

امنیت اطلاعات:

از آگاهی تا آموزش

مؤلفان

دکتر محمد حسن زاده

عضو هیات علمی دانشگاه تربیت مدرس

مهندس نورگس جهانگیری

کارشناس ارشد آموزش و پرورش



تهران / ۱۳۹۰

حسن زاده، محمد، ۱۳۵۶ _

امنیت اطلاعات: از آگاهی تا آموزش / نوشته محمد حسن زاده، نرگس جهانگیری

تهران: کتابدار، ۱۳۹۰

۲۰۵ص: جدول، نمودار

فهرست نویسی بر اساس اطلاعات فیبا

موضوع: شبکه های کامپیوتری -- اقدامات تامینی

موضوع: تکنولوژی اطلاعات -- اقدامات تامینی

موضوع: کامپیوترها -- ایمنی اطلاعات

شناسه افزوده: جهانگیری، نرگس

رده بندی کنگره: ۱۳۹۰ ۸ الف ح ۵/۵/۱۰ TK۵۱۰

رده بندی دیویی: ۰۰۵/۸

شماره کتابشناسی ملی: ۲۶۰۹۶۸۷



www.ketabdar.org

mohseni@ketabdar.org

عنوان: امنیت اطلاعات: از آگاهی تا آموزش

مؤلفان: دکتر محمد حسن زاده، مهندس نرگس جهانگیری

مجموعه کتابدار: ۲۳۲، فناوری اطلاعات و ارتباطات: ۲۶

نوبت چاپ: اول، ۱۳۹۰ / شمارگان: ۱۵۰۰ نسخه

قیمت: ۶۰۰۰ تومان

شابک: ۹۷۸-۶۰۰-۲۴۱-۰۳۲-۰

تلفن: ۴-۸۸۴۸۱۳۵۳ / ۸۸۹۷۹۵۶۱

دورنگار: ۸۸۹۷۹۵۶۰ / همراه: ۰۹۱۲۱۸۸۳۵۸۱

نشانی پخش: کتابدار، تهران، صندوق پستی ۱۹۷۳ / ۱۴۱۵۵

فهرست مطالب

پیشگفتار مولفان.....	۱۱
----------------------	----

فصل اول

کلیات.....	۱۳
مقدمه.....	۱۳
عصر کنونی، عصر اطلاعات و دانش.....	۱۳
مفاهیم داده و اطلاعات.....	۱۵
داده.....	۱۵
اطلاعات.....	۱۵
اهمیت اطلاعات.....	۱۷
اهمیت و نقش اطلاعات در سازمان.....	۱۸

فصل دوم

مفاهیم امنیت اطلاعات.....	۲۱
امنیت چیست؟.....	۲۱
امنیت اطلاعات چیست؟.....	۲۱
اهمیت امنیت اطلاعات در سازمان.....	۲۳
تاریخچه امنیت اطلاعات.....	۲۵
امنیت اطلاعات در عصر کامپیوتر.....	۲۶
اینترنت و امنیت اطلاعات.....	۲۷
عناصر کلیدی در امنیت اطلاعات.....	۲۸
اصطلاحات امنیتی.....	۳۰
مزایای سرمایه گذاری در امنیت اطلاعات.....	۳۱
ضعف در بعد امنیت.....	۳۲
حوادث امنیتی.....	۳۳

فصل سوم

مروری بر مدلها و رویکردهای مدیریت امنیت اطلاعات.....	۳۷
مقدمه.....	۳۷
مدلهای مدیریت امنیت اطلاعات.....	۳۸
رویکردهای متفاوت مدیریت خطرات امنیتی در پیاده سازی امنیت اطلاعات.....	۵۰
جزئیات مدل امنیتی دفاع در عمق.....	۵۲

۵۵	بررسی لایه سیاست‌ها، رویه‌ها و اطلاع‌رسانی
۵۸	بررسی لایه امنیت فیزیکی
۶۱	بررسی لایه محدوده عملیاتی شبکه
۶۵	بررسی لایه شبکه داخلی
۶۸	بررسی لایه کامپیوترها و دستگاه‌های میزبان
۷۱	بررسی لایه برنامه‌های کاربردی
۷۳	بررسی لایه داده

فصل چهارم

۷۷	نقش عوامل مختلف در امنیت اطلاعات
۷۷	نقش عوامل مختلف در سازمان
۷۷	مقدمه
۷۷	لایه‌های امنیت اطلاعات
۷۹	عوامل مختلف در امنیت اطلاعات
۸۰	تکنولوژی
۸۲	فرایندها و عملیات
۸۳	افراد
۸۳	نقش عوامل غیر فنی در امنیت اطلاعات
۸۵	نقش عوامل انسانی در امنیت اطلاعات
۹۰	نمونه‌های از عوامل انسانی مرتبط با امنیت اطلاعات

فصل پنجم

۹۳	آگاهی از امنیت اطلاعات
۹۳	مقدمه
۹۳	سطوح آگاهی از امنیت اطلاعات
۹۴	سطح اول آگاهی امنیتی: دانش
۹۴	سطح دوم آگاهی امنیتی: نگرش
۹۵	سطح سوم آگاهی امنیتی: رفتار و بروندمی
۹۵	استراتژی ارزیابی آگاهی از امنیت اطلاعات کارمندان
۹۶	ارزیابی
۹۷	طراحی
۹۷	پیااده‌سازی و اجرا
۹۷	ارزیابی و بازخورد
۹۷	بشپتیانی

فصل ششم

۹۹	آموزش امنیت اطلاعات به کاربران
۹۹	آموزش امنیت اطلاعات به کاربران
۱۰۱	طیف دانش امنیت اطلاعات به کاربران

۱۰۲	سطوح یادگیری امنیت اطلاعات.....
۱۰۲	آگاهی.....
۱۰۳	تربیت.....
۱۰۳	آموزش.....
۱۰۳	تفاوت و مقایسه آگاهی، تربیت و آموزش.....
۱۰۴	متدلوژی آگاهی، تربیت و آموزش امنیت اطلاعات.....
۱۰۵	طراحی.....
۱۰۹	توسعه.....
۱۰۹	پیاده‌سازی.....
۱۱۱	پشتیبانی و حمایت.....

فصل هفتم

۱۱۳	گزارش یک مطالعه موردی و معرفی مدل.....
۱۱۳	گزارش یک مطالعه موردی و معرفی مدل.....

فصل هشتم

۱۱۷	گامهای عملی در آموزش امنیت اطلاعات.....
۱۱۷	پست الکترونیکی، ضمانت و هرزنامه.....
۱۱۸	ضمانت نامه‌های الکترونیکی.....
۱۱۹	مراحل لازم برای حفاظت خود و سایر افراد موجود در فهرست دفترچه آدرس.....
۱۲۰	هرزنامه.....
۱۲۱	متن نامه‌های الکترونیکی ناخواسته.....
۱۲۱	آدرس‌های پست الکترونیکی، چگونه جمع آوری می‌گردند؟.....
۱۲۳	چگونه می‌توان میزان هرزنامه را کاهش داد؟.....
۱۲۶	روش‌های حفاظت از اطلاعات.....
۱۳۱	مراقبت از داده‌های حساس.....
۱۳۳	فایل‌های حذف شده.....
۱۳۵	نحوه حفاظت و ایمن‌سازی سیستم.....
۱۳۵	انتخاب و حفاظت رمزهای عبور.....
۱۳۶	چرا به یک رمز عبور نیاز است؟.....
۱۳۶	چگونه می‌توان یک رمز عبور خوب را تعریف کرد؟.....
۱۳۸	نحوه حفاظت از رمزهای عبور.....
۱۳۹	مهندسی اجتماع.....
۱۳۹	یک حمله مهندسی اجتماعی چیست؟.....
۱۴۰	یک حمله Phishing چیست؟.....
۱۴۰	نحوه پیشگیری از حملات مهندسی اجتماعی و کلاهبرداری.....
۱۴۱	اقدامات لازم در صورت بروز تهاجم.....
۱۴۲	یادافزارها.....
۱۴۲	ویروس و آنتی ویروس.....

۱۴۳	انواع ویروس
۱۴۸	کرمها
۱۴۹	تراجانها
۱۴۹	آگهی افزار یا Adware
۱۴۹	وارز (Warez)
۱۵۰	بمبهای منطقی
۱۵۰	جمع بندی رادهای مقابله با بدافزارها
۱۵۲	تشخیص و پیشگیری از نرم افزارهای جاسوسی
۱۵۲	نرم افزارهای جاسوسی چیست؟
۱۵۳	نحوه تشخیص نرم افزارهای جاسوسی
۱۵۳	نحوه پیشگیری از نصب نرم افزارهای جاسوسی
۱۵۵	نحوه حذف نرم افزارهای جاسوسی
۱۵۵	تجسس کننده کلیدانزایی برای جاسوسی
۱۵۸	هک و انواع هکر
۱۶۲	آشنایی با محتویات فعال و کوکی
۱۶۳	محتویات فعال و انواع آن
۱۶۴	کوکی چیست؟
۱۶۵	انواع کوکی
۱۶۵	تفاوت http با https در امنیت اطلاعات
۱۶۷	دیواره آتش (فایروال) چیست؟
۱۶۷	انواع فایروال
۱۶۸	نحوه پیکربندی بهینه یک فایروال به چه صورت است؟
۱۶۹	VPN چیست؟
۱۶۹	دسته بندی شبکه خصوصی مجازی براساس رمزنگاری
۱۷۰	دسته بندی VPN براساس لایه پیاده سازی
۱۷۱	دسته بندی VPN براساس کارکرد تجاری
۱۷۲	امضای دیجیتال
۱۷۲	نحوه عملکرد یک امضای دیجیتال
۱۷۳	نحوه ایجاد و استفاده از کلیدها
۱۷۴	حفظ امنیت موبایل
۱۷۵	دفاع از تلفن های موبایل در مقابل حملات
۱۷۶	حفاظت موبایل در مقابل تهدیدات
۱۷۷	۹ روش برتر برای حفظ امنیت دستگاه های موبایل
۱۷۸	راه های پیشگیری از شنود مکالمات به وسیله تلفن همراه
۱۷۹	توصیه ها و پیشنهادات
۱۷۹	گزارش دهی حوادث امنیتی
۱۷۹	التزام و رعایت سیاست های امنیتی سازمان

فصل نهم

۱۸۱	جمع بندی
۱۸۱	مقدمه
۱۸۱	کاربران کامپیوتر و حداقل دانش لازم
۱۸۵	نحوه برخورد با یک سیستم آلوده
۱۸۶	نحوه تشخیص آلودگی سیستم
۱۸۶	اقدامات لازم در صورت آلودگی سیستم
۱۸۷	اقدامات لازم به منظور کاهش حملات مشابه
۱۸۸	رهنمودهایی برای نشر اطلاعات در اینترنت
۱۹۰	ده قانون تقریباً پذیر امنیت اطلاعات
۱۹۵	منابع و مراجع
۱۹۵	منابع
۱۹۹	واژه نامه
۱۹۹	واژه نامه انگلیسی به فارسی
۲۰۳	واژه نامه فارسی به انگلیسی

پیشگفتار مولفان

امروزه کمتر کسی را می‌توان یافت که اطلاعاتی برای از دست رفتن نداشته باشد. همه ما در معرض از دست دادن اطلاعاتی هستیم که ممکن است به دست آوردن آن‌ها دیگر امکان‌پذیر نباشد. از سوی دیگر نوع دیگری از دزدی و ناامنی در محیط‌های کاری رواج یافته است که ریشه در گسترش فناوری اطلاعات و ارتباطات و آسیب‌های همراه آن دارد. آن ناامنی اطلاعاتی است که در گذشته‌های دور بارزترین مصداق آن دانستن جای کلید گاو صندوق بزرگانی بود که گنجینه‌ای نهفته در آن داشتند. اما امروزه همه ما صندوقچه‌ای از اطلاعات گرانبها را در اختیار داریم و معمولاً امکان دسترسی به آن از سوی افراد مختلف به راه‌های گوناگون وجود دارد. حوزه‌ای که این بُعد از زندگی امروزی را تحت پوشش قرار می‌دهد، امنیت اطلاعات است.

بدون شک، شاه بیت امنیت اطلاعات آگاهی است. در صورتی که همه ما از جوانب مختلف امنیت اطلاعات یا ناامنی‌های اطلاعات آگاه باشیم، کمتر دچار ضرر و زیان می‌شویم. البته دردناک‌ترین بُعد ناامنی اطلاعات زمانی است که اطلاعات به یغما رفته تنها اطلاعات فردی و شخصی نیست بلکه مربوط به گروهی از افراد یا یک سازمان و حتی یک کشور است که امکان خراب‌کاری با مقیاس بزرگ‌تر را فراهم می‌آورد. ساده‌ترین و موثرترین راه برای دستیابی به آگاهی، آموزش است؛ بنابراین آموزش امنیت اطلاعات یکی از مهم‌ترین مباحثی است که باید در سطح فردی، سازمانی و ملی به آن پرداخته شود.

این کتاب به عنوان دستاوردی از نگاه جامع به امنیت اطلاعات، با این هدف تدوین شده است که دانش مناسبی از امنیت اطلاعات، اهمیت آن، مدل‌ها و مبانی نظری آن ارائه نماید و سپس با تاکید بر اهمیت آگاهی و کسب آن از رهگذر آموزش چارچوبی برای این مفهوم فراهم آورد. در گام بعدی ضمن ارائه خلاصه‌ای از یافته‌های یک تحقیق میدانی، آموزه‌هایی عملی از امنیت اطلاعات را به خوانندگان عرضه کند؛ فصل‌های نه گانه این کتاب تلاش کرده است مفهوم امنیت اطلاعات را از آگاهی تا آموزش پوشش دهد.

در فصل اول، کلیات امنیت اطلاعات تبیین شده است. در فصل دوم، مولفه‌های تشکیل دهنده امنیت اطلاعات به همراه مصداق‌ها و واژه‌های بیابانگر آنها به تفصیل بررسی شده است. فصل سوم کتاب به مدل‌های امنیت اطلاعات اختصاص یافت و در فصل چهارم، عوامل تاثیرگذار بر امنیت اطلاعات بررسی و بر نقش عوامل انسانی در ارتقای امنیت اطلاعات تاکید شده است. فصل‌های پنجم و ششم به آگاهی از امنیت اطلاعات و آموزش آن اختصاص یافته است تا به صورت توانمند دو مفهوم کلیدی این کتاب را تبیین کنند. فصل هفتم نمونه‌ای از یک مطالعه موردی گزارش شده که در یک موسسه عالی به انجام رسیده است. در نهایت، فصل‌های هشتم و نهم کتاب به ارائه راهکارهای عملیاتی در حوزه ارتقای امنیت اطلاعات به تفکیک نقاط آسیب پذیر پرداخته است.

این کتاب در وهله اول برای طیف وسیعی از کسانی تدوین شده است که به مبحث امنیت اطلاعات علاقه‌مندند. در وهله دوم برای کسانی است که به صورت حرفه‌ای با فناوری اطلاعات و ارتباطات کار می‌کنند و مسئولیتی در ارتباط با آن در سازمان خود دارند و بنابراین نیازمند یک نگاه جامع (از نظر تا عمل) هستند. در مرحله سوم به صورت ویژه برای دانشجویان رشته‌های علوم کتابداری و اطلاع‌رسانی، مدیریت فناوری اطلاعات و پژوهشگران حوزه منابع اطلاعاتی سازمان‌ها که به صورت عمقی به دنبال فهم مفهوم امنیت اطلاعات و چارچوب فکری حاکم بر آن هستند، مفید خواهد بود.

همانند هر نوشتاری این مجموعه نیز خالی از اشکال نیست. اصولاً نویسندگان به دنبال اثبات بی‌نقصی این مجموعه نیستند بلکه تلاش کرده‌اند که دانسته‌ها و دستاوردهای خود را در قالب این کتاب به علاقه‌مندان عرضه کنند. دانسته‌هایی که حاصل تلاش علمی فراوان است و ریشه در یافته‌های دیگران دارد. لذا، تکمیل و اصلاح آن در طول زمان با پیشنهادات دلسوزانه و سازنده خوانندگان محترم حاصل خواهد شد. با علاقه وافر آماده شنیدن نظرات و ارشادهای دوستان هستیم.

من ... توفیق و علیه التکلیف

محمد حسن زاده - نرگس جهانگیری

زمستان ۹۰