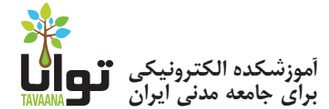
امنیت دیجیتال
برای فعالان کمپین‌های انتخاباتی

توانا
TAVAANA
آموزشکده الکترونیکی
برای جامعه مدنی ایران

پروژهٔ
e-collaborative
for civic education



http://www.tavaana.org

پروژهٔ

e-collaborative
for civic education

http://www.eciviced.org

امنیت دیجیتال برای فعالان کمپین‌های انتخاباتی

ناشر: E-Collaborative for Civic Education

تدوین: نیما راشدان

e-collaborative
for civic education

E-Collaborative for Civic Education (ECCE) یک سازمان غیرانتفاعی در ایالات متحده آمریکا، تحت 501c3 است که از فن‌آوری اطلاعات و ارتباطات برای آموزش و ارتقای سطح شهروندی و زندگی سیاسی دموکراتیک استفاده می‌کند.

ما به عنوان بنیانگذاران و مدیران این سازمان، اشتیاق عمیق مشترکی داریم که شکل‌دهنده ایده‌های جوامع باز است. همچنین برای ما، شهروند، دانش شهروندی، مسئولیت و وظیفه شهروندی یک فرد در محافظت از یک جامعهٔ سیاسی دموکراتیک پایه و اساس کار است؛ همان طور که حقوق عام بشر که هر شهروندی باید از آنها برخوردار باشد، اساسی و بنیادی هستند. ECCE دموکراسی را تنها نظام سیاسی قادر به تأمین طیف کاملی از آزادی‌های شهروندی و سیاسی برای تک تک شهروندان و امنیت برابری و عدالت می‌داند. ما دموکراسی را مجموعه‌ای از ارزش‌ها، نهادها و فرایندها می‌دانیم که مبشر صلح، توسعه، تحمل و مدارا، تکثرگرایی و جوامعی شایسته‌سالار که به کرامت انسانی و دستاوردهای انسانی ارج می‌گذارند، است.

ما پروژهٔ اصلی ECCE یعنی «آموزشکده توانا: آموزشکده مجازی برای جامعهٔ مدنی ایران» را در سال ۲۰۱۰ تأسیس کردیم. آموزشکده توانا در ارائه منابع و آموزش در دنیای مجازی در ایران، یک نهاد پیشرو است. توانا با ارائه دوره‌های آموزشی زنده در حین حفظ امنیت و با ناشناس ماندن دانشجویان، به یک جامعهٔ آموزشی قابل اعتماد برای دانشجویان در سراسر کشور تبدیل شده است. این دروس در موضوعاتی متنوع مانند نهادهای دموکراتیک، امنیت دیجیتال، حقوق زنان، وبلاگ‌نویسی، جدایی دین و دولت و توانایی‌های رهبری ارائه می‌شوند. آموزشکده توانا آموزش زندهٔ دروس و سمینارهای مجازی را با برنامه‌هایی مثل مطالعات موردی در جنبش‌های اجتماعی و گذارهای دموکراتیک، مصاحبه با فعالان و روشنفکران، دستورالعمل‌های خودآموزی، کتابخانهٔ مطالب توصیفی، ابزارهای کمکی و راهنمایی برای آموزشگران ایرانی و حمایت مداوم و ارائه مشاورهٔ آموزشی برای دانشجویان تکمیل کرده است.

تلاش ما برای توسعهٔ توانایی‌های آموزشکده توانا متوجه گرد آوردن بهترین متفکران ایرانی و صداهای محذوف است. به همین ترتیب، به دنبال انتشار و ارتقای آثار مکتوب روشنفکران ایرانی هستیم که ایده‌های آنان توسط جمهوری اسلامی ممنوع شده است.

یکی از نقاط تمرکز تلاش توانا، ترجمه متون کلاسیک دموکراسی و مقالات معاصر در این باره و نیز ترجمه آثار مرتبط با جامعه مدنی، حقوق بشر، حاکمیت قانون، روزنامه‌نگاری، کنشگری و فن‌آوری اطلاعات و ارتباطات است. امید ما این است که این متون بتواند سهمی در غنای فردی هموطنان ایرانی و برساختن نهادهای دموکراتیک و جامعه‌ای باز در ایران داشته باشد.

سپاسگزار بازتاب نظرات و پیشنهادهای شما

اکبر عطری

مریم معمارصادقی

فهرست مطالب

امنیت دیجیتال برای فعالان کمپین‌های انتخاباتی

در سال‌های اخیر اینترنت به یکی از ابزارهای محوری در فعالیت انتخاباتی تبدیل شده است. کاندیداها، احزاب سیاسی و مدیران کمپین‌ها بخش عمده‌ای از فعالیت انتخاباتی خود را روی اینترنت و با استفاده از ابزارهای دنیای دیجیتال انجام می‌دهند.

کاندیدای الف برای عضویت در شورای شهری کوچک قصد فعالیت دارد. او ایده کاندیداتوری خود را در وب‌سایت خود و شبکه‌های اجتماعی مطرح می‌کند. بلافاصله هزاران کاربر استاتوس او را با توئیتر و فیس‌بوک بازنشر می‌کنند. کاربران بسیاری به این ایده واکنش نشان می‌دهند. از مطالعه کامنت‌ها و واکنش‌های آنان، کاندیدا می‌تواند نقاط قوت و ضعف خود را در مناطق مختلف شهر دریابد. او رأی‌دهندگان را از روی فیس‌بوک به گروه‌هایی مثل: زنان جوان، مردان متاهل، زنان خانه‌دار، مردان کارگر و شهروندان کهنسال و... تقسیم کرده و برای فهم مطالبات، ارزش‌ها و انتقادات هر گروه تلاش می‌کند. پس از آن شعار و پیام کمپین خود را در اشکال مختلف برای گروه‌های فوق ارسال می‌کند؛ مطالب ویژه سالمندان در سایت‌های مورد علاقه ایشان، پیام به مردان جوان در سایت‌های پرطرفدار آنها مانند سایت‌های خودرو و بازی‌های ویدئویی و غیره. دیگر استفاده بسیار مهم اینترنت تشکیل لیست‌های بزرگ داوطلبان است. شمار بسیار بزرگی از علاقه‌مندان به کاندیدا یا حزب می‌توانند به صورت آنلاین و از طریق وب‌سایت یا صفحه فیس‌بوک کاندیداها به لیست داوطلبان حامی ایشان بپیوندند و حتی برای فعالیت‌های غیراینترنتی مثل پخش تراکت و... اعلام آمادگی کنند.

از اینترنت می‌توان برای نظرسنجی، میزان موفقیت و تاثیرگذاری کمپین و یا تشویق شهروندان به خروج از خانه و رأی و یا نظارت بر تخلفات انتخاباتی نیز استفاده کرد.

در انتخابات سال ۲۰۱۲ ریاست جمهوری ایالات متحده آمریکا، دو نامزد اصلی احزاب جمهوری‌خواه و دموکرات بخش قابل توجهی از توجه کمپین خود را بر اینترنت متمرکز کردند: باراک اوباما برنده نهایی انتخابات بیش از ۵۲ میلیون دلار صرف انتشار آگهی‌های آنلاین کرد. این رقم برای رقیب او، میت رامنی ۲۶/۲ میلیون دلار بود. دنبال‌کنندگان آقای اوباما روی توئیتر ۱۸ میلیون نفر و در گوگل‌پلاس نزدیک به ۲ میلیون نفر و روی فیس‌بوک ۲۷/۱ میلیون نفر بودند.

انتخابات ۱۳۸۸ در ایران و اینترنت

انتخابات ریاست جمهوری خرداد ۱۳۸۸ در ایران، نقطه عطفی در استفاده از اینترنت در خلال کمپین انتخاباتی آقایان خاتمی، موسوی و کروبی بود. هواداران این سه کاندیدا و همچنین هواداران محمود احمدی نژاد در مقیاسی کوچکتر، از شبکه‌های اجتماعی خصوصا فیس‌بوک در تبلیغات انتخاباتی خود استفاده کردند.

ستاد ملی جوانان ۸۸ و پویش حمایت از خاتمی – موج سوم دو گروه اصلی سازماندهی حمایت جوانان از کاندیداهای اصلاح‌طلب بودند. بعدها مقامات نظامی جمهوری اسلامی ایران این دو گروه را متهم به تشکیل لیست اینترنتی چندصد هزار نفره‌ای

از شهروندان کردند؛ امری که در دیگر کشورهای جهان جزء لاینفک فعالیت اینترنتی در انتخابات است.

این کمپین‌ها در ابتدا با جمع‌آوری نام، آدرس ایمیل و مشخصات ده‌ها هزار ایرانی، خواستار شرکت خاتمی در انتخابات شدند و این فهرست به تدریج به فهرست طویلی از فعالان انتخاباتی در سراسر جهان بدل گشت.

فیس‌بوک نوظهور در ایران بلافاصله به یکی از اصلی‌ترین ابزارهای مورد استفاده حامیان کاندیداهای

مختلف بدل گشت و میلیون‌ها کامنت حاوی نقطه نظرات علاقه‌مندان خاتمی، کروبی، موسوی، هواداران تحریم انتخابات و دیگران در شبکه‌های اجتماعی مبادله شد.

انتخابات ۸۸ بلافاصله پس از اعلام آراء و اعتراض کاندیداهای منتقد یعنی میرحسین موسوی و کروبی به نتایج دستکاری شده انتخابات، به گسترده‌ترین موج اعتراضات مردمی در ایران از انقلاب ۱۳۵۷ انجامید. ده‌ها شهروند در جریان سرکوب اعتراضات به قتل رسیدند و ده‌ها هزار شهروند بازداشت و شکنجه شدند. رهبران و بسیاری از معترضان انتخابات ۱۳۸۸، حتی هم‌اکنون در بازداشت به سر می‌برند.

در خلال ماه‌های پیش از انتخابات خرداد ۱۳۸۸، فعالان انتخاباتی منتقد، علیرغم موفقیت خارج از انتظار در بهره‌گیری از ابزارهای آنلاین، اشتباهات غیرقابل جبرانی را نیز مرتکب شدند. این اشتباهات در موج بازداشت‌های پس از اعلام نتایج، پیامدهای تلخی را برای این گروه از فعالان به دنبال داشت.

با بازداشت مسئول فنی وب‌سایت یک کمپین اصلاح‌طلب و شکنجه او، نیروهای امنیتی به فهرست کامل فعالان آن کمپین و تمامی اسناد و مدارک مربوط به آن دست یافتند و امنیت هزاران فعال به خطر افتاد.

نیروهای امنیتی با نفوذ به فیس‌بوک، اعضای شاخص کمپین‌ها و روزنامه‌نگاران، تمام کامنت‌ها، تصاویر و دیگر اطلاعات را آرشیو کردند و بعد در فراغ بال به بازداشت شهروندان منتقدی پرداختند که گناه برخی از آنان تنها یک like یا share محتوای انتقادی در فیس‌بوک بود.

نیروهای امنیتی با نفوذ به سایت‌های اشتراک لینک نظیر بالاترین، اخبار کذب، ترور شخصیت، گمراه‌سازی و ارعاب شهروندان را با درجه بسیار بالایی از موفقیت اجراء نمودند. هر روز اخبار دروغین تجاوزهای هولناک، قتل، ناپدید شدن و کشتار دسته جمعی به چاپ می‌رسید تا انگیزه معترضان به حضور آرام خیابانی از بین برود، در شبکه‌های اجتماعی سیلی از اخبار ضد و نقیض از پخش سلاح میان معترضان، تصاویر جعلی معترضان با سلاح و تشکیک در محل برگزاری تجمعات منتشر شد.

تصاویر با کیفیت بسیار بالا از صورت معترضان در شبکه‌های اجتماعی به اشتراک گذارده شد، از روی این تصاویر به راحتی می‌شد هویت واقعی چهره‌ها را شناسایی کرد. سایت‌های نظامی سرکوبگر از همین تصاویر برای شناسایی معترضان استفاده کردند.

توصیه‌های امنیت عمومی

سپاه پاسداران انقلاب اسلامی و دیگر نیروهای امنیتی تمامی مراحل کمپین‌های انتخاباتی در ایران را رصد می‌کنند. این تصمیم شماست که با هویت واقعی خود به هواداری از یک کاندیدا بپردازید و یا یک هویت و شناسه مجازی را انتخاب کنید. انتخاب هویت واقعی خصوصا برای هواداری از کاندیداهای منتقد دولت، همواره حاوی ریسک است. این ریسک نه تنها متوجه شما که شامل خانواده، دوستان و نزدیکان شما نیز می‌شود.

بازی انتخابات ریاست جمهوری ۱۳۸۸، در ابتدا قانونی و در چهارچوب موازین پذیرفته شده جمهوری اسلامی ایران به نظر می‌رسید. حکومت حتی شهروندان را تشویق به شرکت در فرایند تبلیغات و رأی‌گیری می‌کرد. اما زمانی که صدها هزار ایرانی با حضور در خیابان‌ها و تشکیل موج سبز به انتقاد

از احمدی‌نژاد و سیاست‌های کلی آیت‌الله خامنه‌ای پرداختند. هجوم نیروهای امنیتی به دفاتر انتخاباتی و بازداشت فعالان حتی قبل از اعلام نتایج مخدوش انتخابات آغاز شد.

شما با هویت واقعی وارد پروسه انتخابات می‌شوید، پروسه‌ای که ممکن است به سرعت خشن شود. بسیاری از فعالان انتخاباتی در ایران بلافاصله پس از آغاز درگیری‌ها نام‌های خود را به نام‌های مجازی «میرحسین ایرانی» و... تغییر دادند، چرا که در معرض شناسایی و بازداشت قرار داشتند. بنابراین انتخاب میان فعالیت انتخاباتی با اسم واقعی و یا یک ایمیل، شناسه و پروفایل مجازی انتخابی، انتخابی است که می‌تواند برای شما پیامدهای جدی و غیرقابل پیش‌بینی به همراه آورد.


کد خبر: ۵۶۰ تاریخ انتشار: ۰۷ دی ۱۳۸۸ - ۱۷:۵۰ تعداد نظرات: ۶۷ نظر

منوی اصلی » آرشیو اخبار

روابط عمومی مرکز بررسی جرایم سازمان یافته سایبری اعلام می کند

اغتشاشگران و حرمت شکنان عاشورای حسینی را شناسایی کنید(3)

بدینوسیله از تمامی کاربران و خانواده های ایرانی انتظار می رود در صورتی که هر گونه مشخصاتی از عکس های ذیل و همچنین هرگونه اخبار و اطلاعاتی اعم از عکس ، فیلم ، مقاله ، خبر ، ایمیل و آدرس اینترنتی و یا شکایتی که در خصوص جریان های اغتشاش طلب و حرمت شکنان عاشورای حسینی دارند از طریق سایت گرداب به اطلاع مرکز بررسی جرایم سازمان یافته برسانند.

حرمت شکنان عاشورای حسینی را شناسایی کنید

توصیه‌های عمومی امنیت دیجیتال شامل فعالیت انتخاباتی نیز می‌شود. یک تبلت، لپ‌تاپ و تلفن هوشمند امن اساسا لازمه هر نوع فعالیتی است. اطلاعات بیشتر در خصوص محافظت از کامپیوترهای شخصی، تلفن همراه و یا شبکه‌های اجتماعی را می‌توانید در جزوات امنیت دیجیتال توانا بیابید.

امنیت فیزیکی کمپین

دفتر ستاد یا کمپین شما، محلی که با کاندیداها مصاحبه می‌کنید. داوطلبان را پذیرفته و سازماندهی و متون کمپین را تهیه می‌کنید و یا اتاقی که در آن کامپیوترها، دستگاه‌های فکس، تلفن و... قرار دارند برای کمپین شما واجد امنیت حیاتی هستند.

نیروهای امنیتی در مواردی در روزهای نزدیک به برگزاری انتخابات با یورش به این دفتر، درب‌ها را قفل زده و مانع از ورود مدیران و فعالان به ساختمان ستاد شده‌اند. این عمل مدیریت ستاد را دچار اختلال کرده و به کمپین آسیب جدی می‌زند. همچنین در مواردی دیگر تلفن‌ها و سیستم SMS مدیران کمپین و حتی کل کشور، قطع شده است تا مانع از تماس سازمان‌یافته مدیران با فعالان شود. هر یک از موارد فوق می‌بایستی از قبل مطالعه و مورد بررسی قرار گیرد و راه‌های جایگزین برای این موارد پیشنهاد شوند و نقشه‌های متفاوتی طراحی شود تا در صورت وقوع هر حالت، فعالیت کمپین ادامه یافته، ضربه و ضرر محدود شود.

نیروهای امنیتی غالبا خطوط تلفن، فکس و پیامک ستاد شما را کنترل می‌کنند. در داخل اتاق‌های

کمپین، وسایل شنود نصب کرده و ورود و خروج فعالان را به صورت ۲۴ ساعته ضبط می‌کنند. هر یک از موارد فوق نیازمند توجه است. داده‌های فوق‌العاده حساس کمپین را می‌بایست به صورت رو در رو و در محلی خارج از ساختمان، بدون وجود تلفن‌های همراه و با کمترین احتمال شنود مبادله کرد. از فعالان منتقد و زندانیان سیاسی بخواهید احتمال مراقبت فیزیکی از ورود و خروج به ساختمان ستاد را مد نظر قرار دهند و از حضور غیرضروری در کمپین خودداری کنند.

سرقت وسایل دیجیتال کمپین شگرد دیگری برای ایجاد رعب و البته دستیابی به اطلاعات کمپین شماست. از کامپیوترهای شخصی مسئولان کمپین خصوصا کامپیوترهای حاوی تماس با خبرنگاران، حامیان مالی کمپین، رسانه‌های فارسی‌زبان و لیست داوطلبان به شدت محافظت کنید. اگر این کامپیوترهای شخصی داخل ساختمان نصب شده باشند، این امکان وجود دارد که با شکستن قفل‌ها مورد سرقت قرار گیرند و اگر به صورت لپ‌تاپ توسط شما حمل شوند، می‌توانند در خودرو یا خیابان دزدیده شوند. در هر صورت اطلاعات حساس کدگذاری نشده، بهترین هدیه به نیروهای امنیتی است در حالیکه اطلاعات کدگذاری شده و ذخیره شده در محلی امن، کار ایشان برای استخراج فهرست‌ها را بسیار مشکل خواهد کرد.

امنیت وب‌سایت انتخاباتی

اگر برای کاندیدا یا حزب سیاسی یا گروه هواداران خود یک وب‌سایت درست می‌کنید توجه به موارد ذیل می‌تواند امنیت شما را تا حد قابل توجهی ارتقاء بخشد.

۱. نام دامنه را به نام یکی از دوستان نزدیک خود، که ساکن خارج از ایران است، ثبت کنید. از او بخواهید اطلاعات درست و واقعی خود را بر اساس مدارک شناسایی در اختیار شرکت ثبت‌کننده دامنه قرار دهد. این شرکت می‌بایستی مانند Goddady سرویسی مانند Certified Domain validation – ترجیحا تلفنی در اختیار شما قرار دهد. نکته دیگر، استفاده از امکان ثبت دامنه به صورت خصوصی مانند Domains by Proxy است. در این نوع ثبت، مشخصات عمومی صاحبان دامنه‌ها با جستجوی اینترنتی قابل مشاهده نیست. بسیاری از عرضه‌کنندگان دامنه و میزبانی وب، خود در بسته‌های پیشنهادی به شما گواهینامه SSL پیشنهاد می‌کنند؛ با اطمینان از مرجع صادرکننده مانند Verisign, Thawte, Geotrust حتما برای وب‌سایت خود امکان SSL فراهم آورید.

۲. نکات بالا را در خصوص میزبانی وب نیز رعایت کنید. از میزبان‌های وب خارج از ایران، شناخته

شده و دارای محافظت در برابر حملات مختلف، خصوصا DDOS فضا تهیه کنید. میزان حمایت از مشتری میزبان را با جستجوی اینترنتی مورد ارزیابی قرار دهید تا در صورت حملاتی مانند پست تعداد بسیار زیاد کامنت، برای راه‌اندازی مجدد سایت خود دچار مشکل نشوید. این میزبان همچنین می‌بایستی امکان بک‌آپ مرتب، امکان ساخت لیست خبرنامه با ایمیل را ارائه دهد و ایمیل‌های ارسالی از این میزبان توسط فیلترهای اسپم در گوگل و... فیلتر نشود. همچنین اطمینان حاصل کنید هاست شما دائما نسخه‌های نرم‌افزارهای تحت وب خود را آپدیت و به‌روزرسانی می‌کند و قادر است اطلاعات تفصیلی از میزان، منبع و کیفیت مراجعات به وب‌سایت شما را در اختیارتان قرار دهد.

۳. شما احتمالا برای مدیریت محتوای خود از سیستم‌های مدیریت محتوا (CMS) مانند وردپرس، دروپال یا جوملا استفاده می‌کنید. متأسفانه نرم‌افزارهای برآمده از PHP کارنامه خوبی در زمینه امنیت ندارند و اشکالاتشان شامل فهرست بلندبالایی از حفره‌ها و ضعف‌های امنیتی می‌شود. بحث پیرامون نحوه انتخاب این نرم‌افزار موضوع این جزوه نیست. تنها به خاطر داشته باشید که افزونه‌ها - پلاگین‌ها و قالب‌ها - پوسته‌های صددرصد شناخته شده را مورد استفاده قرار دهید. بسیاری از پوسته‌های رایگان حاوی کد جاوا، برای سرقت ترافیک و یا اطلاعات شما هستند. در اغلب موارد استفاده از پوسته سبک، ارجینال و ساده وردپرس بهتر از استفاده از پوسته‌ای زیبا، سنگین و حاوی کدهای انتقال ترافیک است. اساسا سبک بودن پوسته با وضعیت اینترنت در ایران خصوصا زمان انتخابات همخوانی بیشتری دارد.

۴. در هنگام طراحی و اجرای وب‌سایت از نمایش عمومی اطلاعات کاربران خودداری کنید. لیست حمایت از کاندیداها را به نمایش نگذارید. کامنت‌ها را به صورت اتوماتیک منتشر نکنید. انتشار ویرایش‌شدهٔ کامنت‌ها، جلوی اشتراک لینک‌های آلوده‌ای را که با هدف شناسایی کاربران سایت شما ارسال می‌شوند، خواهد گرفت. عوامل امنیتی غالبا در شکل کاربر ظاهر شده و با ایجاد ارتباط از طریق کامنت، ارسال لینک آلوده و... قصد شناسایی گردانندگان سایت و کاربران فعال آن را دارند.

این لینک‌ها می‌تواند به صورت ارجاع به یک سایت آلوده با نرم‌افزارهای فلش یا جاوااسکریپت و یا در قالب ایمیل و فایل الصاقی (attachment) وُرد یا پی‌دی‌اف باشد. کافیست شما آن پی‌دی‌اف آلوده را برای کاربران سایت خود ارسال نمائید تا صدها یا هزاران کامپیوتر دیگر آلوده شوند.

۵. هکرهای دولتی، از امکاناتی برای شناسایی حفره‌ها و ضعف‌های امنیتی وب‌سایت‌ها برخوردارند. از این حفره‌ها برای نفوذ به وب‌سایت شما استفاده خواهد شد. شما می‌توانید از امکانات فراوانی که برای کشف و ارزیابی این آسیب پذیری‌ها وجود دارد، استفاده کنید. فهرست این امکانات نیز خارج از حوصله این جزوه است، اما استفاده از امکانات رایگان modsecurity.org توصیه می‌شود.

۶. بر اساس تجربه من از حملات پیشین علیه وب‌سایت‌های منتقد، بخش اعظم این حملات یا با بازداشت و ضبط فیزیکی کامپیوتر و پسوردهای عوامل فنی این سایت‌ها همراه بوده است و یا با استفاده از شیوه‌های مهندسی اجتماعی مانند ظاهر شدن در لباس یک دوست، یک داوطلب کمک و... با هدف نفوذ به سیستم. حفاظت فیزیکی ابزارهای دیجیتال خود را جدی بگیرید. از پخش اطلاعات غیرکدگذاری شده روی کامپیوترهای مختلف یا تلفن‌های هوشمند و تبلت‌ها اکیدا خودداری کنید. با شکستن قفل، ورود به دفتر شما و یا سرقت یکی از این کامپیوترها، افراد می‌توانند همه اطلاعات شما را

سرقت کنند.

لیست‌های حساس بهتر است به صورت کدگذاری شده روی cloud یا سرورهای مطمئن خارج از ایران مانند Google یا آمازون ذخیره شود. فایل لیست را با نرم‌افزارهای کدگذاری مختلف کدگذاری کرده و سپس روی cloud ذخیره کنید.

پسورد دسترسی به این فایل‌ها را در اختیار یکی از دوستان خود در خارج از ایران قرار دهید تا پس از بازداشت احتمالی شما، پسورد و شماره تلفن ارسال پیام کوتاه تائید یا sms verification را به سرعت تغییر دهد.

۸. برای مقابله با حملات DDOS خصوصا در روزهای نزدیک به انتخابات، از امکانات Cloudflare و Deflect استفاده کنید، راهنمای پیشگیری از حملات DDOS در آدرس زیر در دسترس است:
http://tech.tavaana.org/story/ddos-Deflect

امنیت کمپین روی شبکه‌های اجتماعی

کمپین‌ها ده‌ها و صدها صفحه، شناسه و یا گروه را روی شبکه‌های اجتماعی راه‌اندازی می‌کنند: روزنامه‌نگاران حامی یک کاندیدا، مادران علیه کاندیدای دیگر، صفحه خراسانی‌ها برای کاندیداتوری یک کاندیدا و غیره.

در یک انتخابات آرام و غیررقابتی ریسک زیادی در ایجاد و عضویت در این صفحات و گروه‌ها وجود ندارد. به عنوان صاحب شناسه، گروه و یا صفحه، شما باید توصیه‌های امنیت شبکه‌های اجتماعی را رعایت کنید؛ در پذیرش عضویت‌ها دقت کنید، از تگ شدن در عکس‌ها و مطالب حساسیت‌برانگیز جلوگیری کنید، اجازه پست تائید نشده را روی وال خود ندهید و دائما اعضای صفحه و گروه را با ریسک کاری که انجام می‌دهند آشنا کنید، به ایشان بگویید در گروه‌های عمومی، نیروهای امنیتی دائما اعضاء را فهرست و شناسایی می‌کنند. بنابراین اگر شغل حساسی دارند یا از ایشان تعهدی مبنی بر عدم فعالیت سیاسی اخذ شده و یا به دلایل مشابه، فعالیت سیاسی - انتخاباتی ایشان حتی در چهارچوب‌های قانونی مورد پذیرش پلیس سیاسی نیست، از عضویت و فعالیت با نام و مشخصات واقعی خود خودداری کنند. توجه داشته باشید که آنها دائما در حال ضبط و ذخیره‌سازی تصاویر و ویدئوهای منتشره شما و دوستان شما هستند تا بعدها علیه شما در ساخت برنامه و یا انتشار اخبار دروغ و... مورد استفاده قرار گیرد.

نیروهای امنیتی با ایجاد شناسه‌های جعلی قصد ایجاد ارتباط و شناسایی فعالان ناشناس را دارند. در مورد فعالان شناخته شده نیز برای تشکیل پرونده اتهامی و دلیل بازداشت سعی خواهند کرد با پست کامنت‌های رادیکال و تهییج، آنان را وادار به پست مطالبی کنند که بعدها بتوان برای محکوم کردن ایشان مورد استفاده قرار داد. اگر در یک کمپین انتخاباتی و در چهارچوب‌های سیاست قانونی جمهوری اسلامی ایران فعالیت می‌کنید، اجازه ندهید فعالان شناخته شده در صفحه شما وارد گفتگو و تبادل نظر با افراد حساس از منظر دستگاه‌های امنیتی شوند. تردیدی وجود ندارد که نیروهای امنیتی خود به این نوع تبادل نظر دامن می‌زنند تا بعدها بتوانند سر منشاء فعالیت سیاسی شما را خارج از کشور معرفی کرده و رهبری کمپین شما را به عناصر غیرقانونی از دیدگاه حاکم منتسب نمایند.

پروفایل خصوصی – پروفایل سیاسی

پروفایل خصوصی شما جایی است که اعضای خانواده، دوستان نزدیک، پسرخاله، دخترداییو مادر شما تصاویر خانوادگی را به اشتراک می‌گذارند، اما پروفایل سیاسی شما شناسه‌ای است که کمپین و فعالیت سیاسی – مدنی خود را از آن طریق پیگیری می‌کنید. بهتر است میان این دو پروفایل دوست مشترکی نداشته باشید. در پروفایل خصوصی خود هیچ فرد ناشناسی را قبول نکنید و در پروفایل سیاسی، امکان تگ کردن و پست روی وال را از بین ببرید. پست کردن مطلب توسط افراد ناشناس روی دیوار شما، امنیت دوستان شما را به خطر خواهد انداخت. از راهنمای شبکه‌های اجتماعی توانا برای بالابردن امنیت هر دو پروفایل استفاده کنید.

امنیت تلفن‌های همراه

تلفنهای هوشمند و همراه به بخش جدایی‌ناپذیر کمپین‌ها تبدیل شده‌اند، از شرکتی که قصد تبلیغ بستنی خود با پخش پنج تُن بستنی در ولنجک تهران را با ارسال SMS به شهروندان دارد گرفته تا کمپین هواداران کاندیداهای انتخابات، همه و همه از سرویس‌های مختلف تلفن همراه برای بالابردن کارایی کمپین خود استفاده می‌کنند.

نکات زیر را به هنگام استفاده از تلفن‌های همراه، مورد نظر قرار دهید:

۱. ساخت لیست اشتراک SMS در ایران برای فعالیت‌های انتخاباتی ایده‌ای با ریسک بالاست، دولت قادر است ارسال یک SMS یکسان را به فهرست مشترکان شما رصد کند و از آنجا که خرید سیم‌کارت در ایران بدون ارائه اوراق شناسایی و احراز هویت ممکن نیست، دولت به سادگی لیست صاحبان شماره‌های مشترک شما را در اختیار دارد.

۲. ساماندهی فعالان ستادهای انتخاباتی با توزیع سیم‌کارت ستاد میان ایشان، این ریسک را به همراه می‌آورد که منابع دولتی رفت و آمد همه فعالان شما را از طریق رصد موقعیت جغرافیایی صاحبان این سیم‌کارت‌ها کنترل کنند و در هنگام بازداشت گسترده اعضای ستاد، به سادگی همه افراد را بیابند. اگر از این سیستم استفاده می‌کنید به اعضای شبکه خود بگویید در هنگام قرارهای حساس و یا ریسک بازداشت دست جمعی، تلفن خود را همراه نداشته باشند.

۳. دولت معمولا در هنگام ناآرامی، سرویس کل شبکه تلفن‌های همراه را به سادگی متوقف خواهد کرد؛ برای تماس با اعضای ستادهای خود راه‌های سنتی و جایگزین سراغ داشته باشید.

۴. تلفن همراه را هم مانند پروفایل یا ایمیل خصوصی و سیاسی، با تلفن همراه خصوصی خود یکجا مورد استفاده قرار ندهید. یک سیم‌کارت برای فعالیت در ستاد انتخاباتی و یک سیم‌کارت خصوصی شماست. توجه داشته باشید در صورت بازداشت یا هک تلفن خصوصی شما، تصاویر، ویدئوها، داده‌ها و دفترچه تلفن، فهرست تماس‌ها و... بر علیه شما مورد سوء استفاده امنیتی – سیاسی قرار خواهد گرفت.

۵. تلفن همراه، کول دیسک، فلش درایو یا سی‌دی نیست. داده‌های خود را با تلفن حمل و نقل نکنید. داده‌های خود را مرتبا از روی تلفن‌ها پاک و حافظه آنها را با نرم‌افزارهای معرفی شده در توانا، غیرقابل بازیافت کنید.

۶. روی تلفن همراه خود برنامه‌هایی را نصب کنید که قادرند در صورت سرقت تلفن همراه حافظه تلفن را پاک کنند. بلافاصله پس از سرقت، تلفن خود را بلوکه کنید.

۷ سرویس موقعیت یاب (GPS) تلفن خود را به هیچ وجه روی شبکه‌های اجتماعی و سرویس‌هایی نظیر latitude فعال نکنید و از فعالان کمپین خود نیز بخواهید این امکان را غیرفعال کنند. با فعال بودن این سرویس به راحتی همه محل‌های حضور شما در ماه‌های گذشته به راحتی قابل مشاهده خواهد بود.

۸. اگر در تجمع حساسی قصد استفاده از تلفن همراه برای ضبط ویدئو را دارید، از تلفن بدون سیم‌کارت استفاده کنید.

توجه به عملیات روانی

در نظام‌های سرکوبگر، عملیات روانی، ارعاب و گمراه‌سازی شهروندان و فعالان، بخش محوری عملیات رسانه‌ای دستگاه‌های امنیتی است. بلافاصله پس از آنکه جمعی از جوانان راهپیمایی بی‌خشونتی در اعتراض به تقلب انتخاباتی برگزار می‌کنند؛

۱. دستگاه‌های امنیتی با انتشار دروغ از یک سو راهپیمایی را تلاش خشونت‌آمیز و بعضا مسلحانه، غارت بانک‌ها و آتش‌زدن مغازه‌ها جلوه می‌دهند تا افکار عمومی با احساس خطر، حساسیت کمتری در برابر سرکوب خشونت‌بار منتقدین داشته باشد.

۲. همین دستگاه‌ها گزارشات دروغی مبنی بر ناپدید شدن، قتل دسته‌جمعی و تجاوز گروهی به جوانان و خصوصا زنان معترض را در شکل وسیعی و با سوء استفاده و فریب روزنامه‌نگاران و فعالان خوشنام منتقد منتشر می‌کنند. انگیزه این اخبار دامن زدن به جو ناامنی و ترغیب خانواده‌ها به جلوگیری از خروج فرزندان خود از خانه است. هفته‌ها پس از ایفای این نقش، نیروهای امنیتی این‌بار خود این اخبار را کذب اعلام کرده و رسانه‌های منتقد را متهم به دروغگویی و فریب افکار عمومی می‌کنند. نمونه روشن این عملیات ماجرای سعیده پورآقایی در خلال ناآرامی‌های سال ۱۳۸۸ است.

۳. بخش دیگری از عملیات روانی، ایجاد تردید و از بین بردن انسجام نیروهای منتقد است. با ایجاد یک شبهٔ پروفایل‌های مختلف در قالب طرفداران تحریم و یا هواداران کاندیداهای منتقد و دیگر منتقدین حکومت، جو توهین، چند دستگی و ستیز بر منتقدان تحمیل می‌شود.

۴. با انتشار شایعات و اخبار دروغین در شبکه‌های اجتماعی خصوصا فیس‌بوک و توئیتر و سایت‌های اشتراک لینک نظیر بالاترین، رهبری اعتراضات مورد هدف قرار می‌گیرد. در جریان اعتراضات سال ۱۳۸۸ اخبار متعددی دال بر هک و مشکوک بودن سایت کلمه و یا تصرف رسانه‌های اصلاح‌طلب و انتشار آنان توسط نیروهای امنیتی منتشر شد. با انتشار هر بیانیه و دعوت به تجمع در یک میدان مشخص، چند بیانیه و دعوت بی‌نام‌ونشان دیگر برای تجمع در مراکز دیگر منتشر می‌شدند و نیروهای امنیتی به صورت شبانه‌روزی سرگرم ایجاد سردرگمی میان معترضین بودند. محافظت فنی از رسانه‌های سهل‌الوصول منتقدین و تماس مداوم و اطلاع‌رسانی با روزنامه‌نگاران مورد اعتماد راه را بر رواج اینگونه شایعات خواهد بست.

۵. خاصیت شبکه‌های اجتماعی نظیر توئیتر، علاقه کاربران به بازنشر سریع و لحظه‌ای اخبار است. رسانه‌های جدی‌تر و مراکز ارتباطی کمپین همواره می‌بایستی اخبار با منشاء بلاگ‌های ناشناس، فیس‌بوک و توئیتر را با وسواسی دو چندان، راست‌آزمایی کنند. گاه تاخیر در انتشار خبر، بسیار بهتر از انتشار خبر کذب و ضرربار است.

۶. از مهمترین بخش‌های عملیات روانی نیروهای سرکوبگر، دامن زدن به پارانویا و ارعاب، ادعای حضور حکومت و اشراف کامل اطلاعاتی است. هدف از این عملیات به خانه راندن فعالان و توقف فعالیت‌های منتقدین است. در خلال اعتراضات سال ۱۳۸۸ به صورت روزانه چندین لینک روی بالاترین و شبکه‌های اجتماعی با مضامینی شبیه این منتشر می‌شد: ایرانسل همه فعالیتهای شما را برای سپاه می‌فرستد.؛ هر کس SMS اعتراض به نتایج انتخابات دریافت کرده است، پنهان شود، والا دستگیر خواهد شد؛ سپاه همه چیز شما را کنترل می‌کند؛ تمام سایت‌های مخالفین در حقیقت در اختیار سپاه و کمینی برای شما هستند.

http://www.tavaana.org

پروژهٔ

e-collaborative
for civic education

http://www.eciviced.org