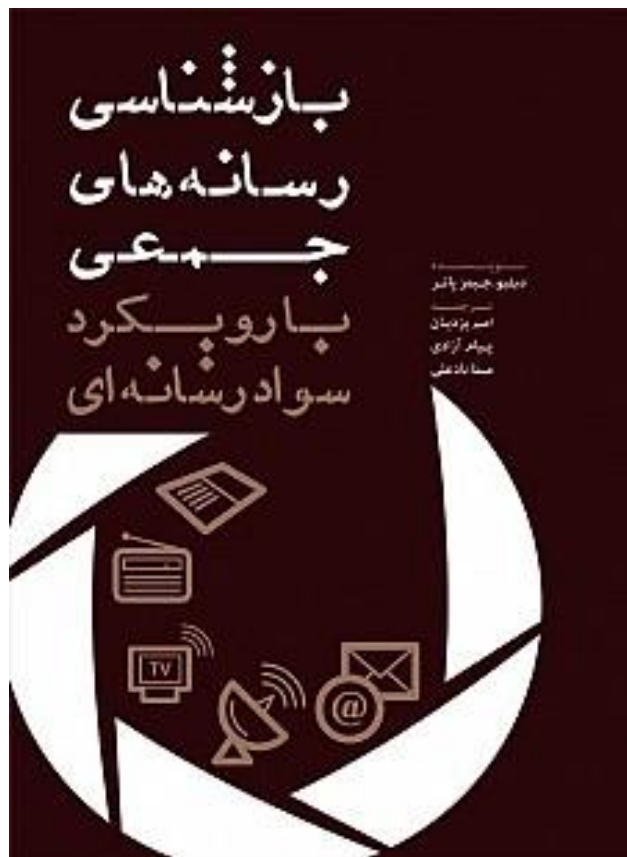


حریم خصوصی



برگرفته از کتاب بازشناسی رسانه‌های جمعی با رویکر سواد رسانه‌ای

نوشته دلیو جیمز پاتر

ایده اصلی

- شرکت‌ها، آژانس‌های دولتی و حتی افراد، بسیار بیشتر از آنچه تصور می‌کنید، درباره شما می‌دانند. دانستن این نکته که اطلاعات مربوط به شما چگونه به دست می‌آید و فروخته می‌شود، بسیار مهم است. شما از این طریق می‌توانید سطوحی از حریم خصوصی خود را باز پس بگیرید
- با در نظر گرفتن فن‌آوری جدید رایانه‌ها و اینترنت، تفکر درباره مرزبندی حریم خصوصی، بیش از پیش اهمیت دارد؛ چون امروزه تجاوز به حریم خصوصی، بیش از پیش برای افراد و شرکت‌ها آسان شده است. از آنجا که رایانه‌ها و اینترنت جدید هستند، بیشتر افراد تجربه کافی در به کارگیری این رسانه ندارند و درک نمی‌کنند که این کانال ارتباطاتی تا چه اندازه برای سوء استفاده، باز و در دسترس است. (در اوایل دهه ۱۹۸۰، کمتر از ۰.۵٪ از خانواده‌های آمریکایی یک رایانه داشتند، ولی در طول ۲۰ سال، این آمار به دو سوم از خانواده‌های آمریکایی افزایش یافت)

حریم خصوصی ما

- همهٔ ما اطلاعاتی شخصی داریم که می‌خواهیم آن‌ها خصوصی بمانند و آن‌ها را با افرادی خاص به اشتراک نگذاریم. برای مثال، می‌خواهیم دوستانمان شماره تلفن، نشانی و رایانامه ما را داشته باشند، ولی مایل نیستیم اطلاعات تماس خود را در اختیار بازاریاب‌های تلفنی و دیگر آگهی‌دهندگان قرار دهیم بیشتر ما هنگام تعامل با بنگاه‌های تجاری نیز چنین انتظاری از آن‌ها داریم؛ یعنی هرگاه چیزی از یک مغازه یا سایت اینترنتی می‌خریم، انتظار داریم این فعالیت میان ما و بنگاه تجاری باقی بماند و با دیگر بنگاه‌های تجاری خارج از این معامله، به اشتراک گذاشته نشود. چنین چیزی معمولاً رخ نمی‌دهد. بنگاه‌های تجاری تمام اطلاعات مربوط به شما را جمع‌آوری می‌کنند و به دیگر بنگاه‌های تجاری می‌فروشند
- با وجود رایانه‌ها، بازاریاب‌های اینترنتی، رایانامه، و تلفن، به طور پیوسته به حریم خصوصی ما تجاوز می‌شود.

تجاوز به حریم خصوصی

■ در این بخش، شش روش مورد استفاده برای تجاوز به حریم خصوصی مطرح می‌شود:

1. زیر نظر گرفتن
2. فروش اطلاعات
3. سرقت هویت افراد
4. کنترل رایانه شخصی دیگران
5. ویروسی کردن
6. ارسال هرزنامه

■ در بیشتر این موارد، بدون اجازه و آگاهی شما به حریم خصوصی‌تان تهاجم می‌شود.

زیر نظر داشتن

- اطلاعات زیادی در اینترنت وجود دارد که زیر نظر گرفتن فعالیتهای دیگران را آسان می‌سازد. برای مثال، بسیاری از خانم‌ها، تاریخ‌های احتمالی را در گوگل جست‌وجو می‌کنند. مردم از فن‌آوری ماهواره‌های آن‌لاین برای دید زدن حیاط دیگران استفاده می‌کنند، با دسترسی به سایت‌های شبکه‌ اجتماعی به اطلاعات شخصی دست می‌یابند و ...
- بنگاه‌های تجاری فعالیتهای افراد را زیر نظر دارند. بانک‌ها و شرکت‌های کارت اعتباری تمام هزینه‌های شما را دنبال می‌کنند.
- وسیله‌ای که زیر نظر گرفتن فعالیتهای شما را ممکن می‌سازد، **کوکی** نام دارد. خدمات‌دهندگان اینترنتی، بازاریاب‌ها و دیگر شرکت‌ها، با قرار دادن فایل کوچکی به نام کوکی در حافظه رایانه شما، یک فن‌آوری برای زیر نظر گرفتن فعالیتهای شما در اختیار دارند. در حالی که فروشگاه‌های آن‌لاین به شما می‌گویند که برای کارآمدتر کردن خریدتان از کوکی‌ها استفاده می‌کنند.

فروش اطلاعات

- برخی از شرکتها با استفاده از کوکیها جای داده شده در رایانههای مشتریان خود، اطلاعات را جمعآوری می کنند و با تشکیل داده بنیادها، آنها را به دیگر شرکتها می فروشند. برای مثال، سایت **toysrus.com** متهم بود که بدون اطلاع رسانی به مصرف کنندگان، اطلاعات شخصی خریداران را در اختیار یک شرکت تحلیل داده قرار داده است.
- بسیاری از شرکتها، فروش اطلاعات مشتریان را منبعی برای درآمدزایی بیشتر در نظر می گیرند.

هرزنامه

- افرادی که از سرویس رایانامه استفاده می‌کنند، می‌دانند که نشانی رایانامه ظاهراً عمومی است.
- آگهی‌دهندگان آگهی‌های تجاری خود را به رایانامه افراد می‌فرستند. البته گاهی اوقات نیز شاید از دریافت اطلاعاتی که کالاهای خوب خوشحال شویم. در بیشتر موارد زیر بمباران پیام‌هایی قرار می‌گیریم که هرگونه کالایی را تبلیغ می‌کنند و ما هیچ علاقه‌ای به آن‌ها یا توانایی مالی خرید آن‌ها را نداریم.
- این پیام‌های ناخواسته، رایانامه ما را پر می‌کنند و وقت زیادی از ما می‌گیرند. به رایانامه‌های ناخواسته، هرزنامه می‌گویند.
- بیش از ۱۵ میلیارد مورد هرزنامه به طور روزانه ارسال می‌شود.
- شرکت‌های امریکایی امروزه بیش از ۸۰۰ میلیون دلار برای جلوگیری از ارسال هرزنامه هزینه می‌کنند.
- در سال ۲۰۰۷، تقریباً ۶۰٪ از کل رایانامه‌های ارسالی، هرزنامه بوده است.

سرقت هویت

- با ظهور اینترنت، خطر سرقت هویت نیز مطرح شد. این جرم از ناتوانی مصرف‌کنندگان در نظارت بر گستره دسترسی به اطلاعات حساس و شیوه حفاظت از آنها ناشی می‌شود. کلاهبرداران حرفه‌ای می‌توانند با فریب دادن شما به قسمت‌های مهم اطلاعات شما دست یابند و هویت شما را سرقت کنند.
- برخی از کلاهبرداران حرفه‌ای حتی به برقراری تماس با شما برای دستیابی به اطلاعات شخصی شما نیاز ندارند؛ چون آنها با نفوذ به پایگاه‌ها اطلاعاتی بزرگ، اطلاعات میلیون‌ها نفر را یک‌جا می‌دزدند. بیش از آنچه تصور کنید، چنین اتفاقی رخ می‌دهد. تنها در سال ۲۰۰۵، به دلیل وجود شکاف‌های امنیتی، اطلاعات شخصی ۵۰ میلیون نفر به خطر افتاد.

کنترل رایانه شخصی دیگران

- یکی از روش‌ها وقتی است که فردی رایانه شخصی را به کنترل خود درآورد و در فعالیتی شبکه‌ای با دیگران مرتبط می‌سازد. از این‌رو، بازاریاب‌ها از این شبکه به عنوان منبعی برای ارسال میلیون‌ها پیام به نام نشانی آی. پی. شما استفاده می‌کنند.
- یکی دیگر از روش‌ها این است که با استفاده از یک مرورگر، کنترل صفحه شخصی شما را در اختیار می‌گیرند یا موتور جست‌وجوگری را در رایانه شخصی شما جای می‌دهند. این مرورگر یا موتور جست‌وجوگر به گونه‌ای طراحی شده است که شما را فقط به وبسایت‌های تبلیغاتی خاصی رهنمون می‌سازد.

آلوده‌سازی

- هکرهایی وجود دارند که تنها به قصد از بین بردن فایل‌های رایانه‌ای، ویروس‌های رایانه‌ای می‌سازند. انگیزه انتشاردهندگان ویروس، سرقت اطلاعات شخصی یا هدایت شما به سمت سایتی خاص برای بهره‌وری اقتصادی نیست، بلکه در عوض، انگیزه این افراد صرفاً در راستای اهداف خراب‌کارانه است.
- ویروس‌های رایانه‌ای به شدت انتقال‌پذیر هستند. هرگاه فایل آلوده در رایانه‌ای جدید باز شود، ویروس هم باز می‌شود. وقتی رایانه آلوده به یک شبکه متصل شود، ویروس نیز به آن شبکه وصل می‌شود. از آنجا که بیشتر ویروس‌ها مخفی باقی می‌مانند، بیشتر کاربران نیز از وجود و انتقال ویروس آگاه نمی‌شوند مگر زمانی که دیگر خیلی دیر شده است.

حفاظت از حریم خصوصی

- افکار عمومی به شدت به نفع حریم خصوصی است. با این حال، وضع قوانینی که مرز میان امور عمومی و خصوصی را کاملاً مشخص کند، کاری دشوار برای قانون‌گذاران است. با وجود چند قانون در این زمینه، محکومیت و مجازات خاطیان، بی‌نهایت دشوار است. تا زمانی که قانون‌گذاران بتوانند هم‌گام با فن‌آوری‌ها پیش بروند، فشار واقعی بر دوش ماست تا به عنوان افراد این جامعه از خود محافظت کنیم.

افکار عمومی

- در دهه‌های اخیر، حریم خصوصی به موضوعی بسیار مهم برای افکار عمومی در ایالات متحده تبدیل شده است. لو هریس در یک نظرسنجی دریافت که درصد امریکایی‌هایی که نگران موضوع حریم خصوصی خود هستند، از ۳۴٪ در سال ۱۹۷۰، به ۹۰٪ در سال ۱۹۹۸ افزایش یافته است.
- پروژه زندگی امریکایی و اینترنت گزارش داد که ۸۴٪ از مردم امریکا در مورد امکان دسترسی دیگران به اطلاعات شخصی خود «بسیار نگران» یا «تا اندازه‌ای نگران» هستند. با دسترسی هر چه بیشتر مردم امریکا به اینترنت و گزارش مستمر رسانه‌های خبری درباره اتهام‌های جدید شرکت‌های اینترنتی در حوزه تجاوز به حریم خصوصی، این موضوع (حریم خصوصی) به دغدغه اصلی سیاست‌گذاری در عرصه اینترنت بدل شده است.

قوانین مشتری مدار در برابر تجارت مدار

- یکی از بزرگ‌ترین دغدغه‌های پیش روی قانون‌گذاران در بررسی موضوع حریم خصوصی، تعیین میزان نظارتی است که مصرف‌کنندگان می‌توانند بر حریم خصوصی خود داشته باشند.
- در قوانین مشتری‌مدار آنچه پیش فرض انگاشته می‌شود، حریم خصوصی است و مصرف‌کنندگان برای اعطای مجوز به آگهی‌دهندگان برای ارسال پیام یا ضبط اطلاعات در کوکی‌ها باید اقداماتی را انجام دهند.
- در مقابل، در قوانین تجارت‌مدار، وضع به گونه‌ای است که فعالان اقتصادی اجازه دارند هرگونه اطلاعاتی را ارسال کنند و کوکی‌ها را بسازند تا زمانی که مصرف‌کننده از آن‌ها بخواهد چنین کاری را متوقف سازند. فعالان تجاری به شدت طرفدار گزینه تجارت‌محور هستند؛ چون هر کاری که بخواهند، می‌توانند انجام دهند.

قوانین نظارتی

- به موجب مجموعه‌ای از قوانین، استفاده از نام و نشانی اشخاص در فهرست ارسال نامه بدون اجازه آن‌ها ممنوع است.
- از دلایل اعمال نه‌چندان جدی این قوانین آن است که پی‌گیری قانونی افراد خطاکار هزینه‌بردار است و حتی وقتی افراد قانون‌شکن شناسایی شوند، به سادگی از کشور خارج می‌شوند و از مجازات می‌گریزند. برای مثال، اولین مجازات اقتصادی برای یکی از ارسال‌کنندگان هرزنامه در اکتبر ۲۰۰۳ در کالیفرنیا صادر شد که به موجب آن، شرکت بازاریابی پی. دبلیو به پرداخت دو میلیون دلار جریمه به دلیل ارسال رایانامه‌های ناخواسته یا گمراه‌کننده محکوم شد. البته محکومان این پرونده از کشور گریختند تا قانون در مورد آن‌ها اعمال نشود.

خلاصه

- گروه‌های صنعتی در تلاش هستند تا حق ارسال پیام‌های تبلیغاتی به آدرس رایانامه شما؛ جای دادن کوکی‌ها در رایانه شما؛ فروش نامحدود آدرس رایانامه شما و ... را برای خود محفوظ می‌دارند.
- وقتی این فعالان اقتصادی، گزینه‌هایی را برای محدودسازی استفاده از اطلاعات شما در اختیارتان قرار می‌دهند، در واقع، توپ را به زمین شما انداخته‌اند تا به آن‌ها نه بگویید، به جای آنکه خود زحمت کسب اجازه از شما را بر عهده بگیرند.
- امروزه، با در نظر گرفتن ابزارهای تکنولوژیکی رایج، حریم خصوصی افراد به شدت محدود شده است. شرکت‌های تجاری بسیاری، اطلاعات مربوط به شما را گردآوری می‌کنند و به دیگر شرکت‌ها می‌فروشند.