودک منجرخواهد شد. در صورتی‌که باید به حریم خصوصی کودکان احترام گذارده و هوشیارانه و با درایت کارهای 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 تنها کمکی به رفع مشکل شما نخواهد کرد، بلکه آن را بدتر هم خواهد کرد. به عنوان والدین و سرپرست کودک وظیفه شماست که خونسردی خود را حفظ کرده و مدبرانه درصدد شناسایی مشکل و راه‌حل آن باشید.

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

۱ـ اگر کودک شما لباس نامتعارفی به تن می کند یا اینکه پول و هدایایی دریافت می‌کند که توجیهی ندارد، این امر باید والدین را نگران کند. زیرا افرادی که اغلب به دنبال آزار و سوءاستفاده جنسی از کودکان می‌باشند، مبالغ هنگفتی را برای برقراری رابطه دوستی با کودکان و جلب اعتماد و اطمینان آنان صرف می‌کنند. استفاده نامحدود کودک یا نوجوان از خدمات اینترنتی به‌ویژه در نیمه‌های شب، دلیل دیگری برای نگرانی و هوشیاری والدین است.

۲ـ اگر کودک شما به مدت طولانی از دوستان و خانواده خود کناره گرفته، به‌ویژه در مدت زمانی که از اینترنت استفاده می کند، منزوی شده است، باید توجه بیشتری به او و کارهایش نشان دهید.

۳ـ کودک آزاران و افراد متجاوز که کودکان را هدف قرار می‌دهند به شدت به دنبال ایجاد اختلاف و شکاف میان کودک و حامیان آنان (والدین یا سرپرستان) هستند. بزرگ ترین شکاف میان کودکان وخانواده‌ها، در زمان برقراری رابطه آنان با این افراد متجاوز بروز می‌کند.

۴ـ در حال حاضر خدماتی نظیر برنامه‌های فیلترینگ و مرورگرهایی که با قابلیت بلوکه کردن انواع سایت‌های نامناسب اینترنتی است، وجود دارند. با کمک آنها می‌توان محتوای سایت‌ها را ارزیابی و یا مسدود کرد. این برنامه‌ها به شیوه‌های مختلفی عمل می‌کنند. بعضی از آنها سایت‌هایی را که از منابع نامناسب برخوردار هستند، بلوکه می‌کنند. بعضی دیگر از ورود و دسترسی کاربران به اطلاعات شخصی نظیر اسم و آدرس، پست الکترونیکی، شماره تلفن و... جلوگیری می‌کنند. برنامه‌های دیگری هم برای جلوگیری از ورود کودکان به اتاق‌های چت (گفت وگوی اینترنتی) و یا ارسال یا خواندن نامه‌های الکترونیکی طراحی شده‌اند. باید خاطر نشان کرد که نصب برنامه‌های فیلترینگ و بلوکه کردن تنها بخشی از طرح امنیتی اینترنت در خانه شما محسوب می‌شود. وجود آنها نباید باعث شود تا شما نگران و مراقب کودک خود نباشید.

۵ـ والدین باید به فایل‌های گرافیکی که کودکشان ذخیره می کند، توجه کنند. ممکن است بعضی از آنها حاوی مطالب و عکس‌های نامناسبی باشند(فایل‌هایی که با فرمت tif ، bmp، gif، jpg و pcx هستند).

۶ـ 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.

۷ـ خلاق باشید، برنامه‌ریزی کنید. زمانی را به گفت وگو و تبادل تجربه‌ها با سایر والدین درخصوص طرز رفتار با کودکان اختصاص دهید.

۸ـ شیوه‌هایی را برای برقراری ارتباط با کودک خود انتخاب کنید که با شناخت از روحیات آنها انتخاب شده باشند. و نیز صبورانه و درایت آنها را اعمال کنید. کودکان و نوجوانان خود را با خطرات اینترنت آگاه و آشنا سازید. هرگز در گفت وگو با کودک خود بی حوصله نباشید و عجله نداشته باشید.

۹ـ با کودکانتان همراه شوید. همراه کودکتان از خدمات اینترنتی و برنامه‌هایی که کودکتان از آنها استفاده می‌کند، آشنا شوید. از آنها بخواهید تا طرز کار خود را در اتاق‌های گفت وگوی اینترنتی و یا روش‌های بازی‌های آنلاین را برای شما توضیح دهند. ساعتی را کنار کودکانتان و فعالیت‌های اینترنتی آنها بگذرانید.

۱۰ـ با کودک خود درخصوص مسائلی که ممکن است در اینترنت با آن مواجه شود، گفتگو کنید. به جای سرزنش کودک به او بیاموزید که ارزش‌های واقعی زندگی در خارج از اینترنت با آنچه که در اینترنت به عنوان ارزش ارائه می‌شود، بسیار متفاوت است.

۱۱ـ استفاده بیش از حد از اینترنت، روند سلامت کودکان را به خطر می‌اندازد. بهتر است کودکان را به انجام فعالیت‌هایی نظیر تمرینات ورزشی، کارهای هنری، موسیقی و ... در محیطی خارج از خانه ترغیب و تشویق کنید.

۱۲ـ 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.

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

۱۴ـ شما باید الگوی کودکان خود باشید. اگر شما از سایت‌های 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.

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

رهنمودهایی برای والدین

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

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

۲ـ از خدماتی اینترنتی که کودکتان از آنها استفاده می‌کنند، اطلاع حاصل کنید.

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

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

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

۶ـ هرگز به پیغام‌های افراد ناشناس پاسخ ندهید.

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

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

۹ـ به وجود افرادی با هویت ناشناس در اینترنت باید توجه کرد. چرا که کاربران اینترنتی غالباً 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 به‌نظر 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.

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

نکاتی برای کودکان آنلاین

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

۱ـ کلمه رمز استفاده از کامپیوتر و اینترنت، را باید مخفی نگه دارید. از گفتن کلمه رمز به دیگران به جز والدین خود اجتناب ورزید. افشای کلمهٔ رمز به افراد بیگانه، می‌تواند دردسرساز 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؟

۲ـ 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.

۳ـ هرگز نامه‌های الکترونیکی افراد ناشناس، غیرعادی و مشکوک را باز نکنید. و آنها را سریعاً پاک کنید. این نامه‌ها می‌توانند حاوی کدها، ویروس‌ها وکرم‌هایی که بسیار برای سیستم کامپیوتر شما خطرناک است، باشند. اگر به نامه‌ای مشکوک هستید از والدین یا افراد متخصص بخواهید تا به شما کمک کنند.

۴ـ 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.

۵ـ 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 فعالیت‌های مفید تقسیم کنید.

۶ـ قوانین مربوط به وب سایت‌های اینترنتی را مطالعه کنید. این قوانین و خط مشی‌ها مربوط به کاربران سایت‌های اینترنتی است که توصیه‌های ویژه‌ای برای استفاده از سایت‌ها 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.

۷ـ 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.

۸ـ از خود محافظت کنید. هرگز با شخصی‌که در اینترنت ارتباط برقرارکرده‌اید، قرار ملاقات نگذارید. اگر قصد ملاقات باآنها را دارید، در یک محل عمومی و همراه با والدین خود بر سر قرار حاضر شوید.

۹ـ 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 می‌دهد.

۱۰ـ مراقب کامپیوتر خود باشید. بعضی از سایت‌ها که کیت‌های ویروس را ارائه می‌کنند، می‌توانند 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 مقرّراتی وضع شده که با رعایت و توجه به آن تا حدودی مسائل و مشکلات کاربران کاهش می‌یابد. قوانینی که شما را در موارد زیر متعهد می‌سازد:

- من هرگز بدون اجازه اطلاعات شخصی خود را از قبیل آدرس، شماره تلفن، آدرس محل کار والدین و شماره تلفن محل کار، عکس، اسم و آدرس مدرسه‌ام را در دسترس دیگران قرار نخواهم داد.
- اگر با اطلاعاتی روبرو شدم که موجب آزار من شود، بلافاصله به والدینم اطلاع خواهم داد. تقصیر من نیست که چنین اطلاعاتی دریافت کرده‌ام.
- هرگز با شخصی که در اینترنت با او آشنا شده‌ام، بدون آگاهی و تحقیق والدینم ملاقات نخواهم کرد. در صورت موافقت و همراهی آنها بر سر قرار حاضر خواهم شد.

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

منبع:

:Protecting Children from internet By Asian School of cyber Laws

http://www.asianlaws.org/fact

خلاصه

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

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

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

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

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

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

ابزارهای فناوری جدید که ممکن است، فرزندان ما را تهدید کند، عبارت است از: اینترنت، بازی‌های رایانه‌ای و تلفن همراه.

فعالیت کارگاهی

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

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

۳ـ چه بانک‌هایی در ایران خدمات اینترنتی ارایه می‌دهند؟ این خدمات شامل چه فعالیت‌هایی می‌باشند؟ سه نمونه را بیان نمایید.

۴ـ به سایت کتابفروشی «انتشارات نص» مراجعه کنید و روش‌های خرید اینترنتی آن‌را بررسی نمایید.

۵ـ به پوشه Spam حساب پست الکترونیکی خود بروید و کاری کنید که دیگر از آن آدرس‌های فرستنده، برای شما ایمیلی ارسال نشود.

۶ـ چند نرم افزار در رابطه با کنترل والدین در اینترنت پیدا کرده و خصوصیات آنها را با یکدیگر مقایسه کنید.

۷ـ چه راهکارهای عملی بر روی رایانه برای کنترل و نظارت والدین وجود دارد؟ آنها را بررسی نمایید.

۸ـ نرم افزار ضدویروس رایانه خود را بررسی نمایید. آیا می توانید از طریق اینترنت آن‌را به روز نمایید؟

خودآزمایی

۱ـ سایت‌های معتبر چه مشخصه‌هایی دارند؟

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

۳ـ عملکرد ویروس‌ها در رایانه بر چه اهدافی استوار است؟

۴ـ علائم وجود ویروس در رایانه چیست؟

۵ـ سه مورد از نحوه مقابله با ویروس‌ها را توضیح دهید.

۶ـ چرا هدف اصلی تبهکاران آنلاین کاربر نهایی می‌باشد؟

۷ـ پروتکل امنیتی SSL چیست؟

۸ـ چه روش‌های خریدی برای خرید اینترنتی وجود دارد؟ کدام مناسب‌تر است؟

۹ـ مزایای بانک‌های صددرصد اینترنتی چیست؟

۱۰ـ ابزارهای فناوری‌های جدید چگونه فرزندان ما را تهدید می‌کنند؟