رویداد

جزییات طرح جامع فضای مجازی سالم

● **شرق:** طرح جامع توسعه فضای مجازی سالم، مفید و ایمن، در بیست‌ودومین جلسه شورایعالی فضای مجازی مورد بحث و بررسی قرار گرفته و مصوب شد. به‌گفته دبیر شورایعالی فضای مجازی کشور در طرح جامع توسعه فضای مجازی سالم، مفید و ایمن، محتوا و خدمات مفید براساس مشارکت داوطلبانه کاربران فضای مجازی ارایه می‌شود. محمدحسن انتظاری، افزود: براساس مصوبه آخرین جلسه شورایعالی فضای مجازی کشور، تدوین راهبردها و سیاست‌ها، طراحی چارچوب اقدامات، ضوابط و معیارهای خدمات و محتوای مربوط به «طرح جامع توسعه فضای مجازی سالم، مفید و ایمن» با توجه به تعریف و اهداف مصوب شورا به مرکز ملی فضای مجازی کشور واگذار شده است. او ادامه داد: کاربران می‌توانند به صورت داوطلبانه و مشارکتی در فضای مجازی سالم براساس ویژگی‌های جمعیتی از جمله سن، جنس، شغل و تحصیلات از محتوا و خدمات موردنیاز بهره‌مند شوند و حتی‌الامکان در برابر محتوا و رفتارهای آسیب‌زا محفوظ بمانند.

ورود مرکز فضای مجازی به سیاستگذاری پهنای باند اینترنت

● **مهر:** معاون مرکز ملی فضای مجازی از تدوین دستورالعمل قیمت‌گذاری در حوزه باند پهن اینترنت و تصویب آن در کمیسیون عالی تنظیم مقررات این مرکز خبر داد. سعید مهدیون با اعلام این خبر گفت: این دستورالعمل در صف مصوبات شورایعالی فضای مجازی است. او ادامه داد: مدل‌های قیمت‌گذاری پهن‌باند تدوین و در کمیسیون عالی تنظیم مقررات مرکز ملی فضای مجازی مصوب شده است. به گفته او با تصویب این دستورالعمل، از این پس مشخص خواهد شد با چه سیاست‌هایی باید تعرفه‌گذاری در زمینه اینترنت پرسرعت و پهنای باند اینترنت صورت گیرد. او افزود: از پهن‌باند به‌عنوان اکوسیستم اینترنت نام برده می‌شود که مدل‌ها و تعاریف متفاوت و مختلفی دارد؛ به‌نحوی که حتی محتوای اینترنت را نیز شامل می‌شود. او ادامه داد: در این مدل قیمت‌گذاری. پهن‌باند هفت‌الگو در نظر گرفته است که جریان اقتصادی برای تمامی الگوها در نظر گرفته شده است. او همچنین گفت: سیاست‌های توسعه پهن‌باند نیز در دست تدوین است که امیدواریم تا پایان سال به اتمام برسد و به‌دلیل اهمیت موضوع و تصمیم‌گیری و سیاستگذاری برای این بخش، در جلسات آینده شورایعالی فضای مجازی به تصویب برسد.

جزییات تغییر پروانه‌های شرکت‌های اینترنتی و اپراتورها

● **ایسنا:** در سال۹۴ پروانه‌های جدید، در حوزه اینترنت و با دوعنوان ارتباطات ثابت (FCP) و ارایه خدمات ارتباطی ثابت (servco) برای اپراتورهای تلفن‌همراه و شرکت‌های ارایه‌دهنده خدمات اینترنتی از سوی رگولاتوری صادر خواهد شد. سازمان تنظیم مقررات و ارتباطات رادیویی با اشاره به ساماندهی تمامی مجوزهای ارتباطی با صدور پروانه‌های جدید اعلام کرد قرار است به منظور حرکت به‌سمت همگرایی موبایل و تلفن ثابت تغییراتی را در پروانه‌ها ایجاد کند. بر این اساس قرار است پروانه‌های اپراتورهای تلفن‌همراه و اپراتورهای مجازی با عنوان MVNO در دوبخش جداگانه راه‌اندازی شبکه زیرساخت تلفن‌همراه و به‌جز شبکه دسترسی رادیویی و ارایه‌دهندگان سرویس خدمات مجوز بگیرند.

حفره امنیتی FREAK در کمین کاربران

وب‌سایت‌های ایرانی‌ای که امن نیست

علی ارغوان: تیمی حرفه‌ای از کریپتوگرافرها (متخصصان رمزنگاری) به‌تازگی متوجه شده‌اند یک‌حفره امنیتی مربوط به دهه۹۰میلادی به‌نام FREAK گوشی‌ها، تبلت‌های اندرویدی و iOS را به حملات سایبری آسیب‌پذیر کرده است. این مشکل سافاری بر روی مک، iOS یا مرورگر پیش‌فرض (قدیمی) اندروید را مورد هدف قرار می‌دهد. FREAK مخفف عبارت «Factoring attack on RSA-EXPORT Key» یا حمله فاکتوری به کلید RSA نامیده شده است و وقتی کاربر به یک سایت «ایمن» با پروتکل HTTPS مراجعه می‌کند، او را در معرض خطر قرار خواهد داد. فهرست سایت‌هایی که از RSA Export استفاده می‌کنند و احتمال بروز مشکل امنیتی در آنها وجود دارد، در وب‌سایتی به نام freakattack.com درج شده است که نام وب‌سایت‌های مشهوری مانند American Express، BusinessInsider، Sohu، بلومبرگ، 4Shared و در سایت‌های ایرانی «بانک ملی ایران»، «مشرق‌نیوز»، «افکارنیوز»، «تمین»، «انتخاب» و «شفاف» نیز در آن به چشم می‌خورد. به این‌ترتیب اگر با سایت‌های یادشده سروکار دارید، توصیه می‌کنیم از مرورگر سافاری چه در iOS و چه OS X و همچنین مرورگر قدیمی پیش‌فرض اندروید استفاده نکنید. خوشبختانه تعداد سایت‌های آسیب‌پذیر از ۱۲/۲درصد کل یک‌میلیون دامنه برتر در الکسا به ۹/۷درصد کاهش پیدا کرده است.

اما مشکل از کجا آغاز شده است؟ ظاهرا دولت آمریکا مدتی پیش شرکت‌ها را ملزم کرد برای بازدیدکنندگان خارجی از الگوریتم

رمزگذاری ضعیف‌تر ۵۱۲ بیتی استفاده کنند در حالی‌که بازدیدکنندگان آمریکایی از الگوریتم به‌مراتب ایمن‌تر ۱۰۲۴بیتی بهره‌مند می‌شوند. برای سوییچ‌کردن و تشخیص خودکار کاربران، توسعه‌دهندگان SSL یک مکانیسم طراحی کردند که بتواند این‌کار را انجام دهد. با وجود اینکه این محدودیت دولت آمریکا برداشته شد، اما دیگر دیر شده بود. هکرها به‌سادگی می‌توانند برخی مرورگرها را وادار به استفاده از الگوریتم قدیمی‌تر کنند که می‌توان آن را طی هفت‌ساعت توسط ۷۵ کامپیوتر رمزگشایی کرد در صورتی که الگوریتم ۱۰۲۴بیتی برای شکستن نیاز به چندین‌میلیون‌کامپیوتر و یک‌سال زمان دارد! شاید بپرسید چرا سایت ایرانی حساسی مانند بانک ملی باید از SSLهای خارجی استفاده کند؟ جواب اینجاست که تنها چندشرکت معتبر ارایه‌دهنده این گواهینامه‌ها وجود دارد و چیزی تحت عنوان SSL ایرانی نداریم.

به‌گفته «متیو گرین» پروفسور محقق امنیتی این تصمیم امنیتی برای آن گرفته شده بود که NSA یا همان آژانس امنیت ملی آمریکا بتواند به اطلاعات تبادل‌شده «دسترسی» داشته باشد درحالی‌که کماکان حداقل امنیت لازم برقرار است. اگر این حفره امنیتی قدیمی مربوط به دهه۹۰میلادی کماکان می‌تواند کاربران را در معرض خطر قرار دهد، پس تعجبی ندارد که اخیرا خبرهای زیادی در مورد شنود مکالمات و اطلاعات کاربران توسط NSA به گوش می‌رسد.

محققان هنوز نمی‌توانند بگویند آیا کسی از این حفره امنیتی برای نفوذ استفاده کرده یا خیر اما امکان آن را اثبات کرده‌اند. یک نفوذگر ماهر با امکانات مناسب قادر خواهد بود اطلاعات بازدیدکنندگان این وب‌سایت‌ها را بدزدد و حتی به برخی اطلاعات خود سایت نیز دسترسی داشته باشد. به گزارش فارنت، اپل و گوگل هردو اعلام کرده‌اند در تلاش برای رفع این مشکل هستند. درحالی‌که کاربران iOS و OS X می‌توانند تا هفته دیگر این آپدیت امنیتی را دریافت کنند اما ممکن است گوگل نتواند از طریق Google Play Services این آپدیت را عرضه کند؛ پس بهتر است فعلا از مرورگرهایی مانند کروم و فایرفاکس در گوشی یا تبلت‌های اندرویدی خود استفاده کنید.

مدیریت کشور بدون فاوا؟!

سهیل مظلوم واجاری*

آنجایی که کشور فرصت آن را یافته است که برای هدایت نظام مدیریت و برنامه‌ریزی، سازمان مدیریت با معماری جدید احیا و نوسازی شود، به یقین نام آقای نوبخت و دیگر مدیران آن همچون آقای ابتهاج در نظام برنامه‌ریزی کشور ماندگار و به سبب چگونگی تاسیس مجدد آن، همیشه درتاریخ مورد قضاوت واقع خواهند شد. به حکم وظیفه در باب نقش فناوری اطلاعات و ارتباطات در پیشبرد اهداف برنامه‌ریزی و استقرار سازمانی مدرن بر پایه توجه کامل به فناوری اطلاعات و ارتباطات نکاتی را متذکر می‌شوم.

ازمنظر نوسازی دولت

در حال حاضر کشور به شیوه‌ای گران اداره می‌شود. استفاده از روش‌های سنتی کشورداری نتیجه‌ای جز فساد اداری و ناامیدی مردم دربرندارد. در برخی دستگاه‌ها حتی برای انجام کاری کوچک یا باید متوسل به آشنا و توصیه شد یا به طرق دیگری دست به‌کار رفع موانع شد، موانعی که اکثرا پایه قانونی نداشته و عموما ناشی از عدم اطلاع مراجعان یا پیچیده‌بودن فرآیند اداری است. برای حل این معضل، طبق تعریف نوسازی و تحول اداری یکی از وظایف اصلی این سازمان محسوب می‌شود. پر واضح است امروزه نه‌تنها اداره کشوری به وسعت و جمعیت ایران که حتی اداره یک فروشگاه کوچک نیز بدون بهره‌گیری از نظام فناوری اطلاعات و ارتباطات میسر نیست. برای این منظور قانون‌گذار در قانون مترقی مدیریت خدمات کشوری فصلی را به‌طور مشخص به کاربرد فناوری اطلاعات در دستگاه‌های دولتی اختصاص داده و در فصول دیگر خاصه آنجا که به برون‌سپاری وظایف تصدی‌گری دولت می‌پردازد روش‌های نوین در اداره کشور را ملاک می‌داند. براساس منطق حاکم بر این قانون که علی‌الاصول یکی از مبانی فعالیت سازمان جدید را تشکیل می‌دهد این مهم، یعنی تحول اداری و مهندسی مجدد ساختار دولت محقق نمی‌شود مگر با استفاده از ابزار فناوری اطلاعات و ارتباطات و بسط کاربردهای آن در ساختار و وظایف دولت که در ادبیات جاری دنیا به «دولت الکترونیک» مشهور است.

از آنجایی که دستگاه‌های وابسته به دولت برای اصلاح ساختاری خود نیازمند مجوز سازمان مدیریت و برنامه‌ریزی بوده و از سوی دیگر بودجه و منابع مالی آنها نیز تحت‌نظر همین سازمان هزینه خواهد شد، پس بایسته است سازمان جدید با داشتن هدف و برنامه‌ای روشن در زمینه فناوری اطلاعات و ارتباطات، اختصاص بودجه و اصلاح ساختار سازمانی دستگاه‌ها را با توجه به زیرساخت فاوا و نقشی که در مهندسی مجدد آنها ایفا می‌کند، ارزیابی کند. بی‌تردید استفاده از ابزارهای بودجه‌ای و بخشنامه‌ای سازمان مدیریت در اصلاح فرآیندهای ارایه سرویس‌های شفاف و آسان به مردم کلید بسط رفاه عمومی و کاهش هزینه‌های اداره کشور خواهد بود.

ازمنظر درون‌سازمانی

اگر بپذیریم عمده بهانه‌های (شاید دلایل)انحلال سازمان مدیریت و برنامه‌ریزی در دولت سابق رفتار بعضا ناعادلانه، کندی بوروکراتیک و عدم شفافیت عملکرد این دستگاه بوده است، برای آنکه سازمان جدید نیز به همان مسایل مبتلا نشود نیازمند آن است که سریع و شفاف عمل کند، با وجود آنکه واژگان مقدس عدالت و برابری فرصت‌ها در چندسال اخیر متاسفانه مورد سوءاستفاده واقع شده‌اند. اما اگر سازمان بخواهد واقعا به عدالت رفتار کرده و اصل برابری فرصت‌ها را رعایت کند، چه راهکاری جز استفاده از فناوری اطلاعات و ارتباطات دارد؟ برای اداره سازمانی که منابع مالی و انسانی کشور را مدیریت کرده، در استان‌ها دارای سازمان‌های وابسته بوده و در اقصی نقاط کشور ذی‌نفعانی چون مردم عادی، شرکت‌ها، پیمانکاران و دوایر متعدد دولتی دارد و می‌خواهد بنای مستحکمی در بسط عدالت، شفافیت و سرعت در پاسخگویی به نیازهای میان‌مدت و بلندمدت توسعه‌ای کشور باشد، حق آن است که خود به مهم‌ترین زیرساخت توسعه، یعنی فناوری اطلاعات و ارتباطات مجهز باشد. پس بایسته است شالوده سازمان جدید بر زیرساخت فاوا بوده و کلیه فرآیندهای سازمان برپایه این فناوری راه‌اندازی شود.

ازمنظر نظارتی

یکی دیگر از مبانی قانونی فعالیت سازمان مدیریت آتی قانون برنامه و بودجه است. حسب ماده۲۲ این قانون، احراز صلاحیت و رتبه‌بندی پیمانکاران و مشاوران از وظایف سازمان است. باوجود اینکه در سال‌های اخیر با راه‌اندازی سامانه موسوم به ساجات قدم‌هایی در راه مکانیزه‌شدن این وظیفه در سازمان برداشته شده است، نظری به آگهی صفحات نیازمندی‌های روزنامه‌ها نشان می‌دهد تا حصول به سیستمی شفاف و غیربوروکراتیک راه درازی در پیش و بدون مدد از فاوا غیرممکن است. علاوه‌بر این وظیفه دفتر بخشی فناوری اطلاعات و ارتباطات بر تخصیص منابع و چگونگی هزینه‌کرد آن توسط دستگاه‌های اجرایی هم از دیگر وظایف نظارتی آن سازمان به‌شمار می‌آید.

ازمنظر راهبری کلان فناوری اطلاعات

از سال۱۳۵۹ با مصوبه شورای انقلاب نهادی به‌نام شورایعالی انفورماتیک در زیرمجموعه سازمان مدیریت تاسیس شد. این شورای ۱۱نفره که با حضور نمایندگان دستگاه‌های دولتی ذی‌ربط و نمایندگان بخش خصوصی و مراکز کامپیوتری شکل می‌گیرد، وظیفه نظارت بر مسایل انفورماتیکی کشور از منظر مدیریت اجرایی را عهده‌دار بوده است؛ هرچند در سال‌های اخیر با تاسیس شوراهای گوناگون نظیر شورایعالی اطلاع‌رسانی، شورایعالی فضای مجازی، تاسیس وزارت ارتباطات و فناوری اطلاعات و البته گماردن مسوولان نه چندان آشنا با مباحث کلان فناوری اطلاعات بر این شورا، به همراه شوک ناشی از انحلال سازمان و رکود فعالیت شوراها در دولت‌های نهم و دهم جایگاه سال‌های گذشته را از دست داده است اما همچنان یکی از ارکان مدیریت فناوری اطلاعات کشور بوده و جایگاه منحصربه‌فردی در احراز صلاحیت و رتبه‌بندی شرکت‌های فناوری اطلاعات و صدور تاییدیه فنی برای نرم‌افزارهای تولیدی و رعایت حقوق پدیدآورندگان آن طبق قوانین حمایت از پدیدآورندگان نرم‌افزارهای رایانه‌ای مصوب ۱۳۷۹ و قانون ارتقای سلامت اداری مصوب ۱۳۸۹ را دارد.

> **در حال حاضر کشور به شیوه‌ای گران اداره می‌شود. استفاده از روش‌های سنتی کشورداری نتیجه‌ای جز فساد اداری و ناامیدی مردم دربرندارد. در برخی دستگاه‌ها حتی برای انجام کاری کوچک یا باید متوسل به آشنا و توصیه شده یا به طرق دیگری دست به‌کار رفع موانع شد موانعی که اکثرا پایه قانونی نداشته و عموما ناشی از عدم اطلاع مراجعان یا پیچیده‌بودن فرآیند اداری است**

نتیجه‌گیری

بنا به آنچه گفته شد به‌نظر می‌رسد چه از منظر رویکرد درون‌سازمانی و توجه صرف به نقش سازمان مدیریت آتی جهت مدیریت بهینه منابع و نیروی انسانی، چه از منظر نقش توسعه‌ای سازمان برای مهندسی مجدد فرآیندهای اداره ارزان‌تر کشور یا از منظر وظایف نظارتی سازمان یا اجرای وظایف محوله براساس لایحه قانونی مصوب ۱۳۵۹ شورای انقلاب و سایر قوانین مربوط به فناوری اطلاعات، سازمان مدیریت آتی را از توجه به فناوری اطلاعات و ارتباطات گریزی نیست و جا دارد که سطح فناوری اطلاعات تا معاونت در چارت سازمان جدید بالا رود.

درعالم‌واقع

اما در کمال تعجب دیده می‌شود که در چارت جدید پیشنهادی، کلیه وظایف دبیرخانه شورایعالی انفورماتیک به وزارت ارتباطات و فناوری اطلاعات منتقل خواهد شد. جدای از خلاف‌قانون‌بودن این اقدام که وظایف یک دستگاه بدون طی مراحل قانونی به دستگاه دیگر واگذار می‌شود، جداکردن نهاد نظارتی حوزه فناوری اطلاعات از دستگاه فرابخشی سازمان مدیریت و واگذاری آن به یک دستگاه بخشی نظیر وزارت فاوا مثل آن است که فرمانده کشتی تصمیم گرفته باشد در اقیانوسی پرتلاطم، سیستم رادار و کنترل ناوبری خود را به دریا فکنده و با همان شیوه ملوانان کشتی‌های بادبانی با یا بدون قطب‌نما دل به اقیانوس بسپارد. تجربه چندسال گذشته که کشور با انبوه منابع مالی ناشی از فروش نفت با قیمت رویایی مواجه بود نشان داد که بدون نظارت و استفاده از فناوری‌های نوین می‌توان گنج قارون را هم برباد داد. درحالی‌که امروز کشور با مشکلات عدیده مالی درگیر است و بیش از هر زمانی محتاج آن است که با انضباط مالی بیشتر و ارزان‌تر از همیشه اداره شود، تکیه بر روش‌های سنتی کنترل و نظارت یعنی افتادن در همان دامی که در چندسال قبل گسترده و منجر به انحلال سازمان مدیریت شد. گویا هنوز روح رفتارهای گریزان از شفافیت و اداره‌کردن کشور با یک «بودجه‌نامه یک‌صفحه‌ای» از سازمان مدیریت و برنامه‌ریزی کشور رخت برنبسته و مسوولان فعلی آن هم ترجیح می‌دهند از همان رسم به‌غلط جاافتاده در دولت‌های نهم و دهم پیروی کنند. هضم این رفتار زمانی دشوارتر می‌شود که رییس فعلی سازمان مدیریت و برنامه‌ریزی، زمانی که در مسند قدرت نبود، در کسوت یک مدرس و استاد دانشگاه کتابی در باب «دولت الکترونیک» منتشر می‌کند. ظاهرا یا همان مثل قدیمی کوزه‌گر از کوزه شکسته آب می‌خورد دوباره مصداق یافته یا ایشان ترجیح داده‌اند که عافیت‌طلبی پیشه کرده و پای خود و سازمان متبوع خود را از گلیم داغ و توام با تنش و درگیری فناوری اطلاعات و ارتباطات ایرانی بیرون کشیده و عطای مزایای این فناوری را به لقای درگیری‌های آن با ذی‌نفعان دیگر بخشیده و با واگذاری کلی آن به دستگاهی دیگر با همان روش‌های سنتی به اداره منابع مالی و انسانی کشور بپردازند.

***نایب‌رییس پیشین سازمان نظام صنفی رایانه‌ای کشور**

نگاه

سیستم‌عامل انسانی در خطر هک

● گزارش تازه اینتل‌سکیوریتی در مورد زیان‌های ناشی از مهندسی اجتماعی، پست‌الکترونیک را اصلی‌ترین عامل خطر در امنیت سایبری در سیستم‌عامل انسانی می‌داند. سازمان‌ها در همه‌جای دنیا از همه نوع فناوری برای کمک به حفاظت از زیرساخت‌ها و نقاط پایانی در برابر خطرات امنیتی بهره برده‌اند. اما فناوری تنها موردی نیست که باید ایمن‌سازی شود. در گزارش تازه‌ای که شرکت امنیتی اینتل‌سکیوریتی منتشر کرده و عنوان آن «هک‌کردن سیستم‌عامل انسانی» نام دارد، محققان در مورد نقش مهندسی اجتماعی در امنیت سایبری می‌گویند. در این گزارش، مهندسی اجتماعی اینگونه تعریف شده است: «کاربرد عامدانه تکنیک‌های فریبکارانه‌ای که طراحی شده‌اند تا افراد را وادار به افشای اطلاعات یا انجام اقداماتی کنند که احتمال دارد به انتشار آن اطلاعات منجر شود.» اینتل‌سکیوریتی توضیح می‌دهد دونوع حمله مهندسی اجتماعی وجود دارد: شکار و کشت؛ در حملات شکار، مجرمان درصدد کسب اطلاعات و استفاده از کاربران با حداقل تعامل‌اند در حالی که در حملات کشت، مهاجمان ارتباطی با قربانی برقرار و سپس در طول زمان اطلاعات را استخراج می‌کنند. به گزارش مهر، راج سامانی، معاون و مسوول ارشد فناوری در اینتل‌سکیوریتی می‌گوید: ایمیل در تمام انواع مهندسی اجتماعی اصلی‌ترین عامل خطر است. طبق گزارش سازمان فناوری اطلاعات ایران، اینتل‌سکیوریتی با آزمون آنلاینی که در ماه می سال۲۰۱۴ به اجرا درآورد، نشان داد چقدر راحت می‌توان با ایمیل فیشینگی که برای مهندسی اجتماعی طراحی شده، افراد را به دام انداخت. هدف این آزمون کسب اطلاع از میزان مهارت آزمون‌دهندگان در شناسایی حملات فیشینگ بدافزاری در میان ایمیل‌های کاری بود. به گفته این متخصص، در میان بیش از ۱۶هزار شرکت‌کننده این آزمون، ۸۰درصد لااقل در دام یکی از هفت‌ایمیل فیشینگ افتاده‌اند. علاوه‌بر این، معلوم شد کارکنان بخش‌های حسابداری و مالی و منابع انسانی -که حساس‌ترین داده‌های شرکت‌ها را در اختیار دارند- بدتر از سایر بخش‌ها عمل می‌کنند. بسته به اینکه حمله مهندسی اجتماعی برای شکار است یا کشت، اینتل‌سکیوریتی چهارمرحله را برای این حملات شناسایی کرده است؛ نخست تحقیق است که برای برخی از حملات که درواقع هدفی ندارند، اختیاری است. دوم به‌دام‌انداختن است که شامل درگیرکردن هدف و ایجاد داستانی است که موجب شکل‌گیری تعامل می‌شود. مرحله سوم چیزی است که اینتل‌سکیوریتی با عنوان «بازی» از آن یاد می‌کند و این مرحله‌ای از مهندسی اجتماعی است که برای استخراج اطلاعات طراحی شده است. مرحله چهارم و آخر، خروج است که طی آن، هدف مهاجم پایان‌دادن به تعامل با قربانی است؛ بدون اینکه قربانی متوجه شود که مورد سوءاستفاده قرار گرفته است. در گزارش اینتل‌سکیوریتی آمده است افراد، فرآیندها و فناوری برای کاستن از خطر لازمند. فناوری به‌تنهایی برای محافظت کاربران کافی نیست زیرا مسیرهای تهاجم فراتر از مکانیسم‌های ارتباطات دیجیتالی است. مسوول ارشد فناوری در اینتل‌سکیوریتی گفته است: «ایمیل متداول‌ترین روش است اما ارتباط رودررو، تلفن و موارد دیگر را نیز مدنظر قرار دهید. واقعیت این است که تنها مجموعه‌ای از کنترل‌ها می‌تواند بهترین راه مبارزه با این خطر باشد.» به نظر نمی‌رسد در سال۲۰۱۵ و بعد از آن، حملات مهندسی اجتماعی کاهش پیدا کند و احتمال رشد ارزش داده‌های شخصی و تقاضای بازار برای داده‌های سرقتی نیز وجود دارد. به‌گفته سامانی «این روش کار اکثر گروه‌های مجرمان سایبری و نیز گروه‌های هکتیویست است. واقعیت این است که حملات اجتماع‌بنیاد در آینده قابل‌پیش‌بینی همچنان ادامه خواهد داشت.»