باسمه تعالی

دانشگاه فرهنگیان
پردیس آیت ا... خامنه ای کرکان

پدافند غیر عامل چیست؟

به اقدام غیر مسلحانه ای که موجب کاهش آسیب پذیری نیروی انسانی، ساختمان ها، تاسیسات، تجهیزات، اسناد و شریان های کشور در مقابل عملیات خصمانه و مخرب دشمن گردد، پدافند غیرعامل گفته می شود.
پدافند غیر عامل مجموعه اقداماتی است که انجام می شود تا در صورت بروز جنگ، خسارات احتمالی به حداقل میزان خود برسد که این اقدامات برای کاهش احتمال وقوع و به حداقل رساندن اثرات خسارت های اقدامات خصمانه بدون گرفتن ابتکار عمل ایجاد می شود.

*تعریف بکار رفته در اساسنامه سازمان پدافند غیرعامل

به مجموعه اقداماتی که بدون بکارگیری سلاح و تجهیزات نظامی بکار گرفته شود و در نتیجه باعث کاهش آسیب پذیری، افزایش پایداری ملی، تسهیل مدیریت بحران، تداوم کارکرد فعالیت های ضروری و تولید بازدارندگی دفاعی در برابر تهدیدات و اقدامات نظامی دشمن می گردد، اطلاق می شود.
پدافند غیر عامل به مجموعه اقداماتی اطلاق می گردد که مستلزم بکارگیری جنگ افزار نبوده و با اجرای آن می توان از وارد شدن خسارات مالی به تجهیزات و تاسیسات حیاتی و حساس نظامی و غیر نظامی و تلفات انسانی جلوگیری نموده و یا میزان این خسارات و تلفات را به حداقل ممکن کاهش داد.

پدافند غیر عامل در نظام سلامت

*مدیریت نظام سلامت باید بسیار آگاهانه جهت آمادگی و مقابله عمل نماید.
*بدیهی است حیاتی ترین منبع یک کشور منابع انسانی آن است و حفظ سلامت جسم و روح انسان های یک جامعه از مهمترین راهبردهای هر کشوری است.
*وزارت بهداشت، درمان و آمزش پزشکی به عنوان متولی اصلی سلامت کشور، وظیفه تدوین سیاست‌ها، راهکارها و دستوالعمل‌ها را برای پیشگیری، آمادگی و پاسخ به مشکلات سلامتی دارد.

اهداف عالی پدافند غیرعامل در دانشگاه:

- افزایش سطح مهارت و آگاهی با آموزش صحیح
- کاهش تلفات و خسارات
- ایجاد آمادگی برای انجام واکنشهای صحیح و سریع
- ارتقاء فرهنگ ایمنی و مقاوم سازی

نقش و اهمیت پدافند غیرعامل در طرح های دفاعی

پدافند غیرعامل به عنوان یکی از موثرترین و پایدارترین روش های دفاع در مقابل تهدیدات همواره مدنظر اکثر کشورها ی جهان قرار داشته است و حتی کشورهایی مانند آمریکا و شوروی سابق با وجود برخورداری از توان بالای نظامی به این موضوع به صورت ویزه ای توجه داشته اند. در کشور ما با وجود موقعیت خاص از

نظر ژئوپولوتیک ، دارا بودن ثروت های عظیم نفت و گاز، نظام ضد استکبار و ورود به عرصه های فناوری نوین و تهدیدات استکبار جهانی، موضوع پدافند غیرعامل به میزان کافی مورد توجه قرار گرفت و حتی گذر سال های دفاع مقدس نیز در ایجاد هوشیاری لازم برای کاهش آسیب پذیری ها و توجه به محورهای پایداری توسعه از نظر امنیت و دفاع، نقش قابل قبولی ایفا نمود.پدافند غیرعامل به سبب افزایش توان بازدارندگی، نقش ممتازی در کاهش احتمال آغاز درگیری های نظامی داشته و در صورت پیاده سازی صحیح، خواهد توانست آثار مخرب جنگ های پیش رو را تقلیل دهد. راهبرد پدافند غیرعامل فی ذاته از برخی قابلیت های کلیدی برخوردار است که می تواند ضامن توسعه امن محسوب گردند. اهم این قابلیت ها عبارتند از:

- **پدافند غیرعامل بستر مناسب توسعه پایدار کشور**
- **پدافند غیرعامل هم راستا با سیاست های تنش زدایی**
- **پدافند غیرعامل پایدارترین و ارزان ترین روش دفاع**
- **پدافند غیرعامل مناسب ترین راه کار افزایش آستانه مقاومت ملی**
- **پدافند غیرعامل پشتوانه اقتدار ملی**
- **پدافند غیرعامل یکی از مهم ترین ابزارهای بازدارندگی**
- **پدافند غیرعامل بهترین و مناسب ترین شیوه کاهش مخاطرات و کاهش آسیب پذیری**
- **پدافند غیرعامل صلح آمیزترین روش دفاع**
- **پدافند غیرعامل فطری ترین عنصر دفاعی بشر در برابر تمام حوادث است**

مولفه های امنیت ملی و دفاع غیرعامل

	تاثیرات اقدامات دفاع غیرعامل
حفظ جان مردم	**کاهش تلفات جمعیت نظامی و غیرنظامی کشور در برابر تهدیدات و حملات نظامی دشمن به عنوان با ارزش ترین سرمایه های یک کشور**
حفظ تمامیت ارضی	**تقویت توان رزمی نیروهای مسلح و بالابردن آستانه مقاومت کشور در حفظ سرزمین و ایجاد باز دارندگی**
حفظ سیستم اقتصادی و سیاسی	**کاهش آسیب پذیری و خسارات تجهیزات و نیروی انسانی مراکز حیاتی و حساس اقتصادی، سیاسی، تولیدی و... در جهت استقرار خدمات و عملیات**
حفظ استقلال و حاکمیت کشور	**حفظ مراکز عمده هدایت و رهبری سیاسی، نظامی، اجتماعی و زیر ساخت های حیاتی، حساس و مهم در برابر تهدیدات آشکار و نهان دشمنان از جمله عوامل اساسی در حفظ استقلال و حاکمیت کشور می باشد**

اصول پدافند غیرعامل

مجموعه اقدامات بنیادی و زیر بنایی است که در صورت بکارگیری می توان به اهداف پدافند غیرعامل از قبیل تقلیل خسارات و صدمات، کاهش قابلیت و توانایی سامانه های شناسایی اهداف، هدف یابی و دقت هدف گیری تسلیحات آفندی دشمن و تحمیل هزینه بیشتر به وی نائل گردید. اصول عمده پدافند غیرعامل عبارتند از:

***انتخاب عرصه های ایمن در جغرافیای کشور**
***تعیین مقیاس بهینه اسقرار جمعیت و فعالیت در فضا**
***پراکندگی در توزیع عملکردها متناسب با تهدیدات و جغرافیا**
***انتخاب مقیاس بهینه از پراکندگی و توجیه اقتصادی پروژه**
***کوچک سازی، ارزان سازی و ابتکار در پدافند غیرعامل**
***موازی سازی سامانه پشتیبانی وابسته**
***مقاوم سازی، استحکامات و ایمن سازی سازه های حیاتی**
***مکان یابی استقرار عملکردها**
***استتار و نامرئی سازی**
***کور کردن سیستم اطلاعاتی دشمن**
***اختفاء با استفاده از عوارض طبیعی**
***پوشش در همه زمینه ها**
***فریب، ابتکار عمل و تنوع در کلیه اقدامات**
***حفاظت اطلاعات سامانه های حیاتی و مهم**
***تولید سازه های دو منظوره(موانع(**

تهدیدات فناوری پایه

این تهدیدات، نوعی از تهدید می باشند که بر اساس رشد فناوری ها بوجود می آیند. به خاطر ذات فناورانه این گونه تهدیدات، نوع خاصی از تهدیدات به شمار می روند. با توجه به رابطه میان این تهدیدات و فناوری در دنیای امروز و به دلیل سرعت پیشرفت علم بشری، این تهدیدات نیز رشد و قدرتی قابل توجه یافته اند، به گونه ای که در دسته مجزا دسته بندی می گردند و عبارتند از:

***تهدید سایبری**
***تهدید زیستی**
***تهدید شیمیایی**
***تهدید پرتویی**
***تهدید الکترو مغناطیسی**

پدافند غیرعامل سایبری

بواسطه رشد علم و تکنولوژی و به تبع آن فناوری اطلاعات و ارتباطات و ایجاد فضای سایبری و نفوذ هرچه بیشتر آن در جوامع و ملت ها، مسائل مربوط به این حوزه از اهمیت بالایی برخوردار گردید. به گونه ای که مقابله با تهدیدات سایبری برابر است با حفاظت از هویت مادی و معنوی اطلاعات در حوزه های مختلف سیاسی، نظامی، اقتصادی و غیره که در چارچوب مرزهای فیزیکی نمی گنجد.

امروزه در تهدیدات فناوری اطلاعات از مفهومی به نام جنگ سایبری نامبرده می شود که در واقع جلوه ی خشن فناوری اطلاعات زیبارو می باشد. جلوه های فناوری اطلاعات خوش چهره، تمامی محصولات و حوزه های خدمات "الکترونیکی کشور از جمله، تلویزیون، اینترنت، رایانه، تلفن های ثابت و سیار و سایر محصولاتی از این دست را در بر گرفته و از سوی دیگر از جمله مصادیق چهره های خشن و زشت "IT" جنگ سایبری است که سرقت اطلاعات، اختلال در تولید و توزیع اطلاعات، توقف عملیات، تخریب و تحریف اطلاعات و .... از جمله تاثیرات مخرب آن می باشد و تعدادی دارای اثراتی حتی خطرناک تر از بمب اتم است.

با ساخت کارخانجات و تسلیحات جدید سایبری، زیر ساختهای کشورها از راه دور مورد حمله و انهدام قرار می گیرد و این موضوع دلالت بر نوع جدیدی از تهدید و تهاجم دارد .با فراگیری حوزه فناوری اطلاعات و تطبیق آن با دنیای واقعی، کلیه این تهدیدات به این حوزه نزدیک شده اند در عین حال آفند در این حوزه مستلزم هزینه چندانی نمی باشد و نیاز به حضور فیزیکی در محل جنگ ندارد. در حال حاضر مهمترین مراکز مالی دنیا از طریق اینترنت و در هر محلی از جهان قابل دسترس می باشد که باعث افزایش اهمیت پدافند غیرعامل دراین حوزه شده است.

برای تفهیم جنگ سایبری ابتدا باید فضای سایبری و عناصر آن را درک نمود سایبر (Cyber)پیشوندی برای اسامی متعدد و متنوعی است که همگی بر اساس انتشار روزافزون رایانه پدید آمده اند. اغلب عناصر درگیر با اینترنت نیز با این پیشوند قابل تشریح می باشند. اولین اصطلاح در این وادی Cyber Spaceمی باشد یا همان فضای سایبری است که استعاره ای برای تشریح سرزمین غیر فیزیکی تشکیل شده توسط سیستم های کامپیوتری می باشد.

شناخت محیط فضای سایبر و حوزه آسیب پذیر کشور، اولین نکته از پدافند سایبری است. پس از شناخت، پژوهش، طراحی و برنامه ریزی برای هر حوزه خاص، قدم بعدی است. فضای سایبر به شدت مبتنی بر علم و فناوری و دانش بنیان است.

فرماندهان و مدیران این عرصه نیز به همان شدت باید متخصص و مسلح به دانش این فن باشند. دانش این

فضا ترکیبی از علوم مختلف مانند رایانه، الکترونیک، ارتباطات، روانشناسی، جامعه شناسی و حقوق است همچنین فاکتورهای مهم در این مقوله نیز شامل موارد زیر می شود:

۱ -کاربران و نیروی انسانی

پدافند این حوزه را باید به دو بخش تقسیم نمود:

بخش نخست کاربرانی هستند که در فضای سایبر با اطلاعات سروکاردارند تعریف سطح دسترسی افراد به اطلاعات و آموزش تخصصی نیروی انسانی دو گام اساسی این حوزه است.

در تعریف سطح دسترسی یک قانون کارآمد می گوید: " هرکس تنها اطلاعاتی در اختیار داشته باشد که برای پیشبرد کار تعریف شده سازمانی خود، بدان احتیاج دارد و نه بیشتر". نفوذ دشمن از حفره خلاء علمی کاربران می تواند با آموزش مستمر و بروز رسانی این آموزشها مسدود گردد. تایید صلاحیت و شناخت سابقه به همراه نظارت پیگیر می تواند به میزان چشمگیری آسیب پذیری این حوزه را کاهش دهد.

بخش دوم که بخش روانی این حوزه است، در واقع شامل افرادی است که مخاطب فضای مجازی هستند و همیشه تحت تاثیرسناریوهای متخصص روانشناسی و جامعه شناسی دشمن در بستر فضای سایبر قرار دارند.

۲-داده ها و اطلاعات:

طبقه بندی ارزش اطلاعاتی راه گشا و حتی کاهش دهنده هزینه پدافند در این حوزه است. برای صیانت از داده های اطلاعاتی باید به میزان حساسیت و منافعی که آن اطلاعات فراهم می کند، هزینه نگهداری پرداخت نمود و تلاش امنیتی انجام داد. اینکه چه نوع اطلاعاتی و بر روی چه مکانی از فضای سایبر قرار گیرد. و یا کدام پایگاه دانش روی کدام سرور فعالیت نماید.

۳ -پدافند غیر عامل در حوزه سایبری

از آنجا که هیچ گاه نمی توان امنیت را صد در صد برقرار نمود. لذا حتی با رعایت نمودن کلیه موارد ذکر شده، امکان بروز حوادث غیر مترقبه و تهدیدات پیش بینی نشده وجود دارد لذا در اینجا اهمیت پدافند غیرعامل محرز می باشد . دفاع غیرعامل در واقع مجموعه تهدیدات، اقدامات و طرح هایی است که با استفاده از ابراز، شرایط و حتی المقدور بدون نیاز به نیروی انسانی به صورت خود اتکا صورت گیرد چنین اقداماتی از یک سو توان دفاعی مجموعه را در زمان بحران افزایش داده و از سوی دیگر پیامدهای بحران را کاهش و امکان بازسازی مناطق آسیب دیده را با کمترین هزینه فراهم آورد.

ریسک های اصلی مرتبط با تکنولوژی اطلاعات

امروزه امنیت اطلاعات مقوله ای مشترک در زمینه های مختلف بشمار می رود بطور مثال در زمینه های سیستم های ارتباطی و کامپیوتری، مالی و بانکی و سیستم های تحصیلی و سلامت بزرگترین تاثیر تکنولوژی اطلاعات در جامعه امروزه ، اینترنت می باشد به همین دلیل سازمان جهانی تیم پاسخگویی اورژانس کامپیوتری را بنا نهاده است. که در رومانی تحت عنوان CERT-RO و در اروپا به ENISAشناخته می شود. مطابق گزارش منتشر شده توسط CERT-ROدر سال ۲۰۱۳، ۱۲/۵

درصد از IPهای کشور رومانی توسط ویروس های مختلف مورد حمله قرار گرفتند. امروزه تکنولوژی با تغییرات از مرحله آسیب پذیری تا مرحله اقدام پیش می رود.
تخمین نقطه ضعف، مانیتورینگ و مداخله بسیار مهم است بطور مثال کمیسیون اروپا به این نتیجه رسید که یک محیط تکنولوژیک را بنام " دامین ابری " ایجاد کندکه از این طریق ضعف های بالفعل اطلاعاتی تکنولوژیک را پیدا نماید.
بطور کلی می توان ۱۰ حوزه حاوی ریسک را مشخص نمود که در صورت بی توجهی به آن منجر به ریسک های اساسی خطرناک می شوند:

***شبکه اجتماعی در صورتی که به اطلاعات محرنامه بدون دسترسی مجاز دسترسی داشته باشد.**
***استفاده از دستگاههای موبایل بدون توجهبه مدیریت مباحث امنیتی و شناسایی**
***عدم توجه به IT) (ها که منجر به از دست رفتن اطلاعات حیاتی می شود**
***دسترسی کاربران نهایی به اطلاعات و تخریب و دستکاری آنها**
***جاسوسی از شخصیت های حقوقی**
***پروژه های ناتمام و شکست خورده**

مقوله امنیت اطلاعات دارای ابعاد گسترده ای است که برنامه های کاربردی و نرم افزاری، لایه های سخت افزاری و سیاست ها و روال های امنیتی را شامل می شود چه بسا قوانین امنیتی که در سازمان وضع می شود به اندازه تهیه و تامین سخت افزارهای با قابلیت بالا حائز اهمیت است. وجود نقص در هریک از لایه های اشاره شده امنیت یک سازمان را با خطر مواجه می نماید همچنین وجود خلاهای فرهنگی و پیچیدگی های آن نیز یکی دیگر از عوامل تاثیرگذار در اجرای مناسب سیاستهای امنیتی بشمار می آیدکه سازمانها می توانند به کمک آموزش مستمر و بررسی نمونه های مشابه رخ داده شده نسبت به افزایش سطح آگاهی مدیران سازمانی اقدام نمایند. از جمله کمبودهای دیگری که بطور محسوس مشاهده می شود وجود مرکزی پویا در سازمانهاست که در خصوص سیاست گذاری و نظارت مقوله های امنیتی و مدیریت حوادثی از این دست برنامه ریزی و اقدام لازم انجام دهد .

پدافند شیمیایی چیست؟

به طیفی از اقدامات گفته می شود که بتواند پیامدهای ناشی از هرگونه نشت شیمیایی را مدیریت، کنترل، کاهش و با آن مقابله کند. این منشاء می تواند نشت شیمیایی یا صنعتی یا تروریستی باشد. از جهت دیگر پدافند شیمیایی دارای رویکرد دومی نیز می باشد که مصون سازی و کاهش آسیب پذیری های ناشی از تاسیسات شیمیایی می باشد که این رویکرد فنی، مهندسی و شیمیایی خواهد بود و یا به تعبیر دیگر می توان گفت حفاظت و مصون سازی زیر ساخت های شیمیایی . پدافند شیمیایی مجموعه ای از تدابیر، برنامه ها و اقدامات غیرنظامی است که به کاهش امکان وقوع تهدیدات یا حوادث شیمیایی و کاهش آسیب پذیری افراد، زیر ساخت ها و سرمایه ها در برابر تهدیدات شیمیایی منجر و آمادگی مواجهه و واکنش در برابر وقوع تهدیدات شیمیایی را در جامعه بالامی برد.

تروریست ها از جمله داعشی ها و منافقین از ابزار شیمیایی برای اهداف تروریستی خود استفاده می کنند که اصطلاحا به آن کموتروریسم گفته می شود. مثلا متروی بارسلونا، متروی مسگو و اتفاقات مشابه که تروریست ها برای آسیب زدن به مردم از مواد شیمیایی استفاده کرده اند و یا حتی در حوادث سوریه هم شاهد این موضوع بوده ایم.

عناصر شیمیایی به چند دسته تقسیم می شوند:

عناصر خطرناک (در فرایندهای صنعتی از این ترکیبات استفاده می شود و اگر ملاحظات ایمنی یا امنیتی رعایت نشود می توانند خطرناک باشند(
عناصر با خطر متوسط(استفاده از گاز برای پختن غذا یا استفاده در تاسیسات حرارتی و برودتی یا استفاده از گاز کلر در تصفیه خانه های آب(
عناصر بی خطر(گوشی موبایل(

در حوادث شیمیایی خسارت وارده به زیر ساخت های صنعتی از نظر اقتصادی قابل جبران است اما آسیب به مردم قابل جبران نیست.

از منظر پدافند شیمیایی، بسترهای وقوع تهدیدات شیمیایی، به جنگ محدود نشده و هر حوزه ای که در آن حجمی از مواد شیمیایی پرخطر وجود داشته باشد، بسته به شرایط و وضعیتی که در آن قرار گرفته یا از آن اثر می پذیرد می تواند بستر ساز وقوع تهدیدات شیمیایی باشد.

یکی از مهمترین این حوزه ها، حوزه ی "صنعت" است. صنایع مرتبط با مواد شیمیایی پرخطر، بسیار متنوع هستند. برای مثال صنایع نفت و پتروشیمی، صنایع

غذایی و دارویی و کشاورزی که حجم وسیعی از مواد شیمیایی پرخطر را نگهداری یا استفاده می کنند. بنابراین هر صنعتی که در فرایند فعالیت خود با حجمی از مواد شیمیایی پرخطر به عنوان ماده ی اولیه، محصول یا پسماند سروکار داشته باشد بصورت بالقوه بستری برای وقوع تهدیدات شیمیایی به شمار می آید. مخازن حاوی مواد شیمیایی پرخطر در برخی از کارخانه های صنعتی و تانکرهای حامل مواد شیمیایی سمی، آتشگیر یا منفجره، در صورت تحریک منجر به نشت یا فشار و دمای بالا می توانند عامل رفع تهدید و آسیب شوند. متاسفانه در بسیاری از این حوادث افراد زیادی آسیب دیده و بخشی از سرمایه های ملی نابود می گردد.
از منظر پدافند شیمیایی، خرابکاری صنعتی به معنای ایجاد اخلال و اختلال در فرایند و فعالیت صنایع شیمیایی پرخطر است که به نشت مواد شیمیایی سمی یا انفجار و آتش سوزی منجر به آسیب، بیانجامد.

در بررسی تهدیدات شیمیایی حوزه صنعت علاوه بر فرایند تولید، انبار، حمل و نقل و توزیع ، باید به حوزه ی مصرف مواد شیمیایی نیز در سطح جامعه توجه نمود.

حادثه شیمیایی چیست؟

نشت یا خارج شدن ناخواسته و ناگهانی و کنترل نشده ماده شیمیایی در حجم بسیار زیاد است که از طریق آتش، انفجار، نشت یا خروج مواد سمی می تواند سبب:

*بیماری
*صدمه و جراحت
*از کارافتادگی
*مرگ

نیروهای واکنش سریع آموزش دیده در حوادث شیمیایی باید اقدامات زیر را انجام دهند(بر حسب اولویت:(

- افراد را نجات دهند
- آتش یا خروج مواد شیمیایی را مهار کنند
- از افزایش حادثه دیدگان جلوگیری کنند
- رفع آلودگی را شروع کنند و راههای حیاتی را باز نگهدارند
- از خرابی مجدد جلوگیری کنند
- برنامه ریزی برای آمادگی در برابر حوادث شیمیایی
- الف) موارد عمومی

۱-یکی از اهداف برنامه ریزی اضطراری، پیشگیری و کاهش اثرات نامطلوب بر روی سلامت انسان در حادثه شیمیایی است.
۲-مسئولین در بخش ملی و منطقه ای و محلی باید دارای مسئولیت یکسان جهت حفظ سلامت انسانها را در نظر داشته باشند.

بخش های درگیر شامل:

*وزارت بهداشت
*مسئولین منطقه ای و محلی
*کارشناسان بهداشت
*بیمارستانها و یا سایر مراکز دارای تجهیزات، امکانات درمانی
*کارشناسان بهداشت حرفه ای و ایمنی در بخش دولتی و مستقر در کارخانجات
*مراکز اطلاع رسانی
*تجهیزات داروئی
*منابع اعم از انسانی، تجهیزاتی، اعتبارات در یک برنامه حادثه شیمیایی باید مشخص بوده و مسئولیت آن در برنامه فوریت نیز باید تعیین گردد.

معالجه حادثه دیدگان

۱-در حوادث شیمیایی ۴ راه اصلی برای مواجهه وجود دارد:
تنفسی
چشم
پوست
خوراکی

۲-معالجه برای افرادی که با مواد شیمیایی مواجهه داشته اند باید بصورت طبیعی پیگیریهای لازم مطابق مقرارت مدیریت وضعیت های اضطراری انجام گیرد.

۳-کلیه حادثه دیدگان در وضعیت بسیار خوب باید به بیمارستان یا سایر مراکز درمانی هدایت شوند.
*برای انتقال این حادثه دیدگان به مراکز درمانی باید کوتاهترین فاصله را در نظر گرفت.
*علاوه بر کمک های اولیه ممکن است سایر اقدامات درمانی در منطقه حادثه دیدگان باید ارائه گردد.

۴-درمان مسمومیت حاد بستگی به چهار اصل باتوجه به درجه آلودگی دارد:
*پاک نمودن عامل سمی برای پیشگیری از سایر صدماتی که از طریق جذب در بدن بوجود خواهد آمد.
*درمان از طریق نشانه شناسی و مددکاری
*درمان توسط آنتی دوت
*رفع آلودگی

۵-تصمیم گیری بر روی افراد حادثه دیده جهت رفع آلودگی بستگی به نوع و شدت صدمات و آلودگی های شیمیایی دارد.
*قبل از اعزام حادثه دیده به بیمارستان یا سایر مراکز درمانی باید از او رفع آلودگی نمود. در غیر اینصورت موجب خواهد شد که تجهیزات درمانی غیر قابل استفاده شود.
*ایستگاههای رفع آلودگی باید در هر بیمارستان یا مراکز درمانی وجود داشته و گنجایش پذیرش تهداد زیادی از حادثه دیدگان را داشته باشد.

*درمان مسمومیت حاد بستگی به چهار اصل با توجه به درجه آلودگی دارد:

-تریاژ یک فرآیند است که در منطقه حادثه، در زمان حمل و در تجهیزات درمانی اتفاق می افتد.
تریاژ بستگی به ارزیابی و طبقه بندی وضعیت مواجهه افراد و تعیین اولویت رفع آلودگی درمان و حمل آنان به مراکز درمانی، مواجهه در تریاژ، مصدومین را به گروههای مختلف تقسیم می شوند:

برای مثال از نظر ضایعات پوستی:

گروه ۱(ضایعه زندگی پرخطر) صدمات پوستی که ۵۰ درصد سطح بدن را فرا گرفته
گروه ۲(ضایعه شدید) صدمات پوستی که ۲۰ تا ۵۰ درصد سطح بدن را فراگرفته
گروه ۳(ضایعه متوسط) صدمات پوستی که ۱۰ تا ۲۰ درصد سطح بدن را فرا گرفته
گروه ۴(ضایه ملایم) صدمات پوستی که کمتر از ۱۰ درصد سطح بدن را فراگرفته یا صدمه پوستی
مواجهه با گازهای حساسیت زا به گروههای زیر تقسیم می شوند:
گروه۱ (ضایعه زندگی پرخطر) افراد صدمه دیده ای که علائمی مانند سرفه، نارسائی تنفسی و اثرات سیستماتیک
گروه ۲(ضایعه شدید) افراد صدمه دیده با حساسیت شدید که سبب سرفه، مشکلات اما بدون اثرات سیستماتیک
گروه ۳ (ضایعه ملایم) افراد مصدوم با حساسیت خفیف و متوسط سرفه علائم و نشانه های حساسیت چشمی و احتمال سردرد

پیشگیری از مسمویت ها در کودکان:

مسمومیت در کودکان ونوجوانان از اورژانسهای نسبتاً شایع واکثراً قابل پیشگیری می باشد.کودکان نوپا به دلیل کنجکاوی ممکن است هر آنچه در اطراف خود پیدا می کنند به دهان ببرند و بچشند. این موضوع آنها را در معرض خطر انواع مسمومیت ها قرار می دهد .نوجوانان به قصد خودکشی و سوء مصرف مواد هم در معرض مسمومیتهای خطرناک می باشند.دراین سن به نوجوانان توجه بیشتر داشته باشید.

متاسفانه شایعترین مسمومیتها در کودکان منجر به بستری در بیمارستان لقمان حکیم و همچنین مسمومیتهای منجر به فوت در کودکان مسمومیت مواد مخدر مخصوصاً شربت متادون میباشد.

اکثر مسومیتها در منزل اتفاق می افتد .داروها ومواد شیمیایی اضافی و بی مصرف را دور ریخته و در منزل انبار نکنید بیشترین مسمومیتهای کودکان از همان مواد خطرناک موجود در منزل است، به عبارت دیگر خانه را تبدیل به انبار سم و دارو نکنید. همچنین مواظب داروهای مصرفی مادربزرگ و پدر بزرگها و سایر افراد خانه هم باشید.

هرگز کودکان خود را به افراد ناشناس،همسایه، معتاد یا دارای بیماریهای اعصاب و روان نسپارید.
مواد خطرناک درکابینتهای دارای قفل نگهداری شوند. حشره کشها در دسترس کودکان نباشد.مواد سمی و خطرناک مانند الکلها، شربت متادون، نفت ،ضد یخ و... در شیشه مواد نوشیدنی و خوراکی مانند شیشه آب معدنی ریخته نشود.

در صورت خوردن ترکیبات هیدروکربنی خطرناک مثل نفت،بنزین،تینر به هیچ عنوان کودک را وادار به استفراغ نکنید و از خوراندن شیر یا آبلیموبه کودک جداً اجتناب گردد.

مواد مخدرازخانواده تریاک از جمله تریاک،مورفین،هروئین،متادون،بوبپرنورفین(با اسم خیابانیB۲)،ترامادول،دیفنوکسیلات و ... همگی از ترکیبات بسیار خطرناک و کشنده کودکان محسوب میشود حتی با مقادیر بسیار کم ،لذا ازدسترس کودکان اکیداً دور باشد و مصرف هر میزان حتی در حد مالیدن به لب و دهان یا مصرف کمتر از یک جرعه متادون میتواند باعث عوارض جبران ناپذیر وحتی مرگ شود.

یکی از مسمومیتهای جدی و خطر ناک که در سالهای اخیر متآسفانه منجر به چندین مورد مرگ کودکان در کشورمان شده است شربت متادون است که برای

ترک اعتیاد استفاده میشود و ظاهری شبیه آب داشته و کودکان به عوارض خطرناک آن حساسترند و با مقادیر بسیار کم حتی در حد یک سی سی میتواند باعث قطع تنفس نرسیدن اکسیژن به مغز و حتی مرگ شود و با مصرف هر مقدار شربت متادون کودک باید سریعاً مراجعه به پزشک داشته باشد. از ریختن شربت متادون در شیشه مواد آشامیدنی و دارویی دیگرعلی الخصوص آب معدنی جداً اجتناب گردد، چرا که مواد متعددی از مسمومیت با شربت متادون در کودکان به علت مصرف اشتباهی متادون بجای آب بوده است.

از جمله مواد بسیار خطرناک وکشنده دیگر در کودکان مواد سوزاننده اسیدی یا قلیایی است که در خانه ها بیشتر به صورت ترکیبات شوینده قوی مثل گاز پاک کن و یا لوله بازکن،جرم گیر، لکه بر، جوهر نمک،سفیدکننده ها و ...در دسترس است و مصرف کم در حد یک جرعه این ترکیبات نیز میتواندباعث سوختگی وزخم دستگاه گوارش و عوارض تآخیری دردناک وحتی مرگ گردد.

مواد شیمیایی دور از مواد غذایی و در کابینتهای بالایی که از دسترسی نوپایان بدوراست ودارای قفل هستند نگهداشته شوند.
ترکیبات و داروهای گیاهی تهیه شده از عطاری ها مواد بی عارضه و بی خطر نیستند و ممکن است حاوی مواد خطرناک برای کودکان باشد و باید دور از دسترس کودکان باشد.
در صورت بروز مسمومیت قبل از هر اقدامی جهت راهکارمناسب با شماره تلفن۱۱۵ تماس حاصل فرمایید.
هرگز کارهای خطر ناک (مثلاً کشیدن بنزین از باک، خوردن دارو، ...) را مقابل کودکان انجام ندهید، آنها از شما تقلید کرده یا کار شما رابعنوان بازی تلقی کرده و در صورت انجام میتواند باعث آسیب به آنها گردد.

قبل از شروع استفاده از مواد گرمایشی از عملکرد صحیح آنها اطمینان حاصل فرمایید و دودکشهارا کنترل نمایید و در فصول سرد حتماً منافذی برای جریان هوا در محل خواب تعبیه نمایید تا از مسمومیت با گاز سمی منواکسید کربن پیشگیری شود . سردرد،تهوع ،استفراغ و حالت گیجی از علایم اولیه این مسمومیت هستند.در صورت شک به این مسمومیت اولین کار باز کردن در وپنجره ها یا دور کردن فرد مسموم از آن محیط است.

مصرف هر مقدار موادمخدر، مواد محرک(مانند شیشه)، مواد روانگردن، مشروب و... در کودکان خطرناک بوده و باید سریعاً مراجعه به پزشک داشته باشد.این مواد از جمله تریاک و شیشه حتی در صورت استنشاق دود آنها توسط کودک میتواند منجر به مسمومیت شود.

از دانه های گیاهان بعنوان تنقلات استفاده نگردد،ازجمله دانه گیاه کرچک که علی رغم اینکه بسیار سمیست ولی مزه تلخ یا نامطبوع ندارد.
برای درمان بیماری کودک خود به پزشک مراجعه نمایید،از استفاده موادت جویز شده توسط عطاری اجتناب نمایید،بعنوان مثال اخیراً مواردی از مسمومیتهای

خطرناک ناشی از مالیدن سم خطرناک ارگانوفسفات داده شده توسط عطاری به سر جهت رفع شپش سر درکودکان شاهد بودیم.

۱۰ گام برای امن سازی گوشی هوشمند

محبوبیت گوشی های هوشمند روبه افزایش است و هم اکنون آنها همانند بسیاری از کامپیوترها قدرتمند و کاربردی هستند با توجه به رشد تهدیدهایی امنیت سایبری تلفن همراه محافظت از گوشی هوشمندتان دقیقا همانند محافظت از کامپیوترتان حائز اهمیت است.این نکات امنیتی تلفن همراه می تواند به شما در کاهش ریسک قرارگیری در معرض تهدیدهایی امنیت گوشی همراه، کمک کند.

استفاده از پین کدها و کلمات عبور

برای جلوگیری از دسترسی غیر مجاز به گوشی هوشمندتان به عنوان خط اول دفاعی در صورت گم شدن یا به سرقت رفتن گوشیتان یک کلمه عبور یا آدرس شناسایی شخصی (Pin) به روی صفحه اصلی تلفن خود قرار دهید در صورت امکان عبور متفاوت برای هر یک از دسترسی های مهم ؛ ایمیل، بانکداری الکترونیک، سایت های شخصی و غیره) استفاده کنید شما باید گوشی خود را به گونه ای تنظیم کنید تا به صورت خودکار پس از ۵ دقیقه یا کمتر از آخرین استفاده قفل شود همچنین از قابلیت قفل گذاری بر روی سیم کارت نیز بهره مند شوید.

تنظیمات امیتی گوشی هوشمندتان را تغییر ندهید

برای آسودگی خاطر تنظیمات امنیتی را تغییر ندهید. مداخله در تنظیمات پیش فرض گوشی همراهتان جیل درک کردن یا رت کردن گوشی ویژگی های امنیتی پایه ای تلفن همراه ارائه شده توسط سرویس وایرلس و گوشی هوشمند را تخریب می کند، در حالیکه آن را بیشتر در معرض یک حمله قرار می دهد.

تهدید نسخه پشتیبان و امن سازی داده ها

شما باید از تمامی داده های ذخیره شده بر روی گوشیتان مانند مخاطبین، اسناد و عکس ها نسخه پشتیبان تهیه کنید. این فایل ها می توانند بر روی یک کامپیوتر، یک کارت حافظه قابل حمل یا در حافظه ابری ذخیره سازی شود. این امر به شما قابلیت بازیابی آسان اطلاعات را در صورت گم شدن، دزدیده شدن یا هر شکلی پاک شدن اطلاعات از گوشی همراهتان را می دهد.

از منابع مورد اطمینان جهت نصب اپلیکشن استفاده کنید

قبل از بارگذاری یک اپلیکشن برای اطمینان از قانونی بودن آن تحقیق کنید بررسی قانونی یک اپلیکیشن

می تواند؛ شامل بررسی نظرات، تایید قانونی بودن فروشگاه اپلیکیشن و مقایسه وب سایت رسمی اسپانسرهای اپلیکیشن با لینک ارائه شده در فروشگاه اپلیکیشن برای تایید منبع، بسیاری از اپلیکیشن هایی دریافت شده از منابع نامعتبر می تواند شامل ملورهایی باشند که پس از نصب قابلیت سرقت اطلاعات، نصب ویروس ها و آسیب رسانی بر محتویات تلفن همراه شما شوند. هم چنین اپلیکیشن هایی موجود است که می تواند در صورت وجود، هر ریسک امنیتی بر روی تلفن همراهتان به شما اخطار دهند.

قبل از قبول کردن مجوزهای اپلیکیشن از محتوای آنها آگاه شوید

شما باید درباره صدور مجوز دسترسی اپلیکیشن ها به اطلاعات شخصی موجود یا اجرا عملیات ها بر روی گوشیتان هوشیار باشید همچنین از بررسی تنظیمات حریم خصوصی برای هر اپلیکیشن قبل از نصب آن اطمینان حاصل کنید.

نصب اپلیکیشن های امنیتی با قابلیت موقعیت یابی و از بین بردن اطلاعات از راه دور

یک ویژگی امنیتی مهم که به گستردگی در گوشی های هوشمند در دسترس است، به صورت پیش فرض یا یک اپلیکیشن قابلیت موقعیت یابی و پاک کردن همه داده های ذخیره شده روی گوشی شما از راه دور است، حتی در صورت خاموش بودن GPSگوشی همراه

به روز رسانی ها و پتنچ های مربوط به نرم افزار گوشی هوشمندتان را بپذیرید

بهتر است نرم افزار سیستم عامل گوشی خود را توسط فعال سازی به روز رسانی خودکار یا پذیرفتن به روز رسانی زمانی که توسط ارائه دهنده خدمات شما، ارائه دهنده سیستم عامل، تولید کنندگان دستگاه یا ارائه دهنده نرم افزار فعال سازی شده به روز نگاه دارید. با به روز نگاه داری سیستم عامل خود شما ریسک قرار گیری در معرض تهدیدات سایبری را کاهش می دهید.

در استفاده از وای فای های عمومی هوشمند عمل کنید

زمانی که شما به یک شبکه وای فای که استفاده از آن برای عموم آزاد است متصل می شوید، تلفن همراه شما می تواند یک هدف آسان برای مجرمان سایبری باشد. شما باید استفاده خود را از hot spotعمومی محدود کنید و به جای آن از وای فای های محافظت شده از یک اپراتور شبکه قابل اعتماد یا از ارتباط بی سیم موبایل جهت کاهش در معرض خطر قرار گرفتن استفاده کنید. به خصوص زمانی که قصد دسترسی به اطلاعات شخصی یا اطلاعات حساس را دارید. همیشه در زمان باز کردن لینک های وب و به خصوص زمانی که از شما درخواست ورود به حساب کاربری یا اطلاعات ورود به حساب کاربری می شود محتاط و هوشیار باشید.

داده های تلفن همراه خود را قبل از اهدا، فروش، یا بازیافت پاک کنید

در گوشی هوشمند شما، اطلاعات شخصی ذخیره شده است که شما می خواهید آنها را پس از دور انداختن گوشی خود محرمانه حفظ کنید. برای حفاظت از حریم شخصی خود داده های گوشی خود را کاملا پاک کرده و گوشی را به تنظیمات پیش فرض کارخانه بازگردانی کنید. سپس گوشی خود را اهدا، فروش، بازیافت یا آن را به درستی از بین ببرید.

سرقت گوشی هوشمند را گزارش دهید

ارائه کنندگان بزرگ خدمات وایرلس در همکاری با سازمان FFC، یک پایگاه داده گوشی های سرقت شده را ارائه کرده اند. اگر گوشی شما به سرقت رفته است شما باید سرقت گوشی خود را به مراجع قانونی محلی خود اطلاع دهید و سپس گوشی به سرقت رفته را در ارائه کننده خدمات وایرلس خود ثبت نمایید. طی این عمل یک اطلاعیه به تمامی ارائه کنندگان بزرگ خدمات وایرلس ارسال خواهد شد و قابلیت محصور سازی گوشی را از راه دور فعال کرده تا هیچ کس قابلیت فعال سازی آن را در هیچ شبکه بی سیم بدون اجازه شما را نداشته باشد.

امور فرهنگی ستاد نکوداشت هفته پدافند غیرعامل
پردیس آیت ا... خامنه ای گرگان- آبان ۱۴۰۰