


## مالکیت معنوی

خوانندهٔ گرامی همان‌طور که می‌دانید، شما برای دریافت این کتاب به‌صورت الکترونیک هیچ هزینه‌ای پرداخت نکرده‌اید. سود حاصل از فروش این کتاب به مؤسسه خیریهٔ مردم‌نهاد هم کاسه مشهد مقدس تقدیم شده است؛ لذا از شما خواهشمندم حداقل هزینهٔ ده هزار تومان را به‌حساب خیریه مذکور واریز نمایید. اگر تمایل دارید، در این امر خیر مشارکت بیشتری کنید، می‌توانید بسته به صلاحدید و توان خود مبلغی بیش از حداقل هزینه پرداخت کنید.

**آشنایی با بنیاد خیریه هم کاسه**

**از طریق صفحه اینستاگرام**

@ham_kase

**شماره کارت بانکی به نام خیریه هم کاسه**

۵۸۵۹۸۳۷۰۰۹۴۷۱۹۶۸


بسم الله الرحمن الرحيم

| | | |
|---|---|---|
| سرشناسه | : | شریفی، وحید، ۱۳۶۵- |
| عنوان و نام پدیدآور | : | آموزش فناوری، امنیت اطلاعات/مؤلف وحید شریفی. |
| مشخصات نشر | : | تهران: مدیران اندیشه، ۱۴۰۰. |
| مشخصات ظاهری | : | ۱۸۳ ص. |
| شابک | : | ۹۷۸-۶۲۲-۷۷۵۲-۳۵-۹ |
| یادداشت | : | کتابنامه. |
| موضوع | : | اینترنت – تدابیر امنیتی |
| | | internet - Security Measures |
| | | فضای مجازی – تدابیر امنیتی |
| | | syber Space - Security Measures |
| | | حق صیانت از حریم شخصی |
| | | شبکه‌های اجتماعی پیوسته |
| | | Online social networks |
| رده‌بندی کنگره | | TK۵۱۰۵/۵۹: |
| رده‌بندی دیویی | | ۰۰۵/۸: |
| شماره کتاب‌شناسی ملی | | ۷۶۵۷۶۱۱: |

مرکز پخش: کتابفروشی مهدی – مشهد - چهارراه شهدا – نبش بهجت ۲ –تلفن :۰۹۱۵۲۰۲۳۰۶۴

| | |
|---|---|
| **نام کتاب** | **آموزش فناوری، امنیت اطلاعات** |
| **ناشر** | **مدیران اندیشه** |
| **نویسنده** | **وحید شریفی** |
| **طراحی جلد** | **محمد انصاری** |
| **صفحه‌آرایی** | **سید علی حسینی** |
| **چاپخانه و صحافی** | **مدیران اندیشه** |
| **نوبت چاپ** | **اول ۱۴۰۰** |
| **شمارگان** | **۵۰۰ نسخه** |
| **قیمت** | **۵۰۰,۰۰۰ ریال** |
| **شابک** | **۹-۳۵-۷۷۵۲-۶۲۲-۹۷۸** |

# آموزش فناوری، امنیت اطلاعات

تألیف: وحید شریفی

نشر مدیران اندیشه

## تقدیم به:

این کتاب را به روح پدر مهربان و دل‌سوزم تقدیم می‌کنم؛ پدری که وجودش همیشه پشتوانهٔ محکمی بود؛ پدری که نه با حرفش، بلکه با عملش رسم تلاش و پشتکار را به من آموخت و امروز با یاد مهربانی‌هایش زندگی می‌کنم.

این کتاب را به مادر عزیزم تقدیم می‌کنم؛ غم‌خواری که لحظه‌ای من را از دعای پرمهرش بی‌نصیب نمی‌گذارد و دعای خیر او با ارزش ترین سرمایه من است.

این کتاب را به همسرم تقدیم می‌کنم که وجودش شوق زیستن، وفایش مایه عشق، صفایش مایه آرامش و صبرش مایه پشتکار من است.

## هزینه نسخه الکترونیک کتاب و مالکیت معنوی

خوانندهٔ گرامی و فهیم از اینکه امروز نسخهٔ الکترونیک کتاب **آموزش فناوری – امنیت اطلاعات** در اختیار شماست بسیار خوشنودیم؛ همان‌طور که می‌دانید، شما برای دریافت این کتاب به‌صورت الکترونیک هیچ هزینه‌ای پرداخت نکرده‌اید؛ اما این بدین معنا نیست که این کتاب رایگان است. سود حاصل از فروش این کتاب به مؤسسه خیریهٔ مردم‌نهاد هم کاسه مشهد مقدس تقدیم شده است؛

لذا از شما خواهشمندم حداقل هزینهٔ ده هزار تومان را به‌حساب خیریه مذکور واریز نمایید. اگر تمایل دارید، در این امر خیر مشارکت بیشتری کنید، می‌توانید بسته به صلاحدید و توان خود مبلغی بیش از حداقل هزینه پرداخت کنید.



**بنیاد خیریه هم کاسه – مشهد مقدس**

**اینستاگرام @ham_kase**

**شماره کارت بانکی به نام خیریه هم کاسه جهت واریز وجه**

۵۸۵۹۸۳۷۰۰۹۴۷۱۹۶۸

## پیشگفتار:

با توسعه پرشتاب فناوری اطلاعات در سال‌های آغازین هزاره سوم و رشد فراوان کاربران اینترنت و شبکه‌های اجتماعی، ضرورت آموزش و آگاهی نسبت به ابعاد این فناوری اجتناب‌ناپذیر است.

تسهیل در برقراری ارتباط و تبادل اطلاعات با سرعت و حجم بسیار بالا از ویژگی‌های مهم عصر کنونی بوده و در این زمان، اطلاعات به‌عنوان بزرگ‌ترین سرمایه افراد و سازمان‌های امروزی نقش مؤثری در روابط شخصی، اقتصادی، اجتماعی، سیاسی و فرهنگی ایفا می‌کند، اما علاوه بر مزایای فراوان، این سبک بهره‌برداری از فناوری، آسیب‌های فراوانی هم در پی استفاده بدون آموزش و آگاهی گریبان‌گیر افراد می‌گردد، لذا موضوع امنیت اطلاعات و آموزش صحیح مقابله با تهدیدات امنیتی ضروری است.

منابع زیادی در حوزه امنیت اطلاعات سازمانی، امنیت شبکه، زیرساخت و سیستم‌های رایانه‌ای به رشته تحریر درآمده است اما در این نوشتار سعی بر آن است نکات کاربردی و اثرگذار **جهت امنیت اطلاعات فردی** در فضای مجازی تقدیم شما خواننده گرامی گردد.

## فهرست مطالب

# فصل اول :آشنایی با مفاهیم مرتبط با اطلاعات و امنیت اطلاعات

**سؤالات مهم فصل اول:**

- ✓ **اطلاعات چیست؟**
- ✓ **امنیت اطلاعات به چه معناست؟**
- ✓ **مفاهیم اصلی امنیت اطلاعات کدام است؟**
- ✓ **اصطلاحات اصلی حوزه امنیت اطلاعات چیست؟**

## ۱-۱ اطلاعات چیست

درباره مفهوم اطلاعات و ارتباطات تاکنون تعاریف زیادی ارائه شده است. متخصصان حوزه‌های مختلف اغلب کوشیده‌اند جلوه‌ها و ویژگی‌های این پدیده‌ها را تا آنجا که به حوزه‌های تخصصی آنها مربوط می‌شود، تعیین کنند.

ازاین‌رو صاحب‌نظران این پدیده‌ها را در قلمروهای ریاضیات، زبان‌شناسی، اقتصاد، روان‌شناسی، ارتباطات و ... ویژگی‌های متفاوتی برای آنها برشمرده‌اند که در ادامه به برخی از آنها اشاره می‌شود.

برای آنکه داده‌ها تبدیل به اطلاعات گردند، لازم است که دسته‌بندی‌شده، محاسبه گردیده و متراکم گردند.

اطلاعات تصویری بزرگ‌تر **از داده** را جلوه می‌دهد؛ در واقع داده‌هایی با معنا و دارای هدف است.

اطلاعات می‌تواند روندی را در محیط به راه انداخته یا حتی دلالت بر نوعی الگوی فروش برای یک مقطع زمانی معین داشته باشد. به زبان دقیق‌تر اطلاعات در پاسخ به سؤالاتی دیده می‌شود که با واژه‌هایی از قبیل «چه کسی، چه چیزی، کجا، کی و چه تعداد» آغاز می‌گردند. (داون فورت و پرو ساک، ۲۰۰۰).

به عبارتی دیگر هرگاه داده‌ها را مورد تجزیه‌وتحلیل قرار دهیم و آن‌ها را قابل‌فهم و معنادار کنیم به اطلاعات دست‌یافته‌ایم. اطلاعات داده‌هایی هستند که دارای معنا و مفهوم هستند.

## ۲- ۱ امنیت اطلاعات

از ابتدای زندگی بشر امنیت یکی از دغدغه‌های اصلی انسان‌ها بوده است، امروزه با گسترش اینترنت و فضاهای شبکه‌ای لزوم توجه به امنیت برای فعالیت در این فضا بیش‌ازپیش احساس می‌شود. آسیب‌های فراوان ناشی از تخریب مبانی اخلاقی و اجتماعی و نداشتن امنیت روانی و فرهنگی در اثر هجوم اطلاعات آلوده و مخرب و یا سرقت اطلاعات شخصی یکی از دغدغه‌های اصلی کاربران فضای مجازی است.

امنیت اطلاعات[1] یعنی حفاظت از اطلاعات و سیستم‌های دارای اطلاعات در مقابل فعالیت‌های غیرمجاز، این فعالیت‌ها می‌تواند شامل دسترسی، استفاده، افشاء، خواندن، نسخه‌برداری یا ضبط، خراب کردن، تغییر و یا دست‌کاری باشد.(گروه واژه‌گزینی انجمن رمز ایران، ۱۳۹۰)

[1] Information Security

## ۳- ۱ مفاهیم اصلی امنیت اطلاعات

وقتی صحبت از امنیت اطلاعات می‌شود ناخودآگاه واژه‌هایی چون رایانه، کلمه عبور، اسم رمز، قفل‌های سخت‌افزاری و نرم‌افزاری و نرم‌افزارهای دیوار آتش و نظایر آن به ذهن می‌رسد. اما این تنها یکی از ابعاد امنیت اطلاعات است. اطلاعات در تعریف علمی آن به مجموعه‌ای از داده‌ها که دارای معنی و هدف باشند اطلاق می‌شود. می‌بینیم که در این تعریف هیچ صحبتی از رایانه و داده‌های الکترونیکی یا دیجیتالی نشده است. ازاین‌رو اطلاعات می‌تواند به هر نوع از داده‌های معنی‌دار نظیر اطلاعات چاپی، کاغذی، الکترونیکی، صوتی و تصویری گفته شود و حتی گفته‌های شفاهی ما به یکدیگر را نیز پوشش دهد. موارد سه‌گانه

حفظ درستی، محرمانگی و دسترس‌پذیری از مفاهیم اصلی امنیت اطلاعات است.

**درستی** (یکپارچه بودن): یعنی جلوگیری از تغییر داده‌ها به طور غیرمجاز و تشخیص تغییر در صورت دست‌کاری غیرمجاز اطلاعات.

**محرمانگی**: یعنی جلوگیری از دسترسی افراد غیرمجاز به اطلاعات.

**قابل‌دسترس بودن:** اطلاعات باید در زمان موردنیاز توسط افراد مجاز در دسترس باشند.

## ۴- ۱ اصطلاحات مرتبط با امنیت اطلاعات

در مباحث مربوط به امنیت کلماتی چون آسیب‌پذیری، تهدید، حمله و رفتار متقابل به‌دفعات مورداستفاده قرار می‌گیرند. در بسیاری از موارد شیوه به‌کارگیری این لغات اشتباه بوده و به‌جای یکدیگر مورداستفاده قرار می‌گیرند. در این بخش سعی شده تعریف مشخص و واضحی از لغات فوق برای استفاده در این کتاب ارائه گردد.

### ۱-۴-۱ آسیب‌پذیری[۲]

نقطه‌ضعف، حفره یا آسیب‌پذیری در حوزه امنیت اطلاعات عبارت است از هرگونه نقطه‌ضعف نرم‌افزاری، سخت‌افزاری یا تکنولوژیک که قابل سوءاستفاده باشد.(موسوی، ۱۳۹۶)

مشهورترین نقطه‌ضعف‌ها در نرم‌افزارها و سیستم‌های عامل وجود دارند که ممکن است از باگ‌های برنامه‌نویسی ناشی شوند. البته آسیب‌پذیری را فقط نباید در برنامه‌های کامپیوتری خلاصه کرد زیرا یک نقطه‌ضعف امنیتی ممکن است در عادات فردی کاربران نیز خودنمایی کند. مانند کارشناس یا مدیری که رمزهای عبورش را بر روی کاغذی یادداشت کرده و در زیر شیشه میزش قرار می‌دهد یا به بدنه کامپیوتر می‌چسباند و فراموش می‌کند که ممکن

[۲] Vulnerability

است توسط افراد غیرمجاز نیز رویت شود و به‌عنوان مثالی دیگر می‌توان از عدم استفاده از فایروال قدرتمند نام برد.

### ۲-۴-۱ تهدید[۳]

هر عملی که بالقوه با استفاده از آسیب‌پذیری‌های یک سیستم باعث سوءاستفاده از سیستم گردد، به بیان دیگر هر چیزی که می‌تواند آسیب‌پذیری را به طور عمدی یا به طور تصادفی مورد سوءاستفاده قرار دهد و باعث آسیب رساندن یا نابودی یک دارایی اطلاعاتی شود تهدید است در واقع تهدید وجود خطر بالقوه در سامانه‌هاست که در شرایط مناسب قابل‌استفاده برای نفوذ مهاجم به‌منظور سرقت اطلاعات یا ایجاد خسارت برای اطلاعات یا سامانه‌های اطلاعاتی است، همچنین می‌توان گفت تهدید شرایط یا حالتی است که می‌تواند امنیت را مختل کند.(موسوی، ۱۳۹۶)

### ۳-۴-۱ حمله[۴]

حمله تهدیدی هست که از حالت بالقوه به بالفعل درآمده باشد. در اصطلاح کامپیوتر و شبکه، به هرگونه تلاش جهت مشاهده اطلاعات، دست‌کاری اطلاعات، غیرفعال‌سازی سیستم‌های اطلاعاتی، نابودی اطلاعات، سرقت یا دسترسی غیرمجاز برای استفاده غیرمجاز از دارایی‌هایی اطلاعاتی (سرویس‌های اطلاعاتی) سازمان یا افراد (از طریق آسیب‌پذیری‌ها)

---

[۳] Threat
[٤] attack

، حمله گویند به‌عبارت‌دیگر حمله عبارت است از تجاوز به امنیت سیستم و دارایی‌های ارزشمند اطلاعاتی ناشی از تهدید threat از طریق آسیب‌پذیری (vulnerability) سیستم.

### ۱-۴-۴ اقدام متقابل

اقدام متقابل هر نوع فعالیت و تلاشی است که به‌منظور کاهش ریسک یک تهدید صورت می‌پذیرد.

### ۱-۴-۵ بدافزار[۵]

بدافزارها در اصل قطعه کدهایی هستند که توسط برنامه‌نویسان نوشته می‌شوند تا به‌وسیله آن بدون اجازه مالک سیستم، آن را آلوده و اقدام به کارهای ناخواسته یا خرابکارانه کنند.

این واژه به‌صورت عمومی به‌تمامی کدها و برنامه‌های مخرب اطلاق می‌شود و به‌طورکلی هر نوع کدی که روی سیستم شما قرار بگیرد و عملیاتی ناخواسته را انجام دهد به‌عنوان بدافزار شناخته می‌شود. بدافزار می‌تواند گوشی تلفن، تبلت و کامپیوترها را آلوده کند.

بدافزار پس از ورود به سیستم شما می‌تواند کارهایی مانند ارسال ایمیل‌های اسپم، سرقت اطلاعات و رمز عبورهای اکانت هاستینگ و ... انجام دهد.

بدافزارها می‌توانند از انواع روش‌ها و تکنیک‌های مختلف برای اجرای خود استفاده کنند. مثلاً بعضی از آنها از سیستم شما به‌عنوان قربانی برای انجام عملیات تخریب روی دیگر

---

۵ Malware

سیستم‌ها استفاده می‌کنند، بعضی از آنها اقدام به جمع‌آوری اطلاعات شخصی کاربران مانند شماره‌حساب بانکی، رمز عبور و نام‌های کاربری و ... می‌کنند و حتی ممکن است باعث تخریب در سیستم کاربران شوند.

بدافزار همچنین می‌تواند از طریق حفره‌های امنیتی موجود بر روی برنامه سایت شما وارد سیستم شود.

### ۶-۴-۱ باج‌افزار[۶]

اغلب نوعی بدافزار شناخته می‌شود اما به دلیل ریسک جدی که در بردارد، ارزش آن را دارد که به‌صورت جداگانه موردبحث قرار گیرد. باج‌افزار در صورت آلوده کردن رایانه، می‌تواند اطلاعات را در قبال دریافت باج در کنترل بگیرد و در سال‌های اخیر موارد وقوع حملات باج‌افزاری افزایش پیدا کرده است.

### ۷-۴-۱ هک[۷] و هکر[۸]

هک به روشی هوشمندانه برای حل مشکلی ویژه گفته می‌شود، و هکر به کسی گفته می‌شود که از این روش‌های هوشمندانه استفاده می‌کند. ولی متأسفانه امروزه هکر به معنای

---

۶ ransomware
۷ Hack
۸ Hacker

شخصی است که به‌منظور اخاذی و یا خرابکاری در سیستم‌ها و سایت‌ها شروع به خراب‌کاری می‌کند.

### ۸-۴-۱ هکر کلاه سفید[۹]

به هکری گفته می‌شود که به‌منظور پیداکردن مشکلات موجود در سرورها و نرم‌افزارها به آن‌ها نفوذ می‌کند و پس از گزارش مشکل به مسئولین در رفع عیب آن عیب سهیم است. هکرهای کلاه سفید برخی اوقات در مسابقاتی شرکت می‌کنند که شرکت‌های امنیتی برگزار می‌کنند.

مثلاً شرکت گوگل و تلگرام برای گزارش باگ به کاربران هدایای نقدی می‌دهند. هکرهای کلاه سفید می‌توانند از این طریق جوایز ده‌ها هزاردلاری و یا حتی چند صد دلاری برنده شوند. برخی مدیران سایت‌ها و سرورها نیز به گروه‌های هک کلاه سفید مبالغی می‌دهند تا سعی کنند آن سیستم را هک کنند و عیب‌های موجود را گزارش دهند.

[۹] White Hat Hacker

### ۱-۴-۹ هکر کلاه‌سیاه[۱۰]

به هکری گفته می‌شود که به‌منظور اخاذی و یا تخریب وارد سیستم‌ها و سایت‌ها می‌شوند. هکرهای کلاه‌سیاه در همه جای دنیا تحت تعقیب هستند و اعمال آن‌ها خلاف قانون تلقی می‌شوند.

### ۱-۴-۱۰ هکر کلاه خاکستری[۱۱]

به هکری گفته می‌شود که گاهی اعمال هکرهای کلاه‌سیاه و گاهی اعمال هکرهای کلاه سفید را انجام می‌دهد.

### ۱-۴-۱۱ هکر نخبه[۱۲]

هکر نخبه یا الیت هکری است که در بین هکرهای دیگر اعتبار اجتماعی بالایی دارد. این فرد معمولاً مشکلات امنیتی تا به امروز ناشناخته را کشف می‌کند و با گزارش آن‌ها ثابت می‌کند که واقعاً به چیزی دست پیدا کرده که پیش‌ازاین ناشناخته بوده است. آپدیت‌های سیستم‌عامل‌ها معمولاً محصول کشف و گزارش مشکلات توسط این هکرها هستند.

---

[۱۰] Black Hat Hacker
[۱۱] Grey Hat Hacker
[۱۲] Elite hacker

### ۱-۴-۱۲ کِرَکِر[۱۳]

همان‌طور که در بالا گفته شد یک هکر می‌تواند یک شخص مفید و کارآمد باشد، ولی یک کرکر یک شخص کاملاً مضر است. کرکرها به سرور بانک‌ها نفوذ می‌کنند و آن‌ها را متوقف می‌کنند، سایت‌های مهم را با روش‌هایی پیچیده از کار می‌اندازند و یا حتی پسورد کاربران را به سرقت می‌برند و در بازار سیاه می‌فروشند.

### ۱-۴-۱۳ واکِر[۱۴]

واکر به نفوذگر کلاه سیاهی گفته می‌شود که به‌منظور سرقت اطلاعات وارد سیستم‌های دیگر می‌شود. مثلاً یک واکر بر اساس سفارشی که می‌گیرد وارد سامانه ثبت‌احوال شده و اطلاعات محل سکونت یک شخص را در اختیار خلاف‌کاران می‌گذارد.

### ۱-۴-۱۴ پریکِر[۱۵]

پریکرها به شبکه‌های تلفن نفوذ می‌کنند و مکالمه‌ها را استراق می‌کنند. این پریکرها ممکن است پروژه‌هایی را برای سازمان‌های مخفی و خلاف‌کار اجرا کنند، بنابراین پریکر بودن یک جرم است و پریکرها در تمام نظام‌های حقوقی جهان محاکمه و مجازات می‌شوند.

---

[۱۳] Cracker
[۱٤] Wacker
[۱۵] Preaker

البته برخی از پریکرها نیز تنها برای خودکار می‌کنند و از دانش خود برای تماس مجانی استفاده می‌کنند.

### ۱۵-۴-۱ فیک پیج[۱۶]

فیک پیج به معنی صفحه جعلی است. در حملات فیشینگ که دزدیدن اطلاعات کاربران است (مثلاً اطلاعات بانکی) هکر یک صفحه جعلی مشابه درگاه بانک درست می‌کند و کاربر اطلاعات خود را وارد آن می‌کند و گمان می‌کند که این درگاه، درگاه اصلی بانک است، غافل از اینکه به‌راحتی تمام اطلاعات خود را برای هکر فرستاده است. این صفحات جعلی، فیک پیج هستند.

### ۱۶-۴-۱ باگ[۱۷]

باگ به معنی نقص نرم‌افزاری است و می‌تواند منجر به خراب‌شدن، ازکارافتادن یا نشت اطلاعات سیستم شود. نخستین‌بار لفظ باگ به حشره‌ای اطلاق شد که منجر به خراب‌شدن کامپیوترها شده بود ولی با پیشرفت دانش و مستحکم‌تر شدن و کوچک‌تر شدن دستگاه‌ها دیگر حشره‌ها نمی‌توانند به کامپیوترها آسیب جدی‌ای وارد کنند! امروزه باگ به اشکالات نرم‌افزاری گفته می‌شود که در تمام نرم‌افزارها وجود دارد. در دنیای کامپیوتر و شبکه نمی‌توان نرم‌افزار یا سیستم‌عاملی را بی‌عیب‌ونقص و یا به‌اصطلاح بدون باگ یافت، مزیت

---

[۱۶] Fake page
[۱۷] bug

سیستم‌عامل قدرتمندی مانند لینوکس این است که باگ‌هایش به‌سرعت کشف و بر طرف می‌شوند. ولی یافتن باگ در سیستم‌عامل‌ها و نرم‌افزارهای معروف و حرفه‌ای کاری بسیار پیچیده، زمان بر و برای اکثر متخصصین ناممکن است.

### ۱۷-۴-۱ هش [۱۸]

به دلیل پرخطر بودن پایگاه‌های داده متخصصین، پسوردها را به‌صورت معمولی در پایگاه‌داده ذخیره نمی‌کنند و برای ذخیره کردن، آن‌ها را تبدیل به هش می‌کنند تا به‌سادگی نتوان آن‌ها را خواند. البته راه‌حل‌هایی وجود دارد که گاهی نفوذگران برای تفسیر هش‌ها استفاده می‌کنند که برخی اوقات مثمر ثمر هستند.

### ۱۸-۴-۱ کرک[۱۹]

عملیات شکستن سدهای امنیتی و انجام عملیات نفوذ را کرک کردن می‌گویند. مثلاً ممکن است یک نرم‌افزار برای استفاده نیازمند لایسنس خاصی باشد. نفوذگران این نرم‌افزار را به‌اصطلاح کرک می‌کنند تا بدون نیاز به لایسنس بتوان از آن‌ها استفاده کرد.

---

[۱۸] hash
[۱۹] crack

### ۱-۴-۱۹ شل[۲۰]

بسیاری از باگ‌ها و مشکلات موجود در نرم‌افزارها و سیستم‌ها منجر به نفوذی محدود به سیستم می‌شوند. برای افزایش دسترسی پس از نفوذ از شل‌ها استفاده می‌شود.

### ۱-۴-۲۰ باگ‌های پابلیک[۲۱]

همان‌طور که در بالا گفتیم هر سیستم‌عامل و یا نرم‌افزاری باگ‌هایی را در خود دارد. این باگ‌ها ممکن است در دسترس همه نفوذگران باشند، و به دلیل آپدیت نشدن سیستم قابل‌استفاده باشند.

### ۱-۴-۲۱ باگ‌های پریویت[۲۲]

بر عکس باگ‌های پابلیک این باگ‌ها در اختیار برخی از افراد قرار دارند و تا علنی نشدن مورداستفاده قرار می‌گیرند. باگ‌ها بعد از علنی و پابلیک شدن به‌سرعت توسط توسعه دهندگان سیستم بر طرف می‌شوند.

---

[۲۰] shell
[۲۱] PUBLIC BUG
[۲۲] pirouette

### ۱-۴-۲۲ سایت‌های ثبت هک

نفوذگران ممکن است به مدت چند دقیقه بتوانند یک سیستم را هک کنند و صفحه اصلی آن را دی فیس کنند، بعدها برای اثبات اینکه سابقاً توانسته‌اند آن سایت را هک کنند نیاز به یک دلیل معتبر دارند. برخی از سایت‌ها این وظیفه را برعهده دارند و پس از هک شدن یک سایت می‌توانند وضعیت فعلی آن را ذخیره کنند.

یکی از این سایت‌ها سایت zone-h.org است

### ۱-۴-۲۳ بات نت[۲۳]

یک بات نت مانند چمدانی پر از "شبکه ربات" است. در واقع مجموعه‌ای از دستگاه‌های آلوده است که می‌تواند برای فعالیت‌های مشکوک، از رمزگذاری گرفته تا حملات مختلف و نظرات اسپم خودکار در وبلاگ‌ها، مورداستفاده قرار بگیرد.

[۲۳] Botnet

## ۵-۱ جمع‌بندی

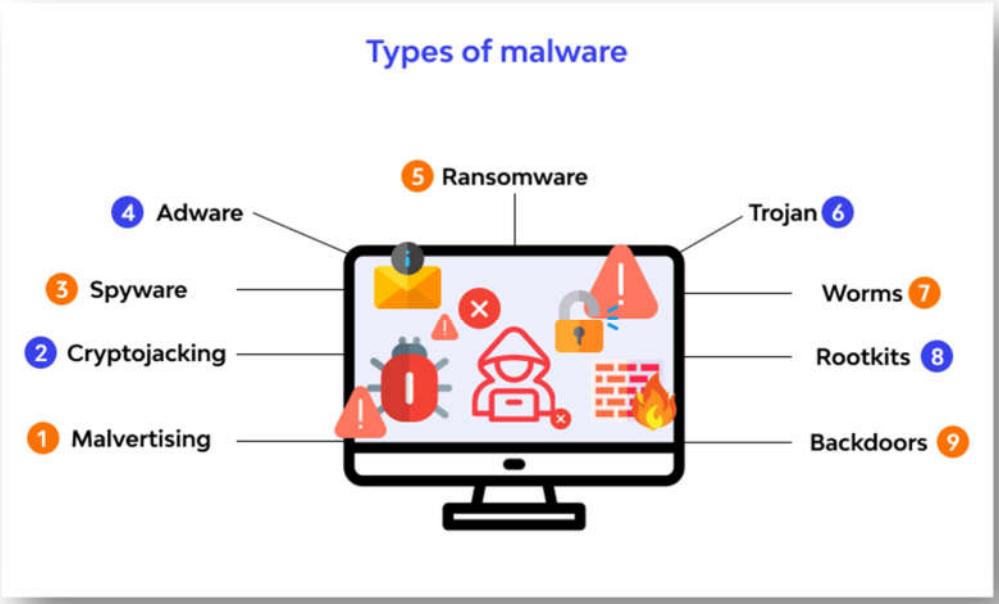
نظر به اینکه تعاریف و اصطلاحات مطرح شده، در فصل‌های بعدی کتاب مکرر استفاده می‌شود در این فصل، سعی شد برای آشنایی بیشتر خوانندگان گرامی با مباحث این حوزه ضمن تعریف دقیق اطلاعات، مفاهیم و اصطلاحات مرتبط با اطلاعات و امنیت اطلاعات نیز توضیح داده شود.

همان‌طور که اشاره شد اطلاعات در تعریف علمی آن به مجموعه‌ای از داده‌ها که دارای معنی و هدف باشند اطلاق می‌شود و امنیت اطلاعات یعنی حفاظت از اطلاعات و سیستم‌های دارای اطلاعات در مقابل فعالیت‌های غیرمجاز.

با توجه به موارد فوق تمامی افراد جامعه بشری امروزه اطلاعات متنوعی را در اختیار دارند که حفاظت از آن در مقابل فعالیت‌هایی از قبیل دسترسی، استفاده، افشاء، خواندن، نسخه‌برداری یا ضبط، خراب کردن، تغییر و یا دست‌کاری امری ضروری است.

در فصل بعد به یکی از مهم‌ترین حوزه‌های امنیت اطلاعات با عنوان انواع حملات سایبری که امروزه اکثر افراد جامعه در فضای مجازی و سیستم‌های رایانه‌ای با آن مواجه هستند پرداخته می‌شود.

# فصل دوم: معرفی بد افزار ها و حملات سایبری




**سؤالات مهم فصل دوم:**

- ✓ **حملات سایبری چیست؟**
- ✓ **انواع بدافزارها کدام‌اند؟**
- ✓ **حمله به روش مهندسی اجتماعی چیست؟**
- ✓ **فیشینگ به چه معناست؟**
- ✓ **باج‌افزار چیست؟**
- ✓ **مهم‌ترین راه کارهای مقابله با تهدیدات کدام موارد هستند؟**

## ۱-۲ حملات نرم‌افزاری

حمله سایبری یک اقدام مخرب و آگاهانه توسط یک فرد یا سازمان برای نقض سیستم اطلاعاتی شخص یا سازمان دیگر است. معمولاً مهاجم به دنبال نوعی مزاحمت برای ایجاد اختلال در سیستم شخصی و یا شبکه قربانی است. به بیان دیگر حمله سایبری هرگونه تلاش برای افشا، تغییر، غیرفعال‌کردن، تخریب، سرقت یا دستیابی به دسترسی غیرمجاز یا استفاده غیرمجاز از یک دارایی است.(گروه واژه‌گزینی انجمن رمز ایران، ۱۳۹۰)

حملات سایبری دامنه متنوعی دارند، از شوخی‌های معمولی گرفته تا کرم‌های مخرب رایانه‌ای که توسط حافظه‌های قابل‌حمل جابه‌جا شده و امنیت کلی کشوری را به مخاطره می‌کشند. ازآنجایی‌که امروزه تمامی زندگی ما به تکنولوژی، رایانه‌ها و اینترنت گره‌خورده است اطمینان از ایمن بودن این ابزارها بسیار حیاتی است.

اغلب هکرها بدافزارها را با اهداف ذیل و بدون آگاهی شما به کار می‌گیرند:

۱- انتقال داده‌ها به خارج از سیستم شما

۲- ردیابی نحوهٔ استفاده از کامپیوتر، تاریخچهٔ فایل‌هایی که به آن‌ها سر زده‌اید، فعالیت بر روی مانیتور و حتی تعداد دفعات فشار دکمه‌ها

۳- دسترسی به دوربین و یا میکروفون کامپیوتر یا تبلت شما

۴- تحت کنترل درآوردن سخت‌افزار دستگاه شما به طور کامل

حمله سایبری یک اقدام مخرب و آگاهانه توسط یک فرد یا سازمان برای نقض سیستم اطلاعاتی شخص یا سازمان دیگر است. معمولاً مهاجم به دنبال نوعی مزاحمت برای ایجاد اختلال در شبکه قربانی است.

حملات سایبری در لیست خطرات جهانی رتبه پنجم را در سال ۲۰۲۰ به خود اختصاص داده است و به یک قاعده جدید در بخش‌های دولتی و خصوصی تبدیل شده است. این صنعت پرخطر در سال ۲۰۲۱ همچنان درحال‌رشد است، زیرا انتظار می‌رود حملات سایبری اینترنت اشیا به‌تنهایی تا سال ۲۰۲۵ دوبرابر شود. (گزارش۲۰۲۰ سایت embroker.com)

## ۲-۲ انواع بدافزارها و حملات

در ادامه به تعدادی از معروف‌ترین انواع حمله سایبری و بدافزارها که مرتبط با کاربران است، اشاره می‌شود:

### ۱-۲-۲ ویروس[۲۴]

ویروس رایانه‌ای نرم‌افزاری است که دائماً از خود کپی می گیرد و آن را در برنامه‌های دیگر قرار می دهد.

[۲۴] Virus

با وجود اینکه همه ویروس ها خطرناک نیستند اما بسیاری از آنها با هدف تخریب برنامه‌های کاربردی و یا حتی سیستم عامل نوشته شده‌اند. از جمله خطراتی که ویروس ها دارند این است که می‌توانند فایل‌های روی یک دیسک را به طور کامل پاک کنند و یا حتی کل هارد دیسک را فرمت کنند. آنها می‌توانند به گونه ای عمل کنند که نرم‌افزار به نحوی آسیب ببیند که دیگر درست نشود و یا باعث کندی سیستم ها و نقص فنی آنها شوند.

### ۲-۲-۲ کرم[۲۵]

کرم های کامپیوتری نوعی از بدافزارها هستند که بوسیله شبکه های کامپیوتری کپی هایی از خودشان را برای دیگران ارسال می کنند.

تفاوت کرم ها با ویروس ها در این است که ویروس ها با متصل شدن به برنامه‌های دیگر تکثیر می‌شوند اما کرم ها بدون نیاز به برنامه‌های دیگر خود را تکثیر کرده و جابجا می‌شوند.جدی ترین آسیب کرم ها آسیبی است که به شبکه وارد می کنند. به‌عنوان‌مثال با تکثیر خود از کامپیوتری به کامپیوتر دیگر و پر کردن هارد دیسک و مصرف کردن پهنای باند شبکه مشکلات جدی را به بار می آورند.

[۲۵] Worm

## ۳-۲-۲ تروجان[۲۶]

تروجان  یک برنامه به‌ظاهر بی‌عیب‌ونقص است که به‌عنوان جلوه ای برای مخفی کردن کد مخرب درون خود عمل می‌کند. تروجان‌ها می‌توانند هر کاری، از سرقت داده‌ها گرفته تا کنترل سیستم از راه دور را انجام دهند. این برنامه نام خود را از اسب معروف یونانی (Trojan Horse) گرفته که از یک آسیب‌پذیری مشابه بهره می برد.

ایده تروجان به یک افسانه یونانی باز می‌گردد. یونانیان که پس از مدت‌ها جنگ نتوانستند قلعه تروا را فتح کنند به نشانه صلح یک اسب بزرگ را به‌عنوان هدیه به درون قلعه می‌فرستند. سربازان قلعه تروا شادمان از پایان جنگ تا پاسی از شب به شادمانی پرداخته بودند ولی غافل از این که درون اسب بزرگ پر بود از سربازان تا دندان مسلح. سربازان درون اسب بزرگ چوبی پس از آرام شدن قلعه و اطمینان از خواب افراد درون قلعه از اسب چوبی خود بیرون آمدند و دروازه را برای سربازان یونانی بازکردند. این ایده دقیقاً در دنیای هک نیز استفاده می‌شود، یعنی ارسال فایلی مخرب به درون سیستم در قالبی آرام و بی آزار، ولی همین فایل بی آزار موجب نابودی سیستم خواهد شد.

مثلاً کاربر یک نرم‌افزار از اینترنت دانلود و اجرا می‌کند درحالی‌که همراه با اجرای نرم‌افزار، کد مخربی از نوع تروجان نیز وارد سیستمش می‌شود.

---

[۲۶] Trojan

### ۴-۲-۲ بَکدُر[۲۷]

بکدُر یک نقطه دسترسی است که جهت دسترسی سریع و غیرمستقیم به برنامهٔا سیستم طراحی شده و معمولاً برای اهداف مخرب کاربرد دارد.

یک بکدر می‌تواند توسط حمله‌ای که از یک آسیب‌پذیری امنیتی شناخته شده استفاده می‌کند، نصب شود و بعداً برای دسترسی به یک سیستم مورد بهره‌وری قرار گیرد.

فرض کنید یک نفوذگر پس از مدت‌ها تلاش بتواند پسورد نفوذ به سیستم را بیابد و به آن نفوذ کند. عملیات نفوذ و دستیابی به اطلاعات ممکن است یک ماه طول بکشد، ولی مدیر سیستم پس از چند روز پسورد سیستم را عوض می‌کند و دسترسی نفوذگر کاملاً قطع می‌شود.

برای نفوذ های بعدی، نفوذگران پس از نفوذ به سیستم در اسرع وقت یک بکدر (در پشتی) روی سیستم قربانی نصب می‌کنند تا در صورت بسته شدن دسترسی‌ها باز بتوانند به آن سیستم نفوذ کنند.

---

[۲۷] Backdoor

## ۵-۲-۲ نرم‌افزار جاسوسی[۲۸]

اسپای ویر این بدافزارها اطلاعات را از سیستم‌های کامپیوتری سرقت می‌کنند و می‌توانند توسط دیگر بدافزارها مانند اسب تروجان یا کرم‌ها، نصب شوند و یا اینکه نفوذگر مستقیماً آنها را نصب کند.

یکی دیگر از روش‌های انتشار نرم‌افزارهای جاسوسی استفاده از روش‌های تحریکات جمعی یا مهندسی اجتماعی مانند استفاده از ایمیل برای ترغیب کاربران به نصب یک برنامه ظاهرا مفید، است.

برخی از نرم‌افزارهای جاسوسی به نام کیلاگر[۲۹] وجود دارند که پس از اجرا هر اطلاعاتی که کاربر تایپ می‌کند را در جایی ذخیره می‌کنند و حتی می‌توانند از کارهای کاربر فیلم تهیه کرده و در شبکه یا اینترنت برای دیگران ارسال نمایند.

---

[۲۸] Spyware
[۲۹] Keylogger

### ۲-۲-۶ کیلاگر

کیلاگر به برنامه مخربی گفته می‌شود که وظیفه ذخیره کلیدهای فشرده شده روی کیبورد و ارسال آن‌ها به شخص نفوذگر بر عهده دارد. شما تقریباً تمام اطلاعات مهم را با استفاده از کیبورد به کامپیوتر خود می‌دهید، نام کاربری ها، رمز عبور و آدرس‌ها. شخص نفوذگر به‌منظور سرقت اطلاعات شما یک کیلاگر را به درون سیستم شما می‌فرستد تا اطلاعات شما را برباید.

### ۲-۲-۷ اکسپلویت

اکسپلویت[۳۰] کدی برای سوءاستفاده از حفره‌های امنیتی در برنامه‌های کاربردی، سیستم‌عامل‌ها، هسته سیستم‌عامل‌ها، وب سرور و در کل هر نرم‌افزاری که در یک شبکه و یا کامپیوتر کار می‌کند است. اکسپلویت ها می‌توانند با زبان‌های مختلف برنامه‌نویسی نوشته شوند و هدف آنها استفاده و ایجاد دسترسی غیرمجاز، ایجاد حملات مختلف و یا اختلال در سیستم‌های کامپیوتری است.

اکسپلویت ها معمولاً هنگام کشف آسیب‌پذیری‌ها و یا بعد از کشف حفره‌های امنیتی نوشته می‌شوند، اکسپلویت نویس ها عمدتاً هکر هستند که با تکنیک‌ها و متدهای مختلف اقدام

---

[۳۰] exploit

به نوشتن کدهای مخرب می‌نمایند، بعضاً دیده می‌شود که متخصصان و مدیران امنیتی مطرح نیز اقدام به نوشتن اکسپلویت، برای اثبات آسیب‌پذیری‌های مهم کرده اند.

به بیان دیگر اکسپلویت  یا همان کد مخرب، حمله‌ای است که از یک ضعف در سیستم شما استفاده می‌کند و می‌تواند در قالب نرم‌افزار، بیت‌های داده و حتی مهندسین اجتماعی ظاهر شود (مثل اینکه تظاهر کند شخصی از تیم IT شما است که برای انجام به‌روزرسانی امنیتی به رمز عبورتان احتیاج دارد). برای به‌حداقل‌رساندن سوءاستفاده باید نرم‌افزار خود را به‌روز کرده و از فنون مهندسی آگاه باشید.

### ۸-۲-۲ رات[۳۱]

رات ها ابزار یا برنامه‌هایی هستند که برای کنترل یک سیستم از سیستمی دیگر استفاده می‌شوند و امکانات بسیار کاملی برای کنترل نفوذگر دارد در واقع رات ها کیلاگر های پیشرفته‌ای هستند که دسترسی بسیار بیشتری به مهاجم می‌دهد.

رات ها می‌توانند برای انواع سیستم‌عامل‌ها باشند برای مثال می‌تواند برای هک یک سیستم ویندوزی باشد و کنترل آن در لینوکس انجام شود یا هر دو فقط در ویندوز انجام

[۳۱] RAT

شوند در کل محدودیت سیستم‌عامل ندارد و می‌تواند برای هر سیستم‌عاملی حتی اندروید باشد.

رات‌ها از کیلاگرها وسیع‌تر هستند و حتی امکان ارسال تصویر از مانیتور و یا حتی وصل کردن مهاجم به کامپیوتر قربانی را بر عهده دارند. ممکن است یک نفوذگر ابتدا با کیلاگر دسترسی‌هایی بر سیستم قربانی بیابد و سپس یک رات را روی آن سیستم نصب کند.

### ۹-۲-۲ حمله با استفاده از مهندسی اجتماعی[۳۲]

خیلی از افراد فکر می‌کنند عملیات هک تنها با دانش فنی و تخصص انجام می‌پذیرد درصورتی‌که اصلاً این‌گونه نیست. بسیاری از پروژه‌های هک بزرگ با کمک مهندسی اجتماعی که کمک‌گرفتن از قربانی است انجام می‌پذیرد.

سناریو زیر را بادقت بخوانید:

یک هکر می‌خواهد وارد یک شبکه کامپیوتری شود ولی نمی‌تواند ضعفی در ورود به شبکه پیدا کند. یک خانم را مأمور می‌کند با یکی از کارمندان آن شبکه دوست شود و به او یک فلش با آهنگ‌های موردعلاقه بدهد. در ساعت کاری این خانم با کارمند شبکه تماس می‌گیرد و می‌گوید یکی از کلیپ‌های موجود در فلش با نامی معین را اجرا کند چون یک آهنگ نیست بلکه یک پیغام صوتی عاشقانه است.

---

[۳۲] social engineering attack

کارمند شبکه باذوق و شوق آن فلش را برای شنیدن آن فایل صوتی به کامپیوتر خود می‌زند و یک ویروس مخرب را ناخواسته وارد آن شبکه می‌کند و برای نفوذگر امکان نفوذی بی‌دردسر را محیا می‌کند. به سناریو مذکور مهندسی اجتماعی می‌گویند.

### ۱۰-۲-۲روت کیت[۳۳]

روت کیت  یک کد مخرب است که خود را در سیستم شما پنهان کرده و از شناسایی خود جلوگیری می‌کند و بدافزارها را قادر می‌سازد به سراسر سیستم شما دسترسی پیدا کنند. اگر مهاجمان به سیستم شما یک‌بار دسترسی کامل داشته باشند، می‌توانند از روت کیت برای ادامه دسترسی برای مدت طولانی استفاده کنند.

روت کیت‌ها پس از نفوذ به سیستم علاوه بر وظایف تروجان‌ها خود را جایگزین بخش‌های مهمی از سیستم‌عامل حتی هسته آن می‌کنند و دسترسی‌های مهلک و بعضاً غیرقابل‌شناسایی به نفوذگران می‌دهند.

اولین روت کیت‌ها در سال ۱۹۹۰ شناسایی شدند و از آن زمان تا کنون روت کیت‌های متنوعی برای سیستم‌های عامل لینوکسی و ویندوزی نوشته شده‌اند، هرچند تعداد روت کیت‌هایی که برای سیستم‌عامل لینوکس نوشته شده است بیشتر از ویندوز است.

البته خطرناک‌ترین نوع روت کیت آن نوعی است که خود را جایگزین هسته سیستم‌عامل می‌کند، چون دیگر هسته سیستم‌عامل را به دست گرفته است و حتی روی عملکرد

---

[۳۳] rootkits

نرم‌افزارهای اسکن ویروس و روتکیت هم تأثیر می‌گذارد و به‌سادگی آن‌ها را غیرفعال و بی‌خاصیت می‌کند. با روت کیت‌های سطح هسته شخص نفوذگر می‌تواند تمام عملیات و فعالیت‌ها را به‌صورت کامل و بی‌دردسر ذخیره و شنود کند.

### ۱۱-۲-۲ دورک[۳۴]

دورک ها شبه کدهای کاربردی در موتورهای جست‌وجو هستند تا جست‌وجو را برای کاربران راحت کنند اما هکرها، استفاده‌های نادرست از این کدها می‌کنند و در یافتن تارگت خود از این کدها استفاده می‌کنند.

در واقع به معنای افشای ناخواسته اطلاعات امنیتی در اینترنت است که توسط موتورهای جستجو انجام می‌شود. برای همین به گوگل دورک، گوگل هکینگ نیز گفته می‌شود، چرا که نتیجه دورک شدن اطلاعات، هک شدن آن توسط هکر ها نیز می‌تواند باشد.

به این صورت که وقتی هکر با استفاده از گوگل هکینگ آسیب‌پذیری را پیدا می‌کند می‌تواند جستجویی که انجام داده است را در اینترنت برای استفاده دیگران قرار بدهد و آسیب‌پذیری‌های سایر وب‌سایت‌ها را نیز شناسایی کند. استفاده از دورک ها می‌توانند گاهی پیچیده باشد به‌طوری‌که نوشتن برخی از آن‌ها در برخی مواقع نیاز به دانش بسیار بالا دارد. البته قابل‌توجه است که این دورک ها تنها به هدف هکینگ نیستند بلکه هدف اصلی آن‌ها انجام جستجوی بهینه است. دورک ها را می‌توانیم دانلود، کپی و استفاده کنیم.

---

[۳۴] Dork

برای اینکه وب‌سایت‌های ما درگیر دورک شدن نشود بهتر است دسترسی موتورهای جستجو به قسمت‌های حساس و امنیتی وب‌سایت و دیگر قسمت‌هایی که پلاگین [۳۵]ها نصب شده‌اند و بر روی وب‌سایت ما نشان داده می‌شوند را مسدود کنیم.

### ۱۲-۲-۲ ابزارهای تبلیغاتی مزاحم

ابزارهای تبلیغاتی[۳۶] ،شاید برای شما هم پیش‌آمده باشد که زمانی که در حال وب‌گردی هستید تعداد زیادی لینک، پاپ‌آپ و تبلیغات بر روی صفحه‌نمایش ظاهر شود که ممکن است باعث نارضایتی شما نیز بشوند.

به‌واسطه کلیک بر روی این تبلیغات به سایت دیگری هدایت می‌شوید که این امر سیستم شما را با خطر مواجه می‌کند. گاهی می‌توان از نصب این ابزارها خودداری کرد اما در بعضی مواقع هم به‌صورت خودکار نصب می‌شوند.

[۳۵] plugin
[۳۶] Adware

### ۱۳-۲-۲ ترس‌افزار[۳۷]

ترس افزار نه‌تنها به سیستم کاربر آسیب می‌زند بلکه او را مجبور می‌کند تا با کارت خود اقدام به خرید نماید.

معمولاً با استفاده از یکسری ترفند، کاری می‌کند که کاربر تصور کند که سیستمش به یک ویروس کامپیوتری یا دیگر برنامه‌های مخرب آلوده شده است و تنها برنامه scareware است که می‌تواند آن را پاک‌سازی کند. به‌محض اینکه کاربر این برنامه را دانلود و نصب کرد ممکن است برنامه مخرب دیگری نیز هم‌زمان بر روی کامپیوتر نصب گردد که می‌تواند اطلاعات شخصی کاربر را بردارد و یا به سیستم کاربر از راه دور دسترسی داشته باشد و از این طریق حملات دیگری را اجرا کند. اما ممکن است هدف بدافزار تنها واریز پول به‌حساب تولیدکننده آن از طریق خرید یک برنامه ضدویروس یا برنامه افزایش کارایی سیستم و یا دیگر برنامه‌های قانونی باشد. در مجموع می‌توان گفت ترس افزار با ترساندن کاربر او را مجبور می‌کند تا برنامهٔ مخربی را بر روی سیستمش نصب کند و یا با پرداخت هزینه نرم‌افزار خاصی را بخرد.

---

[۳۷] Scarewear

## ۱۴-۲-۲ راه‌های جلوگیری از ترس افزار

۱. فعال‌کردن ویژگی مسدودکردن pop-up بر روی مرورگر.

۲. دانلود نکردن برنامه ضدویروس از پنجره pop-up یا لینکی ارسالی از طریق ایمیل.

۳. استفاده از دکمه X سیستم‌عامل در گوشه پنجره pop-up در هنگام بستن pop-up.

۴. نصب برنامه ضدویروس به همراه برنامه ضد اسپم و به‌روزرسانی آن

۵. به‌روزرسانی خودکار سیستم‌عامل و دیگر نرم‌افزارهای نصب شده بر روی آن.

۶. استفاده از حساب کاربری استاندارد به‌جای حساب کاربری مدیر.

۷. روشن نگه‌داشتن دیواره آتش ویندوز (فایروال).

### ۱۴-۲-۲ باج‌افزارها

در روش باج‌افزار[۳۸] هکر با قراردادن باج‌افزار روی دستگاه قربانی او را تهدید می‌کند، باج‌افزار یک نوعی از بدافزارها است که به مجرمان این امکان را می‌دهد تا بتوانند از طریق یک کنترل از راه دور، کامپیوتر قربانی را قفل کنند به‌طوری‌که کاربر نتواند از سیستم خود استفاده کند.

گاهی اوقات مجرمان تنها قسمتی از کامپیوتر قربانی را که قابل‌دسترسی است، قسمت keypadیا صفحه‌کلید مجازی قرار می‌دهند که قربانی بتواند رمز را وارد و پول را پرداخت کند، گاهی هکرها با قراردادن یک تصویر نامناسب روی کامپیوتر شخص یا اتهام فعالیت غیرقانونی به آن‌ها، شخص را تحت‌فشار می‌گذارند که هر چه سریع‌تر پول درخواستی آن‌ها را پرداخت کنند تا هکرها قفل کامپیوتر آن‌ها را باز کنند.

[۳۸] Ransomware

برای جلوگیری از ورود باج‌افزار

۱- هیچ‌گاه به ایمیل‌های ناشناس پاسخ ندهید یا ایمیل‌هایی را که در قسمت spam ایمیلتان قرار دارد را باز نکنید.

۲- تنها از وب‌سایت‌های رسمی و امن یا وب‌سایت‌هایی که می‌شناسید استفاده کنید.

۳- قبل از آنلاین شدن، از وجود آنتی‌ویروس و دیوار آتش مؤثر و به‌روز روی کامپیوتر خود مطمئن شوید.

به طور منظم از اطلاعات خود نسخه پشتیبان تهیه کنید چرا که برخی از باج‌افزار ها می‌توانند حتی فایل‌های مبتنی بر ابر ذخیره سازی را نیز آلوده کنند.

اگر کامپیوتر شما از طریق باج‌افزار قفل شده باشد، حتماً برای مشاوره و راهنمایی از یک منبع قابل‌اعتماد استفاده کنید و با یک متخصص مورد اعتماد مشورت نمایید و به‌هیچ‌وجه پول را واریز نکنید چرا که حتی اگر آن‌ها قفل کامپیوتر شما را باز کنند، پس از مدتی دوباره از شما باج‌گیری و کامپیوتر شما را قفل می‌کنند؛ بنابراین به دنبال یک راه قطعی و مطمئن باشید.

### ۱۵-۲-۲ حمله از نوع MitM[۳۹]

حمله MitM چنان‌که از نامش هم پیدا است زمانی رخ می‌دهد که هکر خود را به نحوی در مسیر اتصال کاربر با یک سرور قرار می‌دهد. به نظر می‌رسد این نوع حمله خطرناک‌ترین نوع حمله باشد؛ هکر سال‌ها تمام اطلاعات شما را بدزد و عملیات‌های مخرب دیگری انجام دهد و شما نفهمید، درحالی‌که برای شما همه چیز عادی به نظر برسد.

مثلاً تصور کنید شما در یک مکان عمومی به وای‌فای وصل شده‌اید. فردی که صاحب آن مودم است قبل از اینکه شما به اینترنت وصل شوید هر کاری را که می‌کنید ثبت و ضبط کند. اگر در آن موقع به ایمیلتان سر بزنید، وارد شبکه‌های اجتماعی شوید و یا از درگاه‌های پرداخت اینترنتی استفاده کنید احتمالاً همه چیزتان را از دست داده‌اید.

### ۱۶-۲-۲ حمله از نوع فیشینگ[۴۰]

فیشینگ یک روش مخرب برای دسترسی به اطلاعات بانکی افراد و سرقت اموال ایشان است. هکرها در سال‌های اخیر تلاش‌های زیادی برای به سرقت بردن موجودی حساب‌های کاربران اینترنت کرده‌اند. حملات فیشینگ را می‌توان از حملات مرتبط با حوزه مهندسی اجتماعی دانست. شخص نفوذگر با استفاده از فیشینگ شروع به سرقت اطلاعات از حجم عظیمی از کاربران می‌کند. یکی از حملات معروف فیشینگ ارسال ایمیل‌های جعلی از

---

[۳۹] Man-in-the-Middle
[۴۰] phishing

سمت بانک است. بدین نحو که یک نفوذگر ایمیل جعلی از سمت یک بانک را برای تعداد زیادی کاربر ایمیل می‌کند و در آن یک لینک قرار می‌دهد که به‌جای هدایت به صفحه اصلی بانک کاربر را به صفحه‌ای مشابه صفحه بانک هدایت می‌کند. کاربر پس از دیدن صفحه‌ای مشابه صفحه بانک و واردکردن نام کاربری و رمز عبور خود در دام هکر می‌افتد. در برخی حملات فیشینگ نام کاربری و رمز عبور هزاران کاربر بانک به سرقت می‌روند.

البته فیشینگ به سرقت اطلاعات از طریق مکالمات تلفنی یا پیام کوتاه نیز اطلاق می‌شود. به این معنا که گاهی نفوذگران با تماس تلفنی سعی در تخلیه اطلاعاتی کاربران دارند.

### ۱-۱۶-۲-۲ انواع مختلف فیشینگ

فیشینگ انواع مختلفی دارد که به روش‌های مختلف تلاش می‌کنند به اطلاعات بانکی شما از طریق روش‌های متنوع مهندسی اجتماعی (Social Engineering) که در حوزه فیشینگ مانند ایمیل، تماس تلفنی، صفحات جعلی پرداخت، پیامک، انواع مدل‌های ربات‌های تلگرام و انواع روش‌های جدیدی که انتظار آن نمی‌رود، دست یابد.

برخی از معروف‌ترین روش‌های فیشینگ عبارت‌اند از:

### ۲-۱۶-۲-۲ فیشینگ با ایمیل‌های فریبنده

در این روش از حمله‌های فیشینگ، شخص کلاهبردار با ارسال ایمیل‌های فریبنده به قربانیانش می‌کوشد با بیان دلایل مجاب‌کننده مخاطبان را به واردکردن اطلاعات بانکی خود وادار کند.

ممکن است ایمیل به‌ظاهر از طرف بانک شما، یک شرکت معتبر فین‌تک و یا حتی بانک مرکزی ارسال شود و از شما درخواست کند ظرف زمان معینی اطلاعات بانکی خود را ارسال کنید. متأسفانه بارها افرادی فریب این حملات فیشینگ را خورده‌اند.

نکته: سیستم مالی و بانکی هیچگاه از طریق ایمیل از شما درخواست نمی‌کند اطلاعات بانکی‌تان را برای آن‌ها ارسال کنید، شما حتی مجاز به اعلام رمز بانکی خود به کارکنان بانک هم نیستید.

### ۲-۱۶-۲-۳ فیشینگ تلفنی

هکرها در این روش از طریق تلفن با طعمه‌های خود ارتباط برقرار می‌کنند و ضمن اینکه خود را نماینده بانک، شرکت معتبر و یا سازمانی که شما می‌شناسید معرفی می‌کنند از شما می‌خواهند جهت دریافت جایزه خود اطلاعات بانکی خود را در اختیار ایشان قرار دهید. یا در روشی دیگر، با ارسال پیامک به شماره همراه شما، اعلام می‌کنند که حساب بانکی شما دچار مشکل شده است و شما را به زنگ زدن به شماره تماسی جعلی (سرویس

تلفن اینترنتی) سوق می‌دهند و در ادامه از شما شماره‌حساب و رمز کارت و یا حتی رمز دوم را می‌خواهند.

نکته: برای واریز هرگونه وجه به‌حساب شما اعم از جایزه، پاداش و مزایا نیازی به اعلام رمز بانکی شما نخواهد بود. برای مقابله با هکرها و حملات فیشینگ این نکته را فراموش نکنید.

**۴-۱۶-۲-۲ طراحی صفحه‌ای مشابه درگاه پرداخت بانک**

شخص هکر در این روش صفحه‌ای مشابه درگاه پرداخت آنلاین بانک‌ها طراحی می‌کند و با قراردادن این صفحه جعلی در فروشگاه‌های صوری و با ارائه پیشنهادهای وسوسه‌کننده خرید سعی می‌کند شما را وادار کند وارد صفحه پرداخت جعلی که طراحی کرده بشوید و وجه انتقال دهید.

به‌محض ورود به این صفحه جعلی و ارائه اطلاعات بانکی اطلاعات شما به‌صورت خودکار برای هکر ارسال می‌شود و او قادر خواهد بود حساب شما را خالی کند.

امن‌ترین درگاه پرداخت، درگاه پرداخت بانک مرکزی به آدرس https://xxx.shaparak.ir است و در کنار آن حتماً باید نام یکی از psp[۴۱]ها (شرکت‌های پرداخت الکترونیک) مطرح درج شده باشد.

[۴۱] شرکت هایي که ابزارها و راهکارهاي پرداخت الکترونیک ارائه مي دهند

### ۵-۱۶-۲-۲ راه مقابله با فیشنگ

راه مقابله با چنین حملاتی داشتن **تفکر انتقادی** است. اگر ایمیل شما پر شده از ایمیل‌هایی که خوانده نشده راه‌حل کلیک‌کردن روی آنها نیست. عنوان آنها را چک کنید، موس را روی آنها نگه دارید و ببینید چه اتفاقی می‌افتد. در مورد ایمیل‌هایی که در صندوق اسپم قرار دارند بیشترین وسواس را برای بازکردن ایمیل به خرج دهید و تا مطمئن نشده‌اید که ایمیل از طرف یک فرد واقعی ارسال شده آن را باز نکنید. خلاصه که همهٔ جوانب قضیه را بسنجید تا مطمئن شوید که همه چیز درست است.

چگونه در خریدهای اینترنتی قربانی صفحات فیشینگ نشویم؟

چنانچه خریدهای اینترنتی طبق اصول خود انجام نشود ممکن است خطراتی از قبیل درگاه‌های فیشینگ، اجناس تقلبی، کلاهبرداری و عدم ارسال کالا را در پی داشته باشد.

چندین نکته مهم در انجام خریدهای اینترنتی وجود دارد که توجه به آنها می‌تواند امنیت خریدهای آنلاین را تضمین نموده و شما را از کلاهبرداری‌های فیشینگ در امان نگه دارد شامل موارد زیر هستند:

۱-خریدهای خود را از سایت‌های معتبر و دارای نماد اعتماد الکترونیکی انجام دهید.

۲-قبل از خرید قوانین فروشگاه و شرایط مرجوعی کالا را بررسی نمایید تا در صورت وقوع هرگونه مشکل بتوانید از خدمات پس از فروش استفاده نمایید.

۳-حتی‌الامکان پرداخت را درب منزل و هنگام تحویل گرفتن کالا انجام دهید.

۴-در صورت پرداخت آنلاین، درگاه پرداخت بانکی را بررسی نمایید.

۵-تا جایی که امکان دارد از دستگاه رایانه‌ای شخصی خود برای خرید استفاده کنید.

### ۱۷-۲-۲ حمله درایو- بای

حمله درایو – بای[۴۲] نیز یکی از انواع حملات سایبری است که بسیار در سطح وب شایع است؛ یک روش معمول برای پخش نرم‌افزارهای مخرب. هکرها وب‌سایت‌های ناامن را پیدا می‌کنند و یک اسکریپت (کد) مخرب را به کدهای یکی از صفحات اضافه می‌کنند. این اسکریپت ممکن است بدافزارها را مستقیماً روی رایانهٔ کسی که از سایت بازدید می‌کند نصب کند یا ممکن است قربانی را به یک سایت تحت کنترل هکر هدایت کند.

حتماً بارها شده که در هنگام بازدید از یک وب‌سایت به صفحه‌ای دیگر هدایت شوید یا یک پنجرهٔ پاپ‌آپ برای شما باز شود که اصلاً به چیزی که دنبال می‌کنید ارتباط ندارد. ممکن است با کلیک روی آن یا بدون کلیک شما یک چیزی دانلود شود. بر خلاف حمله فیشینگ، این نوع حمله به فعالیت کاربر و کلیک او یا بازکردن ضمیمه ایمیل وابسته نیست.

---

[۴۲] Drive-by

### ۱-۱۷-۲-۲ چطور در مقابل حمله درایو - بای از خود مراقبت کنیم؟

برای محافظت از خود در برابر این حملات، باید مرورگرها، سیستم‌عامل و آنتی‌ویروس‌های خود را به‌روز نگه دارید و از ورود به وب‌سایت‌هایی که ممکن است حاوی کد مخرب باشند را اجتناب کنید. حتی سایت‌هایی که به طور معمول از آنها استفاده می‌کنید اگر امن نباشند می‌توانند هک شوند.

### ۱۸-۲-۲ حمله کلمه عبور[۴۳]

ازآنجاکه مکانیزم کلمه عبور رایج‌ترین روش برای تأیید هویت کاربران برای ورود به یک سیستم است، به‌دست‌آوردن کلمه عبور یک رویکرد شایع و البته کارآمد است. رمز عبور شخصی را می‌توان با نگاه‌کردن به میز کار شخصی افراد، روش‌های هک MitN ، استفاده از مهندسی اجتماعی، دسترسی به پایگاه‌داده یک سایت یا حدس زدن به دست آورد .

### ۱۹-۲-۲ حمله برات‌فورس۴۴

هدف فریب‌دادن کاربران و یا نفوذ به سیستم‌های دفاعی است. هکر ممکن است خودش یا به وسیلهٔ یک ربات سعی کند با به‌کاربردن یک سری رشته‌کلمات وارد حساب کاربری شما شود. مثلاً در نظر بگیرید که صفحه ورود به سایتتان را بازکرده و دائماً باتوجه‌به نام، عنوان شغلی، کد ملی، شماره‌تلفن، و موارد مشابه، نام کاربری و رمز عبور وارد می‌کند و امیدوار

---

[۴۳] Password
[۴۴] Brute-force

است پس از مدتی بالاخره وارد سایت شود. اگر در انتخاب رمزهایتان نکات امنیتی را رعایت نکرده باشید احتمالاً این کار چند روز یا حتی چند ساعت بیشتر برای هکر زمان نبرد.

### ۲۰-۲-۲ حمله لغت‌نامه [۴۵]

در یک حمله دیکشنری، هکر یک لیست از کلمات کلیدی معمول که اکثر آدم‌ها از آن استفاده می‌کنند دارد و از آنها برای ورود به‌حساب استفاده می‌کند. مثلاً اگر شما رمز صفحه تنظیمات مودم خود را عوض نکرده‌اید احتمالاً هکر با نام کاربری و پسورد admin می‌تواند وارد صفحه تنظیمات شود و وای‌فای خانه شما را هک کند.

اگر یک کاربر عادی شبکه‌های اجتماعی هستید یادتان باشد که رمز حساب‌های خود را ترکیبی از حروف کوچک و بزرگ، عدد و کاراکتر انتخاب کنید بدون اینکه نیاز باشد برای شما معنایی داشته باشند. سعی کنید آنها را به‌خاطر بسپارید و آن را جایی در دسترس یک هکر بالقوه قرار ندهید. همچنین بسیاری از اپلیکیشن‌ها رمزهای دومرحله‌ای را به شما پیشنهاد می‌دهند که استفاده از آنها امنیت شما را بالاتر می‌برد. اگر مدیر سایت هستید آدرس صفحه ورود به سایتتان را تغییر دهید و با پلاگین‌های موجود از حملات بروت‌فورس جلوگیری کنید.

---

[۴۵] dictionary attack

### ۲۱-۲-۲ حمله ایکس اس اس [۴۶]

این‌گونه از انواع حملات سایبری کاربران سایت را هدف می‌گیرد. هکر مانند حمله قبلی یک کد را از طریق فرم‌های سایت وارد سایت می‌کند. به طور خاص، مهاجم یک کد جاوا اسکریپت (JavaScript) را به پایگاه‌داده سایت تزریق می‌کند. هنگامی که کاربری یک صفحه را از وب‌سایت را باز می‌کند، کد مخرب در مرورگر قربانی اجرا می‌شود. به‌عنوان‌مثال، ممکن است کوکی‌هایی که قربانی به سرور ارسال می‌کند، توسط مهاجم رصد شود و یا حمله MitNپایه‌ریزی شود. این نوع از حملات مهاجم را قادر می‌سازد که نه‌تنها کوکی‌ها را سرقت کند بلکه کلاهبرداری‌هایی داشته باشد از طریق فیلم گرفتن از صفحه کاربران، کشف و جمع‌آوری اطلاعات و دسترسی و کنترل از راه دور موبایل یا کامپیوتر قربانی.

برای دفاع در برابر حملات XSS ، توسعه‌دهندگان وب (developers) باید داده‌های ورودی سایت را که توسط کاربران در فیلدهای فرم‌های سایت وارد می‌شوند قبل از ارسال به سرور امن کنند. برای مثال کدهایی که دارای کاراکترهایی از قبیل ( < ,> ,/ ,& ,?) هستند را فیلتر کنند.

---

[۴۶] XSS (Cross-site scripting)

## ۲-۲-۲۲ حمله استراق سمع

حملات استراق سمع[۴۷] یا شنود از طریق چک کردن ترافیک شبکه رخ می‌دهد. با استفاده از این نوع از انواع حملات سایبری، هکر می‌تواند رمزهای عبور، شماره کارت اعتباری و سایر اطلاعات محرمانه را که کاربر ممکن است از طریق شبکه ارسال می‌شود، به دست آورد.

رمزگذاری اطلاعات، راه‌حل جلوگیری از این نوع حملات است. یعنی ارتباط میان کاربران و سایت مخصوصاً زمانی که اطلاعاتی را به سایت منتقل می‌کنند توسط مکانیزمی رمزگذاری (encrypt) شود تا هکر معنای این داده‌های انتقالی را درک نکند.

گواهینامه SSL که امنیت سایت‌ها را افزایش می‌دهد برای تغییر آدرس سایت HTTP به HTTPSدر اینجا توصیه می‌شود.

## ۲-۲-۲۳ آسیب‌پذیری یا حمله روز صفر[۴۸]

آسیب‌پذیری روز صفر، نوعی از آسیب‌پذیری است که تا مدت‌ها تنها تعداد کمی هکر از آن اطلاع دارند. این نوع آسیب‌پذیری‌ها تا زمانی که توسط متخصصین شناسایی و بر طرف نشوند روز صفر می‌مانند.

---

٤٧ Eavesdropping
٤٨ Zero Day

از جمله آسیب‌پذیری‌های Zero Day که در کشور ما اتفاق افتاده است می‌توان به ویروس Sutxnet که به نیروگاه‌های هسته‌ای آسیب وارد کرد و همچنین ویروس Flame که به پالایشگاه‌های نفت ایران نفوذ کرد اشاره کرد.

به دلیل سطح بالا بودن این نوع آسیب‌پذیری‌ها تقریباً هیچ نرم‌افزار و آنتی ویروسی نمی‌تواند آن‌ها را شناسایی کند و حتی سازندگان نرم‌افزار به‌سادگی قادر به حل کردن این دست آسیب‌پذیری‌ها نیستند.

البته پکیج‌های گران‌قیمت تست نفوذی وجود دارند که مجموعه‌ای از Zero Day های نرم‌افزارها را در خود دارند و توسط متخصصین امنیت مورداستفاده قرار می‌گیرند. یکی از این فریم‌ورک‌های تست نفوذ، canavas نام دارد.

### ۲-۲-۲۴ جعل IP[۴۹]

در این حمله هکر با جعل هویت یک کاربر دیگر سرور را متقاعد می‌کند که کاربر قابل‌اطمینان شبکه است. او با جعل IP یک کاربر از این به بعد با سرور ارتباط خواهد داشت و در ادامه به‌عنوان واسطه میان سرور و کامپیوتر قربانی قرار می‌گیرد.

[۴۹] IP Spoofing

## ۲-۳ مقابله با تهدیدات امنیت سایبری

راه‌حل‌های بسیاری برای مقابله با تهدیدات امنیت سایبری وجود دارد که در ادامه به چند نمونه از این راه‌حل‌ها اشاره می‌کنیم.

### ۲-۳-۱ ضد بدافزار

ضد بدافزار[۵۰] یا همان آنتی‌ویروس مجموعه‌ای از نرم‌افزارها هستند که به‌منظور مسدودکردن، ریشه‌کن کردن و ازبین‌بردن ویروس‌ها، کرم‌ها و سایر موارد ناگوار که در این لیست توضیح داده شده، طراحی شده‌اند. این محصولات، برای اطمینان از اینکه در برابر تهدیدات جدید همچنان مؤثر هستند، باید مرتباً به‌روز شوند. آنها می‌توانند در نقاط مختلف رایانه‌های شخصی زنجیره شبکه (ایمیل، نقطه انتهایی، مرکز داده، ابر) و یا درون سازمان مستقر شده، یا از طریق ابر تحویل داده شوند

### ۲-۳-۲ امنیت در فضای ابری

امنیت ابر[۵۱]، زیر مجموعه‌ای از امنیت اطلاعات و امنیت شبکه است. امنیت ابر یک اصطلاح گسترده است که می‌تواند شامل سیاست‌های امنیتی، فناوری‌ها، برنامه‌ها و کنترل‌هایی

---

۵۰ Anti-malware

۵۱ Cloud security

باشد که برای محافظت از داده‌های حساس کاربر که در یک فضای ابر عمومی، خصوصی یا ترکیبی نمایش داده می‌شوند، استفاده می‌گردد.

نقض امنیت به‌ندرت در اثر ضعف محافظت از داده‌های ابر ایجاد می‌شود. بیش از ۴۰٪ نقض امنیت داده‌ها به دلیل خطای کاربران رخ می‌دهد.(موسوی، ۱۳۹۶) بهبود امنیت کاربر برای ایمن سازی بیشتر فضای ذخیره سازی ابر، یکی از توصیه های مهم است. عوامل زیادی در امنیت کاربر در سیستم ذخیره سازی ابر نقش دارند. بسیاری از این موارد بر آموزش کاربران تمرکز دارند.

رمزهای عبور ضعیف، رایج‌ترین آسیب‌پذیری امنیتی کاربران در فضای ابری است. بسیاری از کاربران کلمات عبور خود را بر روی کاغذ می‌نویسند. این باعث بروز مشکل در سیستم امنیتی خواهد شد. احراز هویت چندعاملی می‌تواند این مشکل را برطرف کند.

### ۳-۳-۲ امنیت پست الکترونیک

امنیت پست الکترونیک[۵۲]، به فناوری‌ها، خط‌مشی‌ها و شیوه‌های استفاده شده برای تأمین امنیت دسترسی و محتوای پیام‌های ایمیل اشاره دارد. بسیاری از حملات، خواه حملات هدفمند (مانند فیشینگ) یا پیوست‌ها یا پیوندهای مخرب، از طریق پیام‌های ایمیل انجام

[۵۲] Email security

می‌شوند. یکی از موارد حفظ  بالابردن امنیت ایمیل، شناسایی ایمیل فیشینگ است که بازکردن و پاسخ‌دادن به این‌گونه ایمیل‌ها تبعات جبران‌ناپذیری خواهد داشت.

مشکلات مربوط به امنیت پست الکترونیک دو منشأ دارند: اول کاربرانی که توجه کافی به امنیت رمز عبورشان ندارند (استفاده از کلمات عبور ضعیف، استفاده از یک کلمه عبور در چند پلتفرم) و دوم شرکت‌هایی که نسبت به اطلاعات محرمانه کاربرانشان بی‌تفاوت هستند (ذخیره کردن کلمات عبور کاربران به‌صورت متن ساده و غیره). وقتی این اشتباهات هم‌زمان با هم تکرار شوند، آسیب‌هایی جبران‌ناپذیر به کاربران و سازمان‌ها وارد می‌شود.

در ادامه به برخی نکات ساده اما مهم امنیتی  راجع به ایمن‌سازی پست الکترونیک اشاره می‌کنیم:

### ۱-۳-۳-۲ حساب‌های ایمیل جداگانه

اگر شما همانند بیشتر مردم هستید، حساب ایمیلتان احتمالاً قطب مرکزی فعالیت‌های شخصی شماست. همه اطلاعیه‌های فیسبوک، ثبت‌نام‌های وبگاه، خبرنامه‌ها، پیام‌های شما، و غیره به ایمیلتان فرستاده می‌شوند. داشتن حساب‌های ایمیل جداگانه نه‌تنها به افزایش امنیت شما کمک خواهد کرد، بلکه همچنین به ارتقا بهره‌وری شما می‌انجامد.

### ۲-۳-۳-۲ مراقبت از اطلاعات حساس

زمانی که می‌خواهید اطلاعاتی شخصی، از قبیل آدرس و یا شماره‌تلفن را ارسال کنید، مطمئن شوید که آدرسی که به آن می‌خواهید این نامه را ارسال کنید، برای همان شخصی باشد که واقعاً قصد فرستادن ایمیل برایش را دارید. اطلاعات حساس، همچون گذرواژه‌ها، شماره‌حساب‌های بانکی و اعداد امنیتی شما، نباید از طریق ایمیل ارسال شوند و یا حداقل باید آنها را در فایلی نوشت، روی آنها رمز گذاشت و فایل را ارسال کرد و سپس، از طریقی دیگر، رمز آن فایل را نیز به‌طرف مقابل داد.

### ۳-۳-۳-۲ فیشینگ از طریق ایمیل

اکثر کلاهبرداری‌های فیشینگ از طریق ایمیل‌ها و پیام‌ها صورت می‌پذیرد و قربانیان به‌صورت مستقیم اطلاعات حساس و محرمانه خود را در وب‌سایت‌های جعلی که در ظاهر کاملاً شبیه وب‌سایت‌های سالم و قانونی است وارد می‌نمایند. حقهٔ فیشینگ یکی از تکنیک‌های مهندسی اجتماعی برای فریب کاربران است که از ضعف امنیتی یک وب سایت برای انجام عملیات مجرمانه خود استفاده می‌کنند.. همیشه شرکت ایمیل دهنده را در اینترنت جستجو کرده و از صحت ایمیل اطلاع پیدا کنید.

۲-۳-۳-۴ فایل‌های ضمیمه

همیشه قبل از بازکردن ضمیمه‌ها، آنها را نرم‌افزار ویروس‌کش، اسکن کنید. فایل‌های ضمیمه ایمیل‌های اسپم و یا از طرق سایت‌های نامعتبر را باز نکنید. ضمیمه‌هایی که پسوند .exe داشته باشند، مشکوک به وجود ویروس در آنها هستند

## ۲-۳-۳-۵ پیام‌های ناخواسته

این ایمیل‌ها که اسپم نامیده می‌شوند، یکی از انواع مخرب‌ها و بدافزارها هستند. با نصب یک نرم‌افزار کنترل اسپم بر روی سیستم خود و یا با ساختن ایمیل در سایتی معتبر که قابلیت فیلتر اسپم به طور اتوماتیک را داشته باشید، از ایمیل خود در مقابل این ایمیل‌ها محافظت کنید. در موقع انتخاب سرویس‌دهندهٔ ایمیل، سرویس‌دهنده‌ای را انتخاب کنید که به شما کمک می‌کند از دریافت ایمیل‌های ناخواسته (اسپم) جلوگیری کنید و هرگز به ایمیل‌های ناخواسته (اسپم) پاسخ ندهید.

۲-۳-۳-۶ استفاده از گذرواژه‌های مناسب

گذرواژه تنها در صورتی دسترسی غریبه‌ها به منابع موجود را محدود می‌کند که حدس زدن آن به‌سادگی امکان‌پذیر نباشد. گذرواژه‌های خود را در اختیار دیگران قرار ندهید و از یک گذرواژه در بیشتر از یک جا استفاده نکنید. در این صورت اگر یکی از گذرواژه‌های شما لو برود، همه منابع در اختیار شما در معرض خطر قرار نخواهند گرفت.

### ۷-۳-۳-۲ پرهیز از وای - فای عمومی

و در نهایت، هنگامی که در اینترنت عمومی هستید از بررسی ایمیل خود پرهیز کنید. بله، می‌دانم هنگامی که منتظر هواپیما برای رسیدن به ورودی (گیت) پرواز خود هستید، این می‌تواند برای بیرون کشیدن گوشی هوشمند یا رایانه شما برای بررسی پیام‌های جدید، وسوسه‌انگیز باشد. متأسفانه، وای - فای عمومی می‌تواند بسیار ناامن باشد.

### ۴-۳-۲ دیواره آتش

برای درک بهتر دیواره آتش[۵۳]، تصور کنید موارد بد و مخربی در اینترنت هستند که برای متوقف کردن آن‌ها چیزی وجود ندارد. یک فایروال، دیواری است که بین محیط مورد اعتماد شما و محیط بیرونی آن قرار دارد و دسترسی را بر اساس قوانین امنیتی، کنترل می‌کند. فایروال می‌تواند سخت‌افزاری، نرم‌افزاری، یک دستگاه امنیتی مستقل یا یک راه‌حل ارائه شده از ابر باشد.

معمولاً افراد پس از نصب ویندوز به‌اشتباه تنظیمات دیواره آتش را غیرفعال و یا در حالت کمترین حساسیت قرار می‌دهند و به‌راحتی زمینه افزایش آسیب‌پذیری رایانه خود را فراهم می‌کنند.

---

[۵۳] Firewall

## ۴-۲ خلاصه راه کارهای مقابله با تهدیدات

۱- آنتی‌ویروس‌هایی بر روی سیستم نصب کرد که هنگام اجرا و یا دانلود فایل‌های آسیب‌دیده، آنها را شناسایی کنند. البته برای شناسایی ویروس‌های جدید، آپدیت کردن آنتی‌ویروس را نباید فراموش کرد.

۲- ارتقا به‌موقع پچ‌های امنیتی در سیستم‌عامل میزبان شما.

۳- از اطلاعات خود مرتباً پشتیبان تهیه نمایید.

۴- دانلودهای ناخواسته را به حداقل برسانید.

۵- نرم‌افزارهای امنیتی خود را مکرراً آپدیت کنید.

۶- نرم‌افزارهای موردنیاز خود را از سایت‌های مطمئن دانلود و نصب کنید.

۷- فایروال مجزا بر روی سیستم خود نصب کنید و به‌درستی تنظیم کنید.

۸- بر روی فایل‌های پیوست شده در ایمیل‌ها که از طرف اشخاص ناشناس ارسال شده کلیک نکنید.

۹- در Wi-Fi ناامن عمومی، مهاجمان می‌توانند خود را بین دستگاه بازدیدکننده و شبکه قرار دهند و بدون اطلاع، بازدیدکننده تمام اطلاعات را از طریق مهاجم منتقل می‌کند.

## ۵-۲ جمع‌بندی

مقابله با حملات سایبری و بدافزارها نیازمند این است که شما ابتدا آنها را خوب بشناسید که در این فصل با تعدادی از **پرکاربردترین انواع حملات سایبری و بدافزارها** که هکرها به کار می‌گیرند آشنا شدید.

مقابله با این تهدیدات علاوه بر اینکه نیازمند تخصص امنیت است، نیازمند رعایت برخی اصول ساده هم است.

مواردی همچون داشتن تفکر انتقادی و بروز رسانی آنتی‌ویروس و توجه به فایروال سیستم شخصی، نکات مهمی است که هر فردی می‌تواند انجام دهد، تا از آسیب‌های احتمالی در امان باشد.

در این فصل ضمن معرفی بدافزارها به تناسب به راه‌های مقابله با آن‌ها نیز پرداخته‌ایم تا راهنمای شما خواننده گرامی برای اقدامات عملی مقابله با حملات نیز باشد.

# فصل سوم: امنیت در تلفن همراه هوشمند

**سؤالات مهم فصل سوم:**

- ✓ **ضرورت امنیت در تلفن همراه هوشمند چیست؟**
- ✓ **انواع تهدیدات امنیتی تلفن همراه هوشمند کدام است؟**
- ✓ **روش‌های مؤثر افزایش امنیت کاربران در سیستم‌عامل اندروید چیست؟**
- ✓ **نکات مهم امنیتی تلفن همراه هوشمند چیست؟**

## ۱-۳ ضرورت امنیت در تلفن‌های همراه  هوشمند

قبل از محبوب شدن تلفن‌های هوشمند، به امنیت تلفن‌های همراه چندان اهمیت داده نمی‌شد. واقعاً چه چیزی در گوشی‌های قدیمی ما ذخیره شده بود؟ تعدادی مخاطب، بازی‌های کلاسیک، و چند تصویر تار برای پس‌زمینه. بااین‌حال امروزه همه چیز تغییر کرده، تعداد زیادی از مردم برای اجرای بسیاری از امور، از گوشی‌های هوشمند استفاده می‌کنند از ورود به‌حساب بانکی تا داشبورد شرکت برای انجام کارهایی که به آنان واگذار شده، بنابراین اهمیت امنیت گوشی‌های هوشمند بیشتر از قبل شده است.

تحقیقات حاکی از آن است که فقط ۲۲ درصد از کاربران موبایل اقدامات منظم امنیتی را انجام می‌دهند، درحالی‌که بیشتر مردم تنها هنگامی که لازم باشد اقدام به این کار می‌نمایند. اما، به‌عنوان کاربران گوشی هوشمند باید اهمیت امنیت گوشی‌های هوشمند را در اولویت قرار دهیم تا در حد امکان از پیش‌آمدن عواقب ناخوشایند جلوگیری کنیم.(لطفی، حدادیان، و رهی، ۱۳۹۷)

هنگامی که موبایلتان هک می‌شود، شما در معرض مشکلات بزرگ مالی و همچنین ازدست‌رفتن یا سو استفاده از اطلاعات شخصی قرار می‌گیرید. ما همه چیز را در تلفن همراه خود ذخیره می‌کنیم تا در مواقعی که به آن احتیاج داشتیم کاملاً در دسترسمان باشد اما این کار بسیار نگران‌کننده است. این روزها هکرها برای ورود به گوشی تلفن ما بسیار زیرک، قدرتمند، و سریع عمل می‌کنند.

## ۲-۳ ماهیت تهدیدات امنیتی تلفن همراه

تهدیدات امنیتی تلفن همراه حملاتی هستند که هدف آن‌ها به خطر انداختن یا سرقت اطلاعات دستگاه‌های تلفن همراه مانند تلفن‌های هوشمند و تبلت‌ها است. این تهدیدها اغلب به شکل بدافزار یا نرم‌افزار جاسوسی هستند که به افراد متخاصم اجازه دسترسی غیرمجاز به دستگاه‌ها را می‌دهند. در بسیاری از موارد، کاربران حتی از وقوع این حملات آگاهی ندارند.

با این دسترسی، مهاجمان می‌توانند اقدامات مخرب مختلفی را از سرقت و فروش داده‌ها گرفته تا دسترسی به مخاطبین و ارسال پیام و برقراری تماس انجام دهند. همچنین می‌توانند از دستگاه برای سرقت اعتبارنامه‌های ورود به‌حساب‌های کاربران و جعل هویت استفاده کنند. این حملات، کاربران و سازمان‌ها را به طور یکسان تحت‌تأثیر قرار می‌دهد، چرا که تنها نقض اطلاعات یک شخص می‌تواند منجر به نشت اطلاعات در مقیاس بزرگ شود.

## ۳-۳ انواع تهدیدات امنیتی تلفن همراه

تهدیدات امنیتی موبایل در هر شکل و با هراندازه ای وجود دارد، اما به‌طورکلی در چهار دسته زیر قرار می‌گیرد:

### ۳-۳-۱ تهدیدهای موبایل مبتنی بر برنامه‌های کاربردی

برنامه‌ها اغلب ریشه آسیب‌پذیری‌های دستگاه تلفن همراه هستند. این نوع حملات زمانی که کاربران برنامه‌های مخرب را بارگیری می‌کنند یا به برنامه‌ها بدون توجه به میزان امنیت آن برنامه اجازه دسترسی به داده‌های دستگاه را می‌دهند رخ می‌دهد.

### ۳-۳-۲ تهدیدهای موبایل مبتنی بر وب

حملات تحت وب موبایل معمولاً از طریق فیشینگ یا کلاهبرداری انجام می‌شود. مهاجمان یک ایمیل، متن یا پیامی که به نظر می‌رسد از یک منبع معتبر باشد ارسال می‌کنند درحالی‌که این پیام حاوی یک لینک یا پیوست مخرب است. وقتی کاربران روی این لینک کلیک کرده و یا اطلاعات شخصی خود را ارائه می‌دهند، شخص متخاصم می‌تواند دسترسی غیرمجاز به دستگاه تلفن همراه را به دست آورده یا از طریق مدارک سرقت شده، هویت را جعل کند.

### ۳-۳-۳ تهدیدهای شبکه

این نوع حمله زمانی اتفاق می‌افتد که مهاجمان، اتصالات Wi-Fi عمومی ناامن یا رایگان را هدف قرار می‌دهند. در برخی موارد، هکرها حتی ممکن است باهدف فریب کاربران، شبکه وای فای جعلی[۵۴] را راه‌اندازی کنند. شبکه‌های جعلی از کاربران می‌خواهند با استفاده از نام کاربری و رمز عبور خود یک حساب کاربری ایجاد کنند و این فرصت را به هکرها می‌دهند تا دستگاه‌ها و اعتبارنامه‌ها را به خطر بیندازند.

### ۳-۳-۴ تهدیدهای فیزیکی

دستگاه‌های گمشده، دزدیده شده و بدون مراقبت، کاربران را در معرض مشکلات جدی امنیتی موبایل قرار می‌دهند. اگر از یک گذرواژه قوی، PIN یا احراز هویت بیومتریک استفاده نکرده و یا از برنامه‌ها و سرویس‌های رمزنگاری نشده استفاده کنید، تلفن شما به‌راحتی قابل هک شدن است. به‌خصوص با درنظرگرفتن این که امروزه چشم‌انداز تهدیدات امنیتی بسیار پیچیده‌تر شده است.

---

[۵۴] network spoofing

## ۳-۴ مهم‌ترین تهدیدات امنیتی تلفن همراه

این که مهاجمان می‌توانند از هرکدام از انواع تهدیدات گفته شده در بالا برای حمله به کاربران استفاده کنند بسیار بد است. اما چیزی که حتی از این موضوع بدتر است این است که رفتار روزمره و فعالیت‌های تلفن همراه ما می‌تواند برای آن‌ها این راه را آسان‌تر کند.

در ادامه برخی از متداول‌ترین روش‌هایی که داده‌ها و هویت خود را در معرض تهدیدات امنیتی موبایل قرار می‌دهیم، و نکاتی در مورد چگونگی محافظت از خود در برابر این تهدیدات آورده شده است.

### ۱-۴-۳ بارگیری برنامه‌های مخرب و اعطای مجوزهای بیش از حد

برنامه‌هایی که از منابع دیگری به جز از فروشگاه‌های رسمی برنامه‌ها بارگیری می‌شوند، می‌توانند منجر به نشت داده شوند، زیرا بسیار بعید است که از محافظت‌های مناسبی برخوردار باشند. به‌علاوه، مهاجمان ممکن است برنامه‌های مخربی را که هدف آنها سو استفاده از کاربرانی است که آنها را بارگیری می‌کنند (مثلاً سرقت اطلاعات از دستگاه و فروش آنها به اشخاص ثالث) منتشر کنند. نشت داده‌ها همچنین می‌تواند از طریق برنامه‌های سازمانی آلوده به بدافزار که کد مخربی را در سیستم‌عامل‌های تلفن همراه توزیع می‌کنند و بدون شناسایی شدن در شبکه سازمان گسترش می‌یابند انتقال یابد.

**چگونه ریسک را به حداقل برسانیم؟** برنامه‌ها را فقط از Google Play، App store و سایر ارائه دهندگان مطمئن بارگیری کنید. علاوه بر این ، مجوزهایی مانند دسترسی به داده‌های مکان ، دوربین و میکروفن را رد کنید ، مگر اینکه برنامه ای که از آن استفاده می‌کنید واقعاً به آن احتیاج دارد.

### ۲-۴-۳ اتصال به شبکه‌های وای فای نا امن

به‌احتمال زیاد، استفاده از شبکه‌های وای فای که دسترسی به آن‌ها در مکان‌های عمومی مانند فرودگاه‌ها، کافی‌شاپ‌ها و کتابخانه‌ها رایگان است برای شما جذاب هستند. زیرا این امکان را به شما می‌دهد تا از اینترنت تلفن همراه خود استفاده نکنید. اما بسیاری از این شبکه‌ها ناامن هستند. به‌عبارت‌دیگر مهاجمان می‌توانند از این طریق به‌راحتی به دستگاه‌های کاربران دسترسی پیدا کرده و امنیت داده‌های آنها را به خطر بیندازند.

**چگونه ریسک را به حداقل برسانیم؟** قبل از اتصال به وای‌فای رایگان، خوب فکر کنید و هرگز از شبکه‌هایی که شما را مجبور به ایجاد حساب کاربری یا گذرواژه می‌کنند استفاده نکنید. اگر نیازی به استفاده از یکی از این شبکه‌ها دارید، صرفاً فعالیت‌های کم‌خطر را انجام داده و هرگز از این شبکه‌ها برای دسترسی به‌حساب‌های شبکه‌های اجتماعی، برنامه‌های بانکی یا خرید آنلاین استفاده نکنید.

در اماکن عمومی دسترسی به اینترنت به‌هیچ‌عنوان رمز عبور خود را بر روی مرورگر ذخیره نکنید.

پس از اتمام کار حتماً از حساب‌های کاربری خود نظیر ایمیل خارج شوید.

برای واردکردن رمزهای عبور خود ترجیحاً از صفحه‌کلید مجازی استفاده کنید چراکه احتمال نصب برنامه‌های کیلاگر (برنامه خواندن و ذخیره کردن کلیدهای صفحه‌کلید) وجود دارد.

بهتر است پس از اتمام کار تاریخچه مرورگر خود را ازروی سیستم رایانه‌ای حذف کنید.

درصورتی‌که فایلی شخصی را دانلود کرده و بر روی سیستم رایانه‌ای قرار داده‌اید پس از اتمام کار حتماً این‌گونه فایل‌ها را حذف کنید.

### ۳-۴-۳ قرارگرفتن به‌عنوان هدف حملات مهندسی اجتماعی

اخیراً حملاتی مانند فیشینگ و ''smishing'' (فیشینگ با sms) به طور فزاینده‌ای در هر دو دستگاه موبایل و رایانه شایع شده‌اند. بااین‌حال، کاربران تلفن همراه بیشتر در معرض این حملات هستند زیرا اندازه صفحه‌نمایش کوچک‌تر، اطلاعاتی را که می‌تواند در هر لحظه در یک ایمیل مخرب مشاهده شود، محدود می‌کند. با این کار شانس کلیک کاربران بر روی پیوندها بدون درنظرگرفتن عواقب آن افزایش می‌یابد.

**چگونه ریسک را به حداقل برسانیم؟** هرگز روی پیوند موجود در ایمیل یا پیام متنی کلیک نکنید، حتی اگر به نظر می‌رسد از طرف فرستنده معتبری باشد. در عوض، آدرس را در نوار آدرس مرورگر وب خود وارد کنید تا بتوانید قانونی‌بودن پیوند را تأیید کنید.

### ۳-۴-۴ رعایت‌نکردن بهداشت سایبری

در حال حاضر رعایت بهداشت سایبری برای افراد، بیش از هر زمان دیگری مهم است. اما بسیاری از افراد همچنان از گذرواژه‌های ضعیف استفاده می‌کنند، گذرواژه یکسانی را در حساب‌های کاربری مختلف خود به کار می‌برند، داده‌ها را با دوستان و همکاران خود به اشتراک می‌گذارند و از به‌روزرسانی برنامه‌ها و سیستم‌عامل‌ها خودداری می‌کنند.

دستگاه‌های قدیمی همچنین می‌توانند باعث ایجاد مشکلات زیادی در زمینه امنیت سایبری تلفن همراه شوند. خواه به دلیل عدم ارائه به‌روزرسانی توسط شرکت سازنده باشد و خواه اینکه کاربر تصمیم به بارگیری نسخه‌های جدید نرم‌افزار نداشته باشد. این خلأ باعث ایجاد شکاف‌هایی می‌شود که مهاجم می‌تواند برای نفوذ به دستگاه استفاده کند.

علاوه بر این، کاربران می‌توانند به دلیل مدیریت نامناسب نشست، قربانی تهدیدات امنیتی تلفن همراه شوند. بسیاری از برنامه‌ها از توکن‌ها استفاده می‌کنند تا تجربه را برای کاربران راحت‌تر کنند (به‌عنوان‌مثال به آنها اجازه می‌دهد بدون احراز هویت مجدد اقداماتی را انجام دهند). اما این توکن‌ها در صورت‌باز ماندن نشست‌ها، گاهی می‌توانند ناخواسته با مهاجمان به اشتراک گذاشته شوند.

**چگونه ریسک را به حداقل برسانیم؟** از گذرواژه‌های قوی استفاده کنید، ابزارهای احراز هویت چندعاملی (MFA) را نصب کنید، دستگاه‌های خود را طوری تنظیم کنید که به

طور خودکار به‌روز شوند و پس از اتمام استفاده از آنها، از برنامه‌ها و وب‌سایت‌ها خارج شوید و البته، اطلاعات شخصی و ورود به سیستم را نزد خود نگه دارید.

### ۵-۴-۳ کارکردن با رمزنگاری شکسته شده یا بدون رمزگذاری دوطرفه

در حال حاضر با صرف وقت بیشتر مردم در خانه، استقبال چشمگیری در استفاده از ابزارهای کنفرانس ویدئویی در دستگاه‌های تلفن همراه ایجاد شده است. اگرچه این موارد برای کمک به همکاران و خانواده‌ها برای برقراری ارتباط بسیار مناسب هستند، اما خطرات زیادی نیز در این زمینه وجود دارد. به‌خصوص اگر از برنامه یا سرویسی استفاده می‌کنید که مکالمه را رمزگذاری نمی‌کند، با استفاده از الگوریتم‌های ضعیف کار می‌کند یا دستگاه‌ها را در معرض حمله قرار می‌دهد.

**چگونه ریسک را به حداقل برسانیم؟** اگر صاحب کسب‌وکار هستید و یا استفاده شخصی از این ابزارها دارید، اطمینان حاصل کنید که شما و تمام کسانی که با آنها ارتباط برقرار می‌کنید از برنامه‌ها و ابزارهای آنلاینی استفاده می‌کنید که حفظ امنیت هویت و داده‌ها را در اولویت قرار می‌دهند.

## ۵-۳ فراوانی بدافزارهای اندرویدی

تنوع و تعداد بسیار برنامک‌های قابل نصب برای سیستم‌عامل اندروید موجب شده است تا دستگاه‌های مجهز به آن نیز بیش از دیگر دستگاه‌ها فروش داشته باشد و بخش عظیمی از بازار تلفن‌های همراه و تبلت به این سیستم‌عامل اختصاص پیدا کند. همین موضوع نیز موجب شده تا سیستم‌عامل اندروید در صدر جدول سیستم‌های عامل هدف برای اقدامات خرابکارانه قرار بگیرد.

به گزارش آزمایشگاه‌های کسپرسکی سال ۲۰۱۴ بیش از ۹۴ درصد از تهدیدات امنیتی تلفن‌های همراه مربوط به سیستم‌عامل اندروید بوده است که از این مقدار نسخه نان زنجبیلی ( Gingerbread- Android۲,۳,۶) و بستنی حصیری ( Ice Cream Sandwich-Android۴,۰,۴) رتبه‌های اول و دوم را به خود اختصاص می‌دهند.(موسوی، ۱۳۹۶)

همچنین بیش از نیمی از بدافزارهای شناسایی شده توسط کسپرسکی، در گروه تروجان‌های پیام کوتاه قرار گرفته‌اند، بنابراین به شما توصیه می‌کنیم در صورت مشاهده ارسال پیام‌های مشکوک و ناخواسته توسط تلفن همراهتان، به‌سرعت نسبت به نصب نرم‌افزارهای امنیتی و به‌کارگیری روش‌های مقابله با بدافزارها اقدام کنید. همچنین سعی کنید سیستم‌عامل دستگاه اندرویدی خود را به‌روز نگه دارید؛ زیرا بسیاری از بدافزارها سیستم‌عامل‌های قدیمی‌تر را هدف قرار می‌دهند.

همان‌طور که گفتیم دستگاه‌های مجهز به سیستم‌عامل اندروید بیش از دستگاه‌های دیگر در معرض خطرات احتمالی قرار دارند. اما این نکته را فراموش نکنید که بدافزارها تهدیدی برای تمام سیستم‌های عامل به شمار می‌روند و سیستم‌عامل IOS و گوشی‌های ساخت شرکت اپل نیز دچار مشکلاتی همانند گوشی‌های اندروید هستند.

روش‌های مؤثر برای افزایش امنیت کاربران در سیستم‌عامل اندروید چیست؟

۱- استفاده از قفل صفحه‌نمایش یا لاک اسکرین[۵۵]
۲- فعال کردن قابلیت آگاهی از سرویس‌های مکان‌یاب[۵۶]
۳- غیر فعال‌کردن تبلیغات مبتنی بر علایق کاربر[۵۷]
۴- استفاده از فروشگاه گوگل‌پلی[۵۸]
۵- آگاهی از دسترسی‌های اپلیکیشن‌ها[۵۹]
۶- استفاده از نسخه پولی و بدون تبلیغات اپلیکیشن‌ها
۷- درنظرگرفتن تدابیر امنیتی برای سرویس‌های ذخیره‌سازی ابری
۸- استفاده از اپلیکیشن‌های حفاظتی

---

[۵۵] Lock Screen
[۵۶] Location Services
[۵۷] Opt out of interest-based ads
[۵۸] Google Play Store
[۵۹] Application Permissions

## ۶-۳ خطرات ناشی از بدافزارهای سیستم‌عامل آی او اس[۶۰]

میزان خطرات ناشی از بدافزارهای سیستم‌عامل iOS به‌مراتب بیشتر از خطرات ناشی از بدافزارها در سیستم‌عامل اندروید است؛ زیرا بدافزارها در iOS دسترسی بیشتری به اطلاعات شخصی شما دارند (در بیشتر موارد دستگاه‌های آلوده به بدافزار، دسترسی به فایل‌های سیستمی در آنها فعال بوده است).

اولین بدافزار سیستم‌عامل iOS در اواسط سال ۲۰۱۲ منتشر شد که نتیجه آن آلودگی تعداد زیادی از دستگاه‌های مجهز به این سیستم‌عامل و سرقت اطلاعات تماس کاربران و ارسال آنها به سرورهای دیگر بود. در نهایت نیز این اطلاعات برای ارسال پیام‌های کوتاه تبلیغاتی مورداستفاده قرار گرفت. در همان موقع یک هکر نوجوان هندی توانست نمونه‌ای از بدافزار قابل‌اجرا در ویندوز فون ۸ را ارائه کند. البته انتشار نیافتن این بدافزار آسیبی به کاربران این سیستم‌عامل وارد نکرد، اما این اقدام، احتمال آلوده شدن دستگاه‌های مجهز به این سیستم‌عامل توسط بدافزارهای دیگر در آینده را از بین نمی‌برد.

---

۶۰ iOS

## ۳-۷ دسترسی‌های نرم‌افزارها در تلفن همراه

دسترسی‌ها همان مجوزهایی هستند که سیستم به هر برنامه می‌دهد. گاهی اوقات برنامه نیازمند دسترسی به بخش‌های خاصی مانند عکس یا مخاطبین است و به‌خاطر حفظ حریم شخصی، تنها در صورتی مجوز استفاده از این قسمت‌ها صادر می‌شود که شما اجازه دهید

هریک از برنامه‌هایی که بر روی تلفن یا تبلت خود نصب می‌کنیم مجموعه‌ای از دسترسی‌ها را دارند، اما گاهی اوقات دسترسی‌های بعضی برنامه‌ها از آنچه باید باشد فراتر رفته و غیرقابل‌قبول می‌شود. برای مثال یک برنامه ویرایش عکس هیچ دلیلی ندارد که به پیامک‌های موبایل شما دسترسی داشته باشد، یا یک برنامه تقویم برای چه به دوربین موبایل دسترسی داشته باشد؟! در ادامه با موبایل کمک همراه باشید..

برنامه‌ها برای فعالیت به این مجوزها نیاز دارند و بدون آن‌ها برنامه نمی‌تواند کارش را به‌درستی انجام دهد. مثلاً در برنامه نقشه گوگل اگر برنامه به Location موبایل دسترسی نداشته باشد، دیگر نقطه‌ای که هستید را مکان‌یابی نکرده و تنها شبیه به یک نقشه معمولی می‌شود.

یا به‌عنوان نمونه اپلیکیشن اینستاگرام را در نظر بگیرید. برای گرفتن عکس از طریق خود اپلیکیشن، برنامه نیازمند داشتن دسترسی به قسمت Camera است و بدون این مجوز نمی‌توانید هیچ‌گونه تصویر جدیدی با اینستاگرام به ثبت برسانید.

### ۱-۷-۳ بررسی دسترسی‌ها

دسترسی‌ها تا زمانی که به‌صورت دستی غیرفعال نشود، همچنان باقی می‌ماند. تمام برنامه‌ها این‌گونه بوده و این خود شما هستید که اجازه دسترسی به بخش‌های مختلف را به برنامه‌های نصب شده بر روی تلفن همراه می‌دهید. البته چندین راه برای اینکه ببینید برنامه چه دسترسی‌هایی دارد نیز هست:

#### ۱-۱-۷-۳ مشاهده دسترسی‌ها پیش از نصب برنامه

درصورتی‌که همچنان برنامه را نصب نکرده‌اید یکی از روش‌ها برای دیدن مجوزها، رفتن به صفحه گوگل‌پلی اپلیکیشن است. اگر از کامپیوتر استفاده می‌کنید در قسمت Permissions [پایین صفحه] روی گزینه View Details کلیک کنید. با این کار اطلاعات مربوط به دسترسی‌های برنامه و علت اینکه چرا اپ به آن‌ها نیاز دارد را خواهید دید.

در صورتی هم که از طریق اپلیکیشن پلی‌استور به صفحه برنامه می‌روید، باز در پایین و بخش Developer باید گزینه Permission Details را انتخاب نمایید. این‌گونه اطلاعاتی که می‌خواهید به نمایش درمی‌آیند. البته بعد از دانلود برنامه و هنگام نصب آن نیز [همانند ورژن‌های قدیمی] دوباره لیستی از تمام دسترسی‌ها به کاربر نشان داده می‌شود.

#### ۲-۱-۷-۳ مشاهده دسترسی‌ها برنامه‌های نصب شده

اگر یک اپلیکیشن نصب شده دارید و قبلاً به اینکه چه مجوزهایی می‌خواهد دقت نکرده‌اید، باید به قسمت تنظیمات یا همان Setting موبایل بروید و سپس روی Apps [در بعضی

موبایل‌ها Installed Apps] کلیک کنید. در این صورت لیستی از برنامه‌های نصب شده به نمایش درمی‌آید.

حالا برای دریافت اطلاعات بیشتر از برنامه‌ها، آیکون هر اپلیکیشنی که می‌خواهید را لمس نمایید. در صفحه جدید، دسته‌بندی با نام Permissions وجود دارد و با کلیک روی آن لیستی از مجوزهای برنامه نشان داده می‌شود. در اینجا می‌توانید هرکدام از دسترسی‌ها را که خواستید غیرفعال کنید.

البته راهی هم وجود دارد که یکجا تمام دسترسی‌های برنامه‌ها را ببینید. برای این منظور، در قسمت تنظیمات دوباره به بخش Apps بروید. حالا جای اینکه تک‌تک برنامه را انتخاب کنید، روی آیکون چرخ‌دنده کلیک کنید. با این کار بخش‌هایی که برنامه‌ها نیازمند دسترسی آن‌ها هستند [مثلاً لوکیشن یا مخاطبین] به نمایش درمی‌آیند.

با کلیک روی هرکدام از این بخش‌ها، اپلیکیشن‌هایی که مجوز دسترسی به آن‌ها را داده‌اید خواهید دید. فقط فراموش نکنید که تنها روی اندروید ۶,۰ و بالاتر می‌توانید دسترسی‌های برنامه‌ها را قطع کنید. گوگل قبلاً در بخشی با نام App ops همین ویژگی را به روشی متفاوت به سیستم‌عامل‌های قدیمی اندروید آورده بود ولی بعدها تصمیم گرفت آن را حذف کند.

### ۳-۱-۷-۳ تشخیص دسترسی‌های مشکوک

خیلی ساده است؛ تنها باید به کارایی‌های برنامه نگاه کنید. مثلاً اینکه گوگل مپ مجوز استفاده از موقعیت جغرافیایی کاربر را می‌خواهد اتفاق عجیبی نیست. چون سازوکار برنامه به‌گونه‌ای است که بدون این مجوز نمی‌تواند بعضی کارهایش را انجام دهد.

ولی اگر یک اپلیکیشن کتاب‌خوان همین مجوز را بخواهد باید شک کنید. در واقع مجوزها رابطه مستقیمی با کارایی برنامه داشته و درصورتی‌که اپ نیازمند دسترسی‌های اضافی باشد دو فرضیه به وجود می‌آید: یا با یک بدافزار مواجه هستید و باید پاکش کنید و یا سازنده بدون توجه به نیازهای برنامه، دسترسی‌ها را انتخاب کرده است.

جالب اینجاست این مسئله تنها محدود به اپلیکیشن‌های کوچک نبوده و برای برنامه‌های بزرگ نیز شاهد این دسترسی‌های عجیب هستیم. چند سال پیش به‌خاطر همین مسئله بعضی کاربران اپلیکیشن معروف Facebook Messenger را تحریم کردند.

### ۴-۱-۷-۳ نحوه تغییر دسترسی‌های یک برنامه

اگر قطع دسترسی‌ها برایتان کافی نیست، می‌توانید آن‌ها را تغییر دهید. اپلیکیشن Advanced Permission Manager آمده تا همین مسئولیت را بر عهده بگیرد. با این اپ، کاربرانی که نگران دسترسی‌های بی‌مورد هستند می‌توانند مجوزهای هر برنامه را پیدا کرده، لیست کارهایی که انجام می‌دهند را دیده و در صورت نیاز دسترسی را قطع نمایند.

البته باتوجه‌به اینکه گوگل بعد از اندروید ۶ کنترل بیشتری روی دسترسی‌ها به مخاطب داده، بنابراین استفاده از Advanced Permission Manager تنها به کسانی پیشنهاد می‌شود که سیستم‌عامل‌های قدیمی‌تر دارند. استفاده از این اپ نیازمند موبایل روت شده نبوده و فراموش نکنید که قطع بعضی دسترسی‌ها برنامه را از کار می‌اندازد.

### ۸-۳ نکات مهم امنیتی تلفن همراه هوشمند

کارهای مهم و ساده‌ای که هر فرد می‌تواند جهت افزایش امنیت تلفن همراه خود انجام دهد

- ✓ Wi-fi و بلوتوث را زمانی که از آن‌ها استفاده نمی‌کنید، خاموش کنید.

اگر wi-fi و بلوتوث شما روشن باشد، مهاجمان و هکرها می‌توانند به اطلاعات شما بر روی گوشی دسترسی پیدا کنند.

- ✓ برای حفاظت از داده‌ها و اطلاعات از پسورد و رمزگذاری استفاده کنید.

برای جلوگیری از دسترسی‌های غیرمجاز به اطلاعات ذخیره شده بر روی گوشی موبایلتان از پسورد و رمزگذاری داده استفاده نمایید و آن را فعال کنید.

- ✓ تهیه فایل پشتیبان (Backup) از اطلاعات را به طور منظم انجام دهید.

در این صورت اگر به هر دلیلی و رخدادی اطلاعات گوشی شما از دست برود شما این امکان را خواهید داشت که آن‌ها را بازیابی کنید.

کارهایی که نباید انجام دهید؟

- ✓ به شبکه اینترنت بی‌سیم ناشناس متصل نشوید.

ممکن است هکرها یک شبکه اینترنت wi-fi بدون نیاز به رمز برای اتصال در اماکن عمومی ایجاد کنند که بعد از اتصال افراد به این اینترنت، هکرها می‌توانند اطلاعاتی را که توسط افراد از طریق اینترنت منتقل می‌شود، سرقت و ردیابی کنند.

- ✓ سیستم‌عامل گوشی خود را دست‌کاری نکنید.

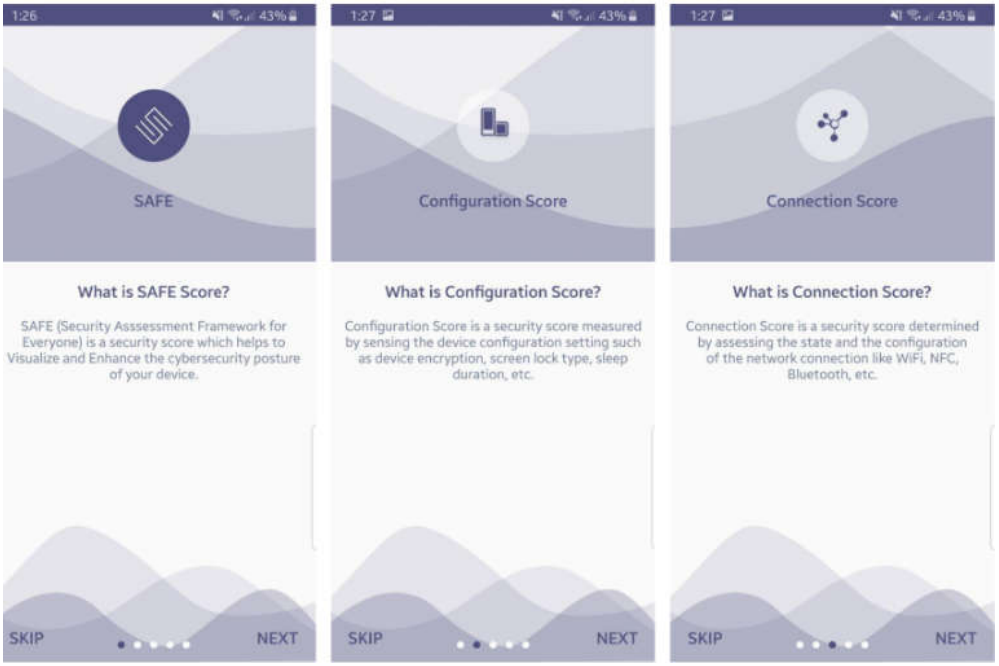
اعمالی مانند Jailbreak و یا rooting بر روی سیستم‌عامل گوشی خود انجام ندهید. زیرا باعث ازبین‌رفتن گارانتی گوشی شما می‌شود. همچنین سبب آسیب‌پذیری سیستم‌عامل می‌شود که هکرها می‌توانند آن را مورد سوءاستفاده قرار دهند.

## ۹-۳ معرفی  نرم‌افزار safe

در پایان این فصل به معرفی نرم‌افزاری تحت عنوان Safe می‌پردازیم که با استفاده از آن می‌توانید وضعیت امنیت گوشی اندرویدی خود را متوجه شوید.

نرم‌افزار یاد شده یک آنتی‌ویروس نیست و تنها به شما کمک می‌کند تا متوجه شوید کدام ویژگی‌های گوشی با فعال‌بودنشان می‌توانند سطح امنیت تلفن هوشمند شما را پایین بیاورند.

اپلیکیشن Safe نام خود را از مخفف واژه‌های Safe Assessment Framework for Everyone به معنای «چارچوب ارزیابی همگانی» گرفته و هدف آن امکان بررسی ساده کیفیت امنیت گوشی‌های هوشمند است. تنها کافی است این نرم‌افزار را نصب کنید تا متوجه شوید که فعال‌بودن کدام ویژگی‌های گوشی امنیت آن را به خطر انداخته است.




نرم‌افزار Safe میزان کیفیت امنیت گوشی شما را پس از بررسی نمره دهی می‌کند. این نمره همراه با یک رنگ خاص نمایش داده می‌شود که به اگر سبز باشد به معنای امنیت خوب و اگر قرمز باشد به معنای امنیت بسیار پایین گوشی شما خواهد بود. همان‌طور که گفتیم بررسی همه تنظیمات برای بالابردن امنیت گوشی زمان بر است و گاهی فراموش می‌کنیم که کدام یک از آن‌ها را قبلاً تغییر داده بودیم.

نرم‌افزار Safe پس از بررسی اپلیکیشن‌ها و تنظیمات اعمال شده در سیستم‌عامل، نمره‌گذاری روی گوشی را در چند بخش متفاوت انجام می‌دهد و در نهایت نمره نهایی امنیت گوشی شما را نمایش خواهد داد.

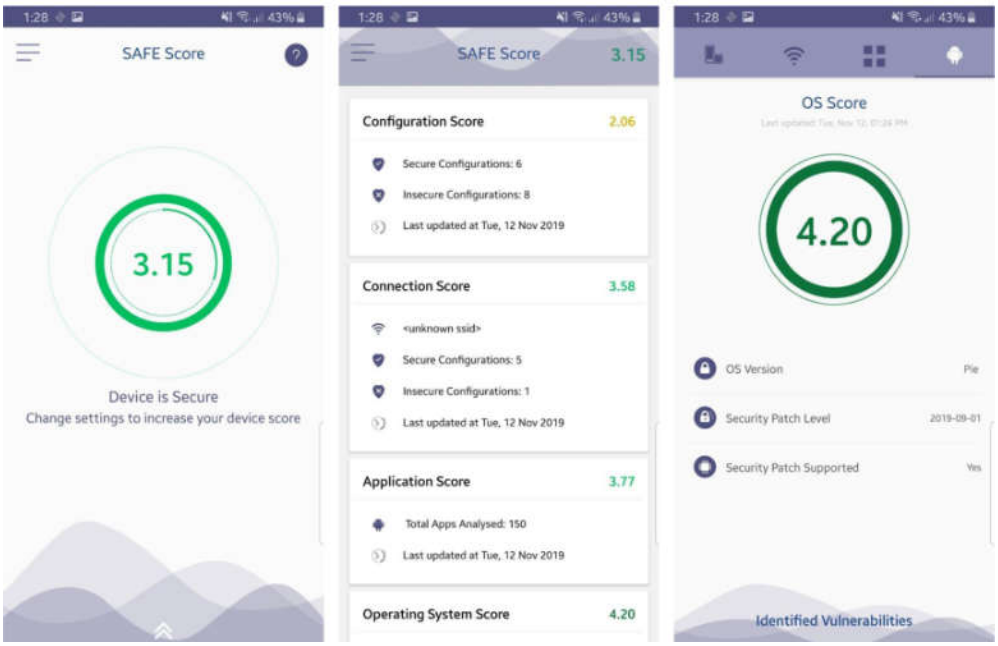
تعداد بخش‌های یاد شده چهار مورد هستند: نمره سیستم‌عامل، اپلیکیشن، اتصالات و اینترنت و در نهایت تنظیمات. نمره دهی به بخش سیستم‌عامل با تحلیل سیستم نصب شده روی گوشی انجام می‌شود. این که آخرین آپدیت‌ها را دارد و یا این که آخرین پچ امنیتی روی سیستم‌عامل نصب شده یا خیر. پس از دریافت نمره می‌توانید بخش مربوطه را اجرا کنید تا همه مواردی که گوشی را به خطر می‌اندازند را مشاهده نمایید.

بخش بعدی مربوط به اپلیکیشن‌هاست. نمره دهی به بخش یاد شده باتوجه‌به دسترسی‌هایی که هرکدام از نرم‌افزارهای نصب شده در اختیار دارند انجام می‌شود. Safe با بررسی همه اپلیکیشن‌های نصب شده روی گوشی تلاش می‌کند تحلیلی مناسب داشته باشد و درصورتی‌که اپلیکیشن خاص دسترسی‌های بی‌موردی در اختیارش قرار گرفته باشد نمره این بخش کاهش پیدا می‌کند.

بخش سوم مربوط به اینترنت و اتصالات گوشی است. نمره دهی به این بخش با تحلیل وضعیت اینترنت و نوع متصل شدن گوشی به روتر انجام می‌شود. همچنین هر نوع اتصال دیگر مثل NFC، بلوتوث و غیره در این بخش تحلیل و بررسی خواهند شد.

بخش نهایی نمره دهی به تنظیمات است. بسیاری از گزینه‌ها در بخش تنظیمات گوگل برخی دسترسی‌های نه‌چندان مناسب را در اختیار برخی اپلیکیشن‌ها و حتی مهاجمین قرار می‌دهد. اپلیکیشن Safe با تحلیل وضعیت ویژگی‌های موجود در تنظیمات و تغییراتی

که اعمال کرده‌اید کیفیت امنیت گوشی را می‌سنجد و با یک نمره آن را به اطلاعتان می‌رساند.




بعد از دریافت نمره کاربران می‌توانند با واردشدن به هر بخش در جریان جزئیات امنیت گوشی خود قرار بگیرند. با ورود به هر بخش، همه موارد مثبت و منفی که روی امنیت گوشی تأثیرگذار هستند نمایش داده خواهند شد. با زدن روی هرکدام از موارد می‌توانید جزئیات بیشتری راجع به آن‌ها مطالعه کنید و ببینید که به چه دلیل ممکن است روی امنیت گوشی شما تأثیرگذار باشند.

شما می‌توانید موارد مثبت و منفی یاد شده را مرتب کنید تا به‌راحتی همه موارد را به‌صورت مجزا مشاهده نمایید. همچنین یکی از مزیت‌های قابل‌توجه اپلیکیشن Safe این است که با

ورود به هرکدام از مواردی که تأثیری منفی روی امنیت گوشی شما گذاشته است، می‌توانید مراحل رفع مشکل را مطالعه کنید و با انجام توصیه‌های گفته شده در آن بخش، امنیت تلفن هوشمند خود را بالا ببرید.

نرم‌افزار Safe در حال حاضر در گوگل‌پلی در اختیار کاربران اندرویدی قرار گرفته است و می‌توانید با دانلود آن امنیت گوشی خود را بسنجید. یکی از مزیت‌های بسیار خوب این اپلیکیشن عدم نمایش تبلیغات و کاملاً رایگان بودن آن است. با استفاده از Safe می‌توانید از کیفیت امنیت گوشی خود مطمئن شوید و با بررسی مواردی که روی این موضوع مهم تأثیر می‌گذارد، با اطمینان بیشتری از تلفن هوشمند خود استفاده کنید.

لازم به ذکر است که اپلیکیشن یاد شده فقط برای سیستم‌عامل اندروید عرضه شده است.

## ۳-۱۰ جمع‌بندی

امروزه تلفن‌های همراه از مهم‌ترین ابزارهای مورداستفاده روزمره انسان‌ها است که به آسان‌تر شدن هر چه بیشتر فرایندها کمک می‌نمایند.

تلفن‌های همراه بدون شک به عضو جدایی‌ناپذیر زندگی انسان تبدیل شده‌اند و مزایای فراوانی دارند. اما در کنار این فواید، معایبی هم دارند که بدون رعایت نکات امنیتی نمی‌توان به‌راحتی از کنار آن گذشت. در واقع گوشی‌های تلفن همراه به گنجینه‌هایی باارزش از اطلاعات تبدیل شده‌اند.

گنجینه‌هایی که می‌توانند تصاویر و فیلم‌های خصوصی باشند یا اطلاعات بانکی یا اطلاعات کاری و محرمانه که در صورت انتشار عواقب جبران‌ناپذیری به دنبال خواهند داشت. کارشناسان امنیتی می‌گویند سیاست مجرمان استفاده از آسیب‌پذیری گوشی‌های هوشمند است و به همین دلیل گوشی‌های هوشمند دستگاه موردعلاقه هکرها به شمار می‌روند.(موسوی، ۱۳۹۶)

گوشی‌های تلفن همراه مجهز به امکانات ارتباطی متنوعی مانند wifi، bluetooth hotspot و Mobile data و NFC هستند؛ هنگامی‌که از این امکانات ارتباطی استفاده نمی‌کنیم باید آن‌ها را غیرفعال کرد. مجرمان می‌توانند تا با هک و نفوذ به گوشی ما، اختیار آن را در دست گرفته، ضمن برقراری تماس‌های تلفنی از شماره ما، اطلاعات و محتواهای

درون‌گوشی را نیز به سرقت ببرند. حتماً توجه داشت در زمان‌هایی که از ابزارهای مربوط به تلفن همراه (بلوتوث، وای‌فای و غیره) استفاده نمی‌شود باید آن‌ها را غیرفعال کرد.

استفاده از تلفن همراه هوشمند در صورت نداشتن آگاهی، ممکن است ناخواسته به سرویس‌های امنیتی ـ جاسوسی کمک قابل‌توجهی در رسیدن به اهدافشان کند.

موقعیت‌یاب جهانی[۶۱] را فقط باید در مکان‌هایی که به آن نیاز داریم روشن نگه داشت. جهت جلوگیری از ورود بدافزار به تلفن همراه، نرم‌افزارهای موردنیاز خود را از سایت‌های معتبر دانلود کنیم. متأسفانه روزبه‌روز شاهد افزایش بدافزارهایی هستیم که موبایل‌ها و گجت‌های هوشمند را به یک ابزار جاسوسی تبدیل می‌کنند. تمامی این اتفاقات ناشی از یک چیز است، مجوزهایی که خودمان به برنامه‌ها هنگام نصب می‌دهیم. هر نرم‌افزار نیاز به مجوزهای خاص خود را دارد. به‌عنوان‌مثال پیام‌رسان‌ها نیاز به مجوز دسترسی به تصاویر ما را دارند تا بتوانند عکس موردنظر ما را ارسال کنند. این یک مجوز منطقی است چون کار پیام‌رسان این است. نصب یک برنامه مخرب می‌تواند اجازه کنترل از راه دور را برای مهاجم فراهم کند و در این حالت گوشی هوشمند ما، یک وسیله جاسوسی هوشمند است تا یک گوشی هوشمند.

---

[۶۱] GPS

بسیاری از بدافزارهای خطرناک تحت پوشش اپلیکیشن‌های متعددی که در وب‌سایت‌ها و فروشگاه‌های آنلاین وجود دارند می‌توانند به دستگاه الکترونیکی، رایانه و گوشی هوشمند کاربران نفوذ یابند و برای هکرها امکان دسترسی به اطلاعات شخصی آن‌ها را فراهم آورند.

# فصل چهارم: امنیت در  شبکه های اجتماعی


سؤالات مهم فصل چهارم:

**رعایت موارد امنیتی در شبکه‌های اجتماعی مجازی به چه معناست؟**

**جعل هویت کاربران با چه اهدافی صورت می‌گیرد؟**

**شگردهای کلاهبرداری در شبکه‌های اجتماعی چیست؟**

**نکات امنیتی مهم در شبکه‌های اجتماعی پرکاربرد مانند اینستاگرام چیست؟**

## ۴-۱ تعریف شبکه‌های اجتماعی

شبکه‌های اجتماعی، نسل جدیدی از وب‌سایت‌ها هستند که این روزها در کانون توجه کاربران شبکه جهانی اینترنت قرار گرفته‌اند. این‌گونه سایت‌ها بر مبنای تشکیل اجتماعات آنلاین فعالیت می‌کنند و هرکدام دسته‌ای از کاربران اینترنتی با ویژگی خاصی را گرد هم می‌آورند. شبکه‌های اجتماعی را گونه‌ای از رسانه‌های اجتماعی می‌دانند که امکان دستیابی به نحوه جدیدی از برقراری ارتباط و به‌اشتراک‌گذاری محتوا در اینترنت عضو صدها شبکه اجتماعی مختلف هستند و بخشی از فعالیت آنلاین روزانه‌شان در این سایت‌ها می‌گذرد.)لطفی و دیگران، ۱۳۹۷(

## ۴-۲ انواع شبکه‌های اجتماعی

شبکه‌های اجتماعی را در ساده‌ترین تقسیم‌بندی می‌توان در دو گروه عمومی و خصوصی قرارداد. در شبکه‌های اجتماعی عمومی کاربران اینترنتی باانگیزه‌ها و اهداف مختلف حضور دارند و شبکه‌سازی مجازی‌شان را از طریق این وب‌سایت‌ها دنبال می‌کنند، ولی شبکه‌های اجتماعی خاص حول موضوعی ویژه شکل‌گرفته‌اند و تعداد کاربرانشان نیز کمتر است. فیس‌بوک، تلگرام و اینستاگرام از مهم‌ترین شبکه‌های اجتماعی عمومی در ایران هستند؛ اما این شبکه‌های اینترنتی عمومی نیز اغلب در ابتدای فعالیتشان با تعریف محدودی آغاز به کارکرده‌اند و به‌تدریج عمومی شده‌اند. چنان‌که فیس‌بوک که امروزه به بزرگ‌ترین شبکه اجتماعی دنیا تبدیل‌شده است در سال ۲۰۰۴ شبکهٔ اجتماعی دانشجویان دانشگاه هاروارد

بود. دایرهٔ کاربران فیس‌بوک در چند مرحله گسترش پیدا کرد تا اینکه در سال ۲۰۰۶ به همه کاربران اینترنت رسید. علاوه بر این‌ها، شبکه‌های اجتماعی خاصی نیز وجود دارد که بر محوریت موضوعی مشخص فعالیت می‌کنند.

## ۳-۴ کارکردهای شبکه‌های اجتماعی

در هر کشور و هر جامعه‌ای متناسب بافرهنگ، تعاملات اجتماعی و فعالیت‌های سیاسی و اقتصادی، کارکردهای شبکه‌های اجتماعی باهم متفاوت است؛ اما برخی کارکردهای شبکه‌ای در تمامی جوامع باهم مشترک است. مهم‌ترین کارکرد شبکه‌های اجتماعی ایجاد گروه‌ها و دسته‌های ارتباطی[۶۲] پیرامون ویژگی یا ویژگی‌های خاص است.

همچنین کارکردهای اقتصادی، مبتنی بر بازاریابی اجتماعی نیز از دیگر کارکرده‌های این شبکه‌هاست. کارکرد دیگری که برای این شبکه‌ها متصور است کارکرد سیاسی است. ایجاد کمپین‌های سیاسی در یک فضای اجتماعی اینترنتی از کارکردهای شبکه‌های اجتماعی است. می‌گذارند، عملاً کارکرد جاسوسی دارند و به‌راحتی این امکان را به دشمن می‌دهند که به اطلاعات مکانی مراکز مهم، حساس و حیاتی بدون کمترین زحمتی دسترسی داشته باشد

[۶۲] Community

## ۴-۴ امنیت در شبکه‌های اجتماعی مجازی

شبکه‌های اجتماعی مجازی در حال حاضر آن‌چنان فراگیر شده است که حتی بسیاری از شرکت‌ها و سازمان‌ها سامانهٔ ارتباطی داخلی بین اعضا و کارکنان خود را به طور رسمی از طریق این سامانه تأمین می‌کنند و روزبه‌روز نیز به شمار کاربران این شبکه‌ها افزوده می‌شود، واژه امنیت اطلاعات حجم وسیع از فعالیت‌ها را تحت پوشش قرار می‌دهد.

معمولاً در شبکه‌های اجتماعی مجازی، جزئی‌ترین اطلاعات کاربران نیز قابل دریافت و انتشار است. علاقه‌مندی‌ها، میزان تحصیلات، ارتباطات خانوادگی، ارتباطات دوستانه، شغل، محل زندگی و... مورد سؤال قرار می‌گیرد.

شبکه‌های اجتماعی مجازی خطرات خاص خود رادارند که ممکن است با رعایت‌نکردن نکات امنیتی برای کاربر دردسرساز شوند و یا هکرها می‌توانند از طریق رسانه‌های اجتماعی به اطلاعات شخصی شما دست پیدا کنند و یا ویروس‌های موردنظر خود را وارد سیستم شما کنند و شمارا مورد آزار و اذیت قرار دهند.

این اتفاقات ممکن است حتی تا جایی پیش بروند که شهرت و اعتبار و موقعیت شغلی شما و درنهایت زندگی شمارا نشانه بروند و آن‌ها را نابود کنند. پس شما نیاز دارید تا در شبکه‌های اجتماعی ایمن بمانید. اقدامات زیر را دنبال کنید و مطمئن باشید زندگی اجتماعی آنلاین شما، ضداجتماعی نخواهد شد.

### ۱-۴-۴ جعل هویت کاربران

یکی از مهم‌ترین موضوعاتی که کاربران را تهدید می‌کند موضوع جعل هویت است. بخصوص درزمانی که کاربر در زمینه‌ای جزو افراد سرشناس و شناخته‌شده باشد. درصورتی‌که در حیطهٔ کسب‌وکار یا حوزهٔ اجتماعی خود، فرد سرشناسی هستید، ممکن است افراد دیگری با سوءاستفاده از محتواها و اطلاعاتی که شما به‌صورت عمومی به اشتراک گذاشته‌اید، با نام و هویت جعلی شما و با راه‌اندازی صفحات مشابه دست به اخاذی، کلاهبرداری و سایر اقدامات مجرمانه بزنند. ازاین‌رو هوشیاری در حفظ اطلاعات و محتواهای خصوصی کاملاً اهمیت دارد. همچنین درصورتی‌که متوجه شدید شخصی باهویت شما اقدامات مجرمانه صورت می‌دهد، موضوع را به پلیس فتا اعلام کنید.

در واقع سرقت هویت به معنای استفاده غیرقانونی از اطلاعات شخصی یک فرد است. مجرمان و کلاهبرداران سایبری می‌توانند اطلاعات شما را سرقت کرده و از آنها برای انجام عملیات‌های مالی و فعالیت‌های مجرمانه سوءاستفاده کنند. آنها همچنین می‌توانند با اطلاعات شما یک حساب بانکی جدید بازنموده یا به هویت شخصی شما لطمه جدی وارد کنند.

برای جلوگیری از جعل هویت موارد ذیل پیشنهاد می‌شود:

۱- از کلمه عبور مناسب برای حساب‌های کاربری خود استفاده کنید.

۲- مطمئن شوید کلمات عبور شما قوی و منحصربه‌فرد هستند.

۳- از اطلاعات محرمانه خود محافظت کرده و آن را در اینترنت قرار ندهید.

۴- قبل از ارسال اطلاعات شخصی خود در شبکه‌های اجتماعی، ابتدا کمی فکر کنید.

۵- مراقب کلاهبرداری‌های فیشینگ باشید.

۶- در هنگام خرید آنلاین، بیشتر مراقب باشید.

۷- مرورگر خود را امن کنید.

۸- با نصب چندین محصول امنیتی مختلف، از رایانه خود محافظت کنید.

۹- از راهکارهای امنیتی ویژه برای مقابله با بدافزارها و سرقت اطلاعات استفاده کنید.

### ۴-۴-۲ محافظت در مقابل کرم‌های رایانه‌ای و تروجان‌ها

برخی از خدمات شبکه‌های اجتماعی مثل اپلیکیشن‌ها در دل خود، کرم‌های رایانه‌ای و تروجان‌ها را انتشار می‌دهند؛ بنابراین در فضای شبکه‌های اجتماعی، به هر خدمتی که از سوی کاربران دیگر به شما پیشنهاد می‌شود اعتماد نکنید.

### ۴-۴-۳ اعتماد نکردن به افراد ناشناس

فضای شبکه‌های اجتماعی مملو از کاربرانی است که باهویت‌های جعلی و برای مقاصد خاص مثل کلاهبرداری، اشاعه فحشاء و سایر اقدامات غیرقانونی و مجرمانه نسبت به ارتباط‌گیری با کاربران اقدام می‌کنند. ازاین‌رو از پذیرفتن افرادی که باهویت، تصاویر و طرح مطالب اغواکننده سعی در ارتباط‌گیری و افزودن شما به لیست دوستان یا علاقه‌مندان صفحهٔ خود رادارند، اجتناب کنید.

### ۴-۴-۴ انجام‌دادن تنظیمات حریم خصوصی

تمامی شبکه‌های اجتماعی، ابزارهایی را در اختیار شما می‌گذارد که نسبت به تنظیم حوزهٔ حریم خصوصی خود اقدام کنید. با استفاده از این ابزارها می‌توانید با خیال راحت‌تر نسبت به‌اشتراک‌گذاری اطلاعات با دوستان اقدام کنید و دسترسی دیگران را محدود نمایید؛ و همچنین با استفاده از تنظیمات حریم خصوصی به‌منظور اطلاع از اینکه چه کسانی اطلاعات شخصی شمارا مشاهده می‌نمایند می‌توان استفاده کرد.

### ۴-۴-۵ رعایت احتیاط در مورد کلیک کردن بر روی لینک‌ها

حتی اگر لینک در پیامی است که از سوی دوست شما فرستاده‌شده است در هنگام کلیک کردن بر روی آن بااحتیاط باشد. به‌این‌علت که ممکن است اطلاعات حساب کاربری ارسال لینک‌های مخرب به لیست تماس‌های او باشند.

### ۴-۴-۶ روش‌های سرقت اطلاعات هویتی کاربران

در ادامه به انواع روش‌های سرقت اطلاعات هویتی کاربران اشاره می‌شود

#### ۴-۴-۶-۱ دزدیدن اطلاعات شخصی از پروفایل

برخی کاربران در صفحه عمومی خود محتوایی شامل اطلاعات شخصی‌شان مانند عکس، تاریخ تولد یا لوکیشن و محل سکونت را به اشتراک می‌گذارند و در دسترس دیگران قرار می‌دهند که هکرها و سایر افراد سودجو به‌راحتی می‌توانند از آن سوءاستفاده نمایند.

#### ۴-۴-۶-۲ دزدیدن اطلاعات شخصی کاربران از طریق حملات فیشینگ

این روزها حملات فیشینگ بسیار رایج است. هکرها با فریب‌دادن کاربران از طریق ایمیل‌های جعلی به‌ظاهر عادی و مناسبی که لینک مخرب و آلوده‌ای دارد، شما را ترغیب می‌کنند اطلاعات حساب کاربری خود مثل نام کاربری و پسورد را در صفحه‌ای وارد کنید و بعد به‌سادگی آن را سرقت می‌کنند.

در نهایت هم می‌توانند با واردشدن به‌حساب شما به داده‌های پروفایلتان دسترسی پیدا کنند. گاهی هم هکرها با ترغیب شما به نصب یک ابزار مخرب که لینک دانلود آن را برایتان می‌فرستند، به اطلاعات شما دست پیدا می‌کنند. به‌عبارت‌دیگر کافی است آن بدافزار را روی دستگاه‌تان نصب کنید تا هکرها بتواند تمام کارهایی که انجام می‌دهید را رصد کنند.

### ۲-۶-۴-۴ دزدیدن اطلاعات شخصی کاربران از طریق نرم‌افزارهای شخص ثالث

گاهی در پنجره‌های تبلیغاتی باز شونده، استفاده از ابزارهای شخص ثالث از جمله نرم‌افزار یا افزونه مرورگر به کاربران پیشنهاد داده می‌شود. بسیاری از کاربران با بی‌توجهی کامل این پیام‌ها را تأیید و ابزاری را نصب می‌کنند که هیچ کارایی خاصی برایشان ندارد و فقط یک نرم‌افزار مخرب است که به طور پنهانی اطلاعات کاربران را جمع‌آوری و به متجاوزان ارسال می‌کند.

## ۴-۴-۷ شگردهای کلاهبرداری در شبکه‌های اجتماعی

ضروری است که همه اشخاص در فضای مجازی و در اینترنت بااحتیاط عمل کنند و با شناخت قوانین و افزایش اطلاعات در حوزه دیجیتال، از تحقق جرائمی مانند کلاهبرداری اینترنتی پیشگیری نمایند.

### ۱-۷-۴-۴ کلاهبرداری با کدهای فعال‌سازی شبکه‌های اجتماعی

کلاهبرداران با شماره‌تلفن شهروندان در شبکه‌های اجتماعی ثبت‌نام کرده و کد پیامک شده جهت تأیید هویت را نیز با ترفندهای گوناگون از قربانی دریافت می‌کنند و پس از فعال‌سازی شماره قربانی در شبکه‌های اجتماعی، اقدام به کلاهبرداری می‌کنند.

اغلب موارد مجرمان سایبری پس از دسترسی غیرمجاز به اکانت شبکه‌های اجتماعی شهروندان، با ارسال پیامی به دنبال‌کننده‌ها، از آن‌ها درخواست مبلغی پول به‌عنوان قرض

را دارند و یا اینکه با دسترسی به اطلاعات دیگر مانند عکس، فیلم و... اقدام به تهدید، اخاذی و هتک حرمت و حیثیت افراد می‌کنند.

برای جلوگیری از هرگونه کلاهبرداری از کاربران شبکه‌های اجتماعی به‌هیچ‌عنوان گوشی همراه و کد فعال‌سازی اکانت شبکه‌های اجتماعی خود را در اختیار دیگران قرار ندهید.

چرا که افراد سودجو با دسترسی به گوشی و اطلاعات شما در کمترین زمان ممکن می‌توانند به اهداف مجرمانه خود برسند.

همچنین اگر پیامی مبنی بر دریافت کمک مالی از سوی دوستان و آشنایان خود از طریق شبکه‌های اجتماعی دریافت کردید، قبل از هرگونه واریز وجهی از اصالت هویت فرستنده پیام با برقراری تماس تلفنی، اطمینان حاصل کنید.

### ۲-۷-۴-۴ اخاذی و کلاهبرداری با دسترسی غیرمجاز به شبکه‌های اجتماعی

برای مثال در پرونده‌ای تمامی قربانیان جستجوی شغل در سایت‌های آگهی فعال بوده و با مشاهده آگهی استخدام منشی با شرایط ویژه، بلافاصله اقدام به تماس با شخص آگهی‌دهنده می‌کنند.

مجرم که درپوشش استخدام یک منشی برای شرکت در کمین قربانی خود است وانمود می‌کند جهت ثبت‌نام نیاز به مشخصات کامل از جمله نام و نام خانوادگی، کد ملی و شماره تماس دارد و باید کدی که برای شماره شما ارسال می‌کنیم را جهت فعال‌کردن پنل کاربری به ما اعلام کنید.

در ادامه و پس از ارائه کد فعال‌سازی توسط شاکی به این مجرم، فرایند کلاهبرداری آغاز می‌شود.

متهم به‌حساب‌های کاربری شاکی در شبکه‌های اجتماعی از جمله تلگرام و واتس‌اپ دسترسی غیرمجاز می‌گیرد و ضمن اخاذی و درخواست‌های غیراخلاقی از قربانی با سوءاستفاده از تصاویر و اطلاعات شخصی وی با ارسال پیام نیاز مالی به مخاطبین شاکی، اقدام به کلاهبرداری از آنها می‌کند.

## ۴-۵ امنیت در شبکه اجتماعی اینستاگرام

یکی از شبکه‌های اجتماعی پربازدید و بسیار فعال اینستاگرام است بنابراین به جهت فراگیری این شبکه و تعداد کاربران فراوان آن در کشور ایران در این بخش نکاتی راجع به امنیت کاربران در این شبکه اجتماعی بیان می‌گردد.

اینستاگرام یک شبکه اجتماعی برای به اشتراک گذاشتن عکس‌ها و فیلم‌های کوتاه است،

کاربران در اینستاگرام مشخصات هویتی و احتمالاً موقعیت مکانی را نیز ثبت می‌کنند، می‌توانند کاربران دیگر را در دایره دوستان خود بپذیرند و عکس‌ها را با آن‌ها به اشتراک بگذارند. سؤالی که مطرح می‌شود این است، آیا اقدامات امنیتی لازم در مورد اینستاگرام را رعایت می‌شود؟

در ادامه به هشت قدم برای حفظ امنیت حساب اینستاگرام اشاره می‌کنیم.

### ۱-۵-۴ حساب کاربری‌تان را خصوصی[۶۳] کنید

یکی از نکته‌های مهم حفظ امنیت حساب اینستاگرام محدودکردن آن به دوستانی است که آنها را می‌شناسید. فقط به دوستان مورد اعتمادتان اجازه دهید عکس‌های شما و خانواده و یا هر عکس دیگری که منتشر می‌کنید ببینند. برای این کار باید حساب کاربری اینستاگرام شما خصوصی باشد:

وارد پروفایل حساب کاربری‌تان شوید. روی گزینه EDIT YOUR PROFILE کلیک کنید

در پایین پنجره باز شده روی گزینه Posts are Private کلیک کنید

مطمئن شود رنگ دکمه Posts are Private آبی شده است به معنی در حالت فعال‌بودن است. حالا می‌توانید مطمئن شوید فقط افرادی که شما را دنبال می‌کنند، می‌توانند عکس‌های شما را ببینند.

[۶۳] Private

### ۴-۵-۲ مسدود نمودن افراد ناشناس

افراد ناشناس که شما را دنبال[۶۴] می‌کنند مسدود[۶۵] کنید، افرادی که شما را دنبال می‌کنند قادر هستند عکس‌ها و همچنین موقعیت مکانی آن‌ها یعنی موقعیت شما را ببینند. نکته مهم در مورد شبکه‌های اجتماعی این است که با کسانی در ارتباط باشید که آن‌ها را می‌شناسید، پس نگاهی به دنبال‌کننده‌های خود بیندازید و ببینید افرادی هستند که هویت آن‌ها برای شما مشخص نیست؟ آنها را مسدود کنید. به‌این‌ترتیب فقط افرادی را در قسمت دنبال‌کننده‌های خود خواهید داشت که می‌شناسید و به آن‌ها اعتماد دارید.

لیست Followers خود را بررسی کنید

آیکن منو در گوشه سمت راست را انتخاب کنید

در پنجره باز شده روی گزینه Block User کلیک کنید

### ۴-۵-۳ حفظ حریم شخصی

در قسمت معرفی خودتان اطلاعات بیش اندازه ننویسید و سعی کنید با منتشر نکردن اطلاعات مهم در باره خودتان، حریم شخصی‌تان را حفظ کنید. وارد قسمت EDIT PROFILEحساب کاربری‌تان شوید و اطلاعات بیش از اندازه و مهمتان را حذف کنید.

---

[۶۴] Follow
[۶۵] Block

این قسمت به خود شما بستگی دارد، ممکن است حتی نوشتن اسم فرزندتان حریم شخصی‌تان را به خطر بیندازد.

### ۴-۵-۴ موقعیت خود را منتشر نکنید

یکی دیگر از اقدامات امنیتی اینستاگرام برای حفظ اطلاعات شناسایی شما و همچنین جلوگیری از خطرات دنیای دیجیتال و واقعی، مخفی نگاه‌داشتن موقعیتتان است. مطمئن شوید که سرویس لوکیشن[۶۶] یا همان موقعیت مکانی شما در حساب کاربری اینستاگرام‌تان خاموش یا غیرفعال است. فراموش نکنید در قدم اول خودتان در عنوان‌های عکس‌هایی که منتشر می‌کنید موقعیت‌تان را ننویسید.

- وارد Profile حساب کاربری‌تان شوید
- وارد قسمت Photo Map شوید
- روی آیکن منو در گوشه سمت راست کلیک کنید
- تغییرات لازم در جهت پاک کردن موقعیت‌تان را انجام دهید.

[۶۶] location

### ۵-۵-۴ تظیمات تأیید تصاویر

تصور کنید فردی برای خصومت و یا هر دلیلی حساب اینستاگرام شما را در عکس نامناسبی تگ[۶۷] بکند و یا شما عکسی را با دوستتان انداخته‌اید که نمی‌خواستید منتشر کنید ولی دوست شما این عکس را در اینستاگرام منتشر می‌کند و شما را تگ می‌کند یعنی نام شما و حساب کاربری اینستاگرامتان به آن عکس اضافه می‌شود!

برای این کار باید گزینه تگ کردن را به حالت دستی تغییر دهید به این معنی که شما تشخیص بدهید کدام عکس به شما تعلق دارد یا نه.

- وارد Profile حساب کاربری اینستاگرام‌تان شوید
- وارد قسمت Photos of You شوید
- روی آیکن منو در گوشه سمت راست کلیک کنید
- روی گزینه add photos manually کلیک کنید

[۶۷] Tagg

### ۴-۵-۶ احراز هویت دو عاملی

یکی از نکته‌های مهم **حفظ امنیت حساب اینستاگرام** فعال‌کردن احراز هویت دو عاملی است. احراز هویت دو عاملی در واقع یک‌لایه امنیتی دیگری برای حفاظت از حساب آنلاین شما اضافه می‌کند. در مواقعی که مجرمان سایبری از هر طریقی به رمز عبور شما دسترسی داشته باشند، با فعال‌بودن احراز هویت دو عاملی نمی‌توانند وارد حساب آنلاین شما شوند زیرا به کد دوم دسترسی ندارند شما این کد دوم یکتا و تاریخ دار را از طریق ایمیل یا پیامک دریافت می‌کنید.

### ۴-۵-۷ دسترسی اپلیکیشن‌های دیگر

احتمالاً با حساب اینستاگرام خود در سرویس‌های دیگر حساب کاربری ایجاد کرده‌اید. اگر این‌چنین است باید این دسترسی‌ها را کنترل کنید و فقط به اپلیکیشن‌های مطمئن و قابل‌اعتماد امکان دسترسی بدهید.

بررسی دسترسی اپلیکیشن‌ها به‌حساب اینستاگرام:

۱ -روی لپ‌تاپ یا کامپیوترتان وارد حساب کاربری اینستاگرام شوید

۲ -روی عکس پروفایلتان کلیک کنید و Edit Profile را انتخاب کنید

۳ -از منوی باز شدهManage Applications را انتخاب کنید. در این صفحه می‌توانید دسترسی اپلیکیشن‌های غیرضروری یا غیرقابل‌اعتماد را قطع کنید.

## ۶-۴ جمع‌بندی

امنیت شبکه‌های اجتماعی بسیار مهم است زیرا ماهیت و طبیعت شبکه‌های اجتماعی، اجتماعی شدن و مراوده است.

به این معنی که کاربران سپر زندگی روزمره را زمین می‌گذارند و بدون هیچ ملاحظه‌ای به گسترش ارتباطاتشان می‌پردازند.

کاربران ایرانی استقبال گسترده‌ای از شبکه‌های اجتماعی کرده‌اند و همان گونه که در زمینهٔ وبلاگ‌نویسی در مقاطعی رتبهٔ اول را در جهان (به نسبت جمعیت) به خود اختصاص داده بودند، در شبکه‌های اجتماعی نیز حضوری گسترده و فعال داشته‌اند به‌عنوان‌مثال پس از راه‌اندازی سامانه اورکات، ایرانی‌ها پس از برزیلی‌ها، آمریکایی‌ها و هندی‌ها به چهارمین ملیت در این شبکهٔ اجتماعی تبدیل شدند اما همواره در کنار این حضور پرحجم حریم شخصی کاربران شبکه‌های اجتماعی نیز باید حفظ شود.

در این فصل ضمن معرفی شبکه‌های اجتماعی و کارکردهای آن به مهم‌ترین موضوعات حوزه امنیت در این شبکه‌ها از تنظیمات حریم شخصی تا پیشگیری از سرقت اطلاعات و شگردهای کلاهبرداران پرداخته شد، تا ضمن معرفی این موارد کاربران شبکه‌های اجتماعی بتوانند از آسیب‌های پیش‌رو جلوگیری نمایند.

# فصل پنجم: امنیت کودکان در فضای مجازی

سؤالات مهم فصل پنجم:

- ✓ محافظت کودکان در برابر آسیب‌ها و تهدیدات فضای مجازی چه ضرورت دارد؟
- ✓ آسیب‌های تلفن همراه هوشمند برای کودکان چیست؟
- ✓ خطرات فضای مجازی برای کودکان کدام است؟
- ✓ آسیب‌های بازی‌های ویدئویی آنلاین چیست؟
- ✓ آیا خریدهای آنلاین توسط کودکان می‌تواند دردسرساز شود؟
- ✓ آیا می‌توان از فناوری جهت حفاظت از فرزندان در برابر تهدیدات فضای مجازی استفاده کرد؟

## ۱-۵ مقدمه

مسئله حضور کودکان در فضای مجازی به یکی از معضلات زندگی خانواده‌های امروزی در عصر دنیای دیجیتال تبدیل شده؛ نگرانی از خطرهای حضور کودکان در این بخش از مسائلی است که ذهن بسیاری از والدین را به خود مشغول کرده است.

بر اساس آخرین آمارهای اعلام شده در سال ۱۳۹۶ از سوی وزارت ارتباطات، ۷۲ درصد کاربران اینترنت در کشور زیر ۲۹ سال هستند. همچنین بر اساس این آمار، ۱۹ میلیون و ۸۰۰ هزار نفر از کاربران اینترنت زیر ۱۸ سال هستند. (گزارش توسعه فناوری اطلاعات وزارت ارتباطات ۱۳۹۶)

در کشورهای دیگر قانون مدون و مشخصی در خصوص استفاده کودکان از تلفن‌های همراه و شیوه ورود به فضای مجازی وجود دارد و این موضوع در کشورمان با خلأ مواجه است.

در بسیاری از کشور اجرای طرح‌ها و برنامه‌هایی برای محافظت از کودکان در فضای مجازی به‌صورت قانون رسمی تصویب شده است. برای مثال بر اساس گزارشی که روزنامه گاردین منتشر کرده، در انگلیس متوسط سن استفاده از موبایل ۱۰,۳ سال اعلام شده است. این کشور با تنظیم قوانینی از کودکان در فضای آنلاین محافظت می‌کند. «طراحی سنی مناسب» یکی از این قوانین است که همه تهیه‌کنندگان سرویس‌های آنلاین را ملزم به رعایت استانداردهای تعیین شده می‌کند.

## ۲-۵ ضرورت محافظت کودکان از آسیب و تهدیدات فضای مجازی

در حال حاضر با وجود شبکه جهانی اینترنت، شبکه‌های اجتماعی عامل اصلی بسیاری از دوستی‌های اینترنتی هستند. اما کودکان و نوجوانانی که در این فضا فعال‌اند ممکن است در معرض خطراتی قرار بگیرند، لذا ضروری است به کودکان کمک کنید که به‌خاطر داشته باشند امنیت سایبری همیشه باید در اولویت باشد.

پیشگیری از آسیب و تهدیدات فضای مجازی بی‌تردید از بزرگ‌ترین چالش‌های پیش‌روی والدین در فضای مجازی است.

اکنون بیش از هر زمان دیگر، ما اهمیت ایمنی را چه به‌صورت آنلاین و چه در دنیای واقعی درک می‌کنیم. شیوع ویروس کرونا میلیون‌ها خانواده را از سراسر جهان وادار کرده است فاصله اجتماعی را اتخاذ کرده و به دستگاه‌های مجهز به اینترنت برای برقراری ارتباط با دنیای خارج، دوستان و خانواده اعتماد کنند.

اما این نوع ارتباط هم دقیقاً مانند ارتباط در فضای واقعی نیازمند مراقبت‌های خاص است درگذشته اگر فرزندان یک ساعت بدون اطلاع والدین بیرون از خانه حضور داشتند چه حساسیت‌هایی برای این مسئله وجود داشت ولی امروزه فرزندان ساعت‌ها در فضای مجازی که به‌مراتب خطرناک‌تر از فضای حقیقی است بدون مراقبت والدین حضور دارند.

ورود به فضای مجازی مانند بسیاری از فعالیت‌هایی که فرزندان در دوران کودکی و نوجوانی خود انجام می‌دهند، نیازمند دارابودن مهارت‌هایی در این زمینه است که این مهارت‌ها در اثر ارائه آموزش درست از سوی والدین و رسانه‌های عمومی تکامل‌یافته و می‌تواند تضمین‌کننده سلامت کاربران باشد.

ورود به فضای مجازی توسط فرزندان می‌تواند در هر سنی که آنان درک کافی از این فضا دارند، اتفاق بیفتد ولی باید توجه داشت که فرزندان باید نسبت به خطراتی که در فضای مجازی وجود دارد در مرحله اول از طریق والدین آگاه شوند و نظارت دقیق نیز روی عملکرد آنان وجود داشته باشد. چنانچه این شرایط مهیا باشد والدین می‌توانند اجازه ورود فرزندان به فضای مجازی را بدهند.

### ۳-۵ آسیب‌های تلفن همراه هوشمند برای کودکان

تلفن‌های همراه وسایل ارتباطی بسیار سودمندی هستند و تعداد زیادی از والدین برای فرزندان خود تلفن همراه تهیه می‌کنند. در واقع امروزه، حدود ۷۰ درصد کودکان بین ۱۱ تا ۱۴ سال دارای تلفن همراه هستند. (گزارش پژوهشکده آمار ایران ۱۳۹۸)

استفاده فراگیر کودکان حتی در سنین ۳ سالگی به بعد آسیب‌های فراوانی به دنبال دارد که ما نظر به موضوع این کتاب به مباحث مرتبط با امنیت آن می‌پردازیم.

علاقه و استقبال کودکان از تکنولوژی‌های روز افزایش چشمگیری داشته و حتی یک کودک نو پا با تسلط کامل و شاید بهتر از خانواده خود از یک موبایل یا تبلت اندرویدی استفاده می‌کند. اما این‌ها مشکلاتی را نیز به همراه دارند که می‌توان به خرید بی‌اجازه از فروشگاه‌های نرم‌افزاری، دسترسی به محتوایی که مناسب سن آن‌ها نیست، ارسال محتوای گوش والدین برای دیگران و یا ارسال اطلاعات حساس برای مجرمان سایبری اشاره کرد.

یکی از موارد مهم پیشگیری از موارد مذکور تعیین دسترسی کودکان توسط برنامه‌های قفل کودک مانند (screen time limits for kids) است که به والدین این امکان را می‌دهد تا موارد ذیل را تنظیم نمایید:

۱. تعیین مدت‌زمان استفاده از برنامه‌های گوشی فرزندان
۲. محدودکردن گوشی کودکان و جلوگیری از نصب برنامه
۳. جلوگیری از ورود کودکان به سایت‌ها و شبکه‌های مجازی
۴. حذف نشدن برنامه
۵. محدودکردن دسترسی کودک به تنظیمات گوشی

## ۴-۵ استفاده کودکان از اینترنت

یکی از مهم‌ترین موارد پیشگیری از آسیبهای کودکان استفاده از اینترنت با نظارت والدین است، نتیجه نظرسنجی ها با موضوع کودک و اینترنت نشان می‌دهد، بسیاری از کودکان از سنین پایین شروع به استفاده از اینترنت می‌کنند، که نظارتی از سوی والدین بر آن نیست. تحقیقات نشان می‌دهند، که بیش از ۷۱ درصد والدین پس از ۱۴ سالگی فرزندان خود هیچ گونه نظارتی بر استفاده آن‌ها از اینترنت ندارند، این در حالی است که ۷۲ درصد گزارش ناپدید شدن کودکان که مربوط به جرائم اینترنتی است، برای کودکان بالای ۱۵ سال اتفاق افتاده است. زارش بنیاد امنیت کودکان در آمریکا نشان می‌دهد، که علی رغم مداخله و خواسته والدین، متأسفانه حدود ۳۲ درصد نوجوانان موفق به پنهان کردن اطلاعات و پاک کردن پیشینه مرورگر های سیستم خود می‌شوند. همچنین، ۱۶ درصد نوجوانان دارای ایمیل و حساب‌های کاربری در شبکه‌های اجتماعی بوده، که والدینشان از آن‌ها بی اطلاع هستند. اغلب کودکان و نوجوانان برای ایجاد این حساب‌های کاربری و جلب توجه دیگران در مورد سن خود دروغ می گویند.( گزارش مرکز تدوین سیاست‌های معاونت محتوایی مرکز ملی فضای مجازی ۱۳۹۹)

بهترین راه‌حل جلوگیری از این آسیب‌ها، نظارت والدین بر استفاده کودکان از اینترنت است.

## ۵-۵ خطرات فضای مجازی برای کودکان

### ۵-۵-۱ شکارچیان جنسی

گزارش مرکز ملی "کودکان گم‌شده و مورد سوءاستفاده قرار گرفته" آمریکا نشان می‌دهد، ۱۵ درصد از کودکانی که مورد سوءاستفاده جنسی قرار گرفته‌اند، به‌وسیله اینترنت در این دام افتاده‌اند.

برخلاف اعتقاد عامه، احتمال اغفال و وسوسه کودکان و نوجوانان، توسط هم‌سالان آن‌ها به‌صورت آنلاین، بیشتر است. حدود ۲۶ درصد از مجرمان جنسی آنلاین، با استفاده از اطلاعاتی که فرد بر روی صفحه شبکه اجتماعی خود منتشر کرده است، توانسته‌اند محل دقیق حضور قربانی خود را بیابند. اکثر کودکان و نوجوانان به‌وسیله دوستان خود ترغیب به‌اشتراک‌گذاری این اطلاعات می‌شوند. عامل اصلی این اتفاق‌های ناراحت‌کننده، عدم محافظت از کودکان در فضای مجازی است.

با رشد هرروزه اینترنت، جذب افراد زیر سن قانونی به آن نیز بیشتر و بیشتر می‌شود. نتایج یک تحقیق در سانتا کلارا نشان می‌دهد که میزان اغفال‌های جنسی آنلاین، در هر ماه به میزان هزار درصد افزایش می‌یابد. این دلیل مهم دیگری است، تا افراد آدرس محل سکونت و اطلاعات این‌چنینی را در اختیار عموم قرار ندهند.

### ۵-۵-۲ دوستی با غریبه‌ها

اغلب نوجوانان و حتی بزرگسالان، در شبکه‌های اجتماعی دوستانی دارند که هرگز آن‌ها را ملاقات نکرده‌اند، ولی اغلب با آن‌ها در تماس هستند. نوجوانان و کودکان راحت‌تر به دیگران اعتماد می‌کنند و اغلب حاضرند با غریبه‌ها ملاقات کنند. البته که دوستی‌های اینترنتی، بخش جدایی‌ناپذیر زندگی امروز هستند، اما والدین وظیفه دارند تا با نظارت، راهنمایی و محافظت از کودکان در فضای مجازی امنیت آن‌ها را در اینترنت فراهم کنند.

### ۵-۵-۳ حفاظت از اطلاعات شخصی

مطالعات نشان می‌دهد که ۱۷ درصد نوجوانانی که از شبکه‌های اجتماعی استفاده می‌کنند، تمام اطلاعات خود، از جمله آدرس محل زندگی و تحصیل، شماره‌تلفن و دیگر اطلاعات این‌چنینی را به‌صورت عمومی به اشتراک گذاشته‌اند.

از هر هفت نوجوان، یکی از آن‌ها از خود عکس برهنه یا نیمه برهنه گرفته است و نیمی از آن‌ها این عکس‌ها را در شبکه‌های اجتماعی یا با دیگران به اشتراک گذاشته‌اند. نکته مهم در این زمینه این است که وقتی داده‌ها بر روی اینترنت قرار گرفت، هیچ راهی برای حذف آن وجود ندارد. آگاهی درست والدین از راه‌های محافظت از کودکان در فضای مجازی و آموزش به کودک خود، از بسیاری اتفاق‌های جبران‌ناپذیر جلوگیری می‌کند.

### ۵-۵-۴ سوءاستفاده آنلاین

وب‌سایت‌ها و شبکه‌هایی وجود دارند که افراد می‌توانند به‌صورت ناشناس از دیگران سؤال مطرح کرده یا اطلاعاتی برای آن‌ها ارسال کنند. با پنهان شدن پشت صفحه رایانه و استفاده از ماسک ناشناس، برخی افراد به مسخره کردن دیگران و یا سایر سو استفاده‌ها پرداخته و موجب ناراحتی و افسردگی آن‌ها می‌شوند.

نکته مهم در این زمینه این است که کودکان و نوجوانان هرگز نباید به این‌گونه پیام‌ها پاسخ دهند و باید پیام‌های مشکوک را به والدین خود گزارش دهند.

### ۵-۵-۵ سرقت هویت در فضای مجازی

کودکان بیش از آنچه که فکر می‌کنید مورد سرقت هویت قرار می‌گیرند. در واقع، احتمال این اتفاق برای افراد زیر ۱۸ سال، ۵۱ برابر افراد بزرگسال است. مجرمان اغلب برای استفاده از اعتمادی که کودکان می‌توانند جذب کنند، از هویت آن‌ها استفاده می‌کنند، با جهل هویت یک کودک می‌توانند به روش‌های مختلف مرتکب جرایم سایبری گردند.

### ۵-۵-۶ خریدهای آنلاین

امروزه خرید آنلاین به دلیل راحتی بیش‌ازپیش رواج یافته است و کودکان و نوجوانان نیز از این امکان بهره می‌برند. مجرمان اینترنتی از این طریق هم می‌توانند به سوءاستفاده بپردازند. جهت هرگونه پیشگیری از مخاطرات فضای سایبری از جمله برداشت‌های غیرمجاز کودکان بر اثر خریدهای مختلف در سایت‌های فروشگاهی و بازی و ... والدین گرامی باید با افزایش آگاهی خود سعی بر نظارت بر استفاده صحیح فرزندان از فضای سایبری را داشته و با کاستن شکاف دیجیتالی خود با فرزندانشان از مخاطرات این فضا جلوگیری نمایند.

### ۵-۵-۷ بازی‌های ویدئویی آنلاین

بازی‌های اینترنتی در سال‌های اخیر طرف‌داران بسیاری پیدا کرده است. والدین باید از این موضوع که کودکان به‌وسیله اینترنت مستقیماً با سایر کودکان و بازی‌کنندگان در ارتباط هستند، آگاه باشند. مجرمان سایبری ضمن سوءاستفاده از ناآشنایی کودکان و نوجوانان با نحوه خرید آنلاین، با تبلیغ فروش اکانت بازی‌های آنلاین، آنها را فریب می‌دهند و در دام مجرمانه خود گرفتار می‌کنند. دریافت وجه و عدم واگذاری بازی از مهم‌ترین شگردهای مجرمانه دراین‌خصوص است که در ابتدا مبلغی به‌عنوان بیعانه از متقاضی دریافت می‌شود و در ادامه فرد کلاهبردار دیگر پاسخگوی قربانی نخواهند بود.

در شگردی دیگر می‌توان به عدم واگذاری دسترسی کامل اکانت بازی اشاره کرد که در این صورت پس از دریافت مبلغ کامل و واگذاری اکانت[۶۸]؛ دسترسی کاربر جدید بازی را با محدودیت مواجه می‌کنند.کودکان و نوجوانان باید حتماً برای خرید اکانت‌های بازی از والدین خود کمک بگیرند تا گرفتار مجرمان سایبری نشوند.

همچنین بهتر است والدین وقت محدودی برای انجام بازی‌های اینترنتی تعیین کنند. اجازه استفاده کودکان از فضای مجازی باید همراه با آموزش به آن‌ها داده شود.

### ۶-۵ آموزش، برای محافظت از کودکان در فضای مجازی

خطر های امنیتی زیادی از جمله شکارچیان جنسی و سرقت هویت، ما را تهدید می‌کنند. کودکان و نوجوانان ۵ تا ۱۵ سال برای استفاده از اینترنت به نظارت بزرگسالان نیاز دارند. توجه به نکات امنیتی خاص مانند به اشتراک گذاری اطلاعات شخصی و همچنین صحبت و آگاه کردن کودکان و نوجوانان از خطرات احتمالی می‌تواند شما و فرزندانتان را از وقوع احتمالی این خطرات تا حد زیادی حفاظت کند.

امروزه ضروری است والدین اگر خودشان به فناوری مسلط نیست برای آموزش فرزندانشان هزینه کنند تا در آینده متحمل هزینه‌های سنگین‌تری نشوند.

---

[۶۸] account

درمورد منابع آموزشی رایگان آنلاین محتاط باشید. فرزند شما هرگز نباید عکس یا اسم کامل خود را برای دسترسی به این منابع استفاده کند. به‌خاطر بسپارید که تنظیمات حریم خصوصی را کنترل کنید تا دریافت اطلاعات را به حداقل برسانید.

## ۷-۵ ضرورت گفتگوی والدین با فرزندان

با فرزندان خود صادقانه راجع به کسانی که با آنها در ارتباط هستند و چگونگی ارتباطشان صحبت کنید. اطمینان حاصل کنید که اهمیت و ارزش تعاملات دوستانه و حمایتگرانه را می‌فهمند و این‌که رفتارهای تبعیض‌آمیز و نامناسب هرگز قابل‌قبول نیستند.

آنها را تشویق کنید که اگر هر یک از این رفتارها را تجربه کرده‌اند فوراً موضوع را با شما یا شخص بالغ و معتمدی در میان بگذارند. نسبت به حالات فرزندتان هنگام کار با اینترنت هشیار باشید که مثلاً آیا غمگین یا پنهان‌کار به نظر می‌رسد، یا اذیت و آزار اینترنتی را تجربه می‌کند.

به همراه فرزند خود قوانینی وضع کنید که چگونه و چه زمانی می‌توانند از این وسایل استفاده کند.

### ۸-۵ استفاده از فناوری جهت حفاظت از فرزندان

مطمئن شوید که لوازم الکترونیکی فرزندتان به آخرین نسخه نرم‌افزار و آنتی‌ویروس مجهز باشد و تنظیمات حریم خصوصی روشن باشد. دوربین (وب‌کم) را در صورت عدم استفاده بپوشانید.

برای بچه‌های کوچک‌تر، از ابزارهایی نظیر برنامه‌های "کنترل والدین بر اینترنت" و "جستجوی امن" استفاده کنید، تا تجربیات آنلاین ایمنی داشته باشند.

## ۹-۵ جمع‌بندی

باتوجه‌به نفوذ وسائل ارتباط جمعی نظیر تلفن همراه، تبلت، کامپیوتر و اینترنت و نقش مؤثر این ابزار در پرکردن اوقات فراغت و تربیت و شکل‌گیری شخصیت کودکان و نوجوانان، موضوع حضور کودکان در این فضا و مواجهه با انواع بازی‌ها و سرگرمی‌ها در فضای مجازی یکی از دغدغه‌های والدین و مسئولان است.

یکی از راه‌های جلوگیری از مخاطرات فضای مجازی، برنامه‌ریزی، کنترل و نظارت بر استفاده و حضور فرزندان در فضای مجازی توسط والدین است؛

علاوه بر نکات ابتدایی (مثلاً دستگاه رایانه را در محلی قرار دهند که در معرض دید والدین باشد و از تنها گذاشتن کودک در این فضا حتی‌الامکان خودداری شود) که والدین باید آن را رعایت کنند، استفاده از برخی ابزارهای کنترلی در این فضا نیز ضروری است. این ابزارها کمک می‌کند که والدین هم بر فعالیت فرزندانشان فضای مجازی نظارت داشته باشند و هم گزارش فعالیت‌های آن‌ها را دریافت کرده و دسترسی فرزندانشان را کنترل و مدیریت کنند.

در این فصل ضمن بیان ضرورت رعایت نکات امنیتی توسط والدین در مواجهه با استفاده فرزندان از فضای مجازی به انواع آسیب‌های احتمالی اشاره شد و مهم‌ترین راهکارهای پیشنهادی برای والدین شرح داده شد.

# فصل ششم: جرایم رایانه ای و مباحث حقوقی

سؤالات مهم فصل ششم:

- ✓ تعریف جرائم رایانه‌ای چیست؟
- ✓ انواع جرائم رایانه‌ای کدام است؟
- ✓ نمونه‌هایی از مصادیق جرائم رایانه‌ای  چیست؟
- ✓ جرائم رایانه‌ای در ایران چه وضعیتی دارد؟
- ✓ برای  پیگیری یک جرم رایانه‌ای چگونه اقدام نماییم؟

### ۶-۱ مقدمه

امروزه با پیشرفت تکنولوژی و گسترش فضای مجازی شکل و ابزار ارتکاب جرم نیز تغییر کرده است. از سوی دیگر، نمی‌توان تأثیر استفاده از اینترنت و وسایل الکترونیکی از جمله رایانه و موبایل بر زندگی افراد را نادیده گرفت، به همین دلیل در سال‌های اخیر جرایم رایانه‌ای به‌مراتب افزایش پیدا کرده است. ازاین‌رو قانون‌گذار به‌منظور جلوگیری از ایجاد اختلال در این فضا، قوانینی را در این زمینه وضع کرده است. در ادامه به جزئیات بیشتر در این زمینه خواهیم پرداخت.

### ۶-۲ تعریف جرائم رایانه‌ای

برای توضیح جرائم رایانه‌ای باید دانست که با توسعه و پیشرفت تکنولوژی و نقش پررنگ آن در جوامع امروزی، این حوزه به‌صورت یک موضوع جدید و پرچالش تبدیل شده است. امروزه نمی‌توان تأثیر استفاده از اینترنت و وسایل الکترونیکی از جمله کامپیوترها و موبایل‌ها بر زندگی افراد نادیده گرفت. حضور افراد در فضای مجازی، ایجاد کسب‌وکار در این فضا، شکل‌گیری روابط اجتماعی در آن و همچنین انجام معاملات تجاری از طریق آن باعث شده است این فضا به‌عنوان یک محیط مجازی درآید که برخی از افراد از آن سودجویی می‌کنند. ازاین‌رو قانون‌گذار برای جلوگیری از ایجاد اختلال در این فضا و مشخص‌کردن قواعد استفاده‌کنندگان، قوانینی را در این زمینه وضع کرده است.

در یک تعریف هر فعل و یا ترک فعل غیرقانونی که یا به‌وسیله رایانه و یا با اخلال در سیستم‌های رایانه‌ای و یا نفوذ در سیستم‌های رایانه‌ای را گویند که به‌موجب قانون برای آن مجازات تعیین شده را جرم رایانه‌ای گویند.

تعریف دیگری که می‌توان ارائه کرده این است که هر جرمی که قانون‌گذار به‌صراحت رایانه را به منزله موضوع یا وسیله جرم جزء رکن مادی آن اعلام کرده باشد (آن رفتار یا عمل مجرمانه به‌وسیله رایانه یا در فضای رایانه اتفاق افتاده باشد).

در تعریف دیگر، جرم کامپیوتری صرفاً عبارت از جرایمی است که در فضای سایبر رخ می‌دهد از این نظر جرایمی مثل هرزه‌نگاری، افترا، آزار و اذیت و سوءاستفاده از پست الکترونیکی و سایر جرایمی که در آنها کامپیوتر به‌عنوان ابزار و وسیله ارتکاب جرم بکار گرفته می‌شود، در زمره جرم کامپیوتری قرار نمی‌گیرد. در تعریف گسترده‌تر از جرم کامپیوتری هر فعل و ترک فعلی که «در» یا «از طریق» یا «به کمک» از طریق اتصال به اینترنت، چه به طور مستقیم، یا به طور غیرمستقیم رخ می‌دهد و توسط قانون ممنوع گردیده و برای آن مجازات در نظر گرفته شده است جرم کامپیوتری نامیده می‌شود.

### ۳-۶ انواع جرائم یارانه‌ای

بنابراین، باتوجه‌به تعریف فوق جرایم رایانه‌ای را می‌توان به سه دسته تقسیم کرد:

اول: جرایمی که در آنها رایانه و تجهیزات جانبی آن موضوع جرم واقع می‌شود. مانند: سرقت، تخریب و....

دوم: جرایمی که در آنها رایانه به‌عنوان ابزار ارتکاب جرم به کار گرفته می‌شود که معمولاً از طریق شبکه‌های رایانه‌ای و اینترنت رخ می‌دهد. مثل کلاهبرداری، جعل و سرقت رایانه‌ای و ....

سوم: جرایمی که می‌توان آنها را جرایم سایبری نامید که در فضای مجازی به وقوع می‌پیوندد، اما آثار آنها در دنیای واقعی ظاهر می‌شود. مانند نفوذ غیرمجاز، شنود غیرمجاز، انتشار ویروس، کرم‌های رایانه‌ای و ...

### ۴-۶ کلاهبرداری رایانه‌ای

همان‌طور که از اسم کلاهبرداری رایانه‌ای پیداست، این جرم در محدوده‌ای فضای مجازی و اینترنت قابل ارتکاب است. از همین نکته یکی از تفاوت‌های مهم این جرم با کلاهبرداری معمول و سنتی مشخص می‌شود. کلاهبرداری سنتی باید در فضای واقعی رخ دهد و فرد، فریب کلاهبردار را بخورد و مالش را در اختیار کلاهبردار قرار دهد.

تفاوت کلاهبرداری اینترنتی با کلاهبرداری سنتی، در ارتکاب محیط این جرائم و همچنین در تفاوت وسایل ارتکاب جرم است. اما در کلاهبرداری رایانه‌ای، کلاهبردار از طریق فضای مجازی و با تغییر دادن داده‌ها و اطلاعات فرد، حتی بدون آگاهی بزه‌دیده، اموال وی را تصاحب می‌کند. مثلاً از طریق فضای مجازی در داده‌های حساب‌های بانکی افراد دست می‌برد و موجودی آن حساب‌ها را به‌حساب خود واریز می‌کند. این جرم در زمره جرایم علیه اموال و مالکیت است که عبارت است از: تحصیل مال غیر که با توسل به وسایل متقلبانه از طرف کلاهبردار ارتکاب می‌یابد.

در دنیای امروز مردم به‌جای پرداخت‌های نقدی از پرداخت‌های بانکی استفاده می‌کنند و همین هم باعث می‌شود تا بیش‌تر کلاهبرداری‌ها در این زمینه صورت گیرد. کلاهبرداری رایانه‌ای به روش‌های زیر می‌تواند انجام شود:

داده‌هایی که به رایانه داده می‌شود اشتباه باشد بیش‌تر موارد در کلاهبرداری‌ها نیز در همین حوزه است که فرد بزهکار از راه بیش‌تر کردن، فرستادن و یا تغییر اطلاعات به مکان دیگری مرتکب جرم شده است.

### ۵-۶ جاسوسی رایانه‌ای

یکی از انواع جرائم رایانه‌ای، جاسوسی رایانه‌ای است. در این جرم هدف برنامه‌های رایانه‌ای است. با پیشرفت تکنولوژی جاسوسی‌ها نیز جدیدتر می‌شوند. از روش‌های عمومی برای دست‌یابی به داده‌ها می‌توان فایل‌ها را کپی کرد زیرا در روش‌های قدیمی مثل رشوه دادن و این که فرد را برای انجام‌دادن کارهایی در مدت کوتاه فرستاده شود.

قانون جرائم رایانه‌ای ایران، مواد ۳،۴ و ۵ را به مباحث جاسوسی اختصاص داده است. ماده ۳ قانون جرائم رایانه‌ای بیان می‌دارد: هر شخصی به‌صورت غیرمجاز نسبت به اطلاعات مخفیانه در حال ارسال و دریافت یا ذخیره شده در سایت‌های رایانه‌ای یا مخابراتی کارهای زیر را انجام دهد مجازات‌های زیر برای او اعمال خواهد شد:

دست‌یافتن به داده‌ها و به‌دست‌آوردن آن‌ها و یا شنیدن محتواهای مخفیانه در زمان انتقال به یک تا سه سال حبس و مقدار بیست تا شصت میلیون جزای نقدی مجازات خواهد شد.

اگر داده‌ها در دسترس افرادی که صلاحیت ندارند قرار بگیرند آن گاه فرد به دو تا ده سال حبس محکوم  نمی شوند.

اگر داده‌ها و اطلاعات دولتی را در اختیار گروه های بیگانه قرار دهد فرد به پنج تا پانزده سال حبس محکوم خواهد شد.

ماده ۴ قانون جرائم رایانه‌ای امده است که هر شخصی که به داده‌های سری دست پیدا کند و سایر موارد امنیتی را زیر پا بگذارد آن ها به شش ماه تا دو سال حبس و جزای نقدی برابر ده تا چهل میلیون محکوم خواهد شد .

ماده ۵ قانون جرائم رایانه‌ای بیان نموده است که اطلاعاتی که در اختیار افراد دولتی قرار می گیرد و روش‌های حفاظت از داده‌ها نیز به آن ها اموزش داده می‌شود حال اگر این اطلاعات به‌خاطر بی احتیاطی در دسترس افرادی که صلاحیت ندارند قرار بگیرد فرد به میزان نود و یک روز تا دو سال حبس و پنج تا چهل میلیون ریال جزای نقدی محکوم خواهد شد. همچنین به میزان شش ماه تادو سال نیز از خدمت محروم خواهد بود.

### ۶-۶ سرقت نرم‌افزار

در ماده ۱۲ قانون جرائم رایانه و سرقت های رایانه‌ای بیان شده است که هر فردی که به‌صورت غیرمجاز داده‌های شخص دیگری را به سرقت ببرد و البته اصل اطلاعات در اختیار خود شخص باشد فرد یا به جزای نقدی برابر یک تا بیست میلیون ریال و یا به حبسی برابر نود و یک روز تا یک سال یا جزای نقدی از پانصد هزار تومان تا دو میلیون تومان یا هردو محکوم خواهد شد.

موارد گفته شده از تقسیم بندی کلی جرائم رایانه‌ای برگرفته شده است ،موارد دیگر آن شامل جعل رایانه‌ای ، ایجاد خسارت داده‌ها و یا برنامه‌های رایانه‌ای ،نفوذ کردن رایانه‌ای ،استراق السمع غیرمجاز و پورنوگرافی رایانه‌ای هستند.

## ۶-۷ مصادیق جرایم رایانه‌ای

مصادیق جرایم رایانه‌ای را می‌توان طبق قانون در موارد زیر دانست. در ادامه به برخی از آنها اشاره خواهیم کرد:

- دسترسی غیرمجاز به داده یا سامانه های رایانه‌ای و مخابراتی
- شنود غیرمجاز محتوای در حال انتقال ارتباطات غیر عمومی در سامانه های رایانه‌ای یا مخابراتی یا امواج مغناطیسی یا نوری
- جاسوسی یارانه‌ای
- جعل رایانه‌ای
- تخریب و اخلال در داده‌ها یا سامانه های رایانه‌ای و مخابراتی
- سرقت و کلاهبرداری مرتبط با رایانه
- جرایم علیه عفت و اخلاق عمومی
- هتک حیثیت و نشر اکاذیب
- تولید، انتشار یا در دسترس قراردادن یا معامله داده‌ها یا نرم‌افزارها یا هر نوع ابزار الکترونیکی
- فروش یا انتشار یا در دسترس قراردادن گذرواژه یا هر داده ای که امکان دسترسی غیرمجاز به داده‌ها یا سامانه های رایانه‌ای یا مخابراتی متعلق به دیگری را فراهم آورد

- انتشار یا در دسترس قراردادن محتویات آموزش دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای و تخریب و اخلال در داده‌ها یا سامانه های رایانه‌ای و مخابراتی

در برخی موارد به صراحت در این خصوص در قانون موردی مطرح نشده، ولی بر اساس تفسیر و رجوع به سایر قوانین، این عمل جرم محسوب می‌شود. مانند مورد ذیل:

بعنوان نمونه برای برخی از کاربران سوال پیش می آید که آیا استفاده از عکس پروفایل دیگران جرم است ؟

در پاسخ باید گفت باتوجه‌به اینکه بر اساس ماده ۱۶ قانون جرایم رایانه‌ای : هرکس به‌وسیله سامانه‌های رایانه‌ای یا مخابراتی، فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر یا تحریف منتشر کند، به نحوی که عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از پنج میلیون (۵,۰۰۰,۰۰۰) ریال تا چهل میلیون (۴۰,۰۰۰,۰۰۰) ریال یا هر دو مجازات محکوم خواهدشد.

تبصره ـ چنانچه تغییر یا تحریف به‌صورت مستهجن باشد، مرتکب به حداکثر هر دو مجازات مقرر محکوم خواهد شد.

(قانون جرایم رایانه‌ای مصوب ۱۳۸۸،۰۳،۰۵با اصلاحات و الحاقات بعدی)

با این شرایط سوءاستفاده از تصویر دیگری و قراردادن عکس شخصی دیگران روی پروفایل صفحه خود در فضای مجازی جرم است و در صورت شکایت شخص ، فرد خاطی به مجازات قانونی محکوم می‌شود.

## ۸-۶ جرایم رایانه‌ای در ایران

به گزارش پلیس فتای ناجا در سال ۱۳۹۹ برداشت غیرمجاز، ۴۹,۵ درصد از جرائم سایبری در کشور را به خود اختصاص داده است.

همچنین سرقت اطلاعات کارت های بانکی از جمله شماره کارت، رمز دوم، کد ۲cvv از طریق صفحات جعلی(فیشینگ)، "اسکمیر" (کپی کردن غیرقانونی داده‌های کارت بانکی)، سوءاستفاده از اعتماد افراد و دریافت کارت و رمز آن، روش‌های پیچیده مجرمان در فریب افراد و تکنیک‌های مهندسی اجتماعی از جمله شگردهای مجرمان است که به برداشت غیرمجاز منجر می‌شود.

کلاهبرداری‌های رایانه‌ای نیز جزو جرائمی است که بیشترین تعدد پرونده‌ها را بعد از برداشت‌های غیرمجاز داراست،

مزاحمت‌های اینترنتی و انتشار فیلم‌های خصوصی و دسترسی غیرمجاز به داده‌های رایانه‌ای نیز از جرائمی است که جزو پنج جرم در صدر محسوب می‌شود. بیشترین جرائم برداشت‌های اینترنتی غیرمجاز یا همان فیشینگ است.

۲۰ درصد مربوط به کپی کارت‌ها است و ۶۰ درصد از پرونده‌هایی که در پلیس فتا تشکیل می‌شود، مربوط به برداشت‌های غیرمجاز از حساب افراد است.

مزاحمت‌های اینترنتی نیز یکی از پنج جرم برتر حوزه پلیس فتا است و یکی از دغدغه‌های ما محسوب می‌شود. در خصوص مزاحمت‌های اینترنتی باید شکایت شاکی خصوصی باشد. این نوع از جرائم از نظر عدد کمتر از ۱۰ درصد کل جرائم اینترنتی را شامل می‌شود، اما همان‌طور که گفتم یکی از دغدغه‌ها ما در پلیس فتای تهران بزرگ است.

بیشترین موضوعات مربوط به دسترسی غیرمجاز به داده‌های رایانه‌ای در خصوص هک اینستاگرام و تلگرام است که مجرمان از طریق آن به داده‌های فرد دسترسی پیدا می‌کنند و در مواردی منجر به کلاهبرداری می‌شود. در موارد نادر نیز هک و نفوذ به داده‌های رایانه و گوشی تلفن همراه و هر وسیله دیگری که به اینترنت متصل می‌شود، صورت می گیرد.

هک وای فای: تعداد پرونده‌هایی که در این خصوص تشکیل می‌شود، بسیار اندک است البته هک اینترنت وای‌فای برای هر کسی محرز نمی‌شود و پلیس نیز تا قبل از شکایت مدعی نمی‌تواند در این زمینه اقدام کند و حتی از نظر فنی نیز قابل تشخیص نیست. شهروندان نیز چون اطلاعات کاملی در این خصوص ندارند و بر این حوزه مسلط نیستند، ممکن است اصلاً در جریان قرار نگیرند، البته تعدادی هم که متوجه می‌شوند به این موضوع اهمیت نمی‌دهند و اعلام شکایت نمی‌کنند، اما تا زمانی که شکایت نشود نه خدمات دهنده قادر به تشخیص هک وای‌فای است و نه پلیس.

## ۹-۶ راههای پیشگیری از جرایم

### ۱-۹-۶ تعریف پیشگیری از جرایم رایانه‌ای

منظور از پیشگیری از جرایم رایانه‌ای این است که کاربران بتوانند با انجام اقداماتی از جرایم رایانه‌ای محتمل و در کمین خود در امان باشند.

مجرمان رایانه‌ای می‌توانند با ارتکاب جرایم رایانه‌ای متداول مانند سرقت رایانه‌ای، کلاهبرداری رایانه‌ای، هک، فیشینگ، شنود غیرمجاز، دسترسی غیرمجاز و... امنیت کاربران را به خطر انداخته و صدمات مالی، اطلاعاتی و یا حیثیتی بسیاری به آنها بواسطه سرقت اطلاعات حساب بانکی یا رمز عبور آنها وارد کنند.

در ادامه چند توصیه مهم و کاربردی برای پیشگیری از جرایم رایانه‌ای به کاربران ارائه می‌کنیم.

### ۶-۹-۲ نرم‌افزارهای سیستم خود را آپدیت نگه دارید!

شرکت‌های سازنده نرم‌افزار و بازی‌های رایانه‌ای یا تلفن همراه، همواره از نظر امنیتی سیستم‌های خود را ارتقا می‌بخشند و با شناسایی حفره‌های امنیتی محصولات خود سعی در افزایش سطح امنیت کاربران دارند.

این اقدامات در قالب آپدیت‌های مختلفی به کاربران اطلاع‌رسانی می‌شود و هر کاربری با آپدیت نرم‌افزار خود می‌تواند از امنیت خود محافظت بیشتری کند.

موضوع آپدیت نگه‌داشتن نرم‌افزارها زمانی حساس‌تر می‌شود که محصولات مذکور در حوزه خدمات مالی و پولی مانند نرم‌افزارهای پرداخت آنلاین باشد.

آپدیت سیستم‌عامل (ویندوز، اندروید، آی او اس و...) نیز اهمیت بسیار زیادی در پیشگیری از جرایم رایانه‌ای دارد.

### ۶-۹-۳ از آنتی‌ویروس‌های معتبر برای پیشگیری از جرایم رایانه‌ای استفاده کنید!

استفاده از آنتی‌ویروس‌های معتبر نقش مهمی در پیشگیری از جرایم رایانه‌ای دارند. کاربران می‌توانند انواع آنتی ویروس‌های رایگان یا غیررایگان را برای سیستم‌عامل‌های خود نصب کنند و حفاظت سیستم خود را تا چند درجه بیشتر کنند.

آنتی‌ویروس‌ها قادر هستند تا فعالیت‌های مشکوک سایبری علیه کاربران را شناسایی و دفع کنند. هر کاربری می‌تواند باتوجه‌به نیاز فنی خود آنتی ویروس شناخته‌شده‌ای را انتخاب و از مزایای آن در جهت پیشگیری از جرایم رایانه‌ای بهره‌مند شود.

### ۴-۹-۶ از رمز عبور غیرقابل‌پیش‌بینی استفاده کنید

مجرمان سایبری از رمزعبورهای ساده نهایت استفاده را می‌کنند. زمانی که کاربر رمز عبور قدرتمند و متنوعی استفاده کند، پیش‌بینی رمز عبور و یا به دست آوردن الگوریتم آن برای مجرمان به شدت دشوار می‌شود.

به همین خاطر برای پیشگیری از جرایم رایانه‌ای سعی کنید رمز عبوری طولانی و متشکل از حروف کوچک و بزرگ، نمادها و اعداد انتخاب کنید.

همچنین تلاش کنید که هر رمز عبور را صرفا برای یک سایت یا نرم‌افزار به کار ببرید و رمز عبورهای تکراری نداشته باشید.

مطابق آمار، آسیب‌پذیرترین رمزعبورها برای سوءاستفاده مجرمان اینترنتی، اسامی اشخاص، اعداد یا حروف پشت سر هم و تاریخ‌های تولد و شماره‌های هویتی (مثل کد ملی) هستند.

### ۶-۹-۵ تاییدات چندمرحله‌ای را فعال کنید

در حال حاضر، نرم‌افزارهای زیادی تاییدات چندمرحله‌ای را پوشش می‌دهند. منظور از تأیید چندمرحله‌ای یا دومرحله‌ای، این است که برای افزایش امنیت استفاده از سایت‌ها و نرم‌افزارهای خاص، کاربران می‌توانند علاوه بر استفاده از نام کاربری و رمز عبور معمول، مرحله دیگری نیز بر فرایند تأیید ورود خود اضافه کنند.

مثلاً برای برخی پیام‌رسان‌ها می‌توان علاوه بر ورود با رمز عبور، مرحله دومی مبنی بر ارسال کد به شکل پیامک یا ایمیل را هم فعال کرد و دسترسی مجرمان اینترنتی را به‌حساب کاربری کاملاً مسدود کرد.

استفاده از ورود دومرحله‌ای در استفاده از نرم‌افزارها، در حال حاضر یکی از موثرترین روش‌های پیشگیری از جرایم رایانه‌ای به حساب می‌آید.

### ۶-۹-۶ تهیه نسخه پشتیبان را جدی بگیرید

علاوه بر تدابیر بالا، همواره به یاد داشته باشید که تهیه نسخه پشتیبان یا بکاپ[۶۹] از اطلاعات اهمیتی اساسی دارد.

---

[۶۹] BackUp

تهیه نسخه پشتیبان غالبا در مواردی اهمیت پیدا می‌کند که مربوط به فایل‌های حساس و مهم مانند، فایل‌های آکادمیک (پایان‌نامه، کتاب‌ها و...)، اطلاعات شغلی یا حتی تصاویر و فیلم‌های خاطره‌انگیز باشد.

پیشگیری از جرایم رایانه‌ای با بکاپ گرفتن از اطلاعات می‌تواند در قالب کپی فایل‌ها در یک هارد اکسترنال یا فلش مموری باشد و یا در فضاهای ابری انجام شود.

### ۶-۹-۷ فایل‌های مشکوک را باز نکنید

یکی از راه‌هایی که مجرمان اینترنتی مانند هکرها، از آن برای نفوذ به اطلاعات کاربران استفاده می‌کنند، ارسال لینک‌ها و فایل‌های ویروسی و ناامن به افراد است.

ممکن است این لینک‌ها و فایل‌ها در قالب ایمیل، پیام در شبکه‌های اجتماعی یا پیام‌رسان‌ها و یا حتی به‌صورت پیامک به دست کاربران برسد.

در چنین وضعیتی یک کاربر ناآگاه می‌تواند با بازکردن لینک یا دانلود فایل مورد نظر، سیستم خود را در معرض خطرات زیادی مانند سرقت اطلاعات یا دسترسی به فایل‌ها قرار دهد.

بنابراین برای پیشگیری از جرایم رایانه‌ای نسبت به فایل‌ها و لینک‌های مشکوک و ناشناس، محتاط باشید.

### ۸-۹-۶ مراقب وای‌فای عمومی باشید

بسیاری از شرکت‌ها، رستوران‌ها، فروشگاه‌ها، مراکز علمی، مراکز تفریحی مانند پاساژها، فرودگاه‌ها، هتل‌ها و... ممکن است خدمات وای‌فای رایگان به مشتریان و راجعان خود ارائه کنند. اگر چه وصل شدن به اینترنت رایگان می‌تواند جذاب باشد اما نباید فراموش کنید که وای‌فای‌های عمومی بسترهای مطلوبی برای سوءاستفاده مجرمان اینترنتی به‌حساب می‌آیند.

به همین خاطر اولاً تا جای ممکن از اینترنت عمومی استفاده نکنید و ثانیاً اطلاعات حساس خود را بر بستر وای‌فای عمومی مبادله نکنید.

## ۱۰-۶ راه‌های پیگیری و استفاده از حمایت قانونی

اگر از طریق دنیای مجازی قربانی جرم قرار گرفته‌اید می‌توانید توسط اشخاص ذیل و به طرقی که گفته می‌شود شکایت خود را مطرح و درخواست پیگیری نمایید:

۱- دادستان کل کشور

۲- دادسرای جرایم رایانه‌ای

۳- پلیس فتا

نحوه طرح شکایت

اولین راه قانونی مراجعه به دادسرای جرائم رایانه‌ای در طریق دفاتر پیشخوان قضایی است و یا مراجعه به سایت پلیس فضای تولید و تبادل اطلاعات (فتا) و همچنین مراجعه به سایت دادستان کل کشور

در طرح شکایت کیفری در جرائم رایانه‌ای دو حالت متصور است:

یا ممکن است شما به شخصی مظنون باشید و او را به‌عنوان مجرم معرفی کنید تا از طریق دادسرا احضار شود و یا ممکن است طرف مقابل برای شما قابل شناسایی نباشد؛ مثل زمانی که مبلغی را به سایتی برای خرید کالایی واریز می‌کنید بدون آنکه بدانید فروشنده چه کسی است.

در این حالت پلیس با بررسی‌های تخصصی خود می‌تواند گره‌گشای این مشکل باشد.

### ۱-۱۰-۶ مراحل اداری طرح دعوی کیفری جرم رایانه‌ای

مراجعه به دادسرای جرائم رایانه‌ای:

اگر در فضای اینترنت در صورت خرید اینترنتی از حساب شما برداشت‌های غیرمجاز شده است یا مورد کلاهبرداری یا سودجویی‌های اینترنتی قرار گرفته‌اید؛ می‌توانید به دادسرای ناحیه ۳۱ استان تهران ویژه رسیدگی به جرائم رایانه‌ای و فناوری اطلاعات مراجعه و طرح شکایت کنید.

این دادسرا در تهران و چند شهر محدود مثل مشهد یا شیراز وجود دارد و در صورت نبود دادسرای رسیدگی به جرائم به دادسرای عمومی انقلاب یا پلیس فتا رجوع کنید.

بنابراین اگر شکایت خصوصی از پایگاه اینترنتی به لحاظ انتشار تصاویر خصوصی، اهانت، نشر اکاذیب، کلاهبرداری، و غیره متضرر شده‌اید باید برای شکایت کتبی به دادسرا مراجعه کنید؛ شما می‌توانید شکواییه موردنظر خود را در بخش تنظیم شکواییه سایت حقوقی بنیاد وکلا جستجو و دانلود کنید یا در صورت نیاز درخواست دهید تا توسط متخصص این امر برای شما به‌صورت اختصاصی تنظیم شود

**مراجعه به سایت پلیس فضای تولید و تبادل اطلاعات:**

در صورت ارتکاب جرم به سایت اینترنتی پلیس فضای تولید و تبادل اطلاعات (فتا) مراجعه و برای ثبت گزارش در سایت مربوطه ابتدا ثبت‌نام نمایید و سپس از آن در صفحه اصلی روی آیکن ارتباط مردمی کلیک کنید و مشخصات و شماره‌تلفن و آدرس سایت یا شبکه اجتماعی ارتکاب جرم و یا عکس آن را بارگذاری کنید و پلیس فتا در کمترین زمان با شما تماس و موضوع را پیگیری خواهد کرد.

البته ثبت شکایت با ثبت گزارش متفاوت است و پلیس اجراکننده احکام قضایی است.

بنابراین پلیس فتا و یا ضابطین بدون دستور قضایی نمی‌توانند جرمی را پیگیری نمایند؛ پس اگر قبل از مراجعه به دادسرا به سایت اینترنتی پلیس فضای تولید و تبادل اطلاعات (فتا) www.cyberpolice.ir رجوع کردید و مراحل ثبت‌نام و مدارک جرم را ثبت نمودید، باید برای پیگیری‌های بعدی به دادسرا مراجعه نمایید.

صلاحیت رسیدگی به جرائم کلاهبرداری‌های اینترنتی، جعل داده‌ها و عناوین، سرقت اطلاعات، تجاوز به حریم خصوصی اشخاص و گروه‌ها، هک و نفوذ به سامانه‌های رایانه‌ای و اینترنتی، جرائم اخلاقی و برخی جرائم سازمان‌یافته اقتصادی، اجتماعی و فرهنگی از وظایف فتا برای رسیدگی به آنها است.

**دادستان کل کشور:**

یکی از کارگروه‌های دادستانی، کارگروه تعیین مصادیق محتوای مجرمانه است که مسئولیت نظارت بر فضای مجازی و پالایش تارنماهای حاوی محتوای مجرمانه و رسیدگی به شکایات مردمی را به عهده دارد.

دادستان کل کشور، رئیس کارگروه تعیین مصادیق محتوای مجرمانه و قانون جرائم رایانه‌ای نیز است.

دادستان کل کشور به‌صورت تخصصی در جرائم رایانه‌ای فعالیتی ندارد ولی سایت‌های قمار و فیلترینگ را شناسایی می‌کنند؛ بنابراین می‌توانید در سایت دادستان کل کشور در قسمت گزارش‌های مردمی وارد شوید و در قسمت فضای مجازی تخلف را اعلام نمایید.

**پیوست شماره ۱ قانون جرایم رایانه‌ای**

قانون جرایم رایانه‌ای مصوب ۱۳۸۸،۰۳،۰۵با اصلاحات و الحاقات بعدی

بخش یکم ـ جرایم و مجازات‌ها

فصل یکم ـ جرایم علیه محرمانگی داده‌ها و سامانه‌های رایانه‌ای و مخابراتی

مبحث یکم ـ دسترسی غیرمجاز

ماده۱- هر کس به طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی که به‌وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از ۰۰۰ /۰۰۰ /۲۰ تا ۰۰۰ /۰۰۰ /۸۰ ریال یا هر دو مجازات محکوم خواهد شد.

مبحث دوم ـ شنود غیرمجاز

ماده۲- هر کس به طور غیرمجاز محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی یا امواج الکترومغناطیسی یا نوری را شنود کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ۰۰۰ /۰۰۰ /۲۵ تا ۰۰۰ /۰۰۰ /۱۵۰ ریال یا هر دو مجازات محکوم خواهد شد.

مبحث سوم ـ جاسوسی رایانه‌ای

ماده۳- هرکس به طور غیرمجاز نسبت به داده‌های سری در حال انتقال یا ذخیره شده در سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به مجازات‌های مقرر محکوم خواهد شد:

الف) دسترسی به داده‌های مذکور یا تحصیل آنها یا شنود محتوای سری در حال انتقال، به حبس از یک تا سه سال یا جزای نقدی از ۶۰/ ۰۰۰ /۰۰۰ تا ۱۸۰/ ۰۰۰ /۰۰۰ ریال یا هر دو مجازات.

ب) در دسترس قراردادن داده های مذکور برای اشخاص فاقد صلاحیت، به حبس از دو تا ده سال.

ج) افشاء یا در دسترس قراردادن داده‌های مذکور برای دولت، سازمان، شرکت یا گروه بیگانه یا عاملان آنها، به حبس از پنج تا پانزده سال.

تبصره۱- داده‌های سری داده هایی است که افشای آنها به امنیت کشور یا منافع ملی لطمه می زند.

تبصره۲- آئین نامه نحوه تعیین و تشخیص داده‌های سری و نحوه طبقه بندی و حفاظت آنها ظرف سه ماه از تاریخ تصویب این قانون توسط وزارت اطلاعات با همکاری وزارتخانه های دادگستری، کشور، ارتباطات و فناوری اطلاعات و دفاع و پشتیبانی نیروهای مسلح تهیه و به تصویب هیأت وزیران خواهد رسید.

ماده۴- هر کس به قصد دسترسی به داده‌های سری موضوع ماده (۳) این قانون، تدابیر امنیتی سامانه های رایانه ای یا مخابراتی را نقض کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ۲۵/ ۰۰۰ /۰۰۰ تا ۱۵۰/ ۰۰۰ /۰۰۰ ریال یا هر دو مجازات محکوم خواهد شد.

ماده۵- چنانچه مأموران دولتی که مسؤول حفظ داده‌های سری مقرر در ماده (۳) این قانون یا سامانه های مربوط هستند و به آنها آموزش لازم داده شده است یا داده‌ها یا سامانه‌های مذکور در اختیار آنها قرار گرفته است بر اثر بی احتیاطی، بی مبالاتی یا عدم رعایت تدابیر امنیتی موجب دسترسی اشخاص فاقد صلاحیت به داده‌ها، حامل های داده یا سامانه‌های مذکور شوند، به حبس از نود و یک روز تا دو سال یا جزای نقدی از ۱۵/ ۰۰۰ /۰۰۰ تا ۱۰۰/ ۰۰۰ /۰۰۰ ریال یا هر دو مجازات و انفصال از خدمت از شش ماه تا دو سال محکوم خواهند شد.

فصل دوم ـ جرائم علیه صحت وتمامیت داده‌ها و سامانه‌های رایانه‌ای و مخابراتی

مبحث یکم ـ جعل رایانه‌ای

ماده۶- هر کس به طور غیرمجاز مرتکب اعمال زیر شود، جاعل محسوب و به حبس از یک تا پنج سال یا جزای نقدی از ۰۰۰ /۰۰۰ /۵۰ تا ۰۰۰ /۰۰۰ /۲۵۰ ریال یا هر دو مجازات محکوم خواهد شد:

الف) تغییر یا ایجاد داده‌های قابل استناد یا ایجاد یا وارد کردن متقلبانهٔ داده به آنها.

ب) تغییر داده‌ها یا علائم موجود در کارتهای حافظه یا قابل پردازش در سامانه‌های رایانه ای یا مخابراتی یا تراشه ها یا ایجاد یا وارد کردن متقلبانهٔ داده‌ها یا علائم به آنها.

ماده۷- هر کس با علم به مجعول بودن داده ها یا کارتها یا تراشه ها از آنها استفاده کند، به مجازات مندرج در ماده فوق محکوم خواهد شد.

مبحث دوم ـ تخریب و اخلال در داده‌ها یا سامانه های رایانه ای و مخابراتی

ماده۸- هر کس به طور غیرمجاز داده‌های دیگری را از سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده حذف یا تخریب یا مختل یا غیر قابل پردازش کند به حبس از شش ماه تا دو سال یا جزای نقدی از بیست و پنج میلیون (۰۰۰ /۰۰۰ /۲۵) ریال تا صد میلیون (۰۰۰ /۰۰۰ /۱۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

ماده۹- هر کس به طور غیرمجاز با اعمالی از قبیل وارد کردن، انتقال دادن، پخش، حذف کردن، متوقف کردن، دستکاری یا تخریب داده ها یا امواج الکترومغناطیسی یا نوری، سامانه‌های رایانه‌ای یا مخابراتی دیگری را از کار بیندازد یا کارکرد آنها را مختل کند، به حبس از شش ماه تا دو سال یا جزای نقدی از ۱۰۰/ ۰۰۰/ ۰۰۰ تا ۲۵/ ۰۰۰/ ۰۰۰ ریال یا هر دو مجازات محکوم خواهد شد.

ماده۱۰- هر کس به طور غیرمجاز با اعمالی از قبیل مخفی کردن داده‌ها، تغییر گذرواژه یا رمزنگاری داده‌ها مانع دسترسی اشخاص مجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی شود، به حبس از نود و یک روز تا یک سال یا جزای نقدی از ۲۰/ ۰۰۰/ ۰۰۰ تا ۸۰/ ۰۰۰/ ۰۰۰ ریال یا هردو مجازات محکوم خواهد شد.

ماده۱۱- هر کس به قصد به خطر انداختن امنیت، آسایش و امنیت عمومی اعمال مذکور در مواد (۸)، (۹) و (۱۰) این قانون را علیه سامانه‌های رایانه‌ای و مخابراتی که برای ارائه خدمات ضروری عمومی به کار می روند، از قبیل خدمات درمانی، آب، برق، گاز، مخابرات، حمل و نقل و بانکداری مرتکب شود، به حبس از سه تا ده سال محکوم خواهد شد.

فصل سوم ـ سرقت و کلاهبرداری مرتبط با رایانه

ماده۱۲- هر کس به طور غیرمجاز داده‌های متعلق به دیگری را برباید، چنانچه عین داده‌ها در اختیار صاحب آن باشد، به جزای نقدی از ۶/ ۰۰۰/ ۰۰۰ تا ۵۰/ ۰۰۰/ ۰۰۰ ریال و در غیر این صورت به حبس از نود و یک روز تا یک سال یا جزای نقدی از ۲۰/ ۰۰۰/ ۰۰۰ تا ۸۰/ ۰۰۰/ ۰۰۰ ریال یا هر دو مجازات محکوم خواهد شد.

ماده۱۳- هر کس به طور غیرمجاز از سامانه‌های رایانه‌ای یا مخابراتی با ارتکاب اعمالی از قبیل وارد کردن، تغییر، محو، ایجاد یا متوقف کردن داده‌ها یا مختل کردن سامانه، وجه یا مال یا منفعت یا خدمات یا

امتیازات مالی برای خود یا دیگری تحصیل کند علاوه بر رد مال به صاحب آن به حبس از یک تا پنج سال یا جزای نقدی از ۵۰/۰۰۰/۰۰۰ تا ۲۵۰/۰۰۰/۰۰۰ ریال یا هر دو مجازات محکوم خواهد شد.

فصل چهارم ـ جرائم علیه عفت و اخلاق عمومی

ماده۱۴- هر کس به‌وسیله سامانه‌های رایانه‌ای یا مخابراتی یا حامل‌های داده محتویات مستهجن را منتشر، توزیع یا معامله کند یا به قصد تجارت یا افساد تولید یا ذخیره یا نگهداری کند، به حبس از نود و یک روز تا دو سال یا جزای نقدی از ۱۵/۰۰۰/۰۰۰ تا ۱۰۰/۰۰۰/۰۰۰ ریال یا هر دو مجازات محکوم خواهد شد.

تبصره۱- ارتکاب اعمال فوق در خصوص محتویات مبتذل موجب محکومیت به حداقل یکی از مجازاتهای فوق می‌شود.
محتویات و آثار مبتذل به آثاری اطلاق می گردد که دارای صحنه ها و صور قبیحه باشد.

تبصره۲- هرگاه محتویات مستهجن به کمتر از ده نفر ارسال شود، مرتکب به ۵/۰۰۰/۰۰۰ تا ۲۰/۰۰۰/۰۰۰ ریال جزای نقدی محکوم خواهد شد.

تبصره۳- چنانچه مرتکب اعمال مذکور در این ماده را حرفهٔ خود قرار داده باشد یا به طور سازمان یافته مرتکب شود چنانچه مفسد فی الارض شناخته نشود، به حداکثر هر دو مجازات مقرر در این ماده محکوم خواهد شد.

تبصره۴- محتویات مستهجن به تصویر، صوت یا متن واقعی یا غیرواقعی یا متنی اطلاق می شود که بیانگر برهنگی کامل زن یا مرد یا اندام تناسلی یا آمیزش یا عمل جنسی انسان است.

ماده۱۵- هر کس از طریق سامانه های رایانه‌ای یا مخابراتی یا حامل‌های داده مرتکب اعمال زیر شود، به ترتیب زیر مجازات خواهد شد:

الف) چنانچه به‌منظور دستیابی افراد به محتویات مستهجن، آنها را تحریک، ترغیب، تهدید یا تطمیع کند یا فریب دهد یا شیوه دستیابی به آنها را تسهیل نموده یا آموزش دهد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از ۰۰۰ /۰۰۰ /۲۰ تا ۰۰۰ /۰۰۰ /۸۰ ریال یا هر دو مجازات محکوم خواهد شد. ارتکاب این اعمال در خصوص محتویات مبتذل موجب جزای نقدی از ۰۰۰ /۰۰۰ /۵ تا ۰۰۰ /۰۰۰ /۲۰ ریال است.

ب) چنانچه افراد را به ارتکاب جرائم منافی عفت یا استعمال مواد مخدر یا روان گردان یا خودکشی یا انحرافات جنسی یا اعمال خشونت آمیز تحریک یا ترغیب یا تهدید یا دعوت کرده یا فریب دهد یا شیوه ارتکاب یا استعمال آنها را تسهیل کند یا آموزش دهد، به حبس از نود و یک روز تا یک سال یا جزای نقدی از ۰۰۰ /۰۰۰ /۲۰ تا ۰۰۰ /۰۰۰ /۸۰ ریال یا هر دو مجازات محکوم می‌شود.

تبصره ـ مفاد این ماده و ماده (۱۴) شامل آن دسته از محتویاتی نخواهد شد که برای مقاصد علمی یا هر مصلحت عقلایی دیگر تهیه یا تولید یا نگهداری یا ارائه یا توزیع یا انتشار یا معامله می‌شود.

فصل پنجم ـ هتک حیثیت و نشر اکاذیب

ماده۱۶- هرکس به‌وسیله سامانه‌های رایانه‌ای یا مخابراتی، فیلم یا صوت یا تصویر دیگری را تغییر دهد یا تحریف کند و آن را منتشر یا با علم به تغییر یا تحریف منتشر کند، به نحوی که عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از ۰۰۰ /۰۰۰ /۱۵ تا ۰۰۰ /۰۰۰ /۱۰۰ ریال یا هر دو مجازات محکوم خواهد شد.

تبصره ـ چنانچه تغییر یا تحریف به‌صورت مستهجن باشد، مرتکب به حداکثر هر دو مجازات مقرر محکوم خواهد شد.

ماده۱۷- هر کس به‌وسیله سامانه‌های رایانه‌ای یا مخابراتی صوت یا تصویر یا فیلم خصوصی یا خانوادگی یا اسرار دیگری را بدون رضایت او جز در موارد قانونی منتشر کند یا در دسترس دیگران قرار دهد، به نحوی که منجر به ضرر یا عرفاً موجب هتک حیثیت او شود، به حبس از نود و یک روز تا دو سال یا جزای نقدی از ۰۰۰ /۰۰۰ /۲۰ تا ۰۰۰ /۰۰۰ /۱۵۰ ریال یا هر دو مجازات محکوم خواهد شد.

ماده۱۸- هر کس به قصد اضرار به غیر یا تشویش اذهان عمومی یا مقامات رسمی به‌وسیله سامانه رایانه‌ای یا مخابراتی اکاذیبی را منتشر نماید یا در دسترس دیگران قرار دهد یا با همان مقاصد اعمالی را بر خلاف حقیقت، رأساً یا به‌عنوان نقل قول، به شخص حقیقی یا حقوقی به طور صریح یا تلویحی نسبت دهد، اعم از اینکه از طریق یاد شده به نحوی از انحاء ضرر مادی یا معنوی به دیگری وارد شود یا نشود، افزون بر اعاده حیثیت (در صورت امکان)، به حبس از نود و یک روز تا دو سال یا جزای نقدی از ۰۰۰ /۰۰۰ /۲۰ تا ۰۰۰ /۰۰۰ /۱۵۰ ریال یا هر دو مجازات محکوم خواهد شد.

فصل ششم ـ مسؤولیت کیفری اشخاص

ماده ۱۹- در موارد زیر، چنانچه جرائم رایانه‌ای به نام شخص حقوقی و در راستای منافع آن ارتکاب یابد، شخص حقوقی دارای مسؤولیت کیفری خواهد بود:

الف) هرگاه مدیر شخص حقوقی مرتکب جرم رایانه‌ای شود.

ب) هرگاه مدیر شخص حقوقی دستور ارتکاب جرم رایانه‌ای را صادر کند و جرم به وقوع بپیوندد.

ج) هرگاه یکی از کارمندان شخص حقوقی با اطلاع مدیر یا در اثر عدم نظارت وی مرتکب جرم رایانه‌ای شود.

د) هرگاه تمام یا قسمتی از فعالیت شخص حقوقی به ارتکاب جرم رایانه‌ای اختصاص یافته باشد.

تبصره۱- منظور از مدیر کسی است که اختیار نمایندگی یا تصمیم گیری یا نظارت بر شخص حقوقی را دارد.

تبصره۲- مسؤولیت کیفری شخص حقوقی مانع مجازات مرتکب نخواهد بود و در صورت نبود شرایط صدر ماده و عدم انتساب جرم به شخص خصوصی فقط شخص حقیقی مسؤول خواهد بود.

ماده۲۰- اشخاص حقوقی موضوع ماده فوق، باتوجه‌به شرایط و اوضاع و احوال جرم ارتکابی، میزان درآمد و نتایج حاصله از ارتکاب جرم، علاوه بر سه تا شش برابر حداکثر جزای نقدی جرم ارتکابی، به ترتیب ذیل محکوم خواهند شد:

الف) چنانچه حداکثر مجازات حبس آن جرم تا پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا نُه ماه و در صورت تکرار جرم تعطیلی موقت شخص حقوقی از یک تا پنج سال.

ب) چنانچه حداکثر مجازات حبس آن جرم بیش از پنج سال حبس باشد، تعطیلی موقت شخص حقوقی از یک تا سه سال و در صورت تکرار جرم، شخص حقوقی منحل خواهد شد.

تبصره ـ مدیر شخص حقوقی که طبق بند «ب» این ماده منحل می شود، تا سه سال حق تأسیس یا نمایندگی یا تصمیم گیری یا نظارت بر شخص حقوقی دیگری را نخواهد داشت.

ماده۲۱- ارائه‌دهندگان خدمات دسترسی موظفند طبق ضوابط فنی و فهرست مقرر از سوی کارگروه(کمیته) تعیین مصادیق موضوع ماده ذیل محتوای مجرمانه که در چهارچوب قانون تنظیم شده است اعم از محتوای ناشی از جرایم رایانه‌ای و محتوایی که برای ارتکاب جرائم رایانه‌ای به کار می رود را پالایش (فیلتر) کنند. در صورتی که عمداً از پالایش(فیلتر) محتوای مجرمانه خودداری کنند، منحل خواهند شد و چنانچه از روی بی‌احتیاطی و بی‌مبالاتی زمینهٔ دسترسی به محتوای غیرقانونی را فراهم آورند، در مرتبهٔ نخست به جزای نقدی از ۶۰/ ۰۰۰/ ۰۰۰ تا ۲۵۰/ ۰۰۰/ ۰۰۰ ریال و در مرتبهٔ دوم به

جزای نقدی از یکصد میلیون (۱۰۰,۰۰۰,۰۰۰)ریال تا یک میلیارد (۱,۰۰۰,۰۰۰,۰۰۰)ریال و در مرتبهٔ سوم به یک تا سه سال تعطیلی موقت محکوم خواهند شد.

تبصره۱- چنانچه محتوای مجرمانه به کارنماهای (وب‌سایتهای) مؤسسات عمومی شامل نهادهای زیر نظر ولی فقیه و قوای سه گانهٔ مقننه، مجریه و قضائیه و مؤسسات عمومی غیردولتی موضوع قانون فهرست نهادها و مؤسسات عمومی غیردولتی مصوب ۱۹ /۴ /۱۳۷۳ و الحاقات بعدی آن یا به احزاب، جمعیتها، انجمن های سیاسی و صنفی و انجمن های اسلامی یا اقلیتهای دینی شناخته شده یا به سایر اشخاص حقیقی یا حقوقی حاضر در ایران که امکان احراز هویت و ارتباط با آنها وجود دارد تعلق داشته باشد، با دستور مقام قضائی رسیدگی کننده به پرونده و رفع اثر فوری محتوای مجرمانه از سوی دارندگان، تارنما (وب‌سایت) مزبور تا صدور حکم نهایی پالایش (فیلتر) نخواهد شد.

تبصره۲- پالایش (فیلتر) محتوای مجرمانه موضوع شکایت خصوصی با دستور مقام قضائی رسیدگی کننده به پرونده انجام خواهد گرفت.

ماده۲۲- قوهٔ قضائیه موظف است ظرف یک ماه از تاریخ تصویب این قانون کارگروه(کمیته)تعیین مصادیق محتوای مجرمانه را در محل دادستانی کل کشور تشکیل دهد. وزیر یا نمایندهٔ وزارتخانه‌های آموزش و پرورش، ارتباطات و فناوری اطلاعات، اطلاعات، دادگستری، علوم، تحقیقات و فناوری، فرهنگ و ارشاد اسلامی، رئیس سازمان تبلیغات اسلامی، رئیس سازمان صدا و سیما و فرمانده نیروی انتظامی، یک نفر خبره در فناوری اطلاعات و ارتباطات به انتخاب کمیسیون صنایع و معادن مجلس شورای اسلامی و یک نفر از نمایندگان عضو کمیسیون قضائی و حقوقی به انتخاب کمیسیون قضائی و حقوقی و تأیید مجلس شورای اسلامی اعضای کارگروه(کمیته) را تشکیل خواهند داد. ریاست کارگروه(کمیته) به عهدهٔ دادستان کل کشور خواهد بود.

تبصره۱- جلسات کارگروه (کمیته) حداقل هر پانزده روز یک بار و با حضور هفت نفر عضو رسمیت می یابد وتصمیمات کارگروه (کمیته) با اکثریت نسبی حاضران معتبر خواهد بود.

تبصره ۲-کارگروه (کمیته) موظف است به شکایات راجع به مصادیق پالایش (فیلتر) شده رسیدگی و نسبت به آنها تصمیم گیری کند.

تبصره۳-کارگروه (کمیته) موظف است هر شش ماه گزارشی در خصوص روند پالایش (فیلتر) محتوای مجرمانه را به رؤسای قوای سه گانه و شورای عالی امنیت ملی تقدیم کند.

ماده ۲۳- ارائه دهندگان خدمات میزبانی موظفند به‌محض دریافت دستور کارگروه(کمیته) تعیین مصادیق مذکور در مادهٔ فوق یا مقام قضائی رسیدگی کننده به پرونده مبنی بر وجود محتوای مجرمانه در سامانه‌های رایانه‌ای خود از ادامهٔ دسترسی به آن ممانعت به عمل آورند.

چنانچه عمداً از اجرای دستور کارگروه(کمیته) یا مقام قضائی خودداری کنند، منحل خواهند شد. در غیر این صورت، چنانچه در اثر بی احتیاطی و بی مبالاتی زمینهٔ دسترسی به محتوای مجرمانه مزبور را فراهم کنند، در مرتبهٔ نخست به جزای نقدی از ۶۰/ ۰۰۰/ ۰۰۰ تا ۲۵۰/ ۰۰۰/ ۰۰۰ ریال و در مرتبهٔ دوم به یکصد میلیون(۱۰۰,۰۰۰,۰۰۰)ریال تا یک میلیارد(۱,۰۰۰,۰۰۰,۰۰۰)ریال و در مرتبهٔ سوم به یک تا سه سال تعطیلی موقت محکوم خواهند شد.

تبصره ـ ارائه دهندگان خدمات میزبانی موظفند به‌محض آگاهی از وجود محتوای مجرمانه مراتب را به کارگروه (کمیته) تعیین مصادیق اطلاع دهند.

ماده ۲۴- هر کس بدون مجوز قانونی از پهنای باند بین المللی برای برقراری ارتباطات مخابراتی مبتنی بر پروتکل اینترنتی از خارج ایران به داخل یا برعکس استفاده کند، به حبس از یک تا سه سال یا جزای نقدی از یکصد میلیون (۱۰۰/ ۰۰۰/ ۰۰۰) ریال تا یک میلیارد (۱/ ۰۰۰/ ۰۰۰/ ۰۰۰) ریال یا هر دو مجازات محکوم خواهد شد.

فصل هفتم ـ سایر جرائم

ماده ۲۵- هر شخصی که مرتکب اعمال زیر شود، به حبس از نود و یک روز تا یک سال یا جزای نقدی از ۲۰/ ۰۰۰/ ۰۰۰ تا ۸۰/ ۰۰۰/ ۰۰۰ ریال یا هر دو مجازات محکوم خواهد شد:

الف) تولید یا انتشار یا توزیع و در دسترس قراردادن یا معاملهٔ داده‌ها یا نرم افزارها یا هر نوع ابزار الکترونیکی که صرفاً به‌منظور ارتکاب جرائم رایانه‌ای به کار می رود.

ب) فروش یا انتشار یا در دسترس قراردادن گذرواژه یا هر داده ای که امکان دسترسی غیرمجاز به داده ها یا سامانه های رایانه‌ای یا مخابراتی متعلق به دیگری را بدون رضایت او فراهم می‌کند.

ج) انتشار یا در دسترس قراردادن محتویات آموزش دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای و تخریب و اخلال در داده‌ها یا سیستم های رایانه‌ای و مخابراتی.

تبصره ـ چنانچه مرتکب، اعمال یاد شده را حرفه خود قرار داده باشد، به حداکثر هر دو مجازات مقرر در این ماده محکوم خواهد شد.

فصل هشتم ـ تشدید مجازات ها

ماده ۲۶- در موارد زیر، حسب مورد مرتکب به بیش از دوسوم حداکثر یک یا دو مجازات مقرر محکوم خواهد شد:

الف) هر یک از کارمندان و کارکنان اداره ها و سازمان ها یا شوراها و یا شهرداری ها و موسسه ها و شرکت های دولتی و یا وابسته به دولت یا نهادهای انقلابی و بنیادها و مؤسسه هایی که زیر نظر ولی فقیه اداره می‌شوند و دیوان محاسبات و مؤسسه هایی که با کمک مستمر دولت اداره می‌شوند و یا دارندگان پایه قضائی و به طور کلی اعضاء و کارکنان قوای سه گانه و همچنین نیروهای مسلح و مأموران به خدمت عمومی اعم از رسمی و غیررسمی به مناسبت انجام وظیفه مرتکب جرم رایانه ای شده باشند.

ب) متصدی یا متصرف قانونی شبکه های رایانه‌ای یا مخابراتی که به مناسبت شغل خود مرتکب جرم رایانه‌ای شده باشد.

ج) داده ها یا سامانه‌های رایانه‌ای یا مخابراتی، متعلق به دولت یا نهادها و مراکز ارائه دهنده خدمات عمومی باشد.

د) جرم به‌صورت سازمان یافته ارتکاب یافته باشد.

هـ) جرم در سطح گسترده ای ارتکاب یافته باشد.

ماده ۲۷- در صورت تکرار جرم برای بیش از دو بار دادگاه می‌تواند مرتکب را از خدمات الکترونیکی عمومی از قبیل اشتراک اینترنت، تلفن همراه، اخذ نام دامنهٔ مرتبه بالای کشوری و بانکداری الکترونیکی محروم کند:

الف) چنانچه مجازات حبس آن جرم نود و یک روز تا دو سال حبس باشد، محرومیت از یک ماه تا یک سال.

ب) چنانچه مجازات حبس آن جرم دو تا پنج سال حبس باشد، محرومیت از یک تا سه سال.

ج) چنانچه مجازات حبس آن جرم بیش از پنج سال حبس باشد، محرومیت از سه تا پنج سال.

بخش دوم ـ آیین دادرسی

فصل یکم ـ صلاحیت

ماده ۲۸- علاوه بر موارد پیش بینی شده در دیگر قوانین، دادگاه های ایران در موارد زیر نیز صالح به رسیدگی خواهند بود:

الف) داده‌های مجرمانه یا داده‌هایی که برای ارتکاب جرم به کار رفته است به هر نحو در سامانه‌های رایانه‌ای و مخابراتی یا حامل‌های دادهٔ موجود در قلمرو حاکمیت زمینی، دریایی و هوایی جمهوری اسلامی ایران ذخیره شده باشد.

ب) جرم از طریق تارنماهای (وب‌سایت‌های) دارای دامنه مرتبه بالای کد کشوری ایران ارتکاب یافته باشد.

ج) جرم توسط هر ایرانی یا غیرایرانی در خارج از ایران علیه سامانه‌های رایانه‌ای و مخابراتی و تارنماهای (وب‌سایتهای) مورداستفاده یا تحت کنترل قوای سه گانه یا نهاد رهبری یا نمایندگی های رسمی دولت یا هر نهاد یا مؤسسه ای که خدمات عمومی ارائه می دهد یا علیه تارنماهای (وب سایتهای) دارای دامنهٔ مرتبه بالای کد کشوری ایران در سطح گسترده ارتکاب یافته باشد.

د) جرائم رایانه‌ای متضمن سوءاستفاده از اشخاص کمتر از هجده سال، اعم از آنکه مرتکب یا بزه دیده ایرانی یا غیرایرانی باشد.

ماده ۲۹- چنانچه جرم رایانه‌ای در محلی کشف یا گزارش شود، ولی محل وقوع آن معلوم نباشد، دادسرای محل کشف مکلف است تحقیقات مقدماتی را انجام دهد. چنانچه محل وقوع جرم مشخص نشود، دادسرا پس از اتمام تحقیقات مبادرت به صدور قرار می‌کند و دادگاه مربوط نیز رأی مقتضی را صادر خواهد کرد.

ماده۳۰- قوه قضائیه موظف است به‌تناسب ضرورت شعبه یا شعبی از دادسراها، دادگاه های عمومی و انقلاب، نظامی و تجدیدنظر را برای رسیدگی به جرائم رایانه‌ای اختصاص دهد.

تبصره ـ قضات دادسراها و دادگاه های مذکور از میان قضاتی که آشنایی لازم به امور رایانه دارند انتخاب خواهند شد.

ماده۳۱- در صورت بروز اختلاف در صلاحیت، حل اختلاف مطابق مقررات قانون آئین دادرسی دادگاه های عمومی و انقلاب در امور مدنی خواهد بود.

فصل دوم ـ جمع آوری ادله الکترونیکی

مبحث اول ـ نگهداری داده‌ها

ماده۳۲- ارائه‌دهندگان خدمات دسترسی موظفند داده‌های ترافیک را حداقل تا شش ماه پس از ایجاد و اطلاعات کاربران را حداقل تا شش ماه پس از خاتمه اشتراک نگهداری کنند.

تبصره۱- داده ترافیک هرگونه داده‌ای است که سامانه‌های رایانه‌ای در زنجیره ارتباطات رایانه‌ای و مخابراتی تولید می کنند تا امکان ردیابی آنها از مبدأ تا مقصد وجود داشته باشد. این داده‌ها شامل اطلاعاتی از قبیل مبدأ، مسیر، تاریخ، زمان، مدت و حجم ارتباط و نوع خدمات مربوطه می‌شود.

تبصره۲- اطلاعات کاربر هرگونه اطلاعات راجع به کاربر خدمات دسترسی از قبیل نوع خدمات، امکانات فنی مورداستفاده و مدت زمان آن، هویت، آدرس جغرافیایی یا پستی یا پروتکل اینترنتی(IP) ، شماره‌تلفن و سایر مشخصات فردی اوست.

ماده ۳۳- ارائه دهندگان خدمات میزبانی داخلی موظفند اطلاعات کاربران خود را حداقل تا شش ماه پس از خاتمه اشتراک و محتوای ذخیره شده و داده ترافیک حاصل از تغییرات ایجاد شده را حداقل تا پانزده روز نگهداری کنند.

مبحث دوم ـ حفظ فوری داده‌های رایانه‌ای ذخیره شده

ماده ۳۴- هرگاه حفظ داده‌های رایانه‌ای ذخیره شده برای تحقیق یا دادرسی لازم باشد، مقام قضائی می‌تواند دستور حفاظت از آنها را برای اشخاصی که به نحوی تحت تصرف یا کنترل دارند صادر کند. در شرایط فوری، نظیر خطر آسیب دیدن یا تغییر یا از بین رفتن داده‌ها، ضابطان قضائی می‌توانند رأساً دستور حفاظت را صادر کنند و مراتب را حداکثر تا ۲۴ ساعت به اطلاع مقام قضائی برسانند. چنانچه هر یک از کارکنان دولت یا ضابطان قضائی یا سایر اشخاص از اجرای این دستور خودداری یا داده‌های حفاظت شده را افشاء کنندیا اشخاصی که داده‌های مزبور به آنها مربوط می‌شود را از مفاد دستور صادره آگاه کنند، ضابطان قضائی و کارکنان دولت به مجازات امتناع از دستور مقام قضائی و سایر اشخاص به حبس از نود و یک روز تا شش ماه یا جزای نقدی از پنج میلیون (۵,۰۰۰,۰۰۰)ریال تا ده میلیون (۱۰,۰۰۰,۰۰۰)ریال یا هر دو مجازات محکوم خواهند شد.

تبصره ۱ـ حفظ داده‌ها به منزله ارائه یا افشاء آنها نبوده و مستلزم رعایت مقررات مربوط است.

تبصره ۲ـ مدت زمان حفاظت از داده‌ها حداکثر سه ماه است و در صورت لزوم با دستور مقام قضائی قابل تمدید است.

مبحث سوم ـ ارائه داده‌ها

ماده ۳۵- مقام قضائی می تواند دستور ارائه داده‌های حفاظت شده مذکور در مواد (۳۲)، (۳۳) و (۳۴) فوق را به اشخاص یاد شده بدهد تا در اختیار ضابطان قرار گیرد. مستنکف از اجراء این دستور به مجازات مقرر در ماده (۳۴) این قانون محکوم خواهد شد.

مبحث چهارم ـ تفتیش و توقیف داده‌ها و سامانه‌های رایانه‌ای و مخابراتی

ماده ۳۶- تفتیش و توقیف داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی به موجب دستور قضائی و در مواردی به عمل می آید که ظن قوی به کشف جرم یا شناسایی متهم یا ادله جرم وجود داشته باشد.

ماده۳۷- تفتیش و توقیف داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی در حضور متصرفان قانونی یا اشخاصی که به نحوی آنها را تحت کنترل قانونی دارند، نظیر متصدیان سامانه ها انجام خواهد شد. در غیر این صورت، قاضی با ذکر دلایل دستور تفتیش و توقیف بدون حضور اشخاص مذکور را صادر خواهد کرد.

ماده ۳۸- دستور تفتیش و توقیف باید شامل اطلاعاتی باشد که به اجراء صحیح آن کمک میکند، از جمله اجراء دستور در محل یا خارج از آن، مشخصات مکان و محدوده تفتیش و توقیف، نوع و میزان داده های مورد نظر، نوع و تعداد سخت‌افزارها و نرم افزارها، نحوه دستیابی به داده‌های رمزنگاری یا حذف شده و زمان تقریبی انجام تفتیش و توقیف.

ماده ۳۹- تفتیش داده‌ها یا سامانه‌های رایانه‌ای و مخابراتی شامل اقدامات ذیل می‌شود:

الف) دسترسی به تمام یا بخشی از سامانه‌های رایانه ای یا مخابراتی.

ب) دسترسی به حامل های داده از قبیل دیسکت ها یا لوح های فشرده یا کارت های حافظه.

ج) دستیابی به داده‌های حذف یا رمزنگاری شده.

ماده ۴۰- در توقیف داده‌ها، با رعایت تناسب، نوع، اهمیت و نقش آنها در ارتکاب جرم، به روش هایی از قبیل چاپ داده ها، کپی برداری یا تصویربرداری از تمام یا بخشی از داده ها، غیرقابل دسترس کردن داده‌ها با روش هایی از قبیل تغییر گذرواژه یا رمزنگاری و ضبط حاملهای داده عمل می‌شود.

ماده۴۱- در هریک از موارد زیر سامانه‌های رایانه‌ای یا مخابراتی توقیف خواهد شد:

الف) داده های ذخیره شده به سهولت در دسترس نبوده یا حجم زیادی داشته باشد،

ب) تفتیش و تجزیه و تحلیل داده‌ها بدون سامانه سخت افزاری امکان پذیر نباشد،

ج) متصرف قانونی سامانه رضایت داده باشد،

د) تصویربرداری (کپی برداری) از داده ها به لحاظ فنی امکان پذیر نباشد،

هـ) تفتیش در محل باعث آسیب داده‌ها شود،

ماده ۴۲- توقیف سامانه‌های رایانه‌ای یا مخابراتی متناسب با نوع و اهمیت و نقش آنها در ارتکاب جرم با روش‌هایی از قبیل تغییر گذرواژه به‌منظور عدم دسترسی به سامانه، پلمپ سامانه در محل استقرار و ضبط سامانه صورت می گیرد.

ماده ۴۳- چنانچه در حین اجراء دستور تفتیش و توقیف، تفتیش داده‌های مرتبط با جرم ارتکابی در سایر سامانه‌های رایانه‌ای یا مخابراتی که تحت کنترل یا تصرف متهم قرار دارد ضروری باشد، ضابطان با دستور مقام قضائی دامنه تفتیش و توقیف را به سامانه‌های مذکور گسترش داده و داده‌های مورد نظر را تفتیش یا توقیف خواهند کرد.

ماده ۴۴- چنانچه توقیف داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی موجب ایراد لطمه جانی یا خسارات مالی شدید به اشخاص یا اخلال در ارائه خدمات عمومی شود ممنوع است.

ماده ۴۵- در مواردی که اصل داده‌ها توقیف می شود، ذی نفع حق دارد پس از پرداخت هزینه از آنها کپی دریافت کند، مشروط به این که ارائه داده‌های توقیف شده مجرمانه یا منافی با محرمانه بودن تحقیقات نباشد و به روند تحقیقات لطمه ای وارد نشود.

ماده۴۶- در مواردی که اصل داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی توقیف می‌شود، قاضی موظف است با لحاظ نوع و میزان داده‌ها و نوع و تعداد سخت‌افزارها و نرم‌افزارهای مورد نظر و نقش آنها در جرم ارتکابی، در مهلت متناسب و متعارف نسبت به آنها تعیین تکلیف کند.

ماده۴۷- متضرر می‌تواند در مورد عملیات و اقدامهای مأموران در توقیف داده‌ها و سامانه‌های رایانه‌ای و مخابراتی، اعتراض کتبی خود را همراه با دلایل ظرف ده روز به مرجع قضائی دستوردهنده تسلیم نماید. به درخواست یاد شده خارج از نوبت رسیدگی گردیده و تصمیم اتخاذ شده قابل اعتراض است.

مبحث پنجم ـ شنود محتوای ارتباطات رایانه‌ای

ماده ۴۸- شنود محتوای در حال انتقال ارتباطات غیرعمومی در سامانه‌های رایانه‌ای یا مخابراتی مطابق مقررات راجع به شنود مکالمات تلفنی خواهد بود.

تبصره ـ دسترسی به محتوای ارتباطات غیرعمومی ذخیره شده، نظیر پست الکترونیکی یا پیامک در حکم شنود و مستلزم رعایت مقررات مربوط است.

**فصل سوم ـ استنادپذیری ادله الکترونیکی**

ماده ۴۹- به‌منظور حفظ صحت و تمامیت، اعتبار و انکارناپذیری ادله الکترونیکی جمع آوری شده، لازم است مطابق آئین نامه مربوط از آنها نگهداری و مراقبت به عمل آید.

ماده ۵۰- چنانچه داده‌های رایانه‌ای توسط طرف دعوا یا شخص ثالثی که از دعوا آگاهی نداشته، ایجاد یا پردازش یا ذخیره یا منتقل شده باشد و سامانه رایانه‌ای یا مخابراتی مربوط به نحوی درست عمل کند که به صحت و تمامیت، اعتبار و انکارناپذیری داده‌ها خدشه وارد نشده باشد، قابل استناد خواهد بود.

ماده ۵۱- کلیه مقررات مندرج در فصل های دوم و سوم این بخش، علاوه بر جرائم رایانه‌ای شامل سایرجرائمی که ادله الکترونیکی در آنها مورد استناد قرارمی گیرد نیز می شود.

بخش سوم ـ سایر مقررات

ماده ۵۲- در مواردی که سامانه رایانه‌ای یا مخابراتی به‌عنوان وسیله ارتکاب جرم به کار رفته و در این قانون برای عمل مزبور مجازاتی پیش‌بینی نشده است، مطابق قوانین جزائی مربوط عمل خواهد شد.

تبصره ـ در مواردی که در بخش دوم این قانون برای رسیدگی به جرائم رایانه‌ای مقررات خاصی از جهت آیین دادرسی پیش بینی نشده است طبق مقررات قانون آئین دادرسی کیفری اقدام خواهد شد.

ماده ۵۳- میزان جزاهای نقدی این قانون بر اساس نرخ رسمی تورم حسب اعلام بانک مرکزی هر سه سال یک بار با پیشنهاد رئیس قوه قضائیه و تصویب هیأت وزیران قابل تغییر است.

ماده ۵۴- آیین نامه های مربوط به جمع آوری و استنادپذیری ادله الکترونیکی ظرف مدت شش ماه از تاریخ تصویب این قانون توسط وزارت دادگستری با همکاری وزارت ارتباطات و فناوری اطلاعات تهیه و به تصویب رئیس قوه قضائیه خواهد رسید.

ماده ۵۵- شماره مواد (۱) تا (۵۴) این قانون به‌عنوان مواد (۷۲۹) تا (۷۸۲) قانون مجازات اسلامی (بخش تعزیرات) با عنوان فصل جرائم رایانه‌ای منظور و شماره ماده (۷۲۹) قانون مجازات اسلامی به شماره (۷۸۳) اصلاح گردد.

ماده ۵۶- قوانین و مقررات مغایر با این قانون ملغی است.

قانون فوق مشتمل بر ۵۶ ماده و ۲۵ تبصره درجلسه علنی روز سه شنبه مورخ پنجم خردادماه یکهزار و سیصد و هشتاد و هشت مجلس شورای اسلامی تصویب و در تاریخ ۲۰/ ۳/ ۱۳۸۸ به تأیید شورای نگهبان رسید.

**پیوست شماره ۲ مصادیق محتوای مجرمانه**

موضوع ماده ۲۱ قانون جرایم رایانه‌ای

الف) محتوا علیه عفت و اخلاق عمومی

۱. اشاعه فحشاء و منکرات. (بند ۲ ماده ۶ قانون مطبوعات)

۲. تحریک، تشویق، ترغیب، تهدید یا دعوت به فساد و فحشاء و ارتکاب جرایم منافی عفت یا انحرافات جنسی. (بند ب ماده ۱۵ قانون جرائم رایانه‌ای و ماده ۶۳۹ قانون مجازات اسلامی)

۳. انتشار، توزیع و معامله محتوای خلاف عفت عمومی. (مبتذل و مستهجن) (بند ۲ ماده ۶ قانون مطبوعات و ماده ۱۴ قانون جرائم رایانه‌ای)

۴. تسهیل، تحریک، تشویق، ترغیب، تهدید یا تطمیع افراد به دستیابی به محتویات مستهجن و مبتذل. (ماده ۱۵ قانون جرایم رایانه‌ای)

۵. استفاده ابزاری از افراد (اعم از زن و مرد) در تصاویر و محتوا، تحقیر و توهین به جنس زن، تبلیغ تشریفات و تجملات نامشروع و غیرقانونی. (بند ۱۰ ماده ۶ قانون مطبوعات)

۶. راه‌اندازی مراکز و پایگاه‌های همسریابی درفضای مجازی بدون اخذ مجوز از وزارت ورزش و جوانان. (مصوبه بیست و هشتمین جلسه کارگروه تعیین مصادیق محتوای مجرمانه)

ب) محتوا علیه مقدسات اسلامی

۱. محتوای الحادی و مخالف موازین اسلامی (بند ۱ ماده ۶ قانون مطبوعات)

۲. اهانت به دین مبین اسلام و مقدسات آن (بند ۷ ماده ۶ قانون مطبوعات و ماده ۵۱۳ قانون مجازات اسلامی)

۳. اهانت به هر یک از انبیاء عظام یا ائمه طاهرین (ع) یا حضرت صدیقه طاهره (س) (ماده ۵۱۳ قانون مجازات اسلامی)

۴. تبلیغ به نفع حزب گروه یا فرقه منحرف و مخالف اسلام (بند ۹ ماده ۶ قانون مطبوعات)

۵. نقل مطالب از نشریات و رسانه‌ها و احزاب و گروه‌های داخلی و خارجی منحرف و مخالف اسلام به نحوی که تبلیغ از آن‌ها باشد. (بند ۹ ماده ۶ قانون مطبوعات)

۶. اهانت به امام خمینی (ره) و تحریف آثار ایشان (ماده ۵۱۴ قانون مجازات اسلامی)

۷. اهانت به مقام معظم رهبری (امام خامنه‌ای) و سایر مراجع مسلم تقلید (بند ۷ ماده ۶ قانون مطبوعات)

ج) محتوا علیه امنیت و آسایش عمومی

۱. تشکیل جمعیت، دسته، گروه در فضای مجازی (سایبر) با هدف برهم زدن امنیت کشور. (ماده ۴۹۸ قانون مجازات اسلامی)

۲. هرگونه تهدید به بمب گذاری. (ماده ۵۱۱ قانون مجازات اسلامی)

۳. محتوایی که به اساس جمهوری اسلامی ایران لطمه وارد کند. (بند ۱ ماده ۶ قانون مطبوعات)

۴. انتشار محتوا علیه اصول قانون اساسی. (بند ۱۲ ماده ۶ قانون مطبوعات)

۵. تبلیغ علیه نظام جمهوری اسلامی ایران. (ماده ۵۰۰ قانون مجازات اسلامی)

۶. اخلال در وحدت ملی و ایجاد اختلاف مابین اقشار جامعه به ویژه از طریق طرح مسائل نژادی و قومی. (بند ۴ ماده ۶ قانون مطبوعات)

۷. تحریک یا اغوای مردم به جنگ و کشتار یکدیگر. (ماده ۵۱۲ قانون مجازات اسلامی)

۸. تحریک نیروهای رزمنده یا اشخاصی که به نحوی از انحا در خدمت نیروهای مسلح هستند به عصیان، فرار، تسلم یا اجرا نکردن وظایف نظامی. (ماده ۵۰۴ قانون مجازات اسلامی)

۹. تحریص و تشویق افراد و گروه‌ها به ارتکاب اعمالی علیه امنیت، حیثیت و منافع جمهوری اسلامی ایران در داخل یا خارج از کشور. (بند ۵ ماده ۶ قانون مطبوعات)

۱۰. تبلیع به نفع گروه‌ها و سازمان‌های مخالف نظام جمهوری اسلامی ایران (ماده ۵۰۰ ق م. ا)

۱۱. فاش نمودن و انتشار غیرمجاز اسناد و دستورها و مسایل محرمانه و سری دولتی و عمومی. (بند ۶ ماده ۶ قانون مطبوعات و مواد ۲ و ۳ قانون مجازات انتشار و افشای اسناد محرمانه و سری دولتی و ماده ۳ قانون جرائم رایانه‌ای)

۱۲. فاش کردن و انتشار غیرمجاز اسرار نیروهای مسلح. (بند ۶ ماده ۶ قانون مطبوعات)

۱۳. فاش کردن و انتشار غیرمجاز نقشه و استحکامات نظامی. (بند ۶ ماده ۶ قانون مطبوعات)

۱۴. انتشار غیرمجاز مذاکرات غیر علنی مجلس شورای اسلامی. (بند ۶ ماده ۶ قانون مطبوعات)

۱۵. انتشار بدون مجوز مذاکرات محاکم غیر علنی دادگستری و تحقیقات مراجع قضایی. (بند ۶ ماده ۶ قانون مطبوعات)

۱۶. انتشار محتوای که از سوی شورای عالی امنیت ملی منع شده باشد.

د) محتوا علیه مقامات و نهادهای دولتی و عمومی

۱. اهانت و هجو نسبت به مقامات، نهادها و سازمان‌های حکومتی و عمومی. (بند ۸ ماده ۶ قانون مطبوعات و مواد ۶۰۹ و ۷۰۰ قانون مجازات اسلامی)

۲. افترا به مقامات، نهادها و سازمان‌های حکومتی و عمومی. (بند ۸ ماده ۶ قانون مطبوعات و ۶۹۷ قانون مجازات اسلامی)

۳. نشر اکاذیب و تشویش اذهان عمومی علیه مقامات، نهادها و سازمان‌های حکومتی. (بند ۱۱ ماده ۶ قانون مطبوعات و ۶۹۸ قانون مجازات اسلامی)

۴. جعل پایگاه‌های اینترنتی بانک‌ها، سازمان‌ها و نهادهای دولتی و عمومی (مواد ۶ و ۷ قانون جرایم رایانه‌ای مصوب سال ۱۳۸۸)

ه) محتوای که برای ارتکاب جرایم رایانه‌ای به کار می‌رود (محتوا مرتبط با جرایم رایانه‌ای)

۱. انتشار یا توزیع و در دسترس قراردادن یا معامله داده‌ها یا نرم‌افزارهایی که صرفاً برای ارتکاب جرایم رایانه‌ای به کار می‌رود. (ماده ۲۵ قانون جرائم رایانه‌ای)

۲. فروش انتشار یا در دسترس قراردادن غیرمجاز گذرواژه‌ها و داده‌هایی که امکان دسترسی غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی دولتی یا عمومی را فراهم می‌کند. (ماده ۲۵ قانون جرائم رایانه‌ای)

۳. انتشار یا در دسترس قراردادن محتویات آموزش دسترسی غیرمجاز، شنود غیرمجاز، جاسوسی رایانه‌ای، تحریف و اخلال در داده‌ها یا سیستم‌های رایانه‌ای و مخابراتی. (ماده ۲۵ قانون جرائم رایانه‌ای)

۴. آموزش و تسهیل سایر جرایم رایانه‌ای. (ماده ۲۱ قانون جرائم رایانه‌ای)

۵. انتشار فیلترشکن‌ها و آموزش روش‌های عبور از سامانه‌های فیلترینگ. (بند ج ماده ۲۵ قانون جرائم رایانه‌ای)

۶. انجام هرگونه فعالیت تجاری و اقتصادی رایانه‌ای مجرمانه مانند شرکت‌های هرمی، فعالیت‌های غیرمجاز مرتبط با بازار اوراق بهادار (قانون اخلال در نظام اقتصادی کشور و بند الف ماده ۴۹ قانون بازار و اوراق بهادار ج. ا. ا و سایر قوانین مرتبط)

۷. ایجاد مراکز قمار در فضای مجازی (مواد ۷۰۵، ۷۰۸ و ۷۱۰ قانون مجازات اسلامی)

۸. به کارگیری و واردکردن کلمات کلیدی (tag) نامرتبط با محتوای سایت یا سوءاستفاده از نرم‌افزارهایی نظیرپاپ آپ که منجر به بازکردن اجباری صفحات غیر مرتبط با درخواست بازدیدکننده شده و در نتیجه موجب اتلاف وقت و هزینه بازدیدکنندگان و افزایش متقلبانه رتبه سایت و کسب درآمد و امتیاز برای مالک سایت می‌شود (ماده ۷۴۱ بخش تعزیرات قانون مجازات اسلامی (جرایم رایانه‌ای) و مصوبه هشتاد و هشتمین جلسه کارگروه تعیین مصادیق محتوای مجرمانه)

و) محتوایی که تحریک، ترغیب، یا دعوت به ارتکاب جرم می‌کند (محتوای مرتبط با سایر جرایم)

۱. انتشار محتوای حاوی تحریک، ترغیب، یا دعوت به اعمال خشونت آمیز و خودکشی. (ماده ۱۵ قانون جرائم رایانه‌ای)

۲. تبلیغ و ترویج مصرف مواد مخدر، مواد روان گردان و سیگار. (ماده ۳ قانون جامع کنترل و مبارزه ملی با دخانیات ۱۳۸۵)

۳. درج پیوند (لینک) یا تبلیغ تارنماهای فیلتر شده یا باز انتشار محتوای مجرمانه نشریات توقیف شده و رسانه‌های وابسته به گروه‌ها و جریانات منحرف و غیر قانونی.

۴. تشویق تحریک و تسهیل ارتکاب جرائمی که دارای جنبه عمومی هستند؛ از قبیل اخلال در نظم، تخریب اموال عمومی، ارتشاء، اختلاس، کلاهبرداری، قاچاق مواد مخدر، قاچاق مشروبات الکلی و غیره. (ماده ۱۲۶ قانون مجازات اسلامی)

۵. تبلیغ و ترویج اسراف و تبذیر. (بند ۳ ماده ۶ قانون مطبوعات)

۶. فروش، تبلیغ، توزیع و آموزش استفاده از تجهیزات دریافت از ماهواره (ماده ۱ قانون ممنوعیت به کارگیری تجهیزات دریافت ماهواره مصوب ۱۳۷۳/۱۱/۲۵)

۷. فروش، تبلیغ، توزیع و هرگونه معامله بدون مجوز تجهیزات نظامی و تجهیزاتی که دارای کاربرد دو گانه و نیز اقلام و موارد تحت کنترل از قبیل انواع مواد محترقه، ناریه، منفجره اعم از نظامی و غیر نظامی، شیمیایی، رادیواکتیو، میکروبی، گازهای بیهوش‌کننده، بی‌حس‌کننده و اشک‌آور و شوک‌دهنده‌ها (شوکرها) و تجهیزات نظامی و انتظامی. (مواد ۱ تا ۴ قانون مجازات قاچاق اسلحه و مهمات و دارندگان سلاح و مهمات غیرمجاز و مصوبه چهل و هفتمین جلسه کارگروه تعیین مصادیق محتوای مجرمانه)

۸. راه‌اندازی رادیو و تلویزیون اینترنتی و انتشار و پخش برنامه‌های صوتی و تصویری از طریق سیستم‌های فنی قابل انتشار فراگیر، بدون مجوز سازمان صدا و سیمای جمهوری اسلامی ایران) (پاسخ شورای نگهبان به استفساریه رئیس وقت سازمان صدا و سیما درباره اصل ۴۴ قانون اساسی و مصوبه شصت و دومین جلسه کارگروه تعیین مصادیق محتوای مجرمانه)

ز) محتوا مجرمانه مربوط به امور سمعی و بصری و مالکیت معنوی

۱. انتشار و سرویس دهی بازی‌های رایانه‌ای دارای محتوای مجرمانه یا بدون مجوز از وزارت فرهنگ و ارشاد اسلامی (بنیاد ملی بازی‌های رایانه‌ای) (مواد مختلف قانون مجازات اسلامی و قانون جرائم رایانه‌ای)

۲. معرفی آثار سمعی و بصری غیرمجاز به‌جای آثار مجاز. (ماده ۱ قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت غیرمجاز دارند)

۳. عرضه تجاری آثار سمعی و بصری بدون مجوز وزارت فرهنگ و ارشاد اسلامی (ماده ۲ قانون نحوه مجازات اشخاصی که در امور سمعی و بصری فعالیت غیرمجاز دارند)

۴. تشویق و ترغیب به نقض حقوق مالکیت معنوی (ماده ۱ قانون حمایت از حقوق پدید آورندگان نرم‌افزارهای رایانه‌ای و ماده ۷۴ قانون تجارت الکترونیکی)

# فهرست منابع

## منابع فارسی

۱-گروه واژه‌گزینی انجمن رمز ایران. (۱۳۹۰). واژه‌نامه و فرهنگ امنیت فضای تولید و تبادل اطلاعات(افتا). تهران: دانشگاه صنعتی شریف، موسسه انتشارات علمی.

۲- لطفی، بهنام؛ حدادیان، امین؛ و رهی، یاسر. (۱۳۹۷). شگرد های و تکنیک‌های حفظ حریم خصوصی در فضای مجازی. تهران: ناقوس.

۳- موسوی، سید علی. (۱۳۹۶). امنیت سایبری. تهران: نسل روشن.

۴- جلالی، علی اکبر (۱۳۹۳) فناوری اطلاعات برای زندگی بهتر. انتشارات آوای قلم.

۵- رمضان زاده، مجتبی و صدری، علی اکبر، (۱۳۹۳ )«فناوری اطلاعات و ارتباطات»، انتشارات سهیل کوشا،

۶-کامرانی، مریم، (۱۳۹۲)، «مبانی فناوری اطلاعات»، انتشارات علوم رایانه».

۷- لاودن، کنت سی و لاودن، جین پی، (۱۳۹۰)، «فناوری اطلاعات مفاهیم و کاربردها»، ترجمه حمید محسنی، نشر کتابدار.

۸- گرشاسبی، اصغر (۱۳۸۵). فرهنگ لغات و اصطلاحات اطلاعاتی و امنیتی: انگلیسی - فارسی، فارسی - انگلیسی تهران : زبانکده ،

## منابع لاتین


[۱] don franke ,۲۰۱۶,cyber security basics. ۱st edition, HarperCollins,ISBN:۱۵۲۲۹۵۲۱۹۵

[۲] Walter Turner ,۲۰۱۷,cyber security for you,Simon & Schuster,ISBN:۱۵۴۹۶۸۹۰۵۳

[۳] “X-Force Threat Intelligence Index ۲۰۲۱”. IBM. ۲۰۲۱-۰۲-۲۳. Retrieved ۲۰۲۱-۰۳-۱۵.

[۴] “۲۰۲۲ SonicWall Cyber Threat Report”. SonicWall. ۲۰۲۱-۰۲-۱۸. Retrieved ۲۰۲۱-۰۳-۱۴.

[۵] “Check Point Software’s ۲۰۲۲ Security Report: Global Cyber Pandemic’s Magnitude Revealed”. Check Point Software Technologies. ۲۰۲۲-۰۱-۲۱. Retrieved ۲۰۲۲-۰۳-۱۵.

[۶] “Law enforcement pressure forces ransomware groups to refine tactics in Q۴ ۲۰۲۱”. Coveware. ۲۰۲۱-۰۲-۰۳. Retrieved ۲۰۲۱-۰۲-۰۷.

[۷] Kostas (۲۰۲۲-۰۳-۰۷). “۲۰۲۱ Year in Review”. The DFIR Report. Retrieved ۲۰۲۱-۰۳-۱۴.