جلسه هفتم : امنیت برای شبکه‌های اجتماعی Social networking

تهیه کننده: نیما راشدان

جلسه هفتم : امنیت برای شبکه‌های اجتماعی Social networking

مثال‌ها و نکاتی برای آموزش تهدیدهای نوین در شبکه‌های اجتماعی

تهدید امنیتی بسیار ساده است :

سامان استاتوس خود در فیس‌بوک را به شکل زیر تغییر می‌دهد :

Its finally holiday time again! I'm on my way to Palm Springs…

از دانشجویان سوال کنید چگونه چنین استاتوس ساده‌ای می‌تواند یک تهدید جدی امنیتی باشد؟

15% از شهروندان ایالات متحده به سادگی در شبکه‌های اجتماعی می‌نویسند که در خانه حضور ندارند. 35% از جوانان 18 تا 34 سال موقعیت جغرافیایی‌شان را در شبکه‌های اجتماعی منتشر می‌کنند.

سارقان منازل از استاتوس افرادی که به مسافرت رفته اند سوء استفاده می‌کنند، آنان اکنون با امکاناتی نظیر Google Street View به راحتی می‌توانند جوانب منزل قربانی و موانع فیزیکی اطراف آن را از قبل مطالعه کنند

اندکی آمار برای آشنایی با وضعیت امنیتی فیس‌بوک

- 4 میلیون کاربر فیس‌بوک روزانه اسپم دریافت می‌کنند.
- حدود 20% فیدهای خبری فیس‌بوک حامل بدافزار هستند.
- روزانه اکانت 600 هزار کاربر فیس‌بوک دزدیده می‌شود.

توصیه‌های ساده و ابتدایی برای کاربران عادی

- از پسورد قوی برای فیس‌بوک استفاده کنید.
- تقاضای دوستی افراد ناشناس را به‌هیچ‌وجه نپذیرید.
- هر مورد به اشتراک گذاشته شده توسط دوستان‌تان را به سادگی کلیک نکنید.
- تحت هر شرایطی از https استفاده کنید.
- از کافی‌نت‌ها یا تلفن‌ها و تبلت‌ها و لپ‌تاپ دیگران وارد فیس‌بوک نشوید.
- حتما پس از استفاده Log out کنید.
- Temporary fileهای مرورگر خود را دائما پاک کنید.
- اگر مسافر کشوری مانند ایران هستید، توجه کنید که در حال حاضر ممکن است همه عکسهای فیس‌بوک شما در اختیار دولت ایران قرار داشته باشد. با اینحال باز قصد سفر دارید؟
- روی لینکهای مشکوک مثل شما برنده یک آیفون هستید، کلیک نکنید.
- در صفحات امنیت فیس‌بوک عضو شوید : facebook.com/security

ابزارهای امنیتی فیس‌بوک

برخی از اساسی ترین امکانات امنیتی فیس‌بوک از قرار ذیل است :

Login : برای ورود به فیس‌بوک نام کاربری و پسورد خود را وارد می‌کنید. ارتباط SSL برقرار می‌شود.

ID verification : (انتخابی : توصیه می‌شود فعال کنید) در اینجا می‌توانید سوالات امنیتی خود و شماره تلفنی را تعریف کنید، فیس‌بوک هربار برای شما کدی را می‌فرستد که با آن می‌توانید وارد اکانت شوید.

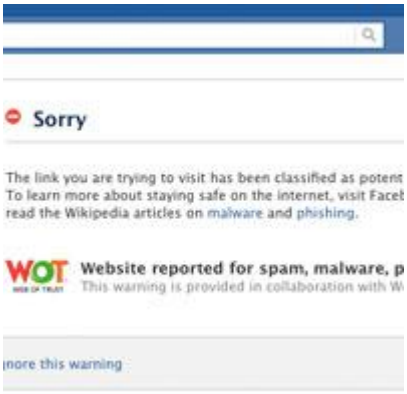
شناسایی اجتماعی – سوسیال Social Authentication :
اگر مشکل خاصی در ورود شما وجود داشته باشد، مثلا امروز صبح از جایی هزاران کیلومتر دورتر لاگین کرده باشید، فیس‌بوک از شما اطلاعاتی را راجع به تاریخ تولد و یا حتی دوستانتان خواهد پرسید تا از هویت واقعی شما مطمئن شود.

One Time Passwords : اگر شماره موبایل خود را قبلا در فیس‌بوک وارد کرده اید، فیس‌بوک برای شما یک پسورد یکبار مصرف تکست می‌کند تا از آن برای ورود به اکانت خود استفاده کنید.
درباره افزایش امنیت در فیس‌بوک با پسوردهای یک‌بارمصرف اینجا بیشتر بخوانید:
http://www.dw.de/dw/article/0,,6116519,00.html

Login Approvals : (انتخابی : توصیه می‌شود فعال کنید)
فرض کنید دفعه گذشته از کامپیوتر خانه به فیس‌بوک رفته اید، این بار اگر تلاش کنید از کامپیوتر جدیدی مثلا در محل کار وارد فیس‌بوک شوید. فیس‌بوک درباره کامپیوتر جدید از شما سوال می‌کند. همچنین در اکانت شما پیامی‌نمایش داده می‌شود مبنی بر اینکه شما با یک دستگاه جدید وارد فیس‌بوک شده اید.

Session Classifier : فیس‌بوک مشخصات هر ورود و خروج شما را به دقت کنترل می‌کند این داده‌ها بررسی می‌شوند تا مثلا کاربری که صبح از سیدنی وارد فیس‌بوک شده، قبل از نهار اینبار از لندن وارد فیس‌بوک نشود.

User Action Classifier : فیس‌بوک رفتار شما را زیر نظر داشته و تحلیل می‌کند، مثلا کاربری که وارد یک گروه شده برای 150 کاربر جنس مخالف یک پیام مشخص را کپی و پیست کند و یا کاربری که قصد تبلیغ و فروش اجناس روی فیس‌بوک را داشته باشد به سرعت شناسایی و دسترسی شان محدود می‌شود.



Link Scanner : لینکهایی که روی فیس‌بوک ارسال می‌شوند هر روز کاملا چک می‌شوند تا کاربران را به سوی سایت‌های حاوی بدافزار هدایت نکنند.

Photo DNA : فیس‌بوک از سیستم DNA تصویری استفاده می‌کند. این سیستم قادر است میلیونها تصویری را که روزانه به فیس‌بوک آپلود می‌شوند. یک به یک تحلیل کرده و مانع از آپلود تصویرهای غیرقانونی و نامتناسب با قوانین فیس‌بوک شود.

Self XSS فیس‌بوک با کنترل کامل بخش آدرس مرورگر مانع از فعالیت اسکریپهای می‌شود که به صورت خودکار قصد انجام عملیات خاصی نظیر تغییر استاتوس یا ارسال اسپم را دارند.

Clickjacking Domain Reputation System :
فیس‌بوک مانع از پدیدار شدن خودکار یک سایت پس از کلیک کردن کاربر روی لینکی که صرفا برای دزدیدن کلیک ارسال شده می‌شود.

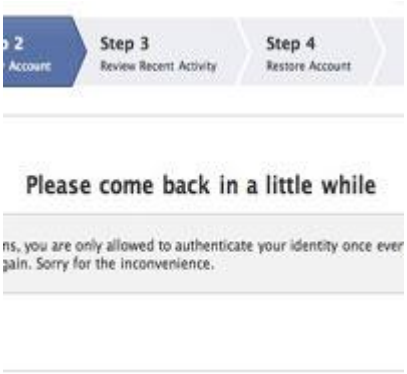
Application Classifier : رفتار اپلیکیشین‌ها یا برنامه‌های کاربردی را کنترل می‌کند و دائما آنان را مورد تستهای مختلفی قرار می‌دهد تا اطمینان حاصل کند خطری برای کاربران به حساب نمی‌آیند.

Suspected Hacking : اگر به هنگام کار با فیس‌بوک تشخیص دهید فرد یا دستگاه دیگری با اکانت شما اکتیو است، می‌توانید از اکانت خارج و تمام پسوردها را عوض کنید.

Remote Logout : فرض کنید از کامپیوتر کس دیگری وارد فیس‌بوک خود شده اید و فراموش کرده اید LogOut کنید به راحتی می‌توانید وارد اکانت خود شوید و در لیست فعالیتها کامپیوتر اکتیو را پیدا کنید و به صورت از راه دور فیس‌بوک را در آن کامپیوتر یا تلفن هوشمند ببندید.

Guardian Angels : اطلاعات اکانت شما در صورت گم کردن پسورد یا مشکلات دیگر می‌تواند برای دوستان نزدیکتان ارسال شود.

Login Notifications : دستگاهها، کامپیوتر و یا تلفن جدیدی که به فیس‌بوک شما متصل شده در لیست اعلانات یا notificationsهای شما نمایش داده می‌شود.



Roadblock : اگر اکانت شما رفتاری غیرعادی خصوصا در زمینه ارسال بدافزار را انجام دهد. دسترسی شما برای مدتی به فیس‌بوک محدود خواهد شد تا این موارد جزء به جزء مورد بررسی قرارگیرند.

با نگاهی به این اینفوگرافیک می‌توانید اطلاعات آماری جالبی درباره حملات فیس‌بوکی در سال ۲۰۱۱ به‌دست آورید:
http://blog.commtouch.com/cafe/web-security/infographic-facebook-attacks-in-2011/

فرصت‌های نوین، تهدیدهای نوین

فعالان مدنی در سراسر جهان با استفاده از توانایی‌های بی نظیر شبکه‌های اجتماعی در بسیج کنشگران تغییرات بنیادین بسیاری ایجاد کرده‌اند. در تهران 2009 ، قاهره و تونس2010 و 2011 حتی تصور گردهم‌آیی‌های چند میلیونی اعتراضی بدون استفاده از فیس‌بوک، توتییر و یوتیوب ناممکن بود.

شبکه‌های اجتماعی ابزارهای درخشان فعالیت مدنی‌اند، اما در عین حال شمشیر دولبه‌ای‌اند که می‌توانند علیه فعالان مدنی عمل کنند.

دولت جمهوری اسلامی ایران از طرق مشابه زیر سایت‌هایی نظیر فیس‌بوک را علیه فعالان منتقد به کار می‌گیرد:

- Impersonation یا جا زدن خود به جای دیگری، ده‌ها و صدها شناسه مجعول با تصاویر افراد مشهور نظیر سید محمد خاتمی، رضا پهلوی، میرحسین موسوی، سمبل‌های اسلامی، هخامنشی و آذری. تیم‌های فوتبال و یا خوانندگان و بازیگران مشهور ایجاد می‌شود. در این شناسه‌ها با الفاظی زننده به رقبای سیاسی توهین می‌شود تا امکان هر نوع گفتگو و تعامل میان مخالفان از میان برود.

مثال : در اردیبهشت ماه سال 1390 صفحه ای جعلی با نام دکتر اردشیر امیرارجمند از چهره‌های سرشناس منتقد دولت ایران آغاز به عضوگیری نمود. این شناسه در فاصله کوتاهی با واکنش سریع امیرارجمند و اعلام گسترده در رسانه‌های منتقد دولت جعلی اعلام شد. اما نگاهی به لیست افرادی که دعوت این شناسه را قبول کرده بودند نشان می‌دهد حتی بسیاری از روزنامه نگاران و فعالان سرشناس نیز به سادگی با اعمال شیوه‌های ساده نفوذ اطلاعاتی در شبکه‌های اجتماعی فریب خواهند خورد.

- در مواردی از یک شناسه provocateur ، توهین به مقدسات دینی ، باورهای قومی، فرهنگی و سیاسی بخشی از شهروندان صورت می‌پذیرد تا رضایت عمومی از سرکوب مخالفان حاصل آید.
- شناسه‌هایی با تصاویر جذاب و بعضا نیمه‌عریان دختران ایجاد می‌شود تا با شبکه گسترده‌ای از فعالان سیاسی تماس برقرار و اطلاعات آنلاین ایشان جمع آوری شود.
- شناسه‌ای جعلی به نام شما ایجاد شده و دوستان لیست شما مجددا دعوت می‌شوند.
- شناسه جعلی مثلا وارد گروه 25 بهمن می‌شود و برخی از افراد آنجا را به لیست خود دعوت می‌کند. پس از آن به گروه ندای سبز آزادی می‌رود و تعدادی دعوت از آنجا می‌گیرد و به همین شکل با رفت و آمد میان گروه‌ها شبکه خود را گسترده می‌کند.

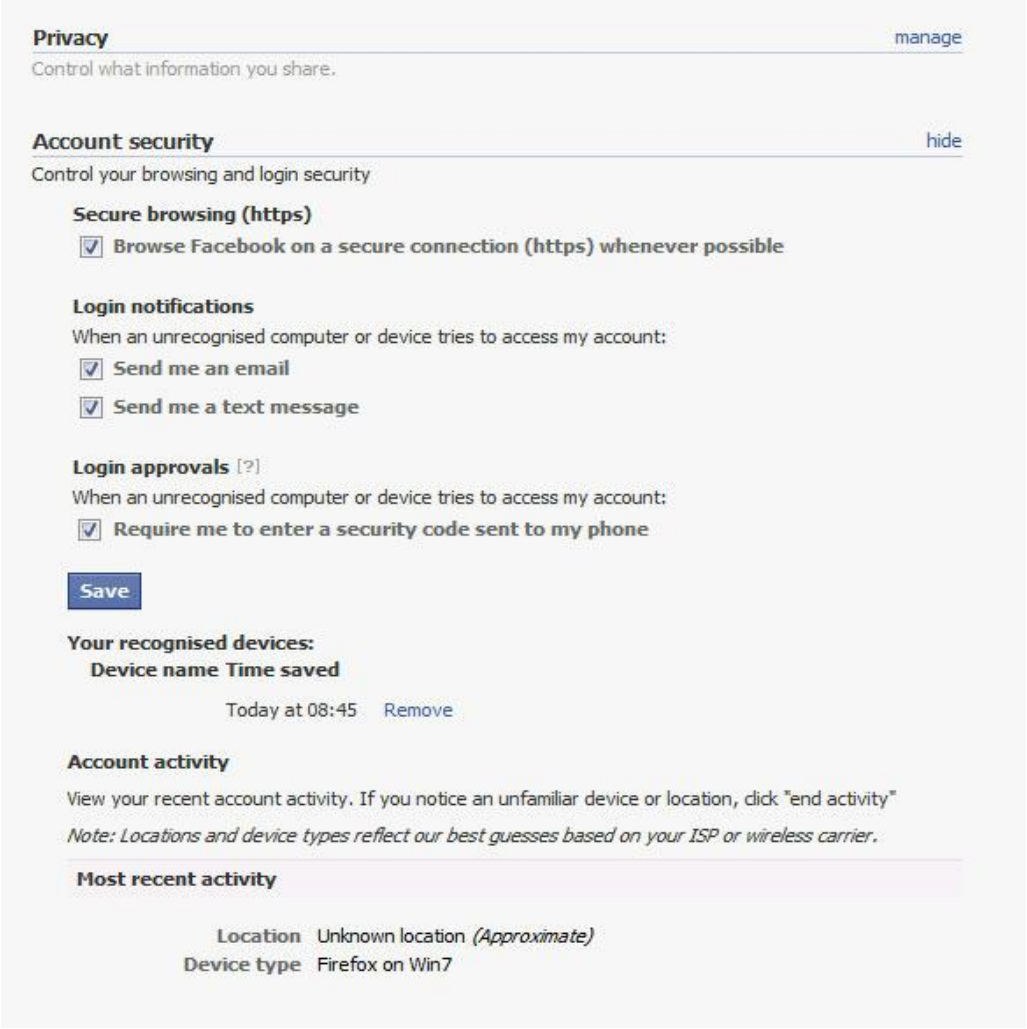
نکات ضروری برای فعالیت در شبکه‌های اجتماعی نظیر فیس‌بوک :

فیس‌بوک امکانات متعددی را برای محافظت از امنیت اکانت شما اضافه نموده است. استفاده از امکانات زیر قویا توصیه می‌شود.

1 – فیس‌بوک را برای استفاده امن https تنظیم کنید.

2 – تنها از یک کامپیوتر برای دسترسی به فیس‌بوک خود استفاده کنید این کامپیوتر را در لیست دستگاههای مجاز خود ثبت نمایید تا اگر فرد دیگری از کامپیوتر دیگری برای ورود به فیس‌بوک تلاش کرد، با ارسال SMS از این اقدام مطلع شوید.

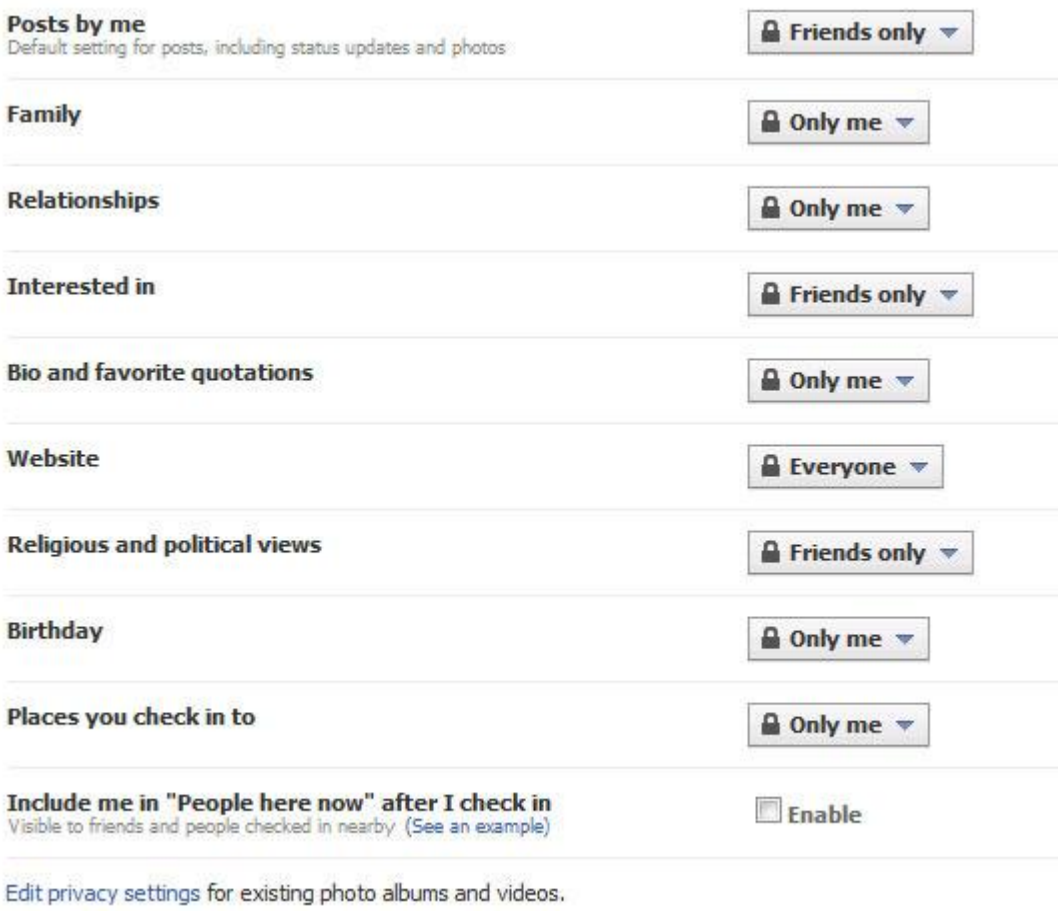
3 – لیست افراد و کامپیوترهایی را که اخیرا به اکانت شما دسترسی داشته اند دائما کنترل کنید.



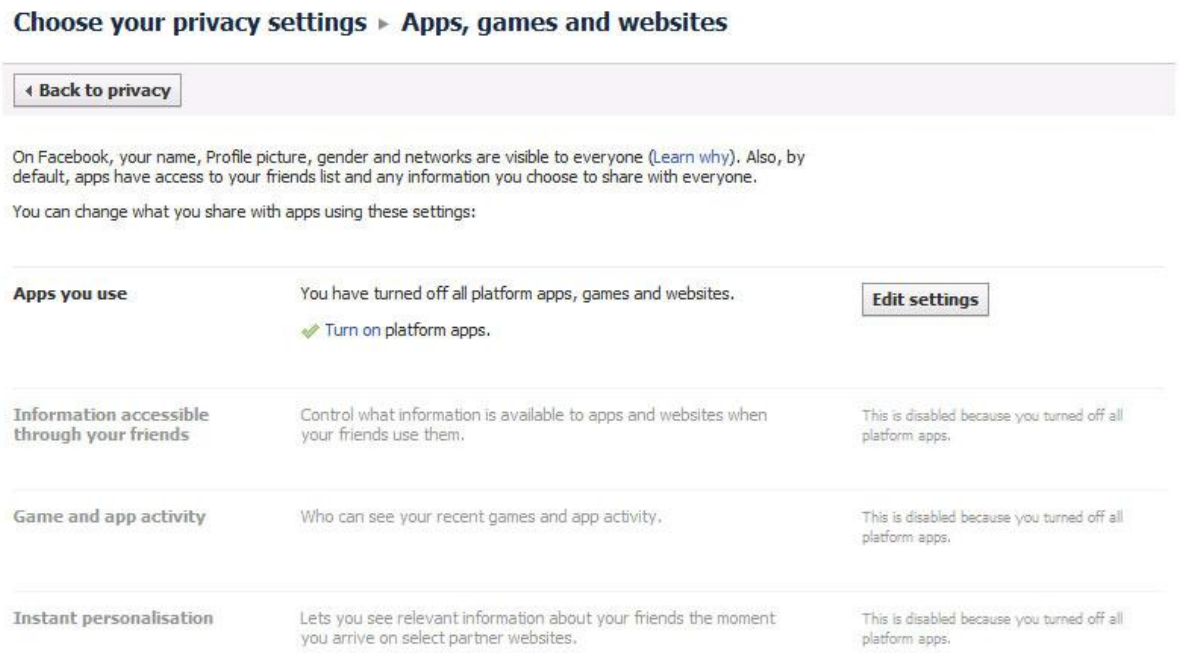
نمایش صورت کامل دوستان اشتباه ترین عمل ممکن است، فرض کنید صورت اسامی دوستان یک فعال سیاسی صاحب نام به صورت عمومی نمایش داده شود. با این کار جان صدها و بلکه هزاران فعال سیاسی ساکن ایران به خطر خواهد افتاد. بلافاصله نمایش عمومی دوستان خود را متوقف کنید. لزومی‌به نمایش دوستان شما برای هیچکس نیست. حتی بسیاری از دوستان شما نیز مایل به نمایش نام‌شان در مجموعه دوستان شما نیستند.

- نام خود را دائما در فیس‌بوک جستجو کنید. اگر کسی با نام و تصاویر شما مشغول فعالیت و گسترش شبکه در فیس‌بوک است این حادثه را سریعا به فیس‌بوک گزارش کنید و از دوستان‌تان هم بخواهید که گزارش این اقدام را برای فیس‌بوک ارسال کنند. این کار به سادگی و تنها با چند کلیک میسر است. این افراد با نام جعلی شما با دوستان واقعی شما مرتبط شده و از آنان کسب اطلاعات می‌کنند.

- افراد ناشناس را به لیست خود اضافه نکنید. اگر روزنامه‌نگار و فعال سیاسی هستید و می‌خواهید که مخاطبانتان را در لیست داشته باشید، شناسه‌های دوم و سومی‌برای اینکار ایجاد کنید. شناسه حاوی اطلاعات شخصی و خانوادگی شما به هیچ وجه نباید در معرض مشاهده افراد ناشناس قرارگیرد.
- از هویت واقعی دوستان خود قبل از اضافه کردن به لیست اطمینان حاصل کنید. پس از افزودن فردی که با تصویر دوست شما ظاهر شده است، او به بسیاری از اطلاعات شما دسترسی خواهد داشت. حذف او پس از اطلاع از جعلی بودن شناسه اش، کمکی به این اطلاعات از دست رفته نخواهد کرد.
- تاریخ تولد ومحل سکونت خود را در پروفایل عمومی‌خود منتشر نکنید. بانکها و موسسات اینترنتی از همین دو داده برای ارسال مجدد پسورد فراموش شده شما و یا تغییر این پسورد و دسترسی به داده‌های حساس استفاده می‌کنند.



حتی الامکان از برنامه‌های کاربردی Third Party Application در شبکه‌های اجتماعی استفاده نکنید. این برنامه‌ها می‌توانند به اطلاعات خصوصی شما دستیابی پیدا کنند. در قسمت تنظیمات امنیتی می‌توانید مانع از این امر شوید.

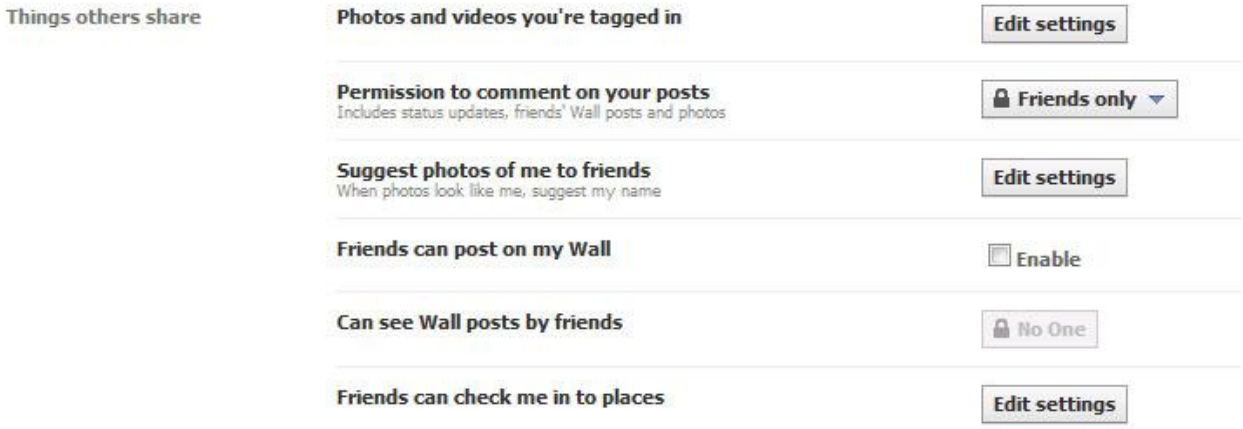


- اجازه ندهید نام شما در جستجوهای فیس‌بوک و پروفایل عمومی‌موتورهای جستجونظیر گوگل به نمایش درآید. در قسمت تنظیمات امنیتی می‌توانید از این کار جلوگیری کنید.

- می‌توانید صورت دوستان مختلفی تنظیم کنید : مثلا فعالان مدنی، روزنامه نگاران ، دوستان نزدیک و غیره. می‌توانید سطح دسترسی این لیستها را تغییر دهید. یعنی مثلا برخی از این گروهها قادر به مشاهده آلبوم خاصی نباشند.

- قسمت Ralationship status خود را غیرفعال کنید
- از نمایش عمومی‌شماره تلفن و آدرس ایمیل خود خودداری کنید

- دسترسی کاربران به مشاهده پست‌های Wall و همچنین نوشتن پست بر Wall خود را محدود کنید.



- نمایش اطلاعات خود روی قسمت social ads را متوقف کنید
- فهرست دوستان‌تان را با تغییر تنظیمات حریم خصوصی، از چشم دیگران پنهان نگه دارید تا بررسی و تحلیل حلقه ارتباطی شما به‌سادگی میسر نباشد. در غیر این‌صورت، حتی کسانی که در فهرست دوستان‌تان نیستند، می‌توانند به لیست دوستان فیس‌بوکی شما دسترسی داشته باشند.

علاوه بر موارد فوق استفاده از سرویس شبکه‌های اجتماعی همراه با تلفنهای هوشمند و کامپیوترهای قابل حمل نیز نیازمند دقت مضاعف و رعایت مواردی است که قبلا درباره رسانه‌های قابل حمل گفته شد.

این اینفوگرافیک اطلاعات جالبی درباره تهدیدهای فیس‌بوکی برای کاربران دارد:
http://blog.trendmicro.com/the-geography-of-social-media-threats

اهمیت تنظیمات حریم خصوصی فیس‌بوک

محیطی که برای تغییر تنظیمات حریم خصوصی کاربران در فیس‌بوک طراحی شده، همواره دستخوش تغییر می‌شود و کاربران فعال و اکتیویست‌های سایبری باید با چک کردن مستمر اخبار و اطلاعات پیرامون آن و تست کردن امکانات جدیدی که اضافه می‌شوند، دانش خود در این زمینه را به‌روز کنند.

تسلط بر تنظیمات حریم خصوصی برای همه کاربران فیس‌بوک اهمیتی حیاتی دارد. اگر می‌خواهید جزئیات و راهنمایی‌های بیشتری در این‌باره بخوانید، این مطلب «۱۰ نکته‌ای که باید درباره تنظیمات حریم خصوصی در فیس‌بوک بدانید» را از دست ندهید:

http://www.dw.de/dw/article/0,,6434375,00.html

توصیه‌هایی برای فعالان سایبری فعال در فیس‌بوک

اگر از جمله کسانی هستید که با مدیریت صفحات گوناگون، از فیس‌بوک برای اکتیویسم آنلاین هم بهره می‌گیرید، باید دقت بیشتری به مساله امنیت و حریم خصوصی داشته باشید. در این مطلب، توصیه‌هایی برای افزایش امنیت اکتیویست‌ها در فیس‌بوک ارائه شده که خواندن آن توصیه می‌شود. ایمن‌سازی حضور اکتیویست‌ها در فیس‌بوک:
http://www.dw.de/dw/article/0,,14988781,00.html

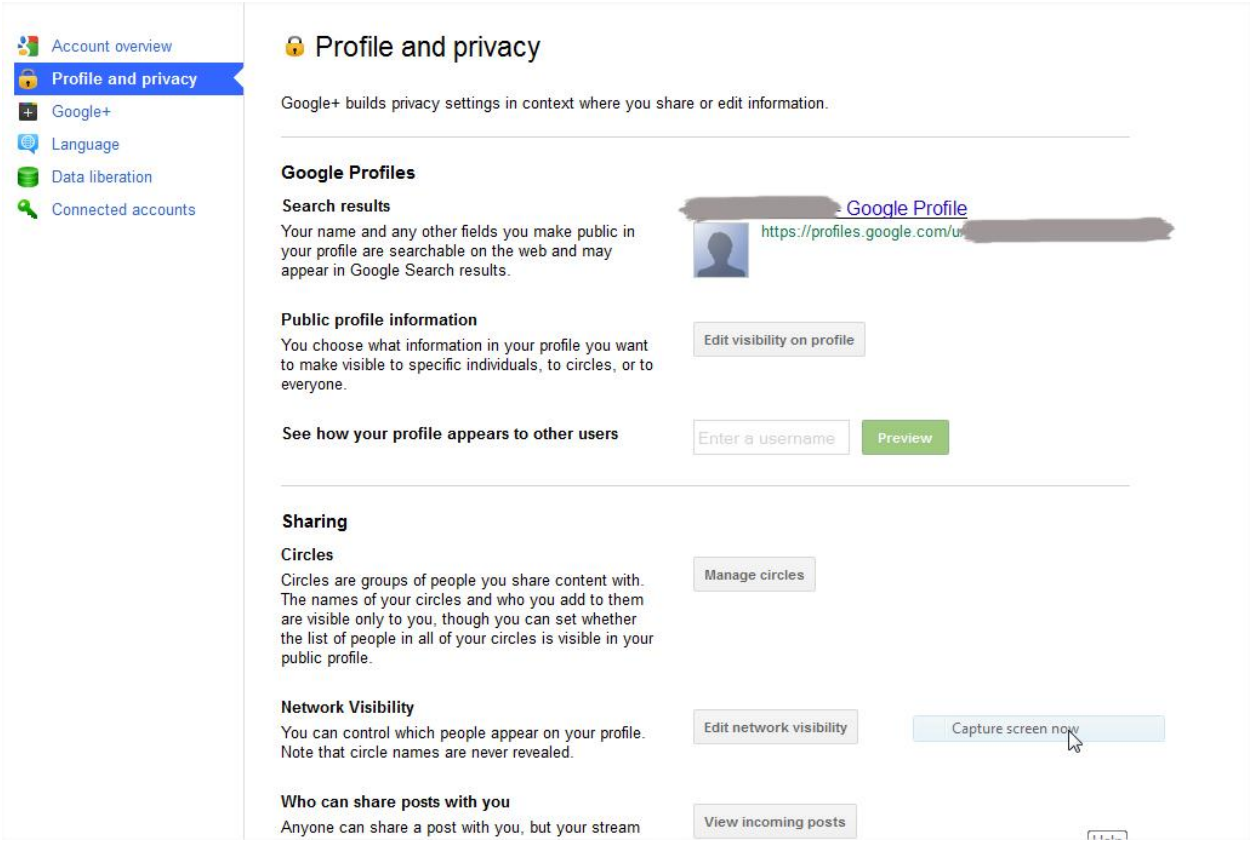
امنیت گوگل پلاس Google+

شرکت گوگل سرویس شبکه اجتماعی خود یعنی گوگل پلاس را از ماه گذشته آغاز نمود، تجربه نشان می‌دهد در ماه‌های ابتدایی شروع به کار یک شبکه و یا سرویس به دلیل عدم آشنایی کاربران، تبهکاران بسیاری به اینگونه شبکه‌ها هجوم می‌آورند، رعایت نکات ذیل به هنگام استفاده از گوگل پلاس ضروری است.

تنظیمات امنیتی گوگل پلاس به طور خلاصه بر پایه تنظیمات امنیتی اکانت شما می‌باشند و در آدرس :

https://plus.google.com/settings/privacy

قابل دسترسی و تغییر اند.



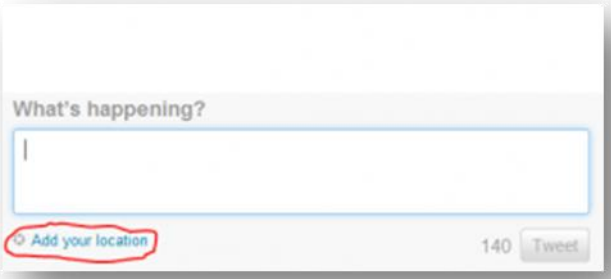
بر خلاف فیس‌بوک اینجا شما می‌توانید دوستان خود را در گروهها یا حلقه‌های مختلفی سازماندهی کنید بدون اینکه مشکل تداخل با اعضای حلقه‌های دیگر را داشته باشند. نکته قابل توجه دیگر گوگل پلاس دسترسی کامل شما به داده‌هایتان است، شما می‌توانید عکسها و سایر اسناد خود را یکجا دانلود کنید.آدرس داده‌های شما در گوگل پلاس:

https://plus.google.com/settings/exportdata

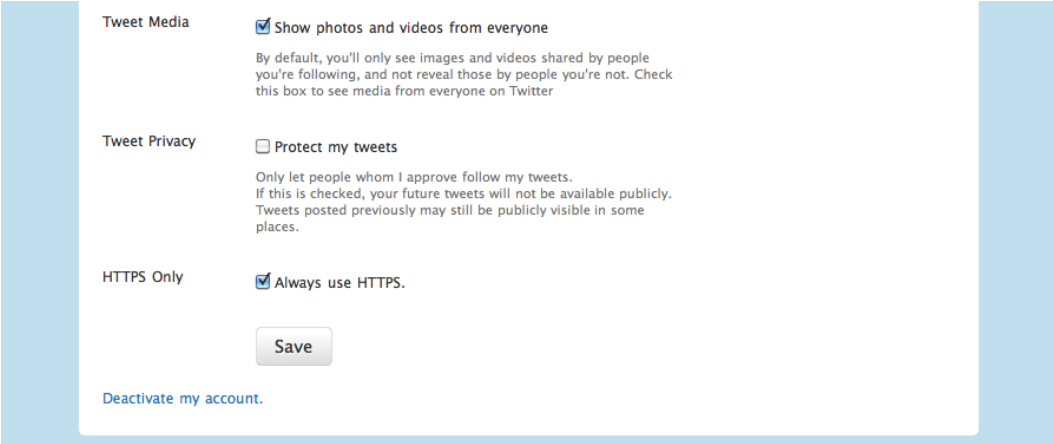
امنیت در توییتر

توییتر، سرویس مایکروبلاگینگ و شبکه اجتماعی محبوبی که حالا بیش از ۲۵۰ میلیون کاربر دارد، امکانات خارق‌العاده‌ای برای اطلاع‌رسانی، هماهنگی و سازماندهی نیروهای اجتماعی و سیاسی ارائه می‌کند. اما دولت‌های سرکوبگر همواره در کمین کاربران توییتر نشسته‌اند تا در شرایط اضطراری و در مواقعی که خطر آنها را تهدید می‌کند، با رهگیری و تعقیب و بازداشت آنها، از آسیب‌پذیری‌های امنیتی خود بکاهند.

به همین خاطر لازم است که کاربران توییتر چند نکته مهم را به‌خاطر داشته باشند. اول این‌که اگر از کشوری مانند ایران توییت می‌کنید، حتما امکان مکان‌یابی را غیرفعال کنید، چون زمانی که این امکان فعال است، موقعیت جغرافیایی شما به‌همراه هر توییت ارسال می‌شود و این به‌شدت از ضریب امنیت‌تان می‌کاهد و تعقیب شما را برای نیروهای امنیتی وابسته به حکومت بسیار ساده‌تر خواهد کرد:



نکته بسیار مهم دیگر این است که باید با مراجعه به بخش تنظیمات، یک‌بار برای همیشه HTTPS توییتر را فعال کنید تا از این به‌بعد از هر سیستمی که به توییتر متصل می‌شود، از نسخه امن آن استفاده کنید. همان‌طور که می‌بینید، این‌کار به سادگی با دو-سه کلیک میسر است.



یک نکته بسیار مهم دیگر: اگر از اتصالات وایرلس ناشناس و بدون‌رمز استفاده می‌کنید و قصد دارید مثلا در یک تجمع اعتراضی از طریق موبایل‌تان توییت کنید، همواره به‌خاطر داشته باشید که با مرورگر موبایل‌تان وارد سایت توییتر شود، نه از طریق اپلیکیشن، چرا که اپلیکیشن‌های موبایل و تبلت‌ها برای فیس‌بوک و توییتر معمولا رابط کاربری خاص خود را دارند و از نسخه HTTPS وارد سایت نمی‌شوند، به همین خاطر ممکن است اطلاعاتی که ارسال می‌کند توسط کسی که اتصال وایرلس خود را باز گذاشته، کنترل شود. با HTTPS و از طریق مرورگر وارد شوید تا اطلاعات کدگذاری شوند و امنیت‌تان افزایش یابد.

حذف همه توییت‌ها با چند کلیک

اگر تحت فشار قرار گرفتید یا احساس می‌کنید ممکن است به‌زودی با نیروهای امنیتی مواجه شوید و توییت‌هایتان به‌هر دلیلی برای‌تان دردسر شود، می‌توانید با استفاده از ابزاری نظیر Tweetwipe به سرعت همه توییت‌هایی که روی اکانت‌تان ارسال کرده‌اید را پاک کنید. این ابزار از اینجا قابل دسترسی است: http://twitwipe.com/

مدیریت حضور در شبکه‌های اجتماعی

اگر می‌خواهید زندگی دیجیتال در شبکه‌های اجتماعی و حضور خود در این محیط‌ها را مدیریت کنید و انتشار پست‌ها در فیس‌بوک و توییتر را با نظم و هماهنگی بیشتری دنبال کنید، می‌توانید از برنامه‌های جانبی قدرتمندی نظیر هوت‌سویت HootSuite استفاده کنید که به‌خاطر رابط خاص کاربری، گاه امکان عبور از سد فیلترینگ را هم به کاربران کشورهایی نظیر ایران می‌دهند.

به‌سادگی می‌توانید از طریق آدرس http://hootsuite.com وارد این سرویس شوید و حتی اگر اکانتی ندارید، با اکانت جی‌میل خود وارد محیط کاربرپسند آن شوید. سپس اکانت‌های گوناگون توییتر و فیس‌بوک خود را به آن معرفی می‌کنید و می‌توانید از امکانات کم‌نظیرش لذت ببرید و برای بهبود و ارتقای فعالیت‌هایتان از آنها استفاده کنید.

اطلاعات کامل مرتبط با برنامه هوتسویت را می‌توانید از اینجا بخوانید:
http://www.dw.de/dw/article/0,,6395966,00.html

امنیت در فرندفید

فرندفید اگرچه هیچ امکان خاصی به کاربران ارائه نمی‌کند، اما همچنان در میان طیفی از کاربران ایرانی محبوبیت خود را حفظ کرده است. اما نکته اینجاست که این شبکه اجتماعی که حالا در تملک کمپانی فیس‌بوک است، به‌شدت ناامن و نامطمئن است و آسیب‌پذیری‌های امنیتی فاحشی دارد. اگر بلاگر، روزنامه‌نگار یا فعال اجتماعی و سیاسی هستید، بهتر است از فرندفید استفاده نکنید و فعالیت‌های خود را در فیس‌بوک، توییتر یا گوگل‌پلاس پی‌گیری کنید.

اما اگر همچنان به استفاده از این شبکه اجتماعی اصرار دارید، باید بدانید که یکی از ضعف‌های امنیتی موجود در آن به کاربران این امکان را می‌دهد که به‌سادگی دایرکت مسج‌ها (پیام‌های مستقیم) شما را بخوانند. بنابراین، هرگز از دایرکت مسج فرندفید برای ارسال اطلاعات حساس استفاده نکنید.