



---

it  
.hsu

## گزارش فعالیت‌های مرکز فناوری اطلاعات

خرداد ۱۳۹۰ - خرداد ۱۳۹۱

.ac

محمود امین طوسی

.ir

---

دانشگاه حکیم سبزواری  
معاونت پژوهشی و فناوری  
مدیریت فناوری اطلاعات

۱۳۹۱/۳/۲۲



از همه‌ی همکاران محترم واحد فناوری اطلاعات دانشگاه به خاطر زحماتی که در این یک سال کشیده‌اند سپاس‌گزاری می‌کنم.  
از آقایان مهندس علی چشمی و مهندس علی زاهدی‌نژاد به خاطر مشارکت در تهیه این گزارش تشکر می‌کنم.

محمود امین طوسی

# فهرست مطالب

۴	پیشگفتار
۵	۱ تاریخچه و امور محوله‌ی مرکز فناوری اطلاعات دانشگاه
۷	۱.۱ همکاران مرکز فناوری و فهرست امور محوله
۸	۱.۱.۱ جناب آقای مهندس بیهقی
۸	۲.۱.۱ جناب آقای صالحی‌نیا
۹	۳.۱.۱ جناب آقای حسینی و جناب آقای چشمی
۱۰	۴.۱.۱ جناب آقای اسدی
۱۱	۵.۱.۱ جناب آقای زاهدی
۱۱	۶.۱.۱ سرکار خانم دولت آبادی
۱۲	۲ راهنمای استفاده از سرویسهای فناوری دانشگاه
۱۲	۱.۲ MATLAB بر روی سرور دانشگاه
۱۳	۲.۲ فعال شدن امکان ترجمه آنلاین در صفحات شخصی اساتید
۱۳	۳.۲ تک‌لایو بر روی سرور دانشگاه
۱۴	۴.۲ بروز رسانی سایت دانشگاه
۱۶	۵.۲ مشکل نمایش سایت دانشگاه در نسخه قدیمی Internet Explorer
۱۷	۶.۲ فعال شدن سرویس wireless
۱۷	۷.۲ کامپایلر C++
۱۸	۸.۲ افزایش سقف دانلود دانشجویان کارشناسی ارشد
۱۹	۹.۲ راهنمای نصب برنامه اتوماسیون اداری
۲۴	۱۰.۲ آموزش ساخت Vpn Connection در win xp
۲۵	۱۱.۲ ترافیک اینترنت دانشگاه
۲۵	۱۲.۲ ارتقای وضعیت دسترسی دانشجویان دکترا به اینترنت
۲۵	۱۳.۲ نصب ویدئو پروژکتور در سایت دانشگاه
۲۶	۱۴.۲ دسترسی همکاران به اینترنت ملی و سایت های داخلی
۲۶	۱۵.۲ نحوه اتصال به شبکه دانشگاه
۲۷	۱۶.۲ قابل توجه همکاران گرامی
۲۷	۱۷.۲ افزایش سقف حجم دانلود دانشجویان دکترا
۲۷	۱۸.۲ تلفن اینترنتی

۳۷	۱۹.۲	سرور چمران گروه فیزیک برای اساتید
۳۹	۲۰.۲	راهنمای سیستم پست الکترونیکی دانشگاه
۳۹	۲۱.۲	اصلاح سیستم صفحات شخصی اساتید
۴۰	۲۲.۲	تغییر نام دانشگاه
۴۰	۲۳.۲	رتبه دانشگاه در رتبه‌بندی جهانی وبومتریک
۴۰	۲۴.۲	استفاده از شبکه مهمانسرا
۴۰	۲۵.۲	قابل توجه کاربران گرامی
۴۱	۲۶.۲	سامانه تشکلهای دانشجویی
۴۱	۲۷.۲	سامانه مدیریت وبلاگ دانشگاه
۴۱	۲۸.۲	آخرین اطلاعات از تغییر دامنه وبسایت های دانشگاه

۴۳	۳	<b>پرسش و پاسخ پیرامون پست الکترونیکی جدید دانشگاه</b>
	۱.۳	در مواردی که حجم ورودی پر شده پیغام خطا دریافت می شود چگونه مشکل حل می گردد؟
۴۴	۲.۳	چرا به صورت خیلی اتفاقی Inbox پست الکترونیکی خالی می شود؟
۴۵	۳.۳	چرا نمی توانیم ایمیل خود را با ضمیمه ارسال نماییم؟
۴۵	۴.۳	چرا هیچ ایمیلی در یافت نمی شود؟
	۵.۳	آیا با استقرار سیستم جدید، آدرس پست الکترونیکی من با آدرس قبلی متفاوت میشود؟
۴۵	۶.۳	چگونه هرزنامه ها را در ایمیل خود کاهش دهیم؟
۴۷	۷.۳	چگونه اطلاعات شخصی مربوط به Account خود (first name, last name) را تغییر داد؟
۴۹	۸.۳	چگونه تصاویر موجود در متن دیده شود؟
۴۹	۹.۳	چگونه می توانیم ایمیل های موجود در هر پوشه ورودی به سیستم خود ( به صورت فایل zip) انتقال دهیم؟
۵۰	۱۰.۳	چگونه می توانیم عکس در متن نامه قرار دهیم؟
۵۱	۱۱.۳	چگونه می توانیم به گیرنده اهمیت نامه را اعلام نماییم؟
۵۲	۱۲.۳	چگونه یک نامه در پست الکترونیکی پرینت گرفته شود؟
	۱۳.۳	شناسه کاربری و رمز ورود برای استفاده از سیستم جدید پست الکترونیکی چیست؟
۵۲		
۵۳	۱۴.۳	برای دسترسی به ایمیل های قبلی خود چه کنم؟
۵۳	۱۵.۳	چگونه ایمیل خود را روی اوت لوک ۲۰۰۷ ( outlook 2007 ) نصب کنیم
۵۸	۱۶.۳	محدودیت های فعلی ایمیل سرور جدید
۵۸	۱۷.۳	نصب Zimbra Desktop
۶۰	۱۸.۳	استفاده دانشجویان دکتری از سیستم پست الکترونیکی دانشگاه
۶۱	۱۹.۳	اصلاح ارسال به Gmail
۶۱	۲۰.۳	چگونه نوشتار خود را راست چین نمایم؟
	۲۱.۳	چگونه نامه های gmail و ی Yahoo خود را بطور اتوماتیک به پست الکترونیکی دانشگاه forward کنم؟
۶۱		

۶۳	۲۲.۳ چگونه نامه های خود را بطور اتوماتیک از mail دانشگاه به ایمیل دیگر forward کنم؟
۶۵	۴ دانستنیهای عمومی فناوری
۶۵	۱.۴ فید rss چیست؟
۶۸	۲.۴ پهنای باند چیست؟
۶۹	۳.۴ اکتیو دایرکتوری چیست؟
۷۰	۴.۴ نکاتی در مورد رمز عبور کاربران
۷۱	۵.۴ به بهانه درگذشت استیو جابز
۷۱	۶.۴ سه داستان استیو جابز در سخنرانی اش در استنفورد
۷۱	۷.۴ نکته امنیتی درباره gmail
۷۲	۸.۴ IP-Phone چیست؟
۷۴	۹.۴ دنیس ریچی هم درگذشت
۷۵	۱۰.۴ IPTV چیست؟
۷۹	۱۱.۴ شبکه VPN چیست؟
۷۹	۱۲.۴ تبلت چیست؟
۸۱	۱۳.۴ پدر هوش مصنوعی درگذشت
۸۲	۱۴.۴ هرزنامه‌ها و سرقت هویت
۸۴	۱۵.۴ بدافزار Stuxnet
۸۶	۱۶.۴ ویروس Duqu بسیار حرفه ای
۸۷	۱۷.۴ نکته که باید درباره LED بدانید
۹۰	۱۸.۴ کنفرانس RSA: مدیریت خطرات حوزه فناوری اطلاعات
۹۱	۱۹.۴ بدافزارهای دسترسی از راه دور، یک تهدید جدی علیه کاربران تلفن همراه
۹۲	۲۰.۴ هشدار به کاربران اینترنت
۹۲	۲۱.۴ پیشگیری از دانلود بدافزارها و تبلیغ افزارها
۹۵	۲۲.۴ بدترین پسوردهای جهان
۹۶	۲۳.۴ یک هکر چگونه رمز عبور شما را هک می کند؟
۹۹	۲۴.۴ SSL چیست؟
۱۰۳	۲۵.۴ دومین جشنواره ملی ارتباطات و فناوری اطلاعات
۱۰۳	۲۶.۴ متن کامل قانون جرائم رایانه ای - مصوب ۱۱ بهمن ۱۳۸۹ مجلس شورای اسلامی
۱۰۴	۲۷.۴ وضعیت امنیت در شش ماهه دوم سال ۲۰۱۱ به گزارش MA۶
۱۰۴	۲۸.۴ اطلاعیه مرکز فناوری اطلاعات و ارتباطات
۱۰۶	۲۹.۴ آشنایی با عملکرد برخی از بدافزارها و نحوه پاکسازی آنها
۱۰۶	۳۰.۴ بدافزار Flame، ابزار شناسایی و نحوه پاکسازی
۱۰۸	۵ دستورالعمل خط مشی امنیت اطلاعات و سیستم های اطلاعاتی دانشگاه
۱۱۲	۶ راهنمای مدیریت وبسایتهای دانشگاه
۱۳۸	۷ راهنمای سیستم پشتیبانی و خدمات رسانی دانشگاه

## پیشگفتار

معمولاً فعالیت‌های مجموعه‌ی مرکز فناوری اطلاعات دانشگاه دیده نمی‌شوند. در این نوشتار قسمتی از فعالیت‌های انجام شده توسط این مرکز در یک سال گذشته، جهت استحضار آمده است. فهرست وظایف محوله به این مجموعه، لیستی طولانی از کارهای مختلف است که به بیشتر آنها در بخشهای آتی اشاره شده است. در تیرماه ۱۳۹۰ سایت جدید مرکز فناوری اطلاعات دانشگاه به منظور اطلاع‌رسانی از مهمترین رخدادهای مرتبط با حوزه‌ی فناوری اطلاعات در داخل (خصوصاً) و خارج دانشگاه راه‌اندازی گردید. سعی همکاران مرکز فناوری اطلاعات بر این بوده است که فعالیت‌های به نتیجه رسیده‌ی این واحد از طریق این سایت به اطلاع همکاران و دانشجویان گرامی رسانیده شود و برای سرویس‌های جدید راه‌اندازی شده راهنماهای مناسبی تهیه و از همین طریق در اختیار افراد قرار داده شود.

مطالب مطروحه در این گزارش، نسخه‌ی مدون شده‌ی از مطالب سایت فناوری می‌باشند که از تیرماه ۱۳۹۰ تا خرداد ماه ۱۳۹۰ در آن درج شده‌اند. امور انجام شده (یا در دست انجام) توسط این مرکز منحصر به این موارد نیستند و موارد زیادی هست که در این گزارش نیامده‌اند. از جمله‌ی این موارد می‌توان به تغییر نام دامنه دانشگاه، نصب زیر سیستم اتوماسیون از ERP، نصب ایمیل سرور SUN برای دانشجویان تحصیلات تکمیلی، تغییرات زیاد به منظور بالابردن امنیت شبکه دانشگاه، ایجاد وبلاگ برای انجمن‌های علمی، سیستم بازنشستگان، پیگیری‌های زیاد برای عقد قراردادهای مختلف و تغییراتی در سایت دانشجویی را نام برد.

به دلیل کمبود نیرو در حوزه‌ی فناوری نسبت به حجم کار مورد انتظار از این واحد، کارهای زیادی هم هست که شروع نشده‌اند و یا علیرغم پیگیری‌های زیاد هنوز به سرانجام مطلوب نرسیده‌اند. از آن جمله می‌توان به شبکه‌ی کابلی و وایرلس دانشگاه، سیستم‌های حوزه‌ی معاونت دانشجویی، پژوهشی، آموزش مجازی و برخی زیرسیستم‌های حوزه‌ی اداری و مالی همچون حسابداری تعهدی و حق‌التدریس را نام برد.

در اولین فصل مروری بر تاریخچه و ساختار خود مرکز فناوری اطلاعات (به نقل از سایت فناوری و گزارشات قبلی) خواهیم داشت. در فصل ۲ برخی از سرویس‌های راه‌اندازی شده و اخبار مرتبط با آنها را خواهیم دید. در فصل ۳ راهنمای ایمیل سرور جدید دانشگاه آمده است. فصل ۴ به ذکر اخباری خارج از دانشگاه اختصاص یافته است که به نظر این مرکز مورد نیاز همکاران گرامی دانشگاه بوده و یا از جمله اخبار مهم روز فناوری دنیا بوده‌اند. در فصل ۵ دستورالعمل خط مشی امنیت اطلاعات و سیستم‌های اطلاعاتی دانشگاه آمده است و فصل‌های پس از آن به دو راهنمای آماده شده فناوری اطلاعات تخصیص یافته‌اند.

## فصل ۱

# تاریخچه و امور محوله‌ی مرکز فناوری اطلاعات دانشگاه



برنامه ریزی جهت فعال نمودن امور کامپیوتری دانشگاه در سال ۱۳۶۸ انجام و در همان سال گروه خدمات ماشینی به چارت سازمانی دانشگاه اضافه گردید. با تأسیس این گروه دانشگاه اقدام به جذب یک نفر مهندس کامپیوتر نمود و امور راه‌اندازی و خرید دو دستگاه کامپیوتر در سال ۱۳۶۸ انجام شد.

اولین بهره‌برداری رسمی از دو دستگاه کامپیوتر در اردیبهشت سال ۱۳۶۹ به شرح زیر آغاز شد:

- ۱- اختصاص یک دستگاه کامپیوتر جهت آموزش عملی دانشجویان رشته ریاضی
- ۲- اختصاص یک دستگاه کامپیوتر جهت ایجاد سیستم نرم افزاری آموزش دانشگاه

سیستم نرم افزاری امور آموزشی دانشجویان اولین سیستم نرم افزاری است که در این دانشگاه طراحی، پیاده‌سازی و عملیاتی گردید.

به مرور زمان و با توجه به نیاز پرسنل دانشگاه، کامپیوترهای موجود افزایش یافتند. تا سال ۱۳۸۲ سیستم‌های نرم افزاری زیر توسط پرسنل گروه خدمات ماشینی کدنویسی و تکمیل شدند:

- ۱- سیستم مدیریت خدمات آموزشی
- ۲- سیستم دستمزد و حقوق اساتید و کارکنان
- ۳- سیستم امانات کتابخانه مرکزی
- ۴- سیستم فهرست نویسی کتابخانه مرکزی
- ۵- سیستم اموال دانشگاه
- ۶- سیستم مدیریت دانشجویی
- ۷- سیستم خوابگاه‌های دانشجویی
- ۸- سیستم انبار
- ۹- سیستم دفتر نظارت و ارزشیابی
- ۱۰- سیستم برنامه ریزی کلاسهای درسی
- ۱۱- سیستم کارگزینی

علاوه بر این موارد در سال ۱۳۷۴ اولین لینک به شبکه های اطلاع رسانی بین المللی از طریق شرکت مخابرات برقرار گردید که اتصال دانشگاه به شبکه اطلاع رسانی کامپیوسرور را ممکن ساخت. اولین ارتباط با شبکه اینترنت از طریق خط Dialup در سال ۱۳۷۶ و در محل ساختمان قدیم دانشگاه از طریق دانشگاه فردوسی مشهد راه اندازی شد. در سال ۱۳۷۸ شبکه داخلی LAN با توپولوژی Bus در ساختمان قدیمی دانشگاه راه اندازی و سیستم آموزش تحت شبکه در آن راه اندازی گردید. پس از بهره برداری از ساختمان دانشکده ادبیات فعلی شبکه داخلی در این دانشکده راه اندازی و یک خط وایرلس از طریق سازمان پژوهشهای علمی و صنعتی ایران جهت دسترسی به اینترنت با پهنای باند ۱۲۸ Kbps را در دانشگاه فراهم نمود.

با توجه به توسعه همه جانبه و روزافزون دانشگاه و افزایش تعداد دانشجویان، نیاز به تغییر در ساختار گروه خدمات ماشینی و تغییر چارت سازمانی این گروه، مدیریت فناوری اطلاعات در دانشگاه ایجاد و متعاقب آن توسعه فراگیر زیرساخت شبکه داخلی و تأمین پهنای باند مورد نیاز اینترنت و اینترنت در دستور کار قرار گرفت، که تقریباً امروزه شاهد اتصال کلیه قسمت‌های دانشگاه به شبکه داخلی می باشیم.

همزمان با توسعه زیرساخت‌های شبکه سیستم های نرم افزاری تحت شبکه و وب جهت رفع نیازمندیهای دانشگاه به شرح زیر تهیه و در دسترس کاربران قرار گرفت:

- ۱- سیستم مدیریت خدمات امور آموزشی
- ۲- پورتال دانشجویی
- ۳- پورتال اساتید و کارکنان
- ۴- سیستم اتوماسیون اداری
- ۵- سیستم انتخاب واحد اینترنتی و پرداخت شهریه
- ۶- سیستم های مدیریت شبکه و پهنای باند اینترنت
- ۷- سیستم دستمزد و حقوق اساتید و کارکنان
- ۸- راه اندازی وب سایت دانشگاه و ارتقاء
- ۹- سیستم کارگزینی و امور پرسنلی کارکنان و اساتید
- ۱۰- راه اندازی ftp دانشگاه
- ۱۱- راه اندازی پست الکترونیک ویژه دانشگاه



- ۱۲- اتصال شبکه دانشگاه به شبکه فیبر نوری مخابراتی دانشگاه  
 ۱۳- ارتقاء پهنای باند از ۱۲۸Kbps به ۳۰Mbps در طول ۸ سال  
 ۱۴- سیستم مجلات  
 ۱۵- سیستم معاونت پژوهشی  
 ۱۶- سیستم مدیریت چاپ که مراحل آزمایشی خود را طی نموده است.  
 مسئولین فناوری اطلاعات از ابتدا تاکنون:  
 ۱- از سال ۱۳۶۹ تا ۱۳۸۲، مهندس محسن بیهقی (مهندسی کامپیوتر دانشگاه صنعتی اصفهان)  
 ۲- از سال ۱۳۸۲ تا ۱۳۸۹، دکتر جواد حدادنیا (دکترای الکترونیک- دانشگاه صنعتی امیرکبیر)  
 ۳- از سال ۱۳۹۰ تاکنون، دکتر محمود امین طوسی (دکترای کامپیوتر- دانشگاه علم و صنعت ایران)

## ۱.۱ همکاران مرکز فناوری و فهرست امور محوله

دکتر محمود امین طوسی (مدیر فناوری اطلاعات)  
 پست الکترونیکی: [m.amintoosi@hsu.ac.ir](mailto:m.amintoosi@hsu.ac.ir)  
 تلفن: ۰۵۷۱۴۰۰-۳۵۳۴

مهندس بیهقی (معاون فناوری اطلاعات)  
 پست الکترونیکی: [beihaghi@hsu.ac.ir](mailto:beihaghi@hsu.ac.ir)  
 تلفن: ۰۵۷۱۴۰۰-۳۵۶۹

آقای صالحی نیا (کارشناس) پست الکترونیکی: تلفن: ۰۵۷۱۴۰۰-۳۵۶۸

آقای چشمی (کارشناس)  
 پست الکترونیکی: [cheshomi@hsu.ac.ir](mailto:cheshomi@hsu.ac.ir) تلفن: ۰۵۷۱۴۰۰-۳۵۷۱

آقای حسینی (کارشناس) تلفن: ۰۵۷۱۴۰۰-۳۵۷۸

آقای اسدی (کارشناس) تلفن: ۰۵۷۱۴۰۰-۳۵۷۲

خانم دولت آبادی (کارشناس) تلفن: ۰۵۷۱۴۰۰-۳۵۷۴

آقای زاهدی نژاد (کارشناس)  
 پست الکترونیکی: [a.zahedi@hsu.ac.ir](mailto:a.zahedi@hsu.ac.ir)  
 تلفن: ۰۵۷۱۴۰۰-۳۵۷۲

اموری که در حال حاضر به عهده هر یک از اعضای مرکز فناوری می باشد به شرح ذیل است.

### ۱.۱.۱ جناب آقای مهندس بیهقی

۱. انجام مکاتبات اداری و امور مورد تقاضا
۲. انجام ارزشیابی سالانه پرسنل فناوری اطلاعات
۳. پیشنهاد و پیگیری خرید تجهیزات سخت افزاری، تجهیزات شبکه
۴. نظارت بر اداره امور مراکز کامپیوتر دانشجویی آقایان و خانمها
۵. پیگیری امور مربوط به فیوژن فیبرهای نوری و تعویض فیبرهای قدیمی و فرسوده
۶. پیگیری امور مربوط به کابل کشی شبکه های داخلی و اتصال دانشکده های جدید با استفاده از فیبر نوری به شبکه دانشگاه
۷. پیگیری امور مربوط به افزایش یا کاهش پهنای باند اینترنت و یا تعویض سرویس دهندگان
۸. پیگیری رفع قطعی خط اینترنت و اینترنت ملی
۹. پیگیری امور مربوط به پرداخت صورت حسابهای ارسالی جهت سرویسهای اینترنت و اینترنت ملی
۱۰. پیگیری و انجام امور مربوط به انعقاد قرارداد خدمات پشتیبانی سخت افزاری و نرم افزاری
۱۱. تهیه و تنظیم کلیه قراردادهای مربوط به حوزه فناوری اطلاعات و پیگیری امورات مربوطه
۱۲. تهیه بولتن خبری مربوط به حوزه فناوری اطلاعات
۱۳. پیگیری خرید سیستمهای وایرلس دانشگاه
۱۴. همکاری در برگزاری آزمونهای الکترونیکی در دانشگاه
۱۵. نظارت بر واگذاری کد کاربری و رمز عبور اساتید، کارکنان و دانشجویان جهت استفاده از شبکه داخلی دانشگاه و شبکه اینترنت
۱۶. نظارت و تنظیم ساعات استفاده از اینترنت و شارژ ماهیانه
۱۷. پیگیری امور مربوط به سرمایه و برق اضطراری مرکز داده ها
۱۸. هماهنگی تشکیل جلسات کمیته تخصصی فناوری اطلاعات و پیگیری امور مصوب
۱۹. برنامه ریزی و هماهنگی تشکیل کلاسهای عملی در سایت کامپیوتر

### ۲.۱.۱ جناب آقای صالحی نیا

۱. مدیریت سیستم اتوماسیون اداری
- سازماندهی و تعریف کاربران جدید
- تغییر نوع کاربری کاربران
- تعیین سطح دسترسی کاربران
- تعریف الگوهای نامه های اداری
- تعریف گروه های مختلف نامه های اداری
- رفع اشکال از کاربران سیستم اتوماسیون
- بایگانی نامه ها در سال قبل و تعریف سال جدید
۲. نظارت بر انجام امور شرکت طرف قرارداد سخت افزار و نرم افزار

- تهیه گزارش ماهیانه پرداخت حق الزحمه قرارداد انجام خدمات
- بررسی لیست گزارشها
- نظارت بر انجام امور
- هماهنگی های لازم جهت رفع مشکلات نرم افزاری و سخت افزاری
- سرکشی و نظارت بر انجام عملیات نرم افزاری و سخت افزاری در حین انجام امور
- ۳. سیستم نرم افزار چاپ
- تعیین سهمیه چاپ کاربران
- تعریف چاپگرهای جدید در محیط شبکه
- تغییرات چاپگرها در شبکه
- ۴. پشتیبانی از سیستمهای نوشته شده
- خوابگاهها
- دانشجویی
- کتابخانه
- اموال
- ۵. همکاری با شبکه و اکتیو دایرکتوری (اساتید- کارکنان - دانشجویان)
- ایجاد کاربران جدید ( اساتید و کارکنان و دانشجویان انتقالی و مهمان)
- رفع اشکال کاربران ( نام کاربری - کلمه عبور و ...)
- ۶. طراحی سیستم الکترونیکی بایگانی پرونده های معاونت دانشجویی
- ۷. بررسی و تهیه لیست خرید سخت افزارهای لازم جهت مجموعه دانشگاه با توجه به سیستمهای روز
- ۸. همکاری در برگزاری کنکورهای دانشگاه
- ۹. برگزاری کلاسهای مدیریت فناوری
- ۱۰. پیگیری بحث امنیت سایت و اینترنت
- ۱۱. پشتیبانی و مدیریت سیستم اتوماسیون جدید

### ۳.۱.۱ جناب آقای حسینی و جناب آقای چشمی

۱. مدیریت و نظارت بر مرکز آی اس پی، شامل:
  - نگهداری تمامی سرورهای فیزیکی دانشگاه
  - پیگیری ارتقای سخت افزاری سرورها شامل کارت شبکه، حافظه و...
  - نصب و نگهداری بیش از ۳۰ سرور مجازی دانشگاه شامل: وب سرور، میل سرور، سرور کتابخانه، سرور صفحات شخصی اساتید، سرور آموزش، سرور امور پژوهشی، سرور امور تغذیه و ....
  - نصب و نگهداری SAN
  - نصب، نگهداری و بروزرسانی نرم افزار مجازی سازی
  - نصب، نگهداری و بروزرسانی سرور متلب با قابلیت استفاده در تمام دانشگاه
۲. پیش بینی موارد امنیتی و حفاظتی تمام سخت افزارها و داده های حیاتی دانشگاه.
۳. پیگیری برای نصب SAN در سازمان مرکزی جهت ایجاد یک کپی از داده های حساس دانشگاه
۴. پیشنهاد و پیگیری نصب تجهیزات مانیتورینگ دمای مرکز ISP
۵. مانیتورینگ برقراری برق مرکز و سیستم های سرمایشی مرکز ISP

۶. نظارت بر ارتباط سخت افزاری شبکه و نگهداری آن و رفع مشکلات سوئیچ و لوازم ارتباطی نصب شده در دانشگاه و کلیه واحدهای استفاده کننده بصورت مستمر و دائم شامل:
  - نگهداری تمام رکهای دانشگاه با تعداد زیادی سوئیچ و حدود ۱۰۰۰ پورت
  - نصب و نگهداری آنتهای بی سیم دانشگاه، مستقر در خوابگاه مریم، سازمان مرکزی و...
  - نصب، نگهداری و مانیتورینگ تجهیزات بی سیم دانشگاه در دانشکده های فنی و مهندسی، برق و کامپیوتر، علوم پایه و....
  - نگهداری و مانیتورینگ صدها متر زیرساخت فیبرنوری و اتصالات آنها
۷. نصب و پشتیبانی سرورهای گروه فیزیک
۸. ایجاد زیردانه برای واحدهای جدید دانشگاه مانند: مدیریت تربیت بدنی، سایت کنفرانسها، سایت مجلات و...
۹. انجام امور زیر بنایی و مواردی که تحت کنترل واحدهای مربوطه نیست، مانند بازنشانی رمزهای عبور، تعریف سطوح دسترسی و...
۱۰. تعیین گروههای مختلف کاربران اینترنت دانشگاه مانند اساتید، کارمندان و دانشجویان و تغییر پارامترهای آنها حسب نیاز
۱۱. نظارت بر موارد استفاده نامناسب از حسابهای کاربری، اخطار و یا قطع اتصال کاربران خاطی
۱۲. نگهداری و بروزرسانی سیستم آنتی ویروس دانشگاه به نحوی که تمام سیستم های دانشگاه به صورت خودکار و با کمترین پهنای باند مصرفی بروزرسانی شوند
۱۳. ایجاد یک مخزن از بسته های بروزرسانی ویندوز به نحوی که تمام سیستمهای دانشگاه به صورت خودکار و با کمترین پهنای باند مصرفی بروزرسانی شوند
۱۴. مدیریت، نگهداری و نظارت بر نرم افزارهای مورد نیاز مرکز فناوری
۱۵. پیگیری برای معرفی تجهیزات مناسب سخت افزاری و نرم افزاری مورد نیاز برای مانیتورینگ قسمتهای مختلف
۱۶. جداسازی ارتباط با سرورهای داخل کشور از اینترنت از طریق اینترنت که موجب استفاده بهینه از پهنای باند دانشگاه می شود.
۱۷. مانیتورینگ چگونگی مصرف پهنای باند دانشگاه و شرکت طرف قرارداد به صورت دائم
۱۸. تمام امور مربوط به آی پی های دانشگاه از قبیل تخصیص آی پی به شرکت های طرف قرارداد دانشگاه جهت نصب برنامه های خریداری شده
۱۹. نصب ماژولها و برنامه های مورد نیاز، حسب درخواست شرکت های طرف قرارداد دانشگاه
۲۰. آماده سازی بستر مناسب جهت فروش امکانات هاستینگ به مؤسسات خارج از دانشگاه و درآمدزایی برای دانشگاه
۲۱. تحقیق و جستجو برای خرید نرم افزار Web Control Panel
۲۲. بررسی و پیگیری مشکلات میل سرور دانشگاه، نصب سرور و نرم افزارهای جدید و انتقال حسابهای کاربری به سیستمهای جدید

#### ۴.۱.۱ جناب آقای اسدی

۱. سیستم پرسنلی و کارگزینی
۲. سیستم دستمزد و حقوق کارکنان رسمی و پیمانی

۳. سیستم دستمزد و حقوق کارکنان قراردادی و کارمعیین
۴. سیستم معاونت دانشجویی ( در حال راه اندازی )
۵. سیستم بازنشستگان ( در حال راه اندازی )
۶. سامانه صفحه شخصی اساتید
۷. وبلاگ انجمنهای دانشجویی
۸. سیستم ارسال و دریافت اس ام اس
۹. ایجاد قالب برای سایت مرکز فناوری

### ۵.۱.۱ جناب آقای زاهدی

۱. پشتیبانی و مدیریت سایت دانشگاه
۲. ایجاد بخش زبان انگلیسی، فرانسه و عربی سایت.
۳. گزارش خلاصه عملکرد دانشگاه
۴. امور مربوط به سمینار جبر
۵. درج اطلاعیه ها و اخبار
۶. مدیریت سایت مرکز فناوری
۷. مدیریت پرتال همایش ها
۸. پشتیبانی اتوماسیون جدید
۹. مدیریت سایت انجمنهای علمی

### ۶.۱.۱ سرکار خانم دولت آبادی

۱. امور آموزشی دانشجویان در دانشکده ها
۲. امور مالی دانشجویان نوبت دوم
۳. پذیرش و ثبت نام
۴. حق التدریس
۵. دبیرخانه مدیریت امور آموزشی
۶. سیستم ارزشیابی اساتید
۷. سیستم کدینگ
۸. مدیریت امور آموزشی
۹. پورتال اساتید
۱۰. پورتال دانشجویی

## فصل ۲

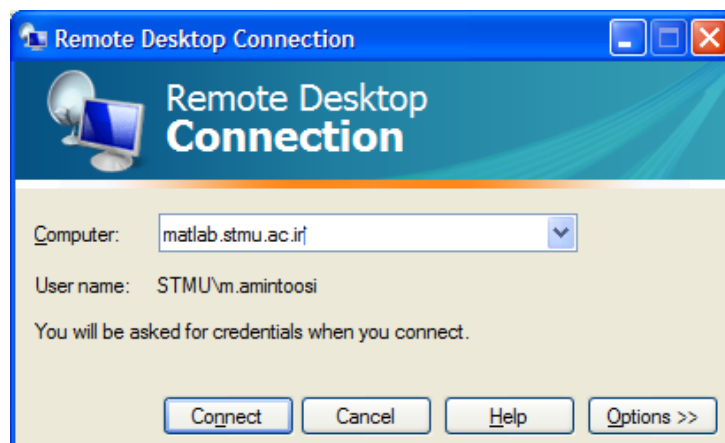
# راهنمای استفاده از سرویسهای فناوری دانشگاه

مطالب این فصل شامل اخبار و اطلاعیه‌هایی است که در یک سال گذشته درخصوص سرویس‌های مرکز فناوری اطلاعات در سایت آن به آدرس [it.hsu.ac.ir](http://it.hsu.ac.ir) درج شده است. ترتیب نشر آنها تقریباً با ترتیب زمانی درج آنها برابر است.

### ۱.۲ MATLAB بر روی سرور دانشگاه



اگر متصل به شبکه دانشگاه باشید، از هر کامپیوتری در دانشگاه قادر به اجرای MATLAB-Remote Desktop Connection روی سرور دانشگاه خواهید بود. به این منظور کافیست از Remote Desktop Connection استفاده کنید.....



پس از اجرای آن مطابق تصویر فوق در کادر Computer ، عبارت matlab.stmu.ac.ir را بنویسید و دکمه Connect را بفشارید . برای ورود به سیستم نام کاربری و کلمه عبور خود را وارد نمایید(نام کاربری و کلمه عبور domain)

Remote Desktop Connection : MATLAB

Remote Desktop Connection را در ویندوز XP در Accessories پیدا خواهید کرد و در ویندوز ۷ کافیت در کادر جستجو چند حرف اول آنرا وارد کنید.

پس از متصل شدن، صفحه یک ویندوز را خواهید دید که دارای MATLAB هست. همانند دستگاه شخصی خود، MATLAB را اجرا و استفاده کنید.

برای تبادل فایلها میان بین سیستم متصل به Domain خود و این ویندوز، باید از پوشه My Documents خود استفاده کنید. لذا همکارانی که متصل به Domain نیستند، امکان تبادل فایل را نخواهند داشت.

این سرور مخصوص دانشجویان است و اساتید گرامی می‌توانند از سرور چمران گروه فیزیک استفاده نمایند.

## ۲.۲ فعال شدن امکان ترجمه آنلاین در صفحات شخصی اساتید



جهت استفاده بهینه تر از وب سایت صفحه شخصی پلاگین ترجمه فعال شده است. با کمک این پلاگین شما می‌توانید سایت خود را به زبان های دلخواه و مختلف در اختیار مخاطبان خود قرار دهید.....

کاربران گرامی جهت فعال کردن امکان ترجمه آنلاین در وب سایت خود ابتدا بر روی گزینه Gtranslate در قسمت تنظیمات کلیک کرده و تنظیمات زیر را انجام دهید.

- ۱- در قسمت Default Language زبان فارسی (persian) را انتخاب نمایید
- ۲- در قسمت Flag language پرچم زبان هایی را که می‌خواهید ترجمه آن را داشته باشد انتخاب کنید- به صورت پیش فرض زبان های اصلی انتخاب شده اند

حال به قسمت ابزارک ها در قسمت نمایش سایت رفته و در منوهای سمت چپ بر روی گزینه Gtranslate کلیک کرده آن را بکشید و به سمت راست صفحه منقل نمایید (ستون کناری ۱) حال ترجمه آنلاین شما در دسترس می باشد.

## ۳.۲ تک لایو بر روی سرور دانشگاه



تک لایو ۲۰۱۱ بر روی سرور دانشگاه نصب شده است و مشابه نحوه‌ی استفاده از MATLAB بر روی سرور دانشگاه می‌توان از آن استفاده کرد. پس از اتصال به سرور دانشگاه

از مسیر Start/All Programs/TeX Live 2011 برنامه TeXworks Editor را انتخاب نمایید....



تک لایو نصب شده نسخه کامل و بروز شده تک لایو تا ۲۶ مهرماه ۱۳۹۰ و شامل بسته‌های زی‌پرشین ، BiDi و Persian-bib می‌باشد. لذا دانشجویان و اساتید گرامی بدون نیاز به نصب تک لایو بر روی دستگاهشان می‌توانند به راحتی اسناد فارسی یا لاتین لاتک خود را بر روی سرور دانشگاه اجرا نموده و خروجی بگیرند.

دقت داشته باشید که در حال حاضر پل ارتباطی شما با سرور دانشگاه - برای تبادل فایل - از طریق My Documents شما می‌باشد که فقط از دستگاههای جزو Domain دانشگاه قابل دیدن و استفاده می‌باشد. البته مثالهای فارسی موجود در دی‌وی‌دی پارسی لاتک ۱۳۹۰ در پوشه F:\ParsiLaTeX1390\Examples قرار دارند که می‌توانید مثالهای آنرا مشاهده فرمایید (در پوشه مذکور اجازه نوشتن ندارید). در صورت نیاز به اجرای مثالها باید مثالهای موردنظر خود را به پوشه My Documents خود کپی نموده و سپس اقدام به اجرا نمایید. قلمهای موردنیاز اجرای مثالها در سرور دانشگاه نصب شده است.

همچنین هنوز تنظیمات زیندی برای استفاده از نمایه در زی‌پرشین بر روی سرور دانشگاه انجام نشده است.

از دانشجویان گرامی تقاضا می‌شود مشکلات احتمالی خود در خصوص اتصال به سرور را با مسؤول سایت در میان بگذارند و پرسشهای لاتک خود را در تالار گفتگوی پارسی لاتک مطرح فرمایند.

این سرور مخصوص دانشجویان است و اساتید گرامی می‌توانند از سرور چمران گروه فیزیک استفاده نمایند.

## ۴.۲ بروز رسانی سایت دانشگاه



همزمان با عید سعید فطر ، قالب سایت دانشگاه بروزرسانی گردید. تصاویر زیر بخشی از برخی از سایتهای جدید دانشگاه را نشان می‌دهند.

سایتهای رسمی دانشگاه با موتور وردپرس: صفحه‌ی اصلی به رنگ آبی تیره، صفحات دانشکده‌ها به رنگ آجری، صفحات واحدهای ستادی و زیرمجموعه‌های آنها به رنگهای سبز و آبی روشن:





صفحات سایتهای مدیریت فناوری اطلاعات، مدیریت فرهنگی و مدیریت تربیت بدنی با موتور جوملا:



صفحات جشنواره و همایشهای دانشگاه:



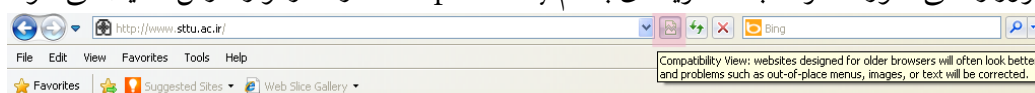
## ۵.۲ مشکل نمایش سایت دانشگاه در نسخه قدیمی Internet Explorer

سایت دانشگاه در مرورگرهای Mozilla Firefox ، Google Chrome و همچنین نسخه های بروز شده Internet Explorer بصورت صحیح نمایش داده می شود. ولی چنانچه از نسخه های قبلی Internet Explorer استفاده میکنید سایت دانشگاه را بصورت ناقص و مانند تصویر زیر مشاهده خواهید کرد:



راه حل مشکل:

برای رفع این مشکل باید از نسخه بروز شده Internet Explorer استفاده نمایید. چنانچه این بروز رسانی صورت گرفته باشد گزینه ای به نام compatibility در کنار نوار آدرس نمایان می شود:



با انتخاب این گزینه مشکل نمایش ناقص برطرف میشود:

## ۶.۲ فعال شدن سرویس wireless



اساتید و دانشجویان گرامی می‌توانند به صورت Wireless از اینترنت و اینترنت، در نقاط مختلف دانشگاه استفاده فرمایند.

## ۷.۲ کامپایلر ++C



کد بلاکس (Code::Blocks) نسخه ۱۰.۰۵ بر روی سرور دانشگاه نصب شده است و مشابه نحوه‌ی استفاده از MATLAB بر روی سرور دانشگاه می‌توان از آن استفاده کرد. Code::Blocks یک محیط توسعه مجتمع است که عمدتاً برای توسعه برنامه‌های C و ++C بکار می‌رود.

پس از ورود به سرور دانشگاه CodeBlocks را اجرا کنید. از این پس همه افرادی که نیاز به یک کامپایلر سبک ++C دارند می‌توانند از این برنامه استفاده کنند. یک راهنمای مناسب زبان ++C

نیز در کنار آن نصب شده است که در محیط Code::Blocks با زدن F1 فعال می‌شود. در صورت نیاز به نصب این نرم‌افزار بر روی دستگاه خود، می‌توانید آنرا از مرکز دانلود دانشگاه برداشته و روی دستگاه خود نصب کنید. دقت داشته باشید که به همراه آن راهنمای ++C نصب نمی‌شود. برای نصب راهنما باید مراحل زیر را طی کنید:

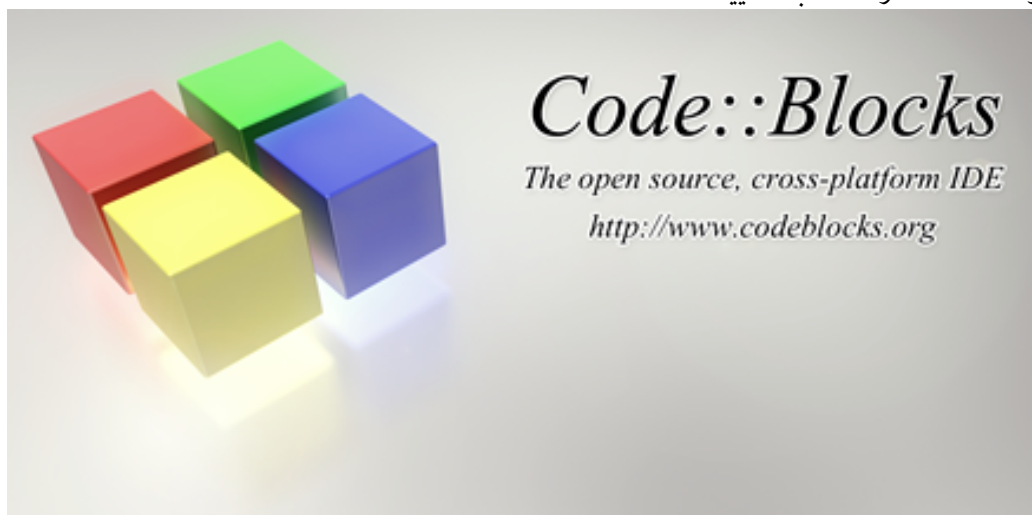
۱. در هنگام نصب کد بلاکس از لیست Contrib Plugins گزینه Help plugin را تیک زده باشید.

۲. فایل cpp.chm را در پوشه محل نصب کد بلاکس کپی نموده و سپس

۳. مطابق صفحه ۲ این راهنما آنرا در محیط Code::Blocks قابل استفاده سازید.

این مراحل در نسخه نصب شده در سرور دانشگاه انجام شده و راهنمای ++C در آن قابل استفاده است.

نکته: اگر پنجره سمت راست راهنمای شما خالی بود، روی فایل cpp.chm کلیک راست نموده و Unblock را انتخاب نمایید.



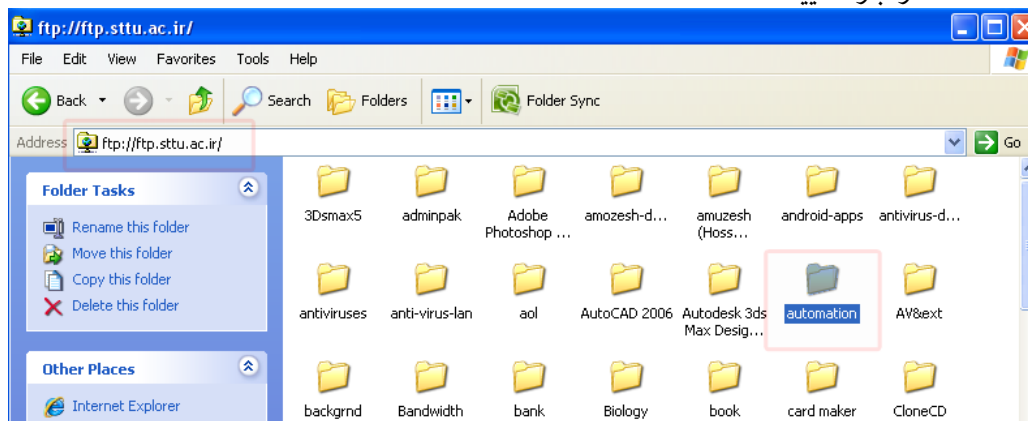
## ۸.۲ افزایش سقف دانلود دانشجویان کارشناسی ارشد



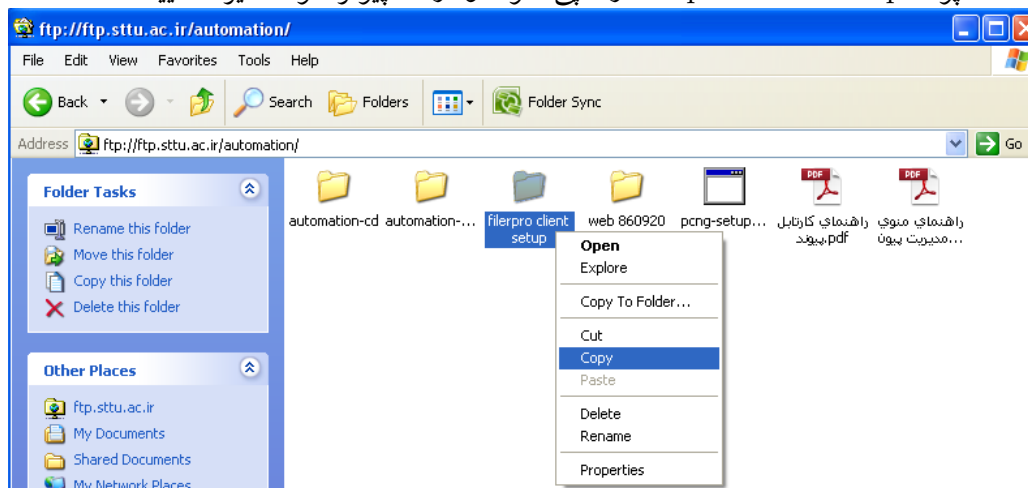
همزمان با اعیاد مبارک قربان تا غدیر و در راستای ارتقای سطح خدمات رسانی، سقف دانلود برای دانشجویان دوره کارشناسی ارشد از ۱G به ۲G افزایش یافت.

## ۹.۲ راهنمای نصب برنامه اتوماسیون اداری

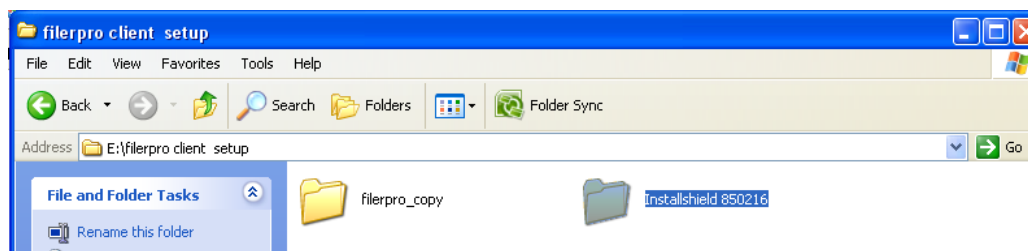
۱- وارد صفحه مرکز دانلود دانشگاه به آدرس <ftp://ftp.sttu.ac.ir/> شوید و پوشه -au tomaton را باز نمایید.

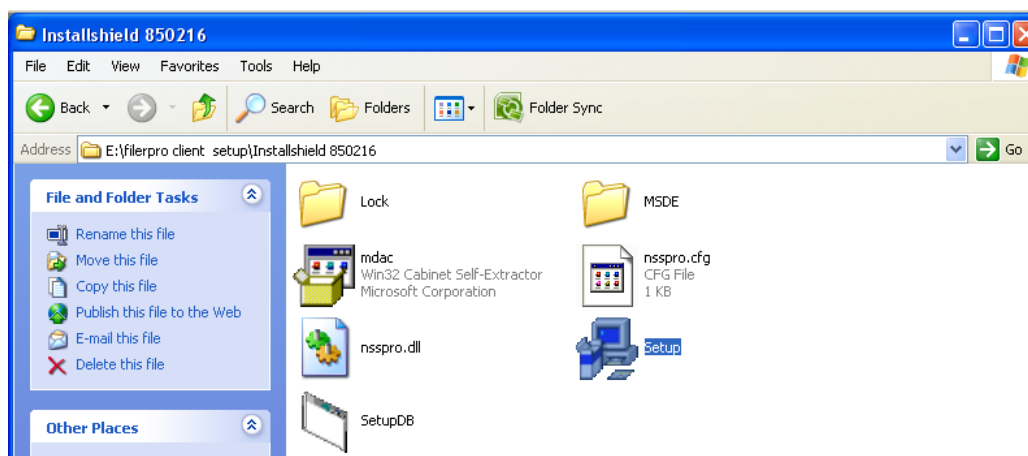


۲- پوشه filerpro client setup را کپی نموده و در کامپیوتر خود ذخیره نمایید.

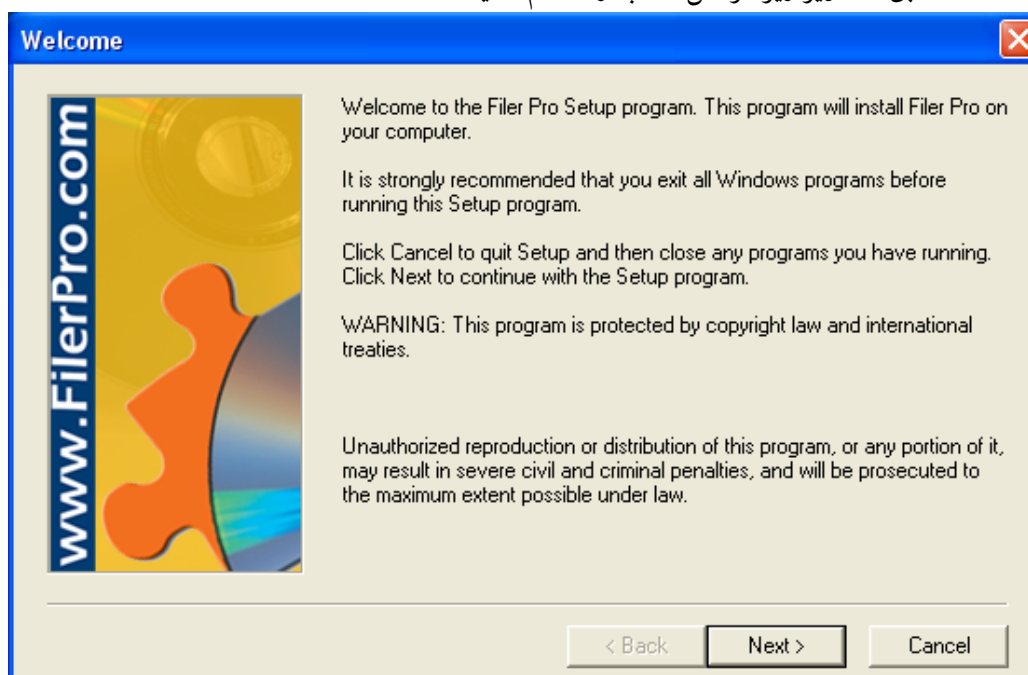


۳- پوشه filerpro client setup حاوی دو پوشه می باشد. پوشه Installshield 850216 را باز نمایید و برای نصب Setup.exe را اجرا کنید.

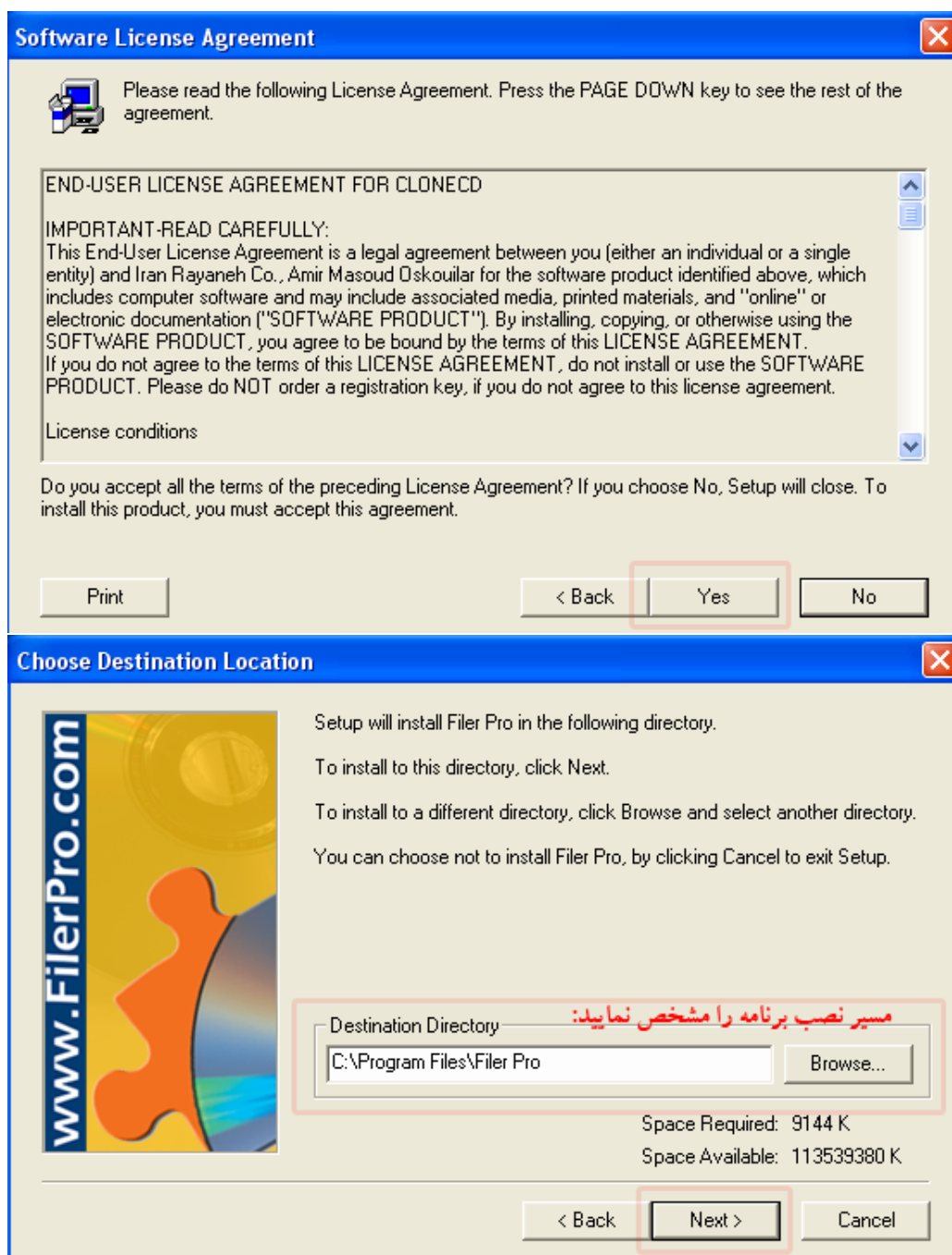


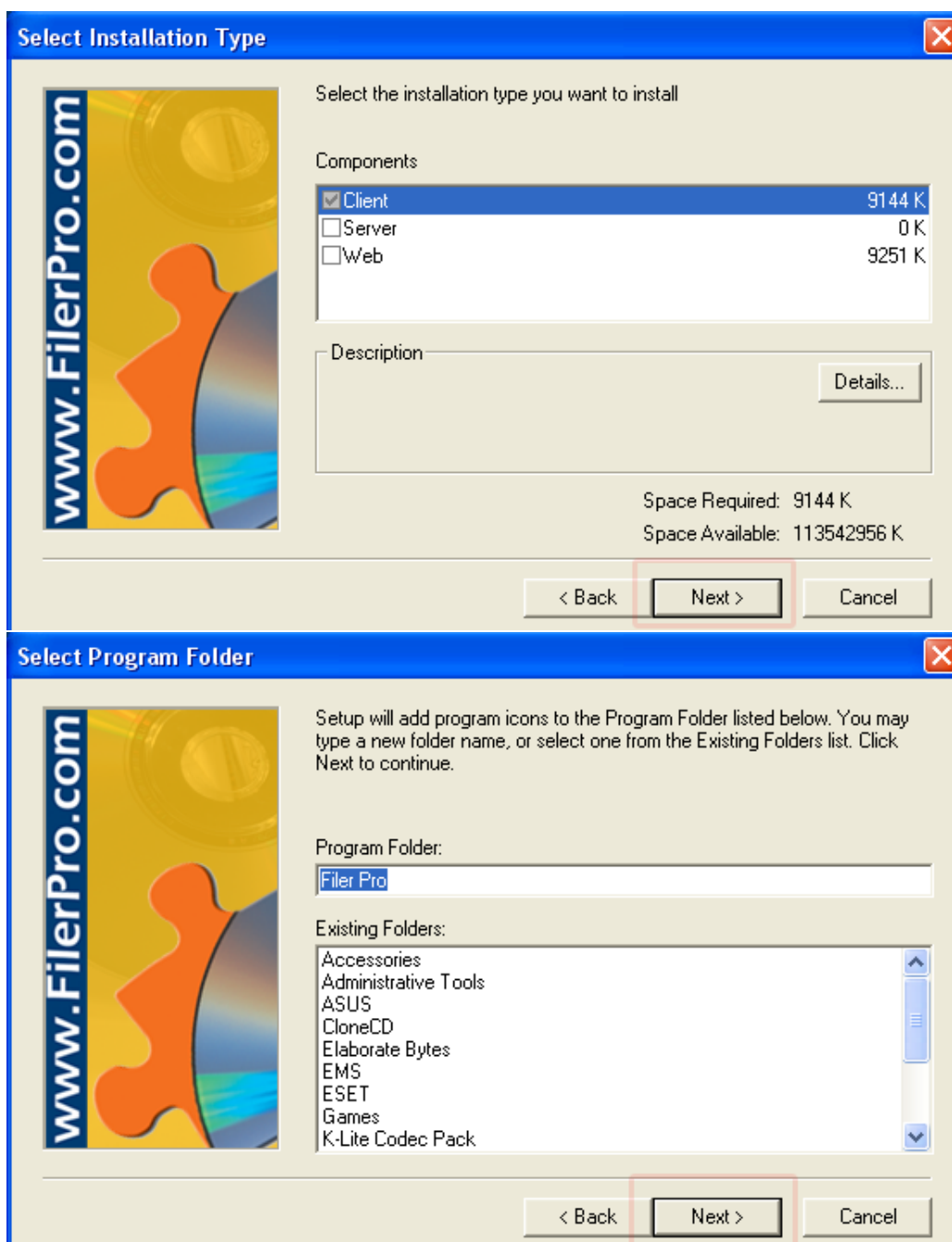


۴ - مطابق تصاویر زیر مراحل نصب را انجام دهید:





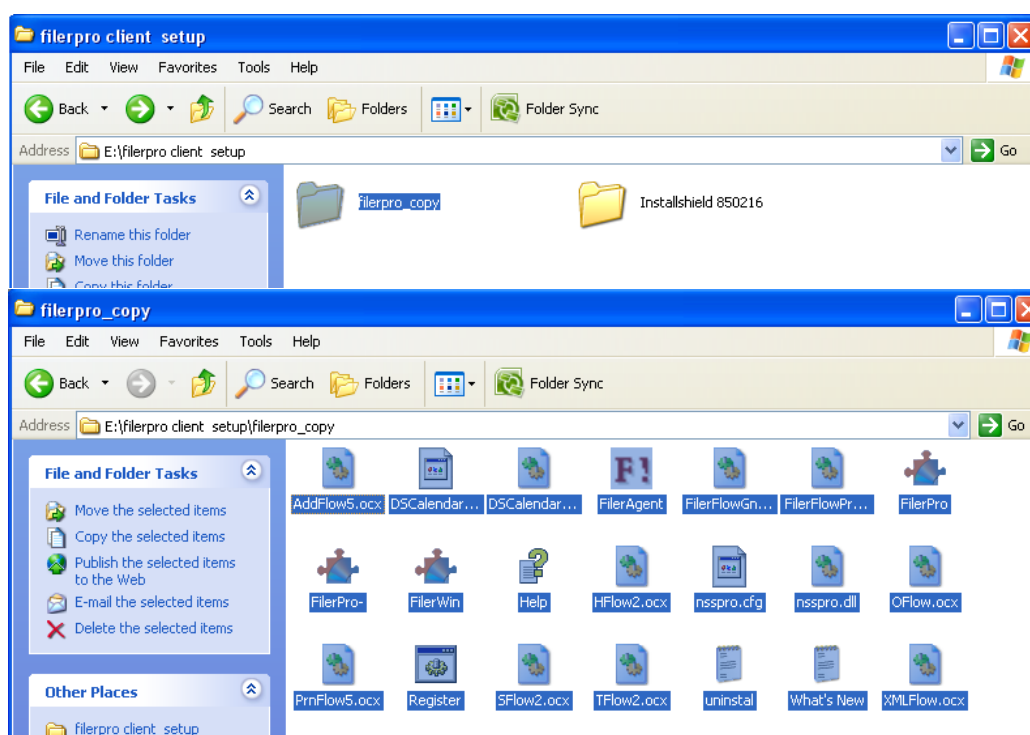








۵- اکنون نصب برنامه پایان یافته است، در پوشه filerpro client setup پوشه filerpro\_copy را باز نمایید و تمام فایل‌های آن را کپی نمایید:



۶- وارد مسیر نصب برنامه شده و فایل های کپی شده را ذخیره نمایید.

## ۱۰.۲ آموزش ساخت Vpn Connection در win xp

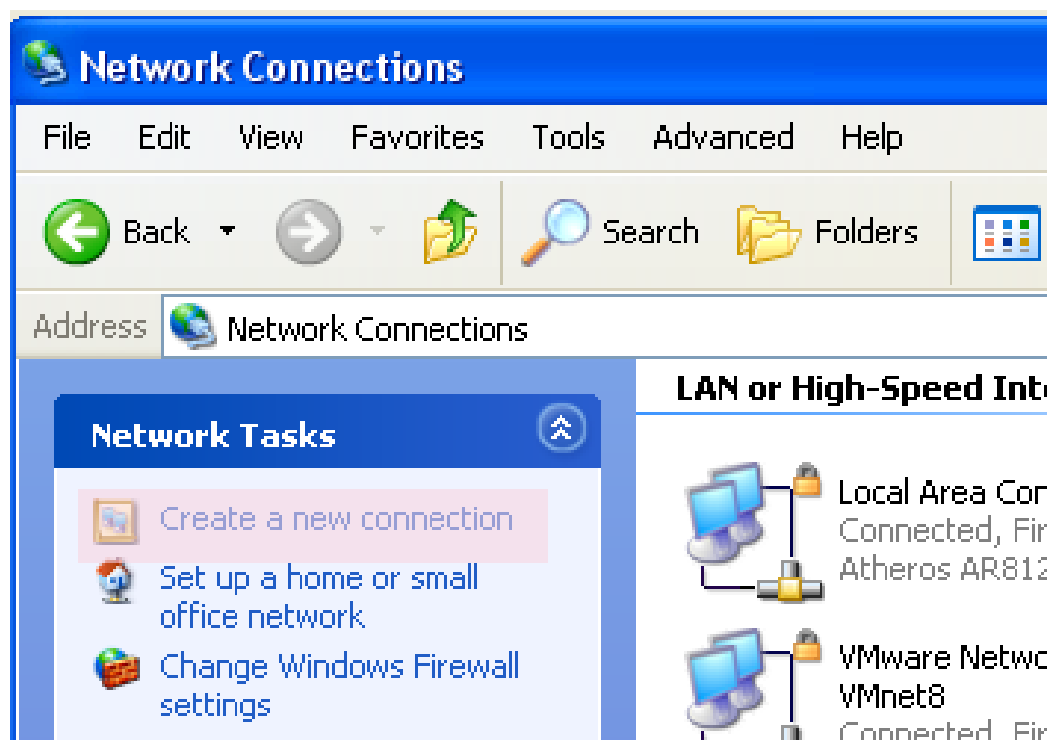
نحوه اتصال به شبکه دانشگاه

ایجاد یک کانکشن vpn طبق مراحل زیر انجام می گردد

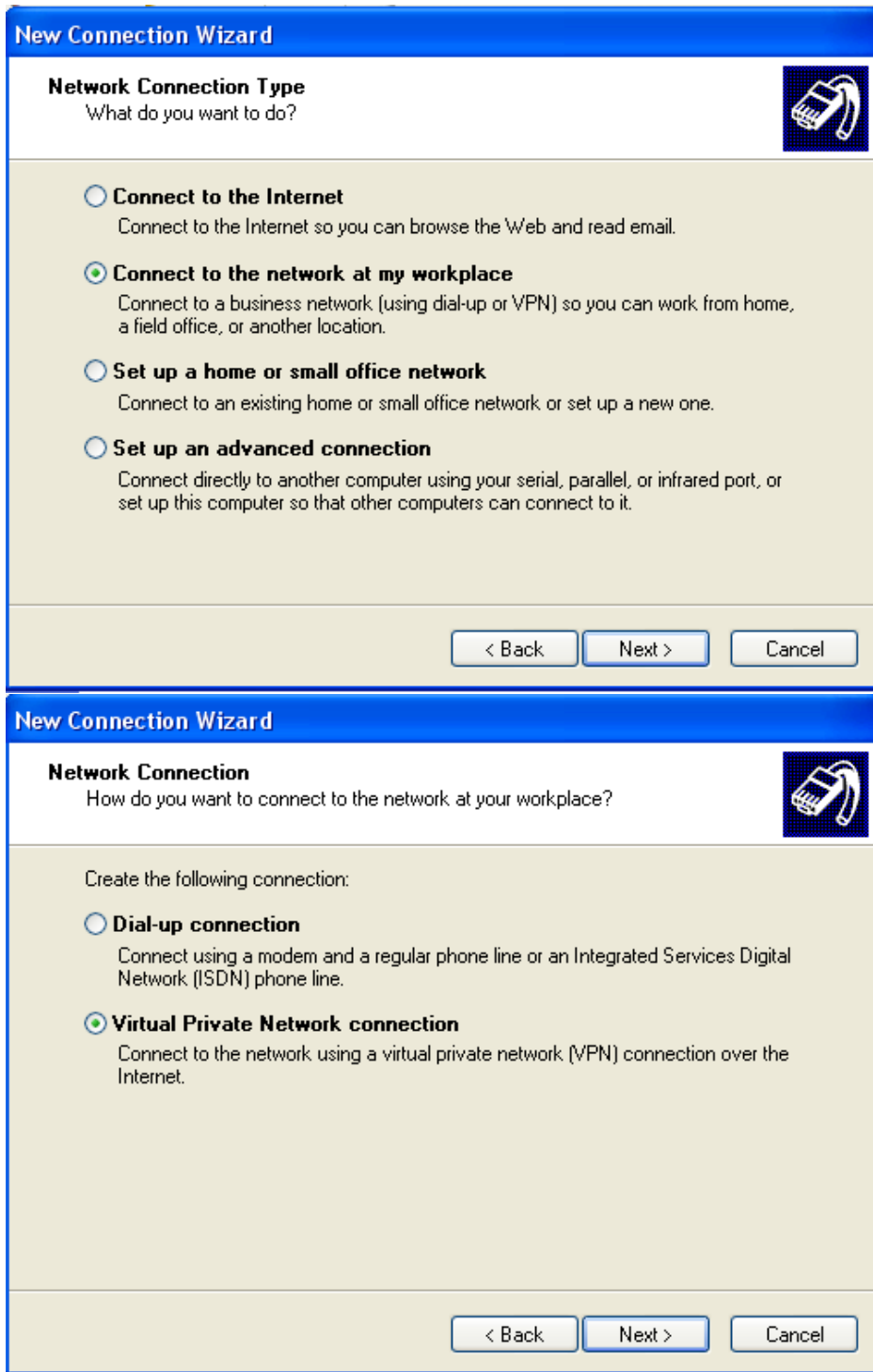
مسیر زیر را دنبال کرده تا وارد پنجره Network Connections شوید:

Start -> Control Panel -> Network Connections

در پنجره Network Connections (شکل زیر) روی گزینه Create a new connection کلیک نمائید تا ویزارد مربوط به ساختن یک ارتباط جدید ظاهر شود.

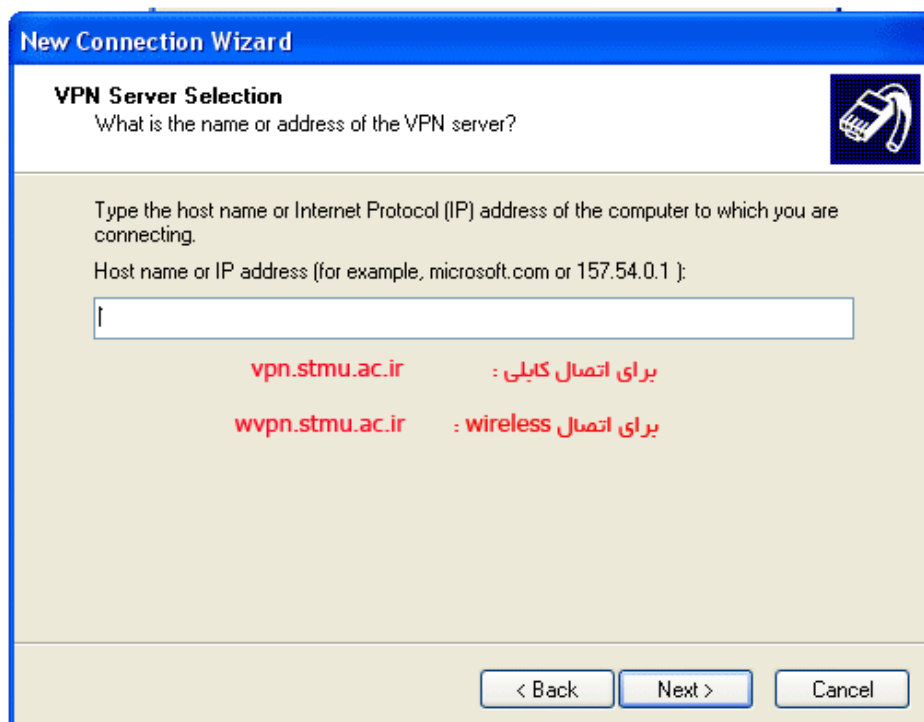


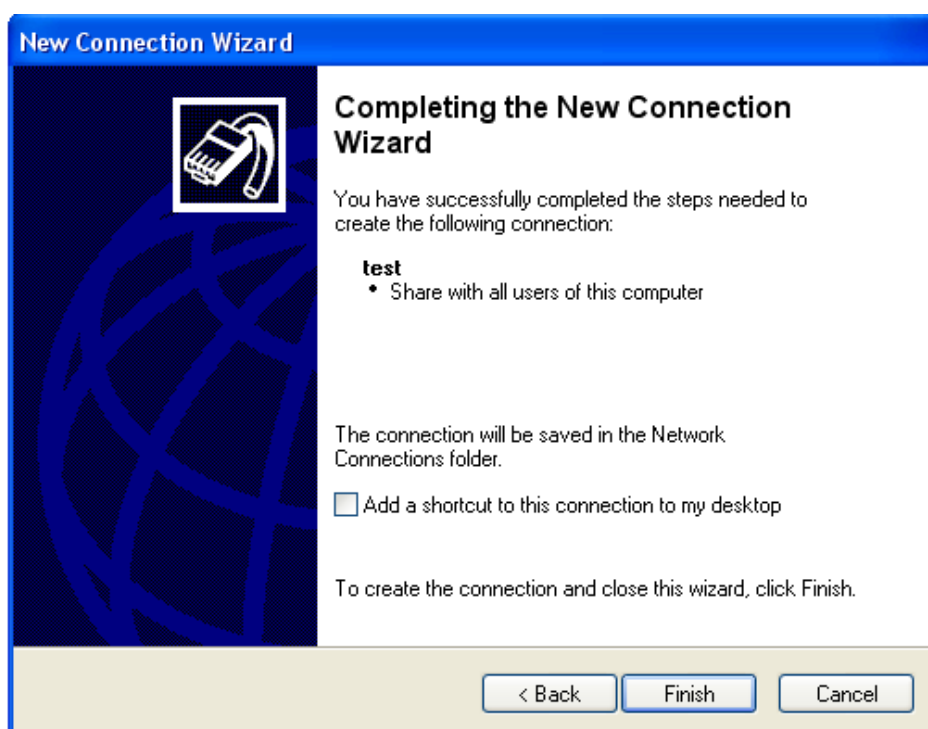
برای شروع کار با این ویزارد (شکل زیر)، ابتدا دکمه Next را فشار دهید، سپس گزینه Connect to the Network at my workplace را از فهرست مربوط انتخاب نمایید و برای ادامه کار دکمه Next را فشار دهید.





نشانی کامپیوتر VPN مورد نظر (که بعنوان مثال vpn.stmu.ac.ir یا .... می باشد) را مطابق شکل زیر در محدوده مورد نظر وارد کرده و دکمه Next را فشار دهید.



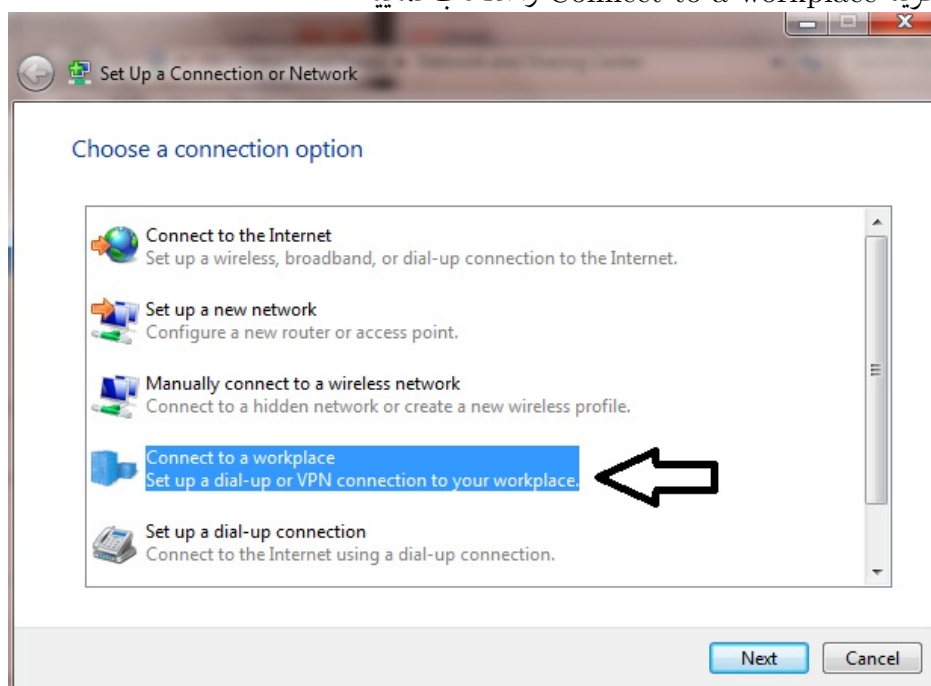




نحوه اتصال به شبکه دانشگاه  
ابتدا وارد Control panel شوید و روی Network and sharing center کلیک کنید  
روی گزینه Set up a new connections or network کلیک کنید

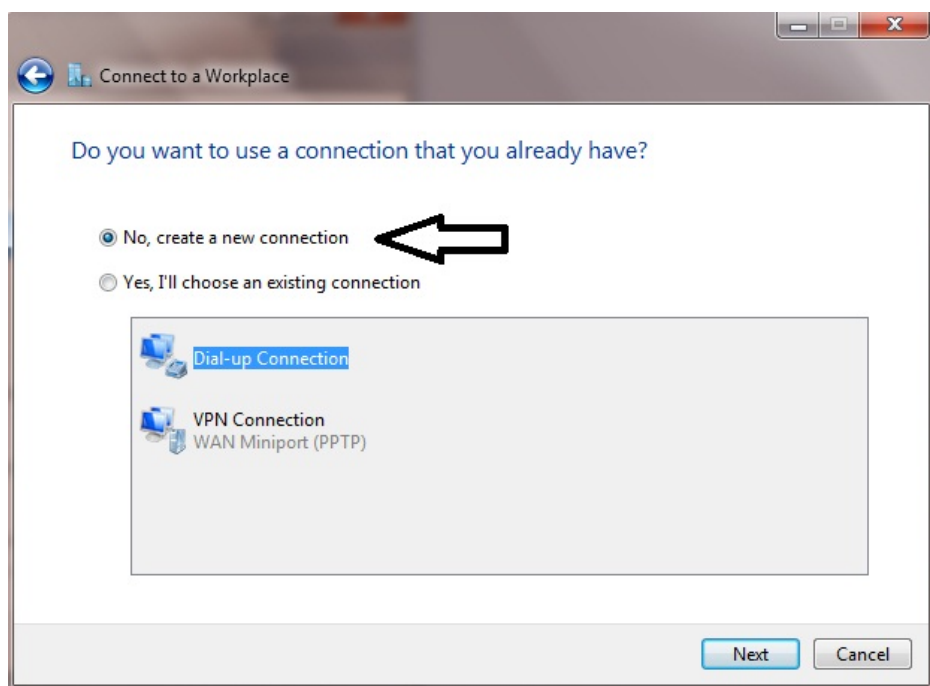


گزینه Connect to a workplace را انتخاب نمایید

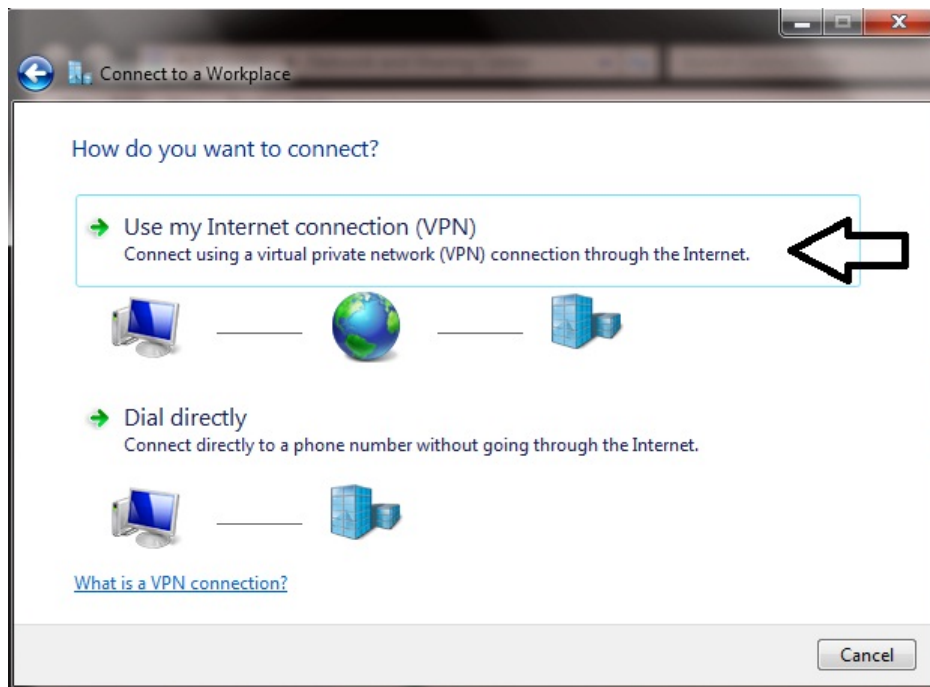


- و در مرحله بعدی همانطور که در عکس می بینید گزینه No, create a new connection را انتخاب کنید

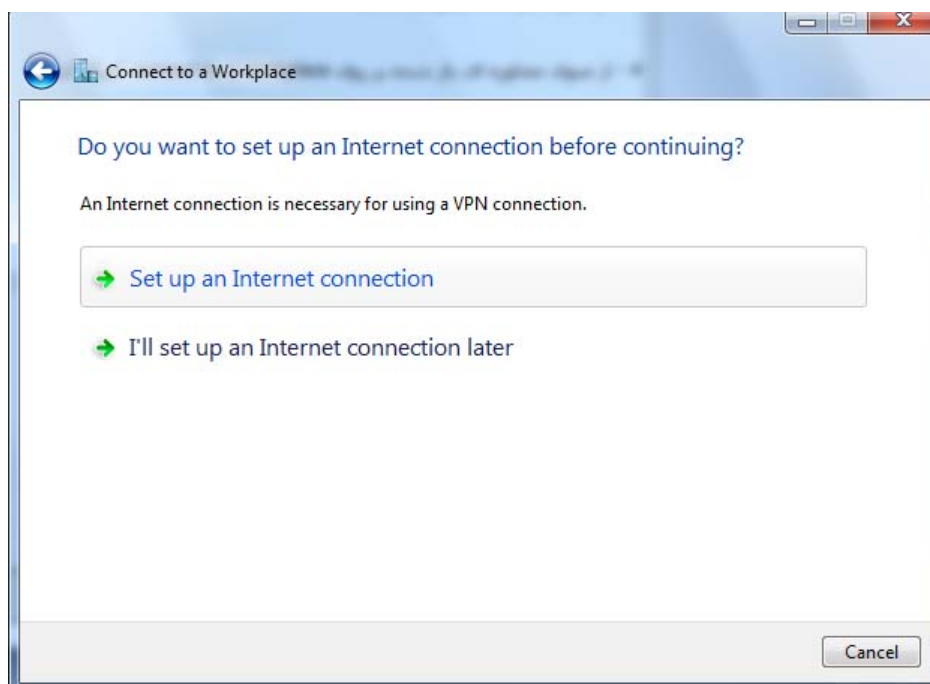




• سپس Use my Internet connection



در منوی بعدی آن باید بر روی گزینه set up an Internet Connection کلیک کنید



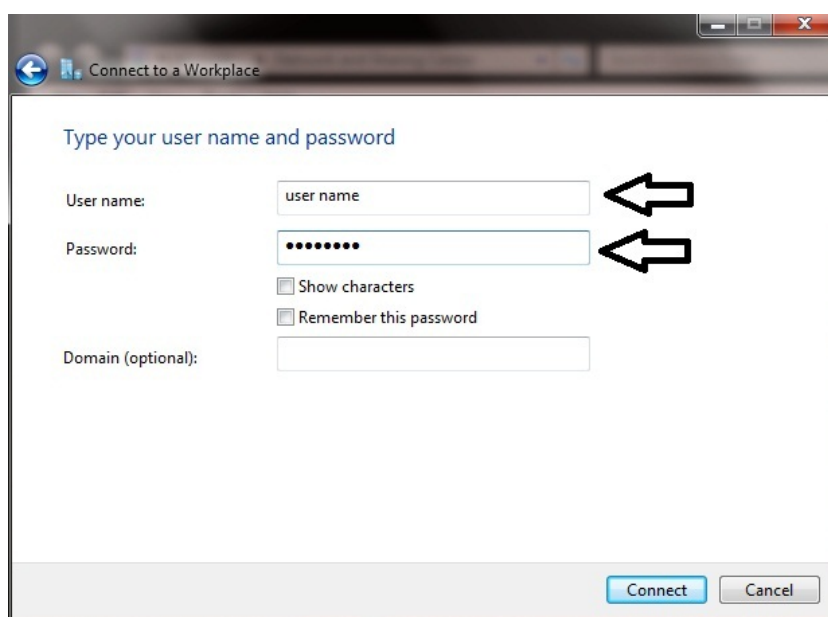
الف) در قسمت Internet Address، IP مورد نظر خود را وارد کنید  
 ب) در قسمت Destination name نام مورد نظر کانکشن خود را وارد کنید



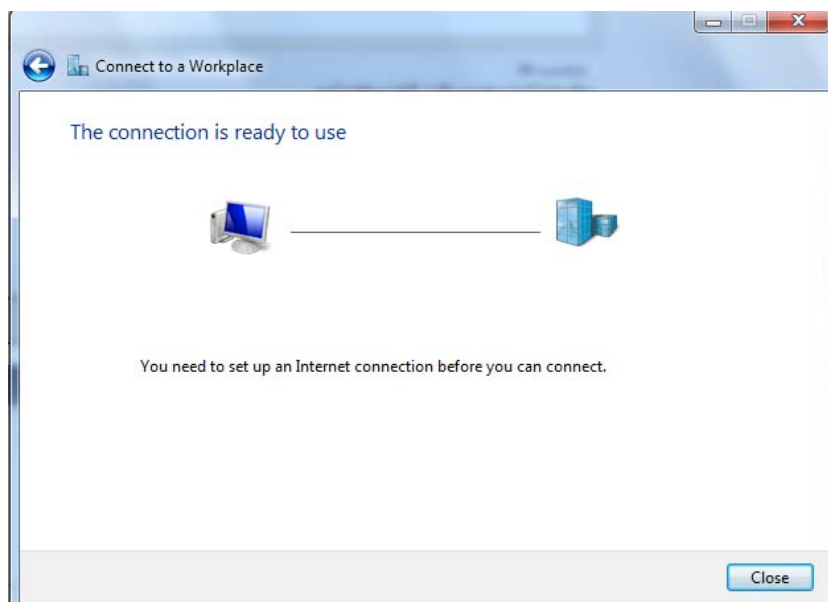
الف) در قسمت User name نام کاربری خود را وارد کنید  
 ب) در قسمت Password رمز عبور کانکشن خود را وارد کنید.  
 ج) با انتخاب چک باکس show Characters کلمات یا اعداد رمز عبور شما نمایان می شوند

د) با انتخاب چک باکس Remember this password کلمه عبور شما ذخیره می شود و در هر بار ورود به کانکشن رمز عبور شما در جای خود باقی است و نیازی به وارد کردن مجدد آن نیست

در آخر بر روی connect کلیک کنید



در صورتی که کانکشن شما با موفقیت ایجاد شود با تصویر زیر رو به رو خواهید شد :



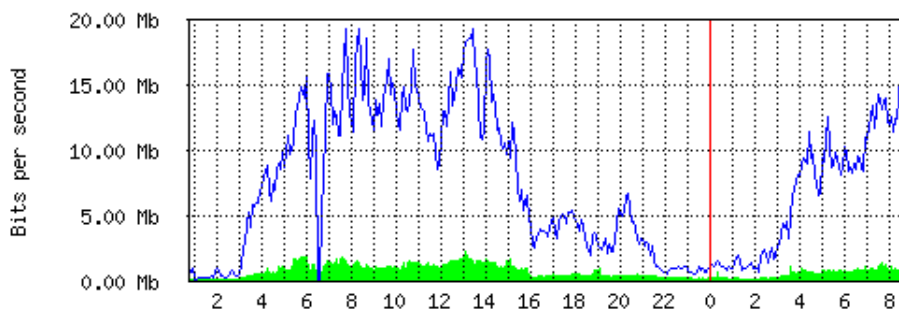
حال بر روی close کلیک کنید



موفق باشید

## ۱۱.۲ ترافیک اینترنت دانشگاه

گراف روزانه ترافیک اینترنت دانشگاه (آبی: ورودی، سبز: خروجی):



قابل ذکر است که در حال حاضر پهنای باند اینترنت دانشگاه ۲۵ مگابیت است و ۵ مگابیت جداگانه مخصوص سایتهای داخلی است که بدون برقراری اتصال VPN قابل استفاده است و جزو سهمیه اینترنت افراد محسوب نمی شود.

## ۱۲.۲ ارتقای وضعیت دسترسی دانشجویان دکترا به اینترنت

از مدتی قبل امکان استفاده بهتر از اینترنت دانشگاه در اتاق دانشجویان دکترای دانشکده مهندسی برق و کامپیوتر فراهم شده است. همچنین به جهت نیاز دانشجویان دکترا به دسترسی بیشتر به اینترنت، مهمانسرای دانشجویی دانشجویان دکترا، به صورت مستقل تحت پوشش اینترنت قرار گرفت... تجهیزات مورد استفاده، تجهیزاتی بودند که قرار بود در دانشکده مهندسی نفت مورد استفاده قرار گیرند که نظر به فوریت نیاز دانشجویان دکترا، در مهمانسرای دانشجویی نصب شدند. امیدواریم با رسیدن تجهیزات جدید، دانشکده مهندسی نفت نیز تحت پوشش وایرلس قرار گیرد.

## ۱۳.۲ نصب ویدئو پروژکتور در سایت دانشگاه



در هفته نخست آذرماه سایت دانشگاه به ویدئو پروژکتور تجهیز شد. این امر به جهت ارتقای کیفیت برگزاری کلاس ها و با تلاش مسئولین امر صورت پذیرفته است.

## ۱۴.۲ دسترسی همکاران به اینترنت ملی و سایت های داخلی



با تلاش همکاران فناوری اطلاعات دانشگاه امکان دسترسی به اینترنت از طریق اتصال VPN فراهم شده است...

بدین ترتیب همکاران گرامی قادر خواهند بود با ایجاد اتصال VPN به آدرس هاست : **Ivpn.stmu.ac.ir** از اینترنت استفاده نمایند. از طریق این اتصال می توانید سایت های داخل ایران از جمله سایت صدا و سیما و .... را بدون نیاز به اینترنت مشاهده نمایید.  
راهنمای ایجاد vpn connection

## ۱۵.۲ نحوه اتصال به شبکه دانشگاه



\*استفاده از سرویس شبکه کابلی و وایرلس مهمانسرای دانشگاه: استفاده از این سرویس از طریق اتصال vpn به آدرس **wvpn.stmu.ac.ir** : امکان پذیر است .  
\*استفاده از وایرلس: استفاده از سرویس وایرلس دانشگاه فقط از طریق اتصال VPN امکان پذیر است. کاربران گرامی جهت استفاده از وایرلس نیاز به اتصال VPN به آدرس : **wvpn.stmu.ac.ir** دارند.

\*استفاده از اینترنت : همکاران گرامی قادر خواهند بود با ایجاد اتصال VPN به آدرس هاست **Ivpn.stmu.ac.ir** از اینترنت استفاده نمایند. از طریق این اتصال می توانید سایت های داخل ایران از جمله سایت صدا و سیما و .... را بدون نیاز به اینترنت مشاهده نمایید.

## ۱۶.۲ قابل توجه همکاران گرامی



همکاران گرامی جهت رفع مشکل سخت افزاری و نرم افزاری سیستم با شماره داخلی ۲۱۲۵ تماس حاصل کرده یا در سیستم پشتیبانی و خدمات رسانی (تیکت) دانشگاه به نشانی <http://ticket.sttu.ac.ir> درخواست خود را برای بخش پشتیبانی نرم افزاری-سخت افزاری ارسال نمایند.

همکاران محترم می توانند با نام کاربری و کلمه عبور دامین (نام کاربری و کلمه عبور اینترنت) خود وارد سیستم شوند.

## ۱۷.۲ افزایش سقف حجم دانشجویان دکترا

سقف حجم دانشجویان دکتری از تاریخ ۹۰/۹/۱۹ به دو برابر افزایش یافت.

## ۱۸.۲ تلفن اینترنتی



با پیگیری مجموعه دانشگاه بستر لازم برای استفاده از تلفن اینترنتی (VoIP) فراهم شد.

سرور مورد نیاز سیستم فوق نصب و ارتباط آن با سیستم تلفن آنالوگ فعلی دانشگاه برقرار گردید. امیدوار هستیم به مرور عموم کارکنان دانشگاه از امکانات این سیستم بهره مند شوند. به لحاظ نیاز مهمانسرای تازه تاسیس دانشگاه به خط تلفن، به جای استفاده از تلفنهای آنالوگ و با هزینه ای کمی بیشتر از هزینه کابل کشی، از مرکز تلفن آنالوگ تا مهمانسرا، بستر لازم برای استفاده کل دانشگاه از تلفن اینترنتی فراهم شد.

## ۱۹.۲ سرور چمران گروه فیزیک برای اساتید

با مساعدت و همکاری گروه فیزیک دانشگاه، امکان استفاده از سرور «chamran» این گروه برای اساتید دانشگاه فراهم شده است.

در حال حاضر در این سرور برخی نرم افزارها همچون MATLAB و TeXWorks وجود دارند که حسب نیاز، موارد جدیدی نصب خواهند شد.





## ۲۰۰۲ راهنمای سیستم پست الکترونیکی دانشگاه



قابل توجه کلیه اساتید محترم و کارکنان گرامی: به اطلاع میرساند سامانه جدید پست الکترونیکی دانشگاه از روز چهارشنبه بصورت آزمایشی راه اندازی می شود و کاربران گرامی جهت ارسال و دریافت پست الکترونیکی بایستی به آدرس [mail.sttu.ac.ir](mailto:mail.sttu.ac.ir) مراجعه نمایند. شناسه کاربری و رمز ورود شما مطابق با شناسه دومین (همان شناسه ای که به اینترنت وصل میشوید) میباشد و آدرس پست الکترونیکی شما بصورت زیر است [domainusename@sttu.ac.ir](mailto:domainusename@sttu.ac.ir) به عنوان نمونه آدرس پست الکترونیکی آقای حسینی با شناسه کاربری [m.hoseini@sttu.ac.ir](mailto:m.hoseini@sttu.ac.ir) این گونه است:

برای کاربرانی که دارای آدرس پست الکترونیکی متفاوت با شناسه دومین می باشند تمهیدی اندیشیده شده است که بتوانند بطور همزمان دارای دو آدرس پست الکترونیکی باشند که نحوه استفاده از این امکان تا ساعت ۱۲ ظهر روز چهارشنبه روی این وب سایت قرار خواهد گرفت. برای دسترسی به ایمیلهای قبلی خود، به آدرس <http://oldmail.sttu.ac.ir> مراجعه فرمایید.

**\*\* لطفاً قبل از شروع کار با سامانه پست الکترونیکی جدید سوالات متداول و راهنمای سامانه را مطالعه نمایید .**

**\*\* کاربران گرامی میتوانند سوالات و یا اشکالات خود را از طریق سیستم پشتیبانی مطرح نموده و جواب و یا راهنمایی لازم را دریافت دارند**

## ۲۱.۲ اصلاح سیستم صفحات شخصی اساتید



سرور صفحات شخصی اساتید (profsite) به همراه موتور وردپرس نصب شده بر روی آن بروزرسانی گردیدند. لذا خطاری که پیش از این برخی ویروس‌یابها در هنگام ورود به صفحات شخصی اساتید صادر می نمودند، برطرف شده است.

## ۲۲.۲ تغییر نام دانشگاه



دانشگاه حکیم سبزواری

با توجه به تغییر نام دانشگاه، مدیریت فناوری دانشگاه نسبت به تغییر لوگو و عناوین وب سایت های تحت حوزه ی خود اقدام کرده است. لذا چنانچه اساتید، همکاران و دانشجویان مواردی را مشاهده نمودند که تغییر پیدا نکرده است به این مدیریت اطلاع دهند:  
پست الکترونیک: a.zahedi@sttu.ac.ir

## ۲۳.۲ رتبه دانشگاه در رتبه بندی جهانی وبومتریکی

با اعلام آخرین نتایج رتبه بندی جهانی وب گاه های دانشگاهی که به «وبومتریکی» مشهور است، دانشگاه حکیم سبزواری در رتبه ۸۹۷۴ جهانی قرار دارد:

[http://www.webometrics.info/rank\\_by\\_country.asp?country=ir&offset=100](http://www.webometrics.info/rank_by_country.asp?country=ir&offset=100)

## ۲۴.۲ استفاده از شبکه مهمانسرا



استفاده از سرویس شبکه کابلی و وایرلس مهمانسرای دانشگاه فقط از طریق اتصال vpn به آدرس: [wvpn.stmu.ac.ir](http://wvpn.stmu.ac.ir) امکان پذیر است.

## ۲۵.۲ قابل توجه کاربران گرامی



سیستم ها و لپ تاپ هایی که دارای آنتی ویروس نامناسب ، و بدون بروز رسانی و همچنین ویندوز بدون بروز رسانی باشند، بصورت خودکار از شبکه وایرلس قطع خواهند

شد.

## ۲۶.۲ سامانه تشکلهای دانشجویی



سامانه تشکلهای دانشجویی، بستری برای فعالیت و انتشار مطالب هر انجمن و کانون در دانشگاه می باشد. هر انجمن می تواند برای ثبت نام در این سامانه به معاونت فرهنگی مراجعه نموده و نام کاربری و پسورد خود را دریافت نماید.

## ۲۷.۲ سامانه مدیریت وبلاگ دانشگاه



سامانه مدیریت وبلاگ با هدف ایجاد صفحه شخصی برای کارمندان محترم و دانشجویان، در مدیریت فناوری اطلاعات راه اندازی شده است. در مرحله نخست امکان ثبت نام برای دانشجویان مقطع دکتری وجود دارد.

## ۲۸.۲ آخرین اطلاعات از تغییر دامنه وبسایت های دانشگاه

با توجه به تغییر نام دانشگاه به حکیم سبزواری و بنا بر مصوبه معاونت پژوهشی و فناوری دانشگاه، دامنه وب سایت های دانشگاه از **sttu** به **hsu** تغییر پیدا کرده است. لذا اساتید، دانشجویان و همکاران گرامی جهت درج نشانی وبسایت های دانشگاه از دامنه جدید استفاده نمایند. لازم به ذکر

است که دامنه قبلی (sttu) تا پایان شهریور فعال می باشد.....

- \* صفحات شخصی اساتید از نشانی profsite.sttu.ac.ir به profs.hsu.ac.ir تغییر یافت. (به تصمیم کمیته فناوری اطلاعات دانشگاه به جای اصطلاح profsite از profs استفاده می شود)
- \* پست الکترونیکی دانشگاه (mail.hsu.ac.ir)
- \* وبلاگ دانشجویان از نشانی blog.sttu.ac.ir به sites.hsu.ac.ir تغییر یافت. (به تصمیم کمیته فناوری اطلاعات دانشگاه به جای اصطلاح blog از sites استفاده می شود)
- \* مدیریت فناوری اطلاعات (it.hsu.ac.ir)
- \* سامانه تشکلهای دانشجویی (farhangi.hsu.ac.ir)

## فصل ۳

# پرسش و پاسخ پیرامون پست الکترونیکی جدید دانشگاه

ضعیف بودن موتور ایمیل سرور قبلی دانشگاه و عدم استقبال اعضای هیات علمی و سایر همکاران دانشگاه از آن سیستم، این مجموعه را بر آن داشت تا نسبت به تعویض ایمیل سرور اقدام نماید. پس از بررسی‌های مختلف کارشناسی، موتور Zimbra انتخاب گردید. یک شرکت ایرانی این ایمیل سرور را به قیمت ۷ میلیون تومان عرضه می‌نمود. با همکاری یکی از دانشجویان کامپیوتر دانشگاه در قالب کارآموزی و همت کارشناسان فناوری این ایمیل سرور بدون هیچ هزینه‌ای در سرور دانشگاه نصب شد و عملیات انتقال حسابها از سرور قبلی به ایمیل سرور جدید نیز انجام شد. آدرس پست الکترونیک جدید دانشگاه: <http://mail.sttu.ac.ir> است و همکاران گرامی با همان حساب کاربری اینترنت خود می‌توانند از آن استفاده نمایند.

حسب نیاز همکاران گرامی، مجموعه‌ای از صفحات وب برای پاسخگویی به پرسشهای معمول کاربران در این زمینه نیز آماده و در وب سایت فناوری اطلاعات قرار گرفت که در این فصل بخشی از آنرا شاهد هستید.

به جز موارد توضیح داده شده، موارد ذیل نیز در سایت فناوری بیان شده‌اند.

### ● دریافت ، نمایش و مدیریت ایمیل ها

- تنظیم نحوه نمایش ایمیل ها
- فرمت نمایش ایمیل ها
- چاپ نامه
- مدیریت ایمیل ها
- خالی کردن پوشه سطل آشغال (Trash)
- هرزنامه ها

### ● ایجاد و ارسال ایمیل

- Forward یک ایمیل
- Forward تنظیم یک آدرس برای ایمیل ها
- استفاده از Spell Check
- اضافه کردن فایل ضمیمه به ایمیل
- ایجاد یک امضا جدید ( Signature )
- امضای پیش فرض (تنظیم Default)

### ● Filter (فیلتر)

- ایجاد یک Filter
- ایجاد یک فیلتر از یک ایمیل
- غیرفعال کردن فیلتر
- ترتیب فیلتر ها
- اجرا کردن فیلتر روی ایمیل های موجود

### ● دفترچه آدرس ها ( Address Book )

- ایجاد تماس (Contact) جدید
- اضافه کردن تماس (Contact) جدید از ایمیل
- اضافه کردن آدرس ها از طریق دفترچه آدرس ها (Address Book) برای ارسال ایمیل
- امکان Import کردن دفترچه آدرس ها (Address Book) به فرمت (.csv)
- Export کردن دفترچه آدرس ها (Address Book) به فرمت (.csv)
- چاپ دفترچه آدرس ها (Address Book)
- ایجاد گروه تماس (Group Contact)
- انتقال ایمیل های موجود در پوشه ورودی به سیستم خود ( به صورت فایل zip).

## ۱.۳ در مواردی که حجم ورودی پر شده پیغام خطا دریافت می شود چگونه مشکل حل می گردد؟

وقتی که فضای پست الکترونیکی ( quota ) پر شده باشد این اخطار می آید که باید ایمیل های اضافی در خروجی و هرزنامه ها را حذف کنیم لازم به ذکر است حتما فولدر سطل آشغال را خالی کنیم

## ۲.۳ چرا به صورت خیلی اتفاقی Inbox پست الکترونیکی خالی می شود؟

در صورتی که شما Microsoft Outlook را باز نمایید به صورت خودکار تنظیمات صورت گرفته و ایمیل‌های شما وارد Outlook می شود این امر باعث می شود ایمیل‌هایتان از روی سرور میل دانشگاه پاک گردد. که در این صورت در منوی Start گزینه all program و سپس office Microsoft بروی گزینه Microsoft Outlook کلیک نمایید اطلاعات خود را در این قسمت خواهید دید.

## ۳.۳ چرا نمی توانیم ایمیل خود را با ضمیمه ارسال نمایم؟

- ۱- در صورتی می توانیم فایل هایی را پیوست یک میل کنیم که فایلها از نوع ،exe، dll، bat، chm ،com، hlp، js، jse نباشند
- ۲- حجم فایل بیشتر از ۹ مگابایت نباشد

## ۴.۳ چرا هیچ ایمیلی در یافت نمی شود؟

- به دو دلیل کاربر ممکن که نتواند ایمیل دریافت کند.
- ۱- فضای در نظر گرفته شده میل پر شده باشد
- ۲- میل به جایی دیگر forward شده باشد



## ۵.۳ آیا با استقرار سیستم جدید، آدرس پست الکترونیکی من با آدرس قبلی متفاوت میشود؟

کاربرانی که شناسه ورود آنها به سیستم (domain) با شناسه پست الکترونیکی آنها یکسان است دارای آدرس پست الکترونیکی یکسان با قبل میباشند. مثلا کاربری که شناسه doamin وی -hos

seini میباشد و شناسه پست الکترونیکی وی نیز hosseini باشد دارای پست الکترونیکی با آدرس `hosseini@sttu.ac.ir` میباشد.

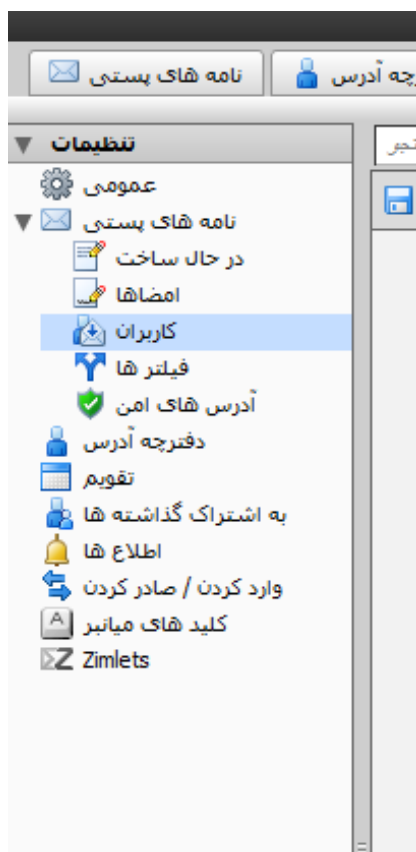
در این سیستم کاربرانی که شناسه domain آنها با شناسه پست الکترونیکی آنها متفاوت است همزمان دارای دو آدرس پست الکترونیکی میباشند و میتوانند از هر دو آدرس برای دریافت و ارسال نامه الکترونیکی استفاده کنند. مثلاً کاربری که شناسه domain وی hosseini و شناسه پست الکترونیکی وی m.hosseini میباشد در این سیستم دارای دو آدرس پست الکترونیکی `hosseini@sttu.ac.ir` و `m.hosseini@sttu.ac.ir` میباشد و میتواند از هر دو آدرس استفاده کند. (بدلیل محدودیت در ارائه این امکان، اعضای هیات علمی در اولویت میباشند)

تنظیمات لازم برای استفاده همزمان از دو آدرس پست الکترونیکی در مورد کاربرانی که شناسه domain آنها با شناسه پست الکترونیکی آنها متفاوت است

۱- ورود به سامانه پست الکترونیکی

۲- انتخاب گزینه تنظیمات

۳- انتخاب گزینه کاربران



۴- انتخاب گزینه add persona






۵- انتخاب آدرس پست الکترونیکی سیستم قدیم (کاربرانی که آدرس پست الکترونیکی قدیم خود را در این گزینه مشاهده نمیکنند میتوانند به آدرس [email@sttu.ac.ir](mailto:email@sttu.ac.ir) نامه ارسال نموده و با ذکر نام و نام خانوادگی و آدرس قدیم خود نسبت به اضافه شدن آدرس قدیم خود اقدام نمایند)

۶- انتخاب گزینه ذخیره کردن از بالای صفحه

## ۶.۳ چگونه هرزنامه ها را در ایمیل خود کاهش دهیم؟

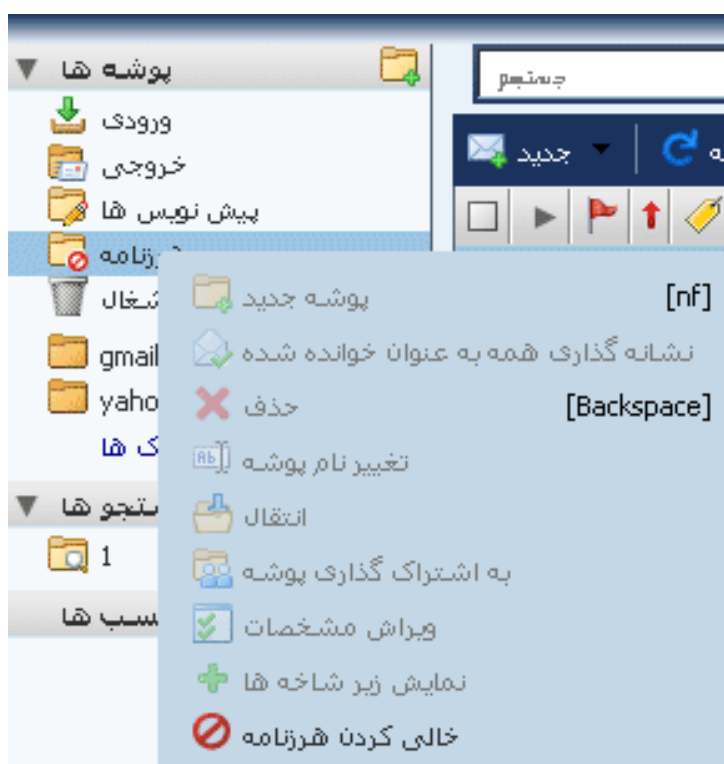
در صورتی که شما ایمیل هایی را از یک فرد خاص دریافت می کنید که مایل به دریافت آن ها نیستید می توانید آن ها را به عنوان هرزنامه یا Spam معرفی کنید تا میل سرور ایمیل های دریافتی از آن فرد را در پوشه هرزنامه قرار دهد.

برای این کار روی ایمیل کلیک کرده و روی گزینه

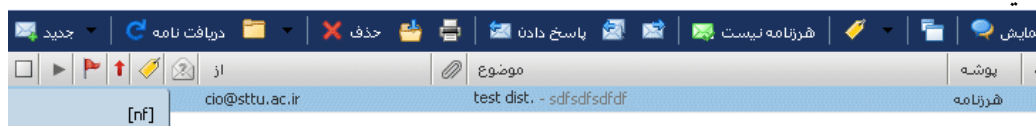
هرزنامه  در منوی بالا کلیک کنید.

در این صورت پس از چندین بار تکرار این عمل تمام ایمیل های دریافتی از آن فرد خاص در این پوشه قرار می گیرد .

در صورتی که می خواهید تمام ایمیل های موجود در پوشه Junk را پاک کنید بر روی آن کلیک راست نموده و گزینه خالی کردن هرزنامه را انتخاب کنید.



اگر ایمیل های یک فرد خاص را به اشتباه به عنوان هرزنامه معرفی کرده اید و مایلید آن ها را به پوشه ورودی خود بازگردانید ایمیل را انتخاب کنید و گزینه هرزنامه نیست را در منوی بالا انتخاب کنید.



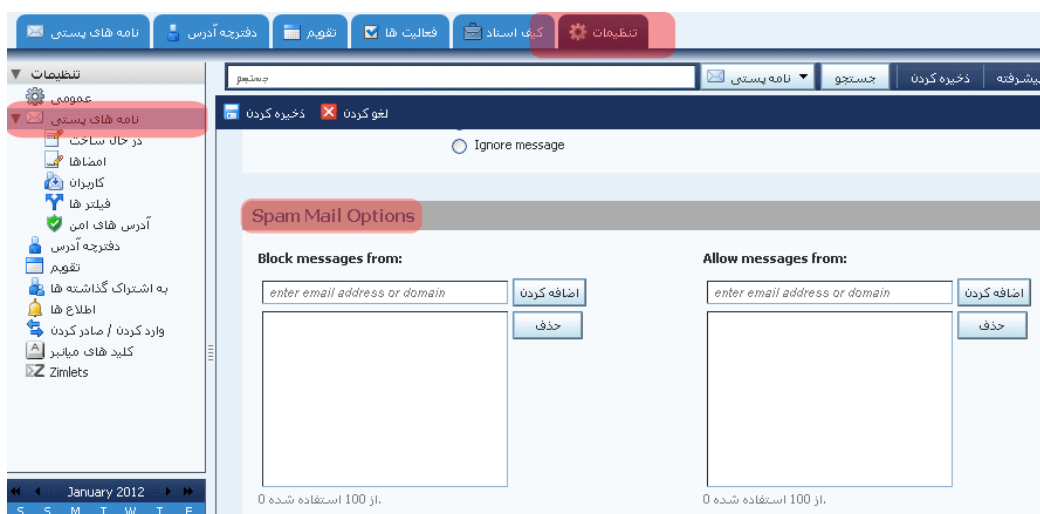
**نکته:** در صورتی که فردی برای شما ایمیل ارسال کند و به همراه ایمیل خود ویروس داشته باشد این ایمیل ها در پوشه هرزنامه قرار می گیرند و پس از مدتی تمام ایمیل های آن فرد در پوشه هرزنامه قرار می گیرد برای رفع این مشکل باید چندین بار ایمیل های آن فرد را به عنوان هرزنامه معرفی کنید بدین صورت که ایمیل ها را انتخاب کنید و گزینه هرزنامه نیست را بزنید و همچنین آن فرد باید سیستم خود را از ویروس پاک کند.

روش دیگری هم برای مسدود کردن (block) ایمیل های دریافتی وجود دارد. در این روش برخی ایمیل آدرس ها را که مایل به مسدود کردن آن ها هستید در لیست Block Messages From قرار می دهید. همچنین آدرس هایی که مایلید همیشه ایمیل هایشان را دریافت کنید در لیست Allow Messages From قرار می دهید.

برای این کار:

در منوی تنظیمات در پوشه نامه های پستی ( سمت چپ ) در قسمت Spam Mail Options آدرس مورد نظر خود را اضافه کنید و سپس گزینه Save در Toolbar بزنید.

۷.۳. چگونه اطلاعات شخصی مربوط به ACCOUNT خود ( FIRST NAME ، LAST NAME ) را تغییر داد؟ ۵۱



۷.۳ چگونه اطلاعات شخصی مربوط به Account خود ( last name ، first name ) را تغییر داد؟

در صورتی که بخواهیم اطلاعات شخصی خود را در ایمیل تغییر دهیم بر روی گزینه تنظیمات کلیک کرده در سمت چپ صفحه بر روی گزینه کاربران کلیک کرده سپس اطلاعات شخصی خود را قسمت Messages Sent from this account have the following settings تغییر می دهیم.



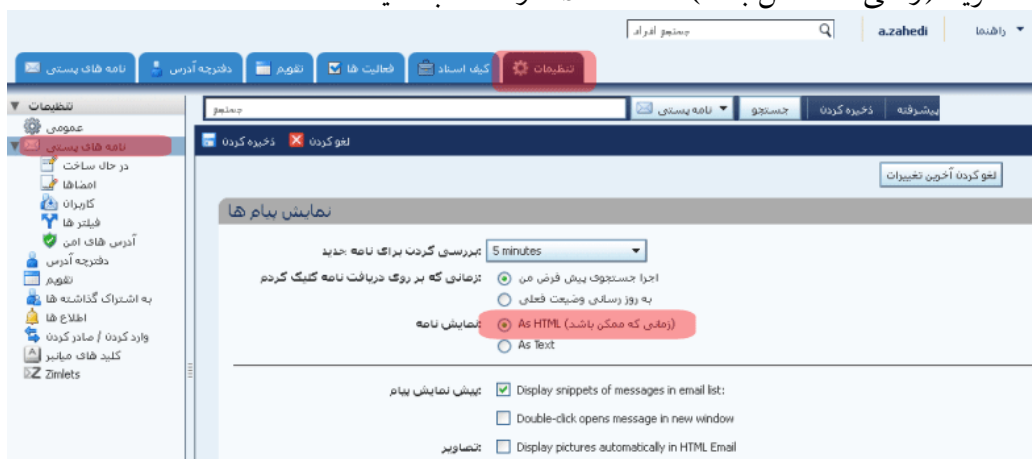
۸.۳ چگونه تصاویر موجود در متن دیده شود؟

برای مشاهده ایمیل هایی که ترکیبی از متن و عکس هستند باید فرمت نمایش ایمیل خود را HTML قرار دهید .

۹.۳. چگونه می توانیم ایمیل های موجود در هر پوشه ورودی به سیستم خود ( به صورت فایل ZIP). انتقال دهیم؟

۵۲

- برای این کار:
- ۱- در منوی تنظیمات وارد پوشه نامه های پستی (در سمت چپ) شوید.
  - ۲- گزینه (زمانی که ممکن باشد) As HTML را انتخاب کنید.



۹.۳ چگونه می توانیم ایمیل های موجود در هر پوشه ورودی به سیستم خود ( به صورت فایل zip). انتقال دهیم؟

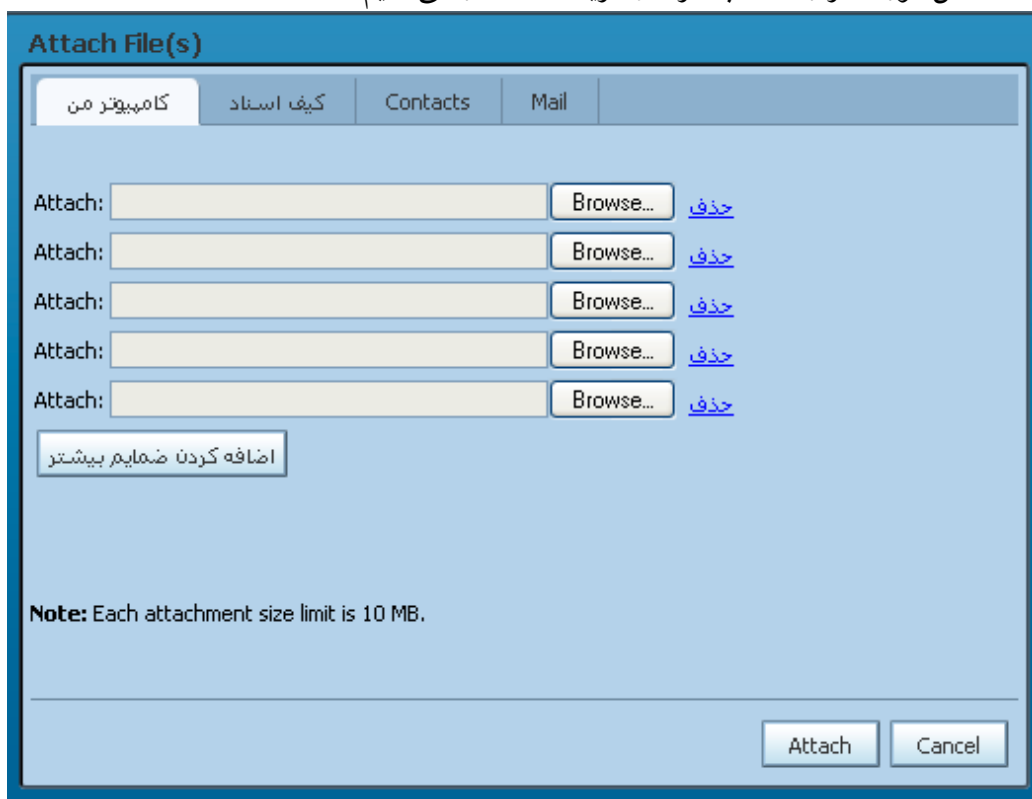
در نوار آدرس موجود در IE خود آدرس زیر را وارد کنید <http://mail.hsu.ac.ir/service/home/~/Inbox.zip> در account خود login نکرده باشید دیالوگ زیر ظاهر می شود و Username و Password را می پرسد. اطلاعات را وارد کنید و دکمه OK را بزنید. ( اگر قبلا در account خود login کرده باشید این مرحله را نخواهید دید) پس از ظاهر شدن دیالوگ ذخیره سازی با زدن گزینه Save و سپس مشخص کردن مسیر ذخیره سازی، این کار انجام می گیرد و ایمیل های موجود در پوشه Inbox به صورت یک فایل zip در مسیر مشخص شده ذخیره می شود.

۱۰.۳ چگونه می توانیم عکس در متن نامه قرار دهیم؟

ابتدا یک میل جدید باز می کنیم سپس بر روی قسمت اضافه کردن ضمیمه کلیک می نمایم



عکس مورد نظر را انتخاب کرده و گزینه attach را می کنیم.



### ۱۱.۳ چگونه می توانیم به گیرنده اهمیت نامه را اعلام نماییم؟

در مواردی که به خواهید اهمیت و فوریت نامه را به شخصی که ایمیل شما را دریافت می کند نمایش دهید زمانی که میل خود را باز می کنید در کنار box مربوط به موضوع در قسمت اولویت گزینه بالا را انتخاب نمایید



### ۱۲.۳ چگونه یک نامه در پست الکترونیکی پرینت گرفته شود؟

برای چاپ نامه:

۱- روی ایمیل موردنظر کلیک کنید

۲- سپس از منوی بالا گزینه



را انتخاب کنید

۳- پنجره استاندارد پرینت باز می شود. سپس پرینتر موردنظر خود را انتخاب کنید و روی گزینه ok کلیک کنید.

**دقت کنید که از گزینه Print در منوی file از Browser استفاده نکنید.**

پس از انتخاب گزینه Print دو پنجره ظاهر می شود که یک پنجره متن نامه ها را برای چاپ نمایش می دهد و دیگری جهت تنظیمات چاپ می باشد. در صورتی که سایز فونت مناسب نیست و مایل به تغییر آن هستید ابتدا دیالوگ مربوط به تنظیمات پرینت را بسته سپس در بالای پنجره ای که متن نامه ها را نمایش می دهد روی علامت + و یا - کلیک کنید و پس از انتخاب سایز مناسب از منوی file گزینه Print را انتخاب کنید.

برای چاپ نامه های موجود در یک دسته (Conversation) ابتدا روی آن دسته کلیک راست نموده و سپس گزینه Print را بزنید. بقیه مراحل همانند بالا می باشد.

### ۱۳.۳ شناسه کاربری و رمز ورود برای استفاده از سیستم جدید پست الکترونیکی چیست؟

شناسه کاربری و رمز ورود شما برای استفاده از سیستم پست الکترونیکی با شناسه کاربری و رمز ورود شما در domain یکسان است.

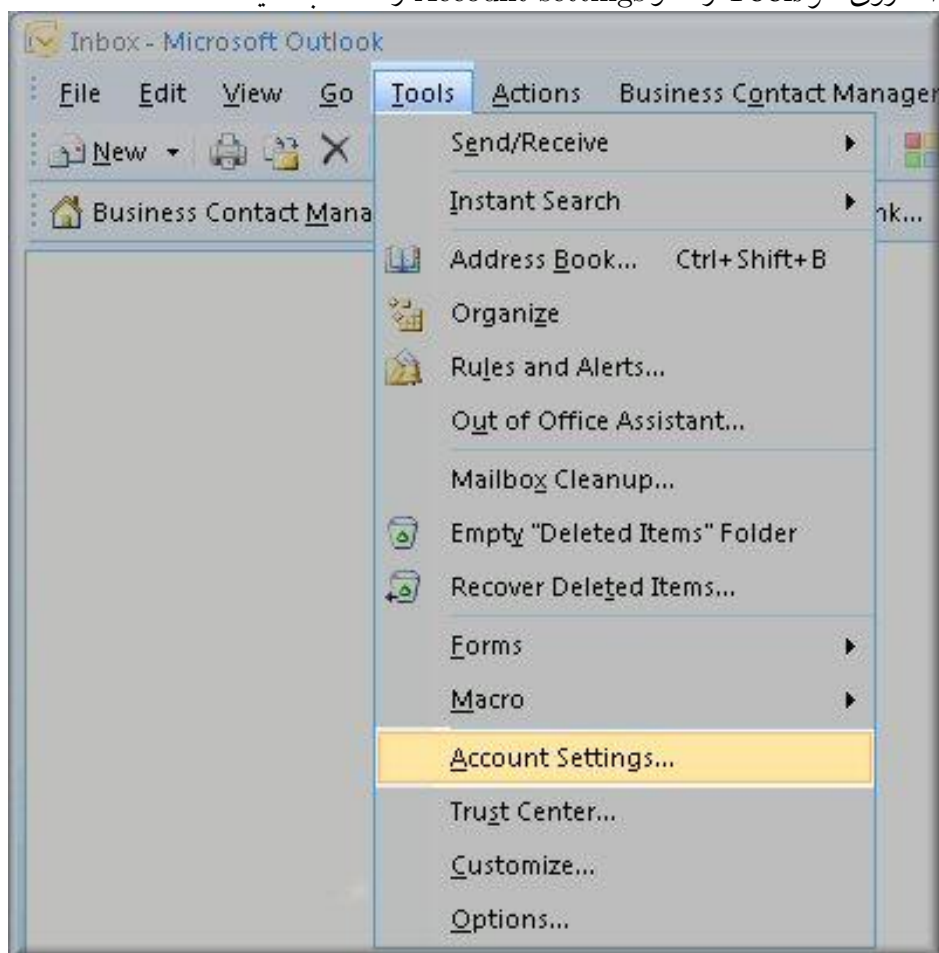
## ۱۴.۳ برای دسترسی به ایمیل‌های قبلی خود چه کنیم؟

برای دسترسی به ایمیل‌های قبلی خود، به آدرس <http://oldmail.sttu.ac.ir> مراجعه فرمایید.

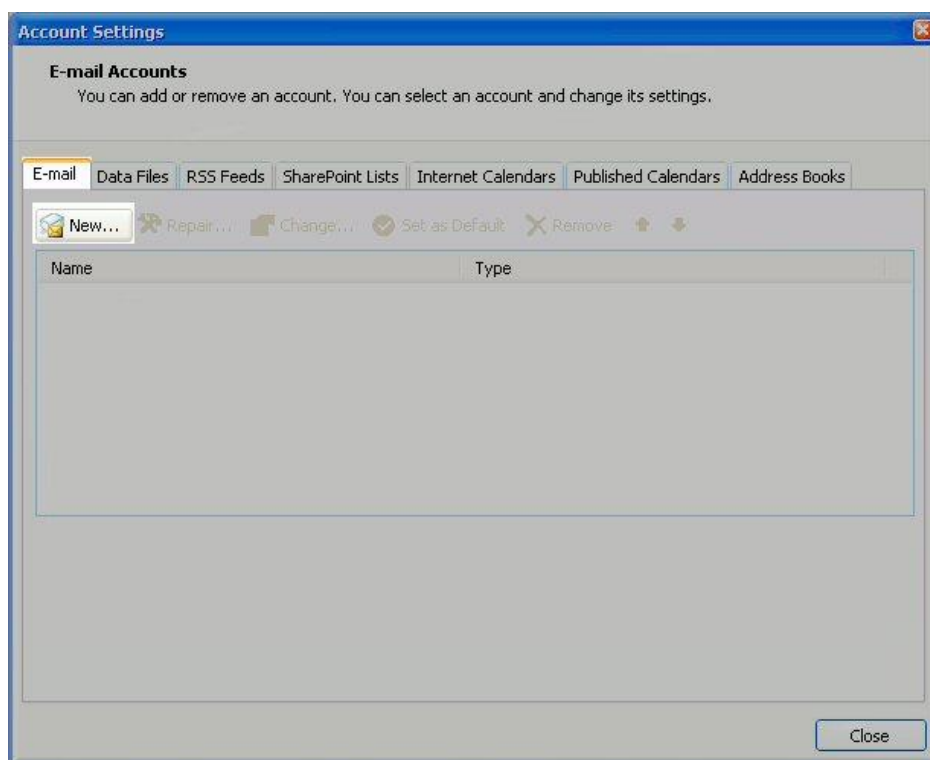
## ۱۵.۳ چگونه ایمیل خود را روی اوت لوک ۲۰۰۷ ( outlook ) نصب کنیم (2007)

مراحل نصب و تنظیمات (این تنظیمات و تصاویر مربوط به اوت لوک ۲۰۰۷ می باشد، برای دیگر ورژن های اوت لوک مشابه همین تنظیمات است که در ادامه می بینیم) :

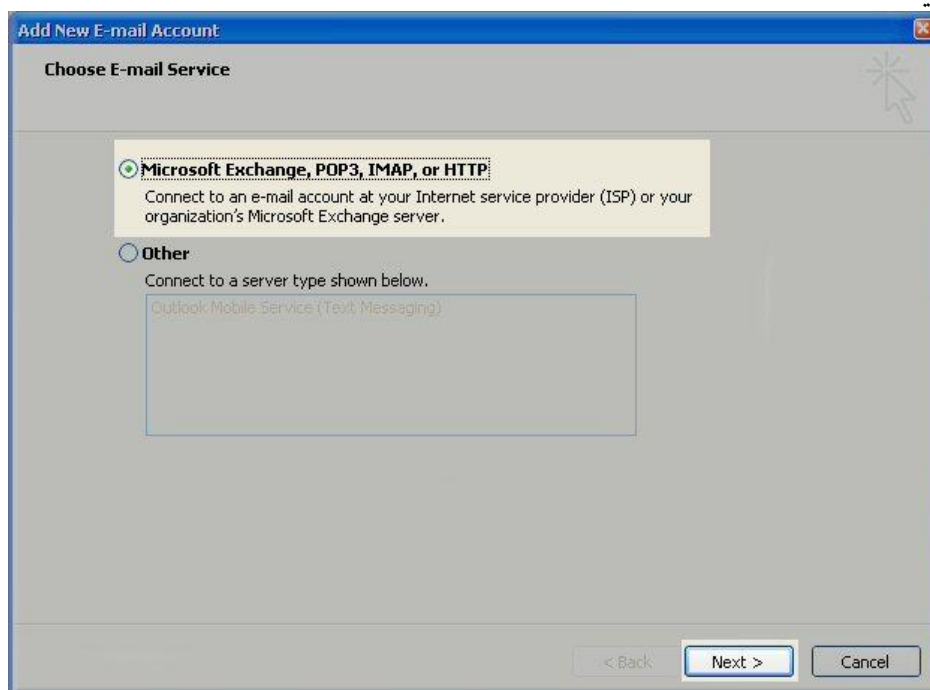
- ۱- اوت لوک ۲۰۰۷ را باز کنید.
- ۲- روی منو Tools رفته و Account settings را انتخاب کنید.



۳- روی برگه E-mail رفته و New را کلیک کنید.



۴- سپس روی Microsoft Exchange, POP3, IMAP or HTTP کلیک کنید و Next را بزنید.



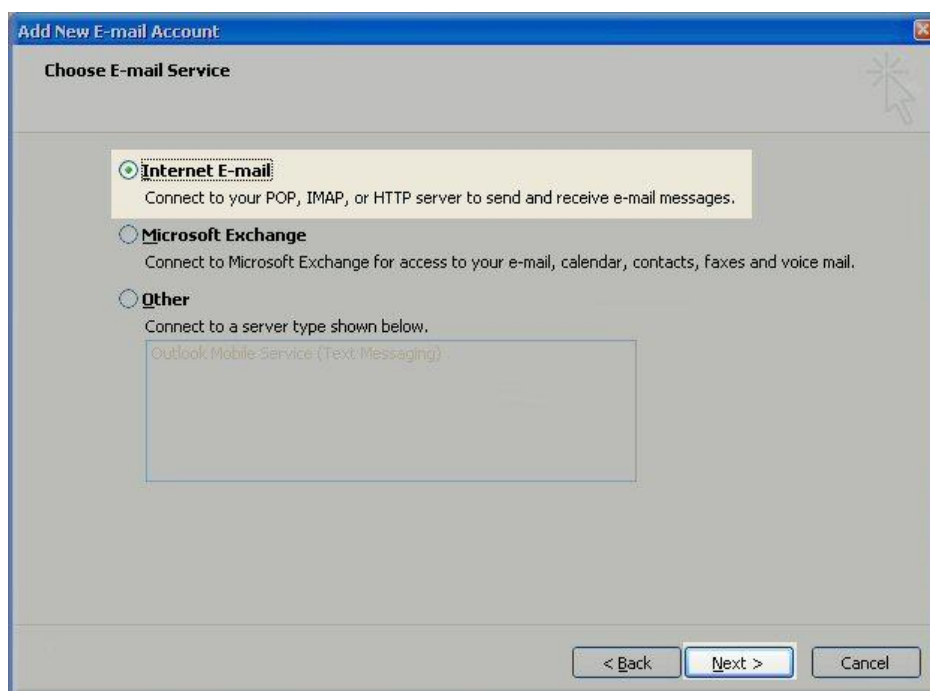
۵- در این مرحله با وارد کردن نام، آدرس ایمیل و پسورد می توانید به راحتی ایمیل خود را بر



روی اوت لوک نصب کنید اما این حالت برای ایمیل های معروفی مانند جیمیل است و اگر شما میل دیگری دارید (مثلا وب میل وب سایت خودتان) باید از راه دستی اقدام به نصب کنید. برای این کار **Manually configure server settings or additional server types** را تیک زده و **Next** را بزنید.

The screenshot shows the 'Add New E-mail Account' window in Outlook 2007. The window title is 'Add New E-mail Account' and the subtitle is 'Auto Account Setup'. It features four input fields: 'Your Name' (with an example: Barbara Senkovic), 'E-mail Address' (with an example: barbara@contoso.com), 'Password', and 'Retype Password' (with a note: 'Type the password your Internet service provider has given you.'). A checkbox at the bottom is checked and labeled 'Manually configure server settings or additional server types'. Navigation buttons at the bottom include '< Back', 'Next >', and 'Cancel'.

۶- Internet E-mail را انتخاب کنید و **Next** را بزنید.



۷- فرم را پر کنید.

- در قسمت اول Your Name نامی که می خواهید نمایش داده شود را بنویسید. معمولاً نام شخص دارنده ایمیل نوشته می شود.
- در قسمت بعدی ایمیل خود را به صورت کامل بنویسید. `username@mt-example.com`
- در این قسمت POP3 یا IMAP را بسته به تنظیمات ایمیل خود انتخاب کنید. برای ایمیل هایی مانند جیمیل و پاپ تری انتخاب می شود.
- Incoming mail server را به شکل `mail.example.com` بنویسید.
- Outgoing mail (SMTP) server را نیز به شکل `mail.example.com` بنویسید.
- Username را به شکل `username@example.com` بنویسید.
- Password نیز پسورد ایمیل شماست که باید آن را وارد کنید.

توجه کنید تنظیمات بالا برای جیمیل به صورت زیر است:

**Email Address:** Enter your full Gmail email address

**Password:** Enter your email password

**Incoming Server:** pop.gmail.com

**Incoming Server Port:** 995

**Outgoing Server:** smtp.gmail.com

**Outgoing server (SMTP) port:** 587

**Encryption:** TLS

برای هاتمیل این تنظیمات به کار برده می شود.

**Incoming Server:** pop3.live.com

**Incoming Port:** 995

**SSL Encryption:** yes

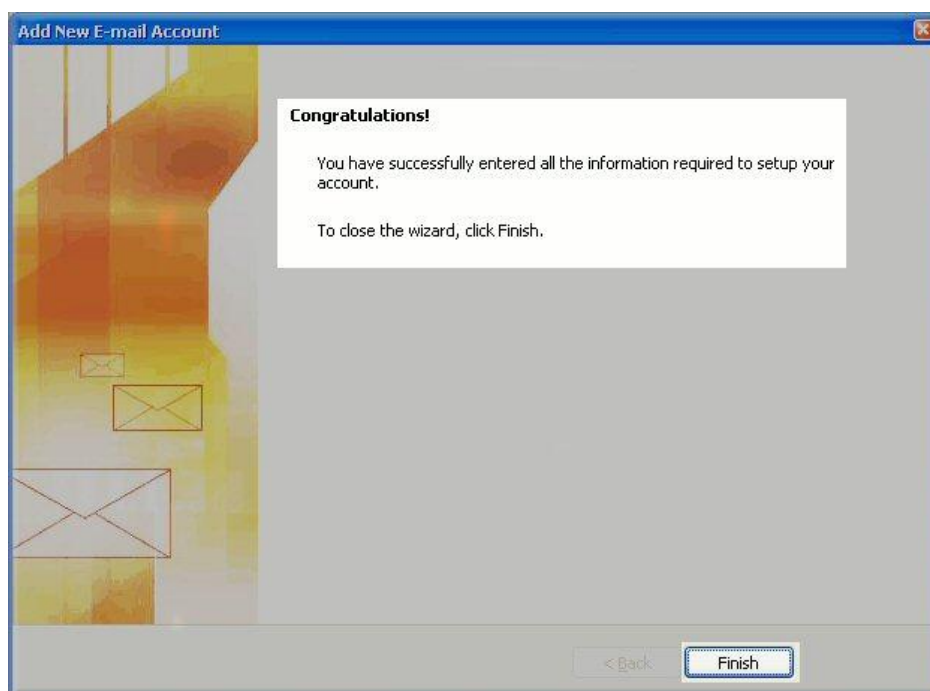
**Outgoing Server:** smtp.live.com

**Outgoing port:** 25 – use port 587 if the default port is not working

**Authentication:** yes

**TLS Or SSL:** yes

۸- روی Next کلیک کنید و Finish را بزنید تا تنظیمات شما ثبت شود.



پی‌نوشت: ما به جای Outlook استفاده از Zimbra Desktop را توصیه می‌کنیم که رابط کاربری آن کاملاً مشابه ایمیل سرور تحت وب دانشگاه می‌باشد و به راحتی می‌توانید ایمیل‌های دانشگاه، جیمیل و یاهوی خود را در آن داشته باشید. توضیحات بیشتر را در اینجا بخوانید.

## ۱۶.۳ محدودیت‌های فعلی ایمیل سرور جدید

ایمیل سرور جدید دانشگاه در حال حاضر محدودیت‌های زیر را دارد:  
ارسال ایمیل به Gmail در حال حاضر ممکن نیست ولی دریافت نامه از Gmail مشکلی ندارد.

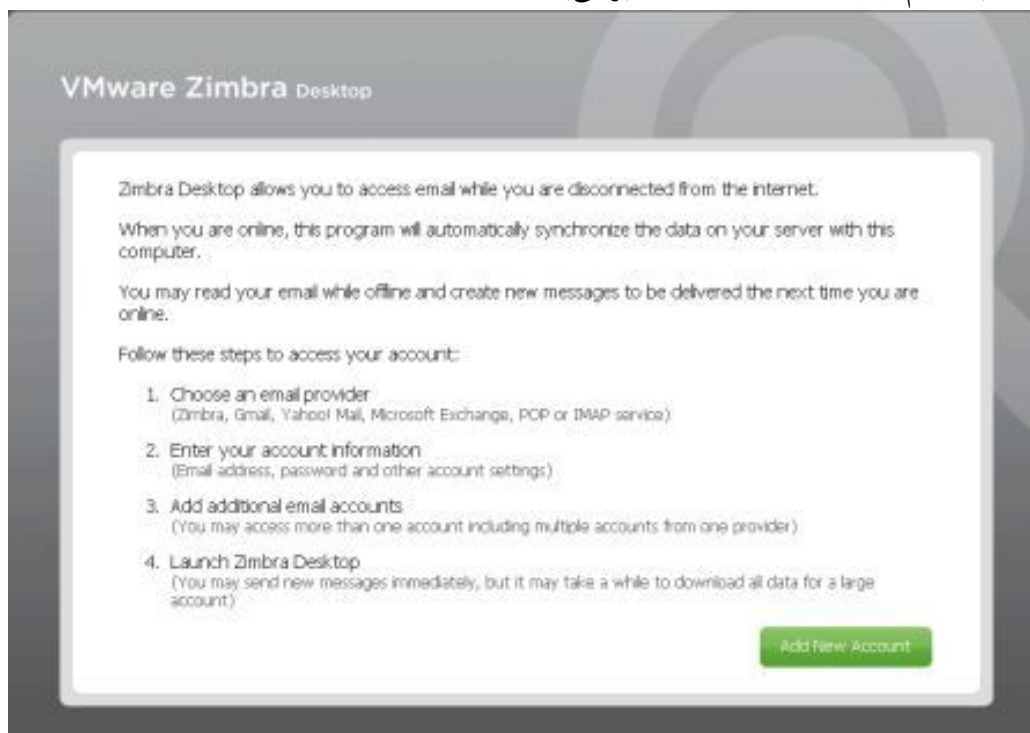
## ۱۷.۳ نصب Zimbra Desktop

شاید با Outlook کار کرده باشید، با استفاده از آن می‌توانید نسخه‌های از ایمیل‌های خود را در دستگاه خود داشته باشید. با استفاده از برنامه Zimbra Desktop می‌توانید امکانات مشابهی را داشته باشید.

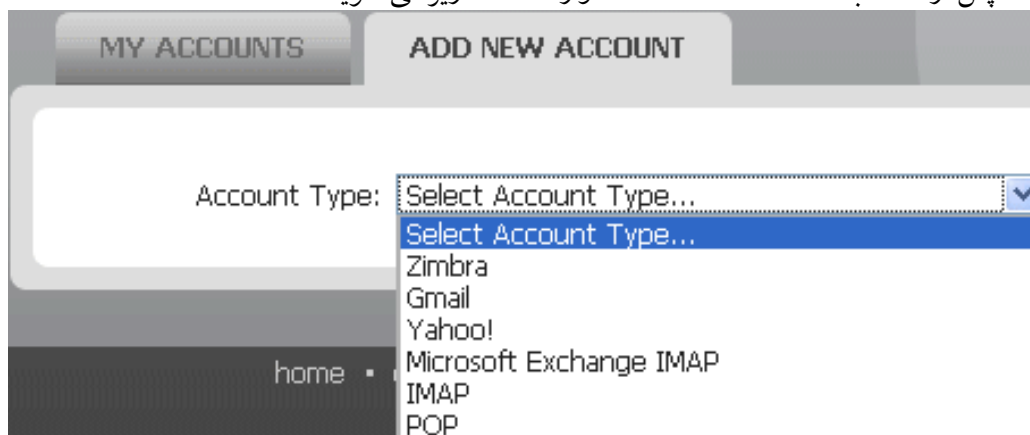
استفاده از آن برای در اختیار داشتن ایمیل‌های دانشگاه، یاهو و جیمیل بسیار آسان است؛ محیط آن همانند نسخه تحت وب ایمیل سرور دانشگاه است و امکانات آن همچون تنظیم قرار ملاقات و اشتراک فایل را دارد.

فایل zimbra desktop را از اینجا دریافت کنید و آن را در سیستم خود نصب نمایید. پس از اجرای zimbra desktop می‌توانید account خود را به آن اضافه نمایید. نحوه تنظیم آن برای استفاده از ایمیل‌های دانشگاه در زیر آمده است. برای تنظیم استفاده از جیمیل و یاهو

تنظیم خاصی لازم نیست، مطابق پیش فرضهای آن جلو بروید. البته دانلود ایمیل‌های یاهو جیمیل شما، بسته به حجم ایمیل‌های شما در آنها زمانبر می‌باشد.



پس از انتخاب add new account وارد صفحه زیر می‌شوید:



از لیست موجود zimbra را انتخاب نمایید:

MY ACCOUNTS    ADD NEW ACCOUNT

Account Type:

**Z** Zimbra Collaboration Suite Network Edition and Open Source Edition servers release 5.0 and later are supported. Verify server compatibility with your system administrator. To learn more about Zimbra Collaboration Suite, visit [www.zimbra.com](http://www.zimbra.com)

Account Name:

Email Address:

Password:

Incoming Server:     Port:  [Edit](#)

Security:  None     SSL

Synchronization Settings

Check Messages:

Enable debug logging

فرم را تکمیل نموده گزینه validate and save را انتخاب نمایید.

## ۱۸.۳ استفاده دانشجویان دکتری از سیستم پست الکترونیکی دانشگاه




قابل توجه دانشجویان دوره دکتری

با توجه به درخواست دانشجویان دوره دکتری جهت استفاده از سیستم پست الکترونیکی دانشگاه به اطلاع این عزیزان می‌رساند با توجه به راه اندازی سیستم پست الکترونیکی جدید امکان ارائه خدمات به شما عزیزان فراهم شده است. لذا شما عزیزان می‌توانید جهت دریافت آدرس پست الکترونیکی با دامنه دانشگاه؛ آدرس درخواستی خود را به [email@sttu.ac.ir](mailto:email@sttu.ac.ir) به همراه نام و نام خانوادگی و شماره دانشجویی ارسال نمایید، لازم به ذکر است که شناسه درخواستی بایستی به صورت زیر باشد:

حرف اول نام . نام خانوادگی بصورت کامل بطور مثال آدرس پست الکترونیکی دانشجویی با نام محمدحسینی بصورت **m.hosseini** می‌باشد

## ۱۹.۳ اصلاح ارسال به Gmail

مشکل ارسال Mail از سیستم پست الکترونیکی دانشگاه به Gmail برطرف شد. 

## ۲۰.۳ چگونه نوشتار خود را راست چین نمایم؟

ایمیل سرور دانشگاه، دکمه‌ای برای راست چین کردن متن در موضوع یا بدنه ایمیل ندارد؛ اما با فشردن Ctrl+Right Shift متن شما راست چین می‌شود و کلمات لاتین و علائم نگارشی در جای موردنظر شما درج و ظاهر خواهند شد.

## ۲۱.۳ چگونه نامه های gmail و ی Yahoo خود را بطور اتوماتیک به پست الکترونیکی دانشگاه forward کنم؟

تنظیمات مورد نیاز برای هدایت ایمیل‌های Gmail خود به ایمیل سرور دانشگاه

فرض می‌کنیم ایمیل شما mail@sttu.ac.ir باشد و شما ایمیل دیگری در جی‌میل دارید مثل mail@gmail.com

- به ایمیل mail@gmail.com وارد شوید. گزینه Setting را انتخاب کنید.

- حالا گزینه Forwarding and POP را انتخاب کنید....

- در کادر forwarding email address آدرس mail@sttu.ac.ir را وارد نموده و دکمه add را انتخاب نمایید.

### Add a forwarding address

Before you can forward to this address, we need to verify that you have permission from the owner. Enter an email address below and we will then send an email to that address with instructions on how to verify permission.

New forwarding email address:

Gmail یک ایمیل همراه با لینک فعالسازی و کد مربوطه برایتان ارسال می‌کند.

۲۱.۳. چگونه نامه های GMAIL و YAHOO خود را بطور اتوماتیک به پست الکترونیکی دانشگاه  
۶۴ FORWARD کنم؟

mail@gmail.com has requested to automatically forward mail  
to your email  
address mail@sttu.ac.ir  
Confirmation code: 38904

To allow mail@gmail.com to automatically forward mail to your address,  
please click the link below to confirm the request:

<https://mail.google.com/mail/vf->

If you click the link and it appears to be broken, please copy and paste it  
into a new browser window. If you aren't able to access the link, you  
can send the confirmation code  
38904 o

Thanks for using Gmail!

Sincerely,

The Gmail Team

- لینک فعالسازی را انتخاب نموده و پس از آن در Forwarding and POP جی میل خود،  
کد مزبور را وارد نموده و دکمه Verify را انتخاب کنید.

**Unverified addresses**  
To enable an address for automatic forwarding, please enter the confirmation code sent to that address.

confirmation code:   or

- در قسمت Forwarding گزینه Forward a copy of incoming mail to را انتخاب  
کنید و آدرس ایمیل دانشگاه (mail@sttu.ac.ir) را انتخاب کنید.

**Filters** Forwarding and POP/IMAP

Disable forwarding  
 Forward a copy of incoming mail to a.zahedi@sttu.ac.ir and keep Gmail's copy in the Inbox

- روی Save Changes که کلیک کنید کار تمام است.  
حالا هر ایمیلی که به آدرس mail@gmail.com ارسال شود یک کپی از آن به mail@sttu.ac.ir  
می رسد. توضیحات کامل تر را می توانید در اینجا ببینید.  
تنظیمات مورد نیاز برای هدایت ایمیل های Yahoo ی خود به ایمیل سرور دانشگاه  
فرض می کنیم ایمیل شما mail@sttu.ac.ir باشد و شما ایمیل دیگری در یاهو دارید مثل  
mail@yahoo.com  
- به ایمیل mail@yahoo.com وارد شوید. از منوی Options گزینه Mail Options را  
انتخاب کنید.  
- حالا گزینه Forwarding and POP را انتخاب کنید.



۲۲.۴۵. چگونه نامه های خود را بطور اتوماتیک از MAIL دانشگاه به ایمیل دیگر FORWARD کنم؟

- در قسمت POP & Forwarding گزینه Forward Yahoo mail to another email address to، را انتخاب کنید و آدرس ایمیل دانشگاه (mail@sttu.ac.ir) را وارد کنید.  
- در لیست پایین افتادنی زیر آن گزینه مناسب خود را انتخاب کنید. (به عنوان مثال اگر مایلید ایمیل های یاهوی شما در صندوق یاهو بنمانند و یک کپی از آن به ایمیل دانشگاه ارسال شود، گزینه Store and Forward را انتخاب کنید)  
- مورد دیگری از سمت چپ را انتخاب کنید تا تغییرات ذخیره شوند. پس از چند لحظه ایمیلی از یاهو به ایمیل دانشگاه شما خواهد رسید که باید آنرا تایید کنید.  
حالا هر ایمیلی که به آدرس mail@yahoo.com ارسال شود یک کپی از آن به mail@sttu.ac.ir می رسد.

پی نوشت ۱: مطلب مربوط به یاهو را من نوشته بودم و برای من به درستی کار می کند. برخی از همکاران اطلاع دادند که برای فعال سازی گزینه Forwarding در ایمیل یاهوی خود با مشکل مواجه شده اند و باید ایمیل خود را ارتقاء دهند که مستلزم هزینه است. شایان ذکر است که حدود یک سال قبل، من تغییراتی در حساب ایمیل یاهوی خود داده بودم که امکان اخذ ایمیل هایم را در اوت لوک داشته باشم. از آن تاریخ گزینه Forwarding برای من فعال مانده است؛ ولی در حال حاضر این امکان برای کاربران یاهو وجود ندارد، مگر اینکه قبلاً مشابه من اقدام کرده باشند. - محمود امین طوسی (مدیر فناوری)

پی نوشت ۲: اگر مایلید در وبمیل دانشگاه مشخص باشد که کدام ایمیل از جیمیل شما آمده است و کدام یک از یاهو، کافی است از فیلترینگ ایمیل سرور دانشگاه استفاده کنید. روش کار را برای جیمیل توضیح می دهیم. تگی با نام مثلاً Gmail بسازید، سپس در قسمت تنظیمات (Preferences)، گزینه Filters را انتخاب نموده و سپس New Filter را انتخاب کنید. در قسمت شرطها، به جای Subject، گزینه To را انتخاب نموده و در جعبه روبروی آن آدرس جیمیل خود را وارد نمایید. در قسمت پایین پنجره (Perform the following actions)، به جای Keep in Inbox، گزینه Tag with را انتخاب و سپس Browse را کلیک کنید. در لیست تگهای ظاهر شده، Gmail را انتخاب کنید.

حال از این به بعد تمام جیمیل های رسیده به صندوق دانشگاه شما مارکدار هستند به علاوه با یک کلیک روی تگ Gmail می توانید جیمیل های خود را مشاهده فرمایید.

پی نوشت ۳: شاید مایل باشید، ایمیل های خود را روی دستگاه خود داشته باشید که در مواقع قطعی اینترنت یا شبکه، به ایمیل های قبلی خود دسترسی داشته باشید. ما به شما Zimbra Desktop را پیشنهاد می کنیم. توضیحات بیشتر را در اینجا بخوانید. شایان ذکر است که زیمبرا دسکتاپ با حسابهای فعلی یاهو مشکلی ندارد.

## ۲۲.۳ چگونه نامه های خود را بطور اتوماتیک از mail دانشگاه به ایمیل دیگر forward کنم؟

وارد سامانه پست الکترونیک دانشگاه شوید و از قسمت تنظیمات (preferences) گزینه نامه های پستی (mail) را انتخاب نمایید. در بخش: در حال دریافت پیام ها (Receiving Messages)، آدرس پست الکترونیکی مقصد را داخل کادر روبروی عبارت Forward a copy to وارد نمایید. پس از اتمام تغییرات را ذخیره نمایید:

## ۲۲.۴۶. چگونه نامه های خود را بطور اتوماتیک از MAIL دانشگاه به ایمیل دیگر FORWARD کنیم؟



## فصل ۴

# دانستنیهای عمومی فناوری

همان‌گونه که در مقدمه ذکر شد این فصل به ذکر اخباری خارج از دانشگاه اختصاص یافته است که به نظر این مرکز موردنیاز همکاران گرامی دانشگاه بوده و یا از جمله اخبار مهم روز فناوری دنیا بوده‌اند.

### ۱.۴ فید RSS چیست؟

فناوری فید feed که آن را در فارسی «خوراک» یا «خبرمایه» هم ترجمه کرده‌اند، فناوری‌ای است که می‌تواند گشت و گذار شما را در اینترنت متحول کند. فید راهی برای دسترسی سریع و بدون دردسر به آخرین اخبار و نوشته‌های سایت و وبلاگ‌هاست.

اگر تا به حال از فید استفاده نمی‌کردید، این نوشته را بخوانید و وقت وب‌گردی یک روزتان را صرف آشنایی با آن کنید، مطمئناً پشیمان نخواهید شد و در آینده از روزی که در آن با فید آشنا شدید به نیکی یاد خواهید کرد!

#### چرا باید فید بخوانیم؟!

تصور کنید که دوست دارید همیشه مطالب چند وبلاگ به خصوص را بخوانید و یا از آخرین اخبار روز دنیا مثلاً در مورد سیاست و اخبار روز، پزشکی یا فناوری مطلع باشید. برای این کار مجبور هستید که هر روز از همه این وبلاگ‌ها و سایت‌های خبری بازدید کنید. این کار چندان ساده نیست و وقت‌گیر است. شما باید هر روز زمان زیادی در انتظار باز شدن صفحات اینترنتی بنشینید و تازه اصلاً هم معلوم نیست که وبلاگ مورد نظر شما به‌روز شده باشد!

فید دقیقاً چیزی است که به کار شما می‌آید. به کمک فید، مرور مطالب تازه سایت‌ها و وبلاگ‌ها بسیار ساده می‌شود.

#### از فید نترسیم؟

خیلی‌ها تا اسم فید به گوششان می‌خورد، با خودشان فکر می‌کنند که کار کردن با فید، فقط به درد خوره‌های کامپیوتر می‌خورد و بس. آنها از تغییر واژه دارند و تصور می‌کنند که خو کردن به فید و ترک عادات وب‌گردی قدیمی‌شان، چیز دشواری است و فواید استفاده از فید به تحمل زحمات آشنایی با آن، نمی‌ارزد! در صورتی که هر کس با هر میان تحصیلات و در هر رشته‌ای که باشد به

تناسب نیاز خود می‌تواند از فناوری از فید بهره ببرد.

### چطور از فید استفاده کنیم و فید بخوانیم؟

اگر لوگو و اضافات گرافیکی و تبلیغات هر سایت را حذف کنیم و فقط مطالب جدید هر سایت را باقی بگذاریم، چیزی که باقی می‌ماند، فید سایت است، به عبارت دیگر فید، نسخه فقط متن سایت‌ها و وبلاگ‌ها هست.

راه‌های خواندن فید، خیلی زیاد هستند. شما می‌توانید فید را با نصب برنامه‌هایی بخوانید یا اینکه فید را از طریق ایمیلتان بخوانید. با این همه فیدخوان یا خبرخوان گوگل Google Reader، در میان فیدخوان‌ها محبوبیت زیادی دارد و آمارها هم نشان می‌دهند که روز به روز تعداد بیشتری از مردم به استفاده از Google Reader روی می‌آورند.

### وب! حالا چطور فیدها را با گوگل ریدر بخوانیم؟

اگر مراحل زیر را قدم به قدم طی کنید، می‌توانید به راحتی فیدها را با گوگل ریدر بخوانید.

۱ - **مرورگر اینترنتی خود را باز کنید** : با همه مرورگرهای رایج می‌توان از گوگل ریدر استفاده کرد، تفاوتی نمی‌کند که اینترنت اکسپلورر داشته باشید یا اپرا یا کروم یا فایرفاکس! با این همه استفاده از مرورگر فایرفاکس را به شما توصیه می‌کنیم. با توضیحاتی که بعداً خواهیم داد، متوجه خواهید شد که چرا فایرفاکس را ترجیح می‌دهیم.

۲ - **با مرورگرتان به گوگل ریدر بروید** . اگر تا به حال حسابی در گوگل برای خود حساب باز نکرده‌اید، یک حساب برای خود باز کنید. نام کاربری و پسورد خودتان را بدهید تا وارد گوگل ریدر بشوید.

۳ - **آدرس فید سایت یا وبلاگ مورد نظر را پیدا کنید** : حالا به مرحله‌ای رسیدیم که باید آدرس فید سایت‌ها و وبلاگ‌ها مورد نظرتان را به گوگل ریدر بدهید. اما چگونه باید آدرس فید را پیدا کرد؟ برای پیدا کردن آدرس فید یک سایت یکی از این کارها را انجام دهید:

الف - شما اگر به سایت یا وبلاگ مورد نظرتان بروید، در صفحه سایت آدرس خروجی فید سایت را پیدا خواهید کرد. در سایت مورد نظرتان، دقت کنید، ببینید که کلماتی مثل فید، RSS، خوراک به چشمتان می‌خورد؟ اگر چنین چیزهایی پیدا کردید، کافی است، آدرسی را که این تصاویر یا لینک‌ها به آن اشاره دارند را کپی کنید و به صورتی که خواهیم گفت وارد گوگل ریدر کنید.

ب- با یک روش دیگر هم می‌توانید، فید سایت را پیدا کنید، اگر از مرورگر فایرفاکس یا اپر استفاده می‌کنید، به نوار آدرس توجه کنید، آیکون فید سایت را در آنجا خواهید دید. کافی است، روی این آیکون کلیک کنید و به فید سایت برسید.

ج- خود گوگل ریدر هم در موارد زیادی می‌تواند به صورت خودکار، آدرس فید را برایتان پیدا کند. کافی است در مرحله ۴ (مرحله بعدی) به جای آدرس فید، آدرس وبلاگ را به گوگل ریدر بدهید.

۴ - حالا باید فید را به خورد گوگل ریدر بدهیم، در ستون سمت چپ گوگل ریدر و در قسمت بالا روی **Add a Subscription** کلیک کنید:

چنین کادری ظاهر می‌شود، در این کادر می‌توانید آدرس سایت را وارد کنید تا خود گوگل ریدر دنبال آدرس فید بگردد و یا اینکه سراسر آدرس فید را وارد کنید:

حالا روی **Add** کلیک کنید و کمی صبر کنید.

شما مشترک فید سایت مورد نظر شده‌اید و قسمت بیشتر کار را انجام داده‌اید. از این به بعد نوشته‌های و پست‌ها تازه به صورت خودکار وارد گوگل ریدر می‌شوند و شما می‌توانید آنها را به راحتی

مطالعه کنید.

حالا مراحلی را که توضیح دادم برای دیگر سایت‌ها و وبلاگ‌های مورد علاقه خودتان انجام بدهید. قبول دارم! شاید مشترک شدن فید همه سایت‌ها و وبلاگ‌هایی که دوست دارید و احیانا در لیست علاقه مندی‌های شما در مرورگرتان قرار دارند، در روز اول وقت‌گیر باشد، اما به نتیجه کار فکر کنید، تصور کنید که چه میزان در روزهای بعدی می‌توانید در وقت و انرژی و هزینه خودتان صرفه‌جویی کنید!

حالا بیایید جزئیات بیشتری را با هم بررسی کنیم!:

**فیدهایتان را در پوشه‌های جدا قرار بدهید:** همان طور که در کامپیوترتان، فایل‌های مختلف را پوشه‌های جدا قرار می‌دهید تا همه چیز مرتب باشد و پیدا کردنش راحت‌تر باشد، خیلی خوب است که فیدهایتان را در پوشه‌های جدا بچینید. با این کار می‌توانید خیلی منظم فیدها را مطالعه کنید. مثلا شما می‌توانید فید همه سایت‌های خبری را در یک پوشه و فید وبلاگ‌های فناوری را در پوشه دیگر قرار بدهید. با این کار با کلیک روی پوشه اخبار فناوری، شما آخرین پست‌های فناوری را خواهید خواند و به شیوه مشابه با کلیک روی پوشه اخبار روز، فقط اخبار را مطالعه خواهید کرد.

برای این کار بعد از مرحله اشتراک هر فید، روی Feed Setting کلیک کنید:

حالا با کلیک روی New Folder، یک پوشه جدید درست کنید و نامی برای آن انتخاب کنید: با این کار، فید مورد نظرتان وارد یک پوشه می‌شود. حالا اگر به ستون سمت چپ گوگل ریدر نگاه کنید، می‌بیند که پوشه جدیدی درست شده و فیدتان داخل پوشه قرار دارد:

با تکرار این کار برای فیدها دیگر و درست کردن پوشه‌های متناسب، فیدهایتان سرو سامان پیدا می‌کنند و برای مطالعه هر دسته از فیدها کافی است روی پوشه آنها در ستون سمت چپ گوگل ریدر کلیک کنید.

**سؤال:** در گوگل ریدر مطالبی که قبلا مطالعه کرده‌ام، دوباره دیده می‌شوند، چه کار کنم که فقط مطالب تازه را ببینم؟

پاسخ: روی new items کلیک کنید:

**سؤال:** از کجا بفهمم که چند مطلب خوانده نشده دارم؟

در کنار کنار هر پوشه و هر فید، تعداد مطالب خوانده نشده، به صورت یک عدد مشخص است. همچنین اگر فیدی حاوی مطالب تازه باشد، به صورت بولد دیده می‌شود، در غیر این صورت فونت آن معمولی است.

برای مثال در تصویر بالا مجله اینترنتی پریانا، ۶ فید خوانده نشده دارد.

**سؤال:** چگونه مطالب جالب را برای خودم ذخیره کنم، طوری که در آینده بتوانم دوباره به آنها

مراجعه کنم و یا سر فرصت آنها را بخوانم؟

پاسخ: در قسمت زیر هر پست، گزینه‌ای برای ستاره‌دار کردن مطالب جالب وجود دارد:

با کلیک بر روی ستاره، مطلب ستاره‌دار می‌شود. شما می‌توانید کلی مطالب جالبی را که آنها را ستاره‌دار کرده‌اید با کلیک بر روی Starred items ببینید:

**به اشتراک گذاشتن مطالب:** با کلیک بر روی Share در زیر هر مطلب، کسانی که با آنها در گوگل تاک چت می‌کنید، می‌توانند آن مطلب را در گوگل ریدر خود ببینند. متقابلا شما هم با کلیک روی Friend's shared items خواهید توانست مطالب به اشتراک گذاشته توسط آنها را ببینید.

با کلیک بر روی share with note، می‌توانید مختصری در مورد هر مطلب اظهار نظر کنید. مثلا بنویسید که چرا مطلب برایتان جالب بوده یا اینکه مثلا با نظر نویسنده مخالف هستید. دوستان شما می‌توانند این نظرات شما را در کنار مطلب ببینند.

**سخن پایانی :** مطمئن باشید که اختصاص دادن زمان وب‌گردی یک روز برای انجام دادن همه کارهای بالا کافی است. از فید نترسید، اطمینان داشته باشید که بعد از چند روز کار با گوگل ریدر و فید، چنان با فید خو خواهید گرفت که نمی‌توانید کنارش بگذارید. راهنمایی که نوشته شد، تنها حاوی مطالب مهم‌تر و ضروری برای کار با فید و گوگل ریدر بود. کار با گوگل ریدر جزئیات بیشتری دارد و به علاوه راه‌های دیگری هم برای مطالعه فید وجود دارد. این راهنما بیشتر برای آشنایی مقدماتی شما با فید است.

— برگرفته از مجله اینترنتی پریانا —  
نوشته شده توسط: علی چشمی

## ۲.۴ پهنای باند چیست؟

پهنای باند، ترجمه لغت به لغت اصطلاح Bandwidth است. در بعضی جاها این اصطلاح را «عرض باند» هم ترجمه کرده‌اند. اگر بخواهیم درک خوبی از معنای این اصطلاح داشته باشیم بد نیست به این مثال توجه کنید. اتوبانی را در نظر بگیرید، معمولاً هر اتوبان یا بزرگراه دارای چند خط (Line) یا باند (Band) است که ظرفیت این بزرگراه را معین می‌کند. مثلاً اگر بزرگراهی دارای ۲ خط باشد طبیعتاً به طور هم‌زمان و از یک نقطه از بزرگراه فقط ۲ عدد ماشین امکان عبور دارند و اگر بزرگراهی دارای ۴ خط یا باند باشد به طور هم‌زمان ۴ ماشین امکان عبور از کنار هم را دارند.

خوب حالا کافی است در این مثال به جای ماشین، بیت (Bit) و به جای بزرگراه یا اتوبان، سیم یا فیبر نوری که در واقع محیط انتقال اطلاعات هستند، بگذارید.

مثال دیگری که می‌تواند به درک بهتر شما از این موضوع کمک کند، لوله‌های انتقال آب است. هر چقدر قطر لوله آب بزرگ‌تر باشد، امکان انتقال آب بیشتری از یک نقطه به نقطه دیگر را دارد. درست مثل پهنای باند، هر چه پهنای باند بیشتری داشته باشیم، امکان انتقال اطلاعات بیشتری از یک نقطه به نقطه دیگر را داریم.

در واقع پهنای باند یا عرض باند به شما می‌گوید به طور هم‌زمان چند بیت می‌تواند از کنار هم رد شوند یا در طول محیط ارتباطی شما با شبکه جابه‌جا شوند.

تنها نکته‌ای که ذکر آن لازم به نظر می‌رسد تفاوت اصلی در مثال‌های ذکر شده با پهنای باند است. در مثال‌های بالا هر چه تعداد خطوط یا پهنای اتوبان بیشتر باشد، تعداد ماشین بیشتری می‌توانند به طور هم‌زمان از کنار هم عبور کنند. همچنین هر چقدر قطر لوله‌های انتقال آب بیشتر باشد، حجم بیشتری از آب می‌تواند در هر لحظه منتقل شود. اما در وسایل مخابراتی و ارتباطی، صحبت از عرض یا پهنای فیزیکی نیست. به عبارت دیگر برای انتقال اطلاعات بیشتر در یک واحد زمان (مثلاً ثانیه) نیازی به پهن‌تر کردن و یا عریض کردن محیط انتقال (مثلاً سیم یا فیبر نوری) نیست. در واقع در محیط‌های مخابراتی این مودم‌ها هستند که وظیفه رد و بدل کردن اطلاعات را به عهده دارند. به عبارت دیگر، هر چه توانایی مودم شما بیشتر باشد، می‌تواند حجم بیشتری از اطلاعات را بر روی محیط انتقال جابه‌جا کند.

آخرین نکته ضروری در این زمینه، واحد انتقال اطلاعات و ضرایب آن است. همان‌طور که می‌دانید واحد انتقال اطلاعات بیت در ثانیه است. در محیط تثوریک هر میزان پهنای باند را می‌توانید متصور شوید. از یک بیت در ثانیه (۱ bps) تا میلیون‌ها بیت در ثانیه (Mbps) و یا بیشتر. اما در

محیط عملی معمولاً با محدودیت‌هایی روبرو هستید. مثلاً شما نمی‌توانید از یک شرکت ارائه دهنده خدمات پهنای باند (نظیر شرکت مخابرات ایران) درخواست پهنای باندی به میزان ۹۱۳ Kbps کنید. کوچک‌ترین واحد رایج پهنای باند ۶۴K است و معمولاً شرکت‌های مخابراتی جدولی را ارائه می‌دهند که نشان دهنده پهنای باندهایی است که امکان ارائه آن را دارند. نوشته شده توسط: علی چشمی

## ۳.۴ اکتیو دایرکتوری چیست؟

مدل (workgroup) ساختار قبلی شبکه دانشگاه بدون (domain) در شبکه‌ها یک مدل ساده می‌باشد. بدین معنی که در این شبکه مدیر مرکزی وجود ندارد و هر کاربر مدیر رایانه خود محسوب می‌شود. در یک چنین مدلی اگر بخواهیم یک تنظیم خاص برای کامپیوترها و یا کاربران تعیین کنیم، بایستی آنرا بصورت جداگانه در یکایک رایانه‌ها تنظیم کنیم. اما در صورت راه اندازی اکتیو دایرکتوری این امکان وجود دارد که یک نفر بتواند تمامی کاربران، رایانه‌ها و منابع را در شبکه مدیریت نماید. همچنین در این حالت میتوان یک تنظیم خاص را فقط یک بار تعریف نمود و آن تنظیم را به تمامی رایانه‌ها و یا کاربرانی که مد نظر می‌باشند، اعمال نمود.

بدون اکتیو دایرکتوری برای مدیریت منابع نیازمند مدیریت تک-تک آنها بصورت منفرد می‌باشیم در حالی که با اکتیو دایرکتوری مدیریت منابع شبکه بصورت مجتمع صورت می‌گیرد. به عنوان مثال با بکارگیری اکتیو دایرکتوری وقتی شما تصمیم به تعویض کلمه عبور خود می‌گیرید تمامی سیستم‌های کاربری شما که با اکتیو دایرکتوری مجتمع شده اند بصورت خود کار با کلمه عبور جدید شما هماهنگ می‌گردند و نیازی به تغییر تک تک آنها نمی‌باشد. (در حال حاضر سیستم حسابرسی مصرف اینترنت کاربران و سیستم مدیریت چاپ، با اکتیو دایرکتوری یکپارچه شده است)

### چرا از اکتیو دایرکتوری استفاده کنیم؟

اکتیو دایرکتوری به ما کمک میکند تا محیط کاری قابل اطمینانی را برای کاربران نهایی (end-user) فراهم کنیم تا کاربر بتواند با کارآمدی بیشتر به امورات خود پردازد و در عین حال امنیت و مدیریت بهتر برایش به ارمغان آورده شود

بطور کلی میتوان مزایای استفاده از اکتیو دایرکتوری ذیلاً برشمرد:

افزایش بهره بروی و بازدهی کاربران

کاهش بار اضافی مدیران شبکه و در نتیجه امکان ارائه خدمات تخصصی تر

بهبودی تحمل خطا جهت کاهش زمانهای قطعی شبکه

بالا بردن امنیت برای افزایش آسودگی خاطر کاربران

مدیریت مجتمع برنامه های کاربری قابل اجتماع با اکتیو دایرکتوری

### افزایش بهره بری کاربران چگونه؟

اعمال قوانین گروهی اعمال قوانین امنیتی، تنظیمات و گزینه ها بصورت استاندارد.

این تنظیمات و قوانین کاربر را در هنگام حرکت به ایستگاههای مختلف کمک میکند تا مجدداً تنظیمات خود را در ایستگاه جدید انجام ندهد

فعال سازی امکانات بر حسب نیاز قوانین گروهی تعیین میکنند تا چه امکاناتی با چه شرایطی در اختیار کاربر قرارگیرد و کاربر را از سردرگمی در انبوهی از تنظیمات و برنامه ها آسوده میسازد و با عت افزایش ضریب امنیتی از طریق جلوگیری از اجرای برنامه های نا خواسته میگردد.

امکان نمایه سیار Roaming Profile این امکان به کاربر اجازه میدهد تا اطلاعات انحصاری خود از قبیل favorites, screen saver settings, application icons و ... را در یک مکان مرکزی ذخیره کند و هنگام ورود به هر یک از ایستگاههای شبکه این تنظیمات را با خود داشته باشد

#### سرویس بروز رسانی ویندوز Service Update Windows

یکی از مسائل مهم امنیتی نصب وصله های امنیتی است که همواره موضوعی پر دغدغه و اساسی در کاربری سیستم عامل ها میباشد. عدم نصب بموقع وصله های امنیتی ، همواره سیستم شما را در معرض دسترسی هکرها و سارقان داده قرار میدهد و این وصله ها دسترسی آنها ، به سیستم شما از طریق حفره های مکشوفه در سیستم عامل مسدود میکند.

حال شبکه ای با وسعت ۱۰۰۰ ایستگاه و ۷۰۰۰ کاربر را در نظر بگیرد و تصور کنید بروز رسانی بموقع و دقیق این شبکه چگونه ممکن است؟ چه مقدار منابع سخت افزاری و نرم افزاری برای انجام این امر میتوان در نظر داشت؟ و..... تنها راه حل عملی و قابل ارائه استفاده از اکتیو دایرکتوری است تا بتواند بصورت متمرکز از طریق سرویس مورد نظر (WUS) کلیه ایستگاههای کاری را بصورت خودکار بروز رسانی کند و آخرین وصله های امنیتی را نصب و پیگیری نماید. البته در نظر داشته باشد این وصله ها شامل برخی از برنامه های کاربردی نیز میگردد و در بعضی موارد منجر به افزایش قابلیتها و کارایی آنها میگردد

#### مساعادت از راه دور Remote Assistance

این یک سرویس جدید در ویندوز XP میباشد که کاربران را قادر میسازد مدیر شبکه و یا سرپرست محلی را برای رفع اشکالات فنی پیش آمده فرا بخواند و وی بدون نیاز حضوری زیر نظر کاربر نسبت به رفع مشکل اقدام نماید.

بنابراین سرپرستهای محلی شبکه در پی کاهش بار پشتیبانی شبکه ناشی از اعمال امنیت مناسب که با استقرار اکتیو دایرکتوری حاصل شده، میتوانند در هر نقطه ای از شبکه که باشند بصورت غیر حضوری به یاری شما بیایند و با شما در رفع مشکلات پیش آمده فنی ، عدم اجرای برنامه ها و ... همراه باشند. البته این دسترسی بصورت یکطرفه میباشد و یاریگر هیچگونه دسترسی به داده های شما ندارد و نمی تواند از آنها کپی تهیه کند و کلیه عملیات او تحت نظاره شما انجام خواهد شد و این فرایند با حفظ حریم خصوصی ارائه میگردد.

#### سرویس نصب از راه دور

این سرویس به مدیر شبکه امکان میدهد تا برنامه ای کاربردی مشترک و مورد نیاز کاربران را بسته به نیاز آنها تهیه و از طریق این سرویس بروی کامپیوتر کاربران نصب کند لذا هنگام ورود سیستم جدید به شبکه مدیر شبکه دیگر نیازی به نصب مجدد کلیه نرم افزار را ندارد و این کار هنگام اتصال به شبکه بصورت خودکار صورت میگردد.

نوشته شده توسط: علی چشمی

## ۴.۴ نکاتی در مورد رمز عبور کاربران



آیا میدانید اولین و اغلب آسانترین روش ورود به سیستمهای شما، کلمه عبور شما میباشد. استفاده از کلمه عبورهایی که حدس زدن آنها راحت است و یا طول آنها کوتاه است موجب نفوذ به سیستم شما و استفاده از امکانات شبکه با نام شما میشود....



هرگز کلمه عبور خود را به کسی نگوئید، حتی به دوستان خود و کسانی که برای انجام تعمیرات و یا نصب نرم افزار به شما مراجعه میکنند.  
در صورتیکه به هر دلیلی شخص دیگری از کلمه عبور شما مطلع شد، در اولین زمان نسبت به تغییر کلمه عبور خود اقدام نمایید.

## ۵.۴ به بهانه درگذشت استیو جابز

### ۶.۴ سه داستان استیو جابز در سخنرانی اش در استنفورد

من هفده سالم بود يك جایی خواندم که اگر هر روز جوری زندگی کنید که انگار آن روز آخرین روز زندگی تان باشد شاید يك روز این نظر به حقیقت تبدیل بشود. این جمله روی من تأثیر گذاشت و از آن موقع به مدت سی و سه سال هر روز وقتی که من توی آینه نگاه می‌کنم از خودم می‌پرسم اگر امروز آخرین روز زندگی من باشد آیا باز هم کارهایی را که امروز باید انجام بدهم، انجام می‌دهم یا نه. هر موقع جواب این سؤال نه باشد من می‌فهمم تو زندگی ام به يك سری تغییرات احتیاج دارم.

من امروز خیلی خوشحالم که در مراسم فارغ‌التحصیلی شما که در یکی از بهترین دانشگاه‌های دنیا درس می‌خوانید هستم. من هیچ وقت از دانشگاه فارغ‌التحصیل نشده‌ام. امروز می‌خواهم داستان زندگی ام را برایتان بگویم. خیلی طولانی نیست و سه تا داستان است.  
ادامه‌ی مطلب را در سایت فناوری ببینید...

## ۷.۴ ۵ نکته امنیتی درباره gmail

داشتن یک رمز عبور قوی در حفظ اطلاعات شما کمک زیادی می‌کند اما علاوه بر این باید چند کار دیگر انجام دهید تا خیالتان از بابت امنیت اکانت جی میل‌تان راحت شود :

۱. حتما از ایمیل تان خارج شوید . بخصوص هنگامی که با استفاده از یک کامپیوتر عمومی به جی میل وارد می‌شوید (مثلا در کافی نت یا سایت دانشگاه) حتما پس از تمام شدن کارتان از صندوق ایمیل خود خارج شوید (sign out). کار سختی نیست، فقط بر روی لینک sign out گوشه بالا و راست صفحه ایمیل‌تان کلیک کنید. اگر می‌خواهید خیالتان راحت تر شود حتما پس از این کار cache ، کوکی ها و تاریخچه (history) مرورگرتان را هم پاک کنید. سپس مرورگر را بصورت کامل ببندید. در کامپیوتر خانگی تان اگر لازم است بصورت مداوم از آن دور شوید می‌توانید آن را با استفاده از یک اسکرین سیور رمزدار محافظت کنید تا کسی بدون اجازه و در غیاب شما به اطلاعات صندوق پستی تان دسترسی نداشته باشد.

۲. مراقب ارسال اطلاعات حساس و محرمانه از طریق ایمیل باشید . هنگامی که شما یک ایمیل را فرستادید دیگر هیچ کنترلی در مورد اطلاعاتی که در آن ایمیل ارسال کرده اید ندارید. این به معنی آن است که اگر گیرندگان ایمیل بخواهند می‌توانند آن را برای کسان دیگری بفرستند یا اطلاعات بعضا محرمانه شما را در محیط عمومی منتشر کنند. حتی اگر به این افراد اعتماد هم داشته باشید باز هم ممکن است بخاطر سهل انگاری آنها ایمیلشان هک شود یا یک ویروس این اطلاعات

را بدزد. اطلاعات حساب های بانکی، کارت های اعتباری، رمزهای عبور و اطلاعات حساسی از این دست به هیچ وجه نباید از طریق ایمیل و به هیچ کس دیگر منتقل شوند. گوگل هیچگاه به شما ایمیل نمی زند تا از شما رمزعبورتان را بخواهد پس هرگز فریب این حقه هکرها را نخورید!

**۳. فعال کردن حالت استفاده از پروتکل https.** هر زمان که شما یک صفحه وب را مشاهده می کنید، کامپیوتر شما نیاز به ارسال و دریافت اطلاعات به شبکه اینترنت دارد. https اطلاعاتی را که بین کامپیوتر و اینترنت منتقل می شود را بصورت رمز درمیآورد تا شناسایی محتوای آنها در این بین غیرممکن باشد. جی میل برای لاگین کاربران خود از این پروتکل استفاده می کند اما شما می توانید صندوق پست الکترونیکی خود را نیز با استفاده از این پروتکل مرور کنید. استفاده از https، باعث کندتر شدن فعالیت شما در جی میل می شود اما اگر بخواهید می توانید با کلیک بر روی settings و انتخاب always use https در زبانه general جی میل را وادار کنید همیشه از این پروتکل برای ارتباط با شما استفاده کند.

**۴. مراقب فایل های ضمیمه مشکوک باشید.** برای محافظت شما از ویروس ها و نرم افزارهای مخرب دیگر جی میل تمام اتچمنت ها را هنگامی که ایمیل به صندوق شما می رسد اسکن می کند. عملیات اسکن یکبار دیگر هنگامی که ایمیل مذکور را باز می کنید تکرار می شود. فایل های ضمیمه ای که شما هم می فرستید توسط آنتی ویروس آنلاین گوگل کنترل می گردد. اما جی میل می گوید باز هم مراقب فایل های ضمیمه باشید و هر فایلی را که انتظار دریافتش را ندارید باز نکنید، حتی اگر از طرف دوست شما باشد. قبل از اینکه فایل ضمیمه ایمیل را باز کنید از فرستنده پرسید که چه چیزی را برای شما فرستاده است و وقتی از بی خطر بودنش مطمئن شدید نسبت به بازکردن آن اقدام کنید.

**۵. اطلاعات مربوط به بازیابی حساب کاربری خودتان را به روز نگه دارید.** اطلاعات بازیابی اکانت به شما کمک می کند تا به حسابتان دسترسی پیدا کنید حتی اگر رمز عبور آن را فراموش کرده باشید یا یک نفر با دسترسی به حساب کاربری شما آن را تغییر داده باشد. در حال حاضر گوگل به سه روش می تواند به شما کمک کند. استفاده از آدرس ایمیل ثانوی، که با تعیین این ایمیل گوگل در هنگام فراموشی رمز توسط شما یک لینک برای ریست کردن رمز به این آدرس می فرستد. استفاده از sms که البته در همه کشورهای جهان (حتی افغانستان) فعال است بجز ایران! و روش سوم هم استفاده از پرسش و پاسخ امنیتی که در این روش باید سوالی را تعیین کنید که جواب دادنش برای شما آسان و برای دیگران غیرممکن باشد.

منبع مطلب

## ۸.۴ IP-Phone چیست؟

تکنولوژی IP-phone فناوری جدید مخابراتی است که در چند سال اخیر به موازات گسترش سایر فناوری های ارتباطی از قبیل شبکه های کامپیوتری، اینترنت و غیره پیشرفت کرده و به سرعت صنعت مخابرات و بازار مصرف را تحت تأثیر قرار داده است. این تکنولوژی در واقع نوع جدیدی از دستگاه های مخابراتی است که بر

روی بستر شبکه های کامپیوتری فعالیت می کند، لذا علاوه بر این که تمامی انتظارات از یک مرکز مخابرات را برآورده می سازد، برای ارائه خدمات و سرویس های نامحدود و جدید انعطاف پذیری می باشد و همین باعث گردیده که فعالان عرصه ارائه خدمات مخابراتی بتوانند با سرمایه گذاری کم

و مخارج عملیاتی پایین، طیف وسیعی از سرویس‌ها را در اختیار استفاده‌کنندگان قرار دهند و نیز توسعه کاربرد IP Phone برخلاف سیستم‌های مخابراتی سنتی منجر به همگرا شدن سرویس‌های صوتی، تصویری و داده‌ها شده است؛ و بنا به گفته‌های بیان‌شده دیگر نیازی به سرمایه‌گذاری جداگانه بر روی تک‌تک سرویس‌های مخابراتی نمی‌باشد و سرمایه‌گذاری فقط بر روی تکنولوژی IP Phone متمرکز می‌گردد.

در این تلفن‌ها همگرایی شبکه‌های صوت و دیتا امکان‌پذیر می‌باشد. IP-Phone یک دستگاه دیجیتالی باهوش با واسط شبکه LAN می‌باشد. IP-Phone دارای یک آدرس IP و کانکتورهای استاندارد (RJ-45) می‌باشد لذا اینگونه تلفن‌ها می‌توانند درون هرپورتی در شبکه LAN قرار گیرند. از آنجائیکه به تلفن‌های مذکور آدرس IP اختصاص می‌یابد لذا امکانات در آن بسیار زیاد است و این امکانات و قابلیت‌ها بستگی به ویژگی‌های Feature که تولیدکنندگان روی آن قرار می‌دهند دارد. کاربردهای مهم آن شامل Unified Messaging Collaboration کنفرانس و غیره می‌باشد. با IP-Phone کاربران می‌توانند Extension خودشان را با خود حمل کرده بطوری که هرگز یک مکالمه را از دست ندهند. با استفاده از این تلفن‌ها می‌توان ارتباطات کنفرانس ایجاد نمود. می‌توان اطلاعات web را در حال پاسخ به مکالمه خواند و یا به یک سرویس Web based برای چک کردن پست الکترونیکی، وضعیت هوا، شرایط ترافیک یا چک کردن موجودی خود در بانک Login کرد. عموماً این تلفن‌ها قادر هستند دیتا و صوت را روی LAN های موجود ارسال نمایند. علاوه بر توانایی‌های مذکور بعضاً این تلفن‌ها قادر هستند کاربردهای بیسیم را همراه با کاربردهای تلفن معمولی در یک ساختار

تلفنی واحد ارائه نمایند. عموماً نرم‌افزار این سیستم‌ها قابل Upgrade شدن می‌باشند. تعدادی از قابلیت‌های دیگر این قبیل تلفن‌ها بقرار ذیل می‌باشند:

- ۱- دارای دکمه کنترلی صدا برای ارتباطات ورودی روی بلندگو و گوشی تلفنی.
- ۲- غیرفعال نمودن یک ارتباط بدون اینکه گوشی را روی قلاب بگذاریم.
- ۳- دارای قابلیت Mute Function برای قطع گوشی و میکروفن بدون استفاده از دست.
- ۴- انتقال مکالمه به Extension دیگر و یا به یک شماره دیگر.
- ۵- انجام Call Forward به شماره‌های داخلی و خارجی.
- ۶- دارای نشانه‌گر انتظار پیام (Stuttered dial tone).
- ۷- توانایی ایجاد Conference
- ۸- توانایی ارائه سرویس Call back
- ۹- توانایی ارائه سرویس Call Conferencing
- ۱۰- توانایی ارائه سرویس Call Forwarding
- ۱۱- توانایی ارائه سرویس Call Hold
- ۱۲- توانایی ارائه سرویس Call Transfer
- ۱۳- توانایی ارائه سرویس Do not disturb
- ۱۴- توانایی ارائه سرویس Intercom
- ۱۵- توانایی ارائه سرویس Paging
- ۱۶- توانایی ارائه سرویس Speed dialing

معمولاً کیفیت صوت و ضریب اطمینان در این سیستم‌ها همانند تلفن‌های سنتی می‌باشد و براحتی قابل مدیریت کردن می‌باشند. این تلفن‌ها می‌توانند به یک PC وصل شده و قادر هستند براحتی با شبکه دیتا ارتباط برقرار نمایند. در جاهایی که فقط نیاز به یک تلفن می‌باشد از لحاظ اقتصادی مقرون

به صرفه است که از IP-Phone استفاده گردد. تلفن‌های بصورت IP استاندارد قابل ارائه می‌باشند و از آنها می‌توان در IP Telephony استفاده نمود.  
 يك IP Telephone نمونه دارای شش دکمه جهت Featureها و تعدادی کلید جهت راهنما قابلیت‌ها و عملکردها می‌باشد. این تلفن قادر است زمان، تاریخ و اسم مشترك تلفن‌کننده و شماره تلفن او و رقم‌هایی که گرفته شده است را نمایش دهد.  
 این تلفن دارای توانایی گرافیکی نیز می‌باشد. روش‌های زیر استفاده از IP-Phone را مقدور می‌سازند:

با استفاده از Buttonها

با استفاده از Soft keyها

با استفاده از Navigation key

دسترسی مستقیم با استفاده از رقم‌های مربوطه

از دیگر قابلیت‌های این سیستم می‌توان به موارد ذیل اشاره نمود:

قادر IP-Phone است پیام‌های ورودی را گرفته و آنها را دسته‌بندی کند و روی صفحه برای کاربر نمایش دهد. با این روش کاربر خیلی موثر و سریع می‌تواند جواب تلفن‌های خود را بدهد. این سیستم دارای دفترچه تلفنی است بنام (Light Weight Directory Access Protocol). LPAP3 نور صفحه نمایش این تلفن قابل تنظیم می‌باشد. این سیستم دارای Ringer Tone و تنظیمات صدا برای کلیه صوتها از قبیل Ringer Head Set, Handset, و بلندگو می‌باشد. با استفاده از این تلفن کاربرها می‌توانند به اطلاعاتی نظیر وضعیت هوا، بورس و یا هر اطلاعاتی که در Web وجود دارد دسترسی پیدا نمایند. با این تلفن می‌توان مستقیماً به شبکه Ethernet متصل شد. Virtual LAN جداگانه جهت PC و تلفن IP توسط مدیریت این سیستم قابل تعریف می‌باشد.

منبع: <http://www.parsptco.com/Read.php?SID=2>

## ۹.۴ دنیس ریچی هم درگذشت

پدر زبان برنامه نویسی C و سیستم عامل یونیکس، دنیس ریچی، در سن ۷۰ سالگی پس از یک بیماری طولانی مدت درگذشت.



آقای دنیس ریچی، خالق زبان برنامه‌نویسی C و از اعضای سازندگان سیستم عامل یونیکس در سن ۷۰ سالگی درگذشت. نوآوری‌های گسترده اوائل انقلاب صنعتی کامپیوتر به واسطه کارهای آقای دنیس ریچی و همکارانش بوده‌است. وی به عنوان تیتان صنعت رایانه شناخته می‌شود. خبر مرگ وی، نخست توسط همکار او در Bell Labs، آقای Rob Pike به اطلاع عموم رسانیده شد. به گزارش وین بتا، آقای دنیس ریچی در سال‌های دهه ۶۰ و ۷۰ میلادی همراه با کسانی همچون Ken Thompson Brian Kernighan Douglas McIlroy و Joe Ossanna سیستم عامل یونیکس را ساخت. وی در Bell Labs توانست زبان برنامه‌نویسی C را طراحی کند. این زبان برنامه‌نویسی تا کنون از محبوبیت جهانی برخوردار است. بخاطر کارهای آقای دنیس ریچی صنعت برنامه‌نویسی رایانه در آن سال‌ها به سرعت محبوب شد و باعث شد که جنبش‌های نرم‌افزار کد باز و آزاد پدید آیند. نرم‌افزارهای آزاد در آینده باعث شدند که شبکه جهانی اینترنت را به پیش ببرند. مرگ آقای دنیس ریچی شاید به اندازه درگذشت آقای استیو جابز (مدیر عامل شرکت اپل) خوراک خبری رسانه‌ها را تشکیل ندهد زیرا که وی به زندگی کاملاً خصوصی و بدور از هیاهو عادت داشت اما دست‌آوردها و کارهای وی برای بشر مطمئناً کمتر از آقای استیو جابز نیست. آقای Pike گفته است که دنیا «یک نابغه واقعی» را از دست داده است. برای درک بهتر کارهای آقای دنیس ریچی میتوان به مثال‌هایی همچون: طراحی زبان C و همکاری در ساخت یونیکس اشاره داشت اما هنگامیکه متوجه می‌شویم که کرنل سیستم‌عامل‌های لینوکس و یونیکس، مکینتاش و شاید حتی ویندوز با زبان C نوشته شده‌اند به راستی به واژه نابغه واقعی میرسیم. تقریباً همه مرورگرهای وب با زبان C و یا ++C نوشته شده‌اند. حتی هنگامیکه آقای Tim Berners-Lee اولین ساختار شبکه جهانی وب را آزمایش میکرد از رایانه NexT استفاده کرد که از سیستم عامل یونیکس بهره میبرد و زبان برنامه نویسی اش C بود. اگر دنیس ریچی نبود، شاید هیچگاه رایانه‌های شخصی به این شکل در اختیار ما نبودند و هیچوقت شبکه جهانی اینترنت خصوصیات و آزادی‌های نرم‌افزاری امروز را نداشت. گفتنی است که آقای دنیس ریچی دارای بلندمرتبه ترین مدال افتخار فناوری از کشور ایالات متحده امریکا است. وی این مدال را در سال ۱۹۹۹ میلادی از دست آقای بیل کلینتون دریافت کرد.

## ۱۰۴ IPTV چیست؟

در این مقاله سعی کرده‌ایم خواننده را با مبانی فناوری IP-TV آشنا کنیم و به طور مختصر به وضعیت ارائه آن در جهان بپردازیم.

### ● IP-TV چیست؟

به ارسال و پخش برنامه‌های تلویزیونی برای مشترکان از طریق زیرساخت باند وسیع و توسط پروتکل اینترنت IP-TV گفته می‌شود. این سرویس معمولاً با سرویس‌های دیگری مانند ویدئو بر طبق تقاضا و تلفن اینترنتی و اینترنت پرسرعت، در قالب یکپستهبه مشترکان ارائه می‌شود. امروزه، بسیاری از سرویس‌دهندگان باند وسیع ارائه سرویس‌های تلویزیونی را روی شبکه‌های IP آغاز کرده‌اند. به علت توسعه باند وسیع و پیشرفت‌های چشمگیر در ارائه فناوری‌هایی چون ADSL<sup>+</sup> که توان پخش محتوای چندرسانه‌ای را با کیفیت بالا دارد و نیز ارائه استانداردهای نوین فشرده‌سازی مانند MPEG-۴ و کاهش هزینه‌های انتقال دیتا و...، بازار IP-TV پتانسیل بسیار خوبی برای رشد پیدا کرده است.

### ● کاربردهای IP-TV

### ■ پخش دیجیتالی تلویزیون:

سرویس‌های پخش دیجیتالی امروزی عموماً از طریق کابل یا ماهواره به مشترکان می‌رسند؛ اما ظهور نسخه‌های جدید و پرسرعت DSL (با توجه به گستردگی زیرساخت آن) IP-TV را به رقیب جدی ارائه سرویس‌های تلویزیونی ماهواره و کابل تبدیل کرده است. از سوی دیگر، IP-TV نسبت به تلویزیون‌های معمولی توانایی رساندن تعداد زیادتری از کانال‌های تلویزیونی به مشترک را دارد. علاوه بر این، به علت ماهیت بسته‌ایدیتا و دوطرفه (تعاملی) بودن خط ارتباطی، بیننده قادر است که تصمیم بگیرد که چه چیز را چه وقتی خواهد بیند.

■ ویدئو بر طبق تقاضا: این سرویس در واقع یک سرویس برای استفاده شخصی مشترکان است که در آن کاربر قادر به انتخاب و دانلود محتوای ویدئویی مورد علاقه خود است. این سرویس برای اپراتورها یک سرویس درآمدزاست و شامل این بخش‌ها است:

- فیلم بر طبق تقاضا که کاربران از یکبانک فیلم‌فیلیم مورد علاقه خود را انتخاب می‌کنند.  
- برنامه‌ها و محتواهای ذخیره‌شده‌ای که لزومی به مشاهده بهنگام آنها نیست و کاربر می‌تواند آنها را دانلود و سپس مشاهده کند. مثل: اخبار، رویدادهای ورزشی، برنامه‌های آموزشی و...

### ■ سرویس‌های تلفنی گوناگون:

تلفن معمولی، تلفن تصویری و ویدئو کنفرانس انواع سرویس‌های تلفنی هستند که می‌توانند توسط IP-TV ارائه شوند.

### ■ دسترسی به اینترنت:

امروزه اتصال به وب یک نیاز ضروری است که کاربردهای بسیار متنوعی دارد؛ IP-TV این نیاز را هم برآورده می‌کند.

### ■ آموزش از راه دور:

با توجه به زیرساخت مناسب و گستردگی توزیع، IP-TV برنامه‌های آموزش از راه دور الکترونیکی می‌تواند از طریق این سرویس به کاربران برسد.

### ● اجزای IP-TV

ارائه مستلزم IP-TV تهیه محتوا برای انتشار، مدیریت محتوا و رساندن آن با کیفیت و امنیت مناسب به کاربر نهایی است. بر این اساس، اجزای IP-TV را می‌توان به این صورت برشمرد:

### ■ منابع محتوا:

منظور محتوای دیجیتالی و ویدئویی است که از تولیدکنندگان محتوا نظیر تهیه‌کنندگان برنامه‌های چندرسانه‌ای، شبکه‌های تلویزیونی و... تهیه می‌شود.

### ■ گره‌های سرویس:

گره‌های سرویس، جریان ویدئو و محتوا با فرمت‌های متفاوت را دریافت کرده و پس از شکل‌دهی مجدد، آنها را با کیفیت سرویس مناسب در ناحیه‌ای وسیع از شبکه به مشترکان ارسال می‌کند.

### ■ هسته توزیع در شبکه:

این بخش توانایی توزیع و سایر قابلیت‌هایی را که برای ارسال مطمئن دیتا به تجهیزات انتهایی (CPE) مشترکان مورد نیاز است فراهم می‌آورد. این بخش شامل زیرساختی از DSLAM و شبکه نوری است که در اداره مرکزی یا نقاط توزیع راه دور واقع شده‌اند.

### ■ شبکه دسترسی مشتری:

ارسال IP-TV به منازل مشترکان از طریق خطوط DSL با سرعت بالا نظیر ADSL<sub>2+</sub> و VDSL و یا خطوط فیبر نوری ممکن است. منظور از شبکه دسترسی نیز همین تکنولوژی‌هاست.

### ■ تجهیزات انتهایی مشترک:

بخشی است که ترافیک IP-TV بدانجا ختم می‌شود و در اختیار مشترک است. این بخش که می‌تواند یک جعبه نصب شدنی باشد، به عنوان بخش عملیاتی سرویس عمل می‌کند و کارهایی چون اتصال به شبکه، کدگذاری دیتا، کنترل نمایش به دلخواه کاربر و... را بر عهده دارد.

#### ● راز جذابیت‌های IP-TV چیست؟

پس از گسترش موج باند وسیع در دنیا، سرویس‌هایی که قابلیت ارائه روی باند وسیع را دارند به سرعت در حال گسترش هستند. در واقع جذابیت این سرویس‌ها است که مشتریان را به سوی تکنولوژی باند وسیع سوق می‌دهند. IP-TV به عنوان یکی از سرویس‌هایی که لازمه ارائه آن وجود زیرساخت باند وسیع است، در حال تبدیل شدن به یکی از جذاب‌ترین سرویس‌ها است. اما به راستی علت این مسأله چیست؟

#### ● امکان پیاده سازی در گستره و مقیاس وسیع

توسعه دو فناوری مهم، زمینه راه‌اندازی گسترده IP-TV را فراهم کرده است. این دو فناوری عبارتند از:

■ فناوری‌های دسترسی با سرعت بسیار بالا مانند: ADSL + VDSL و فیبر نوری در قالب فیبر به خانه

#### ■ فشرده‌سازی به شیوه MPEG-۲

فناوری ADSL+۲ هم کیفیت انتقال را از طریق افزایش پهنای باند زیاد می‌کند و هم با توجه به آنکه با افزایش فاصله، نرخ انتقال دیتا در DSL به شدت افت می‌کند، با افزایش پهنای باند می‌تواند نواحی دورتری را تحت پوشش DSL قرار دهد. فیبر یا FTTH نیز عملکرد بسیار خوبی دارد و از تمامی تکنولوژی‌ها و از جمله ADSL+۲ نیز برتر است. (سرعت ارسال ۱۰۰ Mbps تا ۱ Gbps در مقایسه با ۲۵ Mbps) البته اشکال عمده فیبر، زمان‌بر بودن نصب و گسترش آن و هزینه زیاد ایجاد آن است که معمولاً جز با کمک و همکاری مؤثر دولت‌ها ممکن نیست. MPEG-۴ نیز برای ارسال به نصف پهنای باند MPEG-۲ نیاز دارد که مسلماً مزیتی مهم است.

#### ● مقرون به صرفه بودن سرویس‌های سه‌گانه

منظور از سرویس‌های سه‌گانه، ارائه اینترنت پرسرعت، تلفن و تلویزیون IP در قالب یک بسته مشترک است. مسلماً هر یک از این سرویس‌ها، کاربردها و جذابیت‌های خود را دارد که ارائه همه آنها با هم و با قیمت مناسب، بر جذابیت‌های آنها می‌افزاید. مشخص است که این ارائه این سرویس یک بازی برد-برد برای طرفین است. هم مشتریان نیازهای ارتباطی خود را با پرداخت هزینه‌ای مناسب برآورده می‌کنند و هم شرکت‌های مخابراتی حداکثر استفاده را از سرمایه‌گذاری‌های انجام‌شده در زیرساخت، شبکه دسترسی و تجهیزات خود می‌برند.

#### ● ورود به یک بازار عظیم

بنا به آمار، اپراتورهای کابلی و ماهواره‌ای تلویزیونی در سال ۲۰۰۴، فقط در ایالات متحده، ۵۵ میلیارد دلار درآمد کسب کرده‌اند. بنابراین، به دلیل گردش مالی بسیار زیاد ارائه سرویس‌های تلویزیونی، تمامی اپراتورها مشتاقانه به دنبال فرصت‌هایی نوین برای ارائه سرویس‌های تلویزیونی هستند. توسعه دو فناوری مهم، زمینه راه‌اندازی گسترده IP-TV را فراهم کرده است. این دو فناوری عبارتند از:

■ فناوری‌های دسترسی با سرعت بسیار بالا مانند: ADSL + VDSL و فیبر نوری در قالب فیبر به خانه

#### ■ فشرده‌سازی به شیوه MPEG-۲

فناوری ADSL+۲ هم کیفیت انتقال را از طریق افزایش پهنای باند زیاد می‌کند و هم با توجه به

آنکه با افزایش فاصله، نرخ انتقال دیتا در DSL به شدت افت می‌کند، با افزایش پهنای باند می‌تواند نواحی دورتری را تحت پوشش DSL قرار دهد. فیبر یا FTTH نیز عملکرد بسیار خوبی دارد و از تمامی تکنولوژی‌ها و از جمله ADSL<sub>2+</sub> نیز برتر است. (سرعت ارسال ۱۰۰ Mbps تا ۱ Gbps در مقایسه با ۲۵ Mbps) البته اشکال عمده فیبر، زمان‌بر بودن نصب و گسترش آن و هزینه زیاد ایجاد آن است که معمولاً جز با کمک و همکاری مؤثر دولت‌ها ممکن نیست. ۴-MPEG نیز برای ارسال به نصف پهنای باند ۲-MPEG نیاز دارد که مسلماً مزیتی مهم است.

#### ● یک فرصت استثنایی

IP-TV یک پدیده جهانی است که فرصتی را برای شرکت‌های مخابراتی جهت استفاده بهتر از زیرساخت‌های خود به منظور ارسال ویدئو و محتوای دیجیتال روی شبکه‌های IP فراهم کرده است. تحقیقات نشان می‌دهد که تعداد مشترکان IP-TV از ۲۰۱ میلیون در سال ۲۰۰۴ به ۲۷ میلیون در سال ۲۰۰۸ خواهد رسید و درآمد حاصل از آن در این سال از ۱۵ میلیارد دلار خواهد گذشت. در این میان، قاره آسیا در ارائه IP-TV پیشرو خواهد بود.

بر اساس برخی تحقیقات، از ۱۳ کشور آسیای شرقی ۷ کشور در حال راه‌اندازی یا ارائه IP-TV هستند. بزرگترین شرکت مخابراتی هنگ‌کنگ به نام PCCW هم‌اکنون حدود یک‌سوم تعداد کل مشترکان IP-TV دنیا را در اختیار دارد که عمدتاً بر روی شبکه ADSL با پهنای باند ۶ Mbps سرویس خود را ارائه می‌دهد.

در اروپای غربی نیز هم‌اکنون DSL در میان شیوه‌های دسترسی باند وسیع مقام اول را دارد و رتبه بعدی از آن کابل است. بنا به آمار، هم‌اکنون حدود ۴۰ میلیون خانوار در اروپای غربی مشترک باند وسیع هستند که پیش‌بینی می‌شود این تعداد در سال ۲۰۱۰ به ۱۰۷ میلیون (معادل ۶۳ درصد کل خانوارهای اروپای غربی) برسد.

اما ارائه IP-TV در کشورهای مختلف این قاره نیز آغاز شده است؛ در ایتالیا و سوئد به ترتیب FastWeb به حدود ۲۰۰ هزار مشترک و ViaSat به ۳۰۰ هزار مشترک بر روی فیبر و DSL-IP-TV ارائه می‌کنند. جالب توجه آنکه ViaSat اولین اپراتور اروپایی است که اینترنت باند وسیع را با سرعت ۱۰۰ Mbps (روی فیبر) ارائه می‌دهد. همچنین ارائه ADSL<sub>2+</sub> با سرعت ۲۴ Mbps در ازای ماهیانه ۴۰ یورو، از دیگر خدمات این شرکت است.

در انگلستان VNL ارائه سرویسی موسوم به HomeChoice را از سپتامبر ۲۰۰۴ آغاز کرده است. مشترکان با دریافت این سرویس در حقیقت ۳ سرویس دارند: تلویزیون دیجیتال، اینترنت پر سرعت و تلفن. هزینه این سرویس جذاب در (تابستان ۲۰۰۶) به ماهیانه ۱۵ پوند رسیده است.

#### ● نتیجه‌گیری

IP-TV در حال فراگیر شدن است. گسترش زیرساخت‌های باند وسیع و شبکه‌های مبتنی بر IP و فشار بازار و رقابتی‌تر شدن فضا از یک سو و حرکت سرویس‌ها و تقاضای مشترکان به سمت همگرایی دیجیتالی از سوی دیگر، به تسریع این روند دامن می‌زند. در این میان IP-TV می‌تواند با بهره‌گیری از نقاط قوت و مزایای ذاتی خود نظیر آشنایی طولانی مدت مردم با تلویزیون و گسترش روز افزون شبکه‌های دسترسی باند وسیع به یکی از محبوبترین و گسترده‌ترین سرویس‌های عصر دیجیتال تبدیل گردد.

سرویس‌دهندگان مخابراتی با استفاده از تجربه‌های خود در ایجاد و گسترش شبکه‌های مخابراتی و ارائه سرویس بر روی آنها و اعتباری که نزد مشتریان خود کسب کرده‌اند، می‌توانند در ارائه IP-TV نقش اصلی را بر عهده بگیرند. البته ارائه و بسط یک زنجیره ارزش و ایجاد پیوند و همکاری تنگاتنگ با تولیدکنندگان فیلم و محتوا و صاحبان شبکه‌های تلویزیونی در این میان بسیار ضروری است.



منبع متن : <http://persian-service.mihanblog.com/post/205>

## ۱۱.۴ شبکه VPN چیست؟

شبکه VPN چیست؟

شبکه های خصوصی مجازی در طی ده سال گذشته دنیا دستخوش تحولات فراوانی در عرصه ارتباطات بوده است . اغلب سازمانها و موسسات ارائه دهنده کالا و خدمات که در گذشته بسیار محدود و منطقه ای مسائل را دنبال و در صدد ارائه راهکارهای مربوطه بودند ، امروزه بیش از گذشته نیازمند تفکر در محدوده جهانی برای ارائه خدمات و کالای تولید شده را دارند. به عبارت دیگر تفکرات منطقه ای و محلی حاکم بر فعالیت های تجاری جای خود را به تفکرات جهانی و سراسری داده اند. امروزه با سازمانهای زیادی برخورد می نمائیم که در سطح یک کشور دارای دفاتر فعال و حتی در سطح دنیا دارای دفاتر متفاوتی می باشند . تمام سازمانهای فوق قبل از هر چیز دنبال یک اصل بسیار مهم می باشند : یک روش سریع ، ایمن و قابل اعتماد بمنظور برقراری ارتباط با دفاتر و نمایندگی در اقصی نقاط یک کشور و یا در سطح دنیا اکثر سازمانها و موسسات بمنظور ایجاد یک شبکه WAN از خطوط اختصاصی (Leased Line) استفاده می نمایند. خطوط فوق دارای انواع متفاوتی می باشند. ISDN ( با سرعت ۱۲۸ کیلوبیت در ثانیه ) ، ( OC3 Optical Carrier-3 ) ( با سرعت ۱۵۵ مگابیت در ثانیه ) دامنه وسیع خطوط اختصاصی را نشان می دهد. یک شبکه WAN دارای مزایای عمده ای نسبت به یک شبکه عمومی نظیر اینترنت از بعد امنیت و کارآئی است . پشتیبانی و نگهداری یک شبکه WAN در عمل و زمانیکه از خطوط اختصاصی استفاده می گردد ، مستلزم صرف هزینه بالائی است .

همزمان با عمومیت یافتن اینترنت ، اغلب سازمانها و موسسات ضرورت توسعه شبکه اختصاصی خود را بدرستی احساس کردند. در ابتدا شبکه های اینترنت مطرح گردیدند. این نوع شبکه بصورت کاملاً اختصاصی بوده و کارمندان یک سازمان با استفاده از رمز عبور تعریف شده ، قادر به ورود به شبکه و استفاده از منابع موجود می باشند. اخیراً، تعداد زیادی از موسسات و سازمانها با توجه به مطرح شدن خواسته های جدید ( کارمندان از راه دور ، ادارات از راه دور ) ، اقدام به ایجاد شبکه های اختصاصی مجازی (VPN(Virtual Private Network) نموده اند.

یک VPN ، شبکه ای اختصاصی بوده که از یک شبکه عمومی ( عموماً اینترنت ) ، برای ارتباط با سایت های از راه دور و ارتباط کاربران بایکدیگر، استفاده می نماید. این نوع شبکه ها در عوض استفاده از خطوط واقعی نظیر : خطوط Leased ، از یک ارتباط مجازی بکمک اینترنت برای شبکه اختصاصی بمنظور ارتباط به سایت ها استفاده می کند.  
ادامه مطلب را در سایت فناوری ببینید...

## ۱۲.۴ تبلت چیست؟

تبلت چیست؟

به رایانه های قابل حملی که سیستم ورود اطلاعات آن بوسیله ی صفحه ی لمسی (touch screen)

است تبلت گویند. از ویژگی های بارز آن می توان به شکل و سایز منحصر به فرد و ارتباط بیسیم و قابلیت اتصال آن به شبکه های محلی یاد کرد. همچنین تبلت ها دارای سیستم عامل های گوناگونی هستند که بعضی از آنها مانند سیستم اپل (ios) و یا اچ پی (webos) مختص محصول خود آن شرکت هستند، اما اکثر تبلت ها از سیستم عامل های ارائه شده توسط شرکت های تولید کننده نرم افزار استفاده می کنند که در این زمینه می توان به سیستم windows 7 از ماکروسافت و یا android گوگل اشاره کرد.

تاریخچه:

پروژه های که در سال ۱۹۸۹ در مرکز مطالعات شرکت اپل شروع شد، اولین بار در سال ۱۹۹۳ با نام newton به بازار عرضه شد، اما گام دوم تکمیل این محصول را باید از آن شرکت مایکروسافت دانست که در سال ۲۰۰۱ به ارائه سیستم عامل xp با نام تبلت پرداخت. همچنین برای اولین باری بود که نام تبلت به آن اطلاق شد و باید ریشه ی این اسم را در شرکت مایکروسافت دانست نه اپل. از ویژگی های این محصول مایکروسافت می توان به قلم نوری و صفحه لمسی که امکان تایپ دستی را بر روی آن فراهم می آورد اشاره کرد. این مدل را می توان آغازگر ورود برندهای دیگر بجز اپل، ابداع کننده ی در آن زمان منزویش دانست. اما در نهایت سال ۲۰۱۰ را باید سال ورود باشکوه اپل به بازار تبلت دانست. اتفاقی که هواداران بیشمار اپل مدتها منتظر آن بودند بالاخره در این سال تحقق یافت و اپل توانست با اقتدار کامل سکان هدایت بازار این محصول را بار دیگر در دست گیرد. محاسن و معایب:

مزیت تبلت نسبت به نوت بوک و البته نت بوک وزن و سایز آن است که امکان استفاده از آن را در شرایط های گوناگونی چون هنگام نشستن بر روی مبل، در حال دراز کشیدن و یا حتی هنگام راه رفتن به راحتی هر چه تمام تر فراهم می آورد.

اما در مورد معایب این محصول می توان به صفحه ی لمسی آن اشاره کرد که علاوه بر آنکه در موقعیت های مختلف در معرض آسیب دیده گی قرار دارد امکان تایپ با آن را بسیار دشوارتر از کیبورد های سنتی کرده است. همچنین این دستگاه نسبت به نت بوک، لپ تاپ و pc ها دارای قدرت پردازش پایین و به تبع امکانات و کاربری کمتری است. سیستم عامل:

همانطور که در بالا اشاره شد این محصول در بازار خود سیستم عامل های (os) گوناگونی می بیند که می توان از ios، android، windows به عنوان مطرح ترین ها اشاره کرد. با ورود ipad در سال ۲۰۱۰ که سیستم عامل ویژه اپل (ios) بر آن نصب بود ios توانست با فروش خوبی که در این محصول داشت به تنهایی بیش از ۹۰ درصد سهم سیستم عامل ها را به خود اختصاص دهد. اما در طی یکسال گذشته شرکت گوگل که به تازه گی توانسته عنوان برترین برند سال ۲۰۱۱ را کسب نماید بی کار ننشسته و با ارائه ورژن های مختلف از آندروید با نامهایی کامتوانسته رشد خوبی را در این زمینه داشته باشد. موسسه ی آمار و اطلاعات بین المللی در (IDC) آخرین گزارشات خود، سه ماهه ی سوم ۲۰۱۰ را با داشتن ۹۳ درصد از آن ios دانست، این در حالی است که در این دوره android حضور قابل توجهی در بازار نداشته است. اما در سه ماهه آخر ۲۰۱۰ با ورود گلگسی تب سامسونگ که اصلی ترین مجرای عرضه آندروید به حساب می آید توانست ۱۷ درصد بازار را بدست آورد. همچنین xoom Motorola آنکه از اصلی ترین ارائه دهندگان آندروید به حساب می آید در سه ماهه ی نخست ۲۰۱۱ تنها ۳/۲ درصد از سهم بازار را کسب کرد، که به عقیده ی برخی کارشناسان این میزان شکستی برای Motorola به حساب می آید. گرچه همچنان اپل با در اختیار داشتن بیش

از ۶۰ در صد همچنان در صدر قرار دارد ولی نسبت به سال گذشته ۳۰ درصد از سهم خود را به گوگل تقدیم کرده است.

اما در مقام مقایسه می توان داشتن طراحی زیبا ، سادگی، قابلیت airply و از همه مهم تر ویژگی های سخت افزاری مناسب را از ویژگی های سیستم عامل اپل دانست و در مقابل سیستم آگاه سازی آسان، مولتی تسکینگ کارآمد، صفحه خانگی مناسب، ابزار های منحصر به فرد دوربین و در نهایت خرید آسان برنامه ها روی مرورگر و بدون نیاز به هماهنگ سازی را از عوامل متمایز کننده آندروید دانست.

بازار جهانی فروش تبلت :

در حال حاضر اپل با داشتن نزدیک به ۸۰ درصد از سهم بازار یکه تاز این عرصه است. جدی ترین رقیب آی پد یعنی گلکسی تنها ۴ درصد این بازار را در اختیار دارد. اما با گسترش و تکمیل سیستم عامل گلکسی (آندروید) که در حال حاضر در زمینه گوشی های همراه توانسته سهم قابل توجهی را از اپل بگیرد انتظار می رود در زمینه تبلت هم این روند ادامه پیدا کند و در آینده ای نه چندان دور شاهد گسترش بازار فروش تبلت های آندرویدی باشیم.

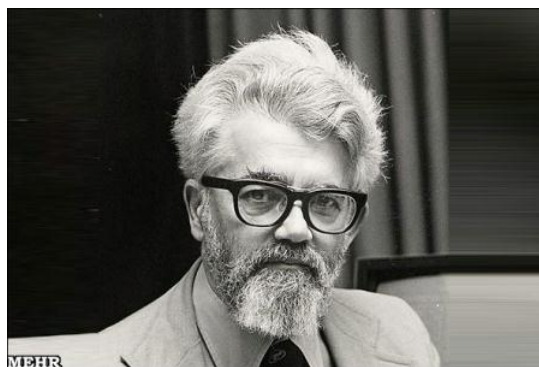
تبلت در ایران :

در ایران نیز تبلت عضوی تازه وارد در بازار محسوب IT می شود. اما با توجه به موج فراگیری که در سطح جهان ایجاد شده ایران را نیز تحت تاثیر قرار داده و در آینده ای نه چندان دور می توان استقبال خوبی را از تبلت ها شاهد بود.

ادامه ی مطلب را در سایت فناوری ببینید...

## ۱۳۰۴ پدر هوش مصنوعی درگذشت

زمانی که ابرایانه 'دیپ بلو' در ماه می ۱۹۹۷ موفق شد قهرمان شطرنج جهان گری کاسپاروف را شکست دهد، این پیروزی به عنوان موفقیتی بزرگ برای هوش مصنوعی توصیف شد، اما جان مک کارتی (John McCarthy)، نظری متفاوت داشت، به اعتقاد او هوش مصنوعی هنوز راه طولانی را در پیش داشت.



پدر هوش مصنوعی که در سال ۱۹۵۶ موضوعی به این نام را برای اولین بار در یکی از مقاله هایش مطرح کرده و زبان برنامه نویسی Lisp را ابداع کرده است، در سن ۸۴ سالگی درگذشت.

به گزارش «مهر» زمانی که ابرایانه دیپ بلو در ماه می ۱۹۹۷ موفق شد قهرمان شطرنج جهان گری کاسپاروف را شکست دهد، این پیروزی به عنوان موفقیتی بزرگ برای هوش مصنوعی توصیف شد، اما جان مک کارتی، مردی که این اصطلاح را برای اولین بار خلق کرد و در توسعه هوش مصنوعی پیشگام شد، نظری متفاوت داشت، به اعتقاد او هوش مصنوعی هنوز راه طولانی را در پیش داشت.

وی در سال ۱۹۵۶ نه تنها عبارتی جدید را به واژه نامه عمومی افزود، بلکه بنیانگذار عصری کاملاً جدید از تحقیقات در زمینه علوم رایانه ای شد. وی در سالهای بعدی موفق به ابداع زبان، Lisp یکی از تاثیرگذارترین زبانهای برنامه نویسی رایانه ای در جهان شد و در توسعه سیستمهای اشتراک گذاری زمان نقشی کلیدی ایفا کرد، سیستمی که بدون آن اینترنت مدرن به وجود نمی آمد.

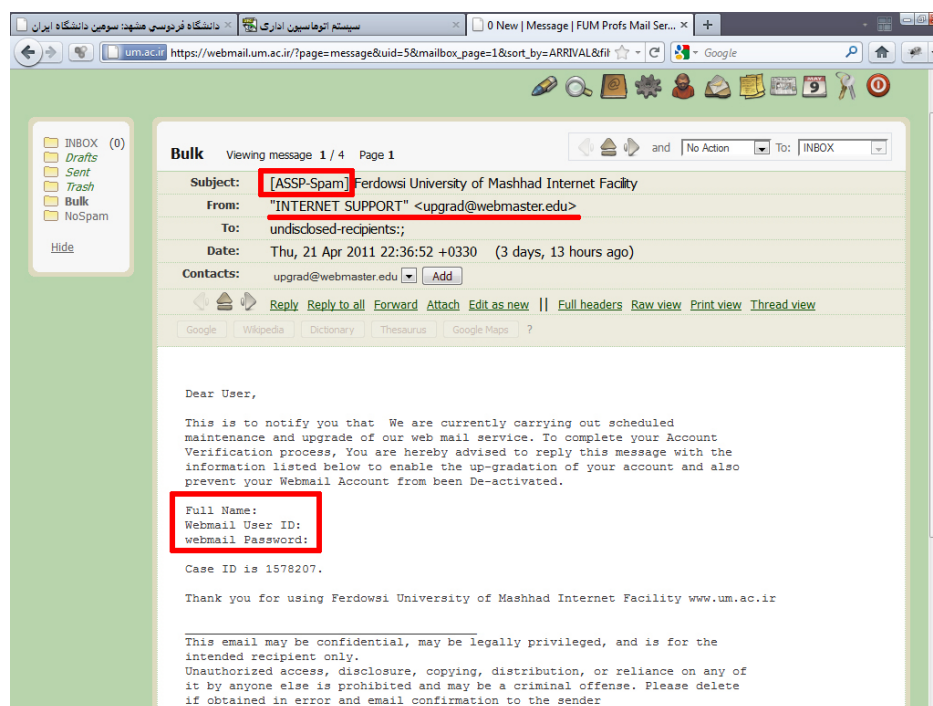
مک کارتی که برای چهار دهه در دانشگاه استنفورد مشغول به کار و مطالعه بود، در سل ۱۹۶۲ لابراتوار هوش مصنوعی استنفورد را پایه گذاری کرد. او در سال ۲۰۰۳ به شرکت گوگل پیوست تا در ساخت خودروهای خودکار این شرکت مشارکت داشته باشد.

بر اساس گزارش وایرد، بسیاری از متخصصان مک کارتی را اولین فردی می دانند که چاشنی محاسبات رایانه ای را به زبان ساده برنامه نویسی افزود و با این کار و ابداع زبان برنامه نویسی Lisp تاثیر بزرگی بر روی زندگی انسانها گذاشت.

<http://www.jamnews.ir/NSite/FullStory/News/?Id=23215>

## ۱۴.۴ هرزنامه‌ها و سرقت هویت

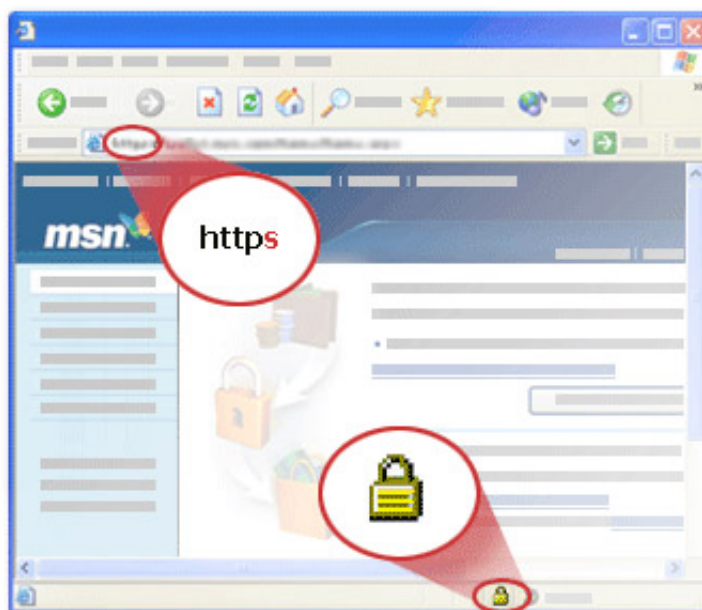
طبق آمار اعلام شده، در سال ۲۰۱۰ بیش از ۱۰۰ میلیون میلیون (۱۰۰ با ۱۲ صفر جلوش) رایانامه ارسال شده است که بیش از ۸۰ درصد آن هرزنامه بوده است. هرزنامه به نامه الکترونیکی ناخواسته گفته می شود که به صورت گروهی و انبوه ارسال می شود. بیشتر هرزنامه‌ها جنبه تبلیغاتی دارند، اما هرزنامه‌هایی نیز وجود دارد که با هدف دریافت اطلاعات شخصی شما طراحی و ارسال می شوند. در این نوع نامه الکترونیکی، نفوذگر سعی می کند در پوشش نهادهایی مانند بانک یا بیمه و یا حتی اداره‌ای که در آن کار می کنید، اطلاعات شخصی و هویتی شما را دریافت کند. به این کار سرقت هویت می گویند. این عمل نفوذگر مانند ماهی گیری است که تور خود را با طعمه‌ای فریبنده پهن کرده است و ماهیان ناشی نیز در دام او می افتند. بهتر است در این زمینه مثال مستندی بزنیم. به تصویر زیر دقت کنید.



متن نامه الکترونیکی را مشاهده می‌کنید که به یکی از کاربران سرویس پست الکترونیک دانشگاه ارسال شده است. در این نامه فرستنده خود را بخش پشتیبانی اینترنت معرفی کرده است و موضوع نامه را نیز تسهیلات اینترنتی دانشگاه فردوسی مشهد انتخاب کرده است. در متن نامه نیز با بیان این که سرویس پست الکترونیک دانشگاه در حال به‌روزرسانی است از کاربر خواسته شده است که نام خود، شناسه کاربری پست الکترونیکی و رمز عبور آن را برای راستی‌آزمایی ارسال نماید و در انتها نیز از این که شما سرویس پست الکترونیکی دانشگاه را انتخاب کرده‌اید، تشکر شده است. این نامه نمونه کامل یک هرزنامه است که با هدف فریب شما و سرقت اطلاعات شخصی شما طراحی و ارسال گردیده است. تجسم کنید که شما فریب آن را می‌خورید و اطلاعات خواسته شده را اعلام می‌کنید. اولین کاری که نفوذگر انجام می‌دهد این است که با این اطلاعات به پست الکترونیکی شما وارد می‌شود و رمز عبور را عوض می‌کند. در این صورت شما دیگر مالک این نشانی الکترونیکی نیستید. سپس به صندوق نامه‌های دریافتی و ارسالی شما مراجعه می‌کند. شما تمامی اطلاعات قبلیتان را ذخیره کرده‌اید از جمله نامه‌های الکترونیکی که در تأیید عضویت شما در وب‌گاه‌های گوناگون ارسال شده است و حاوی شناسه کاربری و رمز عبور شما است. به آن‌ها نیز سر می‌زنند و رمز عبور آن‌ها را نیز تعویض می‌کند. اگر از آن‌دسته افراد باشید که اطلاعات بانکی شامل شماره حساب، رمزهای عبور سامانه بانکداری الکترونیکی و دیگر اطلاعات خود را در پست الکترونیکی ذخیره می‌کنید، پس باید بگوئیم که نفوذگر یک ماهی خاویار صید کرده است! پس تا این جا هویت شما به سرقت رفته است. حالا نوبت سوءاستفاده از این هویت است. نفوذگر نامه الکترونیکی به فهرست نشانی‌های الکترونیکی شما ارسال می‌کند که در آن ذکر شده که شما در یک کشور خارجی هستید و مدارک و پول شما دزدیده شده است و برای این که بتوانید برگردید نیاز به پول دارید و شماره حساب نیز اعلام می‌کند. حالا اگر شخصی از میان کسانی که شما نشانی الکترونیکی او را در فهرستان داشتید

نیز فریب این نامه را بخورد، ماهیان تور نفوذگر همچنان بیشتر می‌شود. این نمونه‌ای از سوءاستفاده احتمالی است و ممکن است مانند این‌ها نیز اتفاق بیافتد. برای جلوگیری از این سوءاستفاده‌ها به نکته‌های زیر توجه کنید:

- ۱- تحت هیچ شرایطی رمز عبور خود را افشا نکنید (آن را در اختیار خانواده، دوست و همکار خود قرار ندهید و همچنین آن را در جایی یادداشت نکنید).
- ۲- از ارسال و نگهداری اطلاعات مهم به صورت نامه الکترونیکی خودداری کنید.
- ۳- نامه‌های الکترونیکی ناشناس را باز نکنید.
- ۴- قبل از این که از صحت پیوندهای ذکر شده در نامه‌های الکترونیکی مطمئن نشدید بر روی آن‌ها کلیک نکنید. همچنین حتماً به جای کلیک مستقیم بر روی آن‌ها سعی کنید نشانی موردنظر را خودتان در مرورگر وب تایپ کنید.
- ۵- از سرویس‌دهندگان معتبری که خدمات پست الکترونیک ارائه می‌دهند، استفاده کنید.
- ۶- اگر از سرویس‌هایی مانند بانکداری الکترونیکی و خرید الکترونیکی استفاده می‌کنید، به‌خاطر داشته باشید که وب‌گاه‌هایی که این خدمات را ارائه می‌دهند از پروتکل‌های امن استفاده کرده باشند که نشانه آن علامت قفل در پائین و **https** در ابتدای نشانی وب‌گاه است.



<http://its.um.ac.ir/Article317.html>

## ۱۵.۴ بدافزار Stuxnet



اخيراً يك بدافزار خطرناك به نام Stuxnet در همه كشورهای جهان و به خصوص

ایران گسترش پیدا کرده است که هدف آن ایجاد اختلال در شرکت ها و سازمان های مرتبط با زیرساخت های حیاتی همچون نیروگاه ها است. بدافزار مذکور با سوءاستفاده از يك حفره امنیتی در ویندوز گسترش پیدا می کند و... به دنبال سیستم هایی است که از نرم افزار WinCC Scada که متعلق به زیمنس است، استفاده می کنند. نرم افزار مذکور معمولاً توسط سازمان های مرتبط با زیرساخت های حیاتی مورد استفاده قرار می گیرد. بنا بر اطلاعات ارائه شده توسط سایمانتک، کرم رایانه ای Scada که هدف آن شرکت ها و سازمان های مربوط زیرساخت های حیاتی هستند، نه تنها به سرقت اطلاعات می پردازد، بلکه يك back door را نیز بر روی سیستم قربانی قرار می دهد تا بتواند از راه دور و به طور مخفیانه کنترل عملیات زیرساخت های مذکور را در اختیار گیرد. کرم Stuxnet، شرکت های مربوط به سیستم های کنترل صنعتی در سراسر جهان را آلوده ساخته است، با این وجود بنا بر گزارش های دریافت شده، بیشتر آلودگی ها در ایران و هند مشاهده شده است.

ابزار رفع بدافزار: stuxnet

ابزار مرکز آپای شریف جهت رفع بدافزار stuxnet

ابزار مرکز آپای امیرکبیر جهت رفع بدافزار stuxnet

اصلاحیه های مایکروسافت:

ms۱۰-۰۴۶

ms۱۰-۰۶۱

ms۱۰-۰۶۷

راهنمایی امنیتی:

راهنما و ابزار رفع بدافزار Stuxnet  
به روز رسانی مایکروسافت برای ویندوز

گزارش تحلیلی:

آیا Stuxnet قویترین بدافزار تاریخ است؟  
گزارش سایمانتک از Stuxnet

اخبار:

سوءاستفاده Stuxnet از چهار آسیب پذیری جدید و اصلاح نشده ویندوز (۲۴ شهریور ۸۹)

برگزاری کارگاه آموزشی مقابله با Stuxnet + فایل های کارگاه آموزشی (۱۶ شهریور ۸۹)

اصلاحیه فوری ویندوز (۱۲ مرداد ۸۹)

اصلاحیه فوری ویندوز در راه است (۹ مرداد ۸۹)

خبر تکمیلی: بدافزار جاسوسی به دنبال سیستم های ایرانی (۲ مرداد ۸۹)

ترمیم کننده خودکار مایکروسافت برای يك آسیب پذیری (۳۱ تیر ۸۹)

بدافزار جاسوسی به دنبال سیستم های ایرانی و هندی (۲۹ تیر ۸۹)

اولین آسیب پذیری ویندوز XP بعد از بازنشستگی (۲۷ تیر ۸۹)

منبع خبر: <http://www.certcc.ir>

## ۱۶.۴ ویروس Duqu بسیار حرفه ای



بنا بر یافته های جدید محققان کاسپرسکی درباره تروجان Duqu، نویسندگان این ویروس حداقل چهار سال برای ایجاد کد حمله تروجان مذکور وقت گذاشته اند. با توجه به اطلاعات بررسی شده در نمونه های جدید این ویروس که ...

توسط محققان سودانی در اختیار کاسپرسکی قرار گرفته، کد حمله آن در آگوست سال ۲۰۰۷ اجرا شده است. بنا بر گفته های یکی از محققان ارشد کاسپرسکی به نام Schouwenberg نمی توان ۱۰۰ درصد از تاریخ مذکور مطمئن بود ولی شواهد دیگری نیز وجود دارد که صحت این تاریخ را تقویت می کند. همچنین، درایوری که در آگوست ۲۰۰۷ اجرا شده، مشخصاً برای ویروس Duqu طراحی شده است، زیرا این درایور را در هیچ جای دیگری نمی توان پیدا کرد.

مایکروسافت تأیید کرده است که این ویروس از يك آسیب پذیری در هسته ویندوز و موتور تجزیه فونت سوءاستفاده کرده است تا بتواند حق دسترسی لازم برای نصب کردن بدافزار بر روی رایانه قربانی را پیدا کند. هنوز اصلاحیه ای برای آسیب پذیری مزبور منتشر نشده است، اما مایکروسافت به کاربران پیشنهاد کرده است تا تجزیه کننده فونت (Font Parser) را موقتاً غیر فعال سازند تا زمانی که اصلاحیه ای در رابطه با این نقص امنیتی منتشر شود.



یکی دیگر از یافته های مهم کاسپرسکی در مورد این ویروس نشان دهنده اینست که ویروس مذکور برای هر حمله هدفدار خود، کد حمله را مناسب با هدف مزبور دستکاری کرده و همچنین برای هر حمله از یک سرور جدید کنترل و فرمان C&C که آدرس آن در فایل های ویروس مخفی شده است، استفاده می کند.

بنا بر گفته های محققان کاسپرسکی، نویسندگان این ویروس، بسیار حرفه ای عمل می کنند و این قضیه احتمال این را که گروه یکسانی در پشت صحنه این تروجان جدید و ویروس مشهور استاکس نت باشند، تقویت می کند.

منبع خبر: <http://www.certcc.ir/index.php?name=news&file=article&sid=1506>

## ۱۷.۴ ۱۰ نکته که باید درباره LED بدانید

بازار تلویزیون در سال های اخیر شاهد عرضه و معرفی تنوع گسترده ای از محصولات با فناوری ها و ویژگی های بسیار متفاوت بوده است. این وضعیت باعث شده تا خریداران برای تصمیم گیری درباره محصول مورد نظر خود با تردیدها و سردرگمی های زیادی مواجه باشند. از سوی دیگر، مدتی است که ورود یک نام جدید به این تردیدها دامن زده و باعث شده که انتخاب حتی در بین تلویزیون های مبتنی بر یک فناوری پایه یعنی LCD نیز چندان ساده نباشد. همانند هر فناوری دیگری، بازار محصولات صوتی و تصویری از انبوه شایعات و اظهار نظرهای غیرواقعی (مثبت و منفی) درباره LED پر شده است و همین موضوع باعث شد تا ما تصمیم بگیریم مهم ترین واقعیت های مربوط به فناوری مذکور را در قالب این مقاله در اختیار شما قرار دهیم. این واقعیت ها در قالب ده نکته فنی مطرح شده اند که در ادامه خواهید خواند.

### یک تلویزیون، LED نوع جدیدی از تلویزیون محسوب نمی شود

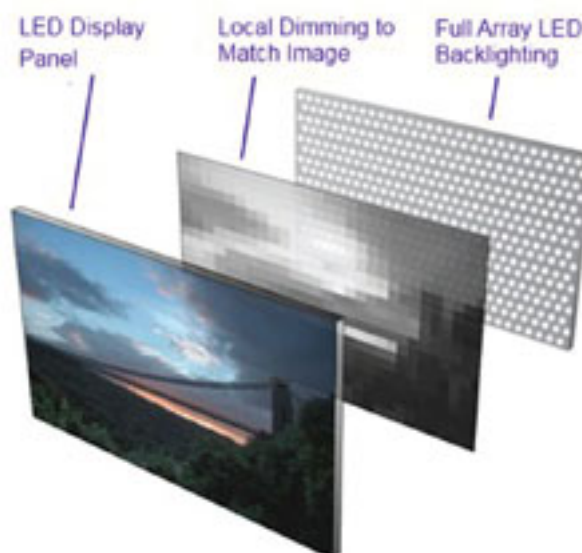
ممکن است صحبت ها یا ادعاهای اغراق آمیز زیادی را در این مورد شنیده باشید، اما یک تلویزیون LED تنها یک مدل LCD است که از نور پشته LED بهره می گیرد، نه نور فلورسنت کاتد سرد یا CCFL استاندارد. از سوی دیگر با وجود آن که تلاش های تبلیغاتی تولیدکنندگان در یکی دو سال اخیر تا حدود زیادی بازار این محصولات را داغ کرده، اما واقعیت این است که تلویزیون های LCD با نور پشته LED از سال ۲۰۰۷ به بازار راه پیدا کرده اند. برخلاف پلاسما و OLED که فناوری های تابنده (Emmisive) محسوب می شوند و در آن ها هر پیکسل دارای منبع نوری جداگانه مخصوص به خود است، LCD یک فناوری انتقال دهنده (Transmissive) محسوب می شود که در آن هر پیکسل باید از پشت روشن شود.

### دو نوع پیکربندی نور پشته LED وجود دارد

در ابتدا، نمایشگرهای مبتنی بر نور پشته LED با یک آرایه کامل از LEDها در پشت LCD روشن می شدند، درست مانند نور پشته CCFL استاندارد. اما برای ایجاد تلویزیون های باریک تر، مهندسين مجبور بودند این لایه اضافی از LEDها را حذف کرده و آن ها را به کناره های صفحه نمایش انتقال دهند. با این شکل ایجاد نور پشته، LEDها در چهار طرف صفحه نمایش تعبیه شده و نور خود را با استفاده از Lightguide به سمت داخل و مرکز آن می تاباندند. این نوع تلویزیون ها عموماً تحت عنوان Edge-lit شناخته می شوند و در حال حاضر متداول ترین مدل موجود به شمار می آیند.

### Local-dimming در هر يك از این پیکربندی‌ها وجود دارد

تمام‌های LCD مبتنی بر LED فعلی که يك آرایه کامل از LED را به‌عنوان نور پشتی به خدمت می‌گیرند، به فناوری خاصی تحت عنوان تاریک‌سازی منطقه‌ای یا Local-dimming مجهز هستند که در آن بخش‌هایی از نور پشتی می‌توانند به‌طور مستقل تاریک‌تر یا روشن‌تر شوند. این تغییرات بر حسب این که نواحی مختلف تصویر تاریک‌تر یا روشن‌تر می‌شوند، صورت می‌گیرند. توانایی تاریک کردن بخش‌هایی از صفحه نمایش به کاهش مقدار نوری که از طریق پیکسل‌های تاریک شده نشت می‌کند، کمک کرده و نتیجه نهایی آن نواحی سیاهی هستند که تاریک‌تر و واقعی‌تر به نظر می‌رسند. از آنجایی که سطوح سیاه در تعیین نسبت کنتراست صفحه نمایش نقش حیاتی دارند، هر چه رنگ سیاه ایجاد شده عمیق‌تر باشد رنگ‌ها برجسته‌تر خواهند بود. همچنین، کل تصویر زنده‌تر به نظر می‌رسد.



یکی از معایب تاریک‌سازی منطقه‌ای، تاثیری است که تحت عنوان Blooming شناخته می‌شود و در آن نواحی روشن‌تر به قسمت‌های تاریک‌تر نفوذ کرده و سطوح سیاه مجاور خود را روشن می‌کنند. این تاثیر Blooming تا حدود زیادی در بین مدل‌های مختلف متفاوت است. وقوع Blooming به‌طور مستقیم با تعداد عناصر LED تاریک‌سازی منطقه‌ای یا مناطق قابل تاریک‌سازی پشت صفحه نمایش ارتباط دارد، اما بعضی از تولیدکنندگان این اطلاعات را به‌درستی منتشر نمی‌کنند. با نور پشتی CCFL استاندارد و اکثر مدل‌های مجهز به نور پشتی Edge-lit، LED کل نور پشتی به‌طور يك جا روشن یا تاریک می‌شود. با این حال، بعضی از تلویزیون‌های جدیدتر این گروه می‌توانند روش مشابهی از تاریک‌سازی منطقه‌ای را با يك پیکربندی Edge-lit پیاده‌سازی کنند. سامسونگ این فناوری را تحت عنوان تاریک‌سازی دقیق معرفی می‌کند تا به ایجاد تمایز بین آن و تاریک‌سازی منطقه‌ای واقعی کمک کرده باشد. در تلویزیون‌های LG نیز این تکنیک را تحت عنوان LED Plus خواهید یافت.

### تلویزیون‌های Edge-lit واقعا باریک هستند، اما مشکل یکنواختی دارند

همان‌طور که اشاره کردیم، مزیت اصلی يك الگوی نور پشتی Edge-lit، LED این است که تولیدکنندگان می‌توانند تلویزیون‌های باریک‌تری بسازند. با این حال، روش مذکور با این مشکل مواجه

است که نور پشتی به اندازه یک آرایه کامل از LED در پشت صفحه نمایش یکنواخت نخواهد بود. در نمایشگرهای Edge-lit، اگر یک تصویر سفید را نمایش دهید متوجه خواهید شد که حاشیه‌های خارجی صفحه نمایش روشن‌تر هستند. همچنین وقتی که یک تصویر کاملاً سیاه را نمایش می‌دهد، حاشیه‌های تصویر تا حدودی خاکستری دیده می‌شوند.

### نور پشتی LED از هر نوعی که باشد زاویه دید LCD را بهبود نمی‌بخشد

برخلاف پلاسما، یکی از معایب تلویزیون‌های LCD این است که اگر با زاویه به صفحه نمایش آن‌ها نگاه کنید، تصویر آن‌ها دچار تحریف می‌شود. نور پشتی LED هیچ تاثیری بر این وضعیت ندارد و در بعضی از موارد حتی می‌تواند آن را تشدید کند.

### بازدهی نور پشتی LED از نور پشتی فلورسنت استاندارد بالاتر است

هیچ تردیدی وجود ندارد که استفاده از نور پشتی LED می‌تواند مصرف برق تلویزیون را کاهش دهد و بعضی از LCDهای مجهز به نور پشتی LED برای هر اینچ از سطح صفحه نمایش خود بالاترین بازدهی انرژی را در بین تمام مدل‌های موجود تلویزیون‌ها آرایه می‌کنند. یک مطالعه در سال ۲۰۰۸ نشان داده بود که تلویزیون‌های LED به‌طور متوسط ۱۰۱ وات برق مصرف می‌کنند، در حالی که این میزان برای تلویزیون‌های LCD استاندارد معادل ۱۱۱ وات است. البته اندازه صفحه نمایش و روشنایی تصویر نیز می‌تواند تاثیر قابل توجهی بر میزان مصرف برق داشته باشند. از سوی دیگر، باید توجه داشته باشید که هر دو نوع تلویزیون‌های LCD مذکور به‌طور قابل ملاحظه‌ای کم‌مصرف‌تر از تلویزیون‌های پلاسما هستند.

### نور پشتی LED در حال بهبود است، اما تا کجا می‌تواند بهتر شود

این یک واقعیت است که الگوهای نور پشتی تولیدکنندگان با گذشت زمان همچنان در حال بهبود هستند، اما پیشرفت‌های واقعی بیشتر در حوزه فناوری Edge-lit خواهند بود. مهندسين تلاش می‌کنند تا نور پشتی Edge-lit را بهبود بخشند تا بتواند به سطحی معادل آرایه کامل LED رسیده و حتی از آن نیز پیشی بگیرد. یکی از مشکلات نور پشتی Full-Array این است که برای دستیابی به بهترین شرایط به ۱/۲ میلیون LED نیاز دارد تا به‌طور جداگانه ۲،۱ میلیون پیکسل را در یک تلویزیون ۱۰۸۰p روشن کند. اضافه کردن این تعداد LED به هیچ‌وجه مقرون به صرفه نخواهد بود. با این حال، مهندسين تلاش می‌کنند تعداد LED قابل تعبیه در پنل‌ها را تا حد امکان افزایش دهند، بدون آن‌که محصولات نهایی به‌طور غیرقابل توجهی گران باشند.

### LED به معنای قیمت بالاتر است

به‌طور طبیعی، تلویزیون‌های مجهز به نور پشتی LED گران‌تر از سایر مدل‌های LCD هستند. این موضوع باعث می‌شود که موضوع مصرف پایین‌تر این تلویزیون‌ها و در نتیجه کاهش هزینه‌های برق شما چندان چشمگیر به نظر نرسد. زیرا شما از ابتدا هزینه بالاتری را برای تلویزیونی با کیفیت تصویری تقریباً یکسان پرداخت کرده‌اید. با گذشت زمان و کاهش قیمت این مدل‌ها، وضعیت کلی تغییر خواهد کرد.

### مدل‌های برتر تلویزیون‌های LED کیفیت تصویری نزدیک به پلاسما را آرایه می‌کنند

تلویزیون‌های LCD مدت‌ها به‌خاطر ناتوانی در تولید سطوح سیاه عمیق مورد حمله تلویزیون‌های پلاسما قرار گرفته‌اند. با معرفی نور پشتی LED به همراه تاریک‌سازی منطقه‌ای، سطوح سیاه روی بهترین تلویزیون‌های LED می‌تواند معادل سطوح سیاه روی بعضی از بهترین مدل‌های پلاسما باشد

و تصویر فوق‌العاده‌ای را ارائه کنند. از سوی دیگر، تلویزیون‌های دارای نور پشتی LED از بازدهی انرژی بسیار بهتری نسبت به تلویزیون‌های پلاسما برخوردار بوده و سبک‌تر نیز هستند. با این حال تحریف تصویر در زوایای دید باز هنوز به قوت خود باقی مانده است در حالی که تلویزیون‌های پلاسما با چنین مشکلی مواجه نیستند. از سوی دیگر، ما با بهبود چندانی در کیفیت تصویر مدل‌های مبتنی بر Edge-lit LED مواجه نیستیم. در بعضی از موارد، تلویزیون‌های LED حتی کیفیت تصویری پایین‌تری را نسبت به همکاران مبتنی بر CCFL خود ارائه می‌کنند. مثل همیشه، عملکرد این تلویزیون‌ها تا حدود زیادی در بین مدل‌های مختلف متغیر است اما نباید وجود نور پشتی LED را به‌عنوان تصویر بهتر تلویزیون تفسیر کنید.

**اگر تنظیمات تصویری صحیح نباشند، تفاوتی بین LED و سایر مدل‌ها وجود ندارد**  
شما می‌توانید بهترین HDTV جهان را با آخرین و بی‌نقص‌ترین فناوری داشته باشید، اما اگر آن را به‌طور صحیح راه‌اندازی و تنظیم نکنید، کیفیت تصویر نهایی تلویزیون هیچ تفاوتی با سایر مدل‌ها نخواهد داشت. بنابراین همان‌طور که می‌بینید کار شما با خرید یک تلویزیون جدید به پایان نمی‌رسد، بلکه باید استقرار و تنظیمات تلویزیون را نیز به‌طور صحیح انجام دهید.  
گرفته شده از پایگاه اطلاع‌رسانی ماهنامه شبکه

## ۱۸.۴ کنفرانس RSA: مدیریت خطرات حوزه فناوری اطلاعات

دبیر کنفرانس RSA در نطق افتتاحیه خود بر این نکته تأکید کرد که خطرات حوزه فناوری اطلاعات با تصمیمات صحیح متخصصان این حوزه می‌تواند به درستی مدیریت گردد.



کنفرانس RSA با یک سخنرانی در مورد بررسی چگونگی تغییرات وضعیت جهان در ۱۲ ماه

گذشته کار خود را آغاز کرد. این در حالی است که وضعیت شرکت RSA در ۱۲ ماه گذشته چندان جالب نبوده و از حملاتی رنج برده است که منجر به افشای اطلاعات شرکت مزبور شده است. دبیر کنفرانس RSA ، آقای Coveillo در نطق افتتاحیه خود خاطرنشان ساخت که خطر يك واقعیت دنیای امروز است و این موضوع منحصر به دنیای فناوری اطلاعات نمی شود. بنا بر گفته های وی، خطرات مزبور می تواند از طریق تصمیمات صحیح متخصصان این حوزه به طور قابل توجهی کاهش پیدا کند. وی همچنین توضیح داد، صحیح است که اینترنت خطراتی را به همراه دارد، اما صنعت امنیت IT توانسته است، اینترنت را به اندازه کافی برای نقل و انتقالات بین المللی امن سازد. وی ادامه داد البته این امنیت روز به روز بیشتر در معرض حملات مختلف قرار می گیرد و اعتماد محض به این امنیت يك اشتباه فاحش است.

<http://www.certcc.ir/index.php?name=news&file=article&sid=1722>

## ۱۹۰۴ بدافزارهای دسترسی از راه دور، يك تهديد جدی علیه کاربران تلفن همراه

در کنفرانس RSA سال ۲۰۱۲، مدیر اجرایی مك کافی، جورج کرتز و دیمیتری آلپروویچ يك ابزار دسترسی از راه دور را بر روی يك گوشی آندورید ۲.۲ نصب کردند. این عمل با استفاده از يك رخنه اصلاح نشده در WebKit ، مرورگر پیش فرض در سیستم عامل صورت گرفته است. محققان امنیتی اظهار داشتند بدافزارهایی که به مهاجمان اجازه می دهد تا از راه دور دسترسی کامل تلفن های هوشمند را بدست بیاورند به يك تهديد جدی برای کاربران سراسر دنیا تبدیل شده است.

در کنفرانس RSA سال ۲۰۱۲، مدیر اجرایی مك کافی، جورج کرتز و دیمیتری آلپروویچ يك ابزار دسترسی از راه دور را بر روی يك گوشی آندورید ۲.۲ نصب کردند. این عمل با استفاده از يك رخنه اصلاح نشده در WebKit ، مرورگر پیش فرض در سیستم عامل صورت گرفته است. محققان به حاضران نشان دادند که چگونه این بدافزار، از طریق يك پیام کوتاه می تواند بر روی تلفن هوشمند نصب شود و پس از آن برای رهگیری و ضبط مکالمات، ضبط ویدئو، سرقت پیام های متنی، ردگیری شماره هایی که با آن ها تماس گرفته شده و محل دقیق موقعیت جغرافیایی کاربری که در حال تماس است، مورد استفاده قرار بگیرد.

کورتز اشاره کرد که ابزار مورد استفاده در این حمله به راحتی از منابع موجود بدست آمده است. تروجان دسترسی از راه دور استفاده شده در این حمله نسخه تغییر یافته ی Nickispy ، ابزار معروف بدافزار چینی است. مساله کلیدی آن است که حملات مشابه علیه هر تلفن هوشمندی دیگری نیز ممکن است صورت بگیرد.

به عنوان مثال WebKit به عنوان مرورگر پیش فرض سیستم عامل های تلفن همراه به طور گسترده استفاده می شود از جمله در iOS اپل، سیستم عامل تبلت بلک بری، مرورگرهای سافاری اپل و کروم گوگل.

کورتز گفت: در این حمله يك پیام کوتاه که به نظر می رسد از يك ارائه دهنده خدمات بی سیم ارسال شده است برای کاربر فرستاده شد و از کاربر تقاضا کرد تا يك به روز رسانی مهم را نصب نماید. کاربر با کلیک کردن بر روی این لینک باعث شد تا تروجان بر روی تلفن همراه دانلود شود.

بنابراین، کاربران تلفن همراه باید مطمئن شوند که تمامی اصلاحیه های مرتبط با سیستم عامل تلفن همراه خود را نصب کرده اند و توجه داشته باشند که چه مواردی را دانلود می نمایند و نسبت به حملات فیشینگ تلفن همراه آگاه باشند.

<http://www.certcc.ir/index.php?name=news&file=article&sid=1723>

## ۲۰.۴ هشدار به کاربران اینترنت

۳۷ درصد کاربران، اینترنت را با استفاده از نسخه های ناامن جاوا مرور می کنند. در يك بازه زمانی سه ماهه، محققان CSIS به بررسی و نظارت ۵۰ ابزار سوءاستفاده متفاوت بر روی ۴۴ سرور یکتا پرداختند. آنها در نتیجه تحقیق مذکور دریافتند که ۳۱.۳ درصد آلودگی ها به علت عدم نصب اصلاحیه های امنیتی اتفاق افتاده است. در واقع کاربرانی بیشتر در معرض خطر بوده اند که از نسخه های قدیمی تر برنامه های کاربردی و افزونه های مرورگرها استفاده می کرده اند. در بین نرم افزارهای مورد استفاده کاربران اینترنت، جاوا JRE، ۳۷ درصد بیشترین برنامه های کاربردی آسیب پذیر را به خود اختصاص داده است و پس از آن Adobe Reader/Acrobat با ۳۲ درصد و Adobe Flash با ۱۶ درصد قرار دارند.

کارشناسان امنیتی به کاربران هشدار می دهند که نه تنها از يك آنتی ویروس خوب استفاده کنند بلکه به صورت مرتب و مداوم برای نصب اصلاحیه های امنیتی سیستم عامل و نرم افزارهای کاربردی خود اقدام نمایند.

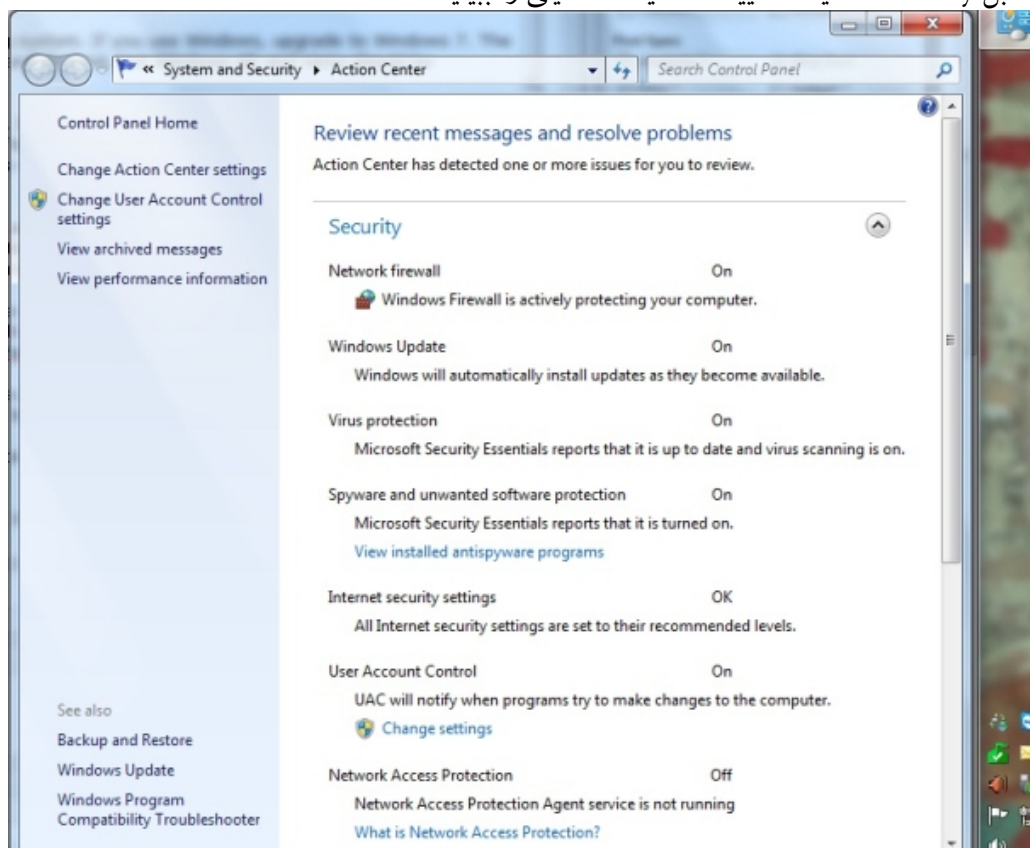
<http://www.certcc.ir/index.php?name=news&file=article&sid=1446>

## ۲۱.۴ پیشگیری از دانلود بدافزارها و تبلیغ افزارها

هر روز مجرمان کامپیوتری راه های جدیدی را برای فریب دادن ما پیدا می کنند تا ویروس ها، نرم افزارهای ثبت کننده ضربات صفحه کلید، تبلیغ افزارها و نرم افزارهای دیگری که برای سرقت اطلاعات شخصی، جاسوسی یا آزدن ما در نظر گرفته شده اند، دانلود کنیم. اما پیشگیری از دانلود بدافزار نباید چندان پیچیده باشد. چند احتیاط ساده می تواند کامپیوتر ما را عاری از آلودگی نگه دارد. آخرین نسخه از نرم افزارهایی که استفاده می کنید را دریافت نمایید امنیت کامپیوتر با سیستم عامل شروع شده و پایان می یابد. اگر شما از سیستم عامل ویندوز استفاده می کنید، آن را به ویندوز ۷ ارتقاء دهید. قانون ارتقاء به آخرین نسخه برای نسخه های قدیمی تر سیستم عامل های Mac OS X، لینوکس و اندروید سختگیری کمتری دارد، اما ویندوز xp و ویندوز ویستا باید ممنوع در نظر گرفته شوند. در مرحله بعد، اطمینان حاصل کنید که نرم افزارها به طور خودکار به روز رسانی می شوند. در گذشته توصیه می شد که به روز رسانی های ویندوز به طور خودکار دانلود شوند، اما بهتر است ابتدا بررسی گردد که خود این به روز رسانی ها باعث ایجاد مشکل نمی شوند، سپس به صورت دستی نصب گردند. شانس صدمه زدن به کامپیوتر شما توسط به روز رسانی ویندوز به مراتب کمتر از توانایی بالقوه يك آلودگی به دلیل عدم اعمال يك به روز رسانی امنیتی مهم است. زمانی به روز رسانی های خودکار آزاردهنده است که پس از اعمال آن ها به راه اندازی مجدد نیاز باشد و در کار شما وقفه ایجاد

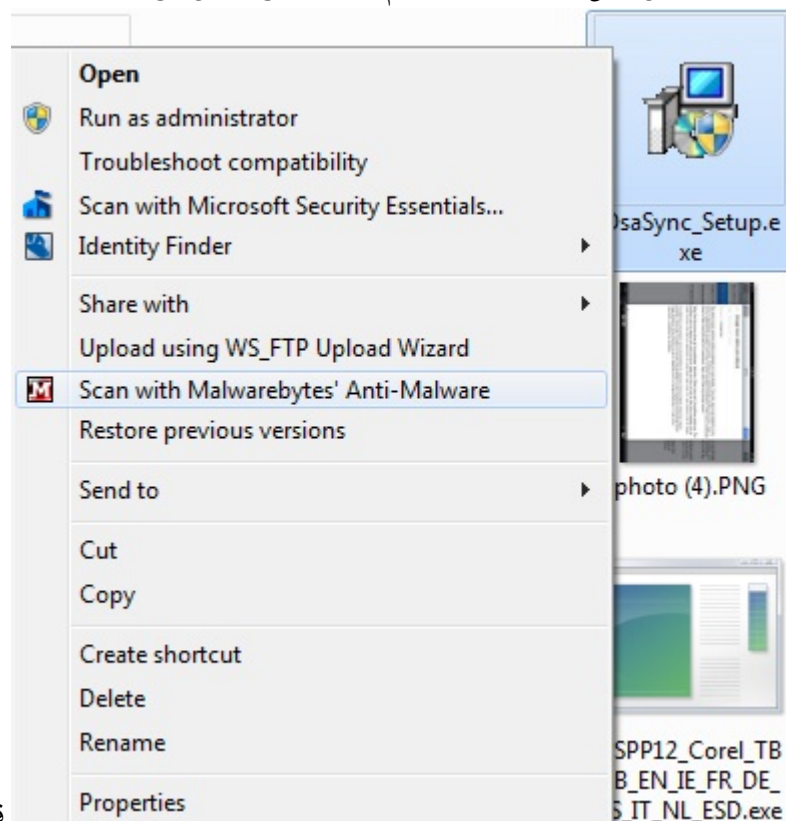


کنند، اما این زمان‌های برنامه ریزی نشده قطعاً هزینه کمتری نسبت به پرداخت هزینه برای بازیابی ایمنی سیستم دارند. بررسی این موضوع که ویندوز و نرم افزارهای امنیتی به روز هستند یا خیر، بسیار راحت است. کافی است نگاهی به نواحی اخطار بیاندازید و آیکون‌هایی را که تیک قرمز دارند و یک مشکل را نشان می‌دهند، مشاهده کنید. برای بررسی تنظیمات امنیتی در ویندوز ۷، بر روی آیکون پرچم در ناحیه اخطار کلیک کنید و گزینه Open Action Center را انتخاب نمایید. بر روی فلش مقابل Security کلیک کنید تا تنظیمات امنیتی را ببینید.



در ویندوز ۷، گزینه Action center، تنظیمات امنیتی جاری سیستم شامل فایروال، به روز رسانی‌های ویندوز، آنتی ویروس و حفاظت در برابر جاسوس افزار را نشان می‌دهد. مراقب ایمیل های سرقت هویت باشید در پیام‌های دریافتی، بر روی لینک‌ها و دانلود فایل پیوست کلیک نکنید، مگر آن‌که منتظر دریافت آن‌ها باشید. این امر را حتی برای پیام‌هایی که به نظر می‌رسند از طرف شخصی است که وی را می‌شناسید و به او اعتماد دارید، در نظر بگیرید. سارقان هویت اغلب دسترسی به لیست-های تماس افراد را بدست می‌آورند و از طرف حساب‌های به سرقت رفته، پیام‌هایی به همراه لینک‌ها و پیوست-های مخرب ارسال می‌کنند. اگر فکر می‌کنید که حساب ایمیل شما هک شده است، با استفاده از یک برنامه ضد بدافزار دیگر به غیر از برنامه ای که برای حفاظت دائمی سیستم از آن استفاده می‌کنید، یک اسکن کامل بر روی سیستم انجام دهید. به عنوان یک پیشنهاد می‌توانید از ضد بدافزار رایگان Malwarebytes استفاده کنید. پس از آن که اطمینان حاصل شد ماشین شما عاری از بدافزار است، رمز عبور حساب ایمیل خود را تغییر دهید. مواظب دانلودهای پنهان

باشید هر کسی که به طور منظم از کامپیوتر شخصی استفاده می‌کند، می‌داند که هشدارها و اعلام خطرها غالباً به صورت پاپ‌آپ‌های غیرمنتظره هستند. حتی با وجود مسدود کننده‌های پاپ‌آپ در مرورگرها، باز هم با پنجره‌های ناخواسته‌ای که ما را به سایت‌های مختلف هدایت می‌کنند مواجه می‌شویم. بسیاری از ما به سادگی بر روی هر دکمه‌ای که ظاهر می‌شود کلیک می‌کنیم تا پاپ‌آپ‌ها را ببندیم و بعد از آن به کار خود بازگردیم. تولیدکنندگان بدافزار بر این امر تکیه می‌کنند که افراد ابتدا بر روی یک لینک کلیک می‌کنند و سپس در مورد آن فکر می‌کنند. حتی سایت‌های به ظاهر معتبر ممکن است بازدیدکنندگان را برای کلیک بر روی لینک‌های دانلود مخرب فریب دهند. یک راه برای اطمینان از این که تنها نرم‌افزاری را که می‌خواهید و به آن احتیاج دارید، دانلود می‌کنید، این است که آن نرم‌افزار را از مبدا اولیه یا از سایت‌هایی که نزدیک به مبدا اولیه است، دانلود نمایید. نرم‌افزار امنیتی شما باید تمامی فایل‌هایی را که دانلود می‌کنید به طور خودکار اسکن کند، اما قبل از کلیک کردن برای بازکردن یک فایل یا نصب یک برنامه، توجه بیشتری داشته باشید، فولدر مورد نظر را باز کنید (فولدری که آن را دانلود کرده‌اید)، بر روی فایل اجرایی آن کلیک راست کنید، و گزینه‌ای را انتخاب کنید که این فایل را با استفاده از نرم‌افزار امنیتی اسکن می‌کند.



قبل از بازکردن یک

فایل دانلود شده یا نصب یک برنامه، فایل را با استفاده از نرم‌افزار امنیتی موجود در کامپیوتر شخصی خود اسکن کنید. گاهی اوقات بی‌خطرترین راه آن است که هنگامی که یک پنجره پاپ‌آپ به طور غیرمنتظره باز شد، بر روی آن کلیک نکنید. برای بستن پنجره‌های پاپ‌آپ، بدون کلیک کردن باید کلیدهای **Ctrl+F4** را فشار دهید. برای ایمنی بیشتر در برخورد با یک بدافزار بالقوه، برای بستن مرورگر خود کلیدهای **Alt+F4** را فشار دهید. اگر مجبور شدید، تمامی سربرگ‌ها را ببندید و آن‌ها



را ذخیره نکنید تا از بازشدن مجدد آن‌ها، زمانی که مرورگر را راه اندازی مجدد می‌کنید، جلوگیری کنید. یک برنامه حتی زمانی که مطمئن به نظر می‌رسد، پس از شروع به استفاده می‌تواند به یک برنامه مخرب تبدیل شود. به همین دلیل بهتر است تا زمانی که مطمئن شوید می‌خواهید آن برنامه را نگه دارید، اطلاعات شخصی بیشتر از آنچه نیاز است را ارائه نداده و ثبت نکنید. اگر احتمال می‌دهید که از یک برنامه کاربردی رایگان دیگر استفاده نخواهید کرد، پس از استفاده آن را از روی سیستم حذف نمایید. شما همیشه می‌توانید جدیدترین نسخه یک نرم افزار را، وقتی که می‌خواهید دوباره از آن برنامه استفاده کنید، دانلود نمایید. این کار رویکرد بهتری در مقایسه با استفاده از یک نسخه غیر امن و تاریخ گذشته است.

<http://www.certcc.ir>

## ۲۲.۴ بدترین پسوردهای جهان



**Password** انتخاب یک پسورد مناسب یکی از ضرورت های استفاده از خدمات آنلاین امروزی است و سهل انگاری در این زمینه می تواند در برخی از موارد خسارات سنگینی به بار بیاورد. با توجه به اهمیت این موضوع موسسه اسپلش دیتا (SplashData) به انتشار ۲۵ پسورد اقدام کرده است که به اعتقاد این موسسه بدترین پسوردهای جهان هستند و بیش از هر پسورد دیگری مورد حمله هکرها قرار گرفته اند...

انتخاب یک پسورد مناسب یکی از ضرورت های استفاده از خدمات آنلاین امروزی است و سهل انگاری در این زمینه می تواند در برخی از موارد خسارات سنگینی به بار بیاورد. با توجه به اهمیت این موضوع موسسه اسپلش دیتا (SplashData) به انتشار ۲۵ پسورد اقدام کرده است که به اعتقاد این موسسه بدترین پسوردهای جهان هستند و بیش از هر پسورد دیگری مورد حمله هکرها قرار گرفته اند...

رتبه نخست بدترین پسوردهای جهان به خود واژه پسورد (password) اختصاص دارد و اگر فردی چنین پسوردی را برای حساب های کاربری خود انتخاب کند، هکرها به راحتی می توانند به اطلاعات وی دسترسی پیدا کنند.

اسپلش دیتا لیست زیر را بر اساس میلیون ها پسوردی تهیه کرده است که توسط هکرها دزدیده شده اند:

- ۱ - password
- ۲ - ۱۲۳۴۵۶
- ۳ - ۱۲۳۴۵۶۷۸
- ۴ - qwerty
- ۵ - abc۱۲۳

- 6 - monkey
- 7 - ۱۲۳۴۵۶۷
- 8 - letmein
- 9 - trustno۱
- 10 - dragon
- 11 - baseball
- 12 - ۱۱۱۱۱۱
- 13 - iloveyou
- 14 - master
- 15 - sunshine
- 16 - ashley
- 17 - bailey
- 18 - passw•rd
- 19 - shadow
- 20 - ۱۲۳۱۲۳
- 21 - ۶۵۴۳۲۱
- 22 - superman
- 23 - qazwsx
- 24 - michael
- 25 - football

## ۲۳.۴ یک هکر چگونه رمز عبور شما را هک می کند؟

فکر می کنید اگر یک هکر قصد نفوذ به اکانت شما را داشته باشد، با چند بار سعی و خطا موفق خواهد شد؟ این لیست ده مورد از اولین احتمالات یک هکر برای کشف رمز عبور شما است که البته پیدا کردن این اطلاعات هم بسیار ساده تر از آن چیزی است که تصور می کنید:

- ۱ - اسم پدر، مادر، همسر، فرزند و یا حیوان خانگی شما اولین موردی است که امتحان می شود. البته همیشه عدد ۰ یا ۱ را هم بعد از آن باید امتحان کرد. زیرا بسیاری از سایت ها از شما می خواهند که از عدد هم در رمز عبورتان استفاده کنید.
- ۲ - چهار رقم آخر شماره موبایل و یا کد ملی تان
- ۳ - ۱۲۳ یا ۱۲۳۴ یا ۱۲۳۴۵۶
- ۴ - کلمه password
- ۵ - شهر محل اقامت یا دانشگاهی که در آن تحصیل می کنید و یا اسم تیم فوتبال محبوب تان
- ۶ - روز تولد خود، والدین و یا فرزندان تان
- ۷ - کلمه god
- ۸ - هدف بزرگ شما در زندگی
- ۹ - کلمه money
- ۱۰ - کلمه love

هکرها به دور از هر گونه اصول اخلاقی برای بدست آوردن اطلاعات مورد نظرشان از هر ابزاری استفاده می کنند. تنها مرز و سد نگه دارنده بین فاش شدن و محرمانه ماندن اطلاعات تان رمزعبوری است که انتخاب می کنید و به شما بستگی دارد که این حصار را تا چه اندازه قدرتمند بسازید.

یکی از ساده ترین راه های نفوذ، استفاده از روشی به نام Brute Force attack است. در این روش هکر با استفاده از نرم افزارهایی که در دسترس همه قرار دارند و شما هم می توانید با مراجعه به وب سایت insecure.org یک لیست ده تایی از نمونه های رایگان آن را ببینید به اکانت شما نفوذ می کند.

- چگونه ممکن است که کسی بتواند اکانت من را هک کند و به رمزعبورم دست پیدا کند؟ شیوه کار من به عنوان یک هکر می تواند این باشد:

- احتمالاً از یک رمزعبور مشترک برای اکانت های زیادی استفاده می کنید! این طور نیست؟ برخی از وب سایت ها مانند سایت بانکی تان و یا VPN اتصال به اداره تان معمولاً از امنیت قابل قبولی برخوردارند. پس هکر خبره ای مانند من اصلاً وقت خود را برای آن تلف نمی کند. - به هر حال وب سایت های دیگری مانند فروم ها، سایت های ارسال کارت تبریک و سیستم های خرید آنلاین وجود دارند، که شما همیشه به آن ها مراجعه می کنید و خوشبختانه آن ها از امنیت پایین تری برخوردارند، بنابراین من آن ها را برای شروع انتخاب می کنم.

- الان وقت آن است که برنامه هایی از قبیل Brutus یا Wwwhack و The Hydra را از بند آزاد کنم. این برنامه ها در مدت زمان بسیار کوتاهی ۱۰ تا ۱۰۰ هزار نام کاربری و رمز عبور مختلف را با استفاده از دستور عملی که من در اختیارشان قرار داده ام، می سازند.

- چیزی که من تا اینجا به دست آورده ام تعداد زیادی نام کاربری و رمزعبور طبق الگوی ۱۰ گانه بالا است که می توانم بر روی سایت های هدف امتحان کنم.

- دست نگه دارید .... من از کجا بدانم که حساب شما در کدام بانک است و نام کاربری تان چیست؟ یا اینکه سایت هایی را که مرتباً با رمزعبور بازدید می کنید، چه هستند؟ تمام این وب سایت ها، کوکی هایی را بر روی حافظه مرورگر تان بر جای می گذارند که رمزنگاری نیستند و اطلاعات لازم را در اختیار من قرار می دهند. فقط لازم است به این شیرینی های (کوکی) خوشمزه دست پیدا کنم!

سؤال مهمی که در اینجا مطرح می شود این است که طی این پروسه چقدر زمان لازم دارد؟

زمان انجام این کار به سه عامل مهم بستگی دارد: اول به طول رمزعبور و ترکیبی بودن آن، دوم سرعت کامپیوتر هکر و در آخر سرعت خط اینترنت هکر.

جدول زیر زمان های تخمین زده شده برای این کار را بر اساس نحوه انتخاب رمزعبور نشان می دهد. در این تخمین ها سایر امکانات یکسان هستند. به تفاوت زمان کشف یک پسورد هشت کارا کتری که فقط با حروف کوچک به وجود آمده با پسورد دیگری با همان تعداد کارکتر ولی استفاده از حروف کوچک و بزرگ و نشانه ها دقت کنید. تغییر یکی از حروف به حرف بزرگ و استفاده از علامت ستاره زمان را از ۴/۲ روز به ۱/۲ قرن افزایش می دهد!

البته زمان های فوق بر اساس کارکرد کامپیوترهای معمولی محاسبه شده است و اگر به عنوان مثال از کامپیوترهای گوگل برای این کار استفاده شود، کشف رمز هزار برابر سریعتر انجام خواهند شد.

تا همین جا هم کاملاً واضح است که اولین اقدام مهم شما برای حفظ امنیت تان، استفاده از رمزعبور مناسب و خودداری از انتخاب رمزهای عبور ضعیف است.

نگهداری رمزهای عبور طولانی و متعدد در ذهن، آزار دهنده و گاهی اوقات غیر ممکن است، اما برای هر مشکل راه حلی وجود دارد...

### در اینجا به ارائه چند راه حل خوب می پردازیم :

- اگر از الفبای انگلیسی استفاده می کنید، از اعداد به جای حروفی هم قیافه شان استفاده کنید. به عنوان مثال از عدد '۰' به جای حرف 'o'، از '۳' به جای 'E' و از '@' در کلماتی که 'a' دارند استفاده کنید.

- به صورت تصادفی از حروف بزرگ استفاده کنید. ( مانند Mod\*ITF\*ord )  
- در جوانی به چه چیزی علاقه داشته اید؟ دقت کنید از اسم شخص استفاده نکنید زیرا اسامی و کلماتی که در دیکشنری دارای مفهوم هستند به سرعت در حملات Brute Force attack لو می روند.

- اسم مکانی که آن را دوست داشتید یا یک روز تعطیل جذاب و شاید رستوران مورد علاقه تان می توانند رمزعبور خوبی باشند، البته به استفاده از بند اول و دوم در اینجا هم توجه داشته باشید.

- یک کلمه فارسی با مفهوم در شرایطی که زبان کامپیوتر شما انگلیسی است، یک رمز عبور مطمئن خواهد بود! اما باز تأکید می کنم که حروف بزرگ تصادفی را فراموش نکنید.

- اگر به خاطر سپردن رمزهای عبور برایتان سخت است، برنامه LastPass را به شما توصیه می کنیم. این نرم افزار امکان نگهداری اطلاعات اکانت های مختلف شما را به صورت رمز نگاری شده برایتان فراهم می کند. با استفاده از LastPass تنها حفظ یک رمز عبور اصلی ضرورت دارد و خود نرم افزار فرم های نام کاربری و رمز عبور را به صورت خودکار، پس از دریافت رمز اصلی، پر می کند. نمونه های دیگری مانند keepass و Roboform نیز وجود دارند که همین کار را برای شما انجام می دهند.

### با LastPass فرماندهی رمزهای عبور خود را در دست بگیرید

- در نهایت پس از انتخاب رمز عبور، با استفاده از سرویس هایی مانند Password Strength Test مایکروسافت میزان امن بودن آن را آزمایش کنید.

### چگونه یک رمزعبور مطمئن بسازیم و از آن نگهداری کنیم - بخش اول

نکته دیگری که بایستی به آن توجه داشته باشید، این است که همه اکانت های خود را در زمان انتخاب رمزعبور، مهم بدانید. برای مثال برخی از افراد با این توجیه که ایمیل حساسی دریافت نمی کنند، نسبت به امنیت اکانت ایمیل خود بی توجه هستند. غافل از اینکه هکر می تواند با در اختیار داشتن ایمیل شما، حتی با بانک شما مکاتبه کند و درخواست دریافت رمز عبور جدید بنماید. به همین

سادگی آقای هکر محترم به مهمترین اطلاعات شما دسترسی پیدا می کند.

گاهی اوقات افراد اطلاعات مهم را روی کامپیوتر خانگی شان، دور از دسترس سایرین در شرایطی که با یک router و یک Firewall محافظت می شوند. نگهداری می کنند. غافل از اینکه فراموش کرده اند رمز عبور پیش فرض سخت افزار خود را تغییر دهند. بنابراین هکر به سادگی به شبکه خانگی شما متصل شده و اطلاعات را سرقت می کند.

معمولاً انسان ها تا زمانی که با نتیجه دردناک یک اشتباه روبرو نشوند، نکات لازم را رعایت نمی کنند. ولی آیا واقعاً انتخاب یک رمز عبور درست و قدرتمند برای جلوگیری از اتفاقات دردناک و حفظ حریم خصوصی کار دشواری است؟

<http://www.iritn.com>

## ۲۴.۴ SSL چیست؟



واژه‌ی SSL، مخفف Secure Socket Layer است و در واقع عنوانی برای یک فناوری استاندارد و به ثبت رسیده برای ایجاد ارتباطات امن بین وب سرورها و مرورگرهای اینترنت است. استاندارد مذکور، یک استاندارد فنی بوده و در حال حاضر توسط میلیون ها وب سایت در سراسر دنیا مورد استفاده قرار می گیرد.

پروتکل SSL برای اولین بار توسط شرکت Netscape به منظور انتقال اطلاعات به صورت امن بین دو نقطه در اینترنت تهیه شد و سپس توسط دیگر مرورگرها از جمله IE نیز مورد استفاده قرار گرفت. سپس پروتکل مذکور توسط شرکت (IETF) Internet Engineering Task Force به عنوان استاندارد تعریف شده و به ثبت رسید.

بنا بر پروتکل SSL، اطلاعاتی که میان مرورگر و وبسایتی که در حال مرور شدن است، مبادله می شود، به وسیله‌ی کلیدهای خصوصی (private key) رمزنگاری شده و در صورتی که در طول مسیر اطلاعات استراق سمع شوند، قابل استفاده نخواهند بود. به همین جهت است که از پروتکل مذکور برای کاربردهای تجاری استقبال خوبی به عمل آمده است.

در حال حاضر بسیاری از وب سایت ها علاوه بر پروتکل معمول HTTP از SSL نیز حمایت می کنند و برای دسترسی امن به اطلاعات وبسایت های مذکور می توان از HTTPS استفاده کرد. پروتکل HTTP-S همان Secure HTTP است و از پروتکل SSL برای انتقال اطلاعات استفاده می کند. قابل ذکر است که پروتکل HTTP به صورت پیش فرض از پورت ۸۰ استفاده می کند در حالی که پروتکل HTTPS به صورت پیش فرض از پورت ۴۴۳ استفاده می کند. به عبارت دیگر این دو پروتکل دو مجرای ارتباطی کاملاً مجزا دارند.

وب سایت هایی که قصد استفاده از پروتکل SSL را دارند باید گواهینامه ای را برای این منظور دریافت نمایند که به گواهینامه SSL معروف است. دارنده گواهینامه SSL تضمین می کند تمام اطلاعاتی که مابین وب سرور و مرورگر کاربرانش رد و بدل می شود محرمانه و دست نخورده باقی

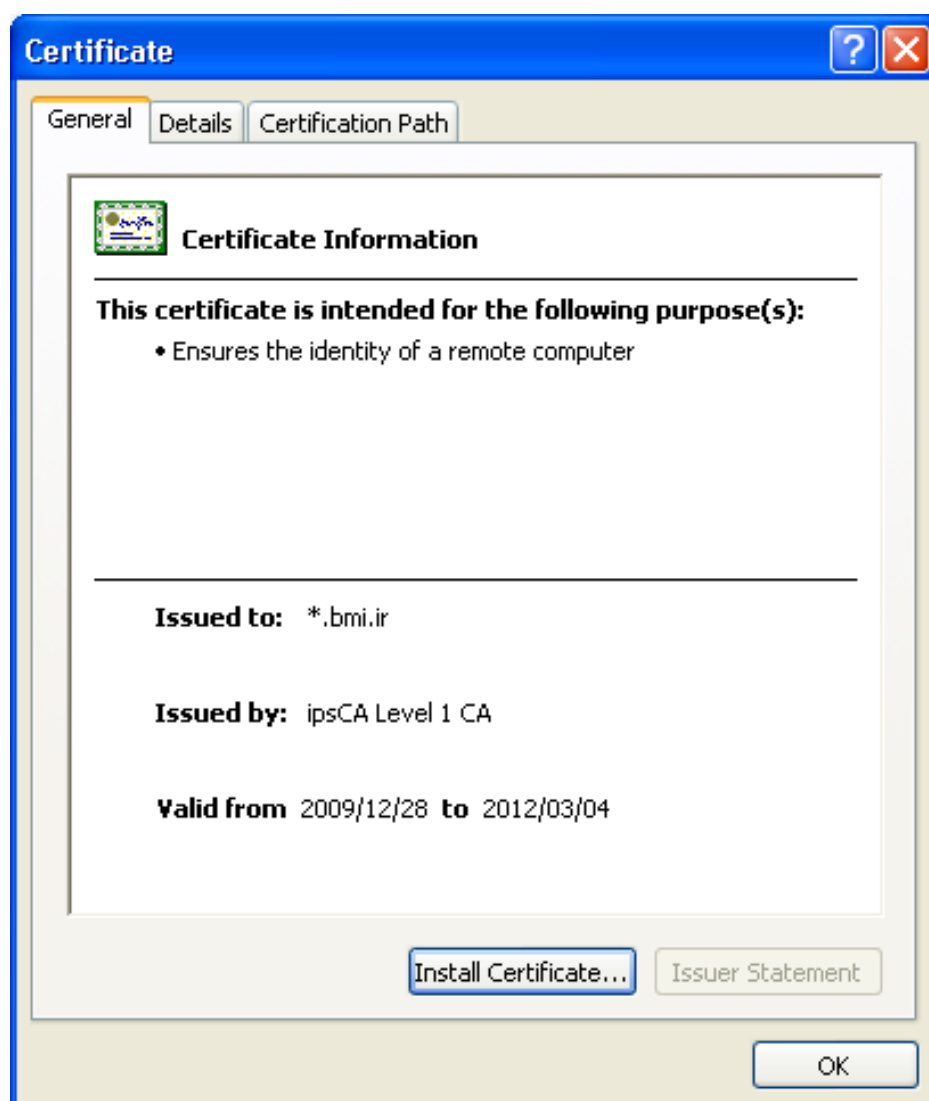
بماند.

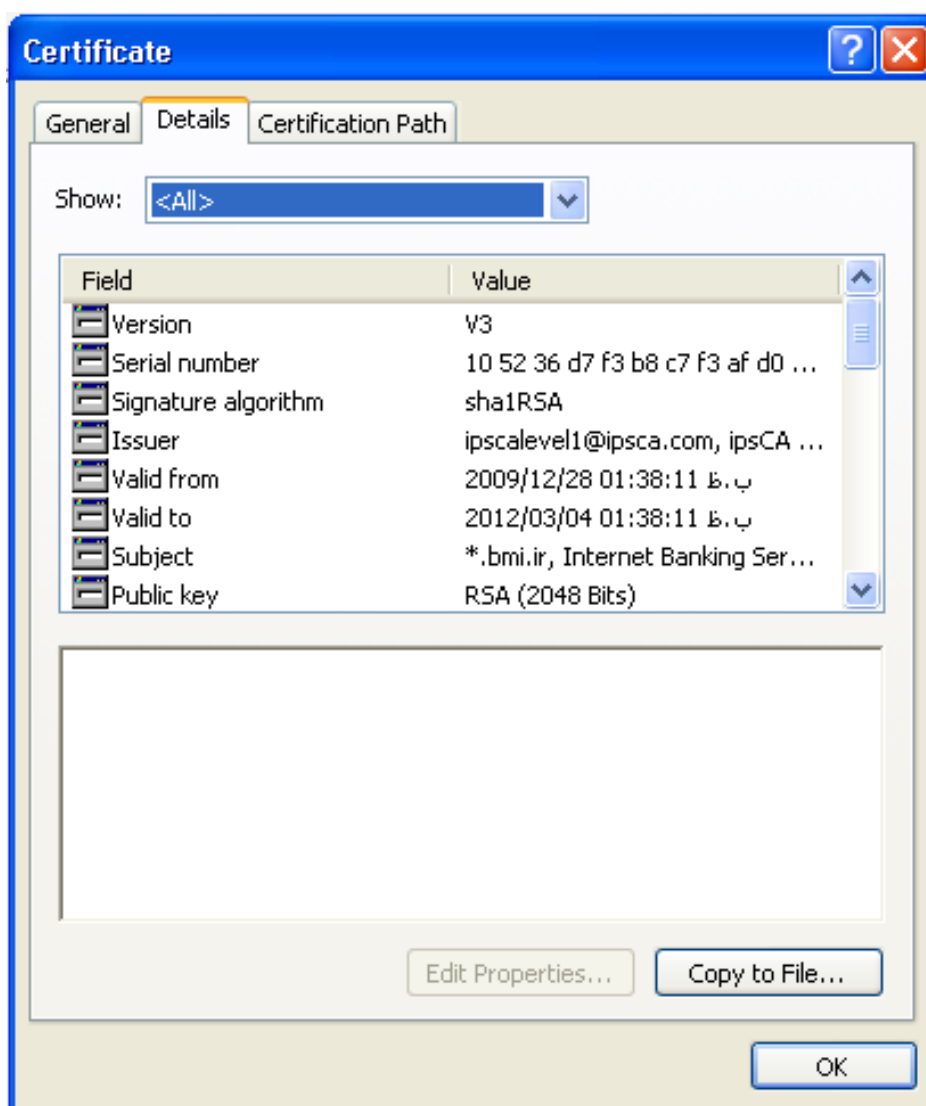
به عبارتی دیگر، گواهینامه‌های دیجیتال يك ارتباط امن را بر مبنای پروتکل SSL تضمین می‌کنند و این کار را اولاً از طریق رمزنگاری بسته‌های اطلاعاتی و ثانیاً از طریق تأیید هویت وب سایت و یا سرویس نرم افزاری دارای گواهینامه انجام می‌دهند.

همان طور که در بالا گفته شد، رمزنگاری بسته‌های اطلاعاتی در هنگام تبادل آنها این امکان را به طرفین می‌دهد که ارتباط خود را در بستری امن و به دور از مداخله شخص ثالث، به صورت رمز شده و غیر قابل خواندن برای دیگران برقرار سازند و از صحت اطلاعات رد و بدل شده اطمینان حاصل کنند. قابل ذکر است که اطلاعاتی که بدون وجود این پروتکل رد و بدل می‌شوند، به سادگی توسط افراد ثالث در گره‌های (Node) بین راه قابل رویت، تغییر و سوء استفاده هستند.

مورد دیگری که گواهینامه‌های دیجیتال تضمین می‌کنند، تأیید هویت وب‌سایت و یا سرویس نرم افزاری است که گواهینامه دیجیتال بر روی آن نصب گردیده است. به عبارت دیگر، کاربر وب‌سایتی که دارای گواهینامه دیجیتال معتبر است می‌تواند از جعلی نبودن وب‌سایت مذکور و هویت حقیقی آن اطمینان حاصل کند و مطمئن باشد که این وب‌سایت با توجه به گواهینامه‌ی معتبری که دارد، واقعاً همان است که ادعا می‌نماید، نه يك وب‌سایت جعلی که شبیه به وب‌سایت اصلی ایجاد شده و با روش‌های متعددی که برای انحراف مسیر و هک کردن وجود دارد کاربر را به سمت خود هدایت کرده است. (پیشگیری از حملات Phishing و man-in-the-middle)

پیچیدگی‌های پروتکل SSL برای کاربران پوشیده است، اما آنها می‌توانند با استفاده از قفل کوچک زرد رنگی که در پایین صفحه مرورگر نمایش داده می‌شود، از برقراری يك ارتباط امن اطلاع حاصل کنند. قابل ذکر است که در نسخه‌های جدید برخی از مرورگرها همچون IE، قفل مذکور در کنار نوار آدرس نمایش داده می‌شود. هنگامی که کاربر روی قفل کوچک زرد رنگ دوبار کلیک کند، گواهینامه وب سایت به همراه سایر جزئیات نمایش داده می‌شود. در زیر مثالی از نمایش مشخصات و جزئیات گواهینامه دیجیتال در مرورگر IE که مربوط به بانک ملی است، آورده شده است:





يك مرورگر اینترنت به يك وبسایت از طریق ارتباط امن SSL متصل میشود ، علاوه بر دریافت گواهینامه SSL (کلید عمومی)، پارامترهایی را نظیر تاریخ ابطال گواهینامه، معتبر بودن صادرکننده گواهینامه و مجاز بودن وبسایت به استفاده از این گواهینامه را نیز بررسی می‌کند و هر کدام از موارد را که مورد تایید نباشد به صورت يك پیغام اخطار به کاربر اعلام میدارد.

<http://certcc.ir>



## ۲۵.۴ دومین جشنواره ملی ارتباطات و فناوری اطلاعات



دومین جشنواره ملی ارتباطات و فناوری اطلاعات، یادواره شهید دکتر قندی، ۲۷ اردیبهشت و همزمان با هفته ارتباطات برگزار می شود.

### حوزه های اصلی

- برترین ارائه کنندگان خدمات ارتباطی و فناوری اطلاعات (اپراتورها، شبکه ها، وایمکس، ISP، PAP، SAP، پست، پست بانک) و الکترونیکی
- برترین های خدمات دولت الکترونیکی (پیشخوان دولت)
- شناسایی، جذب و پرورش استعداد های دانشجویی و دانشگاهی در زمینه تولید دانش و بومی سازی تکنولوژی ارتباطات و فناوری اطلاعات
- معرفی برترین پایگاه های اطلاع رسانی و روابط عمومی الکترونیکی از لحاظ به کارگیری فناوری های نوین اطلاعاتی (بدون ارزیابی محتوا)
- نوآوری در تحقیق و پژوهش از نظر موضوع و روش یا هر دو در ایران و جهان، تولید و پشتیبانی سیستم های مخابراتی و ارتباطی، خلاقیت و نوآوری، کارآفرینی، انتخاب مدیران برتر و بیشترین تأثیرگذاران در حوزه ارتباطات و فناوری اطلاعات

### برنامه های جانبی

۱- با عنایت به گستردگی زمینه های تخصصی مورد اشاره در جشنواره مذکور نمایشگاه جنبی جهت انعکاس فعالیت ها و نمایش علمی برگزار می شود.

۲- برگزاری workshop با تعریف تخصصی و ویژه در کنار جشنواره ارتباطات و فناوری اطلاعات

۳- برگزاری همایش های علمی و تخصصی

۴- چاپ مشخصات، تصاویر و زندگی نامه چهره های برگزیدگان در کتاب ویژه جشنواره رویکردهای دومین جشنواره

- بر اساس رویکرد دومین جشنواره بخش ویژه دانشجویی اضافه شد.

- بر اساس رویکرد دومین جشنواره، با همکاری بنیاد ایرانیان خارج از کشور، نسبت به فراخوان متخصصان ایرانی خارج از کشور اقدام می شود.

- تغییر کارگروه هانسبت به سال گذشته از رویکرد سازمانی به رویکرد فرا سازمانی و مفهومی

- معرفی برترین شرکتهای دانش بنیان

## ۲۶.۴ متن کامل قانون جرائم رایانه ای - مصوب ۱۱ بهمن ۱۳۸۹

### مجلس شورای اسلامی

فصل یکم - جرائم علیه محرمانگی داده ها و سیستم های رایانه ای و مخابراتی  
مبحث یکم - دسترسی غیرمجاز

ماده ۱- هرکس به طور غیرمجاز به داده ها یا سیستم های رایانه ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از پنج تا بیست میلیون ریال یا هر دو مجازات محکوم خواهد شد.  
ادامه‌ی مطلب را در سایت فناوری ببینید...

## ۲۷.۴ وضعیت امنیت در شش ماهه دوم سال ۲۰۱۱ به گزارش M۸۶

گزارشی که در ادامه می آید، برگرفته از گزارشی است که توسط کارشناسان شرکت امنیتی M۸۶ از وضعیت امنیت اینترنت در نیمه دوم سال ۲۰۱۱ تهیه شده است. آزمایشگاه امنیتی M۸۶ متشکل از محققان امنیتی است که تخصص آنها در تهدیدهای وب و ایمیل بوده و به نظارت و تحلیل روندهای امنیت اینترنت، هرزنامه ها، حملات Phishing و فعالیت بدافزارها در اینترنت می پردازند. در ادامه مهمترین مطالب ذکر شده در گزارش شش ماهه‌ی دوم سال ۲۰۱۱ آورده شده است.

### نقشه جهانی بدافزار

نقشه جهانی بدافزار نشان دهنده توزیع محتوای خرابکار در سراسر جهان است. در واقع این نقشه نشان دهنده مکان واقعی میزبان محتویات خرابکار است.  
ادامه‌ی مطلب را در سایت فناوری ببینید...

## ۲۸.۴ اطلاعیه مرکز فناوری اطلاعات و ارتباطات

اطلاعیه مرکز فناوری اطلاعات و ارتباطات کشور در خصوص حملات سایبری به سیستم های اطلاعات تحت شبکه ارگانها و سازمان های دولتی کشور و جلوگیری از انتشار یک نوع بدافزار خاص ...



مرکز فناوری اطلاعات و ارتباطات

شماره ۲۶۹۰۲  
تاریخ ۱۳۹۱/۰۲/۱۶  
پست

باسمه تعالی

### کلیه سازمانهای متصل به شبکه دولت

با سلام و احترام

به آگاهی می‌رساند از آنجایی که حملات سایبری به سیستم‌های اطلاعات تحت شبکه ارگانها و سازمانهای دولتی کشور و با هدف تخریب غیر قابل‌بازیبی داده‌ها و اطلاعات و در نهایت اختلال در مأموریت‌های سازمانهای کشور در دستور کار نظام سلطه قرار گرفته است، که از آن جمله می‌توان به حمله سایبری اخیر، که به صورت نامه الکترونیکی از منبع ناشناس با متن (انگلیسی) "من از تو عکسی دارم، عکس ضمیمه را چک کن خودت هستی یا نه؟ به همراه فایل ضمیمه img98۰۷.zip" حاوی بدافزاری از نوع wiper بوده که نسبت به انهدام کامل اطلاعات اقدام می‌کند، اشاره کرد.

لذا ضروریست برای جلوگیری از انتشار و انتقال این بدافزار، کلیه سازمانها به اجرای موارد ذیل در اسرع وقت اقدام فرمایند:

- اطلاع‌رسانی مناسب به کاربران شبکه در خصوص باز نکردن نامه الکترونیکی مذکور و موارد مشابه.
  - جداسازی فیزیکی و نرم‌افزاری کلیه سرورها و سرویسهای تحت شبکه داخلی از شبکه اینترنت.
  - پشتیبان‌گیری از اطلاعات سیستم‌ها و سرویسهای حساس تحت شبکه.
  - استفاده از ضد ویروس مناسب و نیز دقت در بروز رسانی آن.
- همچنین در راستای ارتقای سطح امنیتی شبکه خود و جلوگیری از آسیب‌پذیریهای احتمالی نسبت به اجرای راهکارهای امنیتی ذیل اهتمام ورزند:
- تهیه قواعد مناسب امنیتی با توجه به شبکه خود و اعمال آنها در شبکه.
  - مسدود نمودن پورتهای آسیب‌پذیر در شبکه.

## ۲۹.۴ آشنایی با عملکرد برخی از بدافزارها و نحوه پاکسازی آنها

مرکز ماهر (مرکز مدیریت امداد و هماهنگی عملیات رخدادهای رایانه ای) به عنوان نقطه کانونی پاسخگویی به حوادث رایانه ای کشور، آشنایی با عملکرد برخی از بدافزارها و نحوه پاکسازی دستی و خودکار آنها را مورد بحث قرار داده است. تحلیل بیان شده درخصوص هر بدافزار با استفاده از استاندارد نامگذاری آنتی ویروس Gdata بیان شده است.

به منظور دستیابی به نام معادل بدافزار مورد جستجوی خود در استاندارد نامگذاری سایر آنتی ویروسها می توانید به وب سایت [www.virustotal.com](http://www.virustotal.com) مراجعه و اطلاعات لازم را کسب نمایید. رئوس مطالب بیان شده در مستند راهنمای پاکسازی بدافزارها شامل موارد ذیل می باشد:

- بررسی میزان تهدیدات و سطح ریسک بدافزار بر سیستم آلوده
- روشهای انتشار بدافزار
- نشانه های يك سیستم آلوده و تغییرات ایجاد شده در آن سیستم
- راهنمای پاکسازی بدافزار از سیستم آلوده
- اسامی معادل استفاده شده توسط آنتی ویروس های معتبر در خصوص بدافزار
- توضیحات تکمیلی در خصوص نحوه انتشار بدافزار در کشورهای مختلف

## ۳۰.۴ بدافزار Flame ، ابزار شناسایی و نحوه پاکسازی



در پی بررسی-های تخصصی انجام شده طی چند ماه گذشته توسط کارشناسان مرکز ماهر و در ادامه تحقیقات صورت گرفته از سال ۲۰۱۰ پیرامون حملات هدفمند سازمان دهی شده استاکس نت و دیوکیو، این مرکز برای نخستین بار اقدام به انتشار اطلاعات آخرین نمونه از حملات این خانواده می نماید. این حمله توسط بدافزاری که از این پس با نام Flame (شعله آتش) معرفی خواهد شد صورت می گیرد. این نام برگرفته از محتویات رمزگشایی شده فایل های اصلی بدافزار است. این بدافزار در واقع پلتفرمی است که قابلیت دریافت و نصب ابزارهای گوناگون جهت فعالیت های مختلف را داراست. در حال حاضر هیچ کدام از اجزای پرشمار تشکیل دهنده این بدافزار توسط بیش از ۴۳ نرم افزار آنتی ویروس در دسترس مورد شناسایی قرار نمی گیرند. با این وجود ابزار شناسایی و پاکسازی این بدافزار در مرکز ماهر تهیه شده و از امروز در اختیار سازمان ها و شرکتهای متقاضی قرار خواهد گرفت.

شماری از قابلیت-های مهم این بدافزار عبارتند از:

- انتشار از طریق حافظه های فلش
- انتشار در سطح شبکه
- پوشش شبکه و جمع آوری و ثبت اطلاعات منابع شبکه و رمز عبور سیستم-های مختلف
- پوشش دیسک کامپیوتر آلوده و جستجو برای فایل-هایی با پسوندها و محتوای مشخص
- تهیه تصویر از فعالیت-های خاص کاربر سیستم آلوده با ذخیره سازی تصاویر نمایش داده شده بر روی مانیتور کاربر

- ذخیره سازی صوت دریافتی از طریق میکروفن سیستم در صورت وجود
- ارسال اطلاعات ذخیره شده به سرورهای کنترل خارج از کشور
- دارا بودن بیش از ۱۰ دامنه مورد استفاده به عنوان سرور C&C
- برقراری ارتباط امن با سرورهای C&C از طریق پروتکل های SSH و HTTPS
- شناسایی و از کار انداختن بیش از ۱۰۰ نرم افزار آنتی ویروس، ضد بدافزار، فایروال و ...
- قابلیت آلوده سازی سیستم- های ویندوز، XP ویستا و ویندوز ۷
- قابلیت آلوده سازی سیستم- های يك شبکه در مقیاس بالا

به احتمال قریب به یقین و با در نظر گرفتن پیچیدگی و کیفیت بالای عملکرد و همچنین اهداف مشابه این بدافزار، می-توان آن را محصولی از خانواده استاکس نت و دیوکیو دانست. نشانه های یافت شده حاکی از آن است که رویدادهای رخ داده اخیر درخصوص از بین رفتن همزمان اطلاعات سیستم- های کامپیوتری نتیجه فعالیت یکی از اجزای این بدافزار می-باشد. با تحلیل انجام شده فهرستی از اجزای تشکیل دهنده این بدافزار شناسایی شده و در جدول زیر ارائه می-گردد. این اطلاعات قابل ارائه به تولیدکنندگان عمده آنتی ویروس می-باشد و از این پس اجزای این بدافزار می-تواند مورد شناسایی آنتی ویروس- ها قرار گیرد.

#### روش پاکسازی :

- ۱- فایل پیوست که Removal\_Tool.rar نام داشته و حجم آن ۹۷۹،۹۳۱ بایت است، حاوی فایل های زیر است:
- ۱- فایل manual\_fa.pdf که راهنمای فارسی استفاده از ابزار است و حجمی برابر ۷۳۵،۲۹۷ بایت دارد.
- ۲- فایل remover.exe که ابزار پاکسازی در این فایل قرار دارد و حجم آن ۱۲۳،۹۰۴ بایت است.
- ۳- فایل vza.exe که ابزار فشرده سازی مورد استفاده ابزار پاکسازی است و حجمی برابر ۵۸۷،۷۷۶ دارد.

#### دانلود ابزار پاکسازی Flame

<http://www.certcc.ir/index.php?name=news&file=article&sid=1892>

## فصل ۵

# دستورالعمل خط مشی امنیت اطلاعات و سیستم های اطلاعاتی دانشگاه

لزوم وجود دستورالعمل مدونی برای امنیت اطلاعات دانشگاه و اطلاع رسانی این دستورالعمل بر کسی پوشیده نیست. به همین دلیل دستورالعمل ذیل توسط جناب آقای مهندس چشمی تدوین و به تصویب کمیته فناوری اطلاعات دانشگاه رسید.

### تعاریف و اصطلاحات

منابع شبکه و ارتباطات : هر نوع تجهیزات کامپیوتری، نرم افزار، شبکه و تسهیلات مربوطه که توسط دانشگاه تأمین شده باشد و اجازه دسترسی به آن توسط دانشگاه صادر گردد.  
مسئولین فناوری اطلاعات : اشخاصی که تحت نظارت مدیریت فناوری اطلاعات متصدی مدیریت و نگهداری اطلاعات فناوری اطلاعات می باشند.  
مدیر سیستم : شخصی که مجوز دسترسی کامل به امکانات يك سیستم فناوری اطلاعات (مثل پست الکترونیکی، وب، اتوماسیون اداری و...) را برای اداره یا نگهداری آن داشته باشد و از طرف مدیریت فناوری اطلاعات منصوب می گردد.  
کاربر : شخصی که به هر طریق ممکن از امکانات دانشگاه استفاده می کند.

### ۱- هدف

هدف اصلی از ایجاد خط مشی امنیت اطلاعات و سیستم های اطلاعاتی، محافظت از دارائیهای دانشگاه و فراهم کردن محیط امن برای دسترسی به اطلاعات و بهره برداری از امکانات سیستم های اطلاعاتی اعضای دانشگاه می باشد. خط مشی امنیت اطلاعات متضمن تأمین اهداف زیر است:

- ۱-۱ - محرمانگی، صحت، اصالت و قابلیت دسترسی به اطلاعات دانشگاه در سطوح مختلف تأمین گردد.

- ۱-۲ - دارائیهای و امکانات فن آوری اطلاعات دانشگاه در مقابل دستبرد، اختلال و دسترسی غیر مجاز مصون بماند.

- ۱-۳ - استفاده غیر مجاز و خلاف قانون از امکانات فناوری اطلاعات دانشگاه صورت نپذیرد.

### ۲- حوزه خط مشی

خط مشی امنیت اطلاعات دانشگاه در بر گیرنده موارد زیر است:

۱-۲- تمام سیستم‌های رایانه‌ای و متعلقات آنها اعم از دستگاه‌های جانبی، نرم‌افزارها، اطلاعات، داده‌های متعلق به دانشگاه (حتی اگر از نظر فیزیکی در محل دیگری واقع شده باشد) و یا در داخل دانشگاه باشد.

۲-۲- سیستم‌های اطلاعاتی که متعلق به دانشگاه نیستند اما کاربرد آنها بر تجهیزات متعلق به دانشگاه یا در داخل شبکه دانشگاه تأثیر می‌گذارد.

۲-۳- بستر شبکه، شبکه دانشگاه اعم از شبکه‌های محلی و شبکه‌ی گسترده‌ی دانشگاه.

۲-۴- کلیه کاربران سیستم‌های اطلاعاتی دانشگاه.

۲-۵- سایر دارائی‌های دانشگاه که ممکن است به علت استفاده نادرست از سیستم‌های اطلاعاتی در معرض تهدید قرار گیرند.

### ۳- مسئولیتها

۱-۳- مسئولیت ایجاد قوانین و معیارهای امنیتی : مسئولیت وضع قوانین و دستورالعمل‌های

امنیتی دانشگاه و همچنین بررسی مجدد و تجدید نظر در آنها بعهدہ کمیته فناوری اطلاعات دانشگاه خواهد بود. این کمیته همچنین عالیترین مرجع قضاوت در مورد مسائل و مشکلات امنیت اطلاعات دانشگاه می‌باشد.

۲-۳- مسئولیت اجرای خط مشی امنیتی : مسئولیت اجرای خط مشی امنیتی در مورد حفاظت فیزیکی، حفاظت شبکه، نرم‌افزارها و اطلاعات از سیستم‌های اطلاعاتی در دانشگاه برعهده مدیریت فناوری اطلاعات خواهد بود. ضمناً هر سیستم اطلاعاتی باید دارای مدیریت مستقلی تحت نظارت مسئول واحد باشد که مجوز دسترسی کامل (به منظور اداره و نگهداری) به آن سیستم را خواهد داشت. وظایف مدیریت سیستم‌ها در بخش ۵ ذکر خواهد شد.

۳-۳- مسئولیت نظارت بر اجرای خط مشی امنیتی : مسئولیت نظارت بر اجرای خط‌مشی‌های امنیتی دانشگاه بر عهده مدیریت فناوری اطلاعات دانشگاه خواهد بود. در این راستا، در صورتی که هر یک از واحدها نتواند خط مشی‌های امنیتی دانشگاه را بنحو مطلوب اجرا نماید، مدیریت فناوری اطلاعات موظف است کلیه اقدامات لازم و قابل قبول را برای تأمین امنیت و جلوگیری از استفاده نادرست از امکانات فناوری اطلاعات دانشگاه به عمل آورد.

۴-۳- مسئولیت آموزش خط مشی امنیتی : مدیریت فناوری اطلاعات دانشگاه موظف است تدابیر لازم را برای آموزش سیاست امنیت اطلاعات به مسئولین واحدهای مختلف دانشگاه، اتخاذ نماید. پس از طی این مرحله، مسئولیت آموزش اعضای هر واحد، بر عهده مسئول آن واحد خواهد بود.

تبصره ۱: تمام اعضای دانشگاه (اعم از اساتید، دانشجویان و کارکنان) بعنوان استفاده کننده از امکانات فناوری اطلاعات دانشگاه، موظف به رعایت معیارهای امنیتی مندرج در سیاست امنیت می‌باشند.

### قوانین

کاربران شبکه رایانه ای دانشگاه مسئول استفاده مناسب از منابع و اطلاعات شبکه و احترام به حقوق دیگران می‌باشند و این قوانین شرایط استفاده مناسب از منابع اطلاعاتی دانشگاه را بیان می‌کند:

کاربران منابع اطلاعاتی دانشگاه بایستی حقوق مولفان و اجازه انتشار مطالب دیگران را احترام بگذارند و از زیر پا گذاشتن حقوق دیگران اجتناب کنند. این دستورالعمل شامل استفاده مناسب از تمام منابع اطلاعاتی دانشگاه شامل رایانه‌ها، شبکه‌ها و اطلاعاتی که در آنها وجود دارد می‌شود.

این قوانین برای همه اساتید، کارکنان، دانشجویان و تمامی کسانی است که اجازه دسترسی به شبکه دانشگاه برای آنها ایجاد شده است .

سیاستها:

- ۱- استفاده از امکانات فن آوری اطلاعات دانشگاه برای اهداف زیر قابل قبول است:
  - تدریس و یادگیری
  - پژوهشهای علمی
  - افزایش دانش شخصی
  - انجام امور مشاوره‌ای برای مؤسسات طرف قرارداد دانشگاه
  - ایجاد ارتباطات برای دستیابی به اهداف فوق
- تبصره ۱: هر گونه فعالیت شخصی در حد متعارف در صورتیکه مرتبط با اهداف تجاری نباشد قابل قبول است و مرجع تشخیص متعارف بودن استفاده از منابع شبکه، مدیریت فناوری اطلاعات دانشگاه می‌باشد . تبصره ۲: کلیه استفاده‌های فوق باید در چارچوب قوانین جاری کشور و با رعایت حقوق سایر افراد صورت پذیرد. تبصره ۳: در مورد فعالیتهایی که در فهرست فوق قرار نمی‌گیرند، صدور مجوز بعهده مدیریت فناوری اطلاعات و در صورت لزوم کمیته فناوری اطلاعات دانشگاه خواهد بود.
- ۲- هر شخصی که به شبکه دانشگاه متصل شود، بطور ضمنی مقررات و خط مشی‌های امنیتی دانشگاه را پذیرفته است.
- ۳- تمام استفاده کنندگان از سیستم‌های فناوری اطلاعات دانشگاه از جمله کارکنان و راهبران سیستم‌ها باید اصل خصوصی بودن اطلاعات در شبکه و حفظ حریم خصوصی افراد را رعایت نمایند.
- ۴- مدیران سیستم تنها در صورت لزوم و با رعایت مفاد آیین نامه‌های استفاده از پست الکترونیکی و اینترنت دانشگاه می‌توانند به اطلاعات کاربران دسترسی پیدا کنند و یا جریان اطلاعات در شبکه را بررسی نمایند.
- ۵- هر قراردادی که میان دانشگاه و طرف دیگری (اعم از حقیقی و حقوقی) منعقد گردد که متضمن استفاده آن طرف از امکانات فن آوری اطلاعات دانشگاه شود، باید شامل ماده‌ای باشد که در آن لزوم رعایت مقررات و خط‌مشی‌های امنیتی شبکه و سیستم‌های اطلاعاتی دانشگاه در آن تصریح گردد.
- ۶- تمامی کاربران بایستی در حفظ و استفاده بهینه از منابع اطلاعاتی شبکه و تجهیزات آن کوشا باشند.
- ۷- کاربران بایستی اقدام به جدا کردن قطعات سخت افزاری از رایانه و یا حذف و نصب نرم افزار روی رایانه های متعلق به دانشگاه نمایند، مگر اینکه اجازه لازم را از مدیریت فناوری دریافت کنند.
- ۸- هیچ کاربری بایستی با دسترسی کاربر دیگری وارد شبکه شود و از منابع شبکه استفاده کند این مورد شامل: تلاش برای تغییر اطلاعات شخصی و یا دانشگاهی افراد دیگر، تلاش برای دسترسی به منابعی که خود شخص اجازه دسترسی به آنها ندارد، تلاش برای ایجاد تغییرات در سیستمها، سیستم عاملها یا منابع اطلاعاتی، تلاش برای از کار انداختن رایانه(ها) ی دانشگاه و یا تلاش برای از بین بردن و یا دستکاری اطلاعات موجود در شبکه دانشگاه، می باشد.
- ۹- کاربران شبکه بایستی نرم افزاری نوشته و یا نصب کنند که باعث اختلال در سایر رایانه ها و یا شبکه شود و به اطلاعات حساس و یا شخصی دیگران دسترسی پیدا کنند، و یا باعث ایجاد اشکال در اجزای نرم افزاری و یا سخت افزاری شبکه شوند.



- ۱۰- کاربران شبکه نبایستی از نرم افزارها و یا برنامه های کاربردی استفاده کنند که باعث اختلال در کار سایر رایانه ها و یا دسترسی به حسابهای کاربری سایرین داشته باشد.
- ۱۱- استفاده از هرگونه نرم افزار مخربی که باعث صدمه زدن به رایانه ها و یا دسترسی غیر مجاز به اطلاعات شبکه شود مصداق جرم رایانه ای است .
- ۱۲- کاربران شبکه دانشگاه نبایستی به رایانه، نرم افزار، داده و یا اطلاعات شبکه، بدون داشتن اجازه دسترسی، دسترسی پیدا کنند و نبایستی در صورتیکه به شبکه دانشگاه دسترسی دارند این دسترسی را به دیگران بدهند.
- ۱۳- لازم است کاربران شبکه هر نوع نقضی را که در نرم افزارها و سیستم امنیت شبکه مشاهده می کنند، بلافاصله به مدیریت فناوری دانشگاه اطلاع دهند تا نسبت به رفع آن اقدام شود.
- ۱۴- کاربری که به وی نام کاربری و رمز ورود اعطا شده است مسئول استفاده صحیح از این نام کاربری و رمز ورود است و استفاده غیر مجاز از آن و یا ارائه آن به دیگران تخلف می باشد.
- ۱۵- کاربران شبکه بایستی حقوق دیگر کاربران را رعایت کنند، اکثر سیستم های دانشگاه مکانیسم هایی برای محافظت از اطلاعات شخصی کاربران دارند، تلاش برای دور زدن این مکانیسمها برای دسترسی به اطلاعات سیستم ها و یا اطلاعات اشخاص مصداق جرم است.
- ۱۶- استفاده از امکانات شبکه ای و ارتباطی دانشگاه جهت گول زدن، تهدید، اذیت و آزار دیگران مجاز نمی باشد.
- ۱۷- منابع ارتباطی و شبکه ای دانشگاه نبایستی جهت ارسال موارد تبلیغاتی شخصی و یا تجاری مورد استفاده قرار گیرد.
- ۱۸- کاربران نبایستی عمدتاً دنبال بدست آوردن کپی یا تغییر در فایل های اطلاعاتی، تغییر در نرم افزارها و یا تغییر در کلمات عبور سایر کاربران باشند.
- ۱۹- منابع شبکه و ارتباطات دانشگاه نباید در جهت جانبداری و یا تبلیغ از احزاب سیاسی مورد استفاده قرار گیرد.

## فصل ۶

# راهنمای مدیریت وبسایتهای دانشگاه

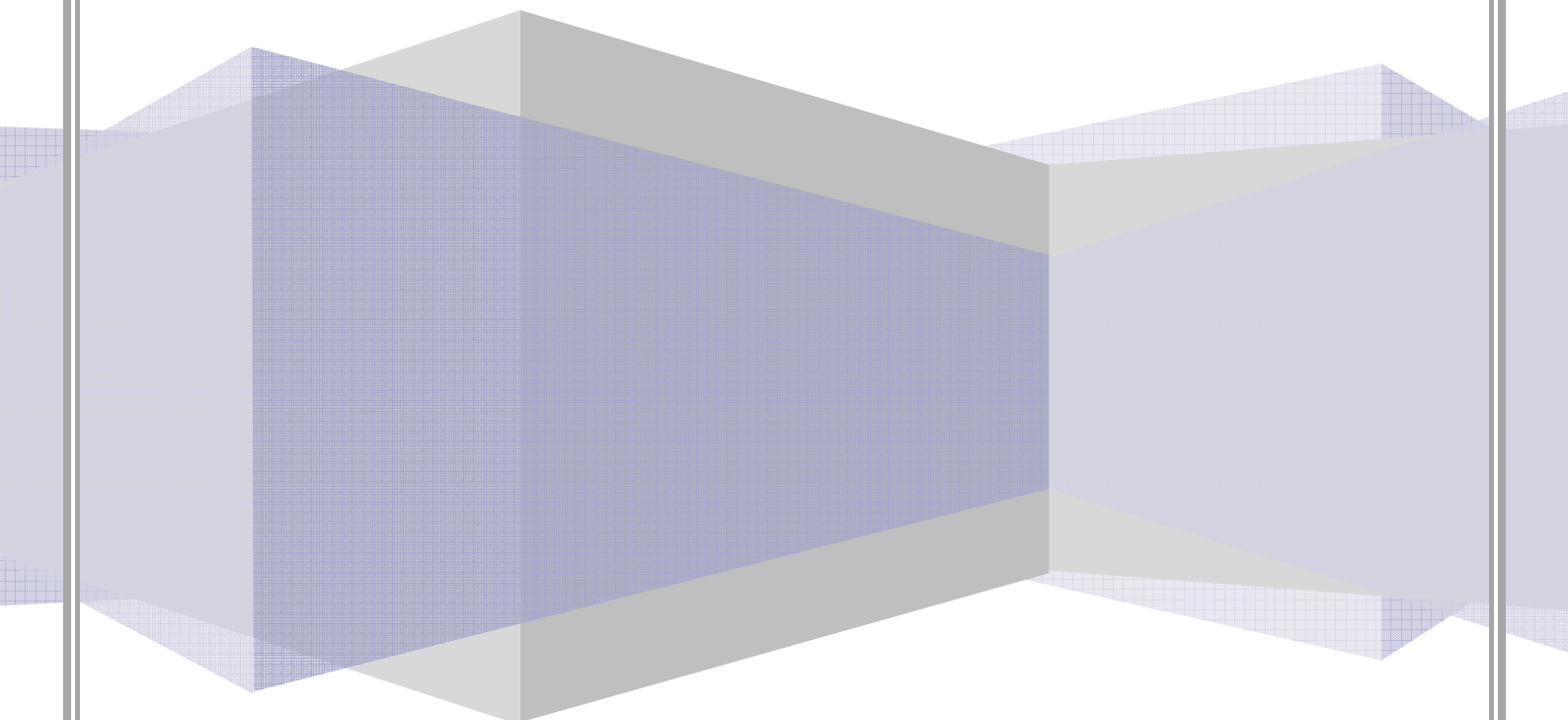
در این فصل فایل راهنمای مدیریت وبسایتهای دانشگاه - که توسط آقای زاهدی نژاد آماده شده است - مستقیماً درج شده است.

بسمه تعالی

# راهنمای مدیریت وب سایت دانشگاه

مدیریت فناوری اطلاعات دانشگاه حکیم سبزواری

علی زاهدی نژاد - کارشناس مدیریت فناوری اطلاعات



عنوان تمام زیر دامنه های دانشگاه که توسط بخش های مختلف پیشنهاد می گردد به انتهای آدرس دانشگاه افزوده میگردد. به عنوان نمونه سایت مدیریت حراست: <http://www.sttu.ac.ir/herasat>

### ورود به بخش مدیریت:

برای ورود به بخش مدیریت سایت باید به انتهای آدرس سایت خود **wp-admin** را بیافزاییم:

<http://www.sttu.ac.ir/herasat/wp-admin>

مدیریت فناوری اطلاعات  
دانشگاه تربیت معلم سبزوار

شما اکنون خارج شدید.

شناسه

رمز

ورود

مرا به خاطر بسپار

[بازنشانی نام کاربری](#) | [بازنشانی رمز عبور](#)

با وارد نمودن شناسه و رمز عبور خود وارد پیشخوان مدیریت خواهید شد:

سایت دانشگاه تربیت معلم سبزوار | بیرون رفتن | Howdy administrator | مدیر شبکه (16) | بیرون رفتن

نویسنده: **بیرون رفتن**

تقریبا 3.3 ماهه است | لطفا هم اکنون به روز رسانی کنید.

راهنما | نظرات صفحه | راهنما

پیشخوان | پیشخوان | سایت های من

گروه نوشته ها | نوشته ها | افزودن نوشته | دسته ها | برجسته های نوشته | رسانه | کتابخانه | افزودن بریده | پیوندها | برگه ها | دیدگاه ها | Slides | Slides | Add New | Slideshows | Settings

فهرست مدیریتی

شماره اکنون

گفت و گوها	محتوا
دیدگاه 0	نوشته 41
تایید شده 0	برگه 46
در انتظار بررسی 0	دسته 8
حذف 0	برجسته 0

Change Theme | به روز رسانی به 3.3

نوشته fum به همراه 1 ابزارک شما از وردپرس 3.1.1 استفاده می کنید.

فضای ذخیره سازی

10 مگابایت فضای مجاز

1.17 مگابایت (12%) فضای استفاده شده

آخرین دیدگاه ها

شور دیدگاهی داده نشده.

نوشته کورگ

نام

بارگذاری گذاشتن

محتوا

برجسته ها

انتشار | بازسازی | ذخیره پیش نویس

آخرین پیش نویس ها

راهنمای ثبت نام می 9, 2011

ضمن تبریک موفقیت شما در آزمون سراسری 1390 ، از ...

نمایش همه

## پیش خوان:

راهنما: در بالای هر صفحه مدیریت زبانه ی راهنما وجود دارد که توضیح کامل در مورد هر آیتم در آن درج شده است. فهرست مدیریتی سمت راست: پیوندهایی برای مدیریت سایت در اختیار شما قرار میدهد. هنگامی که نشانگر خود را روی گزینه های مختلف این فهرست به حرکت در می آورید یک پیکان در سمت چپ آنها نمایان می شود که می توانید بخشهای مختلف این فهرست مدیریتی را با کلیک بر روی همان پیکان باز یا بسته کنید. همچنین می توانید کل فهرست را با کلیک کردن بر روی آیکن جداکننده که در بین بخشهای مختلف فهرست وجود دارد کوچک یا بزرگ نمایید. وقتی که فهرست به حالت کوچک در آمد بخشهای فرعی آن با بردن نشانگر بر روی هر بخش اصلی نمایان می شود.

انتخاب محل قرارگیری هر بخش و همچنین چند ستونه بودن صفحه ی پیشخوان را می توانید در زبانه ی تنظیمات صفحه به دلخواه خود تغییر دهید. برای تغییر دادن محل قرارگیری هر بخش می توانید با کشیدن و رها کردن آن بخش محل جدید را مشخص کنید. همچنین می توانید هر بخش را با کلیک کردن بر نوار بالای آن بسته یا باز کنید.

## تغییر کلمه عبور:

مهم: پس از تحویل شناسه و کلمه عبور خود از مدیریت فناوری، در اولین مراجعه به بخش مدیریت سایت خود، کلمه عبور را از بخش کاربران ← شناس نامه شما، تغییر دهید:

در صورتی که آماده است! لطفا هم اکنون به روز رسانی کنید.

بیشخوان

پیشنهادات

سایت های من

نوشته ها

رسانه

پیوندها

برگه ها

دیدگاه ها

Slides

نمایش

افزونه ها

کاربران

کاربران

افزودن کاربر

شناسنامه شما

ابزارها

تنظیمات

تماس

نوشتنن فوری

نام

بارگذاری/گذاشتن

محتوا

برچسب ها

انتشار

ذخیره پیش نویس

بازسازی

شم اکون

محتوا

گنت وگوها

دیدگاه 0

نوشته 41

برگه 46

دسته 8

برچسب 0

Change Theme

به روز رسانی به 3.3

پوسته Fum به همراه 1 ابزارک

شما از وردپرس 3.1.1 استفاده می کنید.

فضای ذخیره سازی

10 مگابایت فضای مجاز

1.17 مگابایت (12%) فضای استفاده شده

آخرین دیدگاه ها

هنوز دیدگاهی داده نشده.

شناسنامه شما

## شناسنامه:

شناسنامه شما حاوی اطلاعاتی درباره حساب کاربری شما و همچنین برخی از گزینه های شخصی برای استفاده از مدیریت سایت است.

\*رنگ محیط مدیریت قابل تغییر است.

\*نام کاربری غیر قابل تغییر است ولی می توانید از گزینه های دیگر برای وارد کردن نام حقیقی یا مستعار خود استفاده کرده و انتخاب کنید از کدام نام برای نمایش در نوشته های شما استفاده گردد.

\*بخش های مورد نیاز مشخص شده اند؛ بقیه اختیاری هستند.

به یاد داشته باشید پس از پایان کار روی "به روزرسانی شناسنامه" کلیک کنید.



## بخش های کاربردی در سایت:



## نوشته ها:

عنوان	نویسنده	دسته ها	برچسب ها	تاریخ
فصلی شبکه دانشگاه آشنیه (۱۳ دیماه) ساعت ۱۵ الی ۱۶	administrator	اطلاعیه ها	بدون برچسب	۲۲ ساعت پیش منتشر شده
برگزاری مسابقات قهرمانی بسکتبال منطقه ۱۰	solimi	آخرین اخبار	بدون برچسب	۰۷ دی ۱۳۹۰ منتشر شده
نمایشگاه عکس عاشورایی	solimi	آخرین اخبار	بدون برچسب	۰۵ دی ۱۳۹۰ منتشر شده
معارفه مسئولان جدید حراست دانشگاه	solimi	آخرین اخبار	بدون برچسب	۲۰ آذر ۱۳۹۰ منتشر شده
کنفرانس نظام توسعه در بخش نفت و گاز	solimi	آخرین اخبار	بدون برچسب	۲۸ آذر ۱۳۹۰ منتشر شده
اطلاعیه شماره ۲ امور نظریه	solimi	اطلاعیه ها	بدون برچسب	۲۸ آذر ۱۳۹۰ منتشر شده

می توانید نحوه نمایش این صفحه را به چند روش سفارشی کنید:



می توانید ستونها را بر اساس نیازهایتان پنهان /نمایش دهید و بوسیله ی زبانه ی تنظیمات صفحه در مورد نمایش تعداد نوشته ها تصمیم گیری کنید می توانید با استفاده از پیوندهای متنی که در قسمت بالای سمت راست صفحه قرار دارند، فهرست نوشته ها را بر اساس وضعیت نوشته از صافی بگذرانید .وضعیت نوشته ها شامل: همه نوشته ها، نوشته های منتشر شده، پیشنویس ها و نوشته های زباله دان است .حالت پیشفرض نمایش همه نوشته هاست .

می توانید با استفاده از فهرست های کشویی در بالای لیست نوشته ها، لیست را طوری پالایش کنید که فقط نوشته های یک دسته خاص یا ماه خاص را نشان دهد .بعد از انتخاب، روی دکمه صافی کلیک کنید .علاوه بر این می توانید با کلیک روی نویسنده نوشته، دسته یا برچسب در لیست نوشته ها، این لیست را پالایش کنید .  
با حرکت بر روی هر ردیف از لیست نوشته ها می توانید پیوندهای عملیات قابل اجرا روی هر یک از آنها را مشاهده و بدین ترتیب نوشته را مدیریت کنید .عملیات زیر قابل اجرا است :

گزینه ویرایش شما را به صفحه ی ویرایش نوشته می برد .همچنین برای اینکار می توانید برروی عنوان نوشته کلیک کنید .گزینه ویرایش سریع، امکان ویرایش بخشهای مختلف نوشته را در همین صفحه برای شما ایجاد میکند .

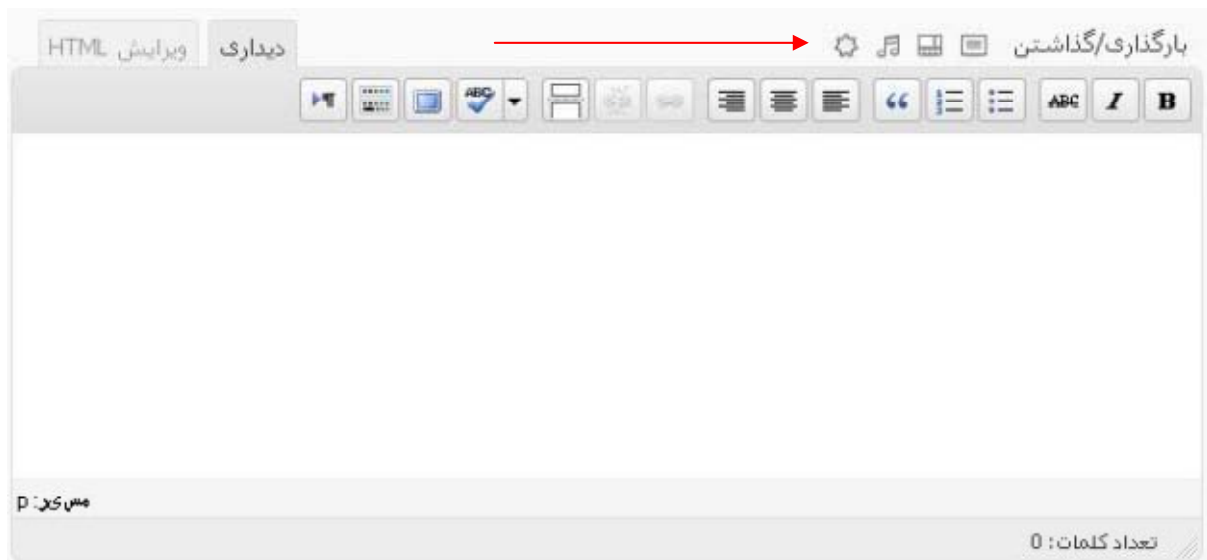
گزینه زباله دان نوشته شما را از این لیست حذف کرده و آن را به زباله دان انتقال میدهد .شما می توانید در آنجا نوشته را برای همیشه پاک کنید .با کلیک روی گزینه پیش نمایش می توانید ظاهر پس از انتشار نوشته های را که هنوز در حالت پیشنویس است، ببینید .با کلیک بر روی گزینه نمایش برای مشاهده نوشته خود به صورت مستقیم به سایت منتقل می شوید .وضعیت نوشته شما مشخص می سازد که از کدام یک از این دو گزینه را می توانید استفاده کنید .

می توانید همزمان چندین نوشته را با هم ویرایش کنید .با تیک زدن کنار هر نوشته، نوشته هایی را که میخواهید ویرایش کنید، انتخاب کنید .گزینه ویرایش را از فهرست کارهای دسته جمعی انتخاب و روی دکمه اجرا کلیک کنید . حال می توانید اطلاعات (دسته ها، نویسنده و ...) همه نوشته های کنار X انتخابی را یکجا ویرایش کنید .برای حذف هر نوشته از این گروه تنها کافیست روی علامت نام نوشته در ناحیه ویرایش دسته جمعی کلیک کنید .

## افزودن نوشته:

بخش عنوان و بخش محتوای نوشته ثابت هستند، ولی شما می‌توانید بقیه قسمت‌ها را با کشیدن و رها کردن به هر حالتی که دوست دارید در کنار هم بچینید. همچنین می‌توانید هر قسمت را از بخش تنظیمات صفحه پنهان کنید یا نمایش دهید و چیدمان صفحه را به حالت تک ستونه یا دو ستونه در بیاورید. عنوان - برای نوشته‌ی خود عنوانی انتخاب کنید، بعد از نوشتن عنوان در قسمت زیر می‌توانید پیوند یکتای نوشته را ویرایش کنید.


**ویرایشگر** - متن نوشته‌ی خود را وارد کنید. برای ویرایش مطالب دو راه وجود دارد، دیداری و HTML. برای انتخاب حالت موردنظر می‌توانید روی زبانه مربوطه کلیک کنید، در حالت دیداری شما یک ویرایشگر پیشرفته‌ی متن خواهید داشت، حالت HTML به شما امکان وارد کردن کدهای HTML را میدهد.



شما همچنین می توانید پرونده های چندرسانه ای را با استفاده از دکمه های بالای ویرایشگر وارد نوشته ی خود کنید.

## افزودن عکس :

بارگذاری/گذاشتن

با انتخاب  می توان به متن مربوطه عکس هم اضافه کرد. با انتخاب این گزینه پنجره ای باز می شود،



می توان عکس مربوطه را از رایانه خود، یا از کتابخانه پرونده های چندرسانه ای (اگر عکسی در کتابخانه موجود باشد)، پس از انتخاب بر روی بارگذاری کلیک می کنیم،

## افزودن پرونده‌ی چندرسانه‌ای از روی رایانه‌ی خودتان

بارگذاری

بیشترین اندازه پرونده برای بارگذاری: 2MB

<p>نام پرونده: c510-camera-sample-42.jpg</p> <p>نوع پرونده: image/jpeg</p> <p>تاریخ بارگذاری: ژانویه 1, 2011</p> <p>ابعاد: 2048 × 1536</p>	
<input type="text" value="c510-camera-sample-4"/>	نام
<input type="text"/>	متن جایگزین
<p>یک متن جایگزین برای تصویر، مثلاً "حکیم ابوالقاسم فردوسی"</p>	
<input type="text"/>	نام
<input type="text"/>	توضیح
<input type="text" value="http://profsite.sttu.ac.ir/masadi/files/2010/12/c510-camera-sample-42.jpg"/>	نشانی (URL) پیوند
<p><input type="button" value="هیچ کدام"/> <input type="button" value="نشانی پرونده"/> <input type="button" value="نشانی نوشته"/></p> <p>نشانی یک پیوند را وارد کنید، می‌توانید از بالا یک نشانی از پیش تعیین شده را برگزینید.</p>	
<p> <input checked="" type="radio"/> هیچ کدام                   <input type="radio"/> چپ                   <input type="radio"/> میانه                   <input type="radio"/> راست  <input checked="" type="radio"/> اندازه کامل                   <input type="radio"/> بزرگ                   <input type="radio"/> میانه                   <input type="radio"/> بند انگشتی             </p> <p> <input type="button" value="باز کردن"/>                   <input type="button" value="استفاده به عنوان تصویر شاخص"/>                   <input type="button" value="گذاشتن در نوشته"/> </p>	<p>چیدمان</p> <p>اندازه</p>

بر روی گذاشتن در نوشته کلیک می‌کنید، عکس به نوشته اضافه می‌شود، اگر بروی عکس کلیک کنید در گوشه سمت چپ چنین شکلی را می‌بیند با کلیک بر روی صفحه‌ای باز می‌شود،

تنظیمات پیشرفته ویرایش تصویر

اندازه

70%  
75%  
80%  
85%  
90%  
95%  
100%  
105%  
110%  
115%  
120%  
125%  
130%

چیدمان

ویرایش عنوان تصویر

ویرایش متن جایگزین

ویرایش توضیح تصویر

نشانی (URL) پیوند

c510-camera-sample-4

//profsite.sttu.ac.ir/masadi/files/2011/01/c510-camera-sample-4.jpg

پیوند به تصویر پیوند کنونی شیخ کدام

نشانی یک پیوند را وارد کنید می‌توانید از بالا یک نشانی از پیش تعیین شده را برگزینید.

لغو به‌روزرسانی

که می‌توان در این صفحه عکس را ویرایش کرد، و یا در قسمت تنظیمات پیشرفته اندازه عکس را تغییر داد و در آخر بروی به روز رسانی کلیک می‌کنیم، با انتخاب می‌توان فایل تصویری به نوشته اضافه کرد، با انتخاب می‌توان فایل صوتی به نوشته اضافه کرد، با انتخاب می‌توان فایل‌های دارای پسوند pdf، doc و غیره که برای گذاشتن جزوات بر روی سایت استفاده می‌شود.

**انتشار** - تنظیمات مربوط به انتشار نوشته در جعبه انتشار قابل انجام است. برای تعیین وضعیت، نمایانی و انتشار (سریع) روی پیوند ویرایش کلیک کنید تا گزینه‌های بیشتری در اختیار تان قرار گیرد. با ویرایش گزینه‌های مربوط به نمایانی می‌توانید برای نوشته خود رمز بگذارید یا کاری کنید یک نوشته همیشه بالای وبلاگتان دیده شود (سنجاقشده) انتشار (فوری) این امکان را به شما می‌دهد تا تاریخ و ساعت خاصی را برای انتشار نوشته تان انتخاب کنید، پس شما می‌توانید با زمانبندی، نوشته‌های را در گذشته یا آینده منتشر کنید.



## برچسب های نوشته:

با استفاده از برچسب های نوشته می توانید کلمات کلیدی را به نوشته ها اختصاص دهید. برچسب ها بر خلاف دسته ها از سلسله مراتب پیروی نمیکنند؛ به عبارت دیگر ارتباطی بین یک برچسب و دیگری وجود ندارد. برچسب ها معمولاً کیدواژههایی غیررسمی هستند که اطلاعات مهم نوشته (اسامی، سوژهها و غیره) را که ممکن است در سایر نوشته ها نیز تکرار شوند، مشخص میسازند. اگر به سایت خود به چشم یک کتاب نگاه کنید دسته ها مانند فهرست مطالب و برچسب ها مانند اصطلاحات مندرج در نمایه هستند.

## رسانه :

سایت دانشگاه تربیت معلم سبزوار

فرستادن رسانه‌ی جدید | Howdy, administrator | مدیر شبکه (16) | بدون رفتن

کتابخانه پرونده‌های چندرسانه‌ای

افزودن پرونده

جست‌وجوی چندرسانه‌ای

همه (117) | تصویر (106) | پیوست‌نشده (59)

کارهای دسته‌جمعی | اجرا | نمایش شیمی تاریخها | صافی

مورد 117

تاریخ	پیوست‌شده به	نویسنده	پرونده
1 ساعت پیش	پیش‌نویس خودکار, 2012/01/03	administrator	A.JPG
2012/01/01	(پیوست‌نشده) پیوست	administrator	f فرم نظر خواهی از مدیر گروه DOC
2012/01/01	(پیوست‌نشده) پیوست	administrator	f فرم نظر خواهی از رئیس دانشکده DOC
2012/01/01	(پیوست‌نشده) پیوست	administrator	بخشنامه ۱۰۰۱۲۲ در خصوص شیوه نامه آیین نامه ارتقا PDF

رسانه

کتابخانه

افزودن پرونده

پیوندها

برگه‌ها

دیدگاه‌ها

Slides

Slides

Add New

Slideshows

Settings

تمامی پرونده‌هایی که بارگذاری نموده‌اید، به ترتیب تاریخ بارگذاری، در کتابخانه‌ی پرونده‌های چندرسانه‌ای لیست شده‌اند. می‌توانید با استفاده از زبانه تنظیمات صفحه‌نحوه نمایش این صفحه را دلخواه و سفارشی کنید. می‌توانید لیست را بر اساس نوع پرونده‌ها و وضعیت آنها، با استفاده از پیوندهای بالای صفحه نمایش مرتب/جزیی تر کنید. همچنین می‌توانید لیست را بر اساس تاریخ و با استفاده از صافی بالای آن بازچینی و مرتب کنید. با حرکت نشانگر روی هر ردیف، پیوندهای ویرایش، پاک کردن دائمی و نمایش ظاهر میشوند. با کلیک روی ویرایش یا نام پرونده رسانه صفحه ساده‌ای برای ویرایش اطلاعات آن پرونده باز می‌شود. با کلیک روی پاک کردن دائمی پرونده از کتابخانه رسانه‌ای (و سایر نوشته‌هایی که به آنها پیوست شده است) پاک می‌شود. با کلیک روی نمایش به صفحه نمایش پرونده موردنظر می‌روید.

اگر یک پرونده‌ی چندرسانه‌ای به هیچ نوشته‌ای پیوست نشده باشد، این مورد را در ستون پیوست شده می‌بینید، با کلیک بر روی پیوست میتوان نوشته یا برگه‌ای به آن پیوست کرد.

تاریخ

پیوست‌شده به

نویسنده

پرونده

1 ساعت پیش

0

پیش‌نویس خودکار, 2012/01/03

administrator

A.JPG

ویرایش | پاک کردن برای همیشه | نمایش

و می‌توانید با کلیک بر روی پیوست در پنجره کوچکی که باز می‌شود، به دنبال نوشته‌ها بگردید و پرونده را به آن نوشته پیوست کنید.

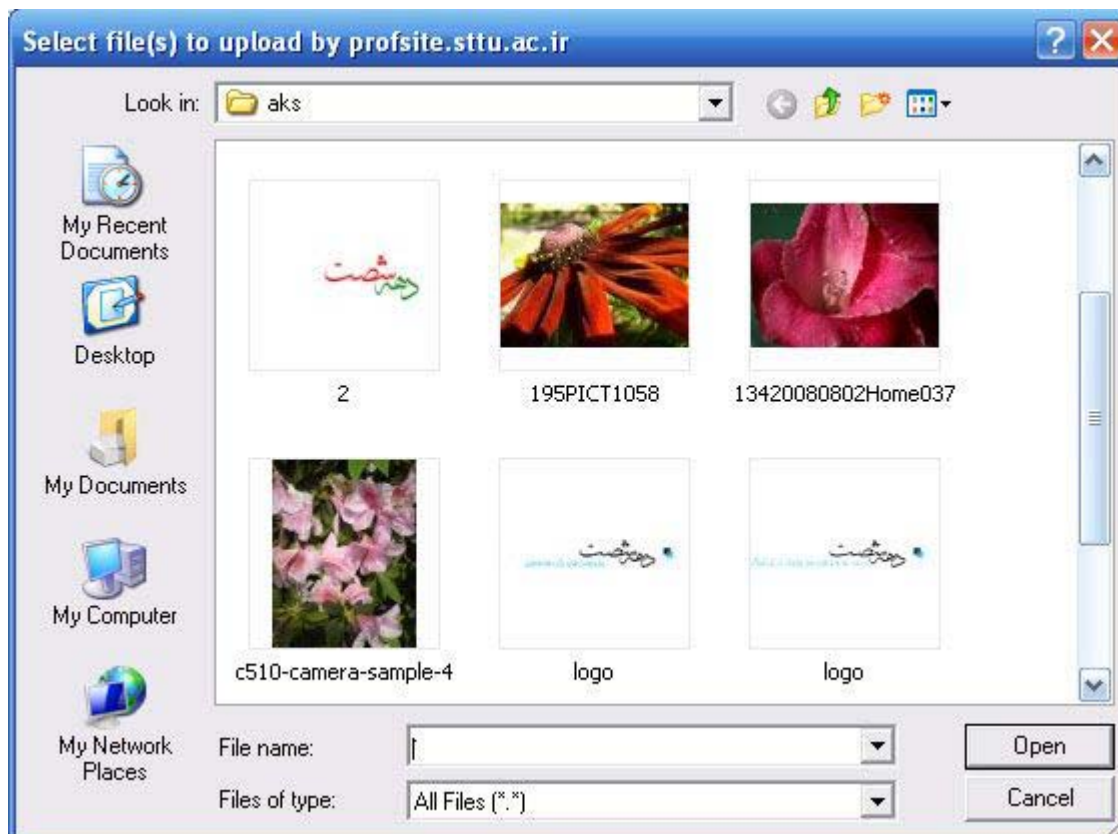




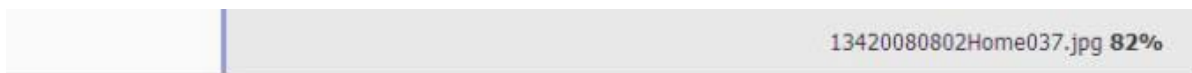
## افزودن پرونده:

دو گزینه برای بارگذاری پرونده‌ها وجود دارد: انتخاب پرونده‌ها برای شما یک بارگذار فلش آماده میکند که توسط آن می‌توانید به صورت همزمان چندین پرونده را بارگذاری کنید. همچنین می‌توانید از بارگذار مرورگر استفاده کنید. بعد از کلیک انتخاب پرونده‌ها یک پنجره باز خواهد شد که پرونده‌های رایانه‌ی شما را نمایش خواهد داد،





کلیک کرده تا عملیات بارگذاری آغاز Open پس از انتخاب پرونده ها در آن پنجره روی دکمه ی شود.



بعد از بارگذاری پرونده ها می توانید تصاویر بارگذاری شده را توسط یک ویرایشگر ساده ویرایش نمایید.

بعد از اعمال تغییرات برای ذخیره کردن، بروی به روز رسانی کلیک کنید.



## برگه ها:

سایت دانشگاه تربیت معلم سبزوار | مدیریت شبکه (16) | بیرون رفتن | Howdy, administrator | برگه تازه

ویرایش 3.3 آماده است | لطفاً هم اکنون به روز رسانی کنید.

برگه ها | افزودن برگه

همه (49) | منتشر شده (4%) | پیش نویس (1) | در انتظار بررسی (2)

کارهای دسته جمعی | اجرا | نمایش همه تاریخها | صاف

تاریخ	نویسنده	عنوان
۰۶ مرداد ۱۳۹۰ آخرین مستکاری	admin	ارضا - در انتظار بررسی
۱۲ آرمیبهشت ۱۳۹۰ منتشر شده	admin	اطلاعیه ها
۰۶ مرداد ۱۳۹۰ منتشر شده	admin	آخرین اخبار
۰۶ مرداد ۱۳۹۰ منتشر شده	admin	اطلاعیه ها
۰۶ مرداد ۱۳۹۰ منتشر شده	admin	تعمیر تحصیلی
۰۶ مرداد ۱۳۹۰ منتشر شده	admin	دانشگاه
۰۳ شهریور ۱۳۹۰ منتشر شده	admin	دستور العمل شاک دانشگاه
۰۳ شهریور ۱۳۹۰	admin	معرفی اجمالی دانشگاه

نمایش

برگه ها مانند نوشته ها دارای عنوان، محتوای متنی و اطلاعات مرتبط هستند، اما برخلاف نوشته ها بخشی از فرایند مبتنی بر ترتیب زمانی جاری در وبلاگ نیستند، در واقع برگه ها به نوعی نوشته هایی دائمی هستند. برگه ها دسته بندی یا برچسب گذاری نمی شوند. با این حال می توان نوعی سلسله مراتب برای آنها تعیین کرد. برای ایجاد گروهی از برگه ها میتوان یک برگه را به عنوان مادر انتخاب کرد و سایر برگه ها را در گروه مورد نظر قرار داد.

مدیریت برگه ها بسیار شبیه به مدیریت نوشته ها است و بخش مدیریت برگه ها نیز میتواند به همان روش شخصی سازی شود. همه این کارها را میتوان روی برگه ها نیز انجام داد: کوچکتر کردن لیست برگه ها با استفاده از صافی ها، اجرای عملیات مختلف روی برگه با استفاده از پیوندهای نمایان شده پس از حرکت روی ردیف ها یا ویرایش همزمان اطلاعات چند برگه با استفاده از فهرست کارهای دسته جمعی.

## افزودن برگه ها:

نوشتن برگه ها بسیار شبیه به نوشتن نوشته ها است، همانطور که صفحه ی نوشتن نوشته هایتان را سفارشی میکنید می توانید صفحه نوشتن برگه ها را نیز با استفاده از کشیدن و رها کردن، زبانه تنظیمات صفحه و جعبه های باز و بسته شونده به دلخواه سفارشی کنید. ویرایشگر برگه تقریباً شبیه به ویرایشگر نوشته عمل میکند با این تفاوت که گزینه هایی برای ویرایش برگه ها در جعبه مربوط به صفات آنها وجود دارد:

**مادر** - شما می توانید برگه های خود را به صورت سلسله مراتبی مرتب کنید. برای نمونه شما می توانید برگه های با نام درباره من داشته باشید و برای این برگه، زیربرگه هایی با نام های دوران کودکی و سابقه کاری بسازید. محدودیتی برای تعداد و ژرفای این زیربرگه ها وجود ندارد.

**قالب** - برخی از پوسته ها ممکن است، قالبهای دلخواهی برای برگه هایی خاص با امکانات اضافی و یا ظاهر متفاوت داشته باشند. در این صورت، شما آنها را اینجا ببینید.

**چیدمان** - صفحه ها معمولاً براساس حروف الفبا مرتب شده اند. اما شما می توانید ترتیب خود را بوسیله ی وارد کردن یک عدد (مثلاً 1 برای اولی) در این کادر وارد کنید.

## دیدگاه:



شما می توانید دیدگاهها را مانند نوشته ها و دیگر موارد مدیریت کنید. این صفحه مانند دیگر صفحات مدیریتی قابل سفارشی شدن است و شما می توانید گزینه های مدیریت دیدگاهها را با حرکت موشواره بر روی هر یک از آنها مشاهده و تغییرات خود را اعمال کنید. ردیف زرد به این معنیست که دیدگاه در انتظار بررسی شماست.

نویسنده دیدگاه IP در ستون نویسنده علاوه بر نام نویسنده، آدرس ایمیل، آدرس وبلاگ و آدرس نوشته IP نیز نشان داده می شود. با کلیک روی این پیوند، همه دیدگاههایی که با این آدرس شده اند، به نمایش درمی آید.

نوشته شده و به دنبال آن تاریخ و "ارسال شده در" در ستون دیدگاه ها، در بالای هر دیدگاه عبارت زمان ارسال دیدگاه مشاهده می شود. کلیک بر روی پیوند تاریخ زمان، شما را به صفحه ی سایتتان که شامل آن دیدگاه است می برد. در ستون "در پاسخ به" سه عنصر وجود دارد. متن، نام نوشته های است که دیدگاه در پاسخ به آن نوشته شده و پیوندی برای ورود به ویرایشگر همان نوشته است. نماد پیوند یکتا "#" که در پایین قابل مشاهده است، شما را به نوشته مورد نظر در سایت هدایت میکند. حباب کوچکی که در آن عدد نوشته شده است، تعداد دیدگاههای نوشته را نشان میدهد. اگر حباب خاکستری بود، همه دیدگاههای نوشته بازبینی شده اند. اگر حباب آبی بود، دیدگاهی در انتظار بازبینی برای آن نوشته وجود دارد. با کلیک بر روی حباب، تنها دیدگاههای نوشته مورد نظر در صفحه نمایش دیدگاه ها نشان داده میشوند.





## اسلاید :

The image shows the 'Slides' management interface. At the top, there is a search bar and a 'Slides' button. Below it, there is a table with the following columns: Date, Slide Link, Slide Title, and Slide Image. The table contains four rows of slide information. A red arrow points to the 'Add New' button in the top right corner. Another red arrow points to the 'Slides' menu item in the right sidebar.

Date	Slide Link	Slide Title	Slide Image
۱۱ دی ۱۳۹۰ آخرین دست‌کاری	No Link	امام موسی کاظم - پیش‌نویس فرمایش   فرمایش سوره   ولادت	
۲۶ آذر ۱۳۹۰ آخرین دست‌کاری	No Link	هفته پژوهش - پیش‌نویس	
۰۷ آذر ۱۳۹۰ آخرین دست‌کاری	No Link	مخبره - در انتظار بررسی	
۲۹ آبان ۱۳۹۰ آخرین دست‌کاری	No Link	کتاب - در انتظار بررسی	

با کلیک کردن روی گزینه **slides** تصاویری را که جهت نمایش در اسلایدهو افزوده اید قابل مشاهده، ویرایش و زباله دان می باشد. با انتخاب **add new** می توانید تصویر مورد نظر را در اندازه ۲۸۰\*۵۸۳ به اسلایدهو اضافه نمایید. با انتخاب **add new** پنجره زیر مشاهده خواهد شد:

سایت دانشگاه تربیت معلم سبزوار

Howdy, administrator | مدیر شبکه (16) | بیرون رفتی

نویسنده: 33 آماده است | لطفا هم اکنون به روز رسانی کنید.

انتشار

دخیره پیش نویس

وضعیت: پیش نویس کتابخانه

نمایش: عمومی نمایش

انتشار فوری

۱۲ دی / ۱۳۹۰ در ۰۹:۰۲

انتقال به نهالستان

انتشار

Slideshows

بیشتر استفاده شده

All Slideshows

عنوان را وارد نمایید

Slide Image (583x280)

قرار دادن تصویر تصویر شاخص

Slide Link

Add the URL this slide should link to

پیشخوان

پیشخوان

سایت های من

نویسندگان

نوشته ها

افزودن نوشته

دسته ها

برچسب های نوشته

رسانه

کتابخانه

افزودن پرونده

پیوندها

برگه ها

دیدگاه ها

Slides

Slides

Add New

Slideshows

Settings

پس از درج عنوان، بر روی قرار دادن به عنوان تصویر شاخص کلیک نمایید:

از رایانه از نشانی کتابخانه پرونده های چند رسانه ای NextGEN Gallery

افزودن پرونده های چند رسانه ای از روی رایانه خودتان

گزینه پرونده برای بارگذاری

پرونده فوری

بیشترین اندازه پرونده برای بارگذاری: 1MB

شما از ارسال کننده Flash استفاده می کنید، مشکلی هست؟ می توانید از [ارسال کننده معمولی](#) استفاده کنید.

پس از اینکه یک پرونده فرستاده شد، شما می توانید به آن نام و توضیحات بیاورید.

فرار دادن به عنوان تصویر شاخص

پیشخوان

پیشخوان

سایت های من

نویسندگان

نوشته ها

افزودن نوشته

دسته ها

برچسب های نوشته

رسانه

کتابخانه

افزودن پرونده

پیوندها

برگه ها

دیدگاه ها

Slides

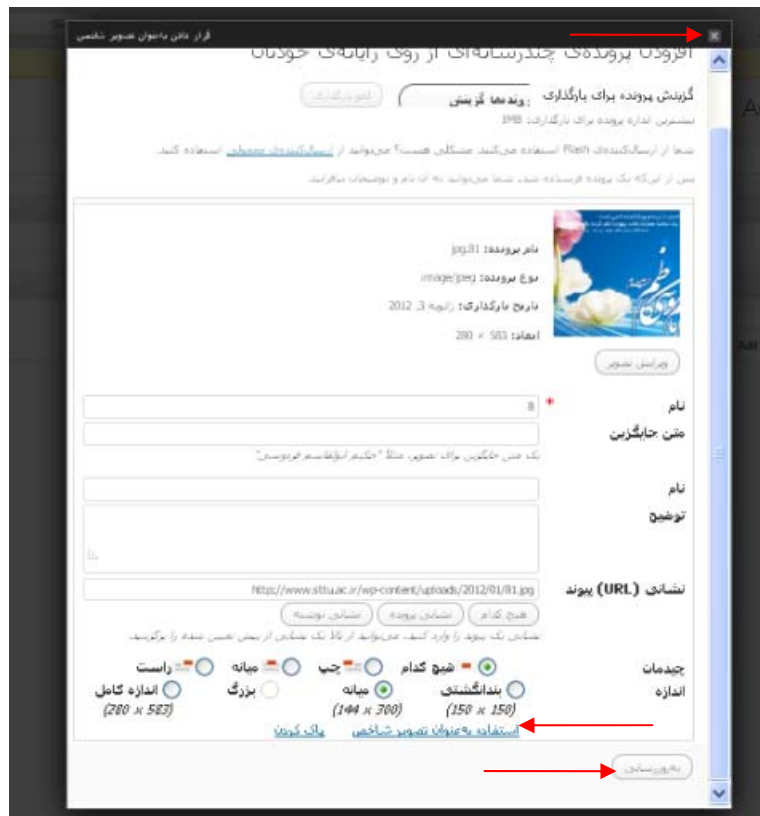
Slides

Add New

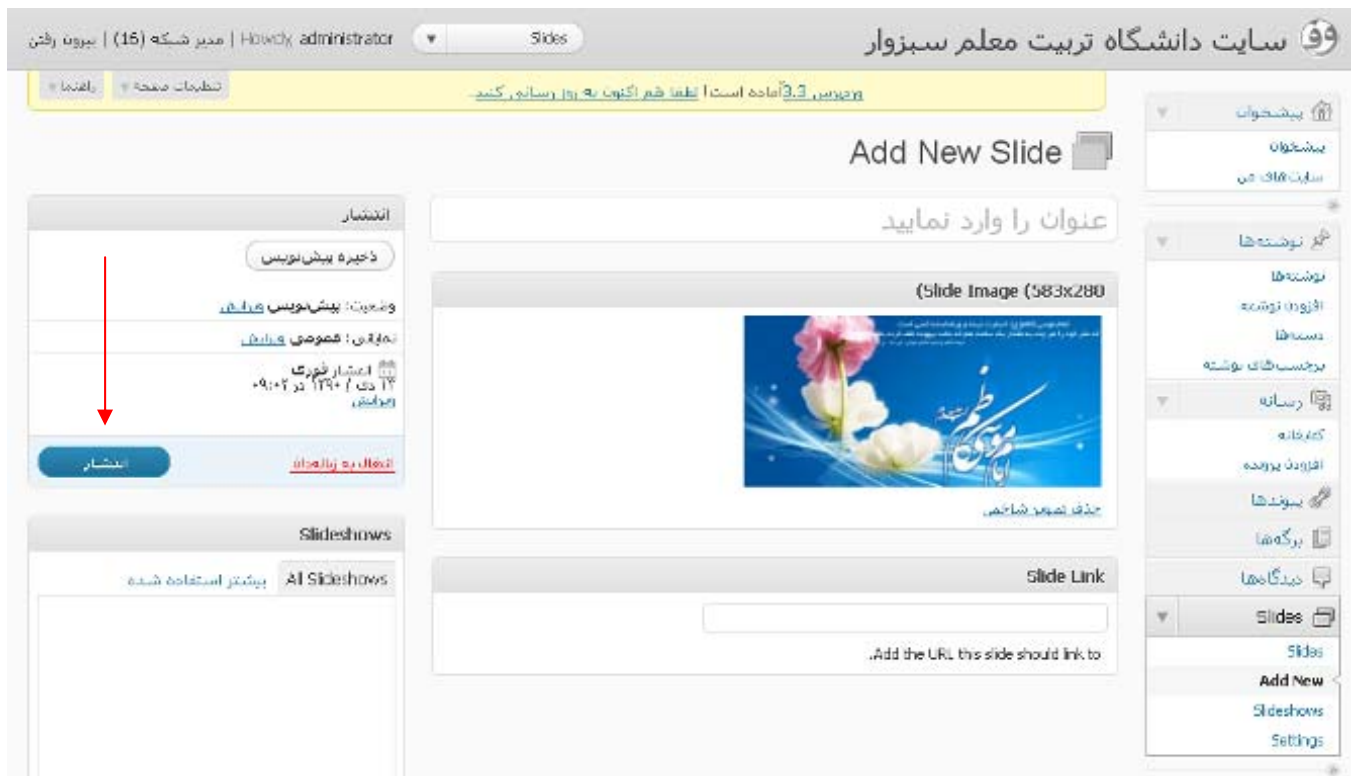
Slideshows

Settings

می توان عکس مربوطه را از رایانه خود، یا از کتابخانه پرونده های چند رسانه ای (اگر عکسی در کتابخانه موجود باشد)، پس از انتخاب بر روی استفاده به عنوان تصویر شاخص، و سپس به روزرسانی کلیک کرده و بعد پنجره را ببندید.



دکمه انتشار را انتخاب نمایید:





نمایش:

ابزارک ها:



ابزارک ها بخشهای مستقلی از محتوا هستند که در ناحیه ابزارک های پوسته (نام متداول آن ستون کناری است) جای میگیرند. ۴ ناحیه در سایت دانشگاه وجود دارد که به ترتیب عبارتند از: left – user – group - link



هر ناحیه حاوی ابزارک متن می باشند که با کلیک بر روی زبانه آن و باز شدن ابزارک می توانید کد **Html** موجود را ویرایش نمایید. بعنوان نمونه در ابزارک متن در ناحیه **link** این کدها موجود است:



## ویرایش کد **Html**:

برای درج اولین پیوند در ابزارک از کدی شبیه زیر استفاده می نمایم:

**<a href="http://www.sttu.ac.ir">دانشگاه حکیم سبزواری</a>**

عنوان پیوند  
آدرس سایت مورد نظر

همانطور که مشاهده می کنید این کد تشکیل شده است از آدرس سایت و عنوان آن.

برای درج عبارت های بعدی از کد زیر استفاده می کنیم:

**</li>**

**<a href="http://prof.sttu.ac.ir/profs/Authenticate.php">پورتال استادان</a>**

**</li>**

همانطور که مشاهده می نمایید تنها تفاوت این کد با کد قبلی اضافه شدن **<li>** به اول و **</li>** به آخر آن است.

**توجه:** برای تغییر تصاویر ناحیه **left** ابتدا باید عکس با اندازه  $۷۳*۲۱۸$  را از قسمت رسانه و افزودن پرونده آپلود نمایید:



سپس نشانی پرونده را مطابق زیر جایگزین عنوان پیوند نمایید:

```
<br>
<a href="http://ww.sttu.ac.ir/doc/olgoye%20poshesh.pps">
</a>
</br>
```

↑  
نشانی پرونده

## کاربران:



این صفحه تمام کاربران سایت شما را فهرست میکند . هر کاربر یکی از پنج نقشی که مدیر سایت برای او تعیین کرده است را دارد : مدیر، ویرایشگر، نویسنده، مشارکت کننده، یا مشترک . کاربران با نقشهای غیر از مدیر، بر اساس نوع نقش، در هنگام ورود به سیستم امکانات کمتری را مشاهده خواهند کرد.

می توانید با استفاده از زبانه تنظیمات صفحه و صافی های صفحه نمایش، شکل ظاهری اطلاعات به نمایش درآمده در این صفحه را مانند سایر صفحهها تغییر دهید. در قسمت شناس نامه شما می توانید اطلاعات مربوط به شناسنامه خودتان را تغییر دهید.

موفق باشید.

## فصل ۷

# راهنمای سیستم پشتیبانی و خدمات رسانی دانشگاه

در این فصل فایل راهنمای سیستم پشتیبانی و خدمات رسانی دانشگاه - که توسط آقای زاهدی نژاد آماده شده است - مستقیماً درج شده است.

## راهنمای سیستم پشتیبانی و خدمات رسانی دانشگاه (ticket)

سیستم پشتیبانی و خدمات رسانی دانشگاه با هدف تسریع در رفع مشکل کاربران تعبیه شده است. کاربران گرامی می توانند با مراجعه به سایت [سیستم پشتیبانی و خدمات رسانی](#) از امکانات موجود در سایت در جهت رفع مشکل خود استفاده نمایند.

The screenshot shows the user interface of the University IT Support System. At the top right, there is a logo and the text "سیستم پشتیبانی و خدمات رسانی" and "دانشگاه تربیت معلم سبزوار". The date "Jan 2012 23" is displayed on the left. The main content area is divided into several sections:

- رفع مشکل** (Problem Solving): Includes a description of the process and a "ورود" (Login) button.
- مرکز اطلاعات** (Information Center): A section for asking and answering questions.
- دائلودها** (Downloads): A list of available files for download.
- اخبار** (News): A section for the latest news and updates.
- پیشنشده ترین مباحث رفع اشکال** (Most Popular Troubleshooting Topics): A list of frequently asked questions.
- آخرین فایل ها برای دائلود** (Latest Files for Download): A list of recently added files.

At the bottom, there is a navigation bar with links for "دائلودها", "اخبار", "رفع مشکل", and "مرکز اطلاعات". The language is set to "Persian (I.R.)".

همانطور که در تصویر مشخص است تمام مراجعین به سایت قادر خواهند بود از مطالب موجود در مرکز اطلاعات، رفع مشکل، اخبار و دائلودها استفاده نمایند.

چنانچه کاربران پاسخ سوال خود را در ۴ بخش فوق دریافت نکردند، می توانند با شناسه و کلمه عبور Domain خود وارد سیستم شده و درخواست خود را برای بخش مورد نظر ارسال نمایند:



در صفحه باز شده پس از تعیین اولویت و درج موضوع ، متن پیام خود را وارد نمایید. چنانچه نیاز به ضمیمه کردن فایلی باشد میتواند با انتخاب گزینه Browse فایل را آپلود نماید

سیستم پشتیبانی و خدمات رسانی  
دانشگاه تربیت معلم سبزوار

مرکز پشتیبانی « ارسال درخواست » عمومی

ارسال درخواست

اگر شما نمیتوانید مشکل خود را در بخش مرکز اطلاعات پیدا کنید، شما می توانید مشکل خود را با جزئیات آن ارسال نمایید.

اطلاعات کلی

اولویت:

جزئیات پیام

موضوع:

نمی توانم به شبکه دانشگاه متصل شوم

بروزرسانی فایل

Persian (I.R.) انتخاب زبان: | مشاهده تیکت | ارسال درخواست | مرکز اطلاعات | رفع مشکل | اخبار | دانلودها

با تأیید ، درخواست شما ارسال می گردد:

سیستم پشتیبانی و خدمات رسانی  
دانشگاه تربیت معلم سبزوار

مرکز پشتیبانی « ارسال درخواست » عمومی

ارسال درخواست

درخواست شما برای بخش مربوطه ارسال شد، یکی از همکاران در اولین فرصت به درخواست شما رسیدگی خواهد کرد.

اطلاعات درخواست

شماره درخواست:	LEV-329084
بخش:	عمومی
نام:	علی زاهدی
پست الکترونیک:	a.zahedi@sttu.ac.ir
اولویت:	معمولی

قطعی شبکه

نمی توانم به شبکه دانشگاه متصل شوم

Persian (I.R.) انتخاب زبان: | مشاهده تیکت | ارسال درخواست | مرکز اطلاعات | رفع مشکل | اخبار | دانلودها

شما می توانید درخواست خود را از بخش مشاهده درخواست در صفحه اول پیگیری نمایید:



مرکز پشتیبانی « لیست درخواست ها »

لیست درخواست ها

لیست زیر درخواستهای ارسالی شماست، شما می توانید با کلیک بر روی هر درخواست نحوه رسیدگی به آن را مشاهده نمایید.

صفحه 1 از 1

بخش	اولویت	وضعیت	آخرین پاسخگو	شماره درخواست
عمومی <td>معمولی <td>باز</td> <td>علی زاهدی</td> <td>LEV-329084</td> </td>	معمولی <td>باز</td> <td>علی زاهدی</td> <td>LEV-329084</td>	باز	علی زاهدی	LEV-329084

[خروج] حساب کاربری >

نام کاربری: **علی زاهدی**

جستجو

جستجو

-- بخشهای پشتیبانی --

در بخش مشاهده درخواست ها، لیست درخواست های شما موجود می باشد که با کلیک بر روی هر مورد میتوانید جزئیات آن را مشاهده کنید.



مرکز پشتیبانی « لیست درخواست ها » LEV-329084

قطعی شبکه >

جزئیات درخواست

شماره درخواست:	LEV-329084	بخش:	عمومی
وضعیت:	باز	اولویت:	معمولی
زمان ایجاد:	25 Jan 2012 4:30 AM	آخرین تغییر:	25 Jan 2012 4:30 AM

[خروج] حساب کاربری >

نام کاربری: **علی زاهدی**

جستجو

جستجو

-- بخشهای پشتیبانی --

ارسال پاسخ

گفتگو

**علی زاهدی** USER

25 Jan 2012 4:30 AM ارسال در: 25

نمی توانم به شبکه دانشگاه متصل شوم

ضمیمه (jpg) (87.11 KB.011)

بازگشت

موفق باشید