

۲۰۲۲۷۵۷

آگاهی‌رسانی امنیت سایبری برای پرسنل

مؤلف:

علیرضا قهرود

مشاور و مدرس راهکارهای امنیت سایبری



**NAGHOOS
PUBLICATION**

۱۳۹۷

سرشناسه

شبان قهرود , علیرضا , ۱۳۶۵ -

Shaban Ghahreod , Alireza

عنوان و نام پدیدآور : آگاهی رسانی امنیت سایبری/مؤلف علیرضا شبان قهرود

مشخصات نشر : تهران : ناخوس , ۱۳۹۷

مشخصات ظاهری : ۲۲۲ص : مصورچندول , نمودار

شابک : 978-600-473-159-1

وضعیت فهرست نویسی : فیا

یادداشت : عنوان دیگر : آگاهی رسانی امنیت سایبری برای پرسنل

یادداشت : کتابنامه ,

عنوان دیگر : آگاهی رسانی امنیت سایبری برای پرسنل

موضوع : تکنولوژی اطلاعات -- تدابیر ایمنی

موضوع : Security measures--Information technology

موضوع : شبکه های کامپیوتری-- تدابیر ایمنی

موضوع : Computer networks--Security Measures

موضوع : کامپیوترها -- ایمنی اطلاعات

موضوع : Computer security

موضوع : حفاظت داده ها

موضوع : Data Protection

رده بندی کنگره : ۷۱۳۷ : ق/۵۱

رده بندی دیویی : ۳۰۳/۲۸۳۳

شماره کتابشناسی ملی : ۵۵۵۷۳۵۰



NAGHOOS
PUBLICATION

برای خرید Online به آدرس زیر مراجعه کنید:

www.naghoos-pers.ir

انتشارات ناخوس

نام کتاب

آگاهی رسانی امنیت سایبری برای پرسنل

ناشر

انتشارات ناخوس

نویسنده

علیرضا شبان قهرود

چاپ اول

: ۱۳۹۷

تیراژ

: ۵۰۰ نسخه

قیمت

: ۵۰۰,۰۰۰ ریال

چاپ و صحافی

: برجسته

شابک

: ۹۷۸-۶۰۰-۴۷۳-۱۵۹-۱

ISBN

: 978-600-473-159-1

کلیه حقوق برای ناشر محفوظ است. تکثیر تمامی یا قسمتی از این اثر به صورت حروفچینی یا چاپ مجدد، چاپ افست، پلی کپی، فتوکپی و انواع دیگر چاپ ممنوع است و پیگرد قانونی دارد.

مرکز پخش: انتشارات ناخوس

۱- خیابان انقلاب- بلوار کشاورز- خیابان ۱۶ آذر- کوچه پارس- پلاک ۱۰

تلفن و فاکس: ۶۶۴۷۸۹۵۴-۶۶۴۷۸۹۵۱

۲- کتابفروشی الیاس: خیابان انقلاب، نبش ۱۲ فروردین تلفن: ۶۶۴۰۵۰۸۴

در دنیای امروز که ارتباطات جزء لاینفک زندگی بشری شده است، فضای مجازی فاصله های کیلومتری بین افراد را از میان برداشته است، برخی مشکلات مثل اختلالات ارتباطی، بدافزارهای اینترنتی و انواع حملات سایبری چالش هایی را در این فضا ایجاد نموده و مانع از جابجایی بهینه ی اطلاعات گشته اند. بر همین اساس افراد بسیاری بصورت شرکت های خصوصی و در قالب تیم محور و همچنین بصورت مستقل سعی در حل این مشکل نموده اند. امروزه حتی دولت های مختلف برای پیشگیری و پاسخگویی به اینگونه حملات نسبت به کشف چنین عواملی قدم برداشته اند و در این خصوص جرایم گوناگونی شناسایی شده و برای آنها راهکارهایی اندیشیده شده است. از آنجا که کشور ایران از دیر باز در منطقه و جهان ا موقعیت استراتژیک برخوردار است، همیشه مورد تهاجم دولت های گوناگونی قرار داشته است. با تغییر رویکردهای بشر به سمت فناوری اطلاعات و سمت و سوی حرکت انسان به سوی فناوری نوین در فضای مجازی تغییر مسیر یافته است، در ماهیت تهاجمات نیز تغییراتی به صورت پارادایم رخ داده است. به اعتقاد بسیاری از متخصصین امروزه جنگ سایبری از مهمترین انواع تهدیدات بشمار می رود. جنگی که پیروزی در آن جز با دفاع به وسیله ی هوشیاری و یاری آحاد ملت و متخصصین میسر نخواهد شد. لذا این کتاب بر آنست با محتوای شیوا و شفاف در مقدمات به معرفی امنیت اطلاعات، ارکان امنیت، سیستم امنیت، ادعای، انواع بدافزارها و حملات سایبری پرداخته و سپس به شیوع و روشهای مقابله دفاع سایبری از منظر هر فرد بصورت شخصی و سازمانی با هر سمت و تخصصی بوسیله آگاهی رسانی امنیت سایبری بپردازد.

فهرست مطالب

فصل اول: امنیت اطلاعات و ارتباطات در چرخه مستمر

۱. جلسه اول: مفهوم امنیت اطلاعات و ارتباطات و دارایی‌های اطلاعاتی

۱.۱ اهداف یادگیری

۱.۲ پیش آزمون

پاسخ نامه:

۱.۳ مقدمه

۱.۴ اطلاعات

۱.۵ امنیت اطلاعات

۱.۶ عناصر امنیت اطلاعات

۱.۷ مفاهیم اساسی امنیت

احتیاط و پیشگیری

نگهداری

واکنش

۱.۸ لایه‌های امنیت

امنیت فیزیکی

امنیت شبکه

امنیت سیستم اطلاعاتی

امنیت برنامه

امنیت کاربر

۱.۹ میزان دستیابی به اهداف یادگیری

۱.۱۰ خودآزمایی

پاسخ‌نامه تشریحی

۲. جلسه دوم: لزوم وجود سیاست‌های امنیتی و ضرورت انطباق با آن‌ها

۲.۱ اهداف یادگیری

۲.۲ پیش آزمون

پاسخ‌نامه

۲.۳ سیاست‌های امنیتی

۲.۴ انواع سیاست‌های امنیت اطلاعات و ارتباطات

۱۷	۲.۵ لزوم وجود سیاست‌های امنیتی
۱۹	۲.۶ ضرورت انطباق با سیاست‌های امنیتی
۲۰	۲.۷ میزان دستیابی به اهداف یادگیری
۲۱	۲.۸ خودآزمایی
۲۱	پاسخنامه تشریحی
۲۳	۳. خلاصه فصل اول
۲۳	جلسه اول
	جلسه دوم

فصل دوم: پیاده‌سازی امنیت در سازمان‌ها

۲۸	۱. جلسه اول: سیستم مدیریت امنیت اطلاعات (ISMS)
۲۸	۱.۱ اهداف یادگیری
۲۸	۱.۲ پیش آزمون
۲۸	پاسخنامه
۲۹	۱.۳ مقمه
۲۹	۱.۴ راهکار مناسب تأمین امنیت اطلاعات و ارتباطات
۳۰	۱.۵ سیستم مدیریت امنیت اطلاعات (ISMS)
۳۳	پیاده‌سازی سیستم مدیریت امنیت اطلاعات در سازمان
۳۴	۱.۶ بیانیه خط‌مشی سیستم مدیریت امنیت اطلاعات
۳۶	۱.۷ میزان دستیابی به اهداف یادگیری
۳۶	۱.۸ خودآزمایی
۳۶	پاسخنامه تشریحی
۳۸	۲. جلسه دوم: تشکیلات سازمانی امنیت و نقش نیروی انسانی در تأمین امنیت سازمان
۳۸	۲.۱ اهداف یادگیری
۳۸	۲.۲ پیش آزمون
۳۸	پاسخنامه
۳۹	تشکیلات سازمانی امنیت اطلاعات
۳۹	چارت سازمانی پیشنهادی امنیت اطلاعات
۳۹	۲.۳.۱ شرح وظایف پیشنهادی معاونت امنیت سازمانی به تفکیک واحدها
۴۱	۲.۴ نقش نیروی انسانی در تأمین امنیت اطلاعات

۴۳	۲.۵ میزان دستیابی به اهداف یادگیری
۴۳	۲.۶ خودآزمایی
۴۴	پاسخ‌نامه تشریحی
۴۵	۳. خلاصه فصل دوم
۴۵	جلسه اول
۴۵	جلسه دوم

فصل سوم: امنیت فیزیکی و محیطی

۵۰	۱. جلسه اول: امنیت فیزیکی و محیطی و انواع آن
۵۰	۱.۱ اهداف یادگیری
۵۰	۱.۲ پیش‌آزمون
۵۰	پاسخ‌نامه
۵۱	۱.۳ امنیت فیزیکی و محیطی
۵۱	۱.۴ انواع راهکارهای امنیت فیزیکی و محیطی
۵۱	۱.۴.۱ استفاده از حصارهای مناسب امنیت فیزیک
۵۱	۱.۴.۲ امنیت ورودی ساختمان‌ها و مراکز حساس
۵۲	۱.۴.۳ استقرار و حفاظت تجهیزات
۵۲	۱.۴.۴ محافظت در برابر تهدیدات بیرونی و محیط
۵۳	۱.۴.۵ تهیه نسخ و سایت‌های پشتیبان
۵۳	۱.۴.۶ امنیت کابل کشی
۵۴	۱.۴.۷ خروج دارایی‌ها
۵۴	۱.۴.۸ امنیت تجهیزات خارج از سازمان
۵۴	۱.۴.۹ امنیت تجهیزات بدون مراقبت کاربر
۵۵	۱.۵ میزان دستیابی به اهداف یادگیری
۵۵	۱.۶ خودآزمایی
۵۵	پاسخ‌نامه تشریحی
۵۷	۲. جلسه دوم: محافظت در برابر تهدیدات فیزیکی و محیطی
۵۷	۲.۱ اهداف یادگیری
۵۷	۲.۲ پیش‌آزمون
۵۷	پاسخ‌نامه

۵۸	۲.۳ انواع تهدیدات فیزیکی و محیطی
۵۸	۲.۳.۱ بلایای طبیعی و حوادث غیر مترقبه
۵۹	۲.۳.۲ تهدیدات انسانی
۵۹	۲.۳.۳ مشکلات فنی
۶۰	۲.۴ برنامه ریزی برای پاسخگویی به حوادث غیرمترقبه
۶۰	۲.۴.۱ مرحله آماده سازی پیش از وقوع حادثه
۶۱	۲.۴.۲ مرحله وقوع حادثه
۶۱	۲.۴.۳ مرحله بازیابی پس از وقوع حادثه
۶۱	۲.۵ میزان دستیابی به اهداف یادگیری
۶۲	۲.۶ خودآزمایی
۶۲	پاسخنامه تشریحی
۶۴	۳. خلاصه فصل سوم
۶۴	جلسه اول
۶۴	جلسه دوم

فصل چهارم: تهدیدات امنیتی در فضای سایبر

۶۸	۱. جلسه اول : مفهوم تهدیدات سایبری
۶۸	۱.۱ اهداف جلسه آموزشی
۶۸	شکل اهداف جلسه آموزشی
۶۸	۱.۲ پیش آزمون
۶۸	پاسخنامه
۶۹	۱.۳ محتوای جلسه آموزشی
۷۰	۱.۴ فضای سایبر
۷۱	۱.۵ میزان دستیابی به اهداف آموزشی
۷۱	۱.۶ خودآزمایی
۷۱	پاسخنامه تشریحی
۷۲	۲. جلسه دوم: انواع حملات سایبری و تکنیک های هک
۷۲	۲.۱ اهداف جلسه آموزشی
۷۲	۲.۲ پیش آزمون
۷۲	پاسخنامه:سبز

۷۳	۲.۳ انواع حملات سایبری
۷۴	۲.۳.۱ Confidentiality (محرمانگی)
۷۴	۲.۳.۲ Integrate (یکپارچگی و صحت اطلاعات)
۷۵	۲.۳.۳ Availability (دسترسی پذیری)
۷۷	افشاسازی
۷۸	تخریب
۷۹	انکار یا در دسترس نبودن
۷۹	۲.۴ نمونه ای از حملات از سرویس خارج کردن - دسترس ناپذیری
۸۰	۲.۴.۱ حملات سایبری DOS
۸۱	۲.۴.۲ حملات سایبری DDOS
۸۲	۲.۵ متدولوژی انجام حملات سایبری
۸۲	۲.۶ میزان دسترسی به اهداف آموزشی
۸۳	۲.۷ خودآزمایی
۸۳	پاسخنامه تشریحی
۸۳	۳. جلسه سوم: طبقه بندی و تشریح انواع ابزار
۸۳	۱.۳ اهداف جلسه آموزشی
۸۳	۲.۳ پیش آزمون
۸۳	پاسخنامه سبز
۸۴	۲.۴ انواع بدافزارها
۸۳	۲.۴.۱ Malware
۸۴	۲.۴.۲ ویروس - Virus
۸۴	۲.۴.۳ کرم - worm
۸۵	۲.۴.۴ اسب های تروا - Trojan horses
۸۵	۲.۴.۵ رد گم کن - RootKit
۸۶	۲.۴.۶ کلیدنگار - key logger
۸۶	۲.۴.۷ جاسوس افزارها - Spyware
۸۷	۲.۴.۸ آگهی افزار یا برنامه های تبلیغاتی - Adware
۸۷	۲.۴.۹ درهای پشتی - Backdoors
۸۷	۲.۴.۱۰ Bot و Botnet
۸۸	۲.۴.۱۱ باج گیر - Ransomware
۸۹	۲.۵ میزان دست یابی به اهداف آموزشی

۹۰	۲.۶ خودآزمایی
۹۰	پاسخنامه تشریحی

فصل پنجم: امنیت در مقابله با تهدیدات فضای سایبری

۹۴	۱. جلسه اول: آگاهی‌رسانی مستمر امنیت‌محور
۹۴	۱.۱ اهداف یادگیری
۹۴	۱.۲ پیش‌آزمون
۹۴	پاسخنامه
۹۴	۱.۳ جایگاه آگاه‌رسانی و آموزش
۹۵	۱.۴ ابزارهای انتقال دانش در جهت افزایش آگاهی‌رسانی
۹۶	۱.۵ میزان دستیابی به اهداف آموزشی
۹۷	۱.۶ خودآزمایی
۹۷	پاسخنامه تشریحی
۹۸	۲. جلسه دوم: به‌روزرسانی سیستم عامل و برنامه‌های کاربردی
۹۸	۲.۱ اهداف یادگیری
۹۸	۲.۲ پیش‌آزمون
۹۹	پاسخنامه
۹۹	۲.۳ اهمیت به‌روزرسانی سیستم عامل‌ها و برنامه‌های کاربردی
۱۰۱	۲.۴ انواع سیستم عامل
۱۰۲	۲.۵ برنامه‌های کاربردی
۱۰۳	۲.۶ به‌روزرسانی سیستم عامل‌ها و برنامه‌های کاربردی
۱۰۴	۲.۷ ارتقای سیستم عامل‌ها و برنامه‌های کاربردی
۱۰۴	۲.۷.۱ روش‌های به‌روزرسانی و ارتقا
۱۰۵	۲.۸ میزان دستیابی به اهداف آموزشی
۱۰۵	۲.۹ خودآزمایی
۱۰۵	پاسخنامه تشریحی
۱۰۶	۳. جلسه سوم: ضد بدافزار و به‌روزرسانی آن
۱۰۶	۳.۱ اهداف یادگیری
۱۰۶	۳.۲ پیش‌آزمون
۱۰۷	پاسخنامه

۱۰۷	۳.۳ تهدیدات به وسیله بدافزارها
۱۰۷	۳.۴ روش های عمده آلودگی به بدافزارها
۱۰۸	۳.۵ راهکارهای مقابله پس از وقوع آلودگی
۱۰۹	۳.۶ بازیابی اطلاعات
۱۱۰	۳.۷ ضد بدافزار و به روزرسانی مستمر
۱۱۰	۳.۸ میزان دستیابی به اهداف آموزشی
۱۱۱	۳.۹ خودآزمایی
۱۱۱	پاسخنامه تشریحی
۱۱۲	۴. جلسه چهارم: مدیریت گذرواژه (PassWord)
۱۱۲	۴.۱ اهداف یادگیری
۱۱۲	۴.۲ پیش آزمون
۱۱۲	پاسخنامه
۱۱۲	۴.۳ تعریف گذرواژه با رمز عبور (پسورد)
۱۱۳	۴.۴ ویژگی های گذرواژه مناسب و امن
۱۱۳	۴.۵ مدیریت گذرواژه
۱۱۴	ذخیره امن گذرواژه ها
۱۱۴	عملکرد آنلاین و آفلاین
۱۱۵	تصدیق هویت دو مرحله ای (Two-Factor Authentication)
۱۱۵	یکپارچگی با مرورگر
۱۱۵	تغییر خودکار رمز عبور (Password Changes)
۱۱۵	هشدارهای امنیتی خودکار (Security Alerts)
۱۱۵	پسوردهای دوره ای یا یکبار مصرف (Throwaway Passwords)
۱۱۶	یادآوری
۱۱۶	۴.۶ میزان دستیابی به اهداف آموزشی
۱۱۶	۴.۷ خودآزمایی
۱۱۷	پاسخنامه تشریحی
۱۱۸	۵. جلسه پنجم: نسخه پشتیبان (BackUp)
۱۱۸	۵.۱ اهداف یادگیری
۱۱۸	۵.۲ پیش آزمون
۱۱۸	پاسخنامه
۱۱۸	۵.۳ تعریف نسخه پشتیبان

۱۱۸	۵.۴ اهمیت تهیه نسخه پشتیبان
۱۲۰	۵.۵ استراتژی تهیه نسخه پشتیبان
۱۲۰	۱. برای انتخاب برنامه یا سرویس پشتیبان‌گیری مناسب، وقت بگذارید
۱۲۰	۲. برنامه‌ریزی مشخصی برای تهیه بک‌آپ داشته باشید.
۱۲۰	۳. از سلامت نسخه پشتیبان و امکان بازیابی آن اطمینان یابید.
۱۲۰	۴. سلامت ابزار نگهداری نسخه پشتیبان را کنترل کنید.
۱۲۱	۵. هارد دیسک‌تان را به صورت دوره‌ای کنترل کنید.
۱۲۱	۶. از چه فایل‌هایی باید نسخه پشتیبان تهیه شود
۱۲۱	۷. میزان دستیابی به اهداف آموزشی
۱۲۲	۸. خودآزمایی
۱۲۲	پاسخ‌نامه تشریحی
۱۲۳	۶. جلسه ششم: فیلتر پراکسی
۱۲۳	۶.۱ اهداف یادگیری
۱۲۳	۶.۲ پیش‌آزمون
۱۲۳	پاسخ‌نامه
۱۲۳	۶.۳ مقدمه
۱۲۴	۶.۴ پراکسی چیست؟
۱۲۴	۶.۵ مزایای استفاده از پراکسی
۱۲۶	یادآوری
۱۲۷	۶.۶ میزان دستیابی به اهداف آموزشی
۱۲۸	۶.۷ خودآزمایی
۱۲۸	پاسخ‌نامه تشریحی
۱۲۸	۷. جلسه هفتم: اعتبارسنجی برنامه‌های کاربردی
۱۲۸	۷.۱ اهداف یادگیری
۱۲۸	۷.۲ پیش‌آزمون
۱۲۸	پاسخ‌نامه
۱۲۹	۷.۳ کد هش Hash Code چیست؟
۱۲۹	۷.۴ Hash Code چه کاربردی دارد؟
۱۳۰	۷.۵ MD۵ یا اثر انگشت فایل‌ها چیست؟
۱۳۰	۷.۶ بهترین نرم‌افزار تولید اثر انگشت فایل یا MD۵ + Checksum
۱۳۰	۷.۷ میزان دستیابی به اهداف آموزشی

۱۳۱	۷.۸ خودآزمایی
۱۳۱	پاسخنامه تشریحی
۱۳۱	۸ جلسه هشتم: چک لیست امنیت کاربران سازمان در قبال حملات سایبری نفوذگران
۱۳۱	۸.۱ اهداف یادگیری
۱۳۲	۸.۲ پیش آزمون
۱۳۲	پاسخنامه
۱۳۲	۸.۳ اهمیت رعایت چکلیست‌های امنیت‌محور توسط کارکنان سازمان
۱۳۲	۸.۴ ده ریسک امنیت کارکنان سازمان
۱۳۲	۸.۵ ده ریسک سرقت دارایی‌های اطلاعاتی کاربران
۱۳۳	۸.۶ چکلیست امنیت کاربران برای جلوگیری از نشت دارایی‌های اطلاعاتی سازمان
۱۳۴	۸.۷ تعریف تکنیک مبتنی بر سبیل‌های مهندسی اجتماعی
۱۳۴	۸.۸ انواع طبقه‌بندی مهندسی اجتماعی
۱۳۴	نوع اول: متکی به اشتغال
۱۳۵	نوع دوم: متکی به تکنولوژی و رسانه
۱۳۶	متن ایمیل
۱۳۷	۸.۹ مهندسی اجتماعی
۱۳۸	۸.۱۰ الگوی نفوذ به واسطه مهندسی اجتماعی
۱۴۰	۸.۱۱ میزان دستیابی به اهداف آموزشی
۱۴۰	۸.۱۲ خودآزمایی
۱۴۰	پاسخنامه تشریحی
۱۴۲	۹ جلسه نهم: آشنایی با سیاست میز کار و صفحه نمایش پاک
۱۴۲	۹.۱ اهداف یادگیری
۱۴۲	۹.۲ پیش آزمون
۱۴۲	پاسخنامه
۱۴۲	۹.۳ بخشنامه و الزام سیاست (CDP) Clean Desk Policy
۱۴۳	۹.۴ هدف سیاست میز کار و صفحه نمایش پاک
۱۴۴	۹.۵ چکلیست ممیزی سیاست میز کار و صفحه نمایش پاک
۱۴۴	۹.۶ میزان دستیابی به اهداف آموزشی
۱۴۵	۹.۷ خودآزمایی
۱۴۵	پاسخنامه تشریحی

فصل ششم: امنیت تجهیزات قابل حمل

- ۱۵۰ ۱. جلسه اول: امنیت در رسانه‌های ذخیره سازی و حافظه‌های جانبی
- ۱۵۰ ۱.۱ اهداف یادگیری
- ۱۵۰ ۱.۲ پیش آزمون
- ۱۵۰ پاسخ‌نامه
- ۱۵۰ ۱.۳ امنیت در رسانه های قابل حمل
- ۱۵۱ ۱.۴ نشست اطلاعات
- ۱۵۱ ۱.۵ تعریف حافظه
- ۱۵۲ ۱.۶ خصوصیات حافظه در معنای عام
- ۱۵۳ ۱.۷ سیاست امنیت اطلاعات در استفاده از تجهیزات ذخیره سازی و حافظه‌های جانبی قابل حمل
- ۱۵۴ ۱.۸ خودآزمایی
- ۱۵۴ پاسخ‌نامه تشریحی
- ۱۵۴ ۱.۹ میزان دست یابی به اهداف آموزشی
- ۱۵۵ ۲. جلسه دوم: امنیت در رایانه های قابل حمل
- ۱۵۵ ۲.۱ اهداف یادگیری
- ۱۵۵ ۲.۲ پیش آزمون
- ۱۵۵ پاسخ‌نامه
- ۱۵۵ ۲.۳ اهمیت امنیت در تجهیزات رایانه‌ای قابل حمل (لپ تاپ)
- ۱۵۶ ۲.۴ سیاست امنیت اطلاعات در استفاده از تجهیزات رایانه‌ای قابل حمل (لپ تاپ)
- ۱۵۸ ۲.۵ خود آزمایی
- ۱۵۹ پاسخ‌نامه تشریحی
- ۱۵۹ ۲.۶ میزان دستیابی به اهداف یادگیری
- ۱۵۹ ۳. جلسه سوم: امنیت در تلفن‌های هوشمند
- ۱۵۹ ۳.۱ اهداف یادگیری
- ۱۶۰ ۳.۲ پیش آزمون
- ۱۶۰ پاسخ‌نامه
- ۱۶۰ ۳.۳ امنیت در تلفن‌های هوشمند
- ۱۶۹ ۳.۴ خودآزمایی
- ۱۶۹ پاسخ‌نامه تشریحی
- ۱۶۹ ۳.۵ میزان دست یابی به اهداف آموزشی

فصل هفتم: جرایم رایانه‌ای، مصادیق و تعهدنامه عدم افشاء اطلاعات

- ۱۷۳ ۱. فهرست مصادیق محتوای مجرمانه
- ۱۷۳ موضوع ماده ۲۱ قانون جرایم رایانه‌ای
- ۱۷۳ الف) محتوا علیه عفت و اخلاق عمومی
- ۱۷۳ ب) محتوا علیه مقدسات اسلامی
- ۱۷۳ ج) محتوا علیه امنیت و آسایش عمومی
- ۱۷۴ د) محتوا علیه غامات و نهادهای دولتی و عمومی
- ۱۷۴ ه) محتوای که برای ارتکاب جرایم رایانه‌ای به کار می‌رود (محتوا مرتبط با جرایم رایانه‌ای)
- ۱۷۵ ز) محتوا مجرمانه مرتبط با امور سمعی و بصری و مالکیت معنوی
- ۱۷۵ و) محتوای که تحریک، ترغیب، دعوای به ارتکاب جرم می‌کند (محتوای مرتبط با سایر جرایم)
- ۱۷۵ قانون جرایم رایانه‌ای
- ۱۷۵ ۲. تعزیرات قانون مجازات اسلامی (قانون جرایم رایانه‌ای) بخش یکم - جرائم و مجازات‌ها
- ۱۷۵ فصل یکم - جرائم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی مبحث یکم - دسترسی غیرمجاز
- ۱۷۶ مبحث دوم - شنود غیرمجاز
- ۱۷۶ مبحث سوم - جاسوسی رایانه‌ای
- ۱۷۷ فصل دوم - جرائم علیه صحت و تمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی مبحث یکم - جعل رایانه‌ای
- ۱۷۷ فصل سوم - سرقت و کلاهبرداری مرتبط با رایانه
- ۱۷۸ فصل چهارم - جرائم علیه عفت و اخلاق عمومی
- ۱۷۹ فصل پنجم - هتک حیثیت و نشر اکاذیب
- ۱۷۹ فصل ششم - مسئولیت کیفری اشخاص
- ۱۸۱ فصل هفتم - سایر جرائم
- ۱۸۲ فصل هشتم - تشدید مجازات‌ها
- ۱۸۲ قانون آیین دادرسی کیفری (آیین دادرسی جرائم رایانه‌ای)
- ۱۸۲ آیین دادرسی جرائم رایانه‌ای
- ۱۸۶ نحوه ارایه شکایت به پلیس فتا

۱۸۶

راه اول

۱۸۶

راه دوم

۱۸۶

تعهدنامه عدم افشاء اطلاعات

منابع

۱۹۱

منابع اصلی

www.ketab.ir