



# حفاظت شخصی در تهدیدات سایبری

گردآوری و تألیف

معاونت پژوهش و تولید علم

دانشگاه اطلاعات

مؤسسه چاپ و انتشارات

۱۳۹۵

حفاظت شخصی در تهدیدات سایبری - گردآوری و تدوین معاونت پژوهش و تولید علم. تهران: مؤسسه

چاپ و انتشارات دانشگاه اطلاعات، ۱۳۹۵

۰۲۴۵ - اول، صور، نمودار. - (شماره: ۲۶۴)

کتابنامه

۱. شبکه‌های کامپیوتری - اقدامات تأمینی ۲. تدابیر ایمنی ۳. فضای مجازی ۴. تکنولوژی اطلاعات

الف. دانشکده اطلاعات معاونت پژوهش و تولید علم

۱۳۹۵ ح/۷۲/۱۰۵/۵

#### مشخصات:

عنوان: حفاظت شخصی در تهدیدات سایبری

گردآوری و تدوین: معاونت پژوهش و تولید علم

ناشر: مؤسسه چاپ و انتشارات دانشگاه اطلاعات

شمارگان: ۱۰۰۰ نسخه

تاریخ انتشار: ۱۳۹۵

نوبت چاپ: اول

بهاء: ۱۷۰۰۰۰ ریال

شابک: ۱ - ۸۸ - ۷۸۱۳ - ۶۰۰ - ۹۷۸

«تمامی حقوق این اثر محفوظ است. تکثیر یا تولید مجدد آن کلی یا جزئی به هر صورت

(چاپ، فتوکپی، صوت، تصویر و انتشار الکترونیکی) بدون اجازه مکتوب ناشر ممنوع است.»

شماره تلفن: ۲۲۴۶۹۷۳۹

تهران: صندوق پستی ۱۶۷۶۵-۱۴۳۸

## مقدمه نادر

همزمان با گسترش استفاده از کامپیوترهای شخصی، مطرح شدن شبکه‌های کامپیوتری و به دنبال آن اینترنت به عنوان بزرگ‌ترین شبکه جهانی، حیات کامپیوترها و دیگر ابزار دیجیتال و کاربران آن دستخوش تغییرات اساسی شده است. به منظور استفاده از دستاوردها و مزایای فن‌آوری اطلاعات و جلوگیری از آسیب‌های احتمالی آن شناخت زوایای پنهان، رعایت اصول خاص و امنیتی و تهدید جدی به تمام مؤلفه‌های تأثیرگذار جزء مسائل اجتناب‌ناپذیر هستند. پرداختن به مفوله امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری و ارتباطی در هر کشور مستلزم توجه تمامی کاربران و سیاست‌گذاران به جایگاه امنیت اطلاعات و ارتباطات بوده و می‌بایست به آن توجه در سطح کلان و از بعد منافع ملی نگاه کرد. وجود ضعف امنیتی در شبکه‌های کامپیوتری و اطلاعاتی، عدم آموزش و توجیه صحیح کاربران نسبت به جایگاه و اهمیت بحث امنیت و حفاظت از وسایل ارتباط دیجیتال، عدم وجود دستورالعمل‌های لازم برای پیشگیری از نقایص امنیتی مسائلی را به دنبال خواهد داشت که ضرر آن متوجه کاربران می‌باشد و در سطح کلان زیرساخت اطلاعاتی یک کشور را می‌تواند در معرض آسیب و تهدید جدی قرار دهد.

امنیت اطلاعات و ایمن‌سازی کامپیوترها و ابزار ارتباطی درخصوص افرادی که دارای مشاغل اطلاعاتی و امنیتی هستند از اهمیتی مضاعف برخوردار است. افراد شاغل در مراکز نظامی و اطلاعاتی مقادیر زیادی اطلاعات مهم و قابل بهره‌برداری را بر روی

سیستم‌های کامپیوتری و تلفن‌های همراه خود دارند یا در حال تبادل این اطلاعات می‌باشند که به جهت آسیب‌پذیری‌های موجود در این خصوص، رعایت نکات حفاظتی چه در بعد شخصی و چه در بعد سازمانی و ملی بسیار حائز اهمیت است.

با وجود تمام مزایایی که تجارت الکترونیک به همراه دارد، انجام تراکنش‌ها و ارتباطات آنلاین محملی بزرگ‌تر برای سوءاستفاده از فن‌آوری و اعمال مجرمانه را فراهم می‌کند. امروزه هکرها و بزه‌کاران سایبری مترصد فرصت و سوءاستفاده از اشخاص و سازمان هستند. مزاحمت رایانه‌ای، سرقت هویت، کلاهبرداری از حکومت‌های بانکی، سرقت اطلاعات مالی و اعتباری، تهدید و ایجاد رعب طیف وسیعی از جرائم سایبری را نشان می‌دهد که دست‌اندرکاران می‌توانند بسیار گسترده و جبران‌ناپذیر باشند.

کتاب پیشرو راهکاری مشخص برای جلوگیری از مورد هدف قرار گرفتن و قربانی شدن در فضای سایبر را ارائه می‌دهد. آک، ساختن خوانندگان از چگونگی وقوع و از بین بردن خطرات احتمالی موضوعی است که این کتاب به آن پرداخته است. شما در این کتاب با بدافزارها، نقاط آسیب‌پذیری کامپیوتری و اینترنتی و در مقابل آنتی‌ویروس‌ها، نرم‌افزارها و توصیه‌های امنیتی و حفاظتی آشنا می‌شوید. گذرواژه و مخاطرات احتمالی مربوطه به آن، سرقت اطلاعات از طریق فیشینگ، سرقت شماره و رمز کارت بانکی، کلاهبرداری و سرقت اطلاعات مالی، تخلیه و حملات تلفنی و خیانت، تدابیر امنیتی لازم موضوعاتی هستند که این کتاب به خوبی به آنها پرداخته است. از دیگر نکات ارزشمند و جالب کتاب حاضر، ارائه خلاصه و نکات مهم و کاربردی در پایان هر فصل می‌باشد. در مجموع حفاظت از رایانه شخصی، داده‌ها و گذرواژه‌ها، حساب‌های کاربری آنلاین، کارت‌های اعتباری نقدی، تلفن همراه، شبکه‌ها و ابزار ارتباطی آنلاین مهم‌ترین عناوین این اثر را تشکیل می‌دهند. بخشی از کتاب حاضر برگرفته از اثری مشابه در زبان

انگلیسی<sup>۱</sup> می‌باشد.

با توجه به لزوم هوشیاری و اهمیت مضاعف آن برای کارکنان دستگاه‌های اطلاعاتی و امنیتی و ضرورت آگاه‌سازی جهت تغییر رفتارهای امنیتی دانشکده اطلاعات با انتخاب، ترجمه و ارائه این کتاب بر آن بوده است تا گامی در جهت تأمین هرچه بیشتر امنیت شخصی، سازمان و ملی بردارد.

معاونت پژوهش و تولید علم

1. Michael Bazzell (2013), Personal Digital Security: Protecting Yourself from online Crime, CCI Publishing.

## فهرست مطالب

|    |                                      |
|----|--------------------------------------|
| ۱۷ | فصل اول: از رایانه خود حفاظت کنید    |
| ۱۷ | ویندوز مایکروسافت                    |
| ۱۸ | ویندوز XP                            |
| ۱۹ | ویندوز سون                           |
| ۲۱ | مدافع ویندوز                         |
| ۲۱ | آنتی ویروس                           |
| ۲۲ | برنامه Microsoft Security Essentials |
| ۲۵ | برنامه AVG Free Edition              |
| ۲۸ | ویندوز ایت                           |
| ۳۰ | Secunia PSL                          |
| ۳۴ | نرم افزار WinPatrol PLUS             |
| ۳۵ | مجموعه ابزارهای امنیتی Sysinternals  |
| ۳۶ | از بین بردن بدافزارها                |
| ۳۷ | CCleaner                             |
| ۴۳ | برنامه Spybot                        |
| ۴۴ | برنامه                               |
| ۴۵ | رایاندهای آلوده                      |
| ۴۵ | ComboFix                             |

|    |                                            |
|----|--------------------------------------------|
| ۴۷ | فهرست پاکسازی                              |
| ۴۸ | نمونه‌ای از بدافزارها                      |
| ۵۳ | امنیت فیزیکی                               |
| ۵۳ | یواس بی درایوهای بدخواه                    |
| ۵۶ | قفل‌های الکترونیک هتل                      |
| ۵۸ | بازکردن قفل‌های اتومبیل                    |
| ۶۰ | کی لاگ‌های فیزیکی                          |
| ۶۱ | کی لاگ‌های نرم‌افزاری                      |
| ۶۴ | KL- Detector                               |
| ۶۵ | Macintosh                                  |
| ۷۱ | به‌روزرسانی سیستم عامل                     |
| ۷۱ | حذف پلاگین‌ها                              |
| ۷۳ | نمایش امضای دیجیتال یک نرم‌افزار در ویندوز |
| ۷۳ | اوانیکس                                    |
| ۷۴ | CCleaner                                   |
| ۷۵ | Sophos                                     |
| ۷۷ | خلاصه فصل                                  |

|    |                               |
|----|-------------------------------|
| ۷۹ | فصل دوم: حفاظت از گذرواژه‌ها  |
| ۷۹ | حمله به گذرواژه‌ها            |
| ۸۰ | حملات لغت‌نامه‌ای             |
| ۸۴ | حملات پر قدرت                 |
| ۸۷ | گذرواژه من چه اندازه امن است؟ |
| ۸۸ | گذرواژه‌های قوی               |
| ۹۳ | کی پس                         |

|          |                                                  |
|----------|--------------------------------------------------|
| ۹۶.....  | لست پس.....                                      |
| ۹۶.....  | پسورد اوتوسیو.....                               |
| ۹۹.....  | جستجوگر اینترنت.....                             |
| ۱۰۰..... | موزیلا فایرفاکس.....                             |
| ۱۰۱..... | گوگل کروم.....                                   |
| ۱۰۲..... | سافارم.....                                      |
| ۱۰۳..... | ورو خودکار.....                                  |
| ۱۰۴..... | مایکروسافت ویندوز.....                           |
| ۱۰۵..... | مکینتاش.....                                     |
| ۱۰۶..... | Ophcrack.....                                    |
| ۱۰۸..... | نکاتی درباره حفاظت از گذرواژه ها.....            |
| ۱۱۵..... | راه هایی برای مقابله با هکرها.....               |
| ۱۱۹..... | خلاصه فصل.....                                   |
| ۱۲۱..... | فصل سوم: حفاظت از حساب های کاربری آنلاین.....    |
| ۱۲۱..... | مدیریت گذرواژه حساب گوگل.....                    |
|          | چگونه می توان در گوگل درایو از شیت های گسترده به |
| ۱۲۳..... | کمک پسورد حفاظت کرد؟.....                        |
| ۱۲۷..... | حافظه های ابری دراپ باکس، اسکای درایو و.....     |
| ۱۲۹..... | حساب های ایمیل.....                              |
| ۱۳۵..... | فیشینگ موسسه مالی.....                           |
| ۱۳۸..... | مقابله با فیشینگ اطلاعات.....                    |
| ۱۴۱..... | فیشینگ اطلاعات محرمانه ایمیل.....                |
| ۱۴۶..... | فیشینگ اطلاعات محرمانه شبکه اجتماعی.....         |
| ۱۴۹..... | فیشینگ اطلاعات محرمانه خرید.....                 |

|     |                                         |
|-----|-----------------------------------------|
| ۱۵۰ | فیس تنک .....                           |
| ۱۵۲ | حملات ریست کردن گذرواژه .....           |
| ۱۵۵ | احراز هویت دو عاملی .....               |
| ۱۶۰ | فوروارد کردن ایمیل .....                |
| ۱۶۲ | آدرس خود را محرمانه نگه دارید .....     |
| ۱۶۶ | خلاصه فصل .....                         |
| ۱۶۷ | فصل چهارم حفاظت از داده‌ها .....        |
| ۱۶۷ | پشتیبان‌گیری از داده‌ها .....           |
| ۱۷۰ | پشتیبان‌گیری در سطح داده‌ها .....       |
| ۱۷۳ | پشتیبان‌گیری در خارج از محل .....       |
| ۱۷۴ | پشتیبان‌گیری ذخیره شده ابری .....       |
| ۱۷۵ | رمزنگاری داده‌ها .....                  |
| ۱۷۶ | نرم‌افزار TrueCrypt .....               |
| ۱۸۱ | بازیابی داده‌ها .....                   |
| ۱۸۲ | Recuva .....                            |
| ۱۸۳ | قابلیت‌های کلیدی نرم‌افزار Recuva ..... |
| ۱۸۶ | جلوگیری از بازیابی داده‌ها .....        |
| ۱۸۷ | پاک کردن فضای خالی .....                |
| ۱۸۸ | پاک کردن کل درایو .....                 |
| ۱۸۹ | نرم‌افزار همتا به همتا .....            |
| ۱۹۴ | منبع ذخیره‌سازی اسناد ابری .....        |
| ۱۹۸ | اسناد فراداده .....                     |
| ۲۰۴ | خلاصه فصل .....                         |

|     |                                                                    |
|-----|--------------------------------------------------------------------|
| ۲۰۷ | فصل پنجم: حفاظت از کارت‌های اعتباری و کارت‌های نقدی                |
| ۲۰۷ | گزارش اعتبار رایگان                                                |
| ۲۱۱ | صرف‌نظر از اعتبار                                                  |
| ۲۱۲ | هشدار درباره کلاهبرداری                                            |
| ۲۱۴ | اصول و فرآیند محافظت از کارت‌های اعتباری                           |
| ۲۱۵ | دستورالعمل‌ها                                                      |
| ۲۱۷ | مسدود کردن اعتبار                                                  |
| ۲۲۳ | کارت‌های اعتباری فعلی                                              |
| ۲۲۴ | کپی کردن کارت اعتباری                                              |
| ۲۲۷ | اسکن کردن کارت                                                     |
| ۲۳۳ | قربانی شدن در محل خرید                                             |
| ۲۳۶ | کارت‌های اعتباری مجازی                                             |
| ۲۳۶ | کارت‌های اعتباری پیش پرداخته                                       |
| ۲۳۸ | گرمین دات                                                          |
| ۲۳۸ | تعیین آسیب‌پذیری‌ها                                                |
| ۲۴۲ | نیاز به کارت نقدی داشتن                                            |
| ۲۴۴ | استاندارد امنیت اطلاعات در کارت‌های اعتباری                        |
| ۲۴۴ | PCI DSS چیست؟                                                      |
| ۲۴۵ | الزامات استاندارد PCI DSS                                          |
| ۲۴۷ | تعیین قوانین امنیتی جدید برای کارخانجات کارت‌های اعتباری           |
| ۲۴۹ | استفاده از فن‌آوری در مواجهه با تهاجمات سایبری به کارت‌های اعتباری |
| ۲۵۰ | انتشار محصولی جدید توسط شورای استانداردهای امنیتی PCI              |
| ۲۵۱ | استفاده از گذرواژه‌های یک‌بارمصرف با استفاده از توکن               |
| ۲۵۲ | شناسایی و اعتبارسنجی                                               |
| ۲۵۲ | کاربر و گذرواژه‌های ثابت                                           |

|     |                                                          |
|-----|----------------------------------------------------------|
| ۲۵۳ | ..... کاربر و گذرواژه‌های یک‌بارمصرف                     |
| ۲۵۳ | ..... گذرواژه‌های یک‌بارمصرف با توکن همگام               |
| ۲۵۴ | ..... گذرواژه یک‌بارمصرف با توکن غیرهمگام                |
| ۲۵۴ | ..... توکن و اعتبارسنجی دومرحله‌ای                       |
| ۲۵۵ | ..... حل مشکل مقیاس‌پذیری در استفاده از توکن‌ها          |
| ۲۵۶ | ..... نتیجه‌گیری                                         |
| ۲۵۶ | ..... خلاصه فصل                                          |
| ۲۵۷ | ..... فصل ششم: حفاظت از تان شخصی خود                     |
| ۲۵۷ | ..... رمز عبور                                           |
| ۲۵۸ | ..... چرا به یک رمز عبور نیاز است؟                       |
| ۲۵۹ | ..... چگونه می‌توان یک رمز عبور خوب راریف کرد؟           |
| ۲۶۱ | ..... شش روش برای حفاظت از اطلاعات                       |
| ۲۶۵ | ..... آنتی‌ویروس                                         |
| ۲۶۷ | ..... اندروید                                            |
| ۲۶۸ | ..... آنتی‌ویروس‌های برتر سال‌های اخیر جهان برای اندروید |
| ۲۸۱ | ..... تست مشترکی از آنتی‌ویروس‌ها                        |
| ۲۸۲ | ..... آیفون                                              |
| ۲۸۲ | ..... بلک‌بری                                            |
| ۲۸۳ | ..... تلفن‌های ویندوز                                    |
| ۲۸۳ | ..... مجازها                                             |
| ۲۸۶ | ..... نرم‌افزار ردیابی                                   |
| ۲۸۶ | ..... اندروید - نقشه دوم                                 |
| ۲۸۸ | ..... آیفون فایو                                         |
| ۲۸۸ | ..... بلوتوث                                             |

|     |                                                        |
|-----|--------------------------------------------------------|
| ۲۹۱ | ..... داده‌های EXIF                                    |
| ۲۹۷ | ..... خلاصه فصل                                        |
| ۲۹۹ | ..... فصل هفتم: حفاظت از خود در برابر دیگر حملات تلفنی |
| ۲۹۹ | ..... کالر آی دی                                       |
| ۳۰۲ | ..... کلاهبرداری در کار هیئت منصفه                     |
| ۳۰۲ | ..... کلاهبرداری بزرسی اف بی آی                        |
| ۳۰۳ | ..... کلاهبرداری خرید ساختگی                           |
| ۳۰۳ | ..... کلاهبرداری در خرید                               |
| ۳۰۴ | ..... دردسر نوه                                        |
| ۳۰۵ | ..... نظرسنجی‌های تلفنی                                |
| ۳۰۵ | ..... پایگاه داده مشتری                                |
| ۳۰۶ | ..... اطلاعات شبکه                                     |
| ۳۰۷ | ..... داده‌های خصوصی                                   |
| ۳۰۸ | ..... فاکتورهای تقلبی                                  |
| ۳۱۰ | ..... کلاهبرداری بله / خیر                             |
| ۳۱۲ | ..... مهندسی اجتماعی                                   |
| ۳۱۶ | ..... انتقال خط تلفن                                   |
| ۳۱۸ | ..... خلاصه فصل                                        |
| ۳۱۹ | ..... فصل هشتم: حفاظت از ابزارهای آنلاین               |
| ۳۲۰ | ..... دوربین‌های نظارتی                                |
| ۳۲۳ | ..... دستگاه‌های کپی                                   |
| ۳۲۶ | ..... شודان                                            |
| ۳۲۶ | ..... هارد درایوها                                     |

|     |       |                                                  |
|-----|-------|--------------------------------------------------|
| ۳۲۷ | ..... | ترموسات ها                                       |
| ۳۲۸ | ..... | وب کم ها                                         |
| ۳۳۰ | ..... | اتوماسیون خانگی و سیستم های هشدار                |
| ۳۳۶ | ..... | خلاصه فصل                                        |
| ۳۳۷ | ..... | فصل نهم: حفاظت از شبکه های وایرلس                |
| ۳۳۸ | ..... | وایرلس خانگی                                     |
| ۳۴۵ | ..... | وای فای عمومی                                    |
| ۳۵۲ | ..... | شبکه های وای فای نقل                             |
| ۳۵۴ | ..... | خلاصه فصل                                        |
| ۳۵۹ | ..... | فصل دهم: حفاظت از کودکان                         |
| ۳۶۱ | ..... | صحبت کردن                                        |
| ۳۶۲ | ..... | پیام های جنسی                                    |
| ۳۶۳ | ..... | تاریخچه                                          |
| ۳۶۳ | ..... | جستجوگر اینترنت                                  |
| ۳۶۴ | ..... | فایرفاکس                                         |
| ۳۶۴ | ..... | کروم                                             |
| ۳۶۴ | ..... | سافاری                                           |
| ۳۶۶ | ..... | پایش حساب های کاربری کودکان                      |
| ۳۶۶ | ..... | فیس بوک                                          |
| ۳۷۳ | ..... | حفاظت از حریم خصوصی کودکان در فیس بوک            |
| ۳۷۴ | ..... | نرم افزار حفاظت از کودکان در دنیای مجازی فیس بوک |
| ۳۷۵ | ..... | قفل امنیتی فیس بوک برای کودکان در انگلستان       |

|     |                               |
|-----|-------------------------------|
| ۳۷۵ | توثیق                         |
| ۳۸۱ | پایش زنده                     |
| ۳۸۴ | موتورهای جستجوی نام کاربری    |
| ۳۸۵ | وبسایت Knowem                 |
| ۳۸۵ | Name Check                    |
| ۳۸۶ | Check User Names              |
| ۳۸۶ | Nipl                          |
| ۳۸۷ | Google Blog Search            |
| ۳۸۷ | Google Alerts                 |
| ۳۹۱ | دسترسی به حساب کاربری فرزندان |
| ۳۹۲ | OS Forensics                  |
| ۳۹۶ | تاریخچه جستجو                 |
| ۳۹۷ | استفاده از رایانه             |
| ۳۹۸ | فروش آنلاین مواد مخدر         |
| ۴۰۰ | خلاصه فصل                     |

|     |                                                    |
|-----|----------------------------------------------------|
| ۴۱۷ | فصل یازدهم: حفاظت از خود در برابر شبکه‌های اجتماعی |
| ۴۱۹ | چگونه شبکه‌های اجتماعی را برای کارمندان ایمن کنیم؟ |
| ۴۲۱ | به کارمندان خود آموزش دهید                         |
| ۴۲۱ | ده نکته امنیتی شبکه‌های اجتماعی                    |

### فصل دوازدهم: شبکه‌های اجتماعی، فضای مجازی،

|     |                                                             |
|-----|-------------------------------------------------------------|
| ۴۲۵ | سواد رسانه‌ای و جامعه اسلامی                                |
| ۴۲۷ | انواع رسانه‌های اجتماعی                                     |
| ۴۳۶ | اثرات رسانه‌های اجتماعی بر سبک زندگی برخی از کاربردهای آنها |

۴۴۱ ..... کودکان و نوجوانان در شبکه‌های اجتماعی

۴۴۳ ..... سواد رسانه‌ای و فرهنگ تعامل با شبکه‌های اجتماعی

۴۵۵ ..... سخن آخر

www.ketab.ir