امنیت اطلاعات

Information Security

کاری از کانون فرهنگی آفتابگردان

تهیه شده توسط: سعید فلاح

استاد راهنما: دکتر حمید رضا نیرومند

نگارش: ۱٫۰

۱۳۹۹

http://security.pdf.aftab.cc

فهرست

مقدمه

همزمان با گسترش استفاده از رایانه‌های شخصی و مطرح شدن شبکه‌های کامپیوتری و به دنبال آن اینترنت (بزرگترین شبکه جهانی)، حیات کامپیوترها و کاربران آنان دستخوش تغییرات اساسی شده‌است. استفاده‌کنندگان کامپیوتر به منظور استفاده از دستاوردها و مزایای فناوری اطلاعات و ارتباطات، ملزم به رعایت اصولی خاصی هستند تا دچار مشکل نشوند.

امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری از جمله مؤلفه‌های مهمی است که نمی‌توان آن را مختص یک فرد یا سازمان در نظر گرفت. پرداختن به مقوله امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری در هر کشور، مستلزم توجه تمامی کاربران صرفنظر از موقعیت شغلی و سنی به جایگاه امنیت اطلاعات و ایمن‌سازی شبکه‌های کامپیوتری بوده و می‌بایست به این مقوله در سطح کلان و از بعد منافع ملی نگاه کرد.

وجود ضعف امنیتی در شبکه‌های کامپیوتری و اطلاعاتی، عدم آموزش و توجیه صحیح تمامی کاربران صرف نظر از مسئولیت شغلی آنان نسبت به جایگاه و اهمیت امنیت اطلاعات، عدم وجود دستورالعمل‌های لازم برای پیشگیری از نقایص امنیتی، عدم وجود سیاست‌های مشخص و مدون به منظور برخورد مناسب و بموقع با اشکالات امنیتی، مسائلی را به دنبال خواهد داشت که ضرر آن متوجه تمامی کاربران کامپیوتر در یک کشور شده و عملاً زیرساخت اطلاعاتی یک کشور را در معرض آسیب و تهدید جدی قرار می‌دهد. [1]

سه‌گانه CIA چیست؟

این نام هیچ ارتباطی به «سازمان اطلاعات مرکزی» امریکا (CIA[1]) ندارد و فقط یک تشابه اسمی است. CIA کوتاه شده واژه‌های «محرمانگی[2]»، «یکپارچگی[3]» و «دسترس‌پذیری[4]» است. این مثلث یک مدل امنیتی و راهنمای بسیار سودمند، برای برقراری امنیت است.

محرمانگی نخستین مؤلفه مثلث CIA است. محرمانگی به معنای جلوگیری از دسترسی افراد غیرمجاز به اطلاعات حساس است. دسترسی می‌تواند عمدی یا به خاطر بی‌کفایتی مسئول امنیت باشد. یکی از روش‌های اصلی برای اطمینان از محرمانگی، «رمزنگاری» است. «رمزنگاری» به تأمین امنیت اطلاعات و جلوگیری از افشای تصادفی آن کمک می‌کند. همچنین در حمله داخلی یا خارجی، از اطلاعات محافظت می‌کند.

یکپارچگی داده‌ها یعنی اطمینان از صحت پیام‌های دریافتی، به‌گونه‌ای که وقتی خوانده می‌شود دقیقاً مشابه زمانی باشد که برای نخستین بار نوشته شده است.

یکپارچگی به سه شکل آسیب‌پذیر خواهد بود:

۱- ایجاد پیامی که اصلاً وجود ندارد.

۲- حذف پیام، طوری که هرگز وجود نداشته است.

۳- دستکاری پیام

برای حفظ یکپارچگی و جلوگیری از آسیب‌پذیری داده‌ها، کد Hash شده آن به عنوان «امضا» یا «اثر انگشت» در انتهای پیام‌ها قرار داده شده و فرستاده می‌شود. برای Hash کردن، داده‌ها در یک فرآیند پیچیده ریاضی به یک

[1] Central Intelligence Agency
[2] Confidentiality
[3] Integrity
[4] Availability

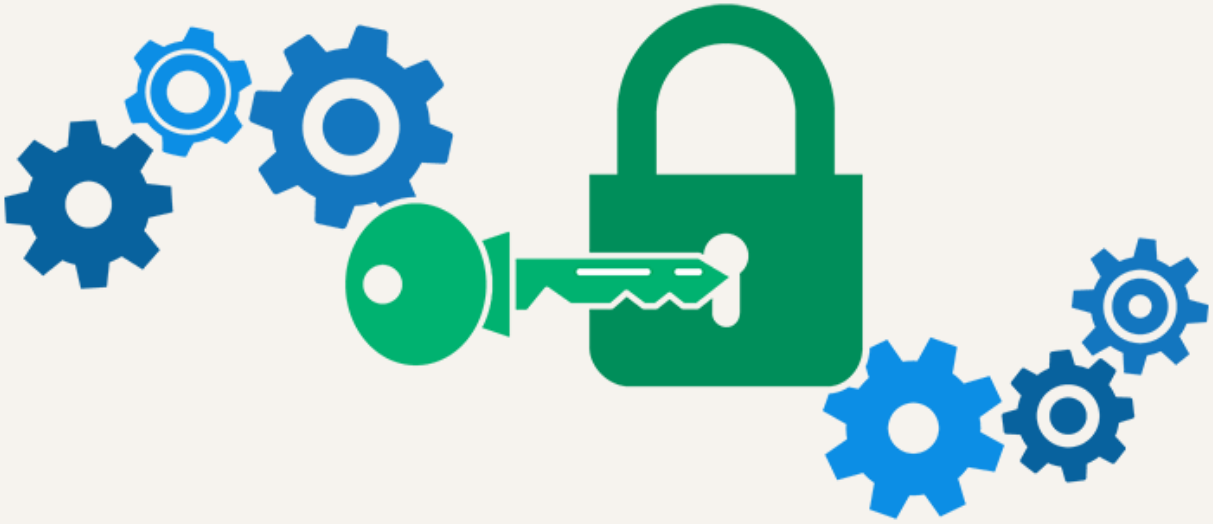
شناسه منحصر بفرد ۳۲ رقمی تبدیل می‌شوند، که حتی اگر یک بیت از آن تغییر کند، امضا تغییر کرده و دیگر معتبر نیست.

دسترس‌پذیری یعنی اطلاعات به صورت به‌هنگام و بی‌وقفه در دسترس افراد مجاز قرار بگیرید. هدف از دسترس‌پذیری، دسترسی همیشگی و جلوگیری از اختلال در ارائه سرویس به دلیل قطع برق، خرابیِ سخت‌افزار و یا بلایای طبیعی مثل سیل و زمین‌لرزه است. برای جلوگیری از قطع برق، از UPS [5]و دستگاه دیزل استفاده شده و با پیش‌بینی خرابی احتمالی سخت‌افزار، سرورهای پشتیبان تهیه می‌شود که از اختلال در دسترسی به اطلاعات جلوگیری شود. همچنین جلوگیری از حمله هکرها برای محروم‌سازی کاربران از دریافت سرویس نیز از جمله اهداف پیشگیرانه است. برای این منظور از دیوار آتش نرم‌افزاری و سخت‌افزاری استفاده می‌شود.

انواع رمزنگاری

در دنیای امنیت، الگوریتم‌های رمزنگاری داده (یا Data Encryption Algorithms) را به دو دسته کلی تقسیم می‌کنند:

۱- الگوریتم‌های رمزنگاری برگشت‌پذیر
۲- الگوریتم‌های رمزنگاری برگشت‌ناپذیر



الگوریتم‌های رمزنگاری برگشت‌پذیر یا Reversible Encryption Algorithms

در این نوع الگوریتم‌ها داده‌ی مورد نظر پس از رمزگذاری، قابل برگشت به داده‌ی اولیه است.

[5] Uninterruptible power supply

الگوریتم‌های رمزنگاری برگشت‌ناپذیر یا Irreversible Encryption Algorithms

در این نوع الگوریتم‌ها داده‌ای که رمزگذاری می‌شود، به هیچ وجه قابل برگشت به داده‌ی اولیه نیست. الگوریتم‌های برگشت‌پذیر، خودشان به دو دسته تقسیم می‌شوند:

۱- الگوریتم‌های رمزنگاری متقارن
۲- الگوریتم‌های رمزنگاری نامتقارن

الگوریتم رمزنگاری متقارن یا Symmetric-key algorithm چیست؟

در این نوع الگوریتم، کلید رمزگذاری و رمزگشایی داده‌ها یکسان است. (یعنی داده‌ها با همان کلیدی رمزگشایی می‌شوند که رمزگذاری شده‌اند) («کلید» را چیزی شبیه به «رمز» فرض کنید)

این، اولین نوع رمزگذاری بود که بشر تعریف کرد. ساده‌ترین و شناخته‌شده‌ترین الگوریتم در این دسته، الگوریتمی است که پادشاه ژولیوس سزار در حدود ۵۰ سال قبل از میلاد به کار می‌برد و به همین دلیل به آن Caesar cipher (رمزنگاری سزار) گفته می‌شود.

گاهی پادشاه سزار به فرمانداران خود در شهرهای دیگر نامه می‌فرستاد، راهزنان و جاسوسان در راه، پیک را می‌گرفتند و نامه را می‌خواندند و همه چیز لو می‌رفت، تا اینکه دانشمندان دربار، الگوریتم سزار را ابداع و استفاده کردند. در این الگوریتم، یک عدد (مثلاً ۴) به عنوان کلید در نظر گرفته می‌شد و سپس هر حرف الفبا به جای اینکه خودش در نامه نوشته شود، ۴ تا بعد از آن نوشته می‌شد. مثلاً اگر قرار بود بنویسند: Hamid، حرف H (و بقیه حروف را) ۴ تا به راست شیفت می‌دادند، پس می‌شد: Leqmh

هر چند این رمزنگاری تا مدت‌ها جواب می‌داد اما بعدها که احتمالاً الگوریتم به بیرون از دربار رسوخ کرد، خیلی راحت شکسته شد. طبیعتاً این الگوریتم‌ها هر روز پیشرفته‌تر و پیچیده‌تر شد تا کم‌کم رسیدیم به الگوریتم DES (مخفف Data Encryption Standard) که البته DES با اینکه بسیار پیچیده بود اما به خاطر یافتن چند نمونه داده‌ی رمزگذاری شده که با طی کردن مراحلی، بدون داشتن کلید به داده‌ی اولیه رسیدند، این الگوریتم زیرسؤال رفت.

اکنون دنیا در حال استفاده از الگوریتم AES (مخفف Advanced Encryption System) است که توسط دو رمزنگار بلژیکی به نام‌های «ژوآن دیمن» و «وینسنت رینمن» توسعه داده شد.

این الگوریتم‌ها تا زمانی که قرار است داده‌ها و رمز فقط نزد خود شما باشد و خودتان از آن استفاده کنید، بهترین گزینه هستند؛ اما مشکل، زمانی پیش می‌آید که شما بخواهید داده‌ها را برای یکی بفرستید و او بخواهد داده‌ها را رمزگشایی و استفاده کند! اینجاست که پای الگوریتم‌های نامتقارن وسط می‌آید.

الگوریتم رمزنگاری نامتقارن یا ASymmetric-key algorithm یا Public-key cryptography چیست؟

در این الگوریتم، کلید رمزگذاری با کلید رمزگشایی متفاوت است. در اصطلاح گفته می‌شود داده‌ها با کلید عمومی (Public Key) رمزگذاری می‌شوند اما با کلید خصوصی (Private Key) رمزگشایی می‌شوند. برای

درک مسأله، بیایید به چند صد سال قبل برگردیم. فرض کنید قرار است شما یک قطعه طلا را به یک شهر دیگر بفرستید به طوری که اگر در راه، راهزن‌ها حمله کردند، طلاها در امان باشد. تنها چیزی که در اختیار دارید، گاوصندوق‌های بسیار محکم است که با هیچ روشی به جز داشتن کلید امکان باز شدن آن‌ها نیست. شما چطور می‌خواهید این قطعه طلا را به آن شهر بفرستید؟

توجه داشته باشید که راهزن‌ها بسیار باهوش هستند! در همه مسیرها منتظر هستند تا طلاها را بدزدند.

فکر می‌کنید واقعاً آن زمان چطور این طلا را جا به جا می‌کردند؟

همانطور که می‌بینید، راه‌حل، خیلی ساده است: هر گاه قرار است یک نفر یک قطعه طلا به شهر دیگر بفرستد، ابتدا یک پیک به آن شهر می‌رود و یک گاوصندوق با قفلِ باز به شهر اول می‌آورد. کلیدِ قفل، نزد گیرنده می‌ماند. حالا طلا را در صندوق قرار می‌دهد و قفل را می‌بندد و به مقصد می‌فرستد. حالا دیگر اینطور نیست که کلید هم ارسال شود که دست راهزن‌ها بیفتد! به همین سادگی!

الگوریتم‌های رمزنگاری برگشت‌ناپذیر یا Irreversible Encryption Algorithms

در این نوع الگوریتم‌ها داده‌ای که رمزگذاری می‌شود، به هیچ وجه قابل برگشت به داده‌ی اولیه نیست. برای مثال Hash کردن یک فایل از این نوع الگوریتم است که پیشتر درباره آن صحبت شد. [2]

Hash چیست و چه کاربردی دارد؟

هش که گاهی اوقات به آن اثر انگشت هم گفته می‌شود، فرایندی است که یک داده با حجم زیاد را به یک مقدار کوتاه با طول ثابت تبدیل می‌کند. یعنی اگر شما فایلی با حجم ۱۰۰ مگابایت به این الگوریتم بدهید، به شما یک کد ۳۲ رقمی تحویل می‌دهد. حتی اگر یک داده بسیار کوتاه مثل «Hello» را هم به آن بدهید، باز یک کد ۳۲ رقمی تحویل خواهد داد.

بیشترین کاربرد Hash کردن، برای نگهداری از Password است. مثلاً Password حساب کاربران و مدیران سایت. برای استفاده از خدمات برخی از سایت‌ها باید حتماً حساب کاربری داشت، اما آیا مدیران سایت‌ها برای حفظ Password کاربران، فکری کرده‌اند؟ اگر سازنده سایت موارد ایمنی را رعایت نکرده باشد، Password کاربران را به همان شکل ذخیره می‌کند! کافیست سایت هک شود، هکر ایمیل و پسورد همه کاربران را دارد. کاربرانی که بیشترشان عادت دارند از یک Password مشابه برای حساب‌هایشان استفاده کنند.

اما برخی از سایت‌ها، پسورد کاربران را Encrypt می‌کنند. همان‌طور که پیشتر گفته شد، این روش برگشت‌پذیر است. کلیدی برای باز کردن این رمزگذاری وجود دارد که هکر با کمی زحمت آن را بدست خواهد آورد و رمزگشایی خواهد کرد. اما بهترین روشی که برای نگهداری از Password به کار گرفته می‌شود، Hash کردن Password است. چراکه به هیچ عنوان برگشت‌پذیر نیست. هنگامی که کاربر Password خود را وارد می‌کند، Password به صورت Hash شده در آمده و با Password موجود در پایگاه داده مقایسه می‌شود. اگر با هم برابر بودند، کاربر وارد حساب کاربری‌اش می‌شود و در غیر اینصورت مجاز نخواهد بود.

آیا رمزنگاری بر روی اطلاعات هارد دیسک و حافظه امکان‌پذیر است؟

با استفاده از قابلیت BitLocker ویندوز می‌توان اطلاعات هارد دیسک یا فلش مموری را رمزنگاری کرد. این قابلیت از ویندوز ویستا به بعد فعال شد. این رمزنگاری با استفاده از الگوریتم AES انجام می‌گیرد. [۳]

> **هشدار:** برای استفاده از این ویژگی ویندوز حتماً اطلاعات کافی کسب کنید و سپس اقدام به فعال‌سازی آن کنید. چراکه احتمال دارد اطلاعات مهم شما به دلیل اشتباه یا عدم رعایت نکات مهم از بین برود که متأسفانه غیرقابل برگشت خواهد بود.

رمزنگاری بر روی شبکه‌های بی‌سیم (Wi-fi) به چه شکل صورت می‌گیرد؟

از ابتدایی‌ترین روش رمزنگاری آغاز می‌کنیم. در سال ۱۹۹۹ یک پروتکل امن به نام WEP که مخفف Wired Equivalent Privacy [۶]است، توسعه داده شد. این اولین پروتکل امنیتی است که برای شبکه‌های بی‌سیم مورد استفاده قرار گرفت. پس از مدتی آسیب‌پذیری و ایمن نبودن این پروتکل مشخص شد. این پروتکل به راحتی قابل هک بود! به همین دلیل امروزه دیگر از WEP استفاده نمی‌شود.

پروتکل جدیدتری به نام WPA یا Wi-Fi Protected Access[۷] معرفی شد. WPA به دلیل به کارگیری رمزنگاری TKIP از قدرت بیشتری برخوردار بود. TKIP مخفف Temporal Key Integrity Protocol است. اما WPA هم کهنه شد و روش جدیدتری به نام WPA2 برای رمزنگاری معرفی شد. پروتکل WPA از TKIP برای رمزنگاری استفاده می‌کرد و در WPA2 الگوریتم متقارن AES به کار گرفته شد.

در روترهای جدید دیگر گزینه WEP وجود ندارد. این پروتکل به دلیل ضعف امنیتی منسوخ شد. همچنین در برخی از روترها علاوه بر گزینه WPA و WPA2 گزینه دیگری به نام WPA/WPA2 دیده می‌شود. این گزینه برای اتصال همزمان دستگاه‌های جدید و قدیمی به روتر است. به این شکل که دستگاه‌هایی که پیش از سال ۲۰۰۶ ساخته شده‌اند با استفاده از پروتکل WPA و دستگاه‌های جدیدتر با به کارگیری از پروتکل WPA2 به روتر متصل شوند. البته باید توجه داشته باشید که استفاده گزینه تلفیقی WPA/WPA2 شبکه شما را در معرض آسیب قرار می‌دهد، چراکه پروتکل WPA به اندازه WPA2 قدرتمند نیست. اگر همه دستگاه‌های شما مدرن هستند بهترین گزینه، WPA2 است که فقط از پروتکل AES برای رمزنگاری استفاده می‌کند.

در سال ۲۰۱۸ پروتکل WPA3 توسط سایت رسمی Wi-fi معرفی شد. این پروتکل با قدرت بالاتری از اتصالات و شبکه شما محاظت خواهد کرد.

تاکنون درباره پروتکل‌های امنیتی محافظت شده با رمز عبور صحبت کردیم. اما یک روش اتصال وجود دارد که به تایپ رمز عبور نیازی ندارد. این روش WPS نامیده می‌شود. WPS مخفف Wi-Fi Protected Setup است و WPS برای افرادی طراحی شده است که اطلاعات کمی درباره شبکه‌های بی‌سیم دارند تا به آسانی بتوانند دستگاه‌هایشان را به شبکه بی‌سیم متصل کنند.

---

[۶] محرمانگی معادل سیمی

[۷] دسترسی حفاظت‌شده به Wi-Fi

مثلاً برای اتصال یک چاپگر بی‌سیم به روتر، باید برای چند دقیقه دکمه WPS را نگه دارید تا این دو دستگاه به یکدیگر متصل شوند. توجه داشته باشید این روش به دلایل امنیتی به هیچ عنوان پیشنهاد نمی‌شود و بهتر است این ویژگی در روتر غیرفعال شود.

روش دیگر برای اتصال به روتر که از امنیت بالایی برخوردار است Access Control یا MAC Filter نام دارد. با استفاده از این گزینه می‌توانید مشخص کنید که چه دستگاهی به شبکه متصل یا دسترسی آن مسدود باشد. با بدست آوردن MAC دستگاه، می‌توانید آن را برای روتر تعریف کنید. تنها دستگاه‌هایی که MAC-شان در روتر تعریف شده است به شبکه دسترسی خواهند داشت. استفاده از MAC، امنیت را تضمین می‌کند.

HTTPS چیست؟

HTTPS ترکیبی از HTTP و SSL است. HTTP که همان پروتکل انتقال صفحات وب است. SSL مخفف Secure Socket Layer و به معنی «لایه‌ی میانیِ امن» است. (سوکت یعنی چیزی که بین دو چیز قرار گیرد. وقتی شما به یک کابل شبکه سوکت می‌زنید، سوکت بین کابل و پریز قرار می‌گیرد). SSL یک لایه امنیتی، بین مبدأ و مقصد است. الگوریتمی به نام RSA که یک الگوریتم نامتقارن به حساب می‌آید، دقیقاً به همان صورتی که در گذشته طلا را بین دو شهر منتقل می‌کردند، داده‌های حساس و طلاگونه‌ی کاربران را بین مبدأ و مقصد، به صورت امن منتقل می‌کند تا دست راهزنان نیفتد. الگوریتم RSA در سال ۱۹۷۷ توسط «رونالد ریوست»، «ادی شامیر»، و «لئونارد آدلمن» ابداع شد.

جهت دریافت HTTPS برای یک سایت باید از سازمان‌های معتبری که مجوز SSL سایت‌ها را پس از دریافتِ مشخصات و ضمانت‌های لازم، تأیید می‌کنند، اقدام نمود. یکی از مهم‌ترین سازمان‌ها، سازمان کومودو (Comodo) است. سایت‌ها برای اینکه اعتماد کاربران را جلب کنند مجوز SSL تهیه می‌کنند و سالانه هزینه‌ای بابت این مجوز پرداخت می‌کنند. سازمان‌هایی که مجوز SSL را صادر می‌کنند مشخصات صاحب سایت را برای ردگیری تخلفات احتمالی در اختیار دارند. هنگام ورود به سایت‌هایی که HTTPS-شان معتبر است، نوار آدرس مرورگر سبز رنگ خواهد شد.

اما چرا گاهی اوقات با اینکه سایت HTTPS دارد، نوار آدرس به رنگ قرمز نمایش داده می‌شود و گاهی هم با هشدار مرورگر روبه‌رو می‌شویم؟

اگر سایتی، از مجوز SSL غیررسمی استفاده کند و مشخصات‌اش در سازمان‌های معتبر ثبت نشود، مرورگر به رنگ قرمز درمی‌آید یا همانند فایرفاکس ابتدا یک صفحه حاوی هشدار نشان می‌دهد. سایت‌هایی که از HTTPS نامعتبر استفاده می‌کنند قابل اعتماد نیستند و احتمال کلاهبرداری وجود دارد. توجه داشته باشید که سایت‌هایی که از HTTPS استفاده می‌کنند، سرعت بارگذاری‌شان پایین‌تر است. چراکه استفاده از HTTPS یعنی حداقل دو رفت و برگشت بیشتر و کلی رمزنگاری و رمزگشایی اضافه‌تر در مبدأ و مقصد! و اینکه اگر مثلاً سرور مجوز ضعیف باشد، تمام سایت‌هایی که HTTPS خود را از آن‌جا گرفته‌اند هم کند می‌شوند و خلاصه کلی پردازش و روال بیشتر و این طبیعی است که سایت‌های HTTPS کندتر باشند. [4]

نماد اعتماد الکترونیکی چیست؟

نشانه‌ای است که منحصراً توسط مرکز توسعه تجارت الکترونیکی صادر شده و به کسب و کارهای مجازی مُجاز با هدف ساماندهی، احراز هویت و صلاحیت آن‌ها اعطا می‌گردد؛ این نماد پس از بررسی درگاه (وب‌سایت) و احراز هویت و صلاحیت مالک (حقیقی یا حقوقی) آن برای مدت یک سال صادر می‌گردد. مدیران سایت، اپلیکیشن و فروشگاه‌های اینترنتی برای فروش مجاز باید حتماً نماد اعتماد تهیه کنند.

اگر سایتی نماد اعتماد داشته باشد، آرم یا نماد در سایت نمایش داده می‌شود که با کلیک بر روی آن اطلاعات کسب و کار اعم از نشانی، تلفن و ایمیل نمایش داده می‌شود.

داشتن نماد الکترونیکی یا ای‌نماد این اطمینان را به کاربران می‌دهد که می‌توانند بدون مشکل خرید کرده و به صورت آنلاین پرداخت خود را انجام دهند، چرا که این نماد نشان می‌دهد این سایت فروشگاهی تحت نظارت است. [5]

هش‌تگ چیست؟

هش‌تگ‌ها کلمات یا عبارات چند کلمه‌ای هستند که محتوا را طبقه‌بندی می‌کنند و موضوعات را در شبکه‌های اجتماعی مثل توییتر، فیس بوک، اینستاگرام و... ردیابی می‌کنند. برای نوشتن یک هش‌تگ از نماد # استفاده می‌شود. این نماد پیش از عبارت اصلی هش‌تگ نوشته می‌شود.

کاربران شبکه‌های اجتماعی با استفاده از هش‌تگ می‌توانند پست‌ها و مطالب مورد علاقه‌شان را به سادگی پیدا کنند. هش‌تگ همچنین به یافتن افرادی که علایق‌شان شبیه یکدیگر است نیز کمک می‌کند تا یک گروه مجازی تشکیل دهند. [6]

نکاتی درباره وب‌گردی

اگر کسی در اینترنت، غیراخلاقی رفتار نکند، با او رفتار غیراخلاقی نخواهند کرد! استفاده از ابزارهای نوین کار بسیار سودمندی است، چرا که امکانات بهتر و بیشتری را با سرعت بالاتر در اختیار ما قرار می‌دهند ولی نتیجه استفاده نادرست از برخی از ابزارها چه خواهد بود؟ استفاده نادرست از گروها و یا کانال‌ها در شبکه‌های اینترنتی جز تلف کردن وقت، افسردگی، بی‌خوابی و ... نتیجه بهتری نخواهد داشت.

وب‌کم

در صورتی که قصد استفاده از وب‌کم را ندارید، حتماً آن را غیرفعال کنید. ساده‌ترین روش برای ایمن‌سازی این است که در صورت امکان وب‌کم از دستگاه شما جدا شود ولی وب‌کم لپ‌تاپ را نمی‌توان جدا کرد. روش دیگر ایمن کردن وب‌کم، پوشاندن وب‌کم با برچسب است. این کار ساده حتی توسط مارک زاکربرگ هم انجام شد!

توجه داشته باشید که هنگام استفاده از وب‌کم، چراغ هشداردهنده، روشن می‌شود. اگر شما در حال استفاده از وب‌کم نیستید این یعنی احتمالاً وب‌کم شما هک شده است. البته هکرها گاهی چراغ هشداردهنده وب‌کم را

هم قطع می‌کنند. اگر از وب‌کم استفاده نمی‌کنید و یا پس از استفاده از وب‌کم، می‌توانید آن را از بخش Device Manager غیر فعال کنید.

پسورد ویندوز

حتماً بر روی ویندوز دستگاه خود Password بگذارید. هنگامی که در حال استفاده از اینترنت هستید یعنی به یک شبکه بزرگ متصل شدید و اگر مسائل امنیتی رعایت نشود یا مشکلی در ISP [8]رخ دهد، اطلاعات شما به خطر خواهد افتاد. به کارگیری یک پسورد امن، می‌تواند از انتشار اطلاعات شما جلوگیری کند.

رعایت حریم شخصی هنگام تحویل رایانه یا موبایل به تعمیرکار

پیش از تحویل رایانه به تعمیرکار، حتماً اطلاعات شخصی‌تان را به یک هارد-دیسک اکسترنال یا فلش انتقال دهید، یا آن را بر روی DVD رایت کنید. حتی انتقال اطلاعات شخصی به پوشه‌های تو در تو با نام غیرمرتبط و پنهان کردن آن می‌تواند از دیده شدن اطلاعات جلوگیری کند. یا با استفاده از BitLocker یا برنامه‌های دیگر بر روی درایوهای رایانه‌تان رمز بگذارید. ولی انتقال اطلاعات راهکار بهتری است. برای تحویل موبایل به تعمیرکار، اطلاعات را به یک حافظه RAM یا رایانه انتقال دهید. البته در سیستم عامل جدید آندروید گزینه‌ای به نام Secure Folder وجود دارد که می‌توانید اطلاعات شخصی اعم از عکس، فیلم و ... را به آن انتقال دهید و با استفاده از اسکن چهره یا روش‌های دیگر به آن دسترسی داشت.

از ویژگی‌های جالب آن می‌توان به انتقال اپلیکیشن‌ها اشاره کرد. برای مثال اگر در یک شبکه اجتماعی حساب کاربری دارید، می‌توانید آن را به Secure Folder انتقال دهید. در صورتی که آن شبکه اجتماعی توسط کسی باز شود، امکان مشاهده حساب کاربری شما را نخواهد داشت و باید اطلاعات حساب کاربری را وارد کند.

روی هر لینکی کلیک نکنید

گاهی اوقات از منبعی نامعتبر لینک دانلود یک اپلیکیشن برای شما ارسال می‌شود. به هیچ عنوان بر روی چنین لینکی کلیک نکنید. اپلیکیشن‌ها از طریق مارکت‌های معتبر در دسترس هستند و توجه داشته باشید که از لحاظ امنیتی بررسی می‌شوند. کافیست نام یک اپلیکیشن را بدانید و آن را از مارکت معتبر دریافت کنید. گاهی لینک‌ها حاوی بدافزار یا جاسوس‌افزار هستند. که با کلیک بر روی آن‌ها متضرر خواهید شد.

نرم‌افزار امنیتی بر روی رایانه‌تان نصب کنید

امروزه که تقریباً همه رایانه‌ها به اینترنت متصل هستند، به کارگیری یک آنتی‌ویروس یا نرم‌افزار امنیتی بسیار مورد نیاز است. بسیاری از نرم‌افزارهای امنیتی نسخه رایگان هم دارند. توجه داشته باشید که همیشه به روز باشید.

[8] Internet Service Provider (رساننده خدمات اینترنتی)

در محل‌های عمومی رد پا، بر جا نگذارید!

یکی از خطرناک‌ترین موارد امنیتی همین است که شما در یک کافی‌نت و یا روی یک کامپیوتر عمومی، به طور مثال، ایمیل خودتان را چک کنید و نکات امنیتی را هم رعایت نکنید!

تمام مرورگرها در منوی Tools، گزینه‌ای با نام Clear Private Data یا Delete Browsing Data قرار داده‌اند. بعد از وبگردی در محل‌های عمومی، حتماً این گزینه را انتخاب کنید تا اطلاعات خصوصی شما حذف شود.

عدم استفاده از Wifi رایگان

مراقب باشید که موبایل را به کجا متصل می‌کنید. از اتصال موبایل یا تبلت به Wifi-های عمومی مثل Wifi رایگان و عمومی فرودگاه‌ها، کافی‌شاپ‌ها و ... بپرهیزید. این Wifi-ها بیشتر اوقات بدون مراقبت هستند و هکرها به سادگی به اطلاعات موبایل شما دست پیدا می‌کنند. در این موقعیت‌ها بهتر است از اینترنت همراه استفاده کنید. همین موضوع برای بلوتوث هم صدق می‌کند. برای مثال شما از اسپیکرهای بلوتوث استفاده می‌کنید و فراموش می‌کنید که بلوتوث موبایل را خاموش کنید. شما با خاموش نکردن بلوتوث یک راه دسترسی مناسب برای هکر فراهم کردید.

از مرورگر ایمن و به‌روز استفاده کنید

مرورگر نقش بسیار مهمی در اجرای درست یک سایت یا ابزارهای آنلاین دارد. همچنین تأمین امنیت وب‌گردی و رعایت حریم شخصی توسط مرورگر بسیار مهم است. مرورگر کهنه‌کار و دوست‌داشتنی فایرفاکس یکی از بهترین گزینه‌هاست. Google Chrome و Opera نیز از مرورگرهای خوب و کارآمد هستند.

اما آیا به راستی امنیت و حریم خصوصی به صورت کامل در مرورگرهای اینترنتی رعایت می‌شوند؟

متأسفانه، تنظیمات پیش‌فرض هیچکدام از مرورگرها واقعاً از حریم خصوصی شما محافظت نمی‌کند بنابراین باید به نکاتی توجه داشت تا این مهم انجام شود. شخصی‌سازی تنظیمات واقعاً ارزشمند است چرا که از ثبت عادت‌های وبگردی، علایق و چیزهای زیادی درباره زندگی شخصی شما جلوگیری می‌کند. [7] [8]

کدامیک از رفتارهای کاربران اینترنتی ثبت می‌شود؟

ردیاب‌های رسانه‌های اجتماعی

سایت‌های رسانه‌های اجتماعی مانند فیس‌بوک، توییتر و LinkedIn ردیاب‌هایی را در دیگر سایت‌ها جاسازی می‌کنند، بنابراین کارهای انجام شده و مشاهدات آنلاین شما را پیگیری می‌کنند. این کار برای نمایش تبلیغات هدفمند به کاربران انجام می‌شود.

استفاده از کوکی‌های ردیاب

کوکی‌ها فایل‌های متنی کوچکی هستند که هنگام مراجعه به یک سایت، بر روی سیستم کاربر ایجاد می‌شوند.

بسیاری از کوکی‌هایی که برای اهداف بازاریابی ساخته می‌شوند، داده‌های مربوط به کاربران مانند آدرس IP، موقعیت جغرافیایی، تنظیمات برگزیده، خریدها و گشت‌وگذار اینترنتی آن‌ها را ثبت می‌کنند. این‌ها، کوکی‌های ردیابی نامیده می‌شوند، زیرا آن‌ها رفتار کاربران اینترنتی را ردیابی می‌کنند. معمولاً از این اطلاعات برای بازاریابی هدفمند و نمایش تبلیغات به مشتریان استفاده می‌شود.

این کوکی‌ها چرا باید روی دستگاه ما قرار بگیرند؟

تقریباً همه وب‌سایت‌ها برای عملکرد بهتر بر روی دستگاه کاربران کوکی ایجاد می‌کنند ولی برخی از سایت‌های برای اهداف بازاریابی و ردیابی این کار را انجام می‌دهند. در اصل، این کوکی‌ها به عنوان یک حافظه عمل می‌کنند و به وب‌سایت این امکان را می‌دهد تا بازدیدکنندگان را از یکدیگر تشخیص دهد. هنگامی که یک کاربر اینترنتی، یک وب‌سایت را بارگیری می‌کند، وب‌سایت بررسی می‌کند که قبلاً کوکی‌هایی در مرورگر تنظیم کرده است یا خیر. در صورت وجود کوکی، مرورگر می‌تواند اطلاعات مربوط به تنظیمات زبان کاربر، مکان، واحد پول، اطلاعات حساب کاربری، فعالیت‌های قبلی، علایق و ... را که در کوکی ذخیره کرده است را بازیابی کند. به این ترتیب وب‌سایت می‌تواند برای کاربر خاص شخصی‌سازی شود. وب‌سایت می‌تواند گذرواژه، نشانی و مشخصات فاکتور کاربر را به خاطر بسپارد، بنابراین دیگر نیازی به وارد کردن دوباره همه این اطلاعات در هر بازدید یا هر بار خرید از آن وب‌سایت نیست. یا برای مثال دکمه‌های اشتراک‌گذاری مطلب در رسانه‌های اجتماعی که در برخی از سایت‌ها تعبیه شده است ممکن است برای تجزیه و تحلیل ساخته شده باشند. کوکی‌ها به مدیران سایت‌ها کمک می‌کند تا فعالیت کاربران را زیر نظر داشته و مورد تحلیل قرار دهند. این تحلیل می‌تواند باعث بهبود و بهینه‌سازی عملکرد سایت در فروش و ارائه خدمات شود.

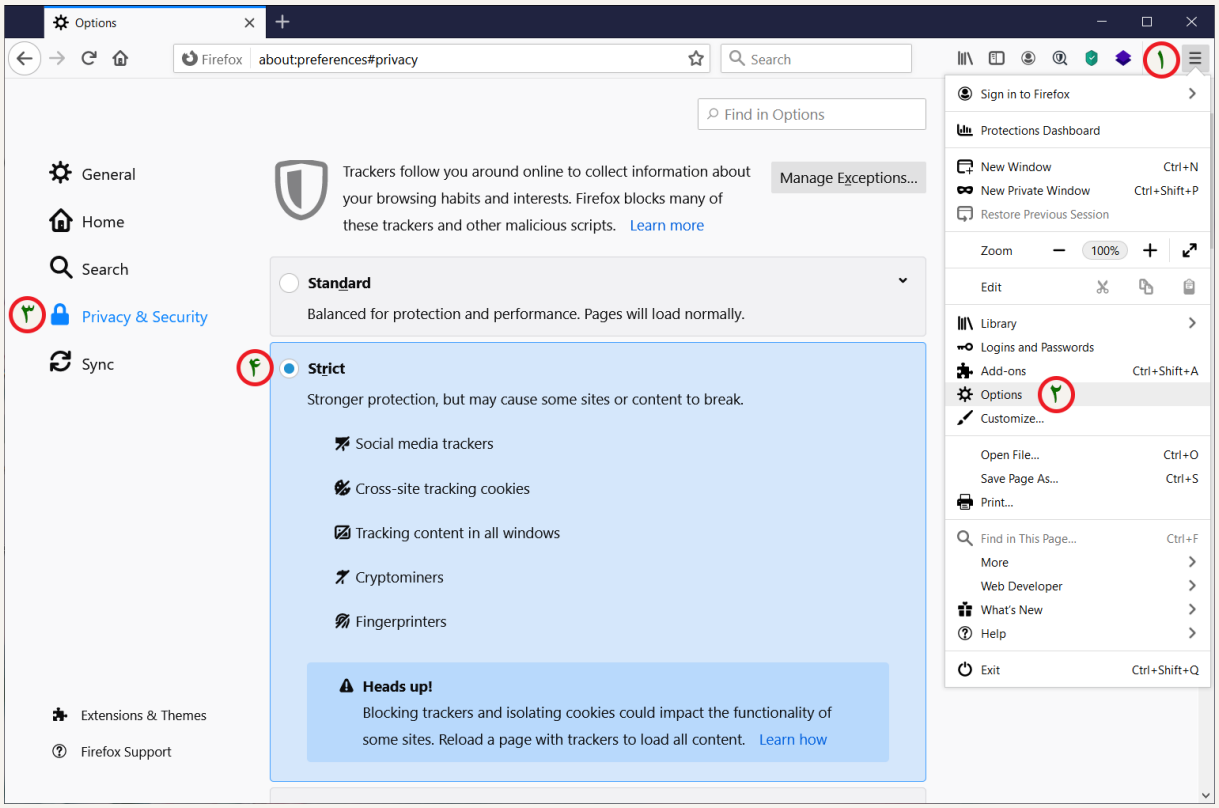
آیا کوکی‌های ردیابی بد هستند؟

کوکی‌های ردیابی نه خوب هستند و نه بد! آن‌ها فایل‌های متنی ساده‌ای هستند که به خودی خود هیچ کاری انجام نمی‌دهند و آسیبی به دستگاه شما نمی‌رسانند ولی به سادگی رفتار شما را در فضای مجازی ثبت می‌کنند و این خلاف آیین‌نامه عمومی حفاظت داده‌ها و حریم شخصی کاربران است.

علاوه بر این گاهی اوقات کاربران اینترنتی مورد حمله Cryptominer-ها قرار می‌گیرند. آن‌ها بدون رضایت شما، با استفاده از مرورگرتان عملیات Mining انجام می‌دهند. برای تولید رمزارز[9] معمولاً محاسبات پیچیده‌ای باید انجام شود و به انرژی زیادی هم نیاز است. بنابراین برخی از سودجویان برای فرار از هزینه برق و منابع محاسباتی از ظرفیت محاسباتی دستگاه شما برای این محاسبات پیچیده استفاده می‌کنند.

آیا راهی برای جلوگیری از موارد مطرح شده وجود دارد؟

بله، در مرورگر موزیلا فایرفاکس Options را کلیک کنید و در بخش Privacy & Security گزینه Enhanced Tracking Protection را بر روی Strict تنظیم کنید.



با فعال کردن این گزینه تبلیغات هدفمند Google و Amazon غیرفعال می‌شود.

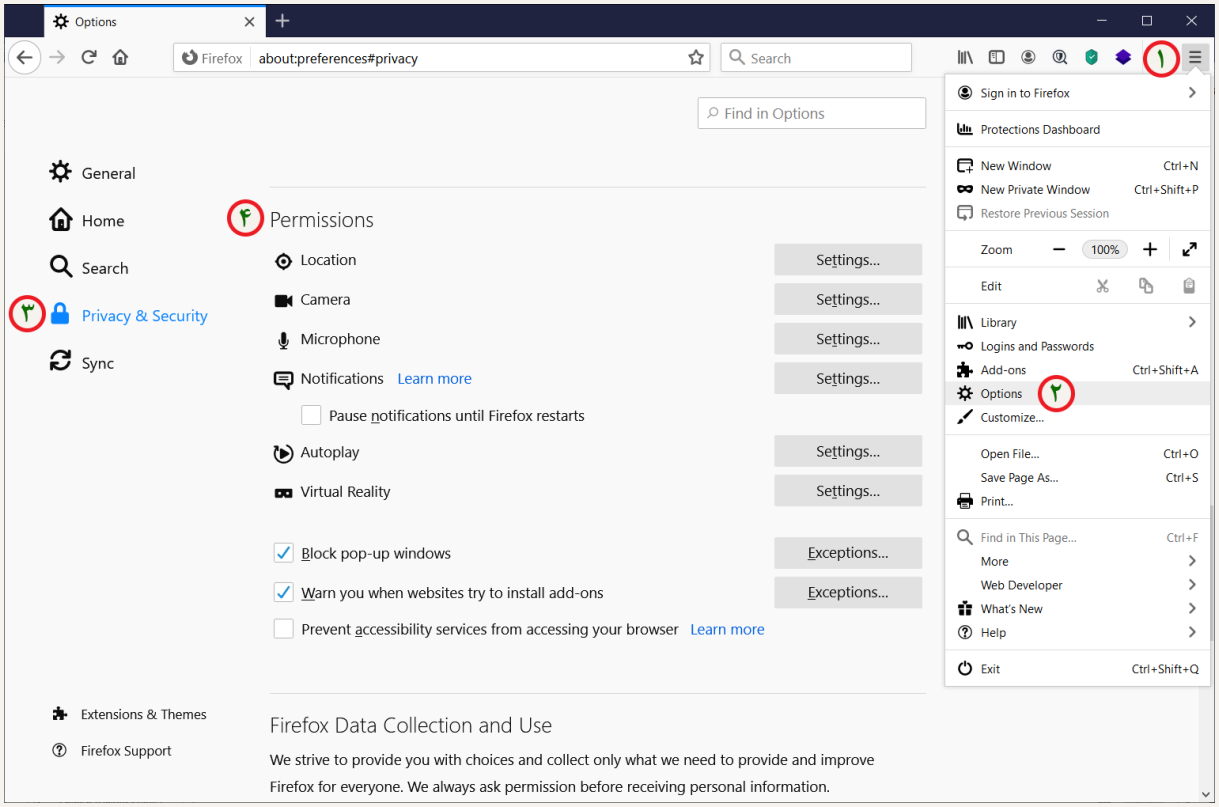
در بخش تنظیمات، Private Browsing Mode را فعال کنید.

این حالت تاریخچه و کوکی‌ها را ذخیره نمی‌کند. استفاده از این ویژگی در کافی‌نت‌ها و سایت‌های دانشگاهی پیشنهاد می‌شود.

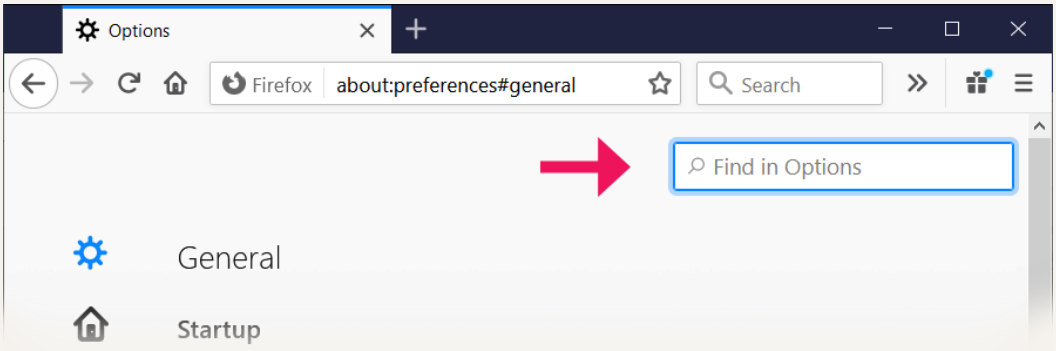
اگر مدتی است که از مرورگرتان استفاده می‌کنید و این تنظیمات را انجام نداده‌اید می‌توانید اطلاعات ذخیره شده را از بخش Cookies & Site Data و History پاک کنید.

[9] Cryptocurrency

مرورگرها به صورت پیش‌فرض امکان دسترسی به میکروفن، وب‌کم و موقعیت مکانی را دارند. به غیر از موارد خاص، نیازی به این دسترسی نیست. پس بهتر است این دسترسی‌ها را محدود کرد. از منوی تنظیمات گزینه Permissions را بیابید و محدودیت دسترسی را اعمال کنید.



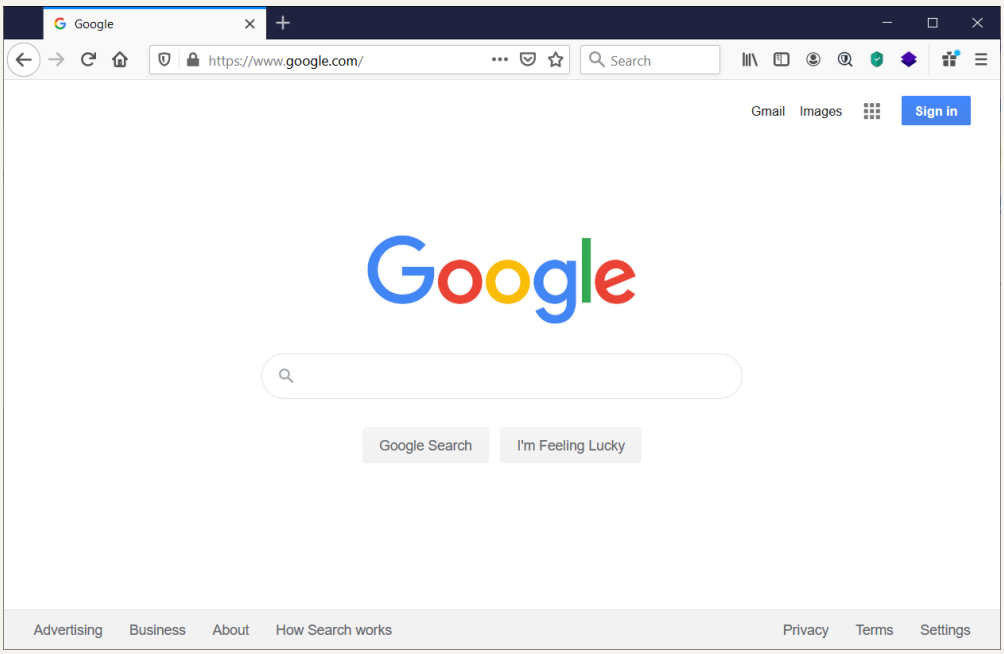
نکته: توجه داشته باشید که اگر گزینه‌ای را نیافتید، به سادگی می‌توانید آن را در کادر بالای مرورگر (Find in Options) جستجو کنید.



دایرکتوری و موتورهای جستجوگر

در گذشته و پیش از عمومی شدن موتورهای جستجوگر، دایرکتوری‌ها فهرستی از سایت‌ها را به صورت دسته‌بندی شده همراه با زیرشاخه‌های متنوع در اختیار کاربران قرار می‌دادند. در بیشتر دایرکتوری‌ها، به وب‌سایت اصلی لینک داده می‌شد و برای صفحه‌های جداگانه پیوندی وجود نداشت. یعنی شاید سایتی درباره موضوعات مختلفی مطلب ارسال می‌کرد ولی به صورت کلی، سایت در دسته «سودمند» قرار می‌گرفت و کاربر از جزئیات مطالب آگاه نمی‌شد. این موضوع موجب محدودیت در دسته‌بندی می‌شد.

دو روش برای یافتن اطلاعات در وب دایرکتوری وجود داشت: جستجو یا مرور. دایرکتوری‌های وب، پیوندها را در یک لیست ساختاریافته فراهم می‌کردند تا مرور راحت‌تر شود. بسیاری از دایرکتوری‌های وب با ارائه موتور جستجوگر برای مشاهده بهتر فهرست، جستجو و مرور را با هم ترکیب می‌کردند. بر خلاف موتورهای جستجو که ورودی‌هایش توسط Crawler-ها به صورت خودکار در پایگاه داده گردآوری می‌شوند، بیشتر دایرکتوری‌های وب به صورت دستی توسط ویرایشگرهای انسانی ساخته می‌شدند. ولی در حال حاضر بیشتر مردم از موتورهای جستجوگر استفاده می‌کنند.



اما موتور جستجوگر و برای مثال گوگل چطور کار می‌کند؟

صدها میلیارد صفحه برای نقشه‌برداری از وب برای ساخت فهرست جستجو تهیه شده است. کتابخانه‌های غول‌پیکری برای هر موضوع ساخته شده تا برای هر جستجو در دسترس باشند.

بیاید با هم «انار» را جستجو کنیم. با جستجوی این واژه، یافته‌های بسیاری نمایش داده می‌شود. از میوه انار گرفته تا شهری که انار نام دارد. اما واقعاً کسی حوصله دارد میان این همه لینک و توضیحات، موضوع دلخواه خود را بیابد؟ این موضوع واقعاً خسته‌کننده و ملال‌آور است. اینجاست که الگوریتم‌های رتبه‌بندی به مرحله اجرا درمی‌آیند. گوگل ابتدا تلاش می‌کند تا واژه جستجو شده را درک کند. حتی اگر دقیقاً نمی‌دانید که چه می‌خواهید یا غلط املایی دارید، این الگوریتم‌ها به یاری شما خواهند آمد تا مناسب‌ترین اطلاعات را در بالای یافته‌ها ببینید و آن را انتخاب کنید.

الگوریتم‌ها چگونه تصمیم می‌گیرند که چه چیز را در صفحه نخست نمایش دهند؟

صدها عامل در رتبه‌بندی نتایج جستجو وجود دارد که در اینجا به تعدادی از آن‌ها می‌پردازیم. سایت‌هایی در ابتدای یافته‌ها نمایش داده می‌شوند که از واژه جستجو شده در عنوان پست خود استفاده کردند و پست‌هایی که واژه را در متن استفاده کردند از اولویت پایین‌تری برخوردار هستند. سن دامنه سایت مهم است. بنابراین گوگل تاریخ انقضای یک دامنه را به عنوان یک فاکتور در ارزش و اعتبار سایت در نظر می‌گیرد. البته میزان اهمیتش چندان زیاد نیست. یکسان بودن نام دامنه سایت با کلمه کلیدی به گوگل کمک می‌کند که بتواند حوزه کاری شما را تشخیص دهد، البته اگر سایت باکیفیت و حرفه‌ای باشد چراکه برای سایت‌های ضعیف این مورد لحاظ نمی‌شود. همچنین استفاده از دامنه رسمی یک کشور، رتبه سایت را بالا می‌برد. مثلاً استفاده از پسوند ir رتبه سایت را در ایران افزایش می‌دهد.

روش دیگر شرکت Google برای رتبه‌بندی صفحات وب در نتایج جستجوگر-اش، استفاده از الگوریتمی به نام PageRank یا به اختصار PR است. PageRank به نام یکی از بنیانگذاران گوگل، Larry Page نام‌گذاری شده است. PageRank روشی برای اندازه‌گیری اهمیت صفحات وب‌سایت است. PageRank با شمارش تعداد و کیفیت پیوندهای یک صفحه کار می‌کند تا تخمین تقریبی از اهمیت وب‌سایت کسب کند. فرض اساسی این است که وب‌سایت‌های مهم‌تر احتمالاً لینک‌های بیشتری را از وب‌سایت‌های دیگر دریافت می‌کنند. در حال حاضر، PageRank تنها الگوریتمی نیست که Google برای نمایش نتایج جستجو از آن استفاده می‌کند، ولی این الگوریتم شناخته‌شده‌ترین الگوریتمی است که توسط این شرکت مورد استفاده قرار گرفته است.

عامل دیگر، موقعیت مکانی است یعنی جایی که جستجو را از آنجا انجام می‌دهید. چراکه مثلاً امکان دارد شما از شهر ساوه درباره جشنواره سالانه «انار» جستجو می‌کنید. اما اگر شما در شهر کرمان بودید، احتمالاً به دنبال اطلاعاتی درباره شهر «انار» در این استان بودید.

عامل دیگر صفحاتی هستند که به تازگی درباره یک موضوع، مطلبی را منتشر کرده‌اند. اغلب این صفحات اطلاعات دقیق‌تری در این خصوص دارند به ویژه اگر آن خبر به سرعت در حال گسترش باشد. البته، هر سایتی در وب سعی نمی‌کند سودمند باشد. دقیقاً همانند ربات‌های تماس‌گیر در موبایل یا هزرنامه‌ها در ایمیل شما، تعداد زیادی سایت، فقط برای کلاهبرداری وجود دارد. مثلاً اگر در سایتی تعداد ۴۰۰ بار واژه «انار» ذکر شده باشد، این دلیل بر این نیست که مطلب مورد نیاز شما پیدا شده است. گوگل زمان زیادی را صرف تشخیص سایت‌های کلاهبرداری و حذف آن‌ها از فهرست یافته‌هایش می‌کند. به هر حال هنگامی که شما در حال جستجو با استفاده از موتور جستجوگر گوگل هستید، گوگل با به کارگیری الگوریتم‌های پیچیده به دنبال درک مفاهیم بیشتری است. تا با سرعت بیشتری و مدت زمان کمتری اطلاعات مفیدتری را به صورت منظم در اختیار کاربران قرار دهد.

در این بین، Alexa هم می‌تواند در زمینه رتبه‌بندی یا اعتبارسنجی به کاربران و مدیران سایت‌ها کمک کند. با نصب Toolbar و یا با استفاده از سایت Alexa می‌توان به اطلاعات بسیار سودمندی دست یافت. الکسا با تحلیل داده‌های آماری و ارائه گزارش، به یاری مدیران سایت‌ها و کسب‌وکارهای اینترنتی می‌آید.

الکسا میزان محبوبیت یک سایت را نمایش می‌دهد، سایت‌های مشابه یا مرتبط را معرفی می‌کند، با استفاده از Wayback Machine دسترسی به کپی دقیقی از یک وب‌سایت در زمان‌های گذشته را فراهم می‌سازد و عباراتی که باعث ایجاد ترافیک برای سایت شده‌اند را در اختیار کاربران قرار می‌دهد.

آمار رایگان با محدودیت در اختیار کاربران قرار می‌گیرد و در صورت پرداخت هزینه، اطلاعات جامع‌تری را می‌توان دریافت کرد. الکسا به مدیران سایت‌ها کمک می‌کند تا آن دسته از کلمات کلیدی که باعث بالا رفتن ترافیک سایت‌های رقیب می‌شوند را پیدا کنند تا آن‌ها را برای پیشبرد اهداف سایت‌شان به کار ببرند. مقایسه معیارهای رقابتی از جمله نحوه ورود کاربران به سایت و کلمات کلیدی و ... انجام می‌شود. نمایش آمار ترافیک وب‌سایت، از جمله رتبه الکسا، معیارهای رتبه‌بندی، منابع ارجاع و موارد دیگر بررسی می‌شود. ارائه گزارش دیدگاه مخاطبین از جمله موضوعاتی که مخاطبین شما بیشتر به آن‌ها اهمیت می‌دهند و کلمات کلیدی آن‌ها را جستجو می‌کنند از دیگر خدمات الکسا است. از دیگر سرویس‌های رایگان الکسا می‌توان به نمایش ۵۰۰ سایت برتر جهانی، نمایش سایت‌های برتر در کشورهای مختلف و سایت‌های برتر دسته‌بندی شده بر اساس موضوع اشاره نمود.

سرویس ایمیل

زندگی دیجیتال، ارتباطات را هم تغییر داد. با روی کار آمدن اینترنت و عمومی شدن آن، ایمیل یا پست الکترونیک جای نامه و فکس را گرفت. شرکت‌ها و سازمان‌های مختلف برای کم کردن هزینه‌های مربوط به چاپ، ارسال یا فکس نامه، از ایمیل استفاده می‌کنند. سرویس‌های رایگان بسیاری برای ارائه خدمات ایمیل وجود دارد. از معروف‌ترین سرویس‌ها می‌توان به Gmail، Yahoo، Outlook و iCloud اشاره کرد.

Gmail سرویس ایمیل رایگانی است که از سوی گوگل ارائه می‌شود. Gmail ساده، ایمن و کاربر پسند است. با داشتن حساب کاربری Gmail، ۱۵ گیگابایت فضای ذخیره‌سازی در اختیار خواهید داشت. البته با داشتن یک حساب Gmail خدمات دیگری از جمله به گوگل درایو دسترسی خواهید داشت. همچنین کاربران سیستم‌عامل آندروید برای دسترسی به اپلیکیشن‌های گوگل‌پلی حتماً باید یک حساب کاربری Gmail داشته باشند.

سرویس ایمیل رایگان Yahoo در ایران محبوبیت بسیاری دارد. محبوبیت یاهو بیشتر به خاطر پیام‌رسان یاهو است که البته این سرویس در سال ۲۰۱۶ به صورت کامل از دسترس خارج شد.

سرویس ایمیل مایکروسافت که به نام اوت‌لوک شناخته می‌شود و از امکانات آن می‌توان به فضای ۵ گیگابایت برای ذخیره پست‌های الکترونیکی، اقدامات امنیتی، فناوری ای‌جکس و یکپارچگی با سرویس‌های ویندوز لایو مسنجر، ویندوز لایو اسپیس، تقویم و تماس‌ها اشاره کرد.

سرویس iCloud به عنوان مرکز هماهنگ کنندهٔ داده‌ها برای ایمیل، تماس‌ها، تقویم، بوک‌مارک‌ها، یادداشت‌ها، فهرست کارها و سایر داده‌ها فعالیت می‌کند و ۵ گیگابایت فضای قابل ارتقا ابری ارائه می‌دهد. این سرویس برای ارائه خدمات به دارندگان محصولات شرکت Apple پیاده‌سازی شده است.

حفظ امنیت حساب‌های کاربری

برای داشتن حساب‌های کاربری باید از رمزهای امن استفاده نمود، به ویژه زمانی که یک حساب کاربری به صورت آنلاین در دسترس است. چرا که هر کسی می‌تواند به آن دسترسی داشته باشد. شما هر روز برای استفاده از رایانه محل کار، ایمیل و ... باید پسوردتان را وارد کنید. ساده‌ترین راه انتخاب یک پسورد ساده و یکسان برای همه آن‌هاست. ولی آیا این کار امنیت دارد؟

این می‌تواند بسیار مشکل‌زا باشد. چراکه به سادگی قابل حدس است. برنامه‌هایی هستند که کافیست اطلاعاتی از شما داشته باشند تا پسورتان را حدس بزنند و به حساب شما وارد شوند. با پیدا شدن پسورد، افراد سودجو به همه حساب‌های شما دسترسی خواهند داشت. بهترین راه، ساخت یک پسورد سخت و غیرقابل حدس است. اولین چیزی که به فکر شما می‌رسد ممکن است استفاده از نام حیوان خانگی، تاریخ تولد، نشانی یا شماره تلفن باشد. ولی این موارد، بسیار آسان پیدا می‌شوند. بنابراین برای ساخت گذرواژه از اطلاعاتی که مربوط خودتان است استفاده نکنید. خوشبختانه روش‌هایی برای بدست آوردن پسوردهای به یادماندنی اما دشوار وجود دارد.

یکی از روش‌ها این است که حروف ابتدایی کلمات یک جمله را یاد بسپاریم. آن جمله می‌تواند یک مصرع شعر، یادآوری یک خاطره یا نام یک ترانه باشد. این پسورد چیزی نیست که به راحتی قابل حدس باشد. از واژه‌های حتی به ظاهر سخت لغت‌نامه برای ساخت پسورد استفاده نکنید، یک کامپیوتر می‌تواند خیلی سریع کلمات لغت‌نامه را آزمایش کند و پسورد را پیدا کند. اما هنوز می‌توانیم با استفاده از حروف بزرگ، اعداد و کاراکترهای ویژه، پسوردمان را قوی‌تر کنیم. سعی کنید از پسوردی استفاده کنید که حداقل ۸ کاراکتر داشته باشد. ولی هنوز هم خطر در کمین است، البته در صورتی که آن را یادداشت کنید. گاهی اوقات یک پسورد، از کاغذهای دور ریخته شده لو می‌رود. حتی پسورد را به افراد خانواده هم نباید گفت. توجه داشته باشید که هنگام ورود پسورد، کسی بالای سر شما ایستاده نباشد. پسورد را نباید به صورت تلفنی یا از طریق پیامک به کسی اعلام کرد. حتی هنگام دریافت ایمیلی که درخواست پسورد می‌شود باید احتیاط کرد. مسأله بعدی در هنگام استفاده از ایمیل، عدم پاسخگویی به ایمیل‌های عجیب، غریب یا به اصطلاح Spam است.

اسپم یا هرزنامه چیست؟

به طور خلاصه، Spam نام یک نوع کنسرو بوده است که در زمان جنگ جهانی، در جبهه‌ها غذای هر روز سربازان بوده است! (مانند کنسرو لوبیا که در سربازی غذای همیشگی سربازهاست!) آنقدر Spam به خورد سربازهای بیچاره می‌دادند که هر وقت اسم Spam می‌آمد از آن به عنوان «یک چیز زیاد و ناخواسته» یاد می‌کردند. به مرور به ایمیل‌های تبلیغاتی Spam گفته شد. (گاهی نیز کلمه Bulk به معنی دسته‌ای و گروهی به این نوع ایمیل‌ها اطلاق می‌شود)

Spammer کیست؟

به کسی که Spam می‌فرستد در اصطلاح اسپمر گفته می‌شود. اسمپرها معمولاً با هدف تجاری شروع به ارسال روزانه میلیون‌ها ایمیل می‌کنند. طبق آمار، ۸۸ تا ۹۲ درصد ایمیل‌هایی که در اینترنت رد و بدل می‌شود، اسپم است! طبق این آمار، آمریکا بیشترین اسپم‌های جهان را ارسال می‌کند. (حدود ۲۰ درصد اسپم‌ها منبعش آمریکاست، ۹.۹ درصد چین، ۶.۴ درصد روسیه، ۶.۳ درصد برزیل و ...)

اسپمرها چگونه ایمیل ما را به دست می‌آورند؟

روش‌های مختلفی برای به دست آوردن ایمیل‌های کاربران وجود دارد؛ برای نمونه به برخی از آن‌ها و روش جلوگیری از آن‌ها اشاره می‌کنم:

۱- ایجاد یک سایت جعلی و درخواست از کاربران برای ثبت نام در آن:

مثلاً خیلی از قربانیان اسپم با چنین پیامی روبه‌رو شده‌اند: تبریک می‌گوییم! شما ۹۹۹۹۹۹۹۹۹ نفری هستید که این فایل را دانلود کرده‌اید، به خاطر این اتفاق جالب، به شما یک جایزه تعلق گرفته است. اینجا کلیک کنید تا جایزه‌تان را دریافت کنید. کاربر هم با اشتیاق تمام اطلاعات و مشخصات خود از جمله آدرس ایمیل و شماره تلفن و ... را در آن فرم وارد می‌کند. اسپمر به سادگی ایمیل و مشخصات را بدست آورده و اسپم ارسال می‌کند.

روش جلوگیری: در هر سایتی سریعاً ثبت نام نکنید، اگر لازم شد، با ایمیل دوم خود ثبت نام کنید:

یکی از بهترین راه‌ها این است که شما یک ایمیل ثانویه برای ثبت نام در سایت‌هایی که ثبت نام در آن‌ها الزامی است داشته باشید و اگر فکر می‌کنید ایمیل‌هایی که از آن سایت خواهد رسید برای شما مهم نیست، با آن ایمیل ثانویه در آن‌ها عضو شوید. مثلاً من یک ایمیل با آدرس x@gmail.com دارم و یکی هم با آدرس x2@gmail.com که معمولاً با x2 در سایت‌هایی که برای دانلود یک فایل نیاز به ثبت نام دارند عضو می‌شوم...

۲- خیانت سایت‌هایی که در آن‌ها ثبت نام کرده‌اید و فروش ایمیل‌های کاربران:

اکثر اوقات ایمیل شما از این طریق دست اسپمرها می‌افتد. یعنی شما در یک سایت (به خصوص خارجی) ثبت نام می‌کنید که از امکاناتش استفاده کنید، او هم کل ایمیل‌های دیتابیسش را به ازای دریافت یک هزینه وسوسه‌کننده در اختیار اسپمرها قرار می‌دهد. متأسفانه حتی برخی سایت‌های ایرانی نیز گهگاه از این کارها می‌کنند! به طور مثال فقط کافی‌ست کلمه «فروش ایمیل ایرانی» را جستجو کنید تا مثلاً با ۵ هزار تومان، ایمیل کل مردم ایران را به شما بفروشند!

پس داشتن ایمیل دوم را فراموش نکنید.

۳- روبات‌های ایمیل‌یاب:

یکی از شایع‌ترین و آسان‌ترین و کم‌هزینه‌ترین روش‌ها برای یافتن ایمیل، استفاده از برنامه‌هایی است که ما در اصطلاح آن‌ها را روبات می‌نامیم. فقط کافی‌ست آدرس یک سایت را به این روبات بدهید تا او تمام صفحات آن سایت را لینک به لینک پیمایش کند و تمام متن آن صفحات را تحلیل کند. در آن‌ها تنظیم شده است که اگر به یک متن با ساختار x@y.z رسیدی، آن‌را در دیتابیس ذخیره کن...

روش جلوگیری: ایمیل خودتان یا دیگران را روی صفحات وب قرار ندهید یا به این صورت قرار دهید:

تا جایی که ممکن است ایمیل خودتان یا دیگران را روی صفحات وب قرار ندهید. دقت کنید که ایمیل اشخاص هم مانند شماره موبایل آن‌ها نزد شما امانت است! نباید به امانت خیانت کنید!

به هم ریختن ساختار: اما اگر به هر حال، قرار شد یک ایمیل را روی یک صفحه وب قرار دهید، ساختار آن‌را به بهم بریزید یعنی به صورت x@y.z قرار ندهید.

مثلاً: info [at] MySite.ir

این به خاطر دور زدن آن روبات ایمیل‌یاب است.

اما این هم خیلی ساده است که با تعریف ساختارهایی مثل x[at]y.z و x[@]y[.]z و x[at]y[dot]z و ... را هم برای روبات معرفی کرد که به دیتابیس اضافه کند.

این روش یک ایراد دارد و آن اینکه متأسفانه خیلی از کاربران نمی‌فهمند چرا شما آدرس ایمیل‌تان را آن‌طور نوشته‌اید! فکر می‌کنند واقعاً ایمیل شما همانطور است و به آن ایمیل پیغام می‌دهند و گلایه می‌کنند که ایمیل من را جواب ندادید!

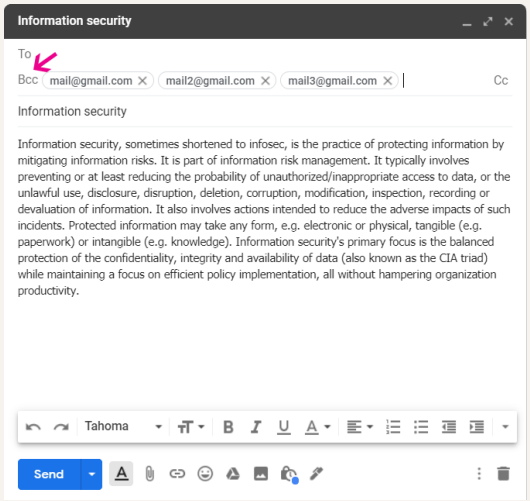
قرار دادن به صورت عکس: روش دیگر و شاید بهتر این است که شما ایمیل خود را به صورت عکس روی وب قرار دهید.

اما بد نیست بدانید که برخی روبات‌ها قادرند با تکنولوژی OCR[10] متن داخل عکس را نیز استخراج کنند و ایمیل را از آن بیرون بکشند. بنابراین شاید بخواهید روی عکس ایمیل‌ها یک سری Noise ایجاد کنید تا تشخیص آن‌ها توسط OCR سخت شود.

یک روش بهتر این است که ایمیل خود را اینطور روی وب قرار دهید: مثلاً: ایمیل من: آی.دی x در سرویس gmail.com است.

۴- خیانت شما به دوستان‌تان یا دوستان‌تان به شما!:

یکی از دلایل پخش شدن ایمیل یک نفر در اینترنت، این است که شما یا دوستان‌تان از یک مطلب خوشتان می‌آید و می‌خواهید به چند نفر ایمیل کنید. سپس ایمیل همه را در فیلد TO در فرم ارسال ایمیل قرار می‌دهید. در این صورت همه‌ی کسانی که ایمیل را دریافت می‌کنند می‌توانند ایمیل بقیه را ببینند! یعنی خیلی راحت ایمیل افراد را پخش کرده‌اید!



روش جلوگیری: باید ایمیل‌ها را در فیلد BCC درج کنید.

وقتی قرار است یک ایمیل را به چند نفر ارسال کنید، نباید آدرس‌ها را در کادر To بنویسید! همه آدرس‌ها باید در کادر BCC قرار گیرند. اگر آدرسها در کادر To نوشته شوند، همه افرادی که به آنها ایمیل ارسال شده است، میتوانند ببینند این ایمیل به چه ایمیل‌های دیگری فرستاده شده است. حالا فرض کنید این ایمیل برای یک کاربر فرصت‌طلب ارسال شود! خیلی راحت، در عرض یک شب، چند صد ایمیل صاحبدار و معتبر بدست آورده

[10] Optical character recognition (نویسه‌خوان نوری)

است و فرصت مناسبیست برای ارسال ایمیل‌های گروهی تبلیغاتی یا همان Spam (اسپم) که دردسری بزرگ برای کاربران شده است. اما اگر در کادر BCC آدرس‌ها را بنویسید، هر کاربر فقط می‌تواند ایمیل خود را ببیند و به آدرس‌های دیگری که این ایمیل برایشان ارسال شده، دسترسی ندارد. [9]

CAPTCHA چیست؟

اسپم‌ها فقط به ایمیل ختم نمی‌شود. گاهی افرادی برای تبلیغات به بخش نظرات یک وب‌سایت حمله می‌کنند. به این شکل که متنی را برای معرفی سایت یا محصول خود که خیلی از اوقات هیچ ارتباطی با مطلب سایت ندارد را در بخش نظرات آن ارسال می‌کنند. گاهی اوقات ربات‌ها مطالب ساختگی و جعلی را به صورت هدفمند در بخش نظراتِ یک فروشگاه اینترنتی منتشر می‌کنند و باعث سردرگمی کاربران می‌شوند. خیلی از ارسال‌ها می‌تواند حاوی لینک‌های مخرب باشد.

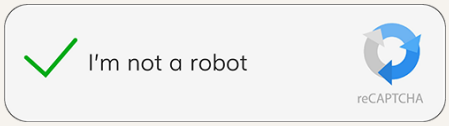
اما برای جلوگیری از این نوع اسپم چه باید کرد؟

یکی از روش‌های مرسوم و بازدارنده بکارگیری CAPTCHA [11]است.

Captcha مخفف «آزمون همگانی کاملاً خودکارشده تورینگ برای مجزا کردن انسان و رایانه» است.

CAPTCHA چیست؟

احتمالاً تاکنون با تصویری از حروف و اعداد که عمداً کج و ناواضح رسم شده‌اند برخورد کرده‌اید و از شما خواسته شده تا آن را به شکل صحیح خوانده و بادقت در یک جعبه متن وارد کنید. اگر چنین است شما با یک کپچا سر و کار داشته‌اید. البته کپچا انواع مختلفی دارد. برای مثال گاهی اوقات از شما خواسته می‌شود تا به یک معادله ریاضی پاسخ دهید یا از شما خواسته می‌شود تا کلماتی که نوشته‌شان کج و کوله است را تایپ کنید. در این مدل کپچا، متن برای افراد نابینا خوانده می‌شود تا آن را تایپ کنند. یکی دیگر از انواع کپچا، شناسایی تصاویر است. مثلاً چند تصویر به کاربر نشان می‌شود تا مورد خاص را تشخیص دهد.



گوگل از سال ۲۰۱۴، کپچایی را طراحی کرده است که در فضای اینترنت بسیار گسترش پیدا کرده است. احتمالاً پیغام «من ربات نیستم» برای شما هم نمایش داده شده است. کافیست این پیغام را تیک‌دار کنید تا گوگل متوجه شود شما انسان یا ربات هستید. گوگل با بررسی حرکت ماوس، کوکی‌ها و آدرس IP، ربات یا انسان را تشخیص می‌دهد. برای مثال ربات‌ها بیشتر اوقات مرکز کادر را برای تیک‌دار کردن کلیک می‌کنند.

[11] Completely Automated Public Turing test to tell Computers and Humans Apart

کاربرد کپچا به اینجا ختم نمی‌شود. بسیاری از ربات‌ها برای خرید آنلاین ساخته شده‌اند که در کسری از ثانیه می‌توانند همه بلیت‌های یک کنسرت یا خودروهای پیش‌فروش را بخرند. ولی با وجود کپچا، می‌توان جلوِ ربات‌ها را گرفت. برخی ربات‌ها به منظور ورود به بخش مدیریتی یک وب‌سایت ساخته می‌شوند، کپچا برای مقابله با این حملات هم به یاری مدیران سایت‌ها می‌آید. البته دانش جلوگیری از هک شدن فقط برای مدیران سایت‌ها نیست و همه کسانی که با اینترنت سروکار دارند باید از آن مطلع باشند.

Phishing چیست؟

یک کاربر اینترنتی باید از کلاهبرداری‌های اینترنتی آگاه باشد و راه‌های مقابله با آن را بداند. مثلاً Phishing[۱۲]، یکی از شایع‌ترین و خطرناک‌ترین روش‌های کلاهبرداری است. در این نوع حملات، هکر سایتی کاملاً شبیه سایت مورد نظر کاربر می‌سازد. برای مثال؛ کلاهبرداران سایت یکی از بانک‌ها را با نشانی مشابه طراحی می‌کنند و به روش‌های مختلف (مثلاً به بهانه شارژ ارزان) به آن سایت هدایت می‌کند. کاربر با دیدن ظاهر و نشانی سایت، احساس می‌کند وارد سایت اصلی شده است و بنابراین اعتماد می‌کند و اطلاعات محرمانه خود را در آن سایت وارد می‌کند اما در حقیقت اطلاعات را در اختیار هکر قرار داده است.

یکی از رایج‌ترین روش‌های فریب کاربران، از طریق ایمیل صورت می‌گیرد. ایمیل‌هایی که به نظر می‌رسد از یک منبع قانونی هستند اما اینگونه نیستند. به عنوان مثال در ایمیلی که به شما ارسال شده است ادعا می‌شود حسابی که در بانک دارید به خطر افتاده و باید سریعاً گذرواژه‌تان را از طریق ایمیل به بانکدار ارسال نمایید! البته باید این را بدانید که هیچ بانکی از طریق ایمیل به شما اخطار نخواهد داد و درخواست ارسال رمز نخواهد کرد. در ضمن هیچگاه اطلاعات شخصی‌تان را به هیچ‌کس ارسال نکنید مگر اینکه آن را به طور کامل می‌شناسید.

کلاهبرداران ترفندهای بسیاری را به کار می‌برند تا اعتماد شما را جلب کنند، مثلاً از دامنه‌های مشابه استفاده می‌کنند.

☒ mail@p0stbank.com

☒ mail@wwwp0stbank.com

وقتی فرستنده ایمیل ناشناس و مشکوک است روی هیچ لینکی از ایمیل کلیک نکنید. اگر قصد تغییر رمز اینترنت بانک خود را دارید مستقیماً نشانی اینترنتی آن را وارد کرده و سپس اقدام به تغییر رمز نمایید. در متنِ خیلی از ایمیل‌هایی که برای کلاهبرداری از کاربران اینترنتی ارسال می‌شود، احساس ترس، شادی و فوریت وجود دارد و شما را به صفحاتی ارجاع خواهند داد که بارها آن‌ها را دیده‌اید و از آن استفاده کرده‌اید و به همین دلیل هنگام مراجعه دوباره به این صفحه‌ها توجه زیادی نمی‌کنید که آیا این صفحه اصلی است یا ساختگی است.

پس دوباره یادآوری می‌کنیم که به URL[۱۳] صفحات دقت کنید. صفحات امن با HTTPS بارگذاری می‌شوند و ابتدای نام سایت یک قفل سبز رنگ قرار دارد.

---

[۱۲] رمزگیری، فیشینگ یا تله‌گذاری

[13] Uniform Resource Locator (مکانیاب منبع یکسان)

DDoS چیست؟

هکرها فقط به اطلاعات بانکی یا شخصی کاربران رضایت نمی‌دهند گاهی اوقات از کاربران اینترنتی برای مقاصد شومی بهره می‌برند. شاید در گشت‌وگذارهای اینترنتی با پیغام «رایانه شما آلوده است» روبه‌رو شده باشید که از شما بخواهد برنامه‌ای را دانلود کنید. همیشه به چنین آگهی‌هایی مشکوک باشید و به هیچ عنوان برنامه یا نرم‌افزاری را از منابع نامعتبر دانلود نکنید.

اما نصب این برنامه‌ها از سوی کاربران چه سودی برای کلاهبرداران دارد؟

علاوه بر بدست آوردن اطلاعات شخصی کاربران، آن‌ها را به اعضای ارتش ناخواسته برای اهداف شوم کلاهبرداران تبدیل می‌کند. آیا درباره حمله Distributed Denial Of Service یا DDoS چیزی شنیده‌اید؟

گاهی اوقات حمله‌هایی عمدی به وب‌سایت‌ها صورت می‌گیرد که مانع دسترس‌پذیری آن‌ها می‌شود. هکرها با ایجاد بارِ بیش از اندازه به وب‌سایت‌ها، آن‌ها را از دسترس خارج می‌کنند. هکرها با استفاده از رایانه‌های آلوده که به Botnet معروف هستند، کار حمله به سایت‌ها را انجام می‌دهند. بدافزارها از طریق سایت‌های نامعتبر، رسانه‌های اجتماعی و ایمیل پخش می‌شوند و رایانه خیلی از کاربران مبتدی، جزو ارتش Botnetها خواهد شد. Botnetها مانند ارتش، قابل کنترل بوده و توسط هکر فرماندهی می‌شوند تا حجم بسیار بالایی از ترافیک را بر روی وب‌سایت هدف ایجاد کرده و آن را از دسترس خارج کنند. برخی از هکرها، Botnetها را با قیمتی ارزان در اختیار کسانی که قصد حمله DDoS دارند قرار می‌دهند. این حملات گاهی جنبه سیاسی دارند و گاهی رقابتی هستند.

Brute Force چیست؟

حملات هکرها به سایت‌های اینترنتی انواع مختلفی دارد و فقط به DDoS ختم نمی‌شود. یکی دیگر از این حملات Brute Force یا «حمله جستجوی فراگیر» نام دارد. حمله Brute Force تلاش برای شکستن رمز عبور یا نام کاربری یک وب‌سایت یا به طور کلی یک حساب کاربری است. این روش قدیمی هنوز هم بین هکرها محبوب است. بسته به طول و پیچیدگی رمز عبور، شکستن آن از چند ثانیه تا سال‌ها زمان می‌برد. برخی هکرها ماه‌ها و حتی گاهی سال‌ها سیستم خاصی را مورد هدف قرار می‌دهند. البته حدس زدن رمز عبور یک کاربر یا سایت مدت زمان زیادی طول می‌کشد، بنابراین هکرها ابزارهایی را برای این کار در دست دارند. هکرها دیکشنری بزرگی از واژگان و رمزعبورهای پرکاربرد کاربران اینترنتی را در اختیار دارند که در این نوع حمله از آن بهره می‌برند و البته ابزارهایی که کمی از دیکشنری‌ها پیچیده‌تر عمل می‌کنند و به جای لیست کردن واژگان، رمزعبورهایی که دارای اعداد و نماد هستند را پیشنهاد می‌دهند.

نگران نباشید، راه‌های بسیاری برای پیشگیری از این حمله وجود دارد. نخست اینکه، همانطور که پیش‌تر توضیح داده شد حتماً از رمزعبور قوی استفاده کنید. برای ساخت حساب در وب‌سایت خود از استفاده نام‌های کاربری معمول همانند Admin جداً خودداری نمایید. در شبکه‌های اجتماعی «تایید دومرحله‌ای» را فعال کنید. مدیران سایت‌ها باید از Captcha استفاده کنند تا ربات‌ها به سادگی مشغول هک سایت نشوند. همچنین در صورتی‌که ورود به حساب کاربری با چندین بار تلاش ناموفق روبه‌رو بود، حساب مسدود شود. مدیران سایت‌ها کاربران را به داشتن پسورد طولانی و قوی اجبار کنند.

Session Hijacking چیست؟

هکرها روش‌های بسیار مختلفی برای سوءاستفاده از یک حساب کاربری پیشِ رو دارند. Session Hijacking یا «نشست‌ربایی» یکی دیگر از این روش‌هاست. در نظر بگیرید که وارد حساب کاربری‌تان در یک وب‌سایت می‌شوید. با ورود شما، یک Session یا Cookie موقت در مرورگر شما تنظیم می‌شود تا به خاطر آورد که وارد وب‌سایت شدید و در حال استفاده از آن هستید. هکرها می‌کوشند تا این Session یا Cookie را از شما بدزدند. هکر برای دزدیدن آن‌ها، کاربر را ترغیب به کلیک بر روی لینک‌های مخرب می‌کنند و با کلیک بر روی اینگونه لینک‌ها هکر به سادگی Session یا Cookie را به سرقت می‌برند. حالا هکر می‌تواند با همان شناسه وارد حساب کاربری شما خواهد شد. در صورتی که هکر موفق شود، هر کاری می‌تواند انجام دهد. مثلاً اگر وارد حساب بانکی شما شود، می‌تواند پول جابه‌جا کند یا با ورود به حساب کاربری شما در یک فروشگاه اینترنتی به اطلاعات هویتی شما دسترسی داشته باشد یا شخصی با یافتن اطلاعات شما و برای منتشر نکردن اطلاعات هویتی‌تان، درخواست پول می‌کند.

Sniffing چیست؟

روش دیگر، Sniffing[۱۴] است. البته Sniffing همیشه برای اهداف بد مورد استفاده قرار نمیبرند. برای مثال گاهی اوقات برای عیب‌یابی یک شبکه از Sniffer استفاده می‌شود. یا مدیران برای کنترل ترافیک شبکه از ابزارهای Sniffing بهره می‌گیرند. مدیران می‌توانند پهنای‌باند گره‌های مختلف را زیرنظر داشته باشند تا در صورتی که گره‌ای استفاده سنگینی از شبکه انجام داد، شناسایی شود و اقدامات مناسب صورت گیرد. اما مجرمان، این روش را برای سوءاستفاده از کاربران یک شبکه به کار می‌گیرند. وقتی داده‌ها در شبکه انتقال می‌یابند، اگر بسته‌های داده رمزگذاری نباشند، اطلاعات درون بسته‌ها می‌توانند Sniff شوند. انگیزه خرابکاران از این کار، بدست آوردن نام کاربری وگذرواژه، جعل یا سرقت اطلاعات بانکی، جاسوسی از طریق ایمیل و شبکه‌های اجتماعی، یافتن شهرت و یا سرقت هویت کاربران است.

SQL Injection چیست؟

یکی از روش‌هایی که بین هکرها متداول است و مدیران سایت‌ها باید اهمیت ویژه‌ای برای آن قائل باشند حمله SQL Injection است. این حمله به معنای تزریق به پایگاه داده است. ابتدا درباره SQL کمی صحبت می‌کنیم.

پیشتر اطلاعات بر روی کاغذ و کاغذها در پرونده و پرونده‌ها در یک کمد بایگانی می‌شدند. اما امروزه آن‌ها را به صورت آنلاین ذخیره می‌کنیم. این ذخیره‌سازی روی چیزی انجام می‌شود که ما آن را پایگاه داده یا DataBase می‌نامیم. SQL[۱۵] زبانی است که به برقراری ارتباط بین ما و پایگاه داده کمک می‌کند. پایگاه داده مانند یک انبار است. داده‌ها شبیه یک پرونده هستند و جداول همانند کمدهایی که پرونده‌ها در آن‌ها قرار گرفتند. برای استفاده از این داده‌ها باید مجوز داشت. سامانه‌های تحت شبکه یا وب این دسترسی را برای کاربران مجاز فراهم می‌کنند.

---

[۱۴] حمله بویش

[15] Structured Query Language

تزریق به پایگاه داده نوعی فن تزریق کد است که هکر به اطلاعات ذخیره در پایگاه داده دسترسی پیدا کند. به این صورت که نفوذگر با یک سری دستورهای SQL، عملیاتی را متفاوت با عملیات عادی موردنظر سازنده وب‌سایت در پایگاه داده آسیب‌پذیر انجام می‌دهد. این آسیب‌پذیری جزو ده آسیب‌پذیری رایج نرم‌افزارهای وب در سال ۲۰۰۷ و ۲۰۱۰ برشمرده شده‌است. در صورتی که سازنده یک سامانه اینترنتی امنیت بخش ورود به بخش مدیریت سامانه را تأمین نکرده باشد به آسانی و با ساده‌ترین روش تزریق کدهای مخرب هک خواهد شد.

اما انگیزه مهاجمان از این کار چیست؟

۱- آن‌ها می‌توانند حساب‌های کاربری جعلی بسازند.
۲- پایگاه داده را به صورت کامل برای خود ذخیره کنند.
۳- از انجام یک سری از امور جلوگیری کنند.
۴- اطلاعات ذخیره شده در پایگاه داده را پاک کنند یا تغییر دهند.

XSS چیست؟

تزریق کدهای مخرب همیشه به منظور SQL Injection صورت نمی‌گیرد گاهی اوقات تزریق اسکریپت در جهت دور زدن کنترل‌های دسترسی مورد استفاده و بهره‌برداری قرار می‌گیرد. البته حملات XSS نسبت به SQL Injection آسیب‌های کمتری دارد. XSS مخفف Cross-site Scripting که برای جلوگیری از اشتباه با یکی از زبان‌های طراحی سایت، علائم اختصاری آن را از CSS به XSS تغییر دادند. در حمله XSS تلاش می‌شود تا یک اسکریپت نامطلوب از لایه‌های امنیتی احتمالی یک وب‌گاه گذر داده شود و همراه با کدهای اجرایی اصلی وب‌گاه دوباره به سمت کاربر بازگردانده شود. در نتیجه مرورگر این کد جدید را با این فرض که متعلق به وب‌گاه است اجرا می‌کند و تغییراتی در ظاهر و کارکرد وب‌گاه حاصل می‌شود.

انجمن‌های گفتگو یا فروم‌ها، message boards و سایت‌هایی که بخش نظرات دارند در معرض خطر این حمله هستند. چراکه هکرها می‌توانند از طریق فیلدهای ورودی اسکریپت موردنظرشان را تزریق کنند.

منابع

[۱] "امنیت اطلاعات," ۷ ۸ ۲۰۲۰. [درون خطي]. Available: https://fa.wikipedia.org/wiki/امنیت_اطلاعات.

[۲] د. ح. نیرومند, "توضیحی در مورد الگوریتم‌های رمزنگاری," آفتابگردان, ۱۸ ۱۲ ۱۳۹۳. [درون خطي]. Available: https://aftab.cc/article/1261.

[۳] "BitLocker چیست و به چه کار می آید؟," آفتابگردان، ۲۳ ۰۱ ۱۳۹۳. [متصل]. Available: https://aftab.cc/modules.php?name=Forums&file=viewtopic&t=5559.

[٤] د. ح. نیرومند, "HTTPS چیست و چگونه کار می‌کند؟," آفتابگردان, ۱۸ ۱۲ ۱۳۹۳. [درون خطي]. Available: https://aftab.cc/article/1261.

[٥] "درباره نماد," ای‌نماد, [درون خطي]. Available: https://enamad.ir/About.

[٦] د. ح. نیرومند، "هش تگ (Hash Tag) یعنی چی؟،" آفتابگردان، ۰۷ ۱۱ ۱۳۹۸. [متصل]. Available: https://aftab.cc/article/1650.

[۷] د. ح. نیرومند، "برخی نکات مهم امنیتی برای وبگردی امن‌تر،" آفتابگردان، ۰۶ ۰۱ ۱۳۸۸. [متصل]. Available: https://aftab.cc/article/790.

[۸] د. ح. نیرومند، "نکات امنیتی جهت حفظ اطلاعات خصوصی - قسمت دوم،" آفتابگردان، ۱۰ ۰۲ ۱۳۸۸. [متصل]. Available: https://aftab.cc/article/796.

[۹] د. ح. نیرومند، "اسپم چیست؟ چرا ایمیل ما اسپمی می‌شود؟ +راه‌های جلوگیری از Spam،" آفتابگردان، ۱۹ ۰۷ ۱۳۹۳. [متصل]. Available: https://aftab.cc/article/1230.