فصل ۹ فرم های آنلاین

هدف های رفتاری

پس از آموزش این فصل، هنرجو می تواند

۱-مفهوم فرم آنلاین را توضیح دهد.

۲-دلایل استفاده کمتر از فرم های آنلاین را بیان نماید.

۳-عناصر تشکیل دهنده HTML را توضیح دهد.

۴-عناصر مختلف یک فرم آنلاین را شناسایی کند.

۵-با فرم آنلاین کار کرده و آنرا پر نماید.

۶-اقدامات امنیتی ویندوز را تشریح کند.

۷-مرورگر وب خود را ایمن نماید.

۱-۹- مقدمه

به راحتی می توان دریافت که رکن اصلی دولت در تعامل با مردم، همان دریافت تقاضای مردم و سپس بررسی آنها و در نهایت در صورت قابل انجام بودن، انجام دادن آنهاست. در این بین اگر هریک از ارکان رسیدگی به تقاضا به خوبی اعمال نشود، موجبات نارضایتی ارباب رجوع که همان مردم است را فراهم می کند. اکثر تقاضاها در دنیای امروز از طریق فرم های سفارشی از مشتری یا ارباب رجوع دریافت می شود و پس از بررسی و مهر و امضای چندین کارمند یا مسئول، نتیجه آن به ارباب رجوع اعلام می شود. فرم می تواند یک صفحه ساده دریافت نام و نام خانوادگی و یا یک فرم پیچیده چند صفحه ای با دریافت انواع عکس، تصویر مدارک و ضمیمه پرونده باشد. ارباب رجوع در سیستم سنتی برای یک درخواست از یک اداره ناچار است ساعتها از وقتش را فقط برای دریافت فرم تقاضا از آن اداره تلف کند.

پس از دریافت فرم هم بایستی فرم تکمیل شده را به همراه مدارک و عکسهای ضمیمه مجدداً به همان اداره ببرد و تحویل مسئول بعدی بدهد و منتظر نتیجه درخواست خودش بماند. این انتظار در برخی موارد به ماهها و سالها می انجامد، چرا که در چرخه اداری، در صورت عدم مسئولیت پذیری یک فرد، کل چرخه زیر سوال خواهد رفت. از طرفی هیچ راه حلی برای آنکه ارباب رجوع روند فعلی و اعمال انجام شده روی فرمش را مشاهده کند وجود ندارد. در این بین باز هم هیچ راه حلی برای کنترل کامل فرم تکمیل شده توسط ارباب رجوع وجود ندارد. به عنوان مثال اگر ارباب رجوع به جای تاریخ دقیق تولد، سال تولد را وارد کند، هیچ راه حلی برای این مساله وجود ندارد، چرا که نمی توان به خاطر یک ماه و روز تولد، مجدداً او را موظف به تکمیل مجدد فرم کرد.

در بعضی موارد یک فرم درخواست از یک اداره به اداره کل یا وزارت جهت تایید ارسال می شود که هزینه های زیادی منجمله هزینه فکس،تلفن، پست، کاغذ، چاپ و ... را بر دولت تحمیل می کند. از همه مهمتر آنکه در طی مدت ارسال فرم به وزارتخانه و سازمان بالاتر، ارباب رجوع بایستی بدون اطلاع از اینکه فرمش در کجاست منتظر بماند و مدام به اداره اولیه مراجعه و از وضعیت درخواستش اطلاع بیابد. برخی موارد حتی هیچ سیستم خبری وجود ندارد که ارباب رجوع را از روند پیگیری فرمش با خبر سازد .مشکل مهم و بسیار بزرگ دیگر در سیستم سنتی غیر قابل پردازش بودن اطلاعات فرمها و غیر قابل جستجو بودن آنها به صورت انبوه است. قطعاً هر چه تعداد فرمها بیشتر شود علاوه بر آنکه

به نیروی انسانی بیشتری نیاز است، دقت و سرعت پردازش به صورت زیادی افت خواهد کرد. از طرف دیگر همه ساله بحران کاغذ در کشور ما توسط مسئولین ذیربط اعلام می شود و هنوز هیچ چاره ای برای کاهش مصرف زائد کاغذ در کشور اندیشیده نشده است .خوشبختانه در طی سالهای اخیر شبکه مخابراتی کشور تحول عمیقی داشته و تعداد کاربران اینترنت در ایران به حد بسیار بالایی رسیده است و این نقطه عطفی برای ایجاد یک تحول ساختاری در نظام اداری دولت است.

دلایل استفاده کمتر از فرم های اینترنتی در ایران می توان به صورت زیر برشمرد:

❊طراحی و تولید یک فرم اینترنتی فرآیندی وقت گیر است. حداقل زمان تولید یک فرم اینترنتی با قابلیت ارتباط با بانک اطلاعاتی و بدون قابلیت گزارش گیری برای یک برنامه نویس متوسط، یک تا سه روز تخمین زده می شود.

❊عدم امکان تغییرات سریع در فرم بدون وجود نیروی متخصص یا پشتیبانی طراح فرم .

❊هزینه بالا : حداقل هزینه طراحی یک فرم اینترنتی برای یک فرم معمولی که اطلاعاتش به ایمیل یا بانک اطلاعاتی ارسال شود بین ۲۵۰۰۰۰ ریال تا ۷۵۰۰۰۰ ریال توسط شرکتهای ارائه کننده خدمات وب انجام می شود .

❊تفکر عدم اعتبار : بسیاری معتقدند در اینترنت اشخاص غیر قابل شناسایی هستند و نمی توان به هویت آنها پی برد ، لذا فرم ارسال شده توسط آنها دارای اعتبار نیست .

❊سرعت اینترنت در ایران پایین است. لذا رغبت به کارکردن در این محیط در بعضی مدیران وجود ندارد .

❊عدم قابلیت مستند سازی: فرمهایی که در اینترنت تکمیل می شوند قابل چاپ و بایگانی بر روی کاغذ نیستند .

❊عدم امکان ایجاد محدودیت مکانی: اینترنت محیطی بدون مرز است که از سراسر دنیا یک صفحه یا فرم قابل دسترس است . به عنوان مثال اگر فرم مربوط به یک وزارتخانه ایران است نباید توسط یک آمریکایی قابل تکمیل باشد و بر روی اینترنت این کنترل وجود ندارد .

❊عدم امکان ایجاد محدودیت دسترسی : به عنوان مثال شاید تکمیل فرم فقط ویژه تعداد خاصی از اعضاء یا همکاران باشد . لذا محیط بدون مرز اینترنت مانع از ایجاد این محدودیت شده است .

اما عمده ترین مساله ، همان وقت گیر بودن و غیر قابل استناد بودن فرمهای وارد شده است .

۹-۲

فرم آنلاین چیست؟

فرم آنلاین از چه اجزایی تشکیل می شود؟

داخل صفحات یک وب سایت اجزای گوناگونی دیده می‌شود که تمام آنها در یک چیز مشترک هستند و آن زبان یا کدی است که آنها را تولید می‌کند که به این زبانHTML یا HyperText Markup Language گویند.

عناصر تشکیل دهنده HTML

HTML زبان وب می‌باشد که دارای عناصر گوناگونی است که با هم تشکیل یک صفحه از سایت را می‌دهند. این عناصر عبارتند از:

(texts & lists) **متن‌ها و لیست‌ها** : نوشته‌های داخل یک صفحه را در برمی‌گیرد.

(images) **عکسها** : عکس‌های داخل یک صفحه که زیبایی خاصی به وب سایتها می‌بخشند.

(tables) **جدول‌ها** : جدول‌ها بهترین عنصر برای سازماندهی و مرتب کردن اطلاعات هستند که نقش اساسی در طراحی یک سایت دارند.

(forms) **فرم‌ها** : عناصری که بیننده سایت به کمک آنها می‌تواند اطلاعاتی را وارد کرده تا ذخیره شده یا فرستاده شود.

(hyperlinks) **نقطه پیوند** : البته این معنی اصلی لغت نمی‌باشد و این عناصر، نقطه پیوند و ارتباط بین دو صفحه از یک سایت یا دو وب سایت متفاوت می‌باشد.

(frames) **چارچوب‌ها** : فریم‌ها یا چارچوب‌ها تنها عناصری هستند که با استفاده از آنها می‌توان چند صفحه اینترنتی را در یک صفحه جای داد.

(multimedia) **چند رسانه‌ای** : به آن صوت و تصویر هم گفته می‌شود، اگرچه از ابتدا صوت و تصویر با HTML نبوده اما در حال حاضر بیشتر مرورگرهای وب از آن پشتیبانی می‌کنند و می‌توان در وب سایت فیلم و موزیک پخش کرد.

(javascript) **جاوا اسکریپت** : یک نوع زبان نوشتاری یا به عبارت بهتر یک نوع کد است که ارتباط نزدیکی با HTML دارد و البته آنها را باید داخل کدهای html بکار برد تا بتوانید یک وب سایت حرفه‌ای با جذابیت بالا طراحی کنید.

(JavaApplets) **جاوا اپلت :** اپلت‌ها برنامه‌هایی هستند که توسط زبان جاوا نوشته می‌شوند و می‌توان آنها را در یک صفحه جاسازی کرد برای کارآیی بالای وب سایت مانند عملیات پیچیده ریاضیات یا ساختن بازی‌ها. زبان برنامه نویسی جاوا خود یک زبان مجزا و دارای محبوبیت خاصی در دنیا می‌باشد که با جاوا اسکریپت فرق دارد.

(style sheets) استایل شیت : این عناصر قابلیت انتقال اطلاعات به عنوان یک الگوی مشترک در بین صفحات را دارد. به عنوان مثال می‌توان یک الگو برای رنگ متن ساخت و سپس آنرا بین صفحاتی به اشتراک گذاشت.

(DHTML) : مخفف دو کلمه Dynamic Html می‌باشد که وظیفه آن روح بخشیدن به صفحات و بالا بردن جذابیت وب سایت می‌باشد، شما می‌توانید با هماهنگی کدهای javascript و Dhtml یک وب سایت پویا و زنده طراحی کنید.

تگ‌های HTML

اولین چیزی که برای برنامه نویسی html باید دانست، اینست که تگ html چیست و چه کاری انجام می‌دهد. تگ‌های html دو نوع هستند، تگ‌های آغازین و تگ‌های پایان دهنده. بطور کل تگ‌ها با دو علامت کوچکتر و بزرگتر، یعنی < > مشخص می‌شوند و بین این دو علامت کد html نوشته می‌شود، مانند:<b>

این یک تگ آغازین است و کد داخل آن به مرورگر ما می‌فهماند که متن بعد از آن باید بصورت حروف ضخیم و bold به بیننده صفحه نشان داده شود و بلافاصله متن مورد نظر را می‌نویسیم و در آخر آن، تگ پایان دهنده که مرورگر بفهمد تا کجا این متن باید بصورت ضخیم نمایش داده شود،

```
<b> This is a bold text. </b>
```

همانطور که مشاهده می‌کنید، تگ‌های پایان دهنده دارای یک علامت Slash (/) میباشد.

اما کار این تگ‌ها چیست؟ مرورگرهای وب مانند Internet Explorer، به علامتهای < > حساس هستند و به محض اینکه به آنها می‌رسند کد داخل آنها را خوانده و عملیات لازم را بر روی متن بعد از آن انجام می‌دهند تا به تگ پایان دهنده برسند. در حقیقت مرورگرها حکم مترجم را برای ما دارند و کلیه تگ‌ها و نوشته‌های داخل آنها را بصورت اطلاعات منظم و قابل فهم در قالب یک صفحه وب برای ما ترجمه کرده و به نمایش می‌گذارند. ما با وارد کردن تگ‌های مناسب، کنترل نمایش صفحه وب را در مرورگرها به دست می‌گیریم. پس باید یاد گرفت که تگ‌های html را چگونه و در کجا نوشت. زبان html هم مانند هر زبان دیگری ساختار و قواعد خاص خود را دارد که در درس‌های دیگر با آنها آشنا می‌شوید.

بنابراین فرم آنلاین یا وب فرم[1] ، **یک صفحه وب و یا قسمتی از یک صفحه وب است که به منظور خاصی طراحی شده و به بازدید کنندگان وب سایت مربوط اجازه می دهد تا اطلاعات درخواست شده یا مطالب خود را درون فیلدهای آن وارد کنند.** سپس اطلاعات وارد شده به وسیله ی برنامه ای به نام Script جمع آوری شده و به آدرس یا آدرس های مشخصی بر روی یک سرویس دهنده ی وب ارسال می شوند. در واقع فرم آنلاین یک فرم الکترونیکی مشابه فرم های کاغذی است که از آن برای ارسال اطلاعات به یک سرویس دهنده ی وب استفاده می شود.

در یک فرم، عناصر مختلفی وجود دارد که عبارتند از:

قاب فیلد

جعبه تاریخ

جعبه متن

جعبه کلمه عبور

فیلدهای مخفی

ناحیه متنی

جعبه انتخاب

دکمه رادیویی

استفاده از فرم های آنلاین معمولاً روش مناسبی برای جمع آوری اطلاعات کاربران و بازدیدکنندگان یک وب سایت ، ممیزی کردن، نظرسنجی ها، ثبت نام یا عضویت در یک سازمان یا یک دوره ی آموزشی، کاهش فرم های کاغذی و .... است. علاوه بر آنکه اطلاعات جمع آوری شده را نیز راحت تر می توان ذخیره و پردازش نمود.

شکل ۱-۹ فرم آنلاین ثبت نام خدمات اینترنتی بانک ملی ایران

همانطور که در شکل ۱-۹ مشاهده می شود، در کنار برخی فیلد ها علامت * وجود دارد که بدین معنی است که تکمیل این فیلدها اجباری است. فیلد اجباری، فیلدی است که مقدار آن حتماً می بایست به وسیله کاربر وارد شود تا فرم مربوطه ارسال گردد. اگر کاربر این فیلدها را خالی بگذارد، معمولاً هنگام ارسال اطلاعات فرم یا بلافاصله پس از عبور از فیلد مربوطه، پیغامی ظاهر می شودکه تاکید می نماید این فیلد باید پر شود. معمولاً فیلد های نام، نام خانوادگی، آدرس پست الکترونیکی، نام کاربری و کلمه ی عبور معمولاً جزو فیلدهای اجباری هستند.

یکی از راه های وارد کردن اطلاعات در فیلدهای یک فرم، استفاده از ماوس است. برای انجام این کار نیز بسته به نوع فیلدهای موجود باید به ترتیب روی گزینه ها یا فرمان های مورد نظر یا داخل تک تک فیلدها کلیک کرده و پس از ظاهر شدن مکان نمای متنی، شروع به وارد کردن اطلاعات نمود. همانطور که ملاحظه می شود، استفاده از این روش به دلیل آنکه به طور همزمان از دست و ماوس استفاده می شود، کمی وقت گیر بوده و زیاد مرسوم نیست. از این رو معمولاً از روش استفاده از صفحه کلید استفاده می شود که در این روش برای حرکت در میان فیلدها از کلید Tab و برای برگشت به فیلد قبلی از کلیدهای Shift+Tab استفاده می شود.

نکته

برای حرکت از یک فیلد به فیلدی دیگر، از کلید Enter استفاده نکنید. زیرا به طور معمول با فشار دادن این کلید تصور می شود که شما می خواهید اطلاعات فرم را ارسال کنید، در حالی که ممکن است هنوز تمام آنرا تکمیل نکرده باشید. در این مواقع معمولاً یک پیام خطا ظاهر می شود. بنابراین توصیه می شود حتی الامکان از کلید Enter استفاده نکنید.

در بسیاری از فرم های آنلاین (به خصوص در فرم هایی که تعداد فیلدهای آن زیاد است)، دکمه مخصوصی وجود دارد که با کلیک بر روی آن شما می توانید تمام اطلاعات فرم را بطور همزمان پاک کرده و سپس اطلاعات جدیدی را وارد نمایید.

پس از تکمیل فرم باید بر روی دکمه ارسال یا Submit کلیک نمود. با کلیک بر روی این دکمه، عملیات ارسال اطلاعات فرم به سرویس دهنده ی وب آغاز می شود. برنامه مخصوصی اطلاعات فرم را جمع آوری کرده و به وسیله یک پست الکترونیکی آنها را به آدرس یا آدرس های مشخصی بر روی یک وب سرور می فرستد. سپس شخص ارسال کننده ی فرم هم صفحه ای موسوم به صفحه تایید را می بیند که به وسیله آن متوجه ارسال فرم می گردد.

مثال: مراحل ساخت پست الکترونیکی در سایت gmail با فرم های آنلاین

اگر بخواهید یک آدرس پست الکترونیکی رایگان داشته باشید، می توانید از سرویس دهنده ی gmail که به مجموعه Google وابسته است، استفاده نمایید. این سرویس یک صندوق پستی ۸۰۰۰ مگابایتی به همراه بسیاری از امکانات جالب و کاربردی در اختیار شما قرار می دهد. برای ساخت یک حساب کاربری در این سایت، لازم است مراحل زیر را طی نمایید:

۱-برقراری ارتباط با اینترنت و ورود به سایت gmail به آدرس www.gmail.com (شکل ۲-۹).

شکل ۲-۹ صفحه ورودی سایت gmail

۲-در سمت راست صفحه ورودی بخش خاصی برای ورود به حساب کاربری وجود دارد. قسمت sign in برای کاربرانی است که قبلاً در این سایت حساب کاربری ایجاد کرده اند. کاربرانی که می خواهند یک حساب کاربری ایجاد کنند، باید بر روی دکمه Create an account کلیک نمایند. (شکل ۳-۹).

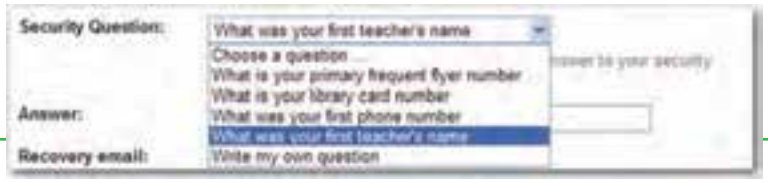
۳-در فرم شما باید برای خودتان یک نام کاربری تعیین کنید. از آنجایی که ممکن است نام کاربری که شما تعیین می کنید، قبلاً به وسیله فرد دیگری در بانک اطلاعاتی gmail ایجاد شده باشد، قابلیتی وجود دارد که شما از این موضوع آگاهی پیدا نمایید و لازم نباشد چندبار فرم را از اول تا آخر پر کنید. (شکل ۴-۹).

شکل ۳-۹ فرم آنلاین ایجاد حساب کاربری در سایت gmail

۴-در بخش سوال امنیتی فرم، شما تعیین می کنید که اگر رمز عبور خود را فراموش کردید، gmail از شما چه سوالی بپرسد. پاسخ به این سوال در بخش Answer درج می شود. (شکل ۵-۹)

شکل ۴-۹ پیشنهادات سایت gmail برای نام کاربری

۵-پس از تکمیل فرم، بر روی دکمه I accept, Create my account کلیک کنید. این دکمه در حقیقت دکمه submit این فرم آنلاین محسوب می شود. در صورتی که خطایی وجود نداشته باشد، شما به صفحه ای مشابه شکل ۶-۹ هدایت می شوید.



شکل ۵-۹ سوال امنیتی برای فراموشی رمز عبور

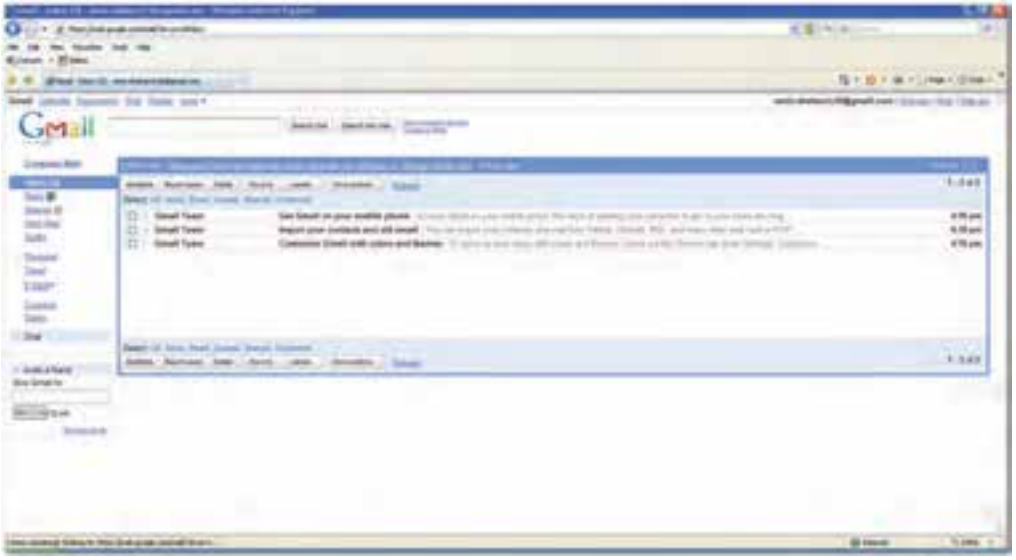
۶-در این قسمت شما می توانید با کلیک بر روی گزینه show me my account به حساب کاربری تان وارد شوید. البته می توانید این صفحه را ببندید و با ورود به صفحه اول (شکل ۲-۹) و تایپ نام کاربری و رمز عبور، به حساب کاربری تان وارد شوید.

شکل ۶-۹ پایان مراحل ایجاد حساب کاربری

۷-پس از ورود به حساب کاربری gmail، صفحه ای شبیه شکل ۸-۹ نمایش داده می شود که در وسط صفحه، خلاصه ای از نامه های موجود در صندوق پستی و محتوای آنها نمایش داده می شود.

شکل ۷-۹ ورود به حساب کاربری

۸-با کلیک بر روی هر نامه الکترونیکی، محتوای کامل نامه به نمایش در می آید. (شکل ۹-۹). حساب کاربری شامل موارد مختلفی است که بررسی آنها به هنرجو واگذار می گردد. برای خروج از حساب کاربری، بر روی گزینه sign out کلیک نمایید.



شکل ۸-۹ حساب کاربری در gmail

شکل ۹-۹ باز کردن نامه الکترونیکی

۹-۳

امنیت در اینترنت

اقدامات امنیتی در سیستم رایانه ای در هنگام حضور در اینترنت چیست؟

گاهی اوقات هنگام گشت و گذار در اینترنت، ممکن است به صفحاتی مانند پنجره های تبلیغاتی برخورد کنید که بطور ناخواسته روی مانیتور شما ظاهر می شوند و می توانند توسط یکسری برنامه های مخفیانه، فایل های جدیدی را روی کامپیوترتان نوشته، فایل های روی آنرا تغییر داده و یا حتی اطلاعات روی دیسک سخت آنرا جمع آوری کرده و کنترل آنرا بدست می گیرند.

در واقع بیشتر این برنامه ها می توانند تمام عملیات اینترنتی شما را ردیابی کنند، از جمله اینکه به دنبال چه می گردید؟ چه چیزی می خرید؟ به چه چیزهایی علاقه دارید؟ شماره کارت اعتباریتان چیست؟ و ...

با استفاده از قابلیت های سیستم عامل ویندوز یا استفاده از نرم افزارهای کمکی، می توان تا حدی جلوی این برنامه‌های نفوذی و مضر را که با عنوان نرم افزارهای جاسوسی[۱] شناخته می شوند، گرفت. یکی از نرم افزارهای مسدود کننده آنها دیوار آتش[۲] می باشد.

دیوار آتش پس از نصب، با قرار گرفتن بین کامپیوتر شما و اینترنت، تمام ارتباطات رد و بدل شده را مورد بررسی قرار داده و جلوی ارتباطات مشکوک را می گیرد. در واقع، نرم افزارهای دیوار آتش به شما اجازه می دهند به صفحات مختلف وب دسترسی پیدا کنید، فایل های مورد نظرتان را بارگزاری نمایید، با دوستانتان گفتگو کنید و ...، بدون آنکه نگران دسترسی غیرمجاز دیگران باشید. بنابراین اگر می خواهید به طور دائم آنلاین باشید، توصیه می شود از این نرم افزارها استفاده کنید. علاوه بر این، سایت های زیادی نیز وجود دارند که می توانند به صورت آنلاین سیستم شما را بررسی کرده و یا بطور مجانی نرم افزارهایی را در اختیار شما قرار می دهند. نرم افزارهای Spyware Doctor متعلق به شرکت نرم افزاری PC Tools و Microsoft Windows Defender و Adware X Eliminator نیز چند نمونه از قدرتمندترین نرم افزارهای ضد جاسوسی هستند.

سیستم عامل ویندوز XP نیز مجهز به یک دیوار آتش موسوم به ICF[۳] است که در هنگام اتصال به اینترنت، مانع از دسترسی سایرین به کامپیوتر شما می شود. با دنبال کردن مراحل زیر می توانید نرم افزار دیوار آتش در ویندوز XP را فعال نمایید:

۱- Spywares ۲- Firewall ۳- Internet Connection Firewall

۱-ورود به پنجره Network Connection از آدرس start/ All Program/ Accessories/ communications/ network Connection

شکل ۱۰-۹ پنجره Network Connection در ویندوز XP

۲-کلیک راست روی آیکن مربوط به اتصال اینترنتی (تفاوتی میان اتصالات مختلف وجود ندارد و تغییرات برای همه اعمال خواهد شد) و انتخاب گزینه properties.

۳-کلیک بر روی زبانه Advanced در کادر محاوره ای ظاهر شده و انتخاب گزینه Setting.

شکل ۱۱-۹

۴-انتخاب زبانه General در کادر محاوره ای Windows Firewall و انتخاب گزینه On. با کلیک بر روی دکمه OK و بستن تمام کادرهای موجود، علامت قفل کوچکی بر روی اتصال اینترنتی شما ظاهر می شود که نشان دهنده ی فعال شدن دیوار آتش ویندوز XP است.

شکل ۹-۱۲

شکل ۹-۱۳

۵-کلیک روی زبانه Advanced در کادر محاوره ای Windows Firewall و سپس کلیک بر روی گزینه Setting در قسمت Security Logging. در اینجا تعداد دفعات تلاش یک نفوذگر به رایانه شما گزارش می شود و وقایع مربوط ثبت خواهد شد.

شکل ۹-۱۴

شکل ۹-۱۵

۶-انتخاب گزینه Log dropped packets و سپس زدن دکمه Ok. شکل ۹-۱۵

۷-کلیک بر روی دکمه Ok در کادر محاوره ای windows Firewall به منظور فعال سازی قابلیت ICF. بعد از انجام این مرحله اگر به اینترنت متصل باشید، پیامی دریافت خواهید کرد که به شما می گوید با ورود دوباره به شبکه، یک فایل ثبت وقایع ایجاد خواهد شد که تمامی فعالیت ها را ثبت می کند.

بجز برنامه ی ICF سیستم عامل ویندوز XP، راه های دیگری نیز برای حفظ امنیت رایانه وجود دارد که یکی از بهترین آنها، ایمن کردن مرورگر می باشد. برای این کار نیز در ویندوز راه های زیادی وجود دارد که یکی از آنها به روزرسانی[1] ویندوز می باشد. انجام این کار باعث ایمن شدن مرورگر خواهد شد. راه دیگر نیز استفاده از برنامه های کمکی مانند ZoneAlarm یا Norton Internet Security یا نرم افزارهای متنوع دیوار آتش مانند Ashampoo و Outpost می باشد که وظیفه آنها بستن حفره های نفوذ به یک سیستم است.

ایمنی مرورگر وب

همانطور که می دانید با نصب سیستم عامل ویندوز XP، شرکت مایکروسافت مرورگر اینترنتی Internet Explorer را بر روی این سیستم عامل در اختیار شما قرار می دهد. این مرورگر دارای ویژگی های امنیتی بسیار بالایی است که اگر آنها را به همراه گزینه های امنیتی ویندوز XP تنظیم کنید، از حریم شخصی شما محافظت بیشتری خواهد شد.

برای تنظیم سطح امنیتی مرورگر اینترنت، مراحل زیر را دنبال کنید:

۱-مرورگر اینترنت خود را راه اندازی کنید.

۲-گزینه Tools / Internet Option را انتخاب کنید تا کادر محاوره ای Internet Option ظاهر شود.

۳-بر روی زبانه Security کلیک نمایید. همانطور که ملاحظه می شود، در این قسمت چهار ناحیه ی قابل تنظیم وجود دارد که هرچه درجه امنیت آنها بالاتر باشد، هنگام گشت و گذار در اینترنت محدودیت های بیشتری اعمال خواهد شد.

۴-برای تغییر سطح امنیتی هر یک نواحی فوق، ابتدا روی ناحیه ی مورد نظر کلیک کرده و سپس به وسیله ی دکمه ی لغزنده موجود در قسمت Security level for this zone، سطح امنیتی مورد نظرتان را انتخاب کنید.

توجه داشته باشید که هرچه سطح امنیتی بالاتری را برای هر ناحیه در نظر

شکل ۱۶-۹

۱- Update

بگیرید، محدودیت بیشتری برای دسترسی به منابع اینترنتی و استفاده آنها خواهید داشت.

۵-پس از اتمام کار، روی دکمه Apply کلیک کنید تا تغییرات جدید اعمال شود.

محافظت در برابر هکرها

به طور کلی، نفوذ به هر سیستم امنیتی را هک[۱] می گویند و هکر[۲] یا نفوذگر فردی است که می تواند به طور غیر مجاز به رایانه دیگران نفوذ کرده و به آنها آسیب برساند. این آسیب می تواند از حذف کردن فایلها گرفته تا دزدیدن اطلاعات با ارزش تجاری یا خصوصی (مانند دزدیدن شماره ی کارت اعتباری یا مشخصات محصولات یا اسناد حقوقی یا سوابق بیمارستانی) را شامل شود. از این رو داشتن کلمات عبور خیلی محرمانه، می تواند به خوبی از صفحات وب و فایل های ذخیره شده در سرویس دهنده های وب محافظت کند. ضمن آنکه رمزدار کردن اطلاعات نیز می تواند از ردیابی آنها در نقل و انتقالات اینترنتی جلوگیری کند، بطوریکه دیگر کسی نتواند بدون داشتن کلید رمز گشایی مناسب، آنها را بخواند.

یکی از متداول ترین سیستم های رمزگزاری، پروتکل SSL نام دارد که با رمز کردن اطلاعات، از آنها در نقل و انتقالات بین مرورگرها و سرویس دهنده های وب محافظت می کند.

البته باید دانست که پروتکل SSL فقط ارتباط بین مرورگرها و سرویس دهنده های وب را امن می نماید و برای محافظت از اطلاعات شما در سرویس دهنده های وب کاری را انجام نمی دهد. بنابراین در مورد شرکت های بزرگی که می توانند برای خود سرور و خطوط ارتباطی اختصاصی تهیه کنند، در صورتی که شما هم به آنها اعتماد دارید، مشکلی ایجاد نخواهد شد. اما معمولاً بسیاری از شرکت های کوچک توانایی خرید سرورهای اختصاصی را ندارند و مجبورند از سرورهای شخص ثالث یا شرکت دیگری استفاده کنند و این درست همان جایی است که عدم امنیت به وجود می آید، زیرا شما مجبورید به میزبانی اطمینان کنید که هیچ شناختی از آن ندارید و واقعاً هیچ تضمینی هم برای این ارتباط وجود ندارد.

بیشتر سرویس دهنده های وب، برنامه ای به نام Form Mail را در اختیار سرویس گیرنده های خود قرار می دهند. این برنامه محتوای فرم های آنلاین را گرفته و از طریق یک پست الکترونیکی آنها را به شرکت یا سازمان مربوطه ارسال می کند. در حالی که برای این پیام نه محافظی وجود دارد و نه اطلاعات آن رمز گزاری می شود.

البته راه های زیادی برای تامین امنیت واقعی در معاملات الکترونیکی وجود دارد. به عنوان مثال، نسخه هایی از برنامه Form Mail وجود دارد که از ایمیل های رمزدار شده استفاده می کند. برخی از سرویس دهنده های وب نیز

۱- Hack ۲- Hacker

اطلاعات را در جایی قرار می دهند که مستقیماً از طریق وب نمی توان به آنها دسترسی پیدا کرد.

همانطور که در فصل های قبلی اشاره کردیم، برای فهمیدن اینکه سایت یا معامله مورد نظر امن است یا خیر، اگر در آدرس مرورگر به جای پروتکل http حروف https ظاهر شد یا اگر در گوشه ی پایین پنجره ی مرورگر یک علامت قفل نمایش داده شد، نشان دهنده ی آن است که شما در حال استفاده از یک وب سایت امن یا یک اتصال رمزدار مطمئن هستید. یک راه دیگر نیز این است که که به آدرس فیزیکی، سابقه و سیاست های آن شرکت نگاهی بیندازید و مطمئن شوید که در آن ذکر شده است که هرگز اطلاعات یک مشتری بدون رمزگزاری از طریق اینترنت جابجا نخواهد شد.

در تجارت الکترونیکی، بانکداری الکترونیکی و سایر وب سایت هایی که از پروتکل SSL استفاده می کنند، برای بررسی صحت و اعتبار اطلاعات از گواهی نامه های دیجیتالی استفاده می شود. این گواهی نامه ها معمولاً به وسیله مراجع ذی صلاح صدور گواهینامه به شکلی کاملاً قانونی و در چهارچوبی کاملاً فنی صادر می شوند و به آنها **کلید عمومی زیر ساخت**[1] گفته می شود. بنابراین بهترین حالت امنیت در یک معامله اینترنتی این است که:

- فرم سفارش امن باشد.
- اطلاعات بصورت رمزدار شده در بین رایانه های مشتری و سرویس دهنده های وب رد و بدل شود.
- در سرویس دهنده های وب، اطلاعات به صورت رمزدار شده در یک پایگاه داده ذخیره شوند.
- فروشنده به وسیله یک ایمیل از رسیدن سفارش ها مطلع شود.
- هیچ گونه اطلاعات مهم و حساسی در ایمیل ها قرار نگیرد.
- فروشنده اطلاعات را از طریق یک ارتباط امن بازیابی کند.

بطور کلی، هیچ روشی به طور صددرصد رایانه و اطلاعات شما را ایمن نمی کند، بلکه فقط احتمال هک شدن آنها را پایین می آورد. برخی از متداول ترین روشهای هک کردن عبارتند از:

- رایج ترین روش هک کردن، حدس زدن رمز عبور است.
- روش رایج دیگر، خواندن رمز عبور از روی دست کاربر در هنگام تایپ کردن است.
- یک روش دیگر ظاهر شدن فرمی مانند فرم Yahoo! است که در آن به ظاهر از شما خواسته می شود به منظور اطمینان از صحت سرویس دهی یا هر چیز دیگری مانند آن، رمز عبور خود را یکبار دیگر وارد کنید. با انجام این کار، معمولاً بلافاصله رمز عبور شما برای هکر ایمیل می شود.
- روش دیگر، حدس زدن جواب سوالی است که شما انتخاب کرده اید تا در صورت فراموش کردن رمزتان از شما پرسیده شود.

۱- PKI: Public Key Infrastructure

❊روش دیگری که کمی تخصصی تر بوده و هر کسی نمی تواند از آن استفاده کند، فرستادن یک فایل آلوده به ویروس یا تروجان[1] به سیستم شما است که با اجرای این فایل، فایل مورد نظر هکر نیز در حافظه ی رایانه جای می گیرد و با هر بار روشن شدن رایانه، در حافظه بارگزاری می گردد. بنابراین با پاک کردن فایل اولیه باز هم مشکل حل نمی شود. این فایل معمولاً رایانه شما را به شکل یک سرور درآورده و یکی از درگاه های آن را برای استفاده هکر باز می گذارد. سپس هکر می تواند با پیدا کردن آدرس IP شما و اتصال به درگاه مربوط، در زمانی که شما هم به اینترنت وصل شده اید، کنترل رایانه شما را بدست بگیرد. به عنوان مثال می تواند رمزهای شما را دزدیده و یا حتی رایانه شما را خاموش کند. البته ارسال فایل همیشه به صورت آنلاین نیست و ممکن است یک هکر که با شما آشناست، فایل مورد نظرش را مستقیماً بر روی رایانه شما اجرا کند. (البته برخی از تروجان ها درگاهی را باز نمی گزارند، بلکه فقط از طریق یک ایمیل، رمزها و اطلاعات محرمانه را برای هکر ارسال می کنند).

با بکارگیری روش های ساده، می توان ایمنی رایانه را در برابر هکرها و حملات اینترنتی، بالا برد:

۱-رمزی انتخاب کنید که حدس زدن آن کار آسانی نباشد. نام، نام خانوادگی، شماره تلفن، شماره شناسنامه، تاریخ تولد و ترکیبی از اینها، معمولاً اولین کلماتی هستند که به ذهن هر کسی می رسند.

۲-سعی کنید در رمز انتخابی خود از ترکیب حروف، اعداد و علامت هایی مانند پرانتز، کروشه، کاما و ... استفاده کنید.

۳-در جاهایی که افراد دیگر حضور دارند، رمزتان را با احتیاط وارد نمایید. برای این کار می توان از کلیدهای منحرف کننده استفاده نمایید. به عنوان مثال یکسری کلید را اشتباهی فشار داده و سپس با کلید های Backspsce یا Delete آنها را پاک کنید تا دیگران متوجه رمز شما نشوند.

۴-بر روی رایانه افرادی که آنها را نمی شناسید یا به آنها اطمینان ندارید، رمزی را وارد نکنید و اگر هم مجبور شدید، با استفاده از کلیدهای ترکیبی Ctrl+Alt+Del و سپس دکمه ی Task Manager پنجره Windows Security، تمام پنجره های مشکوک رابببندید.

۵-هرگز از طریق ایمیل، کلمه عبور و اطلاعات حساس خود را برای کسی نفرستید.

۶-فایل هایی که از طریق افراد ناشناس فرستاده می شوند را به هیچ عنوان باز نکنید.

۷-به هیچ عنوان آدرس، شماره تلفن و منطقه سکونت خود را در اختیار افراد ناشناس در اتاقهای گفتگو قرار ندهید.

۸-قبل از وارد کردن اطلاعات شخصی و محرمانه خود مانند آدرس، شماره حساب بانکی یا شماره کارت اعتباری، ابتدا مطمئن شوید که در یک سایت امن قرار دارید.

۱- تروجان به کدهای مخربی گفته می شود که بر خلاف ویروس های اینترنتی، قابلیت کپی کردن و گسترش خود را ندارند.

۹–از جدید ترین نرم افزارهای ضد ویروس استفاده کرده و بطور مداوم آنها را به روز رسانی کنید.

۱۰–از نرم افزارهای Firewall استفاده نمایید.

سرویس اینترنت را باید از جایی تهیه کرد که امنیت بیشتری دارد. زیرا اگر شبکه ی ISP شما هک شود، دیگر از دست شما کاری ساخته نیست. بهتر است خدمات اینترنت را از جایی دریافت نمایید که سرویس دهنده های آن برای دستیابی به اینترنت از نرم افزارهای Proxy Server استفاده می کنند. همانطور که قبلاً اشاره شد، فایلی که توسط هکر در حافظه رایانه شما اجرا می شود و رایانه شما را به عنوان یک سرور برای حمله هکرها آماده می کند، برای اتصال به اینترنت و فرستادن اطلاعات احتیاج به یک درگاه آزاد دارد. از این رو استفاده از این نوع اینترنت، نه تنها به علت Cache کردن اطلاعات دارای سرعت بیشتری است، بلکه می تواند جلوی برخی از سایت های غیر مجاز و حمله هکرها را بگیرد.

برای تنظیم Proxy یک اتصال Dial–Up مراحل زیر را دنبال کنید:

۱–مرورگر اینترنت خود را راه اندازی کنید.

۲–گزینه Tools / Internet Option را انتخاب کنید تا کادر محاوره ای Internet Option ظاهر شود.

۳–بر روی زبانه Connection کلیک کنید. در این قسمت شما لیست تمام ارتباطات Dial–Up روی رایانه را مشاهده کرده و در صورت نیاز می توانید از دکمه های Add یا Remove، اتصال جدیدی را اضافه کرده یا یکی از اتصال های موجود را حذف نمایید. (در شبکه های محلی از گزینه LAN Setting استفاده می شود).

۴–بر روی دکمه Setting کلیک نمایید.

۵–گزینه Use a Proxy server for this connection را انتخاب کنید.

۶–آدرس و درگاه مربوط به Proxy Server خود را وارد کنید. (این تنظیمات باید از سرویس دهنده خدمات اینترنت گرفته شود.)

۷–در صورت نیاز به تنظیمات پیشرفته تر، روی دکمه Advanced کلیک کنید.

شکل ۹–۱۷

شکل ۹–۱۸

خلاصه مطالب

فرم‌های آنلاین عناصری هستند که بیننده سایت به کمک آنها می‌تواند اطلاعاتی را وارد کرده تا ذخیره شده یا فرستاده شود. به عبارت دیگر، فرم آنلاین یا وب فرم، یک صفحه وب و یا قسمتی از یک صفحه وب است که به منظور خاصی طراحی شده و به بازدید کنندگان وب سایت مربوط اجازه می دهد تا اطلاعات درخواست شده یا مطالب خود را درون فیلدهای آن وارد کنند.

استفاده از فرم های آنلاین معمولاً روش مناسبی برای جمع آوری اطلاعات کاربران و بازدیدکنندگان یک وب سایت ، ممیزی کردن، نظرسنجی ها، ثبت نام یا عضویت در یک سازمان یا یک دوره ی آموزشی، کاهش فرم های کاغذی و .... است. علاوه بر آنکه اطلاعات جمع آوری شده را نیز راحت تر می توان ذخیره و پردازش نمود.

فیلد اجباری، فیلدی است که مقدار آن حتماً می بایست به وسیله کاربر وارد شود تا فرم مربوطه ارسال گردد. اگر کاربر این فیلدها را خالی بگذارد، معمولاً هنگام ارسال اطلاعات فرم یا بلافاصله پس از عبور از فیلد مربوطه، پیغامی ظاهر می شودکه تاکید می نماید این فیلد باید پر شود.

با استفاده از قابلیت های سیستم عامل ویندوز یا استفاده از نرم افزارهای کمکی، می توان تا حدی جلوی برنامه های نفوذی و مضر را که با عنوان نرم افزارهای جاسوسی شناخته می شوند، گرفت. یکی از نرم افزارهای مسدود کننده آنها دیوار آتش می باشد.

نفوذ به هر سیستم امنیتی را هک می گویند و هکر یا نفوذگر فردی است که می تواند به طور غیر مجاز به رایانه دیگران نفوذ کرده و به آنها آسیب برساند. این آسیب می تواند از حذف کردن فایلها گرفته تا دزدیدن اطلاعات با ارزش تجاری یا خصوصی (مانند دزدیدن شماره ی کارت اعتباری یا مشخصات محصولات یا اسناد حقوقی یا سوابق بیمارستانی) را شامل شود.

کوکی ها فایل های متنی کوچکی هستند که به وسیله ی برخی از وب سایت ها بر روی رایانه شما نوشته می شوند و فقط می توانند به وسیله ی همان وب سایت تولید شده، خوانده شوند.

فعالیت کارگاهی

۱-به سایت www.email.com بروید و با فرم های آنلاین آن، یک حساب کاربری پست الکترونیکی برای خود ایجاد نمایید.

۲-بررسی کنید که ویندوز رایانه شما از چه سطح امنیتی برخوردار است.

۳-چگونه می توانید کد HTML یک صفحه وب را نمایش دهید؟

۴-در اینترنت، چند نرم افزار برای مقابله با هکرها را دانلود کرده و امکانات آنها را با هم مقایسه کنید.

۵-آیا می توانید امکانات امنیتی ویندوز XP را با ویندوز ویستا و ویندوز ۷ مقایسه کنید؟

۶-با یک تحقیق ساده، مشخص کنید برای طراحی یک فرم آنلاین، چه نرم افزارهایی وجود دارد؟

خودآزمایی

۱–فرم ساده را تعریف کنید.

۲–فرم آنلاین چیست؟

۳–چرا در ایران استفاده از فرم های آنلاین کمتر صورت می گیرد؟

۴–چرا در پر کردن فرم های آنلاین نباید از کلید Enter استفاده نمود؟

۵–دیوار آتش در ویندوز چه کاری انجام می دهد؟

۶–بهترین حالت امنیت در یک معامله اینترنتی چه حالتی است؟

۷–چه روش هایی برای بالا بردن ایمنی رایانه در برابر هکرها و حملات اینترنتی کاربرد دارد؟