استانداری آذربایجان شرقی
اداره کل پدافند غیرعامل

نشریه پدافند غیرعامل
شماره ۶ – آذر ماه ۱۳۹۴

در این شماره خواهید خواند:

شهادت شیخ نمر و ریختن به ناحق خون او خطای سیاسی دولت سعودی است. خداوند متعال از خون بی‌گناه نمی‌گذرد و خون به ناحق ریخته، بسیار سریع دامان سیاستمداران و مجریان این رژیم را خواهد گرفت. مقام معظم رهبری، حضرت آیت الله خامنه ای (مدظله العالی)

تزریق بی‌صدای نفوذ فکری و فرهنگی با امواج سایبری

«حاکمیت فضای مجازی اما در دست ما نیست، بنابراین قوانین آن نیز در اختیار ما نیست و همین قوانین کاربران فضای مجازی را به سمت شکستن مرزهای اخلاقی و خطوط قرمز ترغیب می‌کند.»

۳ میلیارد کاربر اینترنت در دنیا وجود دارد. از این ۳ میلیارد، ۴۶میلیون و ۸۰۰ هزار نفر ایرانی و از این تعداد ۲۳ میلیون و ۶۰۰ هزار نفر جوان هستند. بر مبنای آمار سامانه مدیریت ضریب نفوذ اینترنت در ایران به ۱۲/۸۲ درصد رسیده است و ضریب نفوذ تلفن همراه به ازای هر یکصد نفر ۹۱ نفر در جهان، در خاورمیانه ۱۰۰ و در ایران ۱۰۵ نفر است. حالا اگر آمار پلیس فتا درباره رشد جرائم اینترنتی در هشت ماه نخست سال را مورد بازبینی قرار دهیم با افزایش ۱۳ درصدی رشد جرائم اینترنتی مواجه می‌شویم که از این میزان ۱۱ درصد آن مربوط به جرائم اخلاقی است و قشر جوان را هدف گرفته است.

در این میان مطابق آمار جهانی در هر ۱۲ ثانیه یک نفر قربانی جرائم سایبری می‌شود. این آمار و ارقام اما بیش از هر چیز هشدار جدی رهبر معظم انقلاب درباره خطر نفوذ را با ادله‌ای از جنس عدد و رقم فریاد می‌کنند. مطابق آمار سن مجرمان در کشور ۱۵ تا ۳۲ سال است و متوسط آن ۵/۲۳ است. این آمار نشانه‌ای از نفوذ فرهنگی و فکری روی ذهن و فکر جوانان کشور ماست که بخش کوچکی از این نفوذ در قامت افزایش جرائم اخلاقی اینترنتی نمود می‌یابد.

به بیان دیگر نمی‌توان از نقش تأثیرگذار فضای مجازی و شبکه‌های اجتماعی در پیاده‌سازی پروژه نفوذ چشم‌پوشی کرد. کشش نسل جوان برای حضور در فضای مجازی و جذابیت‌های فراوان این فضا و قوانین خاص حاکم بر آن موجب شده اینترنت و فضای مجازی به یکی از اصلی‌ترین ابزارها برای نفوذ فکری و فرهنگی بدل شود. حاکمیت فضای مجازی اما در دست ما نیست، بنابراین قوانین آن نیز در اختیار ما نیست و همین قوانین کاربران فضای مجازی را به سمت شکستن مرزهای اخلاقی و خطوط قرمز ترغیب می‌کند. نسل جوان با گرایش بالایی که به سمت و سوی دنیای ناشناخته موجود در فضای مجازی دارد با هجوم اخبار و اطلاعاتی مواجه است که می‌کوشند بنیان‌های فکری‌اش را به هم بریزند.

منبع: http://paydarymelli.ir/fa/news/18887

جاسوسی اقتصادی

امروزه اسرار تجاری و اقتصادی برای دولت ها و سازمان های جاسوسی، از اسرار نظامی اهمیت بیشتری یافته است. به همین جهت جاسوسی اقتصادی روز به روز شدت گرفته و روش های تازه ای برای کسب اخبار و اطلاعات مفید به کار گرفته می شود .

اگرچه دولت ها می دانند که جاسوسی نمی تواند جانشین سیاست و استراتژی شود، ولی به خوبی به این امر واقفند که نمی توان در سیاستگذاری ها و تعیین استراتژی از آن بی نیاز بود. لذا به رغم داشتن هزینه های مادی، مالی، امنیتی و اجتماعی نسبت به جمع آوری اسناد و مدارک طبقه بندی شده اقدام می کنند.

اما جاسوسی به افراد زیرک و با جرأت نیاز دارد که توانایی ریسک پذیری بالایی داشته باشند. جاسوس به دست مأمورین اطلاعاتی آموزش می بیند تا برای انجام کاری به خارج از مرزها اعزام گردد، درحالی که مأمور اطلاعاتی در دفتر کار خود می نشیند و منتظر می ماند تا با وسایلی که در اختیار جاسوس گذاشته شده و اطلاعات رسیده از او به جمعبندی مفهومی و محتوایی برسد. به هر تقدیر امروزه سازمان های جاسوسی به عنوان خط اول دفاع از مصالح و منافع حیاتی کشورها محسوب می شوند.

سیستم اطلاعاتی و جاسوسی، در ابتدای هزاره سوم میلادی درصدد اطلاع از همه چیز در هر زمان و هر مکان و تحت هر شرایط است.

جمع آوری اطلاعات اقتصادی جزئی از قدرت اقتصاد ملی شناخته می شود و از پایه های اساسی امنیت ملی هر کشوری به شمار می آید از این نظر می توان گفت سازمان های جاسوسی مأموریت دارند که آنچه را کشورها با جنگ نتوانستند به آن برسند، با عملیات جاسوسی به انجام برسانند.

سازمان مرکزی اطلاعات آمریکا (سیا) در همه جای دنیا و در هر موقعیتی شروع به اقدام های خرابکارانه، براندازی و یا جاسوسی کرده و می کند. مثلاً این سازمان برای تأمین هزینه های سنگینی که در ویتنام می پرداخت، در اوایل جنگ ویتنام دست به جعل میلیون ها دلار برای خرج کردن در ویتنام زد. سازمان اطلاعات مرکزی آمریکا یک اداره مالی ویژه دارد که این گونه عملیات ها را اداره می کند. این اداره کارمندانی در اختیار دارد که می توانند میلیون ها ارز از هر نوعی را که سیا لازم داشته باشد نقل و انتقال دهند. این کارمندان دارای دفاتری در هنگ کنگ، ژنو، بیروت، بوینس آیرس و ... با نام های مختلف هستند .

آیزنهاور رئیس جمهور اسبق آمریکا گفته بود که آنچه برای ما در دوران جنگ سرد اهمیت دارد تنها این نیست که بدانیم روس ها از چه نقاط قوتی برخوردارند بلکه باید بدانیم آنان چه ندارند و در چه زمینه هایی دچار فقر هستند. همچنین سیا با همکاری موساد با پشتیبانی از شورشیان کنترا در نیکاراگوئه و تخریب نیروگاه های برق، پل ها و مزارع در داخل این کشور تورم را به ۱۷۰۰ درصد رساند و از سوی دیگر با فشار به بانک جهانی و صندوق بین المللی پول از پرداخت هرگونه کمک و وام به این کشور جلوگیری کرده و موجب ایجاد آشوب در این کشور و سرنگونی حکومت دانیل اورتگا شدند. حرکت خرابکارانه و براندازانه تنها گوشه ای از فعالیت های جاسوسی است. دزدیدن اطلاعات نیز همیشه اصل بوده است. در واقع بخش عمده ای از پیشرفت هایی که کشورهای صنعتی به آن نایل آمده اند در سایه جاسوسی اقتصادی به دست آمده است .

فرانسه در سال ۱۹۹۲ شاهد ۷۶۰ مورد جاسوسی صنعتی و علمی و اقتصادی بوده است. همچنین فرانسه در فوریه ۱۹۹۵ اعلام کرد سازمان جاسوسی آمریکا تلاش کرد تا با پرداخت رشوه به برخی از مسئولین فرانسوی، از موضع حکومت فرانسه در قبال مذاکرات سازمان تجارت

جهانی (گات) اطلاع یابد. در این شرایط آمریکایی ها نیز اعلام کردند که سازمان جاسوسی فرانسه با کار گذاشتن میکروفن در صندلی بازرگانان آمریکایی که با خطوط هواپیمایی فرانسه (ایرفرانس) مسافرت کرده اند درصدد شنود مذاکرات آنان برآمده است.

بر اساس گزارشات منتشر شده از سوی فرانسوی ها زمینه های فنی، صنعتی و علمی به تنهایی بیش از ۵۰ درصد از جاسوسی و سرقت اطلاعات از فرانسه را تشکیل می دهد و پس از آن، زمینه سیاسی است که سهم آن ۲۰ درصد است و جاسوسی نظامی از فرانسه در پایان لیست قرار دارد .

دولت های دیگر نیز به نوعی در این بازی عجیب و غریب حضور دارند. مثلاً اسرائیلی ها با وارد کردن برنامه کامپیوتری تله گذاری شده (وعد) به ادارات برق در سرزمین های اشغالی از میزان مصرف برق در منازل فلسطینیان مطلع شده و از این طریق پی می بردند خانه های مذکور از سکنه خالی است یا خیر و از میزان برق مصرفی، تعداد تقریبی ساکنین ساختمان ها را برآورد می کردند .

البته اسرائیل در زمینه جاسوسی پرونده سیاهی دارد. به کارگیری یهودیان در راستای منافع اطلاعاتی اسرائیل سابقه دیرینه ای دارد و استفاده از سازمان های یهودی در دیگر کشورها به قبل از تشکیل دولت یهودی در سرزمین های اشغالی فلسطین در سال ۱۹۴۸ باز می گردد.

به هر حال اکنون جاسوسی اقتصادی در اولویت برنامه اکثر سازمان های جاسوسی قرار گرفته و در این زمینه دوست و دشمن نمی شناسد و شاید کشوری در دنیا نباشد که بتواند ادعا کند هدف جاسوسی اقتصادی دیگر کشورها نیست. سیطره بر جهان از طریق اقتصاد هدف کشورهای بزرگ در قرن بیست ویکم به شمار می رود. با توجه به این که در بسیاری از کشورهای جهان مثل اروپای غربی و آمریکا، کاپیتالیسم و شرکت سالاری حکومت می کند و با عنایت به این که همه چیز در خدمت منافع شرکت های بزرگ و ابرشرکت های بین المللی و چندملیتی است و آنها هستند که دولت ها را می آورند و می برند، بی راه نیست که بدانیم بسیاری از این شرکت ها نیز برای خود دستگاه ها و سازمان های جاسوسی دارند. به عنوان مثال برخی از کارشناسان معتقدند میزان ذخیره یکی از چاه های نفت کشور قزاقستان به نام تانگیز معادل مجموعه ذخیره نفت کویت است و با فعالیت ها و زمینه سازی جاسوسان اقتصادی آمریکایی هم اکنون شرکت های آمریکایی تکزاکو، اکسون موبیل و شیفرون در زمینه های نفتی در این جمهوری فعالیت می کنند. بر اساس اظهارات (لئونل اولمر) معاون اسبق وزارت خارجه آمریکا، ژاپنی ها در زمینه جاسوسی صنعتی و اقتصادی در دنیا دقیق ترین و منظم ترین روش ها را به کار گرفته اند به طوری که سالانه ده ها میلیارد دلار به ثروت خود افزوده اند. در عین حال شرکت های بزرگ ژاپنی مانند سونی و تویوتا نیز خود مورد جاسوسی قرار گرفته و اطلاعات پایه ای خود را از دست می دهند.

اگر هدف از جنگ اقتصادی، نابودی قدرت اقتصادی رقیب باشد، هدف از جاسوسی اقتصادی نابودی اراده رقیب و تسلط بر وی و تبدیل او از یک عنصر فعال به یک عضو منفعل است تا در پی از دست دادن توان اقتصادی، دچار ناتوانی سیاسی و اجتماعی گردد. آری کشورها می توانند با یکدیگر دوست باشند، ولی سازمان های جاسوسی نمی توانند با هم رفتار دوستانه داشته باشند. امروزه با قرارگرفتن کشورها در دهکده جهانی و تکثر بازیگران دولتی و غیردولتی،تهدیدات نیز از ویژگی سیالیت و پیچیدگی برخوردار شده اند.از طرفی با گسترش فن آوری اطلاعات و ارتباطات و رشد شتابان فن آوری های نوین،جنس تهدیدات نیز تغییرکرده است و نفوذ دشمن برمولفه های اقتصادی جزئی از تهدیدات پیچیده است. به همین دلیل سیاست های تقنینی و اجرایی مرتبط با حوزه پدافند غیرعامل نیز بایستی از بالندگی و پویایی برخوردار باشند تا ظرفیت بازدارندگی کشور در قبال تهدیدات نوظهور افزایش یابد، بنابراین پالایش و تصویب قوانین لازم برای مقابله با تهدیدات بالقوه از اهمیت بالایی برخوردار می باشد.

منبع:روزنامه ایران – سایت پایداری ملی

تهیه و تنظیم شمسعلی محمودیان

آشنایی با ویروس آنفلوانزا

آنفلوانزای H1N1 چیست؟

یکی از چالش های قرارگاه پدافند زیستی در سال جاری، انتشار ویروس آنفلوانزا بود. از آنجایی که انتشار این بیماری نگرانی هایی در سطح جامعه ایجاد کرده بود برآن شدیم تا به بررسی آن و روش های کنترلی این بیماری بپردازیم: آنفلوانزا عبارت است از یک عفونت تنفسی مسری و شایع که در اثر یک ویروس ایجاد می شود .مدت زمان شروع علایم از زمان وارد شدن ویروس به بدن 48 -24 ساعت است .سه نوع اصلی ویروس آنفلوانزا وجود دارد (A,B,C) - ، اما این ویروسها توانایی جهش به انواع گوناگونی را دارند.

متاسفانه بیماری آنفلوانزا از نوع H1N1 دارای تمام شاخصه های یک بیماری مسری و خطرناک است که علی رغم تلاشهای مجدانه محققان پزشکی هنوز داروی موثری برای پیشگیری یا درمان قطعی آن وجود ندارد.بنابراین آنفلوانزا از حالت یک بیماری معمولی با درجه خطر پایین به یک بیماری کشنده و عالمگیر تبدیل شده و نگرانی جدی تمامی مردم، دولتها و نهادهای ملی و بین المللی در زمینه بهداشت و سلامت را موجب شده است و در ماه های اخیر به یک بحران جهانی تبدیل شده است.

تعریف و انواع

آنفلوانزای خوکی (Swine flu) یک بیماری تنفسی خوکها است که توسط ویروس آنفلوانزای نوع H1N1ایجاد می شود. این نوع آنفلوانزا معمولا در خوکها بروز می کند . ویروسهای آنفلوانزای خوکی حد بالایی از آلودگی و بیماری را سبب می شوند البته آمار مرگ و میر ناشی از آن در میان خوک ها معمولا کم است و کشندگی زیادی ندارد . آنفلوانزای خوکی معمولا به انسان منتقل نمی شود، هرچند گاهی در موارد نادر این ویروس به انسان، به خصوص افرادی که با خوک ها در تماس نزدیک بودند سرایت می کرد .موارد نادری از انتقال این ویروس از انسان به انسان نیز ثبت شده بود.

اما چه چیزی ویروس کنونی را تبدیل به ویروسی خطرناک کرده است؟ ویروس خوکی نیز مانند تمام ویروس های دیگر خود را تغییر می دهد .اگر خوک های مبتلا به آنفلوانزای خوکی همزمان به آنفلوانزای انسانی یا پرندگان نیز مبتلا باشند، این ویروس ها می توانند در بدن حیوان ژن های خود را تعویض کنند .بدین ترتیب نوعی جدید از ویروس به وجود می آید که هم ژن های انسان و هم ژن های حیوان را در خود دارد .این همان اتفاقی است که ظاهرا در مورد ویروس کنونی افتاده است .گونه های A H1N1" ویروس آنفلوانزا برای نخستین بار در سال 1930 میلادی قرنطینه شدند.

علایم و نشانه ها

نشانه های قابل انتظار آنفلوانزای خوکی در انسان ها مانند نشانه های آنفلوانزای فصلی انسان است.از **جمله ناگهانی تب، بی حالی، در خود فرورفتن، بی اشتهایی و سرفه کردن**. همچنین تعدادی از افراد آلوده با آنفلوانزای خوکی دچار سردرد، سرماخوردگی، گلودرد، کوفتگی و درد مفصل، عطسه، ناراحتی تنفسی، سرخ شدن یا التهاب

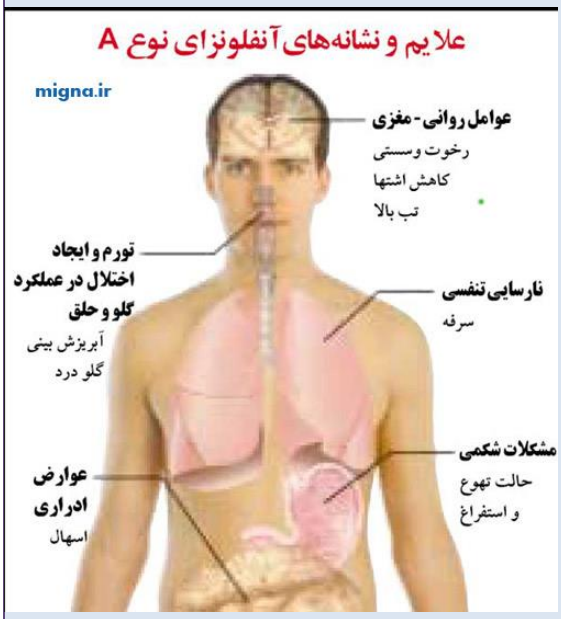
و آبریزش از بینی می گردند . در مواردی نیز تهوع، و استفراغ و اسهال نیز گزارش شده است.

راههای انتقال و شیوع:

ویروسهای آنفلوآنزا میتوانند تا چندین ساعت روی سطوح باقی بمانند و از دست و صورت بیماران منتقل شوند. طریقه شیوع این بیماری به هر صورت که باشد نتیجه این است که در حال حاضر بسیاری از کشورهای دنیا را در بر گرفته و انتظار می رود تمامی کشورها را در بر بگیرد . فراگیری گسترده این ویروس در سطح جهانی نیز از خطرهای دیگری است که در مورد آن هشدار داده شده و سازمان بهداشت جهانی وارد شدن آن به مرحله شش یا شیوع جهانی را تایید کرده است . بر اساس اعلام مرکز پیشگیری از بیماری های واگیر ایالات متحده، آنفلوانزای خوکی از راه مواد غذایی منتقل نمی شود .

راههای پیشگیری

ویروسهای H1N1 آنفلوانزای خوک بسیار متفاوت با ویروسهای H1N1 انسان است ، بنابراین، واکسنهای مورد استفاده برای آنفلوانزای فصلی انسان برای جلوگیری از ابتلا به ویروسهای H1N1 آنفلوانزای خوکی نه در بدن خوک و نه در بدن انسان ایمنی ایجاد نمی کند .بنابراین تا زمان تهیه واکسن این نوع آنفلوانزا صرفا می توان به توصیه های پزشکی و سازمانهای بهداشتی عمل کرد .



پزشکان در پاسخ به این سوال که هر فرد چطور می تواند از خود و خانواده اش در برابر این بیماری مراقبت کند، اظهار می دارند :در حال حاضر باید احتیاط های معمول برای آنفلوانزا را انجام داد که شامل پوشاندن جلوی دهان و بینی به هنگام عطسه و سرفه کردن با یک دستمال کاغذی که باید پس از مصرف حتما دور انداخته شود و مخصوصا از عطسه کردن در کف دست باید خودداری شود .دستهایتان را باید مرتب بشوئید و در صورت نبودن آب و صابون از ژل پاک کننده استفاده شود .اگر هم بیمار شده اید در خانه بمانید. همان طور که هوشیاری در برابر آلودگی برای پیشگیری از ابتلای شما و خانواده تان به بیماری ضروری است، در صورتی که خود مشکوک به ابتلا به آنفلوانزا هستید، حتما هنگام عطسه و سرفه جلوی دهان و بینی خود را بگیرید .اگر دستمال به همراه ندارید، هنگام عطسه یا سرفه قسمت داخلی آرنج خود را در برابر دهان و بینی بگیرید تا دستانتان آلوده نشوند.

- صورت خود را لمس نکنید :دستهای خود را از غشاهای مخاطی (چشم دهان بینی) دور نگه دارید چون- – ویروس از این راه ها وارد بدن می شود.
- از افراد بیمار دوری کنید.
- افراد خانواده و فامیل را از بیماری خود آگاه نموده و در صورت شدت گرفتن علائم ؛ نظیر تنگی نفس، ضعف و خستگی شدید، سردرد و سرگیجه شدید، استفراغ و تهوع غیر قابل کنترل به پزشک مراجعه کنید.

راههای درمان

داروهای ضدویروس ازداروهای موثری هستندکه مانع تکثیر و پیشرفت ویروس آنفلوانزا می شودولازم است فردطی 14 ساعت اولیه شروع علائم ازآن استفاده کند.این داروها عمر بیماری را کوتاه ترکرده وازپیچیده شدن آن جلوگیری می کند.درکنارآنتی ویروسها استفاده ازمسکن ها واستراحت درمنزل یابیمارستان به منظورکنترل تب وحفظ تعادل مایعات بدن توصیه می شود . این بیماری در صورت اقدام به موقع، قابل درمان است .استفاده از آنتی بیوتیک ها در درمان آنفلوانزا جایی ندارد چرا که استفاده نابجای آن ممکن است به مقاومت دارویی منجر شود.ویروسهای آنفلوانزا قابلیت تبدیل وجهش دارند و همین مسئله کارداروسازان را با مشکل مواجه کرده است .اما همانطورکه ذکرشد معمولا این بیماری به طور خود به خود و با اقدامات درمانی فوق الذکر و استراحت ظرف یک هفته بهبود پیدا می کند.

منبع:برگرفته از دستورالعمل کشوری پیشگیری از آنفلوانزا ، تهیه و تنظیم: نیما رستمی

آسیب‌پذیری Poodle چیست؟

در هنگام اولین اتصال به سرویس‌دهنده (وب سرور)، سرویس‌گیرنده (مرورگر کاربر) سعی می‌کند از طریق بالاترین نسخه‌ای که پشتیبانی می‌کند (مثلاً (TLS 1.2)) ارتباط را ایجاد کند. اگر وب سرور نیز قابلیت پشتیبانی از این نسخه را داشته باشد ارتباط برقرار می‌شود در غیر این صورت اگر مثلاً وب سرور از نسخه‌ی TLS 1.0 استفاده کند، مرورگر کاربر نیز به نسخه‌ی پایین‌تر یعنی TLS 1.0 سوییچ می‌کند. به این رویکرد downgrade گفته می‌شود می‌تواند (این کار توسط یک نفوذگر در داخل شبکه می تواند می تواندااتفاق بیافتد). که در اینجا نفوذگر مرورگر کاربر را وادار می‌کند تا از طریق SSLv3 اتصال را برقرار نماید. نهایتا این آسیب‌پذیری توسط مهندسان گوگل اعلام شد و Poodleنام گرفت.

چه کسی تحت تأثیر این آسیب‌پذیری قرار می‌گیرد؟

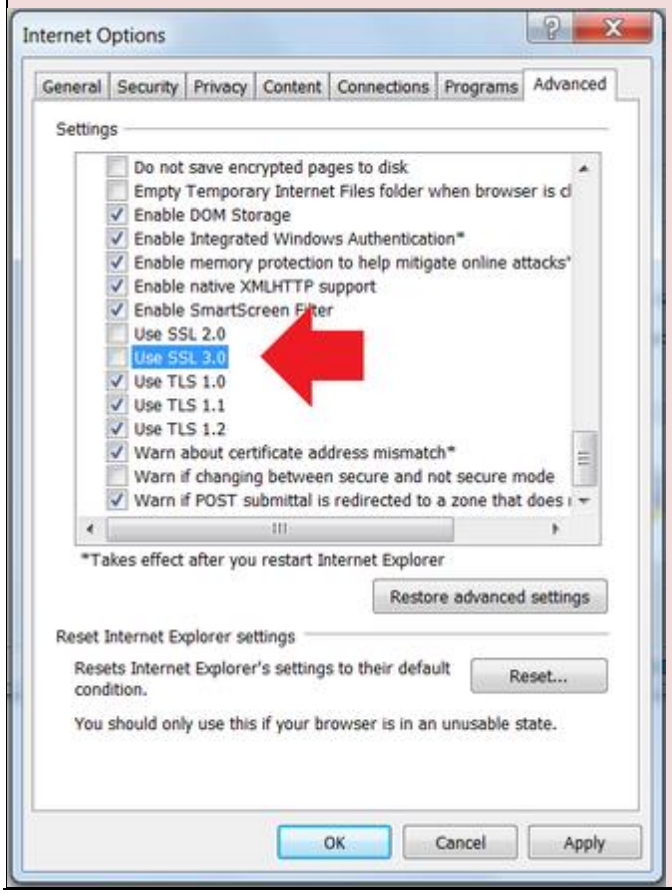
کاربران هر وب‌سایتی (سرویس دهنده) که از SSLv3 پشتیبانی کند (اگر در سمت سرور غیر فعال نشده باشد)، آسیب‌پذیر می‌باشند. در واقع حتی اگر وب سایت از نسخه‌های TLS استفاده کند به دلیل قابلیت downgrade (بازگشت به نسخه‌ی قبلی) آسیب‌پذیر می‌باشد زیرا نفوذگر داخل شبکه می‌تواند مرورگر کاربر را وادار کند تا از طریق SSLv3 اتصال برقرار کند.

کاربر چگونه تحت تأثیر این آسیب‌پذیری قرار می‌گیرد؟

نفوذگر (داخل شبکه‌ی کاربر) با بهره‌برداری از این آسیب‌پذیری می‌تواند اطلاعات حساس کاربر مانند (کوکی که هویت کاربر است) را برباید و در نهایت وارد حساب کاربر شود.

راه‌حل پیشنهادی چیست؟

بهترین راه حل برای این آسیب‌پذیریی عدم استفاده از SSLv3 توسط سرویس‌دهنده (وب سرور) و سرویس‌گیرنده (کاربر) می‌باشد. البته اگر سرویس دهنده‌ای تنها از SSLv3استفاده کند، غیرفعال کردن آن در سمت کاربر (سرویس گیرنده) می‌تواند باعث عدم دسترسی به سرویس‌دهنده شود.



نحوه غیر فعال کردن SSL 3.0 در مرورگرهای مختلف

❖ **مرورگر Internet Explorer**

از منوی Tools گزینه Internet Options را انتخاب کنید.

۱. صفحه Internet Options باز می شود.
۲. در این صفحه برگه Advanced را انتخاب کنید. (نام برگه ها به صورت افقی در بالای صفحه لیست شده است)
۳. در این برگه تعداد زیادی گزینه (چک باکس) وجود دارد که با کلیک بر روی هر کدام می توانید آن گزینه را تیک دار کنید یا تیک آن را بردارید. این گزینه ها در دسته های مختلفی دسته بندی شده اند.
۴. با اسکرول صفحه به سمت پایین به مجموعه گزینه هایی که در دسته Security قرار گرفته اند برسید.
۵. در این دسته، تیک مربوط به گزینه هایی که با عنوان Use SSL شروع شده اند را بردارید (اگر تیک دارند). معمولا دو گزینه Use SSL 2.0و Use SSL 3.0 باید وجود داشته باشند.

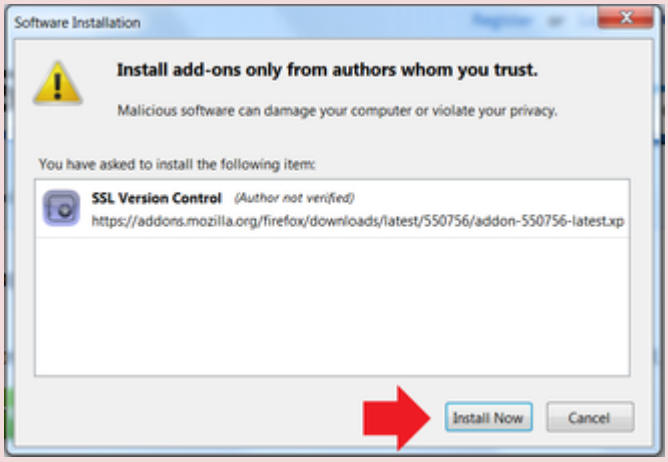
۶. در همین دسته، گزینه هایی که با عنوان Use TLS شروع می شوند را تیک بزنید (اگر تیک ندارند). معمولا گزینه Use TLS 1.0 وجود دارد و ممکن است گزینه های Use TLS 1.1 و Use TLS 1.2 نیز وجود داشته باشند.

۷. در نهایت صفحه شما باید مشابه شکل زیر شده باشد (ممکن است بعضی از گزینه ها وجود نداشته باشند:

۸. دکمه Ok را بزنید تا تغییرات شما ذخیره شوند.

❖ مرورگر Firefox

راه اول: استفاده از افزونه ارائه شده توسط موزیلا. توجه کنید که این راه فقط برای نسخه های ۲۶ به بالای Firefox قابل استفاده است.



۱. توسط مرورگر خود به این آدرس بروید:
https://addons.mozilla.org/en-US/firefox/addon/ssl-version-control

۲. در این صفحه، دکمه Add to Firefox را کلیک کنید.

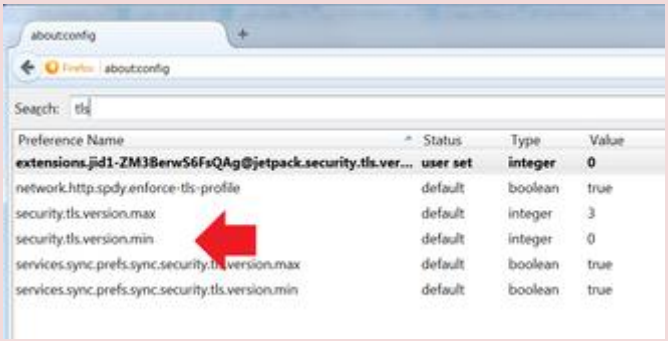
۳. از پنجره ای که باز می شود دکمه Allow را انتخاب کنید.

۴. پس از مدتی پنجره دیگری باز می شود. در این پنجره دکمه Install Now)که در پایین پنجره قرار گرفته است) را کلیک کنید.

۵. پس از مدتی پیغامی مبتنی بر نصب موفقیت آمیز افزونه به شما داده می شود.

۶. این افزونه به طور اتوماتیک همه کارها را انجام می دهد.

راه دوم: استفاده از تنظیمات پیشرفته (فقط برای کاربران حرفه ای)



۱. عبارت about:config را در قسمت آدرس بار مرورگر خود تایپ کنید.

۲. در صفحه باز شده در قسمت جستجو عبارت tls را وارد کنید و دکمه Enter را بزنید .

۳. بر روی سطری که دارای عنوان security.tls.version.min می باشد "دبل کلیک" کنید.

۴. پنجره ای باز می شود که می توانید در آن مقدار وارد کنید.

۵. عدد ۱ را وارد کنید و سپس دکمه Ok را بفشارید.

❖ مرورگر Chrome

در حال حاضر در مرورگر Chrome تنها می توان از طریق گزینه های خط فرمان SSL را غیر فعال کرد. راه حل زیر فقط برای حالتی مناسب است که شما مرورگر خود را از طریق میانبر (shortcut) موجود بر روی دسکتاپ اجرا می کنید.

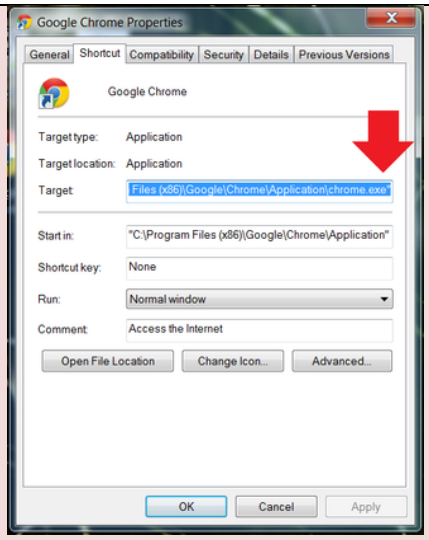
۱. بر روی میانبر Chrome بر روی دسکتاپ کلیک راست کنید و گزینه Properties را از منوی باز شده انتخاب کنید.

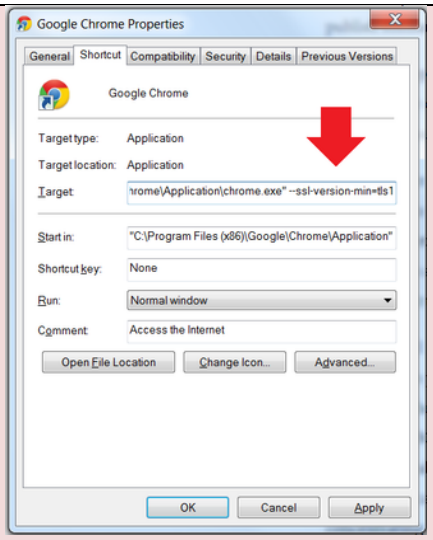
۲. در صفحه باز شده به فیلد Target را پیدا کنید و بر روی جعبه ورودی مقابل آن کلیک کنید.

۳. به انتهای مقدار وارد شده در این جعبه بروید که عبارت ”chrome.exe“ می باشد.

۴. با گذاشتن یک فاصله (space) این عبارت را پس از عبارت بالا وارد کنید:

--ssl-version-min=tls1





۵. دکمه Ok را بزنید.

توجه داشته باشید که برای استفاده از راه حل بالا، از این پس تنها باید از طریق این میانبر مرورگر خود را اجرا کنید. به عنوان مثال اگر کروم را از طریق میانبری که در منوی Start شما قرار گرفته است اجرا کنید طبیعتا در آن حالت مرورگر شما امن نخواهد بود. البته می توانید این کار را برای سایر میانبرهای کروم نیز اجرا کنید.

❖ مدیران سایت‌ها چه کاری باید انجام دهند؟

بهترین راه حل برای گردانندگان سایت‌ها (یا وب مسترها) برای جلوگیری از این آسیب پذیری غیر فعال کردن SSLv3 در تنظیمات web-server است. البته این باعث می‌شود که مرورگر IE6 (که البته دیگر پشتیبانی هم نمی‌شود و سهم کمی در مرورگرها دارد) امکان اتصال به https سایت را نداشته باشد، اما اگر امنیت و راحتی کاربران مهم است (به دلیل وجود مشکلات امنیتی و کارکردی متعدد در IE6) بهتر است این مرورگر (حداقل برای اتصال امن با https) نادیده گرفته شود.

❖ روش غیر فعال کردن SSLv3 در سرورهای مختلف به صورت زیر است.

ضمنا باید به نکات زیر نیز توجه نمود:

- در مورد هر سرور، بعد از تغییر تنظیمات باید سرویس مربوط را restart کرد.
- بهتر است طبق راهنمای موزیلا الگوریتم‌های مورد استفاده وب سرور خود را نیز تغییر دهید.

❖ غیر فعال کردن SSL3 در Apache

کافیست تنظیم زیر در کنار بقیه تنظمیات SSL درج شود (دقت کنید که تنظیم SSLProtocol از قبل وجود نداشته باشد)

```
SSLProtocol All -SSLv2 -SSLv3
```

❖ غیر فعال کردن SSL3 در Nginx

این خط باید به تنظیمات nginx اضافه شود: (در قسمت http یا server)

```
ssl_protocols TLSv1 TLSv1.1 TLSv1.2;
```

❖ غیر فعال کردن SSL3 در Lighttpd

عبارات زیر باید به تنظیمات lighttpd و بعد از خط "ssl.engine = "enable اضافه شوند:

```
ssl.use-sslv2 = "disable"
ssl.use-sslv3 = "disable"
```

منابع:

https://bayan.blog.ir/1393/07/23-1https://bayan.blog.ir/1393/07/23-1
http://news.pandasecurity.ir/index.php/alerts/949-freak-flaw
http://blog.securehost.ir/freak-ssl-vuln

تهیه و تنظیم، لیدا رسول اهری(کارشناس آموزش و پژوهش پدافند غیرعامل استانداری)

جنگ اقتصادی

«تنها راه مقابله با تهدیدها این است که وضعیت داخلی به گونه ای ساماندهی شود که دشمن از پیروزی خود مطمئن نباشد و زمینه را برای ماجراجویی فراهم نبیند.» مقام معظم رهبری (مدظله العالی)

جنگ اقتصادی

پاسخ این که جنگ اقتصادی چیست وچه مفهومی دارد را باید دراین جستجو کنیم که جوامع در طول تاریخ چرا و به چه دلایلی با هم جنگیده و درطی جنگ چه اتفاقی برای آن ها افتاده است؟ به طور منطقی می توان گفت وقتی بین کشورها یا بین جوامع مسائلی وجود داشته است و این مسائل به طرق عادی قابل حل نبوده یا حل نشده است، یکی از طرفین دعوا احساس کرده به لحاظ برتری هایی که دارد ،می تواند طرف خود را کاملا از بین ببرد یاضربه های اساسی به او وارد کند ولذا مبادرت به جنگ نموده است.

گذر زمان و پیشرفت های فکری و تحولات انسانی که برای جامعه بشری حاصل شده است تا حدود زیادی نوع جنگ ها را تغییر داده است. امروزه به وضوح می توان درجوامع بشری نوع دیگری از درگیریها که آن نیز هدف تدریجی مقابله یا نابودی طرف دیگری را دنبال می کند مشاهده نمود.آن چه که تحت عنوان براندازی نرم و یا به طور خاص، براندازی نرم عنوان می شود، در همین مقوله طبقه بندی می شود. با توجه به اهمیت مسائل اقتصادی و نیاز امروز جوامع به یکدیگر از لحاظ اقتصاد، بدیهی است **که یکی از وجوه مهم براندازی های نرم، جنگ اقتصادی است.** درقرن ۲۰ تحولات عمده ای درتاسیس سازمان های بین المللی اتفاق افتاد. هنگامی که کارکرد این سازمان ها را طی دهه های طولانی که از عمرشان گذشته مورد بررسی قرار دهیم ،ملاحضه می کنیم در مواردی این سازمان ها نوعی جنگ از جنس اقتصاد را نسبت به پاره ای از کشورها اعمال کرده و می کنند. در جریان جنگ جهانی دوم و زمانی که مسئله تاسیس سازمان های بین المللی برای نظم بخشیدن به نظام پولی بعد از جنگ در جهان مطرح بود،در کنفرانس برتن وس در سال ۱۹۴۴ تاسیس صندوق بین المللی پول و بانک جهانی و همچنین سازمان جهانی تجارت مورد تصویب قرار گرفت. این سازمان های بین المللی اقتصادی بلا استثناء توسط اقتصاد دانان کشور های توسعه یافته تدوین شده و به عنوان سیاست های اقتصادی برای کشور های توسعه نیافته تجویز می شود. اینان با قدرتی که دارند ،نسخه های تجویزی خود را به کشورهای در حال توسعه تحمیل خواهندکرد. این قدرتها با وام دادن به کشور های در حال توسعه سیاست های استعماری خود را در آن کشورها اجرایی می کنند. اگر کشوری این شرایط را قبول ننماید اعلام می کنند که در آن کشور ریسک سرمایه گذاری بالاست و چنان تبلیغات می کنند که سایر کشور ها نیز در آن کشور سرمایه گذاری ننمایند. عدم سرمایه گذاری باعث می شود مشکلات اقتصادی در آن کشور به وجود آید.

شرایط احقاق جنگ اقتصادی

زمانی است که سرمایه اجتماعی در جامعه هدف تضعیف شده و به نوعی رابطه بین مردم و حاکمیت گسسته شده و اعتماد و باور جامعه یا کشور تضعیف شده باشد. ولی همکاری مردم و دولت و اعتماد مردم به مسئولین و حرف شنوی مردم باعث پیروزی می شود . مسئولین اگر برنامه بلند مدت منسجم نداشته باشند باعث گسست سرمایه اجتماعی می شود .ازاین رو نمی توان امکان تحقق پیروزی را تنها به دشمن نسبت داد ،بلکه بخش عمده ی آن به سیاست گذاری های درون کشور ها بستگی دارد . هر جامعه ای که خود را بهتر اداره کند ،به لحاظ بالا بردن سرمایه اجتماعی در مردم ،امکان شکست خود را در مقابل دشمنی که با جنگ اقتصادی و برای مبارزه با اوآمده است کمتر می کند.

مهمترین راهکار مقابله با جنگ اقتصادی خود باوری است

در این شرایط دشمن اجازه ورود مواد اولیه – تکنولوژی –آموزش نیروی انسانی را که منجر به تقویت بنیه اقتصادی کشور می شود، نمی دهد و باید با باور ایمان و تلاش و پشتکار مشکلات را کم کنیم. اگر باور ایمان در مردم یک کشور نباشد سرمایه اجتماعی تضعیف می شود

ودر نهایت پایداری ملی از بین می رود. در جنگ های نظامی سرزمینی که از دست می رود، مردم و دولت کشور می بینند ولی در جنگ اقتصادی چون جنگ از نوع نرم است و حتی در مواردی رفاه کاذبی برای جامعه درگیر جنگ به ارمغان آورده ،مبارزه را دشوارتر نموده و یا در نظر افراد جامعه کم اهمیت تر می انگارد.عادت مردم به استفاده از کالاهای خارجی در حالی که مشابه آن کالا در داخل تولید می شود بهترین مثل در این مورد است.

عامل دیگر از راهکارهای مقابله با جنگ اقتصادی ،می تواند تلاش و کار بسیار زیاد از طرف مردم آن جامعه باشد. جامعه ای مقاوم است که اقتصاد آن به تولید داخلی متکی است.

دفاع در مقابل تهاجم اقتصادی

وقتی سخن از جنگ به میان می آید ،طرفی که مورد تهاجم واقع می شود،سعی دارد از خود دفاع کند .بنابراین وارد عرصه ای خواهد شد که کنش و واکنش صورت می گیرد .یعنی یکی تهاجم می کند و می داند چه چیزی می خواهد ،اما در بیشتر موارد کشوری که مورد تهاجم قرار گرفته است ،برای دفاع از خود هیچ طرحی ندارد. ورود اجنبی به کشور مانند ورود یک میکروب به بدن است . همه متوجه می شوند و مبارزه می کنند به غیر از گروهی که شاید با خود بیگانگان باشند . در جنگ اقتصادی ،آن عاملی که مورد تهاجم و نابودی قرار می گیرد ،قدرت دفاعی ندارد . مثل ویروسی که بدن آن را نمی شناسد و توانایی دفاع در مقابل آن ویروس ندارد.

وقتی می گوییم اقتصاد، باید فرهنگ اقتصادی را نیز در نظر بگیریم. می توان گفت که اقتصاد یک چارچوب مشخص تولید و توزیع است .شاید بتوان گفت دلیل این که انسان به تهاجم اقتصادی چندان حساس نمی شود و متوجه آن نیست ،این است که در این نبرد ،ابتدا از ابزارهای فرهنگی استفاده می شودکه استفاده از این ابزار ها باعث مختل شدن دستگاه شناسایی ملی جهت تشخیص این نوع تهاجم می شود. مهمترین عنصر این جنگ نابود کردن تولید کنندگان داخلی است . زیرا وارد کننده با توجه به نیاز مصرف کننده کالا وارد جامعه می کند. شیوه های جنگ اقتصادی در زمانهای مختلف متفاوت است و بستگی به نوع ارتباط کشور مورد تهاجم با کشور مهاجم دارد. هرچه کشور مورد تهاجم ارتباط اقتصادی بیشتری با کشور مهاجم داشته باشد ،ضربه پذیری اش بیشتر خواهد شد.

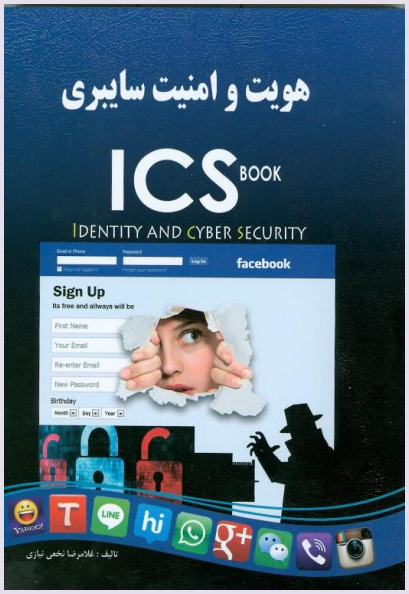
نو استعماری و خود استعماری

در گذشته زمانیکه اشغالگران کشوری را تصاحب می کردند ،دخالتی در امور اقتصاد نداشتند . بلکه اقتصاد داخلی را رها کرده تا به کار خود ادامه دهد و از ارزش افزوده یا مازاد آن به نفع خود استفاده می کردند .بنابراین در ساختار اقتصادی تغییری به وجود نمی آمد .ولی از ۲۰۰سال پیش اتفاق جدیدی رخ داده است . استعمار بر خلاف گذشته برای غارت آمده و ویژگی آن ،این است که دارای اقتصادی است با مازاد تولید . او می خواهد این مازاد تولید خود را دربازارهای جدید بفروشد . از طرفی چون تولید ،ماشینی و انبوه شده است ،لاجرم نیاز به بی نهایت بازار و همچنین نیاز به بی نهایت مواد اولیه دارد .بنابراین لازم است مواد اولیه را از جایی دیگر تامین کند.کاری که انجام می دادند این بود که اقتصاد دیگران را اشغال کنند و شکل جدیدی به آن دهند دراین موارد به معنای واقعی تهاجم اقتصادی به وجود می آید و نهایتا به نو استعماری و خود استعماری می انجامد. در خود استعماری ، نمی توان تشخیص داد که مورد تهاجم اقتصادی قرار گرفته ایم و فکر می کنیم در حال توسعه هستیم. در حالی که با تهاجمی روبرو شده ایم که مواد اولیه را به ثمن بخس از ما خریداری و کالاهایشان را با چند برابر قیمت به ما بفروشند.

شیوه های جنگ اقتصادی در زمان های مختلف متفاوت است وبستگی به نوع ارتباط کشور مورد تهاجم با کشور مهاجم دارد .هرچه کشور مورد تهاجم ارتباط اقتصادی بیشتری با کشور مهاجم داشته باشد ،ضربه پذیری اش بیشتر خواهد بود. درمقابل این نوع تهاجم دشمن (جنگ اقتصادی) نیز می توان ایستادگی کرد ،به شرطی که مبانی ارزش های اسلامی را به کار بگیریم و به منافع ملی توجهی ویژه داشته باشیم.

منبع جنگ اقتصادی: دکتر محسن فردرو - تهیه کننده علی تدین.

معرفی کتاب



کتاب فوق- هویت و امنیت سایبری- در خصوص افزایش مهارت های عمومی کاربران فضای مجازی توسط آقای غلامرضا نخعی نیازی تألیف شده است. مزیت اصلی کتاب جامع بودن و زبان ساده آن است. مولف سعی کرده تهدیدات فضای سایبری را با زبانی ساده و با توسل به حوادثی که در فضای مجازی رخ داده تشریح کند. کتاب در ده فصل متنوع ذیل نگاشته شده است:

فصل اول: اصطلاحات سایبری، فصل دوم: اطلاعات مهم و حفاظت آنها فصل سوم: جرم سایبری و رایج ترین جرایم فصل چهارم: کلمات پرکاربرد به زبان ساده فصل پنجم: امنیت در رایانه آفلاین فصل ششم: امنیت تلفن همراه و تبلت فصل هفتم: بانکداری مجازی فصل هشتم: امنیت در وبگردی فصل نهم: ایمیل و رایانش ابری فصل دهم: شبکه های اجتماعی

در بخش آخر کتاب نیز مولف به رفتارهای غیرمتعارف و غیراخلاقی برخی کاربران شبکه های اجتماعی پرداخته و به برخی نکات امنیتی مهم و اخلاقی اشاره کرده است. قیمت کتاب ۱۵۰۰۰ تومان است. انتشارات فرهنگ روز در سال ۹۴ چاپ دوم آن را در هزار نسخه منتشر کرده است.

عناوین رویدادهای مهم خبری

❖ برای مشاهده متن کامل خبرها روی آنها کلیک کنید

توصیه های لازم برای کاهش آسیب پذیری در فضای مجازی	مأموریت فتنه‌گرانه رژیم صهیونیستی به شبکه «من و تو»
کدام دولت ها ایمیل کاربران را چک می‌کنند؟	راه تشخیص جوهر قند در نان
چه شهرهایی در معرض بزرگترین تهدیدهای جنگ هسته‌ای قرار دارند؟	ردپای اعراب در واردات بنزین آلوده / ماجرای خریدوفروش تلگرامی بنزین
با «موز» خداحافظی کنید	زنگ خطر "پان" برای والدین

سایت های مرتبط با پدافند غیرعامل

❖ وب سایت پایداری ملی	http://www.paydarymelli.ir/
❖ مرکز مطالعات پدافند غیر عامل	http://www.pdrc.ir
❖ پورتال پدافند غیرعامل استانداری آذربایجان شرقی	http://padafand.eaz.gov.ir/
❖ استانداری آذربایجان شرقی – دفتر پدافند غیرعامل	http://ostan-as.gov.ir/?PageID=42
❖ پلیس فتا	http://www.cyberpolice.ir/

صاحب امتیاز: اداره کل پدافند غیرعامل استانداری آذربایجان شرقی
مدیر مسئول: سردار احمد جهانسری
سردبیر: محمد بامدادی
دبیر تحریریه: رامین زارعی
شماره تماس : ۰۴۱-۳۳۳۳۶۲۰۹