

فصل ۹ فرم‌های آنلاین

هدف‌های رفتاری

پس از آموزش این فصل، هنرجو می‌تواند:

- ۱- مفهوم فرم آنلاین را توضیح دهد.
- ۲- دلایل استفاده کمتر از فرم‌های 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 آن را پر نماید.
- ۶- اقدامات امنیتی ویندوز را تشریح کند.
- ۷- مرورگر وب خود را ایمن نماید.

۱-۹- مقدمه



به راحتی می‌توان 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 می‌کند. اکثر تقاضاها در دنیای امروز از طریق فرم های سفارشی از مشتری یا ارباب رجوع دریافت می‌شود و پس از بررسی و مهر و امضای چندین کارمند یا مسئول، نتیجه آن به ارباب رجوع اعلام می‌شود. فرم می‌تواند یک صفحه ساده دریافت نام و نام خانوادگی و یا یک فرم پیچیده چند صفحه‌ای 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 می‌انجامد، چرا که در چرخه اداری، در صورت عدم مسئولیت‌پذیری یک فرد، کل چرخه زیر سؤال 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 مسئله وجود ندارد، چرا که نمی‌توان 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 تأیید ارسال می‌شود که هزینه‌های زیادی من جمله هزینه فکس، تلفن، پست، کاغذ، چاپ و ... را بر دولت تحمیل می‌کند. 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 ذی ربط اعلام می شود و هنوز هیچ چاره ای برای کاهش مصرف زائد کاغذ در کشور اندیشیده نشده است. خوشبختانه در طی سال های 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.

۹-۲

فرم آنلاین چیست؟

فرم آنلاین از چه اجزایی تشکیل می شود؟
داخل صفحات یک وب سایت اجزای گوناگونی دیده می شود که تمام آنها در یک چیز مشترک هستند و آن زبان یا کدی است که آنها را تولید می کند که به این زبان HTML یا HyperText Markup Language گویند.

عناصر تشکیل دهنده HTML

HTML زبان وب می باشد که دارای عناصر گوناگونی است که با هم تشکیل یک صفحه از سایت را می دهند. این عناصر عبارت اند از:

- (texts & lists) **متن ها و لیست ها:** نوشته های داخل یک صفحه را در برمی گیرد.
- (images) **عکس ها:** عکس های داخل یک صفحه که زیبایی خاصی به وب سایت ها می بخشند.
- (tables) **جدول ها:** جدول ها بهترین عنصر برای سازماندهی و مرتب کردن اطلاعات هستند که نقش اساسی در طراحی یک سایت دارند.
- (forms) **فرم ها:** عناصری که بیننده سایت به کمک آنها می تواند اطلاعاتی را وارد کرده تا ذخیره شده یا فرستاده شود.
- (hyperlinks) **نقطه پیوند:** البته این معنی اصلی لغت نمی باشد و این عناصر، نقطه پیوند و ارتباط بین دو صفحه از یک سایت یا دو وب سایت متفاوت می باشد.
- (frames) **چارچوب ها:** فریم ها یا چارچوب ها تنها عناصری هستند که با استفاده از آنها می توان چند صفحه اینترنتی را در یک صفحه جای داد.
- (multimedia) **چند رسانه ای:** به آن صوت و تصویر هم گفته می شود، اگرچه از ابتدا صوت و تصویر با HTML نبوده اما در حال حاضر بیشتر مرورگرهای وب از آن پشتیبانی می کنند و می توان 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 کارایی 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، این است که تگ html چیست و چه کاری انجام می‌دهد؟ تگ‌های html دو نوع هستند، تگ‌های آغازین و تگ‌های پایان دهنده. به طور کل تگ‌ها با دو علامت کوچک‌تر و بزرگ‌تر، یعنی < > مشخص می‌شوند و بین این دو علامت کد html نوشته می‌شود، مانند: این یک تگ آغازین است و کد داخل آن به مرورگر ما می‌فهماند که متن بعد از آن باید به صورت 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 به صورت ضخیم نمایش داده شود،

 This is a bold text.

همان‌طور که مشاهده می‌کنید، تگ‌های پایان‌دهنده 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 پایان‌دهنده برسند. در حقیقت مرورگرها حکم مترجم را برای ما دارند و کلیه تگ‌ها و نوشته‌های داخل آنها را به صورت 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 ، 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 برنامه ای به نام Script جمع آوری شده و به آدرس یا آدرس های مشخصی بر روی یک سرویس دهنده 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 وب استفاده می شود.

در یک فرم، عناصر مختلفی وجود دارد که عبارت اند 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 بازدید کنندگان یک وب سایت، ممیزی کردن، نظرسنجی ها، ثبت نام یا عضویت در یک سازمان یا یک دوره 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 ۹-۱ فرم آنلاین ثبت نام خدمات اینترنتی

بانک ملی ایران

The image shows a web form titled "فرم ثبت نام خدمات اینترنتی" (Internet Services Registration Form). It is divided into several sections:

- اطلاعات شخصی (Personal Information):** Includes fields for name, surname, date of birth, gender, and a dropdown for marital status.
- اطلاعات تماس (Contact Information):** Includes fields for phone number, email, and address.
- اطلاعات خدمات (Service Information):** Includes a dropdown for service type and a checkbox for "I agree with the terms and conditions".
- اطلاعات امنیتی (Security Information):** Includes a dropdown for security level and a checkbox for "I agree with the security policy".
- اطلاعات مالی (Financial Information):** Includes a dropdown for payment method and a checkbox for "I agree with the payment policy".

At the bottom, there is a "ثبت نام" (Register) button.

همان‌طور که در شکل ۹-۱ مشاهده می‌شود، در کنار برخی فیلدها علامت * وجود دارد که بدین معنی است که تکمیل این فیلدها اجباری است. فیلد اجباری، فیلدی است که مقدار آن حتماً می‌بایست 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 می‌شود که تأکید می‌نماید این فیلد باید پر شود. معمولاً فیلدهای نام، نام خانوادگی، آدرس پست الکترونیکی، نام کاربری و کلمه عبور معمولاً جزو فیلدهای اجباری هستند.

یکی از راه‌های 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 گزینه‌ها یا فرمان‌های مورد نظر یا داخل تک تک فیلدها کلیک کرده و پس از ظاهر شدن مکان‌نمای متنی، شروع به وارد کردن اطلاعات نمود. همان‌طور که ملاحظه می‌شود، استفاده از این روش به دلیل آنکه به طور همزمان از دست و ماوس استفاده می‌شود، کمی وقت‌گیر بوده و زیاد مرسوم نیست. از این رو معمولاً از روش استفاده از صفحه کلید استفاده می‌شود که در این روش برای حرکت در میان فیلدها از کلید Tab و برای برگشت به فیلد قبلی از کلیدهای Shift+Tab استفاده می‌شود.

نکته

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

در بسیاری از فرم‌های آنلاین (به خصوص در فرم‌هایی که تعداد فیلدهای آن زیاد است)، دکمه مخصوصی وجود دارد که با کلیک بر روی آن شما می‌توانید 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 وب آغاز می‌شود. برنامه مخصوصی اطلاعات فرم را جمع‌آوری کرده و به وسیله یک پست الکترونیکی آنها را به آدرس یا آدرس‌های مشخصی بر روی یک وب سرور می‌فرستد. سپس شخص ارسال‌کننده فرم هم صفحه‌ای موسوم به صفحه تأیید را می‌بیند که به وسیله آن متوجه ارسال فرم می‌گردد.

مثال: مراحل ساخت پست الکترونیکی در سایت gmail با فرم‌های آنلاین

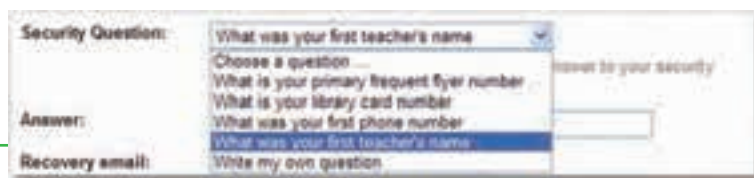
۳- در فرم شما باید برای خودتان یک نام کاربری تعیین کنید. از آنجایی که ممکن است نام کاربری که شما تعیین می کنید، قبلاً به وسیله فرد دیگری در بانک اطلاعاتی gmail ایجاد شده باشد، قابلیت وجود دارد که شما از این موضوع آگاهی پیدا نمایید و لازم نباشد چندبار فرم را از اول تا آخر پر کنید. (شکل ۹-۴).

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

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

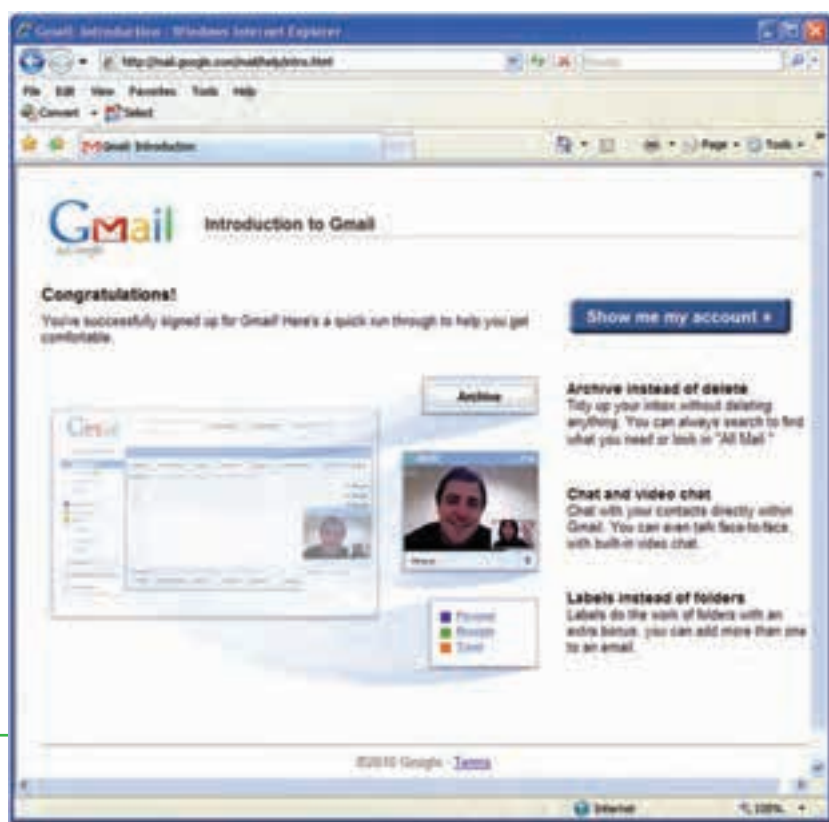
شکل ۹-۴ پیشنهادات سایت gmail برای نام کاربری

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 ۹-۶ هدایت می شوید.



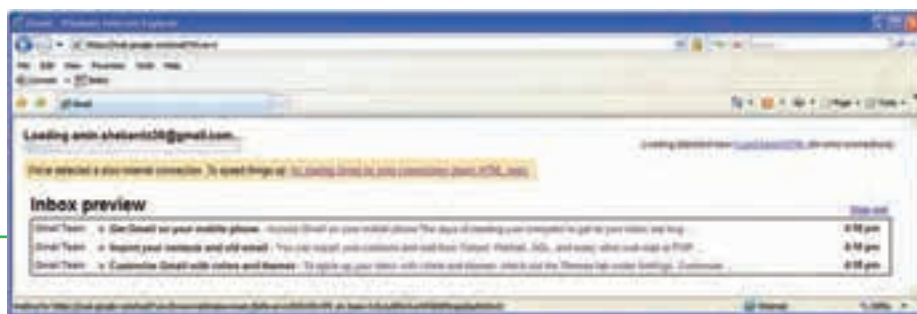
شکل ۹-۵ سؤال امنیتی برای فراموشی رمز عبور

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 ببینید و با ورود به صفحه اول (شکل ۹-۲) و تایپ نام کاربری و رمز عبور، به حساب کاربری تان وارد شوید.



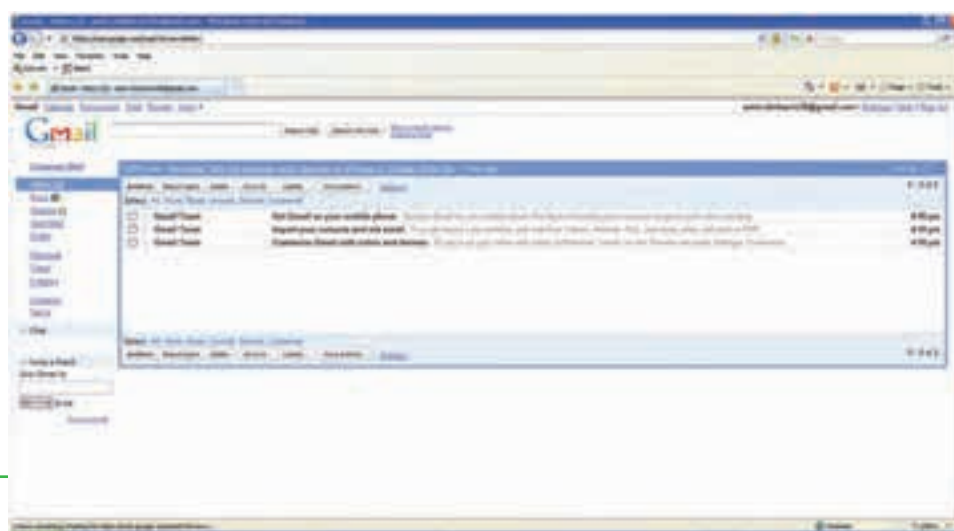
شکل ۹-۶ پایان مراحل ایجاد حساب کاربری

۷- پس از ورود به حساب کاربری gmail، صفحه‌ای شبیه شکل ۹-۸ نمایش داده می‌شود که در وسط صفحه، خلاصه‌ای از نامه‌های موجود در صندوق پستی و محتوای آنها نمایش داده می‌شود.



شکل ۹-۷ 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 هنجار و اگذار می گردد. برای خروج از حساب کاربری، بر روی گزینه sign out کلیک نمایید.



شکل ۹-۸ حساب کاربری در gmail



شکل ۹-۹ بازکردن نامه الکترونیکی

اقدامات امنیتی در سیستم رایانه‌ای در هنگام حضور در اینترنت چیست؟

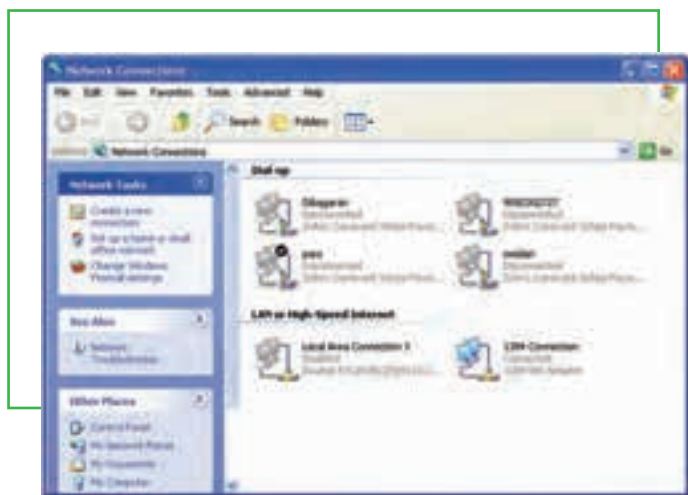
گاهی اوقات هنگام گشت و گذار در اینترنت، ممکن است به صفحاتی مانند پنجره‌های تبلیغاتی برخورد کنید که به‌طور ناخواسته روی مانیتور شما ظاهر می‌شوند و می‌توانند توسط یکسری برنامه‌های مخفیانه، فایل‌های جدیدی را روی کامپیوترتان نوشته، فایل‌های روی آنرا تغییر داده و یا حتی اطلاعات روی دیسک سخت آنرا جمع‌آوری کرده و کنترل آنرا به‌دست می‌گیرند.

در واقع بیشتر این برنامه‌ها می‌توانند تمام عملیات اینترنتی شما را ردیابی کنند، از جمله اینکه به دنبال چه می‌گردید؟ چه چیزی می‌خرید؟ به چه چیزهایی علاقه دارید؟ شماره کارت اعتباری تان چیست؟ و ...

با استفاده از قابلیت‌های سیستم عامل ویندوز یا استفاده از نرم افزارهای کمکی، می‌توان تا حدی جلوی این برنامه‌های نفوذی و مضر را که با عنوان نرم افزارهای جاسوسی^۱ شناخته می‌شوند، گرفت. یکی از نرم افزارهای مسدودکننده آنها دیوار آتش^۲ می‌باشد.

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 می‌گیرد. در واقع، نرم افزارهای دیوار آتش به شما اجازه می‌دهند به صفحات مختلف وب دسترسی پیدا کنید، فایل‌های مورد نظرتان را بارگذاری نمایید، با دوستان تان گفت‌وگو کنید و ... بدون آنکه نگران دسترسی غیرمجاز دیگران باشید. بنابراین اگر می‌خواهید به طور دائم آنلاین باشید، توصیه می‌شود از این نرم افزارها استفاده کنید. علاوه بر این، سایت‌های زیادی نیز وجود دارند که می‌توانند به صورت آنلاین سیستم شما را بررسی کرده و یا به‌طور مجانی نرم افزارهایی را در اختیار شما قرار می‌دهند. 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 7 نیز مجهز به یک دیوار آتش موسوم به ICF^۳ است که در هنگام اتصال به اینترنت، مانع از دسترسی سایرین به کامپیوتر شما می‌شود. با دنبال کردن مراحل زیر می‌توانید نرم افزار دیوار آتش در ویندوز 7 را فعال نمایید:



شکل ۹-۱۰ پنجره Network Connection در ویندوز 7

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

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 ۹-۱۱

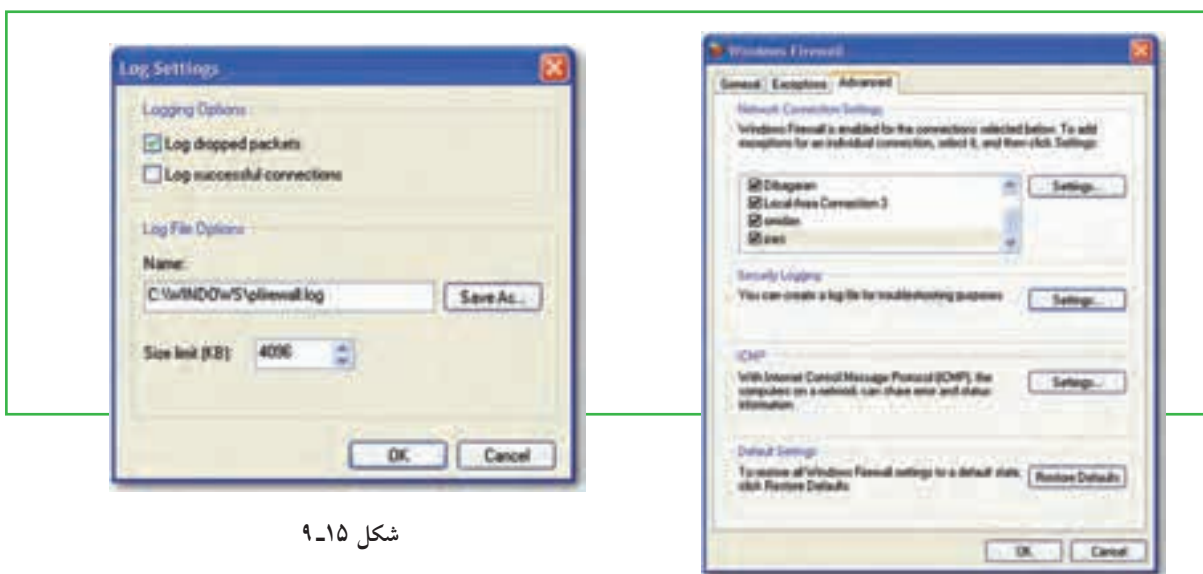
۴- انتخاب زبانه General در کادر محاوره ای Windows Firewall و انتخاب گزینه On. با کلیک بر روی دکمه
OK و بستن تمام کادرهای موجود، علامت قفل کوچکی بر روی اتصال اینترنتی شما ظاهر می شود که نشان دهنده
فعال شدن دیوار آتش ویندوز 7 است.



شکل ۹-۱۳

شکل ۹-۱۲

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 ۹-۱۵

شکل ۹-۱۴

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 ICF سیستم عامل ویندوز 7، راه‌های دیگری نیز برای حفظ امنیت رایانه وجود دارد که یکی از بهترین آنها، ایمن کردن مرورگر می‌باشد. برای این کار نیز در ویندوز راه‌های زیادی وجود دارد که یکی از آنها به روزرسانی^۱ ویندوز می‌باشد. انجام این کار باعث ایمن شدن مرورگر خواهد شد. راه دیگر نیز استفاده از برنامه‌های کمکی مانند ZoneAlarm یا Norton Internet Security یا نرم‌افزارهای متنوع دیوار آتش مانند Ashampoo و Outpost می‌باشد که وظیفه آنها بستن حفره‌های نفوذ به یک سیستم است.

ایمنی مرورگر وب

همانطور که می‌دانید با نصب سیستم عامل ویندوز 7، شرکت مایکروسافت مرورگر اینترنتی Internet Explorer را بر روی این سیستم عامل در اختیار شما قرار می‌دهد. این مرورگر دارای ویژگی‌های امنیتی بسیار بالایی است که اگر آنها را به همراه گزینه‌های امنیتی ویندوز 7 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 راه‌اندازی کنید.

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



شکل ۹-۱۶

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

۴- برای تغییر سطح امنیتی هر یک نواحی فوق، ابتدا روی ناحیه مورد نظر کلیک کرده و سپس به وسیله دکمه لغزنده موجود در قسمت Security level for this zone، سطح امنیتی مورد نظر را انتخاب کنید. توجه داشته باشید که هرچه سطح امنیتی بالاتری را برای هر ناحیه در نظر 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 می‌گویند و هکر^۲ یا نفوذگر فردی است که می‌تواند به طور غیر مجاز به رایانه دیگران نفوذ کرده و به آنها آسیب برساند. این آسیب می‌تواند از حذف کردن فایل‌ها گرفته تا دزدیدن اطلاعات با ارزش تجاری یا خصوصی (مانند دزدیدن شماره کارت اعتباری یا مشخصات محصولات یا اسناد حقوقی یا سوابق بیمارستانی) را شامل شود. از این رو داشتن کلمات عبور خیلی محرمانه، می‌تواند به خوبی از صفحات وب و فایل‌های ذخیره شده در سرویس دهنده‌های وب محافظت کند. ضمن آنکه رمزدار کردن اطلاعات نیز می‌تواند از ردیابی آنها در نقل و انتقالات اینترنتی جلوگیری کند، به طوریکه دیگر کسی نتواند بدون داشتن کلید رمز گشایی مناسب، آنها را بخواند.

یکی از متداول ترین سیستم‌های رمزگزاری، پروتکل SSL نام دارد که با رمزکردن اطلاعات، از آنها در نقل و انتقالات بین مرورگرها و سرویس دهنده‌های وب محافظت می‌کند.

البته باید دانست که پروتکل SSL فقط ارتباط بین مرورگرها و سرویس دهنده‌های وب را امن می‌نماید و برای محافظت از اطلاعات شما در سرویس دهنده‌های وب کاری را انجام نمی‌دهد. بنابراین در مورد شرکت‌های بزرگی که می‌توانند 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 شرکت‌های 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 می‌آید، 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 دهنده‌های وب، برنامه‌ای به نام Form Mail را در اختیار سرویس گیرنده‌های خود قرار می‌دهند. این برنامه محتوای فرم‌های آنلاین را گرفته و از طریق یک پست الکترونیکی آنها را به شرکت یا سازمان مربوطه ارسال می‌کند. در حالی که برای این پیام نه محافظتی وجود دارد و نه اطلاعات آن رمزگذاری می‌شود.

البته راه‌های زیادی برای تأمین امنیت واقعی در معاملات الکترونیکی وجود دارد. به عنوان مثال، نسخه‌هایی از برنامه Form Mail وجود دارد که از ایمیل‌های رمزدار شده استفاده می‌کند. برخی از سرویس دهنده‌های وب نیز اطلاعات را در جایی قرار می‌دهند که مستقیماً از طریق وب نمی‌توان به آنها دسترسی پیدا کرد.

۱_ Hack

۲_ Hacker

همان‌طور که در فصل‌های 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 پایین پنجره مرورگر یک علامت قفل نمایش داده شد، نشان دهنده 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 به آدرس فیزیکی، سابقه و سیاست‌های آن شرکت نگاهی بیندازید و مطمئن شوید که در آن ذکر شده است که هرگز اطلاعات یک مشتری بدون رمزگذاری از طریق اینترنت جابه‌جا نخواهد شد.

در تجارت الکترونیکی، بانکداری الکترونیکی و سایر وب سایت‌هایی که از پروتکل SSL استفاده می‌کنند، برای بررسی صحت و اعتبار اطلاعات از گواهی‌نامه‌های دیجیتالی استفاده می‌شود. این گواهی‌نامه‌ها معمولاً به وسیله مراجع ذی‌صلاح صدور گواهی‌نامه به شکلی کاملاً قانونی و در چهارچوبی کاملاً فنی صادر می‌شوند و به آنها **کلید عمومی زیر ساخت**^۱ گفته می‌شود. بنابراین بهترین حالت امنیت در یک معامله اینترنتی این است که:

- **فرم سفارش امن باشد.**
 - **اطلاعات به صورت رمزدار شده در بین رایانه‌های مشتری و سرویس دهنده‌های وب رد و بدل شود.**
 - **در سرویس دهنده‌های وب، اطلاعات به صورت رمزدار شده در یک پایگاه داده ذخیره شوند.**
 - **فروشنده به وسیله یک ایمیل از رسیدن سفارش‌ها مطلع شود.**
 - **هیچ گونه اطلاعات مهم و حساسی در ایمیل‌ها قرار نگیرد.**
 - **فروشنده اطلاعات را از طریق یک ارتباط امن بازبایی کند.**
- به طور کلی، هیچ روشی به طور صددرصد رایانه و اطلاعات شما را ایمن نمی‌کند، بلکه فقط احتمال هک شدن آنها را پایین می‌آورد. برخی از متداول‌ترین روش‌های هک کردن عبارت‌اند از:
- **رایج‌ترین 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 می‌شود به منظور اطمینان از صحت سرویس دهی یا هر چیز دیگری مانند آن، رمز عبور خود را یک بار دیگر وارد کنید. با انجام این کار، معمولاً بلافاصله رمز عبور شما برای هکر ایمیل می‌شود.**
 - **روش دیگر، حدس زدن جواب سؤالی است که شما انتخاب کرده‌اید تا در صورت فراموش کردن رمزتان از شما پرسیده شود.**

● روش دیگری که کمی تخصصی تر بوده و هر کسی نمی تواند از آن استفاده کند، فرستادن یک فایل آلوده به ویروس یا تروجان^۱ به سیستم شما است که با اجرای این فایل، فایل مورد نظر هکر نیز در حافظه رایانه جای می گیرد و با هر بار روشن شدن رایانه، در حافظه بارگذاری 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 به دست 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 گذارند، بلکه فقط از طریق یک ایمیل، رمزها و اطلاعات محرمانه را برای هکر ارسال می کنند).

با به کارگیری 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 این ها، 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 یک سری کلید را اشتباهی فشار داده و سپس با کلیدهای Backspace 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 Task Manager پنجره Windows Security، تمام پنجره های مشکوک را ببندید.

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 اتاق های گفت وگو 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.

۹- از جدیدترین نرم افزارهای ضد ویروس استفاده کرده و به طور مداوم آنها را به روزرسانی کنید.

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

۱۰- از نرم افزارهای Firewall استفاده نمایید.

سرویس اینترنت را باید از جایی تهیه کرد که امنیت بیشتری دارد. زیرا اگر شبکه 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. همان طور 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 ۹-۱۸



شکل ۹-۱۷

خلاصه فصل

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 می‌دهد تا اطلاعات درخواست شده یا مطالب خود را درون فیلدهای آن وارد کنند.

استفاده از فرم‌های آنلاین معمولاً روش مناسبی برای جمع آوری اطلاعات کاربران و بازدیدکنندگان یک وب سایت، ممیزی کردن، نظرسنجی‌ها، ثبت نام یا عضویت در یک سازمان یا یک دوره آموزشی، کاهش فرم‌های کاغذی و است. علاوه بر آنکه اطلاعات جمع آوری شده را نیز راحت‌تر می‌توان ذخیره و پردازش نمود.

فیلد اجباری، فیلدی است که مقدار آن حتماً می‌بایست 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 می‌شود که تأکید می‌نماید این فیلد باید پر شود.

با استفاده از قابلیت‌های سیستم عامل ویندوز یا استفاده از نرم‌افزارهای کمکی، می‌توان تا حدی جلوی برنامه‌های نفوذی و مضر را که با عنوان نرم افزارهای جاسوسی شناخته می‌شوند، گرفت. یکی از نرم افزارهای مسدود کننده آنها دیوار آتش می‌باشد.

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

کوکی‌ها فایل‌های متنی کوچکی هستند که به وسیله برخی از وب سایت‌ها بر روی رایانه شما نوشته می‌شوند و فقط می‌توانند به وسیله همان وب سایت تولید شده، خوانده شوند.

فعالیت کارگاهی

- ۱- به سایت www.email.com بروید و با فرم‌های 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 می‌توانید 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- 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؟