استانداری آذربایجان شرقی
اداره کل پدافند غیرعامل

نشریه پدافند غیرعامل
شماره ۲– تیر ماه ۱۳۹۴

در این شماره خواهید خواند

وقتی این ملت تصمیم دارد که حرف زور را از هیچ کدام از قلدرها و سرگردنه بگیرهای مسلح دنیا به گوش نگیرد پس باید خودمان را آماده دفاع کنیم.

گزارش عملکرد واحد آموزش پدافند غیرعامل

سردار جهانسری: «پدافند غیرعامل یک دروازه توسعه دارد و آن آموزش و مفهوم سازی است.»

در راستای اجرای اهداف اداره کل پدافند غیر عامل مبنی بر ضرورت مفهوم سازی پدافند غیر عامل در بین دستگاه های اجرایی، سازمان ها و نهاد های استان، واحد آموزش پدافند غیر عامل استانداری در شش ماه دوم سال ۹۳ اقدام به برگزاری (ادامه در صفحه ۲)

ماموریت کمیته پدافند غیرعامل استان

کمیته پدافند غیر عامل استان مأموریت دارد به منظور برآورد تهدید، کاهش آسیب پذیریها و پایدار نمودن استان، تداوم چرخه خدمات ضروری و ارتقاء تحمل و مقاومت مردم، حفاظت از جان مردم، تأمین نیازهای ضروری و مورد نیاز مردم و استفاده از کلیه امکانات مردمی و بسیج منابع در شرایط بحرانی ناشی از تهدیدات نظامی دشمن(ادامه در صفحه ۲)

گزارش عملکرد واحد آموزش پدافند غیرعامل

(ادامه از صفحه ۱) به برگزاری کارگاه های عمومی و تخصصی در حوزه های مختلف پدافند غیر عامل به شرح ذیل نموده است.

۱. برگزاری دوره تکمیلی تربیت مربی پدافند غیرعامل و اعطای گواهی نامه مربی گری پدافند برای ۴۵ نفر از شرکت کنندگان

۲. برگزاری ۳۰ کارگاه آموزشی برای مدیران ، مسئولان و کارکنان دستگاه های اجرایی شهرستان تبریز(بیش از ۱۳۰۰ نفر در سطح تبریز)

۳. برگزاری ۲۰ کارگاه آموزشی برای فرمانداران و مدیران ادارات و کارکنان دستگاه های اجرایی شهرستانها (بیش از ۷۰۰ نفر در شهرستان های استان)

۴. عقد تفاهم نامه همکاری با صدا و سیمای مرکز تبریز برای ترویج وآشنایی و آگاه سازی آحاد جامعه با مفهوم پدافند غیر عامل و حضور در برنامه های رادیویی و تلوزیونی

۵. عقد تفاهم نامه همکاری علمی با آموزش و پرورش استان در خصوص غنی سازی دبیران آمادگی دفاعی مدارس متوسطه و راهنمایی

۶. عقد تفاهم نامه همکاری علمی با دانشگاههای معتبر استان از جمله دانشگاه تبریز، دانشگاه جامع علمی کاربردی، دانشگاه آزاد و دانشگاه صنعتی سهند

۷. عقد تفاهم نامه همکاری علمی با پژوهشکده رانشگرهای فضایی و استفاده از توان نیروهای انسانی و مطالعاتی علی الخصوص حوزه مبحث ۲۱ و سازه های امن

۸. برنامه ریزی برای شناسایی مخاطرات استان جهت مطالعه و برنامه ریزی عملیاتی

لازم به ذکر است که واحد آموزشی اداره کل پدافند غیر عامل آمادگی خود را برای برگزاری کارگاههای عمومی و تخصصی پدافند غیر عامل در حوزه های (پدافند عمومی، زیستی، هسته ای، سایبری، کالبدی، فرهنگی و...) اعلام می دارد.

ماموریت کمیته پدافند غیرعامل استان

(ادامه از صفحه ۱)۱. سازماندهی و ایجاد ساز و کار لازم در پدافند غیر عامل و دفاع غیر نظامی مورد نیاز استان

۲. برآورد تهدیدات و اقدامات دشمن، نقاط آسیب پذیر، هم افزایی ها و مخاطرات در سطح استان در حوزه پدافند غیر عامل

۳. طبقه بندی و اولویت بندی مراکز و زیر ساخت های استان

۴. تداوم چرخه خدمات اساسی و تأمین نیازهای ضروری مردم (نان، غذا، برق، انرژی اضطراری، سلامت و بهداشت و درمان تأمین جان پناه امن برای مردم) در شرایط تهدید نظامی دشمن برای کوتاه مدت، میان مدت، بلند مدت

۵. ارتقاء فرهنگ عمومی مردم با اجرای آموزشهای عمومی و اقدامات فرهنگی و تمرین و رزمایش در خصوص ارتقاء آمادگی و پایداری در حوزه های مختلف در برابر تهدیدات نظامی دشمن

۶ .تهیه طرحهای پدافند غیر عامل و اجرا و نظارت بر آن در مراکز و زیرساختهای استان

۷ .اداره مردم به منظور مقابله با بحران تهدید نظامی با بکارگیری و بسیج امکانات و منابع عمومی، دولتی و مردم استان

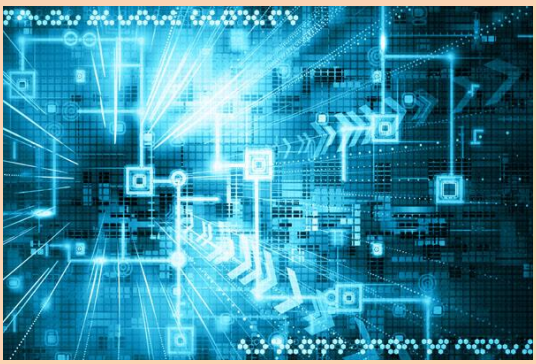
۸. ارتقاء آستانه مقاومت و تحمل مردم استان در برابر تهدیدات از طریق مقابله با عملیات روانی و فرهنگی و اطلاعاتی دشمن

۹. آمادگی دفاع غیر نظامی و پدافند غیر عامل در استان با برگزاری آموزش، تمرین و رزمایش های دوره ای

مقدمه ای بر پدافند سایبری

دفاع سایبری به پایدار نگه‌داشتن زیرساخت‌های ارتباطی و اطلاعاتی که به نحوی با فناوری اطلاعات، شبکه‌های کامپیوتری و اینترنت در هم آمیخته شده است (فضای سایبری) اطلاق می گردد. مصون نگه‌داشتن سیستم‌های SCADA مورد استفاده در صنایع مختلف از بدافزارها و اطمینان از صحت کارکرد این سیستم‌ها، پایدار نگه‌داشتن وب سایت‌های دولتی، شبکه‌های انتقال اطلاعات و سایر خدمات مبتنی بر فناوری اطلاعات از جمله اولویت‌های دفاع سایبری می‌باشد.

فضای سایبری، به فضایی اشاره دارد که بصورت فیزیکی وجود ندارد و قابل لمس نیست. برای آشکار شدن این موضوع فرض کنید دو نفر باهم از طریق تلفن با هم مکالمه می کنند. برای برقرار این مکالمه، تجهیزات مخابراتیِ نظیر سویچ ها، آنتن های BTS، فیبر نوری، کامپیوترها و سایر تجهیزات باهم کار می کنند، تا ارتباط بین دونفر شکل بگیرد، و صدای آنها به همدیگر ارسال گردد. می گوییم که تمامی این اعمال و اتفاقات در فضای سایبری رخ داده است. به طور کلی فضای سایبری به شبکه های کامپیوتری (از جمله اینترنت)، زیرساخت‌های ارتباطی، مخابراتی، تجهیزات استفاده شده در صنایع مختلف (نظیر PLC و RTUها) و اعمال و اتفاقاتی که در این فضا رخ می دهد اتلاق می گردد.



مقدمه ای بر پدافند زیستی

پدافند زیستی: مجموعه ای از اقدامات شامل رصد و پایش، آشکارسازی، هشداردهی، تشخیص تصمیم و عملیات، کنترل، حفاظت و پیشگیری، امداد و نجات و رفع آلودگی در برابر تهدیدات زیستی که موجب حفاظت از سرمایه های ملی در برابر تهدیدات زیستی و کاهش آثار و عواقب ناشی از آنها می گردد.

تروریسم زیستی: استفاده عمدی و سوء از عوامل زیستی (باکتری ها، ویروس ها، قارچ ها و کتورها) و فرآورده های آنها برای آسیب زدن، تخریب و از بین بردن سرمایه های انسانی و منابع ملی (دام، نباتات، محیط زیست، منابع طبیعی، آب آشامیدنی، مواد، تجهیزات و انبیه) و در نهایت ایجاد رعب و وحشت برای حصول موفقیت های سیاسی و اجتماعی می باشد.

جنگ زیستی: استفاده آشکار یا پنهان از تسلیحات زیستی علیه منابع انسانی و یا زیر ساخت های اقتصادی که توسط یک کشور متخاصم و با هدف وارد نمودن ضربه نظامی، از بین بردن مقاومت، تحمیل خسارات اقتصادی و خدشه دار نمودن امنیت ملی کشور انجام می گیرد.

حوزه تهدیدات زیستی: ۱-انسان ۲- دام ۳- نباتات ۴- محیط زیست و منابع طبیعی ۵- غذا و دارو ۶- آب آشامیدنی

اهداف تهدیدات زیستی: فشار به دولت ها برای تسلیم شدن- خدشه دار نمودن چهره مقتدر نیروهای مسلح- قتل و عام مردم و از بین بردن مقاومت مردمی- کاهش توان و آمادگی نیروهای رزم و پشتیبانی در مقابله با دشمن- ایجاد غافلگیری و وارد نمودن ضربه نظامی- آسیب رساندن به سلامت عمومی جامعه و ایجاد تلفات جانی و مالی- ایجاد رعب و وحشت عمومی.

مقدمه ای بر پدافند کالبدی

مفهوم و هدف پدافند کالبدی (عمرانی، معماری و شهرسازی)

عبارت است از مجموعه ای از اقدامات غیر مسلحانه و تدابیر و ملاحضات شامل ایمن سازی، مستحکم سازی، پیش بینی سامانه های جایگزین تسهیل مدیریت بحران در زیر ساخت ها و مکان یابی در حوزه ساختمان سازی به منظورافزایش بازدارندگی، کاهش آسیب پذیری نیروی انسانی، ساختمانها و تاسیسات، تجهیزات و شریان های کشور ، تدوام فعالیت های ضروری ، تسهیل مدیریت بحران و نیز افزایش امنیت روانی و جانی، ارتقا پایداری ملی و افزایش آستانه مقاومت ملی در شرایط بحران.

رسالت نظام فنی و مهندسی پدافند غیرعامل (پدافند کالبدی)

نظام فنی و مهندسی پدافند غیرعامل به عنوان بالاترین مرجع مهندسی پدافند غیرعامل کشور، از طریق سیاست گذاری، برنامه ریزی، راهبری، نظارت و مدیریت یکپارچه در سطح ملی بدنبال ایجاد هم افزایی در نظام فنی و اجرایی کشور جهت مصون سازی، کاهش آسیب پذیری، ارتقا پایداری ملی، افزایش بازدارندگی، تداوم فعالیت های ضروری، تسهیل مدیریت بحران در مقابل اقدامات و تهدیدات خصمانه دشمن می باشد.

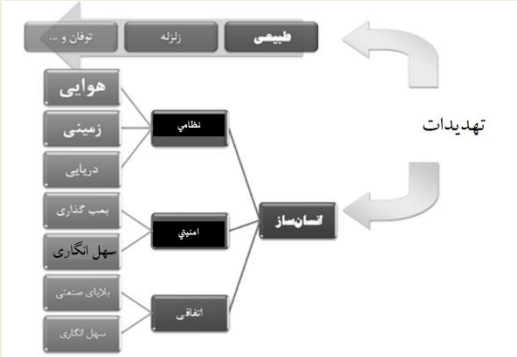
رسالت نظام فنی و مهندسی پدافند غیرعامل کشور، "تدوین، تصویب و ابلاغ، انتشار و آموزش، اعمال، نظارت و واپایش اصول، نظامات، الزامات، پایداری، استحکام و مصون سازی زیرساخت های حساس، حیاتی و مهم کشور در برابر تهدیدات و اقدامات خصمانه دشمن می باشد.

قوانین پدافند غیرعامل

- مبحث ۲۱ مقررا ت ملی ساختمان
- بند الف ماده ۲۱۵ قانون برنامه پنجم توسعه

انواع تهدیدات

به منظور نیل به اهدف فوق، ابتدا بایستی تهدیدات وارد بر سازه ها شناسایی شوند. هر آن چه که باعث به خطر افتادن منافع ملی کشور باشد، تهدید نامیده می شود (لازم به یادآوری است که پدافند غیرعامل با تهدیدات انسان ساز سروکار دارد). بر این اساس:



آشنایی با شبکه‌های اجتماعی ، فرصت ها و تهدیدها

شبکه اجتماعی از ابتدای بشریت وجود داشته ولی نوع مجازی آن از ابتدای قرن ۲۱ نمایان شده و اصطلاح دهکده جهانی را ترجمه کرده اند.

نخستین بار مفهومی با عنوان شبکه‌های اجتماعی اینترنتی با قالب امروزی در سال ۱۹۶۰ اولین بار در دانشگاه ایلی نویز در ایالت متحده امریکا مطرح شد. در سال ۲۰۰۲ شبکه‌های اجتماعی فرنداستر (Friendster)، اورکات (Orkut) و لینکداین (LinkedIn) ایجاد شد در سال ۲۰۰۴، سایت شبکه اجتماعی فیس بوک توسط مارک زوکربرگ در خوابگاه دانشگاه هاروارد راه اندازی شد. در سال ۲۰۰۶ دسترسی عمومی مردم به فیس بوک آزاد شد. زیرا در دو سال قبل، این سایت تنها به صورت پایلوت در دانشگاه هاروارد استفاده می‌شد، همچنین توییتر نیز در این سال پا به عرصه وب سایت های اجتماعی گذاشت.




تعریف شبکه اجتماعی : شبکه‌های اجتماعی اینترنتی عموماً سرویسهای مبتنی بر وب هستند که مردم در آنها می توانند افکار، فعالیتها، نظرات، علاقه‌مندی‌ها و ... را با دوستان و سایرین به اشتراک بگذارند و امکان برقراری ارتباط بین خود و همفکرانشان را در زمینه‌های مختلف مورد علاقه فراهم می کنند. امروزه رسانه های اجتماعی به یک مهارت جدید و مهم برای همه و حتی برای کسانی که حتی درک زیادی از فناوری ندارند تبدیل شده است. شناخت صحیح از این رسانه ها باعث میشود تا کاربران بیش از پیش بتوانند از این ابزارها استفاده مفید و موثر داشته باشند و با شناخت از فواید زیاد

برای پیشرفت و ترقی جوامع، اثرات منفی و مخرب بی نظیری این شبکه ها نرا در نظر گرفته بعد انتخاب بعد مثبت یا منفی هر فناوری بر عهده خود کاربر است.



فرصت های شبکه های اجتماعی: ارتباط جهانی – اشتراک علایق و لحظه ای اطلاعات – شکل گیری و تقویت خرد جمعی– سرعت بالای انتشاراخبار – عبور از مرزهای جغرافیایی و آشنایی با افراد، جوامع و فرهنگهای مختلف – کارکرد تبلیغی و محتوایی (تبلیغات هدفمند) – امکان بیان ایده ها و آشنایی با افکار و سلیقه های دیگران – ارتباط مجازی مستمر با دوستان و آشنایان – یکپارچه سازی بسیاری از امکانات اینترنتی و وبی – توسعه مشارکت های مفید اجتماعی – افزایش سرعت در فرایند آموزش و ایجاد ارتباط شبانه روزی (بین استاد و شاگرد)– افزایش اعتماد، صمیمیت و صداقت – باعث ایجاد نظر و تبادل و تعامل در کسب و کار.

تهدیدات شبکه های اجتماعی: در معرض خطر قرار گرفتن روابط چهره به چهره – جعل هویت و کلاه برداری – اتلاف کننده زمان– ساختگی بودن نحوه ارتباط – تغییر خلقیات افراد – اضطراب ، استرس و افسردگی در میان فرزندان – وابستگی روانی و آسیب های ناشی از آن – درماندگی در فضای مجازی – بی خوابی – تأثیرات سیاسی – تأثیر بر افکار عمومی – ازدیاد روابط ناسالم و خارج از هنجارها – افزایش احساس نیاز به توجه – نابود کردن خلاقیت افراد – مقایسه پیوسته خود با دیگران و عواقب آن – شکل گیری و ترویج سریع شایعات و اخبار کذب – ضربه‌پذیری نوجوانان به دلیل عدم آگاهی و دانایی کافی و لازم – تغییرات خطرناک سبک زندگی اعضای خانواده با این شبکه‌ها – تبلیغات ضد دینی و القای شبهات (بی تفاوتی نسبت به مذهب) – فرد گرایی، بی نیازی و جدایی اعضای خانواده از هم – انزوا و دور ماندن از محیط های واقعی اجتماع – مزاحمت های سایبری و جرایم علیه کودکان– نقض حریم خصوصی افراد و به خطر افتادن آن – رعایت نشدن حریم های خانوادگی – بروز تأثیرات منفی و تغییرات رفتاری در رفتارهای اعضای خانواده – تلاش در جهت از بین بردن عفت و حیای خانواده ها – دگرگونی در تعامل فرزندان با والدین – ایجاد حقارت و از بین رفتن رفتارهای محترمانه (حرمت شکنی) – افزایش اختلافات خانوادگی – تاثیر مخرب بر هویت یابی جوانان – برقرای ارتباط های ناسالم – افزایش طلاق – ایجاد بدبینی و سوءظن در میان اعضای خانواده – سرکشی و فضولی در زندگی دیگران – ایجاد نارضایتی و تنفر از زندگی

نکات امنیتی در مورد مودم ADSL و اینترنت

سرپرست اداره پیشگیری از جرایم سایبری پلیس فتا ناجا با بیان اینکه نداشتن اطلاعات کافی نحوه استفاده از مودم های ADSL باعث دردسرهای زیادی برای این دست کاربران می شود، گفت: مجرمان سایبری با بکارگیری اکانت اینترنتی افراد مرتکب جرم شده و این کاربر است که باید پاسخگویی مقام قضایی باشد.

سرپرست اداره پیشگیری از جرایم سایبری پلیس فتا با بیان اینکه کاربران امکان کنترل از راه دور مودم (Remote Management یا Remote access) خود را غیر فعال کنند، ادامه داد: کاربران توجه داشته باشند که کنترل از طریق اینترنت را غیر فعال کنند اما امکان کنترل از طریق شبکه داخلی می تواند فعال باشد.

آذردرخش گام دیگر افزایش امنیت مودم کاربران را، مخفی سازی SSID و یا به اصطلاح، خاموش کردنBroadcasting SSID عنوان کرد و گفت: کاربران می توانند در تنظیمات مربوط به Wireless مودمشان، این گزینه را پیدا کرده و با خاموش کردن این قابلیت، نام مودم خود را از لیست وایرلس ها ناپدید کنند، از این رو کاربر باید از نام وایرلس خود مطلع باشد تا بتواند با مودم خود ارتباط برقرار کند.

وی بیشترین سوءاستفاده از اکانت اینترنت را برای شرکت ها و موسسات عنوان کرد و گفت: در شرکت ها برای کاربران نام کاربری و پسورد متفاوت تعریف و در صورت قطع همکاری سریع این نام کاربری غیر فعال شود. همچنین به کارکنان در خصوص حفاظت از نام کاربری و پسورد اکانت اینترنت شرکت تایید شود که در اختیار افراد یا همکاران دیگر قرار ندهند.

وی افزود: کاربران شبکه وای فای(بی سیم) خود را رمزگذاری کنند و بهتر است برای رمز گذاری شبکه وای فای خود به جای استفاده از مکانیسم WEP از WPA و یا WPA2 استفاده کنند تا احتمال نفوذ غیر مجاز به شبکه وای فای شما به حداقل برسد.

سرپرست اداره پیشگیری از جرایم سایبری پلیس فتا به مدیران فنی شرکت ها در خصوص فعال کردن امکان MAC filtering توصیه کرد: برای اتصال سیستم های موجود در شرکت ها حتما کارت شبکه (مک آدرس) سیستم را برای مودم تعریف کنید تا امکان ورود کاربران غریبه محدود شود.

وی همچنین در خصوص خاموش بودم مودم در ساعات غیر اداری و بلا استفاده به مدیران فنی شرکت ها و کاربران تاکید کرد و گفت: کاربران و مدیران فنی توجه داشته باشند که قابلیت WPS مودم غیر فعال باشد.

سرهنگ آذردرخش همچنین به کاربران و مدیران فنی در خصوص به روز کردن نرم افزار کنترل مودم هشدار داد و افزود: نسبت به برند و مدل مودم، نسخه های به روز نرم افزار کنترل مودم تهیه شود و برای تهیه این نرم افزار سایت تولید کننده مودم بهتر از سایت های متفرقه است، با دریافت این نرم افزار از سایت تولید کننده مودم مودم خود را آپدیت کنید.

سرپرست اداره پیشگیری از جرایم سایبری پلیس فتا در توضیح یکی از راهکارهای تشخیص استفاده از وای فای شما توسط کاربران دیگر گفت: با وارد کردن آی پی آدرس در نوار آدرس مرورگر اینترنت و ورود به صفحه تنظیمات مودم و کلیک روی گزینه کلاینت می توانید، ببینید چند سیستم به مودم شما متصل است و با کلیک کردن روی دکمه بلوک آن سیستم ها را از استفاده اینترنت از مودم خود محروم کنید.

آذردرخش در خصوص مواد قانونی مرتبط با دسترسی به اکانت اینترنتی به صورت غیر مجاز گفت: ماده یک قانون جرایم رایانه ای به دسترسی غیر مجاز می پردازد و برابر این ماده هر فردی به طور غیر مجاز به داده ها یا سامانه های رایانه ای یا مخابراتی که به وسیله تدابیر امنیتی حفاظت شده است دسترسی یابد، به حبس از ۹۱ روز تا یک سال یا جزای نقدی از پنج میلیون ریال تا ۲۰ میلیون ریال یا هر دو مجازات محکوم خواهد شد. (منبع: سایت تابناک)

وی ادامه داد: البته لازم به ذکر است در صورتیکه شخص بعد از دسترسی به رمز عبور مودم مرتکب جرایم دیگری مانند جعل، سرقت، کلاهبرداری هتک حیثیت، نشر اکاذیب و یا سایر جرایم رایانه ای شود، به مجازات جرم ارتکابی نیز محکوم خواهد شد.

سرپرست اداره پیشگیری از جرایم سایبری پلیس فتا از هموطنان خواست در صورت مواجه با هر گونه مورد مشکوک آن را از طریق سایت پلیس فتا به آدرس Cyberpolice.ir بخش مرکز فوریت های سایبری، لینک ثبت گزارشات مردمی در میان بگذارند.

عناوین رویدادهای خبری هفته

پدافند غیر عامل مهمترین دلیل برای نو شدن انرژیها در ایران

ساتکین با بیان اینکه انرژی‌های تجدیدپذیر امکان فروش بیشتر نفت را فراهم می کنند، پدافند غیرعامل، ایجاد حاشیه امن در سبد انرژی و سازگار بودن با محیط زیست را از جمله مهمترین دلایل لزوم روی آوری به سمت انرژی های تجدیدپذیر در ایران برشمرد... (وب سایت پایداری ملی)

مدرسه جنگ سایبری برای افسران ارتش اسرائیل

ارتش اسرائیل قصد دارد با افتتاح مرکز آموزشی جنگ سایبری برای نظامیان سطوح مختلف، آن‌ها را با تهدیدات و ابزار جنگ سایبر آشنا کند... (وب سایت پایداری ملی)

آمریکا و اسرائیل برای مقابله با تهدیدات سایبری با یکدیگر همکاری می کنند

سفیر آمریکا در اسرائیل در مورد همکاری‌های آمریکا و رژیم صهیونیستی و سرمایه‌گذاری این رژیم در آمریکا در جریان اجلاس تل‌آویو صحبت کرد... (وب سایت پایداری ملی)

دومین نمایشگاه امنیت سایبری ایران برپا می‌شود

دومین نمایشگاه امنیت سایبری ایران با حضور شرکت‌های خصوصی فعال در حوزه امنیت فضای تبادل اطلاعات مردادماه جاری در تهران برگزار می‌شود... (وب سایت پایداری ملی)

تب کنگو در کشور ۳ قربانی گرفت/ گوشت تازه نخورید

معاون مرکز مدیریت بیماری‌های واگیر وزارت بهداشت گفت: ۳۹ نفر به ویروس کریمه کنگو مبتلا و ۳ مورد فوتی گزارش شده است. بنابراین مردم به مُهر تأیید دامپزشکی روی کشتارها دقت و ۲۴ ساعت گوشت نذری را در یخچال نگهداری کنند... (وب سایت پایداری ملی)

هشدار کارشناسان درباره آسیب پذیری در برنامه Instapaper اندروید

به گزارش پایگاه اطلاع رسانی پایداری ملی، گروه امنیتی بیت دیفندر ادعا کرد که یک آسیب پذیری را در برنامه کاربردی Instapaper کشف کردند که کاربر را در برابر حملات MitM آسیب پذیر می کند... **(وب سایت پایداری ملی)**

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

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