

۲. ۴۷۷۹۰



به نام خدا



پدیده مهندسی اجتماعی: شکاف امنیتی سازمان ها در هزاره سوم

مؤلفان:

دکتر داود حسین پور

(دانشیار دانشکده مدیریت و حسابداری، دانشگاه علامه طباطبائی)

دکتر محمد مهدی قوجانی

(دکتری مدیریت دولتی)

دکتر سید امیر موسوی میرکلایی

(دکتری مدیریت رفتاری)



هر گونه چاپ و تکثیر از محتویات این کتاب بدون اجازه کتبی ناشر ممنوع است. متخلفان به موجب قانون حمایت حقوق مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می گیرند.

◀ عنوان کتاب: **پدیده مهندسی اجتماعی:**

شکاف امنیتی سازمان ها در هزاره سوم

◀ مؤلفان: دکتر داود حسین پور

دکتر محمد علی قوچانی

دکتر سید امیر موسوی میرکلایی

◀ ناشر: موسسه فرهنگی هنری دیباگران تهران

◀ صفحه آرای: فروش عبدسبی

◀ ویراستار: زهرا خانیانی

◀ طراح جلد: داریوش فرسای

◀ نوبت چاپ: اول

◀ تاریخ نشر: ۱۳۹۸

◀ چاپ و صحافی: درج عقیق

◀ تیراژ: ۱۰۰ جلد

◀ قیمت: ۴۵۰۰۰۰ ریال

◀ شابک: ۹۷۸-۶۲۲-۲۱۸-۱۶۱-۱

◀ نشرانی واحد فروش: تهران، میدان انقلاب،

خ کارگر جنوبی، روبروی پاساژ مهستان،

پلاک ۱۲۵۱

تلفن: ۲۲۰۸۵۱۱۱-۶۶۴۱۰۰۴۶

◀ فروشگاههای اینترنتی دیباگران تهران :

WWW.MFTBOOK.IR

www.dibagaran-tehran.com

www.mftdibagaran.ir

◀ نشانی تلگرام: @mftbook

سرشناسه: حسین پور، داوود، ۱۳۴۸-

عنوان و نام پدیدآور: پدیده مهندسی اجتماعی: شکاف

امنیتی سازمان ها در هزاره سوم

/ داود حسین پور، محمد مهدی قوچانی، سید امیر موسوی کلایی.

مشخصات نشر: تهران: دیباگران تهران: ۱۳۹۸

نسخه: ظاهری: ۱۲۰ص: مصور،

شابک: ۹۷۸-۶۲۲-۲۱۸-۱۶۱-۱

وضعیت فهرست نویسی: فیبا

موضوع: مهندسی اجتماعی-ایران-نمونه پژوهی

social engineering-Iran-case studies: موضوع

موضوع: فضای مجازی-ایران-نمونه پژوهی

cyberspace-security-Iran-case studies: موضوع

موضوع: کنترل اجتماعی-ایران-نمونه پژوهی

social control-Iran-case studies: موضوع

شناسه افزوده: قوچانی، محمد مهدی، ۱۳۶۶-

شناسه افزوده: موسوی میرکلایی، سید امیر، ۱۳۶۴-

رده بندی کنگره: ۶۶۸ HM

رده بندی دیویی: ۰۰۵/۸۹۵۵

شماره کتابشناسی ملی: ۵۷۷۸۵۷۵

اپلیکیشن دیباگران تهران را از سایت های اینترنتی دیباگران دریافت نمایید.

فهرست مطالب

۷ مقدمه ناشر

۸ مقدمه مؤلف

فصل اول

۹ اهمیت اینترنت و فضای مجازی و حفظ حریم خصوصی در آن

۱۰ مقدمه

۱۲ ماه ساختاری و فنی اینترنت

۱۲ مالکیت اینترنت

۱۳ باز بودن فضای مجازی

۱۴ نقش اینترنت در فضای مجازی

۱۶ شبکه‌های اجتماعی در فضای مجازی و امنیت آن

۲۰ تهدیدات شبکه‌های اجتماعی در اینترنت

۲۳ ارتباط بین اعضا در شبکه‌های اجتماعی

۲۳ بررسی مسائل و تهدیدات شبکه‌های اجتماعی

۲۴ آسیب‌های اجتماعی

۲۸ تهدیدات امنیتی تخصصی

۲۸ جعل هویت

۳۰ تهدیدات و مخاطرات نمایه

۳۱ سرقت از طریق کلیک کردن

۳۱ بازیابی تصویر بر اساس محتوا

۳۱ کرم‌ها و تروجان‌ها

۳۱ حمله از طریق نقطه ضعف‌های امنیتی

۳۳ نرم‌افزارهای کاربردی

۳۳ حمله محله‌ای یا همسایگی

۳۳ فیشینگ

۳۳ انتشار اطلاعات کاربران توسط سرویس‌دهندگان شبکه‌های اجتماعی

فصل دوم

۳۴	مهندسی اجتماعی چیست؟
۳۵	مقدمه
۳۵	تعریف مهندسی اجتماعی
۳۶	پیشینه و انگیزه‌های حملات مهندسی اجتماعی
۳۶	تاریخچه حملات مهندسی اجتماعی
۳۷	هکرها
۳۸	انگیزه‌ها و محرک‌های رفتاری در مهندسی اجتماعی
۴۰	چرخه مهندسی اجتماعی
۴۰	هستی‌شناسی مهندسی اجتماعی
۴۱	محیط‌های شکست‌گیری مهندسی اجتماعی
۴۳	تحقیقات انجام شده در مهندسی اجتماعی

فصل سوم

۴۵	ریشه‌یابی و بررسی روش‌های اجرای حملات مهندسی اجتماعی
۴۶	حملات مهندسی اجتماعی
۴۶	احتمال حملات مهندسی اجتماعی
۴۷	کشف حملات مهندسی اجتماعی
۵۰	روش‌های اجرایی حملات مهندسی اجتماعی
۵۰	شیوه‌های روانی و منشأ حملات
۵۱	روش‌های اجرایی حمله

فصل چهارم

۵۸	چگونگی مقابله با حملات مهندسی اجتماعی
۵۹	جنبه‌های اصلی مهندسی اجتماعی
۵۹	امنیت فضای سایبری
۶۳	روش‌های دفاعی
۶۳	سوالات ساده
۶۴	هکرها و اخلاقی

۶۴	خطامشی مهندسی اجتماعی
۶۶	آموزش
۶۸	مدل مدیریت ریسک مهندسی اجتماعی
۷۰	جدول جامع دفاعی

فصل پنجم

۷۲	مهندسی اجتماعی در عصر جدید
۷۳	مهندسی اجتماعی در شبکه‌های اجتماعی
۷۵	شرکت‌ها: فعال در حوزه مهندسی اجتماعی
۷۵	ثبت کامپیوتری ای بی ام
۷۷	سازمان تحقیقات انسیون
۸۰	مؤسسه مهندسی اجتماعی
۸۱	شرکت کامپیوتری
۸۲	دانشگاه‌های فعال در حوزه مهندسی اجتماعی
۸۲	دانشگاه توننتی
۸۲	دانشگاه کارنگی ملون
۸۳	دانشگاه لوگز امبورگ
۸۳	دیگر دانشگاه‌ها
۸۴	کشورهای فعال در حوزه تحقیقات مهندسی اجتماعی
۸۵	تلفن همراه و کنسول‌های بازی، ابزارهای نوین مهندسی اجتماعی
۸۷	سمینارها و کنفرانس‌های مهندسی اجتماعی
۸۸	سیاست‌گذاری کشورها در حوزه مهندسی اجتماعی

فصل ششم

۹۰	مطالعه موردی مهندسی اجتماعی
۹۱	مقدمه
۹۳	بررسی متغیرهای جمعیت‌شناختی صاحب‌شوندگان
۹۵	بررسی نتایج حاصل از مصاحبه‌ها
۹۵	دیدگاه صاحب‌شوندگان در مورد متغیرهای مدل تحقیق
۹۵	آسیب‌پذیرها

۱۰۱	روش‌های حمله
۱۰۵	روش‌های دفاعی
۱۰۹	پیامدهای حملات مهندسی اجتماعی
۱۱۰	نتایج

فصل هفتم

۱۱۱	نتیجه‌گیری و پیشنهادها
۱۱۲	مقدمه
۱۱۳	پیشینه‌های صاحب‌هوشندگان در مطالعه موردی
۱۱۴	پیشینه‌های مؤلفان
۱۱۵	منابع
۱۱۶	منابع انگلیسی

مقدمه مؤلفین

موضوع مهندسی اجتماعی که به عنوان هنر بهره برداری از رفتارهای آسیب پذیر انسان ها برای ایجاد شکاف امنیتی بدون هیچ ظن و گمانی از سوی فرد شناخته می شود، امروزه به عنوان یکی از مباحث مهم در حوزه امنیت سازمان ها مطرح شده است. رشد و توسعه فناوری اطلاعات و تکنولوژی های سازمان باعث شده تا فرصت های بسیاری برای سوءاستفاده از اطلاعات و افراد در سازمان ها ایجاد شود. در این کتاب در فصل اول و دوم سعی در بیان اهمیت اینترنت و امنیت فضای مجازی، معرفی مهندسی اجتماعی و هستی شناسی این مفهوم نموده است. در فصل سوم ریشه یابی و روش های مهندسی اجتماعی مورد بررسی قرار گرفته است و در فصل چهارم چگونگی مقابله با این حمله ها تشریح شده است. فصل پنجم این کتاب به بیان وضعیت کنونی مهندسی اجتماعی در شرکت ها، دستگاه ها و رویدادهای مختلف جهانی در این حوزه می پردازد.

این کتاب با توجه گسترده استفاده از ابزارهای نوین در سطح سازمانی و افزایش خطر حملات مهندسی اجتماعی، سعی در بیان اهمیت مهندسی اجتماعی نموده است که بدین واسطه بتوان آگاهی در این زمینه را ارتقاء داد به منظور ارائه یک مدل مفهومی در این زمینه و کامل شدن این کتاب، تحقیق میدانی در خصوص مهندسی اجتماعی صورت گرفته است. فصل ششم ارائه شده است؛ تا بتوان مواردی که بصورت تئوریک مورد مطالعه قرار گرفته اند را با صاحب نظران و اندیشمندان این حوزه مورد نقد و بررسی قرار داد و شاخص های مدل تحقیق را با توجه به وضعیت اطلاعات کشور اولویت بندی کرد. قطعاً استفاده از یک مطالعه موردی می تواند مکمل بسیار خوبی برای بخش تئوریک کتاب باشد.

مطالعه این کتاب برای مدیران و کارشناسان حوزه فضای مجازی، به نفع دیگر برای هرکاربر فضای مجازی که حفظ و امنیت اطلاعات شخصی و سازمانی مهم است؛ پیشنهاد می گردد.

پس از حمد و سپاس خداوند متعال، به رسم ادب از شرکت صنایع امنیت فضای تبادل اطلاعات و همچنین ناشر محترم این کتاب قدردانی به عمل می آید. بی تردید متن حاضر خالی از اشکال خطاییست. از خوانندگان گرامی خواهشمنداست ایرادات احتمالی را بر ما ببخشایند و با ارسال نظرات و دیدگاه های ارزشمند شان ما را در بهبود این کتاب یاری نمایند.