امنیت در فضای سایبر

مونا کریمی

چکیده

امنیت یکی از ارکان مهم جامعه و خانواده است و امروزه با پیشرفت تکنولوژی امنیت یک معنای جدیدتری به خود در فضای مجازی گرفته است. فضای مجازی فضایی است که در آن افراد بدون اینکه همدیگر را کاملا بشناسند شروع به ارتباط برقرار کردن با یکدیگر و اشتراک هرگونه فایلی را می کنند. بنابراین مسئله ی اعتماد در این گونه فضاها بسیار کم است و همین مسئله موجب ایجاد مشکلات بزرگی در سطح جامعه شده است و افراد کلاه برداری از این طریق کاربران را فریب داده و از اعتماد آن ها سوء استفاده می کنند و سپس از آن ها اخاذی می کنند. در این مقاله ابتدا فضای سایبری را شرح می دهیم سپس جرائم رایانه ایی ، امنیت و راه های ایجاد امنیت در فضای مجازی توسط کاربر و نکاتی برای پیشگیری از وقوع جرایم رایانه ایی را بررسی می کنیم.

کلید واژه ها : امنیت ، سایبر ، فضای سایبر ، جرائم رایانه ایی ، شبکه های اجتماعی

مقدمه

بشر همواره به داشتن امنیت و اطمینان خاطر در هر زمینه ایی نیـاز دارد و بـا آرامـش و امنیـت اسـت کـه انسان می تواند مسیر زندگی خود را به راحتی و بدون دغدغه ی فکری پیش ببرد.

برای مثال امنیت در خانواده به معنای داشتن یک کانون گرم خانوادگی و آرامش فکری و روانـی والـدین و فرزندان است و امنیت در کشورها به معنای امن و امان بودن کشور و مرزها از هر گونه تجاوز و جنگ (چـه در داخل و چه در خارج از کشور) توسط دشمنان است و ...

امروزه با رشد تکنولوژی اینترنت ، یک معنی دیگری از امنیت تحت عنوان ، امنیت در فضای مجازی بـرای کاربران مد نظر است. که داشتن این امنیت به مراتب مهم تر از امنیت در خانواده و کشور است زیـرا اگـر ایـن امنیت از بین برود کانون خانواده و حتی یک کشور از هم می پاشد.

با رشد تکنولوژی ، دولت ها نیز باید به سوی الکترونیکی شدن قدم بردارند. اما عدم وجود امنیـت کـافی در یک فضای مجازی (الکترونیکی) برای انجام کارهای کاربران از جمله : امور بانکی ، خرید اینترنتی ، عـضویت در شبکه های اجتماعی و ... تمایل کاربران را به داشتن این تکنولوژی کـاهش مـی دهـد و کـاربران همـواره کارهای خود را به صورت سنتی انجام می دهند بنابراین داشتن دولت الکترونیک در کشور متوقف می شود.

اما آیا این دلیل خوبی برای عقب ماندگی از پیشرفت است؟ قطعا خیر. بنابراین بایـد سیاسـتگذاران در هـر کشور با صرف هزینه ی هنگفت و ایجاد یک راهبـرد مناسـب و اسـتفاده از متخصـصین در زمینـه ی امنیـت فضای مجازی دولت و ملت خود را با پیشرفت جهانی همگام کنند.

سایبر[1]

از لحاظ لغوی در فرهنگ های مختلف سایبر به معنی مجازی وغیرملموس می‌باشد، محیطی است مجـازی وغیرملموس موجود در فضای شبکه‌های بین‌المللی (که این شبکه ها از طریق شـاهراه هـای اطلاعـاتی مثـل اینترنت به هم وصل هستند) که در این محیط تمام اطلاعات راجع بـه روابـط افـراد، فرهنـگ هـا، ملـت هـا، کشورها و به طور کلی هر آنچه در کره ی خاکی به صورت فیزیکی ملموس وجود دارد (بـه صـورت نوشـته، تصویر، صوت، اسناد) در یک فضای مجازی به شکل دیجیتالی وجود داشته و قابل استفاده و دسترس کاربران می‌باشند و از طریق کامپیوتر، اجزا ی آن وشبکه‌های بین‌المللی به هم مرتبط می‌باشند.

واژه سایبر از لغت یونانی کایبرنیت[2] به معنی سکاندار یا راهنمـا مـشتق شـده اسـت. نخـستین بـار ایـن اصطلاح سایبرنتیک توسط ریاضیدانی به نام نوربرت وینر[3] در کتابی بـا عنـوان "سـایبرنتیک و کنتـرل در ارتباط بین حیوان و ماشین" در سال 1948 به کار برده شده است.
سایبرنتیک علم مطالعه و کنترل ساخت ها در سیستم های انسانی، ماشینی و کامپیوتر ها است.

فضای سایبر[4]

واژه ی فضای سایبر را نخستین بار ویلیام گیبسون[5] نویسنده داستان علمی تخیلی در کتـاب نورومنـسر[6] در سال 1984 به کار برده است. فضای سایبر در معنا به مجموعه هـایی از ارتباطـات درونـی انـسان هـا از طریق کامپیوتر و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می شود.

یک سیستم آن لاین نمونه ای از فضای سایبر است که کاربران آن می توانند از طریق ایمیل با یکدیگر ارتباط بر قرار کنند. بر خلاف فضای واقعی، در فضای سایبر نیاز به جابجایی های فیزیکی نیست و کلیه ی اعمال فقط از طریق فشردن کلید ها یا حرکات ماوس صورت می گیرد .این عدم جابجایی فیزیکی، محققان را وا داشت که به مطالعه برخی شباهت های فضای سایبر با حالت های نا هشیاری، به خصوص حالت های ذهنیای که در رویا ها ظاهر می شوند، بپردازند.

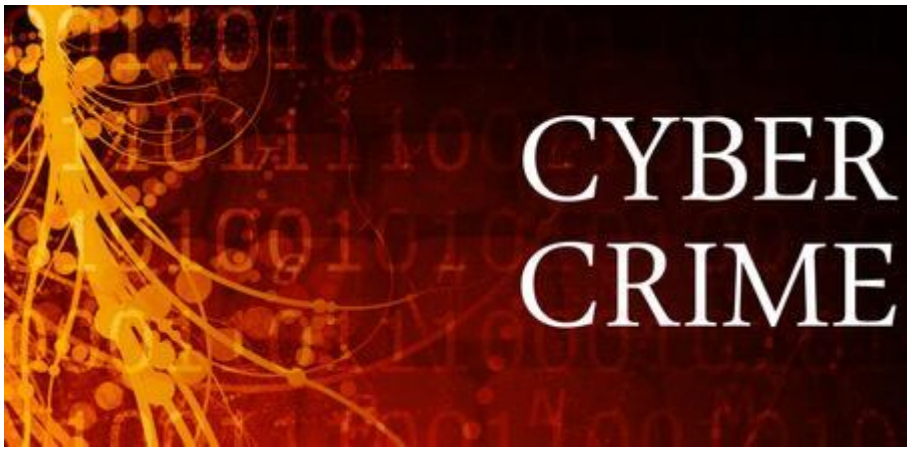
1.Cyber
2.Kybernetes
3.Norbert Wiener
4.Cyberspace
5.William Gibson
6.Neuromancer

ویژگی های فضای سایبر

کاربران می‌توانند به هرگونه خدمات اطلاعاتی الکترونیکی دستیابی پیدا کنند، بدون در نظر گرفتن این که این اطلاعات و خدمات در کدام نقطه ی دنیا واقع شده‌است. محیط سایبر زمینه ی فعالیت های اقتصادی مهم و ابزار ضروری برای انجام کلیه ی معاملات تجاری و در سطح بین‌المللی بدون دخالت مستقیم بشر فراهم آورده‌است. محدوده ی فعالیت کاربر به مرزهای فیزیکی یک خانه یا یک محل کار وحتی مرزهای یک کشور محدود نبوده و در یک سطح کم هزینه هرکاربر می‌تواند در هر زمانی و در هر مکانی با مردم در هر نقطه‌ای از جهان ملاقات کند و اطلاعات مبادله کند ، بدون اینکه ازمحل واقعی و هویت فرد خبر داشته باشد.

جرم سایبری

جرم سایبری بر دو نوع است : در تعریف محدود جرمی که در فضای مجازی (سایبر) رخ می دهد جرم رایانه ای است و بر اساس این دیدگاه ، اگر رایانه ابزار و وسیله ارتکاب جرم باشد آن جرم را می توان در زمره جرائم رایانه ای قلمداد کرد. در تعریف گسترده هر عملی که به کمک یا ، از طریق سیستم های رایانه ای رخ می دهند جرم رایانه ای قلمداد می شود.



جرایم در فضای سایبر

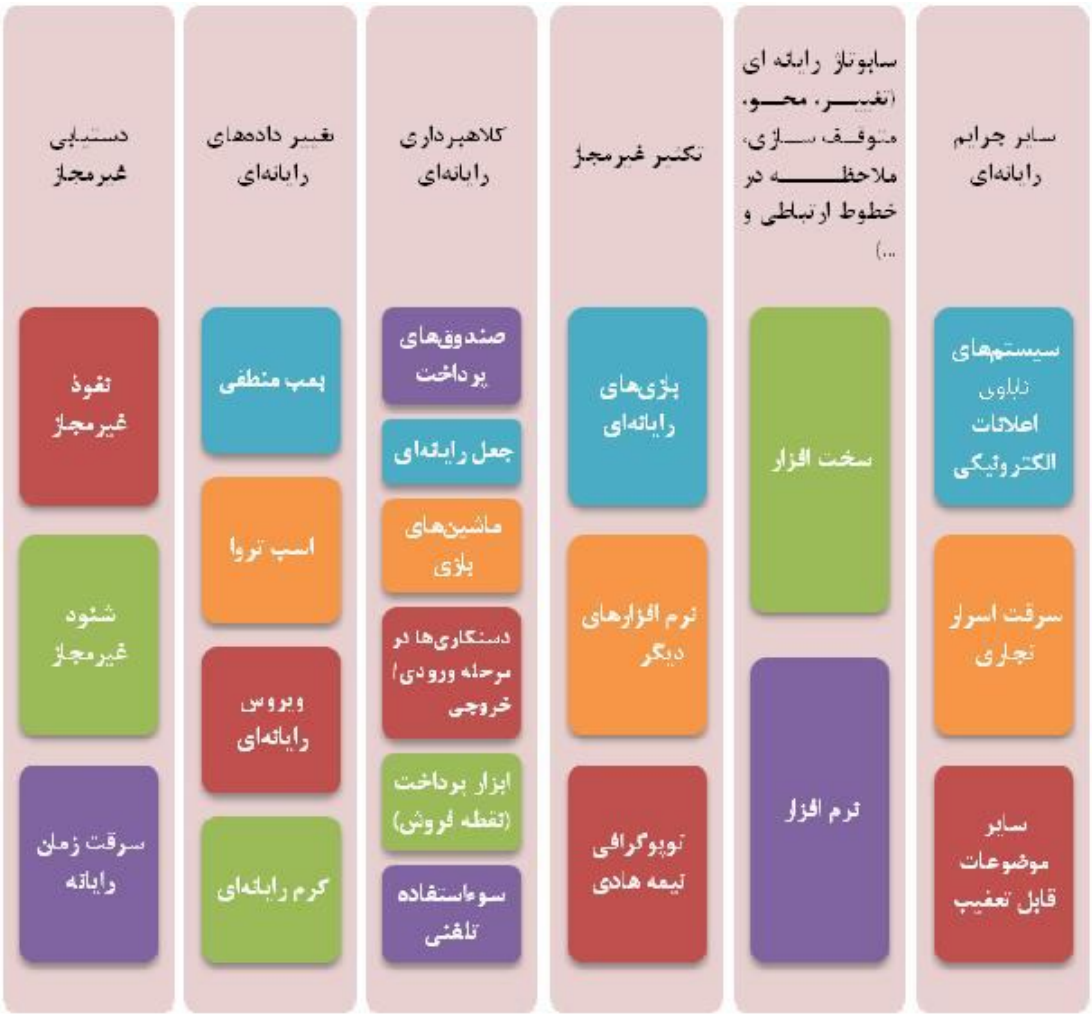
طبیعت این جرایم وسوء استفاده های مرتکب شده دراین دنیای مجازی هیچ گاه در دنیای حقیقی دیده نشده است. امنیت نا کافی تکنولوژی همراه با طبیعت مجازی آن فرصت مناسبی را در اختیار افراد شرور قرار می‌دهد. نگران کننده ترین جنبه ی فضای سایبر انتشار سریع اطلاعات درآن می‌باشد، مثلا در لحظه ی

کوتاهی قسمتی از اطلاعاتی که می‌تواند به طور بالقوه مورد سوءاستفاده قرار گیرد کشف مـی‌شـود. در فـضای سایبر برای جستجو و پیداکردن این جرایم مشکلات پیچیده تر می‌شود. دردنیای واقعی دزدی از بانـک کـاملا مشخص است چرا که بعد از سرقت در خزانه بانک پولی موجود نیست. ولـی در تکنولـوژی کـامپیوتری شـدن یک خزانه می‌تواند بدون هیچ علامتی خالی شود.

برای مثال سارق می‌تواند یک کپی دیجیتال کامل از نرم افزار بگیرد و نرم افزار اصـلی را همـان طـور کـه دقیقا بوده باقی بگذارد. در فضای سایبر کپی عینا عین اصل است. با کمی کار روی سیستم، سـارق مـی‌توانـد امکان هرگونه تعقیب و بررسی مثل پاک کردن اثر انگشت را تغییر دهد.

در اروپا، کشور سوئد به عنوان اولین کشور، با تصویب قانونی در سال 1973 دستیابی غیرمجاز به اطلاعـات ذخیره شده را به عنوان جرم در نظر گرفت.

سازمان پلیس جنایی بین المللی جرائم رایانه ای را طبق نمونه ی ذیر طبقه بندی کرده است :



بحران سازهای سایبر

- ویروس : ویروس‌ها یا برنامه‌های خود همانندساز، برنامه‌هایی هستندکه با هدف آلوده کردن سیستم‌های دیگر نوشته می‌شوند ومعمولا از طریق یک دیسک وگاهی از طریق اینترنت یا شبکه‌های پست الکترونیک سرایت می‌کنند. بعضی ویروس ها ممکن است قادر به حمله به فایل‌های سیستم و ذوب کردن برد اصلی یک رایانه ، پاک کردن تمام داده‌های دیسک سخت و از کار انداختن رایانه باشند.
- عنکبوت‌های موتورهای جستجو و پالس‌های الکترومغناطیس : که می‌توانند دیسک سخت یک رایانه را ذوب کنند.
- کرم ها : می توانند به یک سیستم دسترسی پیدا کنند اما نمی‌توانند در خارج از شبکه به آن دسترسی پیدا کنند. برای مثال از طریق یک دیسک ، گسترش پیدا کنند.کرم ها در یک رایانه مقیم می‌شوند و فضای رایانه را اشغال می‌کنند تا آن که رایانه کند شود یا از کار بیفتد.
- بمب‌های منطقی : آن ها تعمدا زیانبار ساخته می‌شوند اما مانند ویروس‌ها تکثیر نمی‌شوند. آن ها طوری طراحی شده اند که طی یک دوره ی زمانی در رایانه غیر فعال باقی می مانند و سپس با سررسیدن تاریخی که برنامه ی آن ها مشخص شده است منفجر می‌شوند. اهداف این بمب ها متفاوت است.

پلیس سایبر

بعضی ازافسران پلیس از دهه1970 در زمینه جرایم سایبر آموزش دیده اند وتخصص پیدا کرده اند. جرایم سایبر ممکن است در هر جایی اتفاق بیفتد و غالبا قابل ردیابی نیستند. بیشتر ادارات پلیس محلی فاقد پرسنل ماهر یا بودجه لازم برای مبارزه با جرایم سایبر هستند به ویژه به این دلیل که این پرونده ها ممکن است در آن واحد به حوزه های قضایی متعددی مربوط شوند. بنابراین چه کسی مسئول مبارزه با جرایم سایبر خواهد بود؟ علاوه بر آنچه پلیس رایانه‌ای نامیده می‌شود، شهروندانی نیز وجود دارند که به صورت شخصی به جلوگیری از جرایم سایبر و شناسایی مجرمان کمک می‌کند. هنوز هم مباحثات زیادی در مورد روش های مورد استفاده توسط مقامات رسمی، دراجرای قوانین مبارزه با جرایم سایبر وجود دارد. پلیس تا چه حد مجاز است که در تحت پیگرد قرار دادن و دستگیری مجرمان سایبر به ویژه هکرها پیش رود؟ پلیس تا چه حد اجازه دارد که به حریم خصوصی الکترونیک شهروندان پا بگذارد؟ چگونه باید میان حقوق افراد و نیاز مقامات دولتی برای تحقیقات و تشکیل پرونده تعادل برقرار کرد؟ ولی با این وجود پلیس توانسته بسیاری از هکرهای بدخواه را شناسایی کند و در یافتن مجرمان سایبر موفق باشد.

در ایران نیز پلیس سایبر تحت عنوان پلیس فتا (فضای تولید و تبادل اطلاعات) از بهمن ماه 1389 به دستور سردار فرماندهی نیروی انتظامی تولید و تبادل اطلاعات تشکیل شده است و توانسته است مجرمان

رایانه ایی زیادی را به دام اندازد.

تامین امنیت فضای تولید و تبادل اطلاعات کشور، صیانت از هویت دینی، ملی و ارزش‌های انسانی جامعه در فتا، حفظ حریم خصوصی و آزادی‌های مشروع، صیانت از منافع، اسرار و اقتدار ملی در فضای تولید و تبادل اطلاعات، حفظ زیر ساخت‌های حیاتی کشور در مقابل حملات الکترونیک و اعتماد و آسودگی خاطر آحاد شهروندان جامعه برای انجام تمامی امور قانونی از جمله فعالیت های اقتصادی ، اجتماعی و فرهنگی به منظور صیانت از حاکمیت و اقتدار ملی از جمله اهداف تشکیل پلیس فتا است.

درباره مفهوم امنیت اجتماعی

در لغت، امنیت به معنای امن بودن : امنیت داشتن (شهر امن است) و بی خطر بودن (جاده ها امن نیست) امن و امان : آرام و خالی از موجبات بیم و هراس / امنیت : وضع یا کیفیت نبودن خطر یا آشوب ، ایمنی (اینجا شب ها امنیت ندارد. کشور از امنیت برخوردار است.) معادل انگلیسی این واژه **Security** و در عربی امن می باشد.

امنیت در کشورها در گذشته که تکنولوژی مورد بحث نبود به امنیت در مرزها و در داخل کشور با استفاده از سلاح های سرد خلاصه می شد اما امروزه علاوه بر این معنی عمومی امنیت یک معنی جدید در حوزه ی فضای مجازی به خود گرفته است که این امنیت به مراتب مهم تر و قابل توجه تر است چرا که حملات سایبری چه در داخل و چه در خارج از مرزها آسیب های جبران ناپذیری به دولت ها و ملت ها وارد می کند.

امنیت سایبر

به امنیت فناوری اطلاعات، وابسته به سیاست دولت ها، امنیت سایبر گفته می شود. این اصطلاح عموماً توسط مؤسسه های دولتی و سیاستگذاران ملی در اسناد، قوانین و پروژه های تحقیقاتی استفاده می شود و کما بیش مترادف با امنیت اینترنت است .هر دو عبارت به جوانب امنیت شبکه و اصول سیاستگذاری شبکه ها مثل تعریف حریم خصوصی، جرائم سایبر، تجارت و ارتباطات جهانی اشاره دارند.

با وجود تبادل عظیم اطلاعات حیاتی و یا خصوصی از طریق اینترنت باید دید اینترنت تا چه حد برای ارسال داده‌های حساس، مطمئن است. وامنیت شبکه‌ها وقتی داده‌ها درآن جریان پیدا می‌کنند چگونه است؟ چرا که با وجود جریان داده‌ها روی اینترنت طبیعی است که فکر کنیم گوش دادن وگرفتن اطلاعات حساس موجود می‌تواند کار ساده‌ای باشد. اما رمزگذاری روی داده ها(غیر قابل فهم یا غیر قابل خواندن داده ها) ، لایه سوکت‌های امن به عنوان استاندارد ایمنی و رمز عبور معتبر، جداسازی داده‌ها روی کامپیوترهای متعدد وتفکیک پایگاه داده‌ها (جدا نگه داشتن اطلاعات مشتریان) روش‌های پیشرفته در ایمنی داده‌ها می‌باشند.که می‌توانند از دستیابی هکر ها به داده ها جلوگیری کنند.

فناوری های امنیت اطلاعات

امنیت اطلاعات به حفاظت از اطلاعات و به حداقل رساندن خطر افشای اطلاعات در بخش های غیرمجاز اشاره دارد. امنیت اطلاعات مجموعه ای از ابزارها برای جلوگیری از سرقت، حمله، جنایت، جاسوسی و خرابکاری و علم مطالعه روش های حفاظت از داده ها در رایانه ها و نظام های ارتباطی در برابر دسترسی و تغییرات غیرمجاز است.

با توجه به تعاریف ارائه شده، امنیت به مجموعه ای از تدابیر، روش ها و ابزارها برای جلوگیری از دسترسی و تغییرات غیرمجاز در نظام های رایانه ای و ارتباطی اطلاق می شود

فن آوری به کاربرد علم، خصوصاً برای اهداف صنعتی و تجاری یا به دانش و روش های مورد استفاده برای تولید یک محصول گفته می شود.

بنابراین فناوری امنیت اطلاعات به بهره گیری مناسب از تمام فناوری های امنیتی پیشرفته برای حفاظت از تمام اطلاعات احتمالی روی اینترنت اشاره دارد.

طبقه بندی Infosec

طبقه بندی ارائه شده در این مقاله از فناوری های امنیت اطلاعات ، در وهله اول براساس دو ویژگی پایه گذاری شده است:

براساس مرحله خاصی از زمان : به این معنا که در زمان تعامل فن آوری با اطلاعات عکس العمل لازم در برابر یک مشکل امنیتی می تواند کنشگرایانه (کنشی)[7] یا واکنشی[8] باشد.

غرض از کنشگرایانه انجام عملیات پیشگیرانه قبل از وقوع یک مشکل خاص امنیتی است .در چنین مواردی به موضوعاتی اشاره می گردد که ما را در پیشگیری از وقوع یک مشکل کمک خواهد کرد (چه کار باید انجام دهیم تا...)

غرض از واکنشی انجام عکس العمل لازم پس از وقوع یک مشکل خاص امنیتی است در چنین مواردی به موضوعاتی اشاره می گردد که ما را در مقابله با یک مشکل پس از وقوع آن، کمک خواهند کرد (اکنون که ... چه کار باید انجام بدهیم؟)

براساس سطوح پیاده سازی نظام های امنیتی در یک محیط رایانه ای : فناوری امنیت اطلاعات را، خواه از نوع کنشی باشد یا واکنشی، می توان در سه سطح پیاده سازی کرد :

سطح شبکه **Network Level**
سطح میزبان **Host Level**
سطح برنامه کاربردی **Application Level**

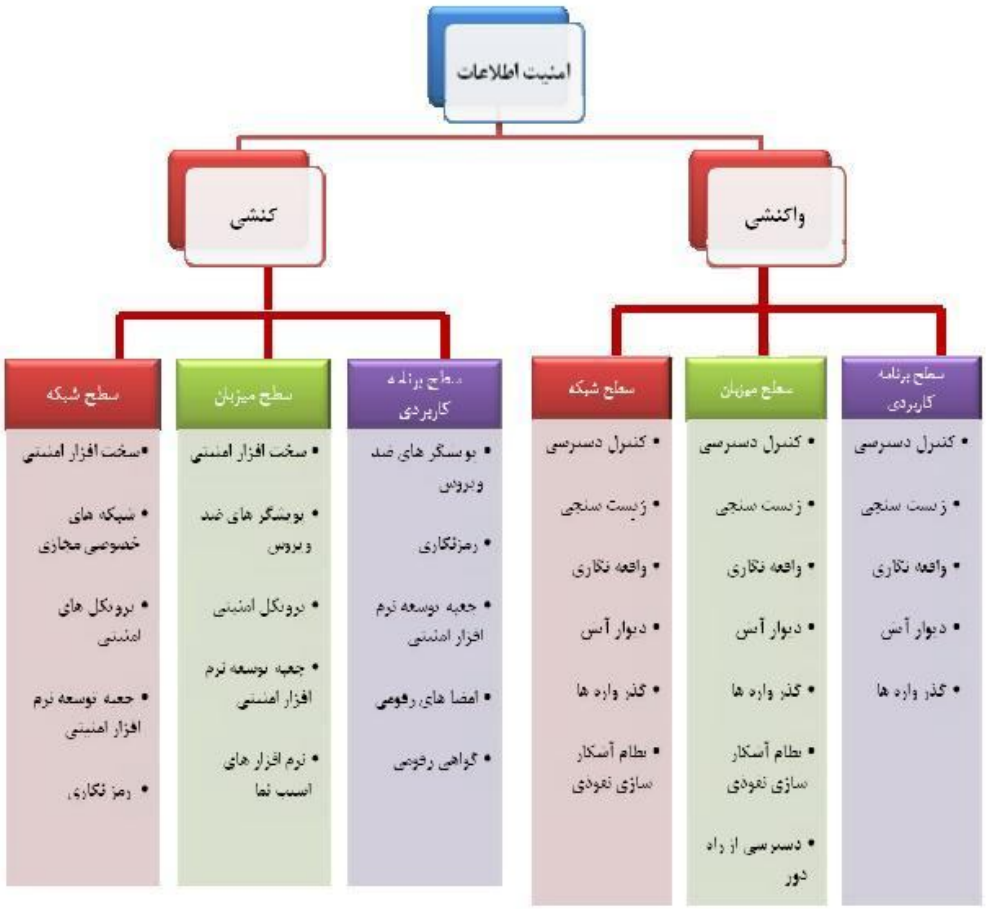
بدین منظور می توان نظام امنیتی را در سطح شبکه و خدمات ارائه شده آن ، در سطح برنامه کاربردی خاص، یا در محیطی که شرایط لازم برای اجرای یک برنامه را فراهم می نماید (سطح میزبان) پیاده کرد.

شکل های زیر فناوری های امنیت اطلاعات را براساس دو ویژگی یاد شده ترسیم می نماید.

7. Proactive
8. Reactive

فناوری های امنیت اطلاعات کنش گرایانه

فناور ی های امنیت اطلاعات واکنشی



فناور ی های امنیت اطلاعات واکنشی و کنشی

شبکه های اجتماعی

شبکه های اجتماعی گونه ایی از وب سایت های اینترنتی هستند که افراد ، گروه ها و سازمان ها ، در آن پیرامون یک یا چند ویژگی مشترک گرد هم می آیند و اطلاعات خود را به اشتراک می گذارند.

با ظهور و بروز تکنولوژی های جدید وب مثل وب 2,0 و وب 3,0 و وب معنایی شبکه های اجتماعی که مبتنی بر تعامل کاربران در ارتباط گیری ، تولید و به اشتراک گذاری محتوا هستند به وجود آمدند تا جایی که مجموع کاربران معروف ترین شبکه های اجتماعی اینترنت مانند FaceBook به بیشتر از یک میلیارد کاربر رسیده است.

در هر کشور و در هر جامعه ایی متناسب با فرهنگ ، تعاملات اجتماعی ، و فعالیت های سیاسی و اقتصادی ، کارکردهای شبکه های اجتماعی متفاوت است. اما برخی کارکردهای شبکه ایی در تمامی جوامع با هم مشترک است.

مهمترین کارکرد های شبکه های اجتماعی ایجاد گروه ها و دسته های ارتباطی پیرامون یک ویژگی خاص، کارکرد های اقتصادی مبتنی بر بازاریابی اجتماعی و کارکرد های سیاسی ، ایجاد کمپین های سیاسی فعالیت دسته ها و گروه های سیاسی ، در یک فضای مجازی است.

شبکه های اجتماعی و حریم خصوصی

حریم خصوصی و محرمانگی اطلاعات شخصی یکی از مهمترین و جنجالی ترین مباحثی است که از ابتدای همگانی شدن اینترنت و بعدتر با ظهور و بروز شبکه های اجتماعی وجود داشته است. تقریبا هیچ کسی پیدا نمی شود که اطلاعات شخصی فردی و خانوادگی خود را به راحتی در اختیار دیگران بگذارد.

در کشورهای غربی سیاست محرمانگی[9] یکی از ارکان کاربری اینترنت است ، به نحوی که قوانین و مقررات آن ایجاب می کند که در تعامل بین وب سایت ها ، خدمات دهندگان اینترنتی و کاربران ، ضمن تعریف سیاست محرمانگی ، این امر به نحو مطلوبی در وب سایت خدمات دهنده به روئیت کاربر رسیده ، حقوق و تکالیف وی یادآور می گردد.

بر اساس سیاست محرمانگی خدمات دهندگان و کاربران توافق می کنند که چه اطلاعاتی از آنان به نمایش درآید یا به هر نحو مورد استفاده قرار گیرد. اگر به هر شکل دیگری خارج از توافق نامه ی محرمانگی اطلاعات کاربران مورد سوء استفاده قرار گیرد ، کاربران امکان اقامه ی دعوی و طرح شکایت را علیه وب سایت خدمات دهنده خواهند داشت.

معمولا در شبکه های اجتماعی جزیی ترین اطلاعات کاربران نیز قابل دریافت و انتشار است مانند : علاقمندی ها ، میزان تحصیلات ، ارتباطات خانوادگی و دوستانه ، شغل ، محل زندگی ، محل تولد ، شماره تماس و ... .

9.Privacy Policy

اگرچه برخی از شبکه های اجتماعی خارجی با توجه به قوانین و مقررات جمهوری اسلامی ایران و فعالیت های مجرمانه ایی که که در فضای آن سایت ها صورت می گیرد ، خارج از دسترسی عادی قرار دارند اما به هر حال برخی از کاربران ایرانی در این شبکه ها عضویت داشته و به روش های مختلف به آن ها دسترسی دارند.

متاسفانه بررسی ها نشان می دهدکه حضور بسیاری از کاربران ایرانی در فضای شبکه های اجتماعی با مخاطراتی در رابطه با تهدید حریم خصوصی آنان مواجه است و سهل انگاری این دسته از کاربران گاه صدمات جدی به آنان وارد کرده است.

بایستی این حقیقت را پذیرفت که مهم ترین چالش شبکه های اجتماعی اینترنتی موضوع اعتماد به مخاطب یا کسانی است که در لیست دوستان شما قرار می گیرند. مطالعه ی سبک کاربری کاربران نشان می دهد که معمولا درخواست دوستی سایر کاربران را به راحتی می پذیرند. این در حالی است که به طور معمول در این شبکه ها دوست یابی صورت نمی پذیرد و تنها دوستان و آشنایان در فضای واقعی در این فضا نیز نسبت به اتصال و اشتراک گذاری اطلاعات و محتوا اقدام می کنند.

در زیر به برخی از نکات مهم در رابطه با تامین امنیت در فضای شبکه های اجتماعی اشاره می شود :

1. مراقب جعل هویت باشید؛ یکی از مهم ترین موضوعاتی که کاربران را تهدید می کند جعل هویت است به خصوص در زمانی که کاربر در زمینه ایی جزو افراد سرشناس باشد. در صورتی که در حیطه ی کسب و کار یا حوزه ی اجتماعی خود فرد سرشناسی هستید ممکن است افراد دیگری با سوء استفاده از محتوا و اطلاعاتی که شما به صورت عمومی به اشتراک گذاشته اید با نام و هویت جعلی شما و با راه اندازی صفحات مشابه دست به اخاذی ، کلاه برداری و اقدامات مجرمانه بزنند. از این

رو هوشیاری در حفظ اطلاعات و محتواهای خصوصی کاملا اهمیت دارد. در صورتی که متوجه جعل هویت خود شدید موضوع را به پلیس فتا اعلام کنید.

2. اسرار ملی و سازمانی را افشا نکنید؛ سازمان ، شرکت یا موسسه ای کـه در آن کـار مـی کنیـد قطعـا اطلاعاتی در اختیار شما می گذارد که انتظار دارد شما آن ها به صورت محرمانه نزد خود نگـه داریـد. برخی از شبکه های اجتماعی نیز طوری طراحی شدند که ناخواسته افراد را به ورطه ی جاسوسی می کشانند. برای مثال : برخی از شبکه های اجتماعی مبتنی بر جانمایی که افراد نام ونشان خیابان هـا ، اماکن و مراکز مهم را به اشتراک می گذارند ، عملا کارکرد جاسوسی دارند و به راحتی این امکـان را به دشمن می دهند که به این اطلاعات بدون کمترین زحمتی دسترسی پیدا کنند.
3. مراقب کرم های رایانه ایی و تروجـان هـا باشـید؛ برخـی از خـدمات شـبکه هـای اجتمـاعی ماننـد Application ها در دل خود کرم های رایانه ایی و تروجان هـا را انتـشار مـی کننـد. بنـابراین در فضای این شبکه ها به هر خدمتی که از سوی کاربران دیگر به شما پیشنهاد می شود اعتماد نکنید.
4. توافق نامه های محرمانگی اطلاعات را مطالعه کنید؛ با مطالعه ی این توافق نامه ها متوجه خواهیـد شد که کدام دسته از اطلاعاتی که شما به اشتراک می گذارید ممکن است در معرض خطر قرار گیرد که به شما کمک می کند با دقت بیشتری از شبکه های اجتماعی استفاده کنید.
5. به هر ناشناسی اعتماد نکنید؛ فضای شبکه های اجتماعی مملو از کاربرانی است که بـا هویـت هـای جعلی و برای مقاصد خاص مانند کـلاه بـرداری ، اشـاعه ی فحـشاء و سـایر اقـدامات غیرقـانونی و مجرمانه نسبت به ارتباط برقرار کردن با کابران اقدام می کنند. از این رو از پذیرفتن افرادی کـه بـا هویت ، تصاویر و طرح مطالب اغوا کننده سعی در ارتباط برقـرار کـردن و افـزودن شـما بـه لیـست دوستان خود یا علاقمندان صفحه ی خود را دارند ، اجتناب کنید.
6. تنظیمات حریم خصوصی را انجام دهید؛ تمامی شبکه های اجتماعی ابزارهایی را در اختیار شـما مـی گذارند که حوزه ی حریم خصوصی خود را تنظیم کنید. با استفاده از این ابزارها می توانیـد بـا خیـال راحت تر نسبت به اشتراک گذاری اطلاعات با دوستان خود اقدام کنید و دسترسی دیگران را محـدود کنید.

ایجاد یک رمز عبور امن

تقریبا ما برای انجام دادن بیشتر کارهای خود در اینترنت به رمزعبـور نیـاز داریـم. بنـابر ایـن داشـتن یـک رمزعبور خوب و ایمن می تواند امنیت ما را در فضای سایبری تا حدود زیادی حفـظ کنـد. رمزهـایی کـه اکثـر کاربران استفاده می کنند به احتمال زیاد یکسری اعداد و حروف است که یادآور نکته ، تـاریخ تولـد و یـا یـک اسم منحصر به فرد است.

در سال 2011، تعداد 37000 نفر از کاربران سونی، حساب های اینترنتی شان هک شـد و اطلاعـات آن‌هـا توسط LulzSec در اینترنت منتشر شد. این اتفـاق در سـال 2010 بـرای 180000 نفـر از اعـضای سـایت Gwaker Mediaرخ داد و اطلاعات آن‌ها نیز لو رفت. اما مطالعاتی که بر روی این رمزها لـو رفتـه انجـام گرفته است، نکات جالب توجهی را آشکار می‌سازد که بد نیست نگاهی به آن‌ها داشته باشیم.

استفاده از رمزهای عبور در چند حساب کاربری: کاربران یک عادت بسیار بد دارند! تعداد بسیار زیادی از این افراد از یک رمز عبور برای حساب‌های مختلف و متعددی بهره می‌گیرند. این عادت شاید سر منشأ تسهیل در حفظ کردن رمزهای عبور را در خود ببیند، اما اگر برای رمز عبور حساب جیمیل، لایو، یاهو میل، پی پل و بسیاری دیگر از سرویس‌ها از یک رمز عبور استفاده کنید، خودتان کار هکرها را راحت‌تر کرده‌اید. بنابراین سعی کنید برای هر حساب اینترنتی خود یک رمز عبور منحصر به فردی داشته باشید.

رمزهایی که از کلمات ساده استفاده می‌کنند: شاید باور نکنید یا حداقل اینکه باور آن برایتان سخت باشد، اما 99% از رمزهای عبور حساب های سونی همگی از کلمات ساده و یا با مفهوم بهره گرفته بودند. این کلمات به طور مثال شامل abc123, summer است. رمز های عبوری که به صورت alpha numeric هستند به راحتی توسط برنامه‌هایی که رمزها را حدس می‌زنند قابل شناسایی و کشف هستند.

متفاوت و عجیب باشید: هکرها برای اینکه بتوانند رمزهای عبور شما را حدس بزنند معمولاً از یک دیکشنری مخصوص استفاده می‌کنند که در واقع انباره ای است از کلمات. بسیار عجیب بود اما 60% رمزهای عبوری که از 37000 رمز لو رفته همگی در این دیکشنری‌ها وجود داشتند. این نشان می‌دهد که کاربران از رمزهای ساده و با مفهوم استفاده می‌کنند که امکان حدس زندن آن‌ها وجود دارد.

کاربران در انتخاب رمز عبور سخت تنبل هستند: مطالعات نشان می‌دهد که کاربران در استفاده از کاراکترهای **! % ^ @ # $ [+** در رمزهای عبور بسیار تنبل هستند و معمولاً رمزهایی بین 6 تا 8 کاراکتری انتخاب می‌کنند. با این اوصاف شما هکرها را به میهمانی ویژه ای دعوت می‌کنید.

اما چگونه می‌توان رمزهای بهتر و قوی‌تری داشت؟

رمز عبور خود را با حروف اول کلمات یک جمله یا متنی که دوست دارید آغاز کنید. به طور مثال:

Can't See the Forest Through the Trees : cstfttt

If the Shoe Fits, Wear It : itsfwi

پسوردها را طولانی‌تر کنید. معمولاً رمزهای عبور 6 تا 8 کاراکتری برای حدس زده شدن جزو رمزهای راحت به حساب می‌آیند. می‌توانید بخش اول را با یک کلمه که مفهوم بیشتری برایتان دارد به هم بچسبانید و طولانی‌تر کنید.

cstftttGmail

puosuVista

itsfwiEpinions

رمز عبورتان را با کمی دست‌کاری پیچیده تر کنید. به طور مثال یکی از حروف آن را با یک کاراکتر غیـری حرفی- عددی عوض کنید.

CstftttGm@il

Puo5uVista

1tsfwiEpinions

از همه این موارد مهم‌تر، عوض کردن دوره ای رمزهای خودتان است. شـما بایـد در یـک بـازه ی زمـانی خاص تمام رمز های خودتان را عوض کنید. در غیر این صورت باز هم امکان حدس زدن رمزتان را به هکرهـا داده‌اید!

بعضی وقت‌ها گذرواژه‌ها به تنهایی امنیت کافی ایجاد نمی‌کنند. بسیاری از سازمان‌ها استفاده از روش تأیید دو مرحله‌ای، مانند ارسال پیام به تلفن همراه جهت تأیید تبادلات بانکی آنلایـن را آغـاز کـرده‌انـد. در بعـضی شرایط، برای مشاغل استفاده از این روش برای ایجاد یک لایه امنیتی دیگر منطقی است.

روشهای تامین امنیت کامپیوتر در اینترنت

1. ابتدا کل اطلاعاتی را که در هاردتان ذخیره نموده اید و داشتن آنها را ضروری مـی دانیـد در حافظـه جانبی اعم از هارد اکسترنال (خارجی) سی دی یا فلش مموری ، بسته به حجـم اطلاعـات ، ذخیـره نموده سپس همان حافظه های جانبی را از کامپیوتر جدا نمایید.
2. سپس کل درایوها را فرمت از نوع کند نمایید.
3. سپس یک سی دی سیستم عامل دارای برنامه بوت ایبل خودکار، در دستگاه قرار داده کـامپیوتر را Restart نموده و برنامه بوت را اجرا نمایید کل درایو ها را حذف نموده و از بین ببرید چون بعـضی فایل های جاسوس بین فاصله دو درایو مخفی می شوند و نرم افزارهای امنیتی نمـی تواننـد آنهـا را شناسایی نمایند. سپس مجدداً پارتیشن بندی (درایو سازی) نموده و سیـستم عامـل و برنامـه هـای کامپیوترتان را نصب نمایید.
4. پس از ساخت Connection اینترنت، در اولین مراجعه در اینترنت سریعاً یک نرم افـزار امنیتـی از یکی از سایت های معتبر دانلود و نصب نمایید سپس نرم افزار را به روز رسانی نمایید.
5. یک فلش مموری چندین گیگابایتی به کامپیوتر خود وصل نموده و مـن بعـد هرگونـه فـایلی کـه از اینترنت دانلود می‌نمایید در آن ذخیره نمایید.
6. هنگام وارد نمودن رمز خود در سایت های بانکی و یا مـشابه (خریـد اینترنتـی) کـه از شـما شـماره حساب و رمزتان را می خواهند حتما از کیبورد مجازی آن سایت و یـا کیبـورد کامپیوترتـان اسـتفاده کنید. از ذخیره اطلاعات فوق در کامپیوتر از طریق کلیک کردن سایت مربوطه خودداری نمایید مگـر آنکه نیاز باشد. در این صورت باید به یاد داشته باشید که پس از خروج از آن سایت حتمـاً و سـریعاً از

طریق بخش Internet Option واقع در کنترل پنل کامپیوترتان رموز (و نیز نشانی سایت های بازدید شده تان را چون برای بعضی جاسوس ها اینکه شما وارد چه سایت هایی می شوید مهم است) کاملاً پاک نمایید. حتماً حتی پس از خروج از اینترنت باز همین روش را اجراء کنید.

7. به یاد داشته باشید که بیشترین فایل های جاسوس در سایت های غیر اخلاقی و سایت های خبری و سیاسی وجود دارند بنابراین باید در مراجعه با اینگونه سایت ها احتیاط نمایید.

8. اشخاص ناشناخته را عضو اد لیست (یاهو) مسنجرتان نکنید و هر ایمیلی را باز نکنید. از هر شخصی چه به صورت آن لاین و چه به صورت ایمیل و حتی سی دی، فایل قبول نکنید. همه نرم افزارهای امنیتی نمی توانند به صورت قطعی فایل های جاسوسی را شناسایی نمایند.

9. من بعد هیچ گونه فایلی را که مایل نیستید دیگران آنرا از کامپیوترتان سرقت کنند در کامپیوترتان نگهداری نکنید چه در هارد و چه در سی دی رام کامپیوترتان. در حقیقت شما باید کامپیوترتان را خالی از هرگونه فایلی که مایل به سرقت آن ها نیستید نموده و در صورتی که می خواهید محتوای سی دی را ملاحظه نمایید باید اینترنت را قطع نموده و پس از پایان کار به یاد داشته باشید که سی دی را از سیدی رام خارج نمایید.

10. هنگامی که کامپیوتر به اینترنت متصل نیست اطلاعات داخل فلش مموری که از اینترنت دانلود و ذخیره موقت نموده‌اید را در هارد اکسترنال (خارجی) یا سی دی رایت نموده و از کامپیوتر جدا کنید و کل فلش مموری را مجدداً فرمت نموده من بعد هنگام مشاهده محتوای فلش مموری، سی دی و هارد اکسترنال و هارد کامپیوتر دیگری، اینترنت را قطع نمایید.

11. ضمن اینکه همیشه هر فایلی را قبل از باز نمودن باید با نرم افزار امنیتی خود اسکن و ویروس یابی کنید حتماً اسامی فایل ها و فولدرهای مهم در هارد و فلش مموریتان را هم به صورت نامشخص و منحرف کننده بگذارید مثلاً به جای واژه عکسهای من بنویسید عکسهایی از شهر تبریز.

12. چنانچه لازم است که از هارد کامپیوترتان استفاده نمایید همیشه به یاد داشته باشید اطلاعاتی را در هارد آن ذخیره کنید که سرقت و یا دستکاری آن ها برای شما دردناک نباشد. هر هفته کامپیوتر خود را به وسیله ی باد نیمه گرم و شدید یک سشوار و سپس یک جارو برقی غبار روبی نمایید. چنانچه برای شما امکان داشته باشد یک سیستم عامل کاملاً Original تهیه نمایید چون بعضی از خود سیستم عامل ها و برنامه های کامپیوتر و نیز یاهو مسنجر و امثال آن ها هم دارای فایل‌های جاسوسی هستند.

به طور کلی یک دستگاه کامپیوتر را مختص ورود به اینترنت نمایید و یک دستگاه دیگر مخصوص کارهای معمولی روزانه خود (کار با هارد و سی دی و فلش و ذخیره ها و تبادل های اطلاعاتی تان). شما با اجرای این موارد امنیتی می توانید تا میزان بسیار زیادی کامپیوترتان را از دسترس هکرها و جاسوسان در امان نگهدارید.

نکاتی برای پیشگیری از وقوع جرائم اینترنتی

استفاده از اینترنت ، پیامد های مثبت و منفی متعددی را در پی دارد اگر چه نباید فرصت های مثبتی کـه از طریق اینترنت ایجاد شده را نادیده گرفت اما از طرفی نمی‌توان از کنار معضلات ، ناهنجاری ها ، بزهکاری ها و .... بـه وجـود آمـده از ایـن طریـق نیـز بـه سـادگی و بـا بـی تـوجهی گـذر کـرد.

پایگاه اطلاع رسانی پلیس فتا ، بـرای پیـشگیری از وقـوع جـرائم اینترنتـی و سـرقت اطلاعـات کـاربران اینترنتی و والدین آن ها هشدار هایی را به کاربران داده است. شما هم با خواندن این هـشدار هـا مـی توانیـد امنیـت خـود را در زمـان اسـتفاده از اینترنـت افـزایش دهیـد.

- از رمزهای عبور متعدد برای امور مختلف استفاده کنید تا از لو رفتن آن ها جلوگیری شود.
- در زمان استفاده از اینترنت در مکان‌های عمومی حتماً از محل های معتبر استفاده کنید.
- رایانه های خانگی را در محلی از منزل قرار دهید که در مقابل دید اعضاء خانواده باشد.
- ساعاتی راکه بچه ها با کامپیوتر کار می‌کنند محدود کنید.
- از ذخیره و نگهداری اطلاعات شخصی در سیـستم هـای رایانـه و گوشـی‌هـای تلفـن همـراه جـدا" خودداری کنید.
- از ارسال اطلاعاتی در اینترنت که هویت شما را آشکار می‌کند خودداری کنید.
- هیچگونه اطلاعاتی را با افراد غریبه که بصورت آن لاین معرفی می‌شوند به اشتراک نگذارید.
- هرگز ضمایم همراه ایمیل‌های افراد ناشناس را باز نکنید.
- حتما از نصب نرم‌افزارهای امنیتی که از سیستم شما در برابر حمـلات ویروسـی هکرهـا و جاسوسـی محافظت کند اطمینان حاصل کنید.
- از رمز عبور طولانی، مشترک از اعداد ،حروف ونشانه‌ها استفاده کنید.
- رمزهای عبور خود را در فواصل زمانی معین تغییر دهید.
- از وجود سه نرم افزار امنیتی ، آنتی‌ویروس ، ابزار ضدجاسوسی و Firewall در سیستم خود اطمینان حاصل کنید.
- تهدیدات و آسیب های اینترنتی را برای فرزندان خود گوشزد کنید.
- در زمان خرید اینترنتی حتما" از واقعی بودن وب‌سایت‌ها اطمینان حاصل کنید.
- در زمان استفاده از اینترنت در محل‌های عمومی حتما قبل از خروج از محل، نسبت به خـروج کامـل از سیستم اطمینان حاصل کنید.
- در زمان خرید تجهیزات رایانه‌ای حتما از محل‌های فروش معتبر و شناخته شده خرید کنید.
- فریب تبلیغات و آگهی‌های فریبنده که هیچگونه برند مشهوری از آن پشتیبانی نمی‌کند را نخورید.
- از قرا دادن آی پی (آدرس سیستم خود) در اختیار دیگران خودداری کنید.

- از پاسخ گویی به ایمیل‌های مشکوک که از سوی افراد ناشناس برایتـان ارسـال مـی‌شـود خـودداری کنید.
- ازشرکت کردن در وب سایت های هرمی تحت عنوان سرمایه گذاری خودداری کنید.
- سیستم‌های معیوب خود را نزد مهندسین تعمیرکار آشنا و مورد اطمینـان ببریـد و از تحویـل سیـستم معیوب به هر تعمیرکاری خودداری کنید.
- از اسکن کردن مدارک و اسناد قانونی خود در سیستم‌های رایانه‌ای شخصی جدا" خودداری کنید.
- از واریز وجه به حساب اشخاص و شرکت‌هایی که آگهی فـروش بـا قیمـت مناسـب زده‌انـد قبـل از بررسی اصالت و هویت واقعی شرکت یا شخص آگهی دهنده جدا خودداری گردد.
- در هر زمان قبل از ورود به اینترنت از نرم‌افزارهای فایروال و آنتی‌ویروس‌های به روز استفاده کنید.
- در هنگام اتصال به اینترنت از طریق گوشی‌های تلفن همراه ، مراقب نامه‌های الکترونیکی مـشکوک و وب سایت های اینترنتی فریبنده باشید.

نتیجه گیری

با توجه به مطالبی که در این مقاله گفته شد در هر کشور امنیت سایبری برای دولـت و مـردم مهـم اسـت. عدم وجود امنیت می تواند تهدید بزرگی برای کشور باشد ، بنابراین باید سرمایه گذاری زیادی بـر روی امنیـت در فضای مجازی انجام شود. در کنار این ، کاربران اینترنتی نیز باید وظایف خود را در زمینـه ی حفـظ امنیـت خود در این فضای مجازی به طور کامل انجام دهند.

منابع

1. زهرا خداقلی ، جرایم رایانه ای ، انتشارات آریان ، تهران
2. مهدی هاتف (کارشناس دفتر تحقیقات کاربردی مع ط.ب.ب ناجا)، چالش ها و چشم اندازهای امنیت در فضای مجازی ، دو ماهنامه توسعه انسانی پلیس، سال ششم، شماره 22 ، فروردین و اردیبهشت 1388
3. پلیس فضای تولید و تبادل اطلاعات ناجا ، امنیت در شبکه های اجتماعی ، 1390
4. http://fa.wikipedia.org
5. http:// cyberpolice.ir