



## امنیت پست الکترونیکی



- ✓ مفاهیم پایه‌ای پست الکترونیکی
- ✓ مخاطرات پست الکترونیکی
- ✓ مکانیزم‌های ایمن‌سازی پست الکترونیکی
- ✓ پروتکل‌های پست الکترونیکی
- ✓ ارائه روشی نوین برای ارزیابی مخاطرات پست الکترونیکی
- ✓ ایمن‌سازی مخاطرات پست الکترونیکی بر اساس نوع سازمان

امنیت پست الکترونیکی

سید حسین رجاء



درباره این کتاب: از ویژگی‌های این کتاب ارائه روشی نوین برای ارزیابی مخاطرات پست الکترونیکی و نیز، ایمن‌سازی مخاطرات پست الکترونیکی، بر اساس نوع سازمان می‌باشد. مطالب متعددی بر اساس این کتاب، در همایش‌ها و مجلات از سوی نویسنده ارائه شده و به چاپ رسیده است. مخاطبین اصلی کتاب، کارشناسان پست الکترونیکی، کارشناسان امنیت، مدیران شبکه، دانشجویان نرم‌افزار، متخصصین لینوکس و علاقه‌مندان به حوزه پست الکترونیکی می‌باشند.

درباره نویسنده: سید حسین رجاء کارشناس ارشد فناوری اطلاعات (IT) مؤسسه تحقیقاتی دانش‌محلی پیشرفته می‌باشد. وی ۱۴ سال سابقه فعالیت در زمینه‌های شبکه، امنیت شبکه و برنامه‌نویسی را دارد. از جمله مدارک علمی ایشان می‌توان به CCSP, RHCSA, CCIE Routing and Switching و LPI 3 اشاره کرد. وی منصب راهاندازی و مدیریت سرورهای Exchange Server و Qmail, Sendmail, Postfix, Exim در زمینه پست الکترونیکی را تجربه کرده است.

مؤلف: مهندس سید حسین رجاء  
 کارشناس ارشد فناوری اطلاعات  
 مؤسسه تحقیقاتی دانش‌محلی پیشرفته



www.PendarePars.com



# امنیت پست الکترونیکی

سید حسین رجاء

انتشارات پندار پارس

سرشناسه	: رجاء، سيد حسين، ۱۳۶۲ -
عنوان و نام پديدآور	: امنيت پست الكترونيكي / حسين رجاء.
مشخصات نشر	: تهران : پندار پارس: مانلي، ۱۳۹۰.
مشخصات ظاهري	: ۱۶۰، XI ص: مصور، نمودار.
شابك	: ۹۷۸-۶۰۰-۶۵۲۹-۰۰-۴ ريال: ۴۵۰۰۰
وضعيت فهرست نويسي	: فيبا
موضوع	: پست الكترونيكي -- پيش بيني هاي ايمني
موضوع	: پست الكترونيكي
رده بندي كنگره	: TK۵۱۰۵/۷۳۰۷۳ ۱۳۹۰ الف ۳ /
رده بندي ديويي	: ۶۹۲/۰۰۴
شماره كتابشناسي ملي	: ۲۵۹۶۴۲۷

#### انتشارات پندار پارس



دفتري فروش: انقلاب، ابتداي كارگرجنوبي، كوچه رشتجي، شماره ۱۴، واحد ۱۶ [www.pendarepars.com](http://www.pendarepars.com)  
 تلفن: ۶۶۵۷۲۳۳۵ - تلفكس: ۶۶۹۲۶۵۷۸ همراه: ۰۹۱۲۲۴۵۲۳۴۸  
[info@pendarepars.com](mailto:info@pendarepars.com)



نام كتاب : امنيت پست الكترونيكي

ناشر : انتشارات پندار پارس ناشر همكار: مانلي

تاليف : سيد حسين رجاء

چاپ نخست : زمستان ۹۰

شمارگان : ۱۰۰۰ نسخه

طرح جلد : محمد اسماعيلي هدي

ليتوگرافي، چاپ، صحافي : ترام سنچ، فرشيوه، خيام

قيمت : ۴۵۰۰ تومان شابك : ۹۷۸-۶۰۰-۶۵۲۹-۰۰-۴



\*هرگونه كبي برداري، نكتير و چاپ كاغذي يا الكترونيكي از اين كتاب بدون اجازه ناشر تخلف بوده و پيگرد قانوني دارد\*

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

## تقدیم به:

سید و سالار شهیدان، حضرت امام حسین(ع)

و

ساحت مقدس مولایمان حضرت مهدی(عج) که

حضرت امام موسی کاظم(ع) در توصیف فرزند

عزیزشان فرموده‌اند:

او طرد شده تنهایی خرابه است ...

## به نام خداوند جان و خرد

### پیش‌گفتار

فن‌آوری پست الکترونیکی، با توجه به استفاده روز افزون از آن در عصر اطلاعات، به یکی از ملزومات زندگی بشر، برای مکاتبات و مراسلات بین افراد، تبدیل شده است. با توجه به این مسئله، نکته قابل اهمیت در مورد پست الکترونیکی این است که سرور و سرویس پست الکترونیکی و پیام‌ها و مکاتبات رد و بدل شده بین افراد، دارای امنیت قابل قبولی باشد تا افراد با اطمینان خاطر از این فن‌آوری، استفاده کنند.

ابتدا به بررسی نحوه عملکرد سیستم پست الکترونیکی و معرفی پروتکل‌های آن می‌پردازیم. با بررسی صورت گرفته مشخص شد که برای ارزیابی مخاطرات سیستم پست الکترونیکی، روش خاصی ارائه نشده است.

با بررسی روش‌های ارزیابی سایر سیستم‌ها و نقاط ضعف و قوت آنها، از روش آقای کانوری که روشی برای ارزیابی در حیطه امنیت شبکه می‌باشد، برای ارزیابی مخاطرات پست الکترونیکی استفاده می‌کنیم. با ارائه جداول خاص و استفاده از فرمول کانوری، به بررسی مخاطرات می‌پردازیم که معیار کار ما برای ارزیابی مخاطرات می‌باشد. پس از آن، به معرفی و بحث بر روی مخاطرات موجود در سرور و سرویس پست الکترونیکی می‌پردازیم.

سپس به مکانیزم‌های امن کردن مخاطرات سرور و سرویس پست الکترونیکی می‌پردازیم. میزان کاهش مخاطره را با به‌کارگیری مکانیزم‌ها و راهکارهای موجود، به صورت مطالعه موردی و به وسیله آزمایش‌هایی بدست می‌آوریم. در نهایت و در فصل نتیجه‌گیری، پست الکترونیکی را از لحاظ امنیت و نوع سازمان، دسته‌بندی کرده و مکانیزم‌های ایمن‌سازی آن را ارائه می‌دهیم.

مخاطبین اصلی کتاب، کارشناسان پست الکترونیکی، کارشناسان امنیت، مدیران شبکه، دانشجویان رشته نرم افزار، متخصصین لینوکس و تمامی افراد علاقه‌مند به حوزه پست الکترونیکی می‌باشند.

این کتاب با توجه به مطالعات علمی و تجربه فنی نگارنده در سرورهای پست الکترونیکی Qmail، Postfix، Sendmail، Exim و Exchange Server تألیف شده است. بدیهی است که مطالب این کتاب، خالی از اشکال نمی‌باشد و نظرات خوانندگان، ما را در بهبود سطح علمی و فنی کتاب، یاری خواهد کرد؛ لذا از خوانندگان محترم درخواست می‌شود هرگونه پیشنهاد و انتقادی در جهت بهبود و اصلاح محتویات کتاب را به آدرس الکترونیکی [hosseinraja@dspr.i.com](mailto:hosseinraja@dspr.i.com) ارسال نمایند.

در نهایت بر خود لازم می‌دانم از موسسه تحقیقاتی داده‌سنجی پیشرفته، جناب مهندس مقدسی و جناب مهندس سید محمد رجاء، که اینجانب را در مراحل مختلف تألیف این کتاب یاری رسانده‌اند، کمال تشکر را داشته باشم.

سید حسین رجاء

پاییز ۱۳۹۰

## فهرست

فصل اول مقدمه.....	۱
۱-۱ طرح مسئله.....	۱
۲-۱ اهداف.....	۴
۳-۱ پرسش‌ها و فرضیات.....	۴
۴-۱ تحقیقات مرتبط.....	۶
۵-۱ ساختار کتاب.....	۸
فصل دوم مفاهیم پایه.....	۱۱
۱-۲ اصول پست الکترونیکی.....	۱۱
۱-۱-۲ سیستم‌های پست الکترونیکی لینوکسی.....	۱۱
MDA.....	۱۲
فیلترگذاری خودکار پست الکترونیکی.....	۱۳
پاسخگویی خودکار پست الکترونیکی.....	۱۴
مقداردهی اولیه برنامه توسط پست الکترونیکی.....	۱۵
MTA.....	۱۵
MUA.....	۱۷
محل ذخیره پیام‌ها.....	۱۷
چگونگی نمایش پیام‌ها.....	۱۷
۲-۱-۲ پروتکل‌های پست الکترونیکی.....	۱۸
پروتکل‌های MTA.....	۱۸
پروتکل SMTP.....	۱۸
پروتکل ESMTP.....	۱۹



۱۹.....	پروتکل‌های MUA	۱۹
۱۹.....	پروتکل POP	۱۹
۲۱.....	پروتکل SMTP	۲-۲
۲۱.....	دستورات کلاینتی SMTP	۱-۲-۲
۲۳.....	پاسخ‌های سرور	۲-۲-۲
۲۴.....	پروتکل‌های POP و IMAP	۳-۲
۲۵.....	MIME	۴-۲
۲۶.....	برنامه Uuencode	۱-۴-۲
۲۶.....	MIME و داده‌های باینری	۲-۴-۲
۲۶.....	فیلدهای سرآیند MIME	۳-۴-۲
۲۷.....	فیلد Content-Transfer-Encoding	
۲۸.....	فیلد Content-Type	
۲۹.....	Multipart Content-Type	
۲۹.....	دسته بندی حملات	۵-۲
۳۰.....	نتایج حمله	۶-۲
۳۳.....	<b>فصل سوم مخاطرات</b>	
۳۳.....	ارزیابی مخاطرات سیستم‌های پست الکترونیکی	۱-۳
۳۵.....	احتمال کلی و تأثیر	۱-۱-۳
۳۵.....	روش‌های دیگر	۲-۱-۳
۳۶.....	روش کانوری	۳-۱-۳
۳۷.....	عناصر جدول ارائه شده	۴-۱-۳
۳۹.....	مخاطرات سرور پست الکترونیکی	۲-۳
۳۹.....	مخاطرات سرورهای خانواده یونیکس	۱-۲-۳

۳۹.....	حملات شبکه ای.....
۳۹.....	دسترسی شبکه ای.....
۴۱.....	۲-۲-۲ مخاطرات بسته‌های پست الکترونیکی Sendmail, Qmail و Postfix.....
۴۱.....	بسته پست الکترونیکی Sendmail.....
۴۲.....	بسته پست الکترونیکی Qmail.....
۴۵.....	بسته پست الکترونیکی Postfix.....
۴۵.....	برنامه‌های اصلی postfix.....
۴۷.....	صف‌های پیام postfix.....
۴۷.....	برنامه‌های کاربردی postfix.....
۴۸.....	برنامه‌های پیکربندی postfix.....
۴۸.....	جدول lookup در postfix.....
۴۹.....	مخاطرات موجود در بسته‌های پست الکترونیکی postfix و qmail, sendmail.....
۴۹.....	نداشتن مجوز مناسب فایل.....
۴۹.....	کاربری با سطح دسترسی بالا.....
۵۰.....	۳-۲-۳ Open Relays.....
۵۲.....	۴-۲-۳ Spam.....
۵۴.....	۵-۲-۳ ویروس‌ها.....
۵۵.....	۳-۳ مخاطرات سرویس پست الکترونیکی.....
۵۵.....	۱-۳-۳ سوء استفاده از برخی دستورات و کاوش گری.....
۶۰.....	۲-۳-۳ سوء استفاده از سرآیندهای پست الکترونیکی.....
۶۱.....	فیلد سرآیند TO.....
۶۴.....	۳-۳-۳ مخاطره نا امن بودن محتوای پیام‌ها.....
۶۵.....	۴-۳-۳ نا امن بودن سرورهای IMAP و POP3.....

۶۶.....	۵-۳-۳ Webmail نا امن بودن
۶۷.....	۴-۳ جدول و نمودار کلی
۶۹.....	<b>فصل چهارم راهکارهای ایمن سازی</b>
۶۹.....	۱-۴ ایمن سازی سرور پست الکترونیکی
۷۰.....	۱-۱-۴ ایمن سازی سرورهای خانواده یونیکس
۷۰.....	مانیتورینگ فایل‌های Log
۷۱.....	جلوگیری از حملات شبکه ای
۷۱.....	بلوکه کردن دسترسی شبکه ای به سرور
۷۲.....	استفاده کردن از سیستم‌های IDS یا IPS
۷۳.....	محاسبه میزان کاهش مخاطره
۷۵.....	۲-۱-۴ ایمن سازی بسته پست الکترونیکی Sendmail
۷۵.....	مجوزهای فایل
۷۵.....	کاربران sendmail
۷۶.....	۳-۱-۴ Qmail و امنیت
۷۷.....	محاسبه میزان کاهش مخاطره
۷۸.....	۴-۱-۴ postfix و امنیت
۷۸.....	۵-۱-۴ اجتناب از open relay
۷۹.....	پیکربندی رله گزینشی
۷۹.....	پیکربندی رله گزینشی در Sendmail
۸۰.....	پیکربندی رله گزینشی در Qmail
۸۱.....	استفاده از برنامه tcpwrapper
۸۱.....	پیکربندی tcpwrapper
۸۲.....	پیکربندی tcpserver

۸۳.....	اجتناب کردن از open relay ها
۸۳.....	محاسبه میزان کاهش مخاطره
۸۵.....	۶-۱-۴ بلوکه کردن Spam ها
۸۶.....	ممانعت کردن از قبول پیامها از میزبانهای spam مشهور
۸۶.....	ایجاد لیست خودتان از میزبانهای spam
۸۷.....	استفاده از ارائه دهنده لیست میزبانهای spam
۸۷.....	اعتبار سنجی اطلاعات جلسه smtp
۸۸.....	فیلتر کردن پست الکترونیکیهای spam
۸۸.....	پیاده سازی بلوکه کردن spam روی Qmail
۸۸.....	ایجاد لیست خودتان از میزبانهای spam
۸۹.....	استفاده از سرور MAPS RSS
۸۹.....	استفاده از فیلتر کردن پیامها
۹۱.....	محاسبه میزان کاهش مخاطره
۹۳.....	۷-۱-۴ فیلتر کردن ویروسها
۹۳.....	فیلتر کردن ویروس بر اساس عبارات شناخته شده
۹۴.....	پویش کردن ویروسها
۹۵.....	پیاده سازی فیلترینگ ویروس
۹۶.....	پیاده سازی پویش کردن ویروس
۹۷.....	محاسبه میزان کاهش مخاطره
۹۷.....	۲-۴ ایمن سازی سرویس پست الکترونیکی
۹۸.....	۱-۲-۴ استفاده از فایروالهای پست الکترونیکی
۹۸.....	غیر فعال کردن برخی دستورات [2]
۹۹.....	ردیابی سرآیندها

۹۹.....	فیلد سرآیند Received
۱۰۱.....	فیلد سرآیند Message-Id
۱۰۱.....	فایروال‌های پست الکترونیکی
۱۰۲.....	درون فایروال شبکه
۱۰۲.....	درون DMZ
۱۰۳.....	به عنوان یک سرور پست الکترونیکی داخلی
۱۰۴.....	محاسبه میزان کاهش مخاطره
۱۰۵.....	استفاده از SASL ۳-۲-۴
۱۰۶.....	SASL چیست؟
۱۰۶.....	SASL چگونه عمل می‌کند؟
۱۰۷.....	مکانیزم‌های تایید هویت SASL
۱۰۷.....	استفاده از SASL درون SMTP
۱۰۹.....	محاسبه میزان کاهش مخاطره
۱۱۰.....	S-MIME ۴-۲-۴
۱۱۰.....	S-MIME Multipart SubType
۱۱۱.....	S-MIME Application SubType
۱۱۲.....	MIME به همراه PGP
۱۱۳.....	محاسبه میزان کاهش مخاطره
۱۱۳.....	امن کردن سرورهای IMAP و POP3 ۵-۲-۴
۱۱۴.....	پروتکل‌های خانواده SSL
۱۱۴.....	پروتکل SSL
۱۱۵.....	پروتکل Record SSL
۱۱۶.....	پروتکل دست دهی SSL

۱۱۷.....	پروتکل تغییر مشخصات رمز SSL
۱۱۸.....	پروتکل هشدار دهنده SSL
۱۱۹.....	پروتکل TLS
۱۲۰.....	بسته OpenSSL
۱۲۳.....	محاسبه میزان کاهش مخاطره
۱۲۴.....	۶-۲-۴ امن کردن سرورهای Webmail
۱۲۴.....	امن کردن سرور MySQL
۱۲۴.....	امن کردن سرور Apache
۱۲۵.....	محاسبه میزان کاهش مخاطره
۱۲۶.....	۳-۴ جدول و نمودار کلی
۱۲۹.....	<b>فصل پنجم نتیجه‌گیری و پیشنهادات</b>
۱۲۹.....	۱-۵ نتیجه‌گیری
۱۳۲.....	۱-۱-۵ پست الکترونیکی‌های با امنیت متوسط برای سازمان‌های اجرایی
۱۳۳.....	۲-۱-۵ پست الکترونیکی‌های با امنیت بالا برای سازمان‌های ملی
۱۳۵.....	۳-۱-۵ پست الکترونیکی با امنیت بالا به همراه محرمانگی، برای سازمان‌های حساس
۱۳۹.....	<b>فصل ششم مراجع و منابع</b>



## درباره مؤلف:

سید حسین رجاء کارشناس ارشد فناوری اطلاعات (IT) موسسه تحقیقاتی داده سنجی پیشرفته می باشد. وی حدوداً ۱۴ سال فعالیت در زمینه های مختلف IT، من جمله تدریس، برنامه نویسی، شبکه و امنیت شبکه را تجربه کرده است. ایشان علاوه بر موسسه تحقیقاتی داده سنجی پیشرفته، موسسه آموزش عالی خیام، شرکت مسیر فن آوری اطلاعات و شرکت فن آوران رجحان را در کارنامه کاری خود دارد. از جمله مدارک علمی ایشان می توان به CCIE Routing and Switching، CCSP، RHCS و LPI 3(301 Open Ldap, 302 Mixed Environment, 303 Security, 305 Mail) اشاره کرد. وی در زمینه پست الکترونیکی، نصب، راه اندازی و مدیریت سرورهای Qmail، Sendmail، Postfix، Exim و Exchange Server را تجربه کرده است.

## درباره این کتاب:

این کتاب به مسئله امنیت پست الکترونیکی می پردازد. ابتدا مفاهیم پست الکترونیکی و نحوه عملکرد پست الکترونیکی را خواهیم آموخت. در ادامه مخاطرات پست الکترونیکی، معرفی شده و به نحوه ایمن سازی آنها اشاره خواهیم کرد. از ویژگی های مهم این کتاب، ارائه روشی نوین برای ارزیابی مخاطرات پست الکترونیکی و همچنین، ایمن سازی مخاطرات پست الکترونیکی، بر اساس نوع سازمان می باشد. بر اساس این کتاب، مقالات متعددی در همایش ها و مجلات از سوی نویسندگان ارائه شده و به چاپ رسیده است. مخاطبین اصلی کتاب، کارشناسان پست الکترونیکی، کارشناسان امنیت، مدیران شبکه، دانشجویان رشته نرم افزار، متخصصین لینوکس و تمامی افراد علاقه مند به حوزه پست الکترونیکی می باشند.



# فصل اول

## مقدمه

### ۱-۱ طرح مسئله

سال‌ها پیش، زمانی که پست الکترونیکی و رایانه‌ای وجود نداشت و سیستم مراسلات به صورت کاغذی و به شکل نامه بود، افراد از فاش شدن محتوای نامه خود هراس داشتند. مسائل مالی، از بین رفتن آبرو و حیثیت اشخاص، مسائل سیاسی، اجتماعی و فرهنگی از جمله دلایلی بودند که فکر امن کردن مراسلات و سیستم آن را به وجود آورد.

با پیشرفت علم و ورود به عرصه رایانه، بشر سیستم جدیدی برای مراسلاتش به وجود آورد. سیستم جدید که همان پست الکترونیکی بود، کار نامه کاغذی را با سرعتی بسیار بالاتر انجام می‌داد. همانند سیستم سنتی، مسئله‌ای که وجود داشت، بحث امنیت پیام‌های رد و بدل شده و همچنین امنیت سیستم ارسال مراسلات بود. البته اهمیت امنیت سیستم الکترونیکی، نسبت سیستم سابق، فزونی می‌یابد. در عصر اطلاعات، بسیاری از تراکنش‌ها چه مالی و چه غیرمالی، به صورت الکترونیکی انجام می‌شوند، تبادل داده‌ها از طریق اینترنت صورت می‌گیرد و سرقت و دست‌کاری و لو رفتن داده‌ها می‌تواند هزینه‌ای گزاف از حیث آبرویی، مالی، سیاسی، اقتصادی و فرهنگی داشته باشد.

در حوزه مراسلات الکترونیکی که پست الکترونیکی باشد، نیز این مسئله وجود دارد و بسی حائز اهمیت است [1].

در حوزه پست الکترونیکی، پروتکل‌ها و مکانیزم‌های مختلفی وجود دارد و درون این پروتکل‌ها و مکانیزم‌ها، انواع مخاطرات وجود دارد. مسئله مهم آن است که:

- مخاطرات را بشناسیم.
- چگونه این مخاطرات را ارزیابی کنیم.
- چگونه این مخاطرات را، از طریق مکانیزم‌های موجود، ایمن نماییم و مخاطره را کاهش دهیم.

## Thank You for previewing this eBook

You can read the full version of this eBook in different formats:

- HTML (Free /Available to everyone)
- PDF / TXT (Available to V.I.P. members. Free Standard members can access up to 5 PDF/TXT eBooks per month each month)
- Epub & Mobipocket (Exclusive to V.I.P. members)

To download this full book, simply select the format you desire below

