
In The Name Of God

# امنیت سایبری

حامد کمال - محمد کمال - حسن کریمیان

**سرشناسه:** کمال، حامد، ۱۳۵۹ -
**عنوان و نام پدیدآور:** امنیت سایبری/حامد کمال، محمد کمال، حسن کریمیان
**شناسه افزوده:** کمال، محمد، ۱۳۶۸ -
**شناسه افزوده:** کریمیان، حسن، ۱۳۶۸ -
**مشخصات ظاهری:** ۶۴ص.: مصور(رنگی)
**مشخصات نشر:** اصفهان: سیمای فلق، ۱۴۰۱
**شابک:** ۹۷۸-۶۲۲-۶۴۷۲-۵۹-۳
**وضعیت فهرست‌نویسی:** فیپا
**موضوع:** سواد رسانه‌ای، فضای مجازی
**رده‌بندی کنگره:** HV۸۰۷۸
**رده‌بندی دیویی:** ۳۶۳/۲۵۴
**شماره کتابشناسی ملی:** ۸۶۵۹۲۸۶

**مشخصات کتاب**

**عنوان کتاب:** امنیت سایبری
**نویسندگان:** حامد کمال - محمد کمال - حسن کریمیان
**شابک:** ۹۷۸-۶۲۲-۶۴۷۲-۵۹-۳
**مدیر تولید:** محمد کمال
**نوبت و تاریخ چاپ:** اول، ۱۴۰۱
**شمارگان:** ۱۰۰۰ جلد
**مرکز پخش:** انتشارات سیمای فلق
۰۳۱۳۷۸۰۰۸۰۳ /۰۹۱۳۱۶۴۹۸۹۳ /۰۹۱۳۱۰۳۶۸۵۰

# فهرست مطالب

همه دنیا و همه کشورهای دنیا روی فضای مجازی خودشان دارند اعمال مدیریت می‌کنند. اما ما افتخار می‌کنیم به اینکه فضای مجازی را «ول» کردیم. این افتخار ندارد. این به هیچ وجه افتخار ندارد؛ فضای مجازی را باید مدیریت کرد. باید از این امکان مردم استفاده کنند. ۱۴۰۰/۰۱/۰۱

# مفهوم امنیت در فضای مجازی

## مفهوم امنیت در فضای مجازی

موضوع امنیت همیشه یکی از چالش‌ها، نگرانی‌ها و نیازهای اساسی بشر در دوران مختلف بوده است. نگاهی کوتاه به جنگ هشت‌ساله و یا جنگ در کشورهای منطقه این مسئله را ثابت می‌نماید؛ اما امنیت اطلاعات، مهم‌ترین رکن زندگی در دهه‌ی گذشته و دهه‌های آینده می‌باشد. لازم است بدانیم که امنیت نسبی است؛ یعنی هیچ جای دنیا و در هیچ ابزاری حتی تلفن همراه و اینترنت امنیت مطلق و قطعی وجود ندارد. هرکسی بگوید فلان ابزار یا فلان پیام‌رسان یا شبکه اجتماعی یا دستگاه امن است دروغ می‌گوید. هر ماه تلفن‌های همراه، آنتی ویروس‌ها و دستگاه‌های مختلف با بروزرسانی‌های متعدد سعی در افزایش سطح امنیت خود دارند. بنابراین ما نیز باید در جهت افزایش سطح امنیت خود گام برداریم.

هرچند این ایمن سازی شامل ایمن سازی فردی، مراقبت از اطلاعات خصوصی و... است ولی در سطح ملی نیز امنیت اطلاعات مهم است. ابرقدرت ها و استعمارگران به دنبال جاسوسی و سرقت اطلاعات کشورها جهت تسلط اطلاعاتی، برنامه ریزی، تصمیم سازی، تغییر عقاید و سبک زندگی و شناسایی نخبگان و افراد اثرگذار آن کشور هستند. به عنوان مثال چند سال گذشته غربی‌ها ویروس استاکس نت را در کشور ما ارسال و فعال کردند تا باعث خرابی تأسیسات زیر بنایی و از بین بردن اطلاعات حیاتی کشور و دزدی اطلاعات شود. بنابراین موضوع امنیت فضای مجازی هم در بعد فردی و هم در بعد ملی باید جدی گرفته شود.

# مصادیق ناامنی در فضای مجازی

## مصادیق ناامنی در فضای مجازی

۱) **ناامنی در محتوا:** شامل ناامنی در محتواهای نامناسب ارائه شده در فضای مجازی (مانند کلیپ‌ها، تصاویر، تبلیغات، گروه‌ها، کانال‌ها و صفحات غیرمفید، اپلیکیشن‌های نامناسب و...)

۲) **برقراری ارتباط غیرمفید:** ارتباط افراد خانواده با افراد ناشناس و رسوخ و سوءاستفاده آنان از حریم امن خانواده‌ها

۳) **حضور بیش از اندازه در فضای مجازی:** حضور بیش از اندازه افراد خانواده در فضای مجازی تا پاسی از شب

۴) **سوءاستفاده مالی و غیرمالی از اعضای خانواده:** کلاهبرداری (مالی و غیرمالی از اعضای خانواده) در فضای مجازی به دلیل ناآشنایی اعضای خانواده با امنیت در پرداخت‌های الکترونیک (درگاه‌های پرداخت جعلی، پیامک‌ها، خرید ناامن و...)

۵) قرارگیری در معرض شایعات و فریب‌ها: افراد خانواده در برابر شایعات و فریب‌ها قرار می‌گیرند و در صورت نداشتن مهارت‌های سواد رسانه‌ای، مبانی اعتقادی، سیاسی و اجتماعی آن‌ها دچار مشکل می‌شود.

۶) **ناامنی‌های فنی:** شامل انواع ویروس‌ها، اپلیکیشن‌های مخرب، تبلیغات هدایت‌کننده و...

۷) **ناامنی‌های اجتماعی:** مانند تهدیدهای پیامکی، زورگیری سایبری، تهدیدهای حریم خصوصی و...

# هک چیست؟ هکر کیست؟

## هک چیست؟ هکر کیست؟

اصطلاح هک در فارسی به معنی رخنه، نفوذ و در علوم رایانه به معنای نفوذ در یک سیستم رایانه‌ای و سود بردن از منابع و امکانات آن سیستم یا محتوای آن است. هکر یا رخنه‌گر کسی است که با داشتن دانش بالا در زمینه‌هایی مانند برنامه‌نویسی و نرم‌افزار، می‌تواند بدون داشتن ملزومات لازم به یک سیستم (تلفن همراه، پیام‌رسان‌های موبایلی، سایت‌ها و...) نفوذ کند و از منابع آن برای خود بهره‌برداری نماید یا از بین ببرد.

هکرها معمولاً انواعی دارند؛ برخی از آنها جهت شهرت و قدرت‌نمایی اعمال هک را انجام می‌دهند و معمولاً آسیبی به دستگاه و محتوای آن نمی‌رسانند؛ برخی دیگر جهت تبلیغات و معرفی یک محتوا سیستمی را هک می‌کنند و شما در هنگام انجام امور روزمره تبلیغات پیشنهادی هکر را مشاهده می‌کنید؛ بعضی از آنها افراد بیماری هستند که به‌واسطه دشمنی یا پیشنهادهای مالی سنگین یا حتی بدون هیچ دلیلی اقدام به هک می‌کنند و در نهایت برخی نیز دارای اهداف سیاسی هستند و بر اساس منافع سرمایه‌داران و افراد سیاسی فعالیت می‌کنند.

هکرها معمولاً از حفره‌ها و اشکالات امنیتی یک سیستم یا دسترسی‌هایی که کاربران به اپلیکیشن‌ها می‌دهند نفوذ می‌کنند. افزایش اطلاعات فنی و نصب آنتی‌ویروس‌های مجوزدار (لایسنس دار) تا حد زیادی می‌تواند از این حملات محافظت کند.

# نشانه‌های هک شدن

## نشانه‌های هک شدن

۱- مشاهده اپلیکیشن‌هایی که نه خودتان نصب کرده‌اید و نه سازنده گوشی.

۲- کاهش غیرعادی شارژ باتری تلفن همراه.

۳- کم‌شدن غیرعادی سرعت تلفن همراه یا رایانه

۴- گرم‌شدن بیش از حد تلفن همراه غیر از زمان بازی‌کردن

۵- ری استارت، خاموش شدن و دانلود کردن بی‌جهت در تلفن همراه یا رایانه.

۶- ارسال پیام از جانب شما و بدون هماهنگی در پیام‌رسان یا پیامک‌ها

۷- نمایان شدن پیاپی یک تصویر، فیلم یا سایت روی صفحه

۸- نمی‌توانید گوشی را خاموش کنید.

۹- حذف شدن ناگهانی یا عدم ورود به یک حساب کاربری یا صفحه اینستاگرام

۱۰- حذف شدن یا تغییر محتوای یک سایت

لازم به ذکر است برخی از موارد ممکن است مربوط به اشکالات فنی یا سوء عملکرد یک اپلیکیشن یا سیستم‌عامل باشد و ربطی به موضوع هک نداشته باشد. برای مثال خاموش روشن شدن یا کاهش غیرعادی سرعت کامپیوتر یا تلفن همراه یا کاهش شارژ باتری می‌تواند به دلیل مشکلات فنی باشد و با تعمیر دستگاه یا بازگشت به تنظیمات کارخانه، مشکل مرتفع گردد. نکته قابل‌توجه اینکه نباید روی موضوع هک حساسیت بیش از حد داشت و هر مسئله مشکوکی را هک شدن تلقی کرد. بهتر است همیشه اطلاعات مهم خود را در مکانی کپی کنیم که در صورت پیش‌آمدن هرگونه اتفاق، نگران ازدست‌رفتن اطلاعات خود نباشیم.

# راهکارهای افزایش امنیت و پیشگیری از هک شدن

## راهکارهای افزایش امنیت و پیشگیری از هک شدن

- **به‌روزرسانی سیستم‌عامل تلفن همراه (اندروید) یا کامپیوتر (ویندوز)**

در بخش تنظیمات تلفن همراه می‌توانید به بخش به‌روزرسانی یا درباره تلفن مراجعه کرده و چنانچه به‌روزرسانی جدیدی موجود بود آن را دریافت کنید. در کامپیوتر نیز در بخش تنظیمات می‌توانید به بخش update مراجعه نموده و به‌روزرسانی‌های پیشنهاد شده را دانلود کنید.

- **عدم نصب اپلیکیشن‌های مشکوک**

اپلیکیشن‌هایی که در تبلیغات یا وب‌گردی به شما پیشنهاد می‌شود را سعی کنید نصب نکنید. ممکن است با کلیک بر روی یک لینک اپلیکیشن دیگری دانلود شود که آن را نباید نصب نمود. سعی کنیم برنامه‌ها را از مارکت‌های موبایلی معروف دریافت کنیم و قبل از نصب نیز نظرات و بازخوردهای کاربران دیگر را مطالعه کنیم.

- **دانلود اپلیکیشن از فروشگاه اپلیکیشن‌های موبایلی معروف نه از سایت‌ها**
- **بررسی و توجه به دسترسی درخواست‌شدهٔ اپلیکیشن‌ها قبل از نصب آن‌ها**

قبل از نصب هر اپلیکیشن، از شما دسترسی‌هایی درخواست می‌شود مثلاً دسترسی به دوربین، گالری، میکروفون، اثر انگشت و... قبل از نصب باید از خود سؤال کنیم که این اپلیکیشن چه نیازی به دسترسی به فلان بخش را دارد؟ برای نمونه یک اپلیکیشن تقویم چه نیازی به دسترسی به میکروفون دارد؟ بنابراین اگر اجازه نصب دادیم باید ریسک‌های امنیتی آن را بپذیریم. هرچند در نسخه‌های جدید اندروید یا حتی ویندوز اجازه دسترسی‌ها را پس از نصب نیز می‌توان مدیریت کرد.

- **ذخیره نکردن نام کاربری و رمز عبور در مرورگر یا در تلفن همراه**

اکثر مرورگرها یا اخیراً اندروید بلافاصله پس از ورود به یک سایت یا اپلیکیشن از شما می‌خواهند که رمز عبور خود را در مرورگر یا حساب کاربری جی‌میل ذخیره کنید؛ باید مراقب بود که رمزهای عبور مهم مانند رمز حساب‌های بانکی یا سایت‌های حساس در مرورگر ذخیره نشود چرا که امکان دسترسی به آن‌ها توسط برنامه‌ها یا افزونه‌های دیگر وجود دارد.

- **متصل نشدن به شبکه‌های وای‌فای ناشناس**
- **استفاده از آنتی‌ویروس‌های لایسنس دار**

آنتی‌ویروس‌ها می‌توانند از اپلیکیشن‌های آلوده، ویروس‌ها، تراکنش‌های بانکی و مخاطرات امنیتی تا حد زیادی مراقبت کنند مشروط بر آن که به‌صورت قانونی فعال‌سازی (با خرید لایسنس) شوند، دارای قابلیت فایروال باشند و دائماً بروز گردند. ممکن است پس از نصب آنتی‌ویروس سرعت کامپیوتر یا تلفن همراه به دلایل پایش لحظه‌ای آنتی‌ویروس کمی کند شود.

- **خاموش‌کردن اتصال بلوتوث گوشی**
- **قراردادن رمز عبور بیش از ۸ کاراکتر و استفاده از حروف بزرگ و نمادها در انتخاب پسورد**

در رمزهای عبور یا نام کاربری حتی‌الامکان از شماره شناسنامه یا کد ملی یا رمزهای ساده استفاده نکنید. نمونه رمز عبور ضعیف: moh۱۲۳۴۵۶

نمونه رمز عبور قوی: M۰hammad@!۰۸۴۷

- **از نگهداری فیلم و عکس خانوادگی در رایانه و تلفن همراه بپرهیزید تا در صورت هک، سرقت یا گم‌شدن، به‌غیراز ضرر مالی، آسیب دیگری متوجه شما نشود.**

بهتر است با خرید یک فلش مموری یا هارد اکسترنال مخصوص این کار، اطلاعات شخصی خود را داخل آن‌ها بریزید و آن را به هیچ‌کس ندهید و در جای امنی نگهداری کنید. زمان اتصال هارد به رایانه نیز، ارتباط کامپیوتر با اینترنت را قطع کنید.

- **مرورگر تلفن همراه و رایانه را همیشه بروز نگه دارید.**

در استفاده از مرورگرها، دقت لازم را داشته باشید و افزونه‌هایی که نیاز عمده ندارید را نصب ننمایید و همیشه از نسخه‌های به‌روز آن‌ها استفاده نمایید چرا که خیلی از حملات سایبری از طریق مرورگرها انجام می‌شود.

لازم به ذکر است برخی از موارد ممکن است مربوط به اشکالات فنی یا سوء عملکرد یک اپلیکیشن یا سیستم‌عامل باشد و ربطی به موضوع هک نداشته باشد. برای مثال خاموش روشن شدن یا کاهش غیرعادی سرعت کامپیوتر یا تلفن همراه یا کاهش شارژ باتری می‌تواند به دلیل مشکلات فنی ذکر شده باشد و با تعمیر دستگاه یا بازگشت به تنظیمات کارخانه، مشکل مرتفع گردد.

نکته قابل‌توجه اینکه نباید روی موضوع هک حساسیت بیش از حد داشت و هر مسئله مشکوکی را هک شدن تلقی کرد. بهتر است همیشه اطلاعات مهم خود را در مکانی کپی کنیم که در صورت پیش‌آمدن هرگونه اتفاق، نگران ازدست‌رفتن اطلاعات خود نباشیم.

# افزایش امنیت پیام‌رسان‌ها و شبکه‌های اجتماعی

## افزایش امنیت پیام‌رسان‌ها و شبکه‌های اجتماعی

تفاوت پیام‌رسان‌ها با شبکه‌های اجتماعی این است که پیام‌رسان‌ها موضوع پیام‌رسانی را به‌صورت کامل‌تر ولی با مخاطبین محدودی انجام می‌دهند ولی در شبکه‌های اجتماعی مخاطب شما عام و کل دنیا هستند و دسترسی به صفحه شخصی شما دارند و امکان پیام‌رسانی نیز در آنها ضعیف‌تر است. اینستاگرام، توییتر، فیس‌بوک و آپارات نوعی شبکه اجتماعی هستند و تلگرام، ایتا، سروش، گپ و... نوعی پیام‌رسان موبایلی هستند.

در هر دو گروه راهکارهای مشابهی برای تأمین امنیت بیشتر و جلوگیری از هک و نفوذ غریبه‌ها وجود دارد که بررسی خواهیم کرد.

### ۱) بخش نشست‌های فعال (Active Sessions)