پدافند غیرعامل

سال اقتصاد مقاومتی، اقدام و عمل

استانداری آذربایجان شرقی
اداره کل پدافند غیرعامل

ماهنامه پدافند غیرعامل
شماره ۱۱ – خرداد ماه ۱۳۹۵

در این شماره خواهید خواند:

رهبر انقلاب در دیدار کارگزاران نظام

ما البتّه برجام را ابتدائاً نقض نخواهیم کرد؛ این را همه بدانند! ما نقض نمیکنیم برجام را...

گزیده ای از سخنان رهبر انقلاب در دیدار کارگزاران نظام

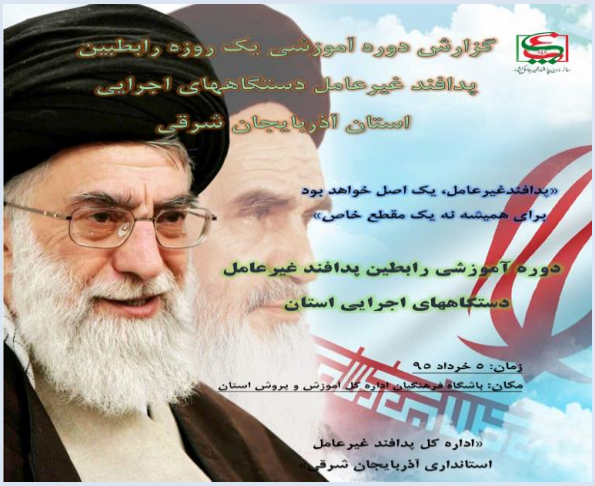
رهبر انقلاب اسلامی، تقویت «مصونیت و اقتدار کشور» را علاج واقعی همه‌ی دشمنی‌های مستکبران خواندند و تأکید کردند: «براساس فرمان صریح قرآن باید هرچه می‌توانیم قوت و قدرت «ایمانی، اقتصادی، دفاعی، علمی، سیاسی و جمعیتی» خود را افزایش دهیم. ایشان با فراخوان مسئولان همه‌ی دستگاه‌ها به ادای کامل وظایف خود در روند افزایش توان و «مصونیت ملی»، به مسئولان وزارتخانه‌ها و دستگاه‌های مرتبط با توان علمی کشور توصیه کردند خود را از حواشی دور نگه دارند ... حضرت آیت‌الله خامنه‌ای، نظرات هر دو گروه موافقان و مخالفان برجام را مبالغه‌آمیز خواندند و گفتند: هم افرادی که از برجام تمجید می‌کنند و هم مخالفان و منتقدان آن، در بیان نظرات خود گاهی مبالغه و اغراق می‌کنند، درحالی‌که برجام هم «نقاط مثبت و محسّنات» دارد و هم «نقاط ضعف و معایب» ما البتّه برجام را ابتدائاً نقض نخواهیم کرد؛ این را همه بدانند! ما نقض نمیکنیم برجام را لکن اگر طرف مقابل نقض کند که حالا همین‌طور این کسانی که نامزد ریاست جمهوری آمریکایند، مدام دارند تهدید میکنند که ما می‌آییم پاره میکنیم، نقض میکنیم، اینها اگر پاره کردند، ما آتش میزنیم. اینکه حالا نقض نمیکنیم، متّکی است به دستور قرآن: اَوفوا بِالعَهد؛(۱۹) بالاخره یک معاهده‌ای است انجام داده‌ایم، نمی خواهیم معاهده را ما به هم بزنیم ...

قرقیزستان هوا صادر می‌کند

به تازگی یک شرکت قرقیزستانی اعلام کرد قیمت یک بسته هوای قرقیزستان ۲۰۰ صوم یعنی حدود ۳,۵ دلار است که در حال حاضر چند سفارش تولید دریافت شده که در این درخواست‌ها هوای مناطق کوهستانی قرقیزستان جایگاه ویژه‌ای را دارد. به گزارش فارس در بیشکک به نقل از «۲٤ کی جی» بتازگی در قرقیزستان هوای فشرده به فروش می‌رسد. «ماکسیم باراویک» تولیدکننده این محصول غیرعادی با بیان تاریخچه اقدامات خود، اظهار داشت: این ایده چند سال پیش در ذهن من بود تا بتوانم هوای پاک را به صورت فشرده بسته بندی تهیه و صادر کنم. وی ادامه داد: در حال حاضر این ایده عملی شده و شرکت ما هوای بسته بندی را تهیه کرده و به کشورهای دیگر از جمله فرانسه و آلمان صادر می‌کند. ماکسیم باراویک تصریح کرد: ما از ۲ سال قبل در نظر داشتیم تا بسته‌بندی و صدور هوا را اجرایی کنیم که با عدم حق ثبت اختراع مواجه شدیم اما چندی قبل این مدرک را دریافت کردیم. وی افزود:قیمت یک بسته هوای قرقیزستان ۲۰۰ صوم یعنی حدود ۳,۵ دلار است که در حال حاضر چند سفارش تولید دریافت شده که در این درخواست‌ها هوای مناطق کوهستانی قرقیزستان جایگاه ویژه‌ای را دارد.

علاوه بر این، هوای قرقیزستان بیشتر برای گردشگران جذابیت دارد . کد خبر :۲۷٦۷۸٤-۲۵ خرداد ۱۳۹۵ - ۲۲:۱۳- سایت فرارو

گزارش دوره آموزشی یک روزه رابطبین پدافند غیرعامل دستگاههای اجرایی استان آذربایجان شرقی



سردار جهانسری مدیرکل پدافند غیرعامل استانداری آذربایجان شرقی

در طول یکسال گذشته با توجه به اهمیت موضوع سازه امن در کشور استان آ.ش با حمایت معاونت محترم سیاسی، امنیتی جناب آقای دکتر شبستری و معاونت محترم عمرانی استان جناب آقای پورمهدی همکاری جدی با بنده داشتند. در این استان نزدیک ٤۰ شرکت دوره عمومی پدافند غیرعامل را طی کرده اند. در مسیر اجرایی کردن مبحث ۲۱ شرکت های مشاوره‌ای مهندسی جهت أخذ گرید پدافند غیرعامل فراخوان شدند که انشاالله امیدواریم تا آخر خرداد ماه این شرکت ها گرید خودشان را أخذ نمایند. باید عوامل سازمانها، مدیران و مسئولان فنی فرمانداری ها وسازمان ها از نظر پدافند غیرعامل توجیه شوند که چه اتفاقاتی در این حوزه رخ می دهد و اشخاصی مستحق این گرید هستند که قبلا دارای گرید برنامه و بودجه بودند و بعد گرید پدافند غیرعامل را اخذ نمایند.

در طول یک و نیمسال گذشته ما بحث های عمومی پدافند غیرعامل را طی کرده ایم خوشحالیم که از این پس در کلاس ها بحث های تخصصی مبحث ۲۱ و اجرایی کردن ماده ۲۱۵ و بحث کالبدی داشته باشیم. با حمایت ها و درایت استاندار محترم جناب آقای دکتر جبارزاده و مسئولین امر از توسعه عمومی پدافند غیرعامل عبور کردیم و به بحث های تخصصی رسیده ایم که سمینار امروز در جهت اجرایی کردن اصول پدافند غیرعامل در بخش کالبدی به صورت تخصصی می باشد.

معاون محترم سیاسی و امنیتی و جانشین شورای پدافند غیرعامل استان

بحث پدافند غیر عامل بحث مهم، ضروری و نیاز امروز کشور است: دکتر سعید شبستری در سمینار اجرایی کردن مبحث ۲۱ در جمع رابطین پدافند غیرعامل دستگاههای اجرایی گفت از زمانی که سردار جهانسری عهده دار مسئولیت پدافند غیرعامل استان شده اند تحول خیلی خوبی را در این زمینه شاهد بودیم تا جایی که بنا به ارزیابی وزارت کشور استان ما جزو استانهای برتر در زمینه پدافند غیرعامل است که جای تقدیر و تشکر دارد. ما از همایش ها و سمینارهای تخصصی اسقبال کرده و از آن حمایت می کنیم. انتظار ما از این نشست ها این است که از کارها و حرف های کلیشه ای خودداری کنیم و وارد مباحث تخصصی شویم و برنامه های کاربردی ارائه دهیم.

جناب آقای مهندس مولوی معاون محترم مدیرکل پدافند غیرعامل وزارت کشور

یکی از ماموریت های اصلی پدافند غیرعامل حفاظت از سرمایه های ملی است. با اینکه عمر پدافند غیرعامل در ایران به صورت سازمانی یک دهه است اما در این مدت شاهد رشد و ساختارهای خوبی در کشور هستیم. معاون پدافند غیرعامل وزارت کشور با تاکید بر همگانی کردن فرهنگ پدافند از طریق آموزش و اطلاع رسانی و تولید محتوا اظهارکرد: باید ساختار پدافند غیر عامل را در شهرستان ها اجرایی کرده و برنامه های عمرانی را به صورت جدی پیگیری کنیم.

آقای یونسی مدیر کل محترم دفتر فنی استانداری

آمایش سرزمینی و جهت گیری های کلان در قالب طرح های آمایش سرزمینی می تواند کمک مؤثری در زمینه سازی برای نهادینه کردن فرهنگ پدافند غیرعامل ضمن کاهش هزینه های اضافی و دوباره کاری باشد.

کلاس آموزشی با موضوع سازه های امن و پدافند شهری

سردار حیدری معاون محترم امور بسیج و استان های پدافند غیرعامل کشور

بیشتر سناریوی دشمنان علیه کشور ما در حوزه پدافند عمومی و مردم محور قرار دارد: تبریز یک شهر صنعتی است و باید تهدیدات یک شهر صنعتی تبیین و بررسی شده و راهکارهای مقابله با آن بیان گردد. ایستگاه مترو تبریز نیز باید طوری طراحی شود که الزامات ۵۰ سال آینده در آن منظور شود. همچنین باید زیرساخت های حیاتی آنالیز شود و تهدیدات و آسیب های آن نیز شناسایی گردد.

جلسه سردار حیدری و مهندس مولوی به همراه مدیرکل محترم پدافند غیرعامل استان و کارشناسان مربوطه با جناب آقای مهندس پورمهدی معاون محترم عمرانی استانداری

معاون عمرانی استاندار در دیدار با معاون محترم امور استانهای سازمان پدافند غیرعامل کشور و معاون محترم مدیرکل پدافند غیرعامل وزارت کشور از آمادگی استان آذربایجان شرقی برای اجرایی کردن مفاهیم پدافند غیرعامل خبر داد و گفت: سعی کردیم تمام زیرساخت ها برای اجرایی کردن مبحث ۲۱ مقررات ملی ساختمان و ماده ۲۱۵ قانون پنجم توسعه کشور در استان آماده باشد بنابراین همه دستگاه های ما مجابند در هر پروژه ای که می خواهند مطالعه و طراحی کنند حتما باید مبحث ۲۱ را رعایت کنند.

مهندس پورمهدی با ابراز رضایت از عملکرد پدافند غیرعامل استانداری گفت: خوشبختانه با تحولی که سردار جهانسری در اداره کل پدافند غیرعامل به وجود آورده اند خیال ما از نهادینه و اجرایی کردن مباحث پدافند غیرعامل در استان راحت است.

جلسه سردار حیدری و مهندس مولوی به همراه مدیرکل محترم پدافند غیرعامل استان و کارشناسان مربوطه با معاونین اداره کل آموزش و پرورش استان آذربایجان شرقی

صمدیان معاون محترم اداره کل آموزش و پرورش استان: در حوزه پدافند غیر عامل ۳۸ عنوان دوره برای بیش از ۳۲ هزار نفر در سال ۹۴ برگزار شد.

در نشست کارگروه استانی پدافند غیر عامل که با حضور معاون محترم مدیر کل پدافند غیر عامل وزارت کشور و معاون محترم امور استان های سازمان پدافند غیر عامل کشور در تالار معلم تبریز برگزار شد صمدیان گفت: ۳۸ عنوان دوره برای بیش از ۳۲ هزار نفر با عناوین پدافند غیر عامل در سال ۹۴ برگزار شد.

نتیجه گیری

معاون محترم امور بسیج و استانهای سازمان پدافند غیرعامل کشور جناب سردار حیدری و نیز معاون محترم مدیرکل پدافند غیرعامل وزارت کشور، جناب آقای مهندس مولوی و هیات همراه بعد از بازدید از برخی طرح های استانی و شرکت در جلسات با مدیران استانی و رابطین پدافند غیرعامل دستگاههای اجرایی استان از عملکرد پدافند غیرعامل استانداری ابراز رضایت کردند.

در نشست نهایی که در ساعت ۲۱ با حضور سردار حیدری، مهندس مولوی، سردار جهانسری و کارکنان پدافند غیرعامل استانداری برگزار شد بر موارد زیر تاکید شد:

۱. آموزشهای پدافند غیرعامل در سطح استان تداوم داشته باشد و این آموزشها به صورت تخصصی دنبال شده و در شهرستانها نیز برگزار گردد.
۲. با توجه به گستردگی استان آذربایجان شرقی، بودجه و اعتبار کافی از سوی سازمان پدافند غیرعامل کشور برای نهادینه کردن مفاهیم پدافند غیرعامل در استان در نظر گرفته شود.
۳. با توجه به عملکرد کم سابقه آموزش پرورش استان در زمینه آموزش و نهادینه کردن مفاهیم پدافند غیرعامل، عملکرد این نهاد به سازمان پدافند غیرعامل کشور ارسال و مورد تشویق سازمان قرار گیرد.
٤. با توجه به همجواری استان با سه کشور دیگر و حساسیت پروژه های مرزی، اعتبار ویژه ای برای پروژه های مرزی استان در نظر گرفته شود.
۵. باید تدابیری اتخاذ گردد تا در برنامه ششم جایگاه قانونی سازمان پدافند غیرعامل مستحکم تر شود و با ابلاغیات و صراحت کامل راه برای اجرایی و عملیاتی کردن مباحث پدافند غیرعامل در کشور باز شود.

اسکیمر چیست و چگونه باعث سرقت اطلاعات کارت‌های بانکی می‌شود؟!

چند صد سال است که در تمام جهان بانک‌ها امین مردم هستند و اغلب افراد پول‌های اضافی خود را در آن‌ها نگهداری می‌کنند تا هم خطر سرقت آن‌ها به حداقل برسد و هم پول‌های راکد، در اقتصاد کشور مورد استفاده قرار گیرند. با وجود اینکه بانک‌ها نهایت سعی خود را در امانت‌داری می‌کنند اما در این بین افرادی نیز هستند که سعی می‌کنند با انجام کارهایی هم نفعی به شرایط اقتصادی خود داشته باشند و هم اعتماد مردم را نسبت به بانک‌ها از بین ببرند.

در حال حاضر اغلب افراد حتی خریدهای کم بهای خود را نیز از طریق کارت‌های عابربانک انجام می‌دهند که این موضوع نشان از حضور چشمگیر این کارت‌ها در زندگی افراد دارد. برخی افراد از طریق اینترنت اقدام به خرید می‌کنند که با وجود آسایش و امنیت بالا، امکان سرقت اطلاعات و در نتیجه سرقت پول کاربر از طریق حملات فیشینگ و موارد مشابه وجود دارد. اما در حال حاضر مشکل جدیدی به‌وجود آمده که عملا نشان از خبره بودن سارقان دارد. چند صباحی است که سرقت‌هایی به‌صورت اسکیمینگ (Skimming)خبرساز شده‌اند.

۱- اسکیمینگ چیست, اسکیمر کیست و ابزار اسکیمر کدامند ؟

اسکیمینگ (Skimming) چیست؟

Skimming یعنی کپی کردن غیر قانونی داده های نوار مغناطیسی کارت بانکی روی یک کارت دیگر.

اسکیمینگ (Skimming) چگونه انجام میشود؟

دستگاه هائی برای خواندن کارتهای بانکی وجود دارند که توسط عده ای از مجرمین از پیش در دستگاه های خودپرداز بانکها نصب شده و داده های نوار مغناطیسی کارت را کپی میکنند.

Pinlogger Keyboard

معمولا کد PIN توسط دوربینی مخفی فیلمبرداری شده یا روی صفحه کلیدی بدلی به نام پین لاگر ضبط میشود. بعضی دیگر به هنگامی که مشتری کد خود را وارد میکند سعی در دیدن آن داشته و سپس آنرا یاد داشت میکنند. این داده ربوده شده روی یک کارت خالی کپی میشود. با توجه به اینکه در کشورهائی غیر از کشورهای اروپائی از تراشه یا چیپ برای کارت بانکی استفاده نمیشود، کپی نوار مغناطیسی روی یک کارت خالی امکان برداشت از حساب بانکی را فراهم میکند.

اسکیمر (Skimmer) کیست

Skimmer به فردی گفته میشود که به اسکیمینگ (Skimming) اشتغال دارد یا مجرمی که کارش کلاه برداری از طریق کارتهای بانکی و استفاده از دستگاه های مخصوص اینکار است.

ابزار اسکیمر

HDP5000 Card Printer
براي چاپ كارت استفاده ميشود

كارت خالي با نوار مغناطيسي و يا با چيپ براي چاپ اطلاعات كارت ربوده شده براي فروش

Reader/Writer MSR206
MSRهاي ديگري نيز وجود دارند ولي Skimmers MSR206 را ترجيح ميدهند

MSR 206 برای خواندن و نوشتن روی باند مغناطیسی استفاده میشود.

Chip card reader multi pro 2000

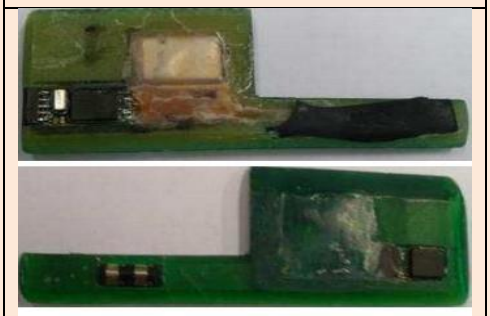
Chip card reader multi pro براي نوشتن و خواندن كارتهاي چيپ دار يا كارتهاي هوشمند استفاده ميشود

Stamper

براي استامپ كردن كارت

Card embosser Z2

براي چاپ برجسته روي كارت



Mini skim ATM

بخاطر داشته باشید

نمونه دیگری از اسکیمر که توسط مجرم روی دستگاه نصب شده است و بسیار شبیه قسمتی از خود دستگاه است. همانطور که می‌بینید تشخیص آن کار آسانی نیست.

اسکیمینگ مرتبا در حال افزایش است و ابزار آن مرتباً توسعه می یابند و ای تی ام ها کوچکتر شده و سیستمهای جدیدی ساخته می شوند. قربانیان متوجه نمیشوند که چه اتفاقی رخ داده است و بعد از گذشت ماه ها و زمانیکه کارتهای تقلبی حاوی اطلاعات فروخته شده و از آنها استفاده شود تازه صاحبان کارتهای اصلی با عملیات غیر طبیعی روی حسابهای بانکیشان که توسط خود انها صورت نگرفته از این امر مطلع میگردند.

اما موضوع خطرناکتر این است که هر کسی میتواند این ابزار را داشته باشد ، آنها روی سایتهائی در اختیار همگان هستند که این طبیعی است چون بعضی از شرکتها از کارتهای مغناطیسی برای بعضی امور استفاده میکنند. ولی خوشبختانه فروش و در دسترس قرار دادن ای تی ام ریدرها ممنوع است و در نتیجه مشکلتر میشود انها را یافت . اگر روزی خودپردازی که به آن رجوع کرده اید کارت شما را بلعید (بدون دلیل و نه بعد از وارد کردن کد اشتباه) در محل باقی مانده و در عین حال بلافاصله با شماره تلفی که روی ان قید شده تماس بگیرید.

همیشه پیش از استفاده از خودپرداز به همه چیز دقت کنید تا احیانا اگر ابزار اسکیمینگی نظیر دوربین یا صفحه کلید دروغین یا هر چیز مظنونی میبینید از ان خود پرداز استفاده نکنید.

بخاطر داشته باشید که یافتن دوربینهای جا سازی شده برای اسکیمینگ آسان نیست چون فقط یک سوراخ بسیار ریز برای فیلمبرداری در بالای صفحه کلید خودپرداز یا در قسمتی که بتوان صفحه کلید را فیلمبرداری کرد دیده میشود که همیشه و یا همه نمیتوانند آنرا تشخیص دهند.

اگر کارت شما به راحتی داخل دهانه ورودی کارت خودپرداز نمیشود اصرار نداشته باشید که به هر ترتیب اینکار را انجام دهید و بهتر است به مسئولین بانک این امر را اطلاع داده و به خود پرداز دیگری رجوع کنید. احتمال دارد که دهانه خودپرداز با یک تقلبی شبیه اصلی برای ثبت اطلاعات کارت جایگزین شده باشد که گاهی به دلیل کمبود وقت اسکیمر یا جلب توجه عده ای و یا تازه کار بودن نتوانسه آن را درست جایگزین کند.

هر گاه چیز مظنون و غیر طبیعی دیدید علاوه بر مطلع کردن مسئولین بانک و یا تماس با شماره تلفن قید شده روی خودپرداز, فراموش نکنید که افرادی را که در پشت سر شما به انتظار نوبت خود ایستاده اند را نیز از احتمال اسکیمینگ مطلع سازید.

راه‌های مقابله با Card Skimming

برای جلوگیری از این نوع کلاهبرداری و تخلف، یک قطعه پلاستیک در دریچه ورود کارت دستگاه‌های خودپرداز قرار داده می‌شود. شکل این قطعه پلاستیکی به نوعی است که جلوی این نوع کلاهبرداری را می گیرد و در عین حال از سهولت در کاربری خودپرداز، نمی‌کاهد. این قطعه با استفاده از استانداردهای امنیتی و برای پوشش امنیتی ساخته شده است و در صورتی که هر نوع دستکاری در دریچه کارت خوان به وجود آید و یا اینکه دریچه تحت فشار فیزیکی قرار گیرد، دستگاه خودپرداز ازحالت سرویس دهی خارج می‌گردد. این قطعه در دریچه کارتخوان دستگاه خودپرداز نصب شده و محفظه ورود کارت را پایش می‌کند و هر نوع ورود غیر مجاز و موارد این چنینی را کنترل می‌نماید.

به عنوان شهروند عادی چه کنیم؟

شاید در ابتدا در ظاهر شناخت این نوع از کلاهبرداری کار سختی باشد اما شهروندان عادی حداقل کاری که می‌توانند بکنند این است که هنگام استفاده از دستگاه‌های خودپرداز دقت کنند که مجرای ورودی کارت دچار شکستگی نشده باشد و دقت کنند که هیچ گونه قطعه اضافی که از بیرون بشود آن را نصب یا حدف کرد روی دستگاه نباشد.

۱-۱- دستگاه‌های POS

سرقت اطلاعاتی مربوط به برداشت از حساب افراد به شکل های متفاوتی صورت می گیرد که شیوه ای از آن نصب دستگاهی کوچک به نام اسکیمر بر روی دستگاه کارت‌خوان (POS) می‌باشد. متأسفانه اکثر کاربران جهت پرداخت مبلغ کالای خریداری شده، کارت خود را تحویل فروشنده می‌دهند که این کار باعث سوءاستفاده شیادان و کلاهبرداران می‌گردد.

سرپرست اداره پیشگیری از جرایم سایبری پلیس فضای تولید و تبادل اطلاعات ناجا با اشاره به استقبال خریداران و فروشندگان از دستگاه POS

بانکی گفت : این امر باعث گردیده تا اسکیمرها با تکنیک اسکیمینگ (Skimming) کپی کردن غیر قانونی داده‌های نوار مغناطیسی کارت بانکی اقدام به سرقت بکنند.

سرهنگ دوم آذردرخش تصریح کرد : با وجود تلاش‌های هماهنگ از سوی مؤسسات مالی در سراسر کشور، تقلب و دستکاری در جهت دسترسی به حساب افراد از طریق دستگاه‌های POS همچنان به صورت یک مشکل، رو به رشد است. وی افزود : مجرمان با نصب ابزاری پیشرفته در محل ورودی کارت‌های بانکی (POS) که قادر است تمامی اطلاعات کارت بانکی را کپی کرده و اطلاعات کارت را بخواند و با بدست آوردن رمز عبور که معمولاً مشتریان در اختیار آنها قرار می‌دهند، تمامی اطلاعات مورد نیاز برای دسترسی به حساب افراد را بدست آورده و از این طریق سرقت الکترونیکی اتفاق می‌افتد.

سرپرست اداره پیشگیری از جرایم سایبری با بیان اینکه برای نوع سرقت‌های الکترونیکی خود کاربر مهمترین نقش را در این رابطه ایفا می‌کند، گفت : کاربران با رعایت یک‌سری نکات، امنیتی ساده می‌توانند ضمن حفظ اطلاعات کارت بانکی خود مانع از سرقت الکترونیکی از حساب بانکی خود باشند. سرهنگ دوم آذردرخش ادامه داد : مشکل اینجاست که متأسفانه دستگاه‌های کارت‌خوان (POS) در اختیار فروشندگان است و خود، کارت خریدار را تحویل گرفته و مبلغ کالای خریداری شده را کسر می‌کنند و اینجاست که امنیت اطلاعات کارت خریدار به خطر می‌افتد و زمینه کلاهبرداری و برداشت غیر مجاز فراهم می‌شود. وی با بیان اینکه مجرمان با نصب قطعاتی بسیار پیشرفته و کوچک به نام اسکیمر، کنار شکاف ورودی دستگاه (POS) کارت‌خوان قادر به خواندن اطلاعات محرمانه داخل کارت عابر می‌شوند، گفت :رمز کارت را نیز خودمان هنگام خرید در اختیار این افراد می‌گذاریم .

سرهنگ آذردرخش با بیان اینکه جهت پرداخت کالای خریداری شده خود شخصاً به دستگاه POS مراجعه کرده و عملیات واریز پول را انجام دهید، گفت : کارت‌های عابر خود را در اختیار فروشندگان قرار ندهید، همچنین در صورتی که شکل دستگاه POS غیر عادی بود، قطعه‌ای بر روی سطح آن نصب شده و یا چسب خورده بود مراتب را به بانک مورد نظر اطلاع دهیم. هنگام وارد کردن رمز عبور به اطراف و اطرافیان خود توجه داشته باشیم و دست خود را حائل قرار دهیم. پس از اتمام عملیات رسید آن را به دقت بررسی و نزد خود نگه داریم. همچنین در صورت ناموفق بودن تراکنش، رسید مربوطه را دریافت و تا حصول اطمینان از کسر نشدن وجه از حساب بانکی نزد خود نگهدارید.

سرپرست اداره پیشگیری از جرایم سایبری در ادامه تصریح کرد : بانک‌ها جهت جلوگیری از نصب قطعات اسکیمر بر روی دستگاه‌های (POS) کارت‌خوان بر روی آنها آنتی اسکیمر نصب کنند.

وی با بیان اینکه بانک‌ها با همکاری اصناف باید دستگاه‌های POS را در محلی که به راحتی در اختیار مشتریان قرار می گیرد نصب نمایند، گفت : راهنمای استفاده از دستگاه‌های POS نیز در محل نصب POS قرار دگیرد تا مشتریان، بتوانند از قابلیت‌های آنها به راحتی استفاده کنند. بانک‌ها باید مجوز نصب این دستگاه POS را فقط در اختیار یک شرکت معین قرار دهند تا تمام مسئولیت‌ها بر عهده یک سازمان باشد. از بکارگیری شرکت‌های کوچک و خرد به صورت پیمانکاری برای نصب دستگاه‌های POS باید خودداری نمایند

http://www.tarfandestan.com/forum/thread122778.html[1]
[2] http://banki.ir/bank-ha/21933
[3] http://way2pay.ir/18479

لیدا رسول اهری-کارشناس آموزش و پژوهش اداره پدافند غیرعامل استانداری آذربایجان شرقی

فضای مجازی، خط مقدم جنگ نرم انقلاب اسلامی

در خصوص تشریح جوانب جنگ نرم دشمن و تأکیدات مقام عظمای ولایت به کارگزاران رسانه: شش اصل از ۲۴ اصول دکترین دفاعی کشور از جمله مدیریت افکار عمومی، اعتماد و انسجام دولت و ملت، ارتقای استانه تحمل عمومی و خنثی سازی جنگ نرم معطوف به صدا و سیماست؛ لذا استراتژی مقابله با حملات دشمن در فضای روانی سایبری و فرهنگ عمومی نیازمند تعامل سه جانبه مسئولان، رسانه و مردم است.

عصر مجازی یا موج چهارم چیست؟

موج چهارم یا عصر مجازی در حقیقت، شکل توسعه و تکامل یافته عصر اطلاعات و دانش است که در آینده‌ای نزدیک ظهور خواهد کرد و فضای سه بعدی را در اختیار بشر قرار خواهد داد. عصر کشاورزی با هدف تهیه و تامین غذا بوقوع پیوست و تقریباً سی هزار سال دوام داشت. عصر صنعت پس از آن شکل گرفت و مشکل ابزار و مواد را که نیاز آن زمان بشر بود برطرف نمود و حدوداً ۵۰۰ سال دوام داشته و در بعضی از کشورها همچنان حاکمیت دارد. موج سوم مربوط به عصر اطلاعات است که با حضور رایانه معرفی شده به سرعت در حال گسترش و توسعه بوده و به پیش می‌رود و حوزه فناوری اطلاعات و ارتباطات را شدیداً تحت تاثیر خود قرار داده است، اینترنت مشخص‌ترین نماد این عصر است. هدف از بوجود آمدن این عصر رفع نیاز اطلاعاتی بشر بوده است که به کمک رایانه و اینترنت همراه با بانکهای اطلاعاتی و شبکه‌های تار عنکبوتی WWW جهانی این نیاز تا حدودی مرتفع شده و در آینده تاثیر خود را با انتقال فضای یک بعدی (متن، پست الکترونیکی و اتاقهای گفتگو) به دو بعدی (فیلم، تصویر و آدمکهای شبیه‌سازی شده)که مشخصه این عصر است بیشتر نمایان خواهد نمود. عمر این عصر کوتاه خواهد بود و فقط از چند دهه تجاوز نخواهد کرد. موج چهارم در راه است و به زودی دنیای سه بعدی را به جهان عرضه خواهد کرد و شرایطی را فراهم می‌کند تا تخیل انسان بتواند به حقیقت نزدیک شده و فضای جدیدی را معرفی خواهد نمود که بسیار توسعه یافته‌تر و متفاوت با جهان امروز است. جامعه اطلاعاتی امروز باید چشم انداز روشنی برای ادامه مسیر خود به سمت رشد و پویایی داشته باشد، عصر مجازی می‌تواند دورنمای تحول درازمدت جامعه اطلاعاتی امروز باشد.

فضای مجازی، خط مقدم جنگ نرم انقلاب اسلامی

در دنیای واقعی انسانها در طول زمان و در چهارچوب مکان محصور بوده و محدوده فعّالیّت‌هایشان متأثّر از این واقعیّات است. امّا در دنیای مجازی با استفاده از فنّاوری‌های نوین ارتباطی و رایانه‌ها به نقاط ضعف انسان که همانا سرعت، دقّت، حافظه و خستگی و مشکل جوامع کاری که همانا زمان، هزینه ...

تغییر و تحولات سریع و شگرف در قرن بیست ویکم در محورهایی چون؛ پیشرفت علم، تکنولوژی و فناوری اطلاعات ضمن اینکه غیر قابل انکار است بلکه غافگیر کننده نیز هست. به گونه ای که اگر لحظه ای از آن غفلت شود سالها عقب خواهی ماند. در این بین ارتباطات از همه مقوله ها پیشرو و جلوتر است به گونه ای که از دیگر موضوعات در حال رشد و پیشرفت پیش قدم است. "بنا به نظر آلوین تافلردر کتاب موج سوم، جوامع بشری تاکنون دو دوره‌ی (انقلاب) کشاورزی و صنعتی را پشت سر گذاشته و هم اکنون در اواخر عصر فراصنعتی یا عصر اطّلاعات که بر پایه الکترونیک و رایانه‌هاست قرار دارند. این عصر، عصریست که در آن قدرت، ثروت و امنیّت بر پایه دانش بوجود آمده و سرعت وجه مشخّصه‌ی آن و اطّلاعات به عنوان ارزشمندترین کالا محسوب می‌شود. "عصر اطّلاعات" یا به روایتی "عصر رایانه‌ها و شبکه‌ها"، جهانی را ترسیم می‌نماید که بر پایه شبکه‌های رایانه‌ای و تعاملات کاربران با رایانه‌ها شکل گرفته و حتّی ارتباطات انسانی و اجتماعی که جزو سنّتی‌ترین

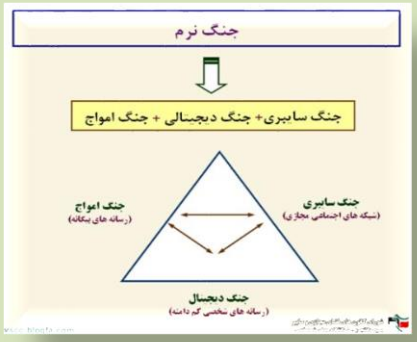
خصوصیّات بشر هستند نیز در حال انتقال به این فضای جدید می‌باشند. این جهان نوپا که به سرعت در حال بسط و گسترش بوده و تمامی شئون زندگی بر روی کره زمین را تحت تأثیر قرار داده است، بر پایه فنّاوری اطّلاعات و رسانه‌های ارتباطی نوین استوار بوده و در فضایی غیر فیزیکی به رشد و بالندگی خود ادامه داده و در حال تسخیر جهان واقعی می‌باشد. این فضا، فضای سایبر (Cyberspace) یا فضای مجازی نام دارد."

فضای سایبر (Cyberspace) عبارتی است که در دنیای اینترنت، رسانه و ارتباطات بسیار شنیده می‌شود. به نظر میرسد بکارگیری این اصطلاح در این زمینه و برای ارجاع به امور فنی به آن رنگ و بویی صرفا فنی و مکانیکی داده باشد. ملاحظه دقیق‌تر این اصطلاح نشان می‌دهد که این واقعیت، وجوه و جنبه های متنوعی از جمله خصلت های روانشناختی قابل توجه نیز دارد. در منابع موجود آمده است که: اما کار واژه سایبر، از ریشه یونانی لغت کنترل گرفته شده و به طور ترکیبی در واژه سایبرنتیک به کار رفته است. همانطور که پیش از این نیز گفته شد مفهوم سایبرنتیک دلالت بر سیستمهای کنترلی ابر تکنولوژی های رایانه های بهم پیوسته، تکنولوژی جدید و واقعیات مصنوعی با راهبردهای دستیابی و کنترل سیستمی دارد.

"فضای مجازی در واقع محیطی است مشتمل بر شبکه‌ای از رایانه‌ها، رسانه‌های ارتباطی و کاربران که لحظه به لحظه به تبادل داده‌ها و اطّلاعات پرداخته و انسان‌ها در آن به کار، تأمین نیازها و پرداختن به علائق می‌پردازند. این فضا باعث کوتاه شدن فاصله‌ها و استقلال از مکان می‌گردد و در نهایت منجر به کم رنگ شدن مفهوم مکان و زمان کلاسیک گشته و به پدیده‌ای که دیوید هاروی آن را فشردگی فضا- زمان می‌نامد تبدیل شده است. این معنا بارزترین تفاوت دنیای واقعی و فضای مجازی می‌باشد، زیرا در دنیای واقعی انسانها در طول زمان و در چهارچوب مکان محصور بوده و محدوده فعّالیّت‌هایشان متأثّر از این واقعیّات است. امّا در دنیای مجازی با استفاده از فنّاوریهای نوین ارتباطی و رایانه‌ها به نقاط ضعف انسان که همانا سرعت، دقّت، حافظه و خستگی و مشکل جوامع کاری که همانا زمان، هزینه، نیروی انسانی و محدودیّتهای جغرافیایی هستند، پوشش داده شده و با سرعتی نزدیک بسرعت نور خواسته‌ها و پاسخها به مقصد و مبداء منتقل میگردد.

در هر حال فضای مجازی در هر تعبیری و با هر تعریفی، قلمرویی وسیع، بدیع و بکر است که برای ساکنان خود امکانات، آزادی‌ها، فرصت‌ها، دلهره‌ها، آسیب‌ها و محدودیّت‌های نوینی را به همراه دارد. اهمیّت این قلمرو تا حدّی است که امروزه برخی اندیشمندان صحبت از دو جهانی شدن دنیای معاصر می‌کنند. در حقیقت فضای مجازی نوع متفاوتی از واقعیّت مجازی و دیجیتالی است که آن را "واقعیّت خلق شده توسّط رایانه" می‌دانند، واقعیّتی که از آن رو مجازی یا مصنوعی است که در دنیای واقعی و محیط مادی، مکانی را اشغال نکرده و در اذهان کاربران و در نتیجه تعامل با واسط الکترونیکی بوجود آمده است. به عبارت دیگر فضای مجازی فضایی است که ساکنان آن محدودیّت‌های جسم و مکان فیزیکی را نداشته و در دنیایی با زمان غیر خطی و فضایی بدون محدودیّت جغرافیایی و ملیّتی به سر می برند و حتی اشخاص میتوانند هویّتی جدید و سوای هویّت واقعی خود داشته و زندگی جدیدی را تجربه کنند.

برای درک بهتر این مفهوم به این جمله توجّه نمایید: "شخصی در خواب می‌بیند که پروانه شده است، وقتی بیدار می‌شود با خود می‌اندیشد: آیا من خواب دیده‌ام که پروانه شده بودم یا اینکه پروانه‌ای هستم که اکنون خواب می‌بینم به مردی بدل شده؟" در ورای این جمله معنایی



نهفته است که توصیفی است از سیستمی‌که در آن خود واقعیّت کاملاً در متنی مجازی و در جهانی واقع نما غرق شده است لذا در فضای مجازی چیزهایی که بر روی صفحه‌ی رایانه‌ها ظاهر می‌شوند فقط تصاویری از تجربه نیستند، بلکه خود تجربه از طریق آنها منتقل می‌شود.

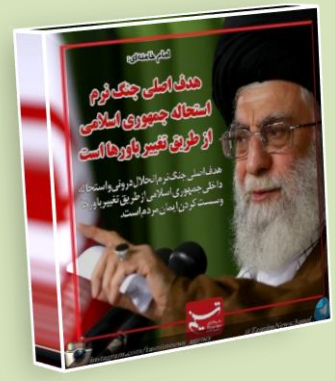
البته نمی‌توان اینترنت را مترادف با فضای مجازی دانست، لیکن اینترنت ابزار ورود به فضای مجازی می‌باشد که امروزه زندگی روزمره ما را تسخیر کرده و از ابزاری لوکس و مخصوص متخصّصان و روشنفکران به یک نیاز اساسی برای همه دولت‌های آینده‌نگر و شهروندان آنان تبدیل شده که بر بستر آن شکل نوینی از زندگی در جریان است. شاید این عبارت گویای بسیاری از مسائل باشد: "اگر روزگاری تمدن‌ها در کنار رودها شکل می‌گرفتند و رشد می‌کردند، هم‌اکنون بر بستر شبکه‌های ارتباطی و درون فضای مجازی شکل می‌گیرند.

فضای سایبر در معنا به مجموعه هایی از ارتباطات درونی انسانها از طریق کامپیوتر و مسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی گفته می شود.یک سیستم آنلاین نمونه ای از فضای سایبر است که کاربران آن می‌توانند از طریق ایمیل با یکدیگر ارتباط بر قرارکنند. بر خلاف فضای واقعی، در فضای سایبر نیاز به جابجایی‌های فیزیکی نیست و کلیه اعمال فقط از طریق فشردن کلیدها یاحرکات ماوس صورت می‌گیرد. این عدم جابجایی فیزیکی، محققان را واداشت که به مطالعه برخی شباهتهای فضای سایبر با حالتهای نا هشیاری، بخصوص حالتهای ذهنی‌ای که در رویا ها ظاهر می‌شوند، بپردازند. عملیات‌های مجازی، استفاده از تمامی امکانات برای اثرگذاری بر افکار، احساسات، اعتقادات، تمایلات و رفتارها در فرهنگ‌ها و ملت‌های مختلف است. فضای مجازی تعبیری است مبتنی بر این فرض که این فضا محلی است که خودآگاهی آدمی (بعنوان مثال هنگامی که از اینترنت استفاده می کند) در چنین محلی قرار می گیرد. مطمئن نیستم که چنین اصطلاحی، گویای چنین مفهومی باشد، اگرچه اکثر مردم، چنین مفهومی را از این اصطلاح درک می‌کنند.در تمام تعاریف فضای مجازی، این فضا محیط الکترونیکی یا محیط شبکه ای از کامپیوتر ها دانسته می شود که با استفاده از جلوه های سمعی و بصری سعی دارد تا اشیاء و واقعیت های سه بعدی جهان واقعی را مشابه سازی کند اما ادعا می شود که فاقد مادیت فیزیکی هستند.گفته می شود که از خصوصیات بارز این فضا بی مکانی و بی زمانی است.

➢ اهمیت و ضرورت توجه به فضای مجازی از نگاه رهبر معظم انقلاب اسلامی

صدور حکمی محکم در خصوص تشکیل شورای عالی فضای مجازی و به دنبال آن تعیین وظیفه ای سنگین مبنی بر ایجاد "مرکز ملّی فضای مجازی کشور" خود به خود ضمن اینکه نشان از هوشمندی معظم له دارد نشان دهنده هدف مند بودن این امر در موقعیت زمانی حاضر نیز به شمار می رود. حال با کمی دقت در متن پیام می توان بیشتر به اهمیت این موضوع پی برد. نکات کلیدی و راهبردی همچون " اشراف کامل در سطوح داخلی و خارجی" مواجهه فعال و خردمندانه"در نظر گرفتن محورهای " سخت افزاری، نرم افزاری و محتوایی" و همچنین تعین و ابلاغ وظایف به پیوست حکم نیز اهمیت موضوع را دو چندان نموده است. تسریع در تشکیل و راه اندازی مرکز و تاکید بر همکاری کلیه دستگاهها نیز از اهمیت و ضرورت موضوع می باشد"این شورا وظیفه دارد مرکزی به نام مرکز ملّی فضای مجازی کشور ایجاد نماید تا اشراف کامل و به روز نسبت به فضای مجازی در سطح داخلی و جهانی و تصمیم‌گیری نسبت به نحوه مواجهه فعال و خردمندانه کشور با این موضوع از حیث سخت‌افزاری، نرم‌افزاری و محتوایی در چارچوب مصوّبات شورای عالی و نظارت بر اجرای دقیق تصمیمات در همه سطوح تحقق یابد. نکات اساسی در مورد وظایف شورای عالی و مرکز فضای ملّی مجازی با تأکید بر توجه جدّی به آن، در پیوست این حکم ابلاغ می‌گردد. در پایان انتظار دارم، ضمن تسریع در تشکیل مرکز ملّی فضای مجازی، رئیس و اعضای محترم شورا تلاش بایسته را در جهت دستیابی این مرکز به اهداف

تعیین شده به کار برند. کلیه دستگاههای کشور موظف به همکاری همه جانبه با این مرکز می‌باشند."



البته توجه به مقوله رسانه های نوین از سوی رهبر انقلاب به حکم اخیر هم بر نمی گردد بلکه بارها توجه مسئولان و مردم و نخبگان را به این موضوع جلب نموده اند. معظم له در پنج سال پیش از این به طراحی غرب در این خصوص اشاره نموده اند." تحولات کشورهای آسیایی و آفریقایی و امریکای لاتین در دام طراحی باندهای قدرت بین المللی افتاده است و طراح اینها صهیونیست و سرمایه داران بین المللی بوده اند. برای اینها آنچه مهم بوده، کسب قدرت سیاسی است که بتوانند در کشورها و دولتهای اروپایی و غیره نفوذ کنند و قدرت سیاسی را در دست بگیرند و پول کسب کنند و این کمپانی ها، سرمایه های عظیم، کارتل ها و تراست ها را به وجود آورند. هدف این بوده است؛ آن وقت اگر اقتضاء می کرده است که اخلاق جنسی ملتها را خراب کنند، راحت می کردند؛ مصرف گرایی را در بین آنها ترویج کنند، به راحتی این کار را انجام می دادند؛ بی اعتنایی به هویت های ملی و مبانیِ فرهنگی را در آنها ترویج کنند، این کار را می کردند .اینها، اهداف کلان آنها بوده است که تصویر می کردند. آن وقت همیشه لشگری هم از امکانات فرهنگی و رسانه ای و روزنامه های فراوان و مسائل گوناگون تبلیغات در مشت اینها بوده است، که اینها امروز یواش یواش دارد پخش می شود و من در روزنامه ها گزارشی از تشکیلِ «ناتوی فرهنگی» را خواندم. یعنی در مقابل پیمان ناتو که امریکایی ها در اروپا به عنوان مقابله ی با شوروی سابق یک مجموعه ی مقتدر نظامی به وجود آوردند؛ اما برای سرکوب هر صدای معارض با خودشان در منطقه خاور میانه و آسیا و غیره از آن استفاده می کردند، حالا یک ناتوی فرهنگی هم به وجود آورده اند. این، بسیار چیز خطرناکی است. البته حالا هم نیست؛ سالهاست که این اتفاق افتاده است. مجموعه ی زنجیره ی به هم پیوسته ی رسانه های گوناگون که حالا اینترنت هم داخلش شده است و ماهواره ها و تلویزیونها و رادیوها - در جهت مشخصی حرکت می کنند تا سررشته ی تحولات جوامع را به عهده بگیرند؛ حالا که دیگر خیلی هم آسان و رو راست شده است."

امروز مؤثرترین سلاح بین المللی علیه دشمنان و مخالفین، سلاح تبلیغات است؛ سلاح ارتباطات رسانه‌ای است. امروز این قوی‌ترینِ سلاح است و از بمب اتم هم بدتر و خطرناکتر است.

در نبرد نرم به جای تصرف نظامی سرزمین دشمن و حکومت مستقیم بر آن، ساختار سیاسی اشغال می شود و مدیریت غیر مستقیم از طریق گماردن دولت دست نشانده در آن، در صدد دست یابی به اهداف خود بر می آیند. راه تسخیر مردم به گونه‌ای است که خود آنان خواسته‌های دشمن‌شان را محقق می سازند. این راه بسیار ساده و در عین حال دشوار است، تصرف قلب‌ها و تسلط بر ذهن‌ها، در نبرد نرم، موجب حرکت مردم در راستای اهداف دشمن می گردد. در جنگ نرم، دشمنان از طریق برتری رسانه‌ای خود، با روش کنترل احساسات و علایق، اراده مخاطبین را تسخیر نموده و در مسیر اهداف خود به حرکت و عمل وا می‌دارند. کیفیت این تسخیر در حدی است که فرد تصرف شده، نسبت به دشمنی که او را تسخیر نموده، هیچ کینه و نفرتی ندارد .

منابع:

- آلوین تافلر. موج سوم. مترجم : شهین دخت خوارزمی. تهران، ناشر: علم – ۱۳۸۵(برگرفته از مقاله آقای مهرداد حقیقی)
- حجت الاسلام دکتر سعید رضا عاملی، (-۱۳۴۰)، دکترای جامعه شناسی ارتباطات از دانشگاه رویال هالووی لندن، دانشیار گروه ارتباطات و رییس دانشکده مطالعات جهان دانشگاه تهران
- بایدها و بایسته های تشکیل «شورای عالی فضای مجازی، بولتن نیوز، دوشنبه ۲۱ تیر ۱۳۹۵ 2016 July 11 - کد خبر :۷۸۳۱۴
- بیانات مقام معظم رهبری در دیدار دانشگاهیان سمنان ۱۸/۰۸/۱۳۸۵
- دیدار جمع کثیری از بسیجیان کشور (۰۴/۰۹/۱۳۸۸)

تهیه و تدوین: حمید غفارلو، کارشناس حفاظت و امنیت

مزاحمت سایبری چیست؟

آزار و اذیت هنگامی روی می دهد که شخصی مرتب برای شخص دیگر مشکل ایجاد می کند یا او را مورد تهاجم و حمله قرار می دهد. اگر آنلاین باشد، این مزاحمت « مزاحمت سایبری » نامیده می شود و معمولاً در نظرات متنی ، پیام ها و ویدیوها مشاهده می شود. افرادی که دیگران را مورد آزار و اذیت قرار می دهند معمولاً به دنبال جلب توجه و عکس العمل افراد دیگر به صورت آنلاین یا در زندگی واقعی هستند. آزار و اذیت می تواند کمی آزار دهنده باشد یا می تواند مشکلات ایمنی بسیار جدی را موجب شود. دانستن فرق بین این دو بسیار مهم است، این که بدانید چه موقع باید فقط کاربر را نادیده بگیرید و یا چه موقع باید مسأله را به یک بزرگ تر مورد اطمینان یا مقام مسوؤل گزارش دهید.

چگونه می توانم آزار و اذیت و مزاحمت سایبری را متوقف کنم؟

هر فردی که آنلاین هست لزوماً فرد خوبی نیست. برخی اوقات ممکن است نظرات تا حدی خشن باشند. چیزی که تقریباً بین همه افرادی که مشوق تنفر هستند مشترک است، این است که سعی می کنند واکنش شما را برانگیزند. در صورتی که نظرات کاربری شما را آزار می دهد، شاید پاسخ به وی فکر خوبی نباشد. به جای آن، نظرات را حذف کنید و کاربر را مسدود کنید تا دیگر نتواند ویدیوهای دیگر شما را مشاهده کرده و نظرات دیگری بدهد. همچنین می توانید نظرات را برای هر ویدیویی که بخواهند غیر فعال کنید یا با درخواست تائید اولیه قبل از پست نظرات، آن ها را مدیریت و کنترل کنید.

- انسداد کاربران مشکل دار
- حذف کردن و انسداد با استفاده از ابزار راهنمایی و ایمنی یوتیوب
- فعال و غیرفعال کردن نظرات ویدیویی
- نحوه کنترل نظرات پست شده به کانال تان

برخی اوقات ممکن است انتقادها و توهین ها شدیدتر شده و به شکل آزاد و اذیت سایبری در آید. در صورتی که تهدیدهای خاصی علیه خود دریافت کردید یا احساس خطر کردید، به یک بزرگ تر مورد اعتماد اطلاع دهید یا را به پلیس فتا گزارش کنید.

چرا باید آزار و اذیت و مزاحمت سایبری را متوقف کرده یا از آن جلوگیری کرد؟

وقتی می آموزید چگونه به خود کمک کنید، می توانید به دیگران نیز نشان دهید چگونه آزار و اذیت و مزاحمت ها را متوقف کنید. وقتی ما همه با این رفتار زشت و بد مبارزه کنیم، محیط بهتری ایجاد می کنیم که در آن کاربران می توانند با یکدیگر ارتباط برقرار کرده و ویدیو به اشتراک بگذارند.

- بدون رضایت قربانیان از آن ها فیلم بردار می کنند
- برای فریب دادن دیگران، خود را به عنوان اشخاصی دیگر در اینترنت وانمود می کنند
- به بخش اکاذیب و شایعات درباره قربانیان می پردازند
- در صورتی که مکرراً مورد مزاحمت قرار می گیرید، شناسه کاربری، نام مستعار یا نمایه خود را تغییر دهید
- مردم را فریب می دهند تا اطلاعات شخص خود را فاش کنند
- نظرات خصومت آمیزی را پست می کنند

ابزار راهنمایی و ایمنی

در حقیقت، ابزار راهنمایی و ایمنی جهت کمک به ما برای اینکه بتوانیم محتوا را شخصاً حذف کنیم یا اطلاع از نحوه مسدود کردن سایر کاربران

و در صورت لزوم گزارش مشکلات به گروه یوتیوب طراحی شده است. معمولاً قربانی مزاحمت سایبری شدن یک تجربه دردناک و رایج است. کسی که مزاحمت سایبری می کند، مرتکب موارد زیر می شود:

- از تاریخ و زمان پیام های ایجاد مزاحمت و هر گونه اطلاعاتی که درباره شناسه فرستنده در دست دارید یادداشت برداری کنید
- از دست به دست کردن ویدیوها یا پیام های مزاحم سایبری بپرهیزید- زیرا با این کار شما نیز رفتار زشت مزاحمت را انجام می دهید
- اگر فکر می کنید شخص دیگری مورد مزاحمت سایبری قرار گرفته است، این امر را نادیده نگیرید. در صورتی که می بینید مزاحمت سایبری ادامه دارد، مورد را گزارش دهید و قربانی را پشتیبانی کنید- به او درباره Cyber Mentors بگوئید
- هر پیام، پست، عکس یا ویدیوی مزاحمتی که مشاهده یا دریافت می کنید، ذخیره و چاپ نمایید
- هر گونه مزاحمت سایبری را گزارش دهید، خواه در مورد خود شما انجام شده باشد یا خیر و آن را برای تیم یوتیوب پرچم گذاری کنید. آن کاربران را نیز مسدود کنید.

مزاحمت های جنسی سایبری

از جمله آثار مخاطب فضای سایبر، به وجود آمدن انحرافات جنسی و اختلالات جنسی است. اینترنت به دلیل رویکرد آزاد اندیشی در روابط جسنی از سوی گردانندگان اصلی آن (غرب و بویژه آمریکا) و نگرش تجاری نسبت به مسائل جنسی، موجب پدید آمدن پدیده شومی بنام «هرزه نگاری» و «هنر پلید شهوانی» و رواج سرسام آور آن گردیده و این پدیده مرزهای اخلاقی را در هم می شکند و تهدید برای فرهنگ ها، بخصوص فرهنگ های دینی همچون فرهنگ اسلامی است.

فریب کودکان و نوجوانان از طریق ارتباط رایانه ای

استفاده از اینترنت روشی جدید برای اغفال دختران و زنان توسط باندهای قاچاق طی سال های اخیر بوده است. دلالان و قاچاقچیان انسان ابتدا از طریق چت و دادن تصویر خود با استفاده از شیوه های خاص طرح دوستی با این دختران را ریخته و سپس با وعده ازدواج، کار خوب و در آمد بالا آنها را به کشور مورد نظر دعوت کرده و در آنجا به قاچاقچیان تحویل می دهند.

هرزه نگاری سایبری

از جمله آثار مخرب فضای سایبر، بوجود آمدن «انحرافات جنسی» و «اختلالات جنسی» است. اینترنت به دلیل رویکرد آزاد اندیشی در روابط جنسی از سوی گردانندگان اصلی آن (غرب و به ویژه آمریکا) و نگرش تجاری نسبت به مسائل جنسی، موجب پدید آمدندن پدیده شومی «هرزه نگاری» و «هنر پلید شهوانی» و رواج سرسام آور آن گردید. این پدیده مرزهای اخلاقی را در هم می شکند و تهدید برای فرهنگ ها بخصوص فرهنگ های دینی همچون فرهنگ اسلامی است. اصولاً، پورنوگرافی یا هرزه نگاری به عنوان نمایش تصویری و یا کلامی رفتارهای جنسی است که با هدف ارضای خواسته های جنسی دیگران تعریف می شود. این مطالب و تصاویر که در طی تحریک جنسی دیگران عرضه می گردد، معمولاً به ارضای غیرطبیعی جنسی مراجعه کنندگان آن می انجامد.

نکته دیگر اینکه رجوع به اینترنت برای دسترسی به مطالب مستهجن، صرفا به افراد نابه هنجار خلاصه نمی شود و حجم قابل توجهی از مراجعه کنندگان را افراد طبیعی تشکیل می دهند. در این عرصه بیشترین خطر متوجه کودکان و نوجوانان است. «لاسر» پس از پژوهشی که در این باره انجام داد، با اشاره به پیامده های منفی هرزه نگاری بر بهداشت روانی می گوید: «این مکان وجود دارد که به واسطه دیدن مطالب و تصویرهای مستهجن رفتارهای جنسی از خود بروز دهند». در مورد بزرگسالان نیز هرزه نگاری اینترنتی می تواند به بروز «رفتارهای جنسی نامعقول» و یا گاهی «اعتیاد جنسی» بیانجامد. اصولاً اینترنت به جوی دامن زده که در سایه ویژگی های خاص خود به تدریج به شکل گیری ناهنجاری های

جنسی در کاربران خود می انجامد.

➢ انتشار متون غیر اخلاقی

امروز به راحتی هرچه تمام می توان تصاویر مستجهن را بدست آورد. «بلوتوث» یا «اینترنت» هیچ فرقی ندارد. تنها فاصله برای دیدن آنها یک اراده ضعیف است. عکس هایی که در حالت های مختلف تهیه می شود و با رنگ و لعابی مجازی در اختیار نوجوانان و جوانان به عنوان بیشترین طیف استفاده کنندگان از اینترنت قرار می گیرد.

براساس بررسی های بعمل آمده، نظام سلطه در غرب، در پی «تشکیک و تخریب حوزه اخلاقیت و اعتقادات اسلامی» بوده و جایگزین آن نیز «سکولاریسم» و «لیبرالسیم» خواهد بود. همه فعالیت های غرب در اینترنت، در راستای فعالیت های باطل گرایانه و شیطانی است.

شاید باور کردنی نباشد ولی امروز سایت هایی جمهوری اسلامی ایران در حال فعالیت هستند که استفاده ابزاری از اعضای خود را پیشه خود قرار دادند. استفاده ای به قیمت حیثیت وجودی فرد که برای حفظ آن بسیاری از افراد از جان خود مایه می گذارند؛ ولی نقطه اینجاست چگونه مشتریان این سایت های غیراخلاقی راضی می شوند تا این حیثیت را به بهای بی آبرویی به حراج بگذارند و کار و کسبی را برای این سایت ها پررونق تر از قبل کنند؟

مهار کردن خواسته های نفسانی یکی از مهمترین عوامل این موضوع به حساب می آید. شاید در ابتدا افرادی برای گذر در صفحات اینترنت یا از سر کنجکاوی سری با این سایت ها بزنند اما با توجه به برنامه ای که در پشت پرده این سایت ها و طراحان آن وجود دارد بیشک نوجوانان و جوانان را به خود جلب می کنند به طوری که این افراد به عنوان مشتریان پروپا قرص این سایت ها درآمده و خود عضوی از آن می شوند!

➢ انتشار تصاویر غیراخلاقی

در فضای مجازی، مطالب شهوانی «تصاویر سکسی» به آسانی در دسترس همگان قرار می گیرد. عرضه گسترده این مطالب و وجود بیشمار «اتاق های گفتگو» سکسی، هر کاربری را به داشتن اولین تجربه در این حوزه تحریک می کند.

یک زن یا شوهر کنجکاو، به راحتی و دور از دیدگان همسر وارد این فضاها می شود و گفت و گوهای سکسی با دیگران را تجربه می کند. چنین سهولتی است که بسیاری را به تجربه رفتارهای ناهنجاری جنسی نه در فضای فیزیکی، بلکه در فضای مجازی هدایت می کند. به ویژه اگر نظارت نهادهای مسئوول در کشورها در این زمینه کم رنگ و ناتوان هم باشد. ناشناخته ماندن مراجعه کنندگان در عرصه اینترنت به نوعی اعتماد به نفس در افراد دامن می زند و این حالت نوعی رفتار غیر مسئولانه را در فرد شکل می دهد. مراجعه کنندگان در چنین شرایطی است که به خود اجازه می دهند تا در خلوت خود به فکر داشتن تجربه ی سکسی با مردان هم بیندیشند. در چنین فضایی است که فرد بدون هیچ گونه دردسری و به گونه ای ناشناخته می تواند با مفاهیمی چون سکس گروهی، هم جنس بازی و مبدل پوشی جنسی آشنا شود. ادامه دارد...

برگرفته از کتاب «کارکردهای پدافند غیرعامل در رویایی با تهدیدهای نرم و سخت، علیرضا غلامی، حبیب خدارحمی، انتشارات جهان جام جم، ۱۳۹۵، صص ۱۶۶-۱۵۷)

اوباما FBI را مسئول پاسخ به حملات سایبری کرد

گزارش سایبربان :دولت آمریکا با تصویب سیاست‌های جدیدی، چندین سازمان دولتی دیگر را وارد حوزه‌ی نظارت بر سیستم سایبری کشور کرد.

به گزارش واحد امنیت سایبربان؛ در روزهای گذشته، سیاست جدیدی در مورد امنیت سایبری و قوانین مقابله با حملات سایبری توسط کاخ سفید به تصویب رسید. طبق این سیاست جدید، دولت فدرال نقش پررنگ‌تری در بررسی و جلوگیری از هک شبکه‌های رایانه‌ای پیدا کرده است.

مشاوران کاخ سفید ادعا می‌کنند این اقدامات ضروری هستند، زیرا هرگز مشخص نیست عامل حملات کدام کشور یا کدام گروه تروریستی یا مجرم خواهد بود. لیزا موناکو(Lisa Monaco) ، مشاور ضد تروریست دولت اوباما دراین‌باره گفت: «این سیاست چهارچوبی شفاف برای هماهنگی پاسخ‌های دولت در رخدادهایی سایبری ایجاد می‌کند. این سیاست مشخص می‌کند کدام سازمان‌های فدرال مسئول پاسخ به چه نوع حملاتی هستند و در صورت بروز مشکل با کدام سازمان باید تماس گرفت».

این سیاست درحالی تصویب شد که این هفته، اطلاعات مهمی در مورد ۲۰ هزار ایمیل سرقت شده از وبگاه کمیته‌ی حزب دموکرات توسط وبگاه ویکی لیکس افشاء شد. آمریکا، هکرهای روسی را عامل این حمله و افشاء این اطلاعات می‌داند، گرچه روسیه چنین اتهاماتی را تکذیب می‌کند.

طبق این سیاست جدید، وزارت امنیت داخلی آمریکا با اتصال به بدنه‌ی اطلاعاتی این کشور، به کاهش تأثیرات حملات سایبری و جلوگیری از سرقت اطلاعات کمک خواهد کرد. همچنین پلیس فدرال آمریکا نیز از این پس مسئولیت پاسخگویی و واکنش به حملات سایبری را بر عهده خواهد داشت. البته دخالت چنین سازمانی در حوزه‌ی فناوری می‌تواند تأثیرات منفی زیادی برای جامعه‌ی آمریکا داشته باشد و فضای مجازی را برای مردم عادی نیز ناامن‌تر کند. این درحالی است که دولت اوباما با تصویب این سیاست، وجود ۱۰ لایه‌ی مخفی سایبری در آمریکا را در سال‌های گذشته افشاء کرد.

عناوین رویدادهای مهم خبری

«برای مشاهده متن کامل خبرها روی آنها کلیک کنید»

❖ سه شبکه اجتماعی ایرانی راه‌اندازی می‌شود	❖ نقشه جنگ با ایران که سعودی‌ها ترسیم می‌کنند
❖ ریزگردها هشداری که جدی گرفته نمی شود	❖ تاب مقابله عربستان در برابر ایران بیش از چند روز نخواهد بود

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 : ۳۳۳۳۶۲۰۹-۰۴۱