

# ویکی‌پدیا

## دانشنامه آزاد

# امنیت اینترنت

از ویکی‌پدیا، دانشنامه آزاد

امنیت اینترنت یکی از شاخه‌های امنیت کامپیوتر است که به‌طور ویژه به اینترنت می‌پردازد که غالباً با مسئله امنیت مرورگر در ارتباط است.

هم‌چنین مسئله امنیت شبکه در یک سطح عمومی‌تر وجود دارند. عملکردهای آن بر مبنای یافتن راهکارها و الگوریتم‌هایی است که بر ضد حملات اینترنتی است.

با توجه به تعداد زیادی از افرادی که به صورت غیرمجاز در اینترنت به کانال گوش می‌دهند، اینترنت کانالی ناامن برای تبادل داده‌ها محسوب می‌شود، یکی از نمونه‌های آن فیشینگ است.

تاکنون الگوریتم‌ها و توابع مختلفی برای انتقال امن داده‌ها استفاده شده‌است.

## محتویات

[امنیت لایه‌های شبکه](#)

[قانون آی پی سک](#)

[توکن امنیتی](#)

[امنیت نامه الکترونیکی](#)

[کد احراز پیام](#)

[منابع](#)

## امنیت لایه‌های شبکه

مجموعه پروتکل امنیت به کمک توابع پروتکل‌های رمزنویسی که تا به حال برای ارتباطات امن در اینترنت نوشته شده‌اند، می‌تواند امن شود. از جمله این قوانین لایه سوکت‌های امن و امنیت لایه انتقال برای ترافیک بر روی وب و محرمانگی نسبتاً خوب برای ایمیل و آی پی سک برای امنیت لایه‌های شبکه است.

## قانون آی پی سک

این قانون برای ایجاد امنیت در ارتباطات مجموعه پروتکل امنیت طراحی شده‌است. این قانون شامل مجموعه‌های امنیتی است که توسط نیروی ضربت مهندسی اینترنت توسعه یافته‌است، هم‌چنین با استفاده از رمزنویسی، امنیت و احراز اصالت را در لایه آی پی فراهم می‌کند. در واقع برای حفاظت از داده‌ها، آن‌ها با استفاده از تکنیک‌های رمزنویسی فرستاده می‌شوند.

دو نوع اصلی انتقال وجود دارد که پایه‌های اساسی آی پی سک را تشکیل می‌دهند:

سرایند احراز اصالت و پیلود فشرده سازی امنیتی

این دو پروتکل سرویس‌های صحت داده، احراز اصالت منبع داده و سرویس ضد ارسال مجدد را فراهم می‌کنند. این

پروتکل‌ها می‌توانند برای فراهم کردن سرویس‌های امنیت اینترنتی برای لایه پروتکل اینترنتی به تنهایی یا به صورت ترکیبی استفاده شوند.

اجزای اصلی معماری امنیت آی پی سک در بخش‌های تابع مند زیر آورده می‌شود:

- پروتکل‌های امنیتی برای سرآیند احراز اصالت و پیلود فشرده‌سازی امنیتی
- انجمن امنیتی برای مدیریت سیاست‌گذاری و پردازش ترافیک
- مدیریت کلید دستی و اتوماتیک برای تبادل کلید اینترنتی
- الگوریتم‌هایی برای احراز اصالت و رمز کردن

مجموعه سرویس‌های امنیتی که در لایه آی پی فراهم می‌شوند شامل کنترل دسترسی، صحت منبع داده، حفاظت علیه ارسال مجدد و محرمانگی.

الگوریتم به این مجموعه‌ها اجازه می‌دهد که بدون اثرگذاری بر کار سایر بخش‌ها به‌طور مستقل از هم کار کنند.

عملیات مربوط به آی پی سک در یک میزبان یا محیط دروازه امنیتی که حفاظت از ترافیک آی پی را می‌دهد انجام می‌شود.

## توکن امنیتی

برخی از سایت‌های آنلاین به کاربران خود قابلیت استفاده از کد شش رقمی را می‌دهند که هر 30-60 روز روی توکن امنیتی به صورت تصادفی تغییر می‌کند. کلیدی که روی نشانه امنیتی قرار دارد یک سری محاسبات ریاضی دارد که اعداد را براساس زمان جاری آن وسیله می‌سازد.

این به این معنا است که هر 30 روز فقط یک آرایه مشخص از اعداد وجود دارد که برای معتبر ساختن دستیابی به حساب کاربری آنلاین وجود دارد. وب سایتی که کاربر به آن وارد می‌شود از شماره سریال آن سخت افزارها آگاهی پیدا می‌کند و بنابراین از محاسبات و زمان لازم برای اعتبارسنجی این مسئله که عدد داده شده یکی از اعداد شش رقمی آی است که در چرخه 30 تا 60 ثانیه‌ای کار خواهد کرد نیز آگاه خواهد شد. بعد از 30 تا 60 ثانیه ابزار یک عدد تصادفی شش رقمی جدید را ارائه خواهد کرد که می‌تواند داخل سایت ثبت شود.

## امنیت نامه الکترونیکی

پیام‌های الکترونیکی در چند مرحله پردازش، نوشته می‌شوند، فرستاده می‌شوند و ذخیره می‌گردند که با نوشتن پیام آغاز می‌گردد. زمانی که کاربر نوشتن پیام خود را به پایان می‌رساند و آن را می‌رساند، پیام در یک قالب مشخص فرستاده می‌شود. بعد از آن پیام می‌تواند فرستاده شود.

سپس پیام می‌تواند انتقال داده شود. با استفاده از یک ارتباط شبکه‌ای، سرویس گیرنده ایمیل که عامل کاربر ایمیل نامیده می‌شود، به عامل انتقال ایمیل که بر روی سرور ایمیل عمل می‌کند، متصل می‌شود.

سپس ایمیل مشتری هویت فرستنده را برای سرور معین می‌کند، سپس با استفاده از فرمان‌های سمت ایمیل سرور، مشتری پیام را می‌فرستد.

## کد احراز پیام

کد احراز پیام یک تابع رمزگذاری است که از یک کلید امنیتی برای رمزگشایی پیام استفاده می‌کند. خروجی این تابع یک کد احراز پیام است که توسط فرستنده با استفاده از کلید رمز مشابه رمزگشایی می‌شود. کد احراز پیام هم از صحت داده پیام و هم از احراز اصالت پشتیبانی می‌کند.

## منابع

---

ویکی‌پدیای انگلیسی [۱] ([https://en.wikipedia.org/wiki/Internet\\_security](https://en.wikipedia.org/wiki/Internet_security))

---

برگرفته از «[https://fa.wikipedia.org/w/index.php?title=امنیت\\_اینترنت&oldid=30572068](https://fa.wikipedia.org/w/index.php?title=امنیت_اینترنت&oldid=30572068)»

---

این صفحه آخرین بار در ۱۱ دسامبر ۲۰۲۰ ساعت ۰۵:۰۶ ویرایش شده‌است.

همهٔ نوشته‌ها تحت مجوز Creative Commons Attribution/Share-Alike در دسترس است؛ برای جزئیات بیشتر شرایط استفاده را بخوانید.

ویکی‌پدیا® علامتی تجاری متعلق به سازمان غیرانتفاعی بنیاد ویکی‌مدیا است.

- سیاست محرمانگی
- دربارهٔ ویکی‌پدیا
- تکذیب‌نامه‌ها
- 
- توسعه‌دهندگان
- آمار
- اظهارنامهٔ کوکی