به همراه آوردن تجهیزات شخصی (به آتش)

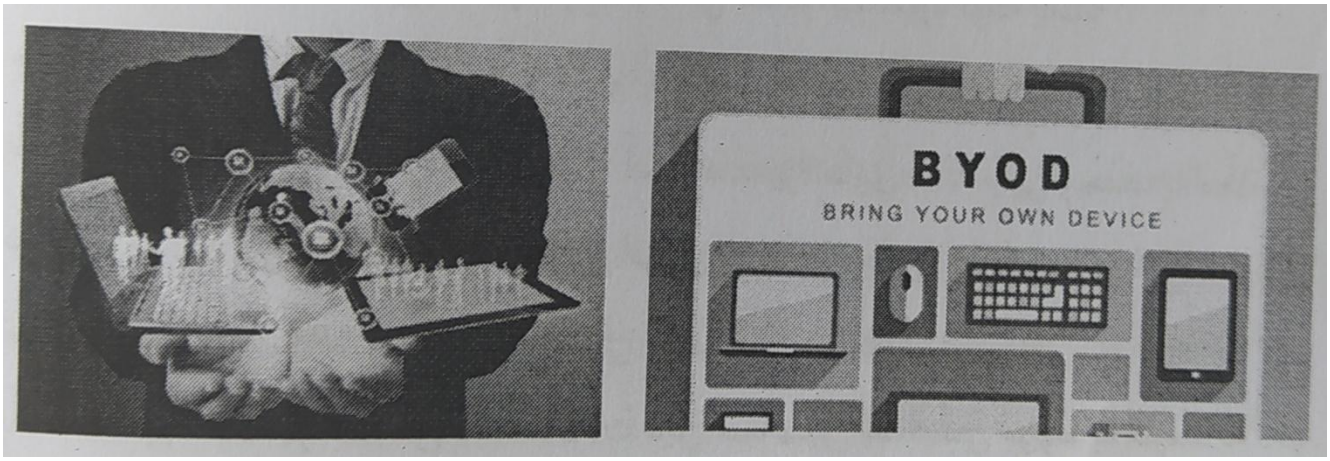
اداره کل پدافند غیرعامل استان قم

بهار ۱۴۰۲

به همراه آوردن تجهیزات شخصی (به آتش)

"به همراه آوردن تجهیزات شخصی" که به طور خلاصه می‌توان آن را **"به آتش"** نامید یا معادل انگلیسی آن را BYOD[1] در متون فنی تعاریف دیگری نیز نظیر فناوری خود را بیاورید، تلفن خود را بیاورید و کامپیوتر شخصی خود را بیاورید دارد، به سیاست‌هایی اطلاق می‌گردد که به کارکنان سازمان‌ها یا شرکت‌ها اجازه به همراه آوردن تبلت‌ها، گوشی‌های هوشمند، لب‌تاپ‌ها یا پوشیدنی‌های هوشمند به محل کار را می‌دهد یا به آن‌ها این اجازه را می‌دهد که به اطلاعات یا برنامه‌های کاربردی در سازمان دسترسی داشته باشند، شکل (۱).

تجربه و مطالعات جهانی نشان داده است عموماً سیاست منع به کارگیری تجهیزات شخصی کاربران نمی‌تواند مانع استفاده ایشان از این تجهیزات در محل کار شود. برای نمونه نزدیک به ۹۵ درصد از کارکنان سازمانی حداقل یک‌بار تجهیزات شخصی خود را در محل کار مورد استفاده قرار داده‌اند. مسأله بغرنج‌تر ظهور اینترنت اشیا (IOT) و سخت شدن کنترل تجهیزات یا اشیایی هستند که می‌خواهند در یک سازمان به خدمات یا اطلاعات دسترسی داشته باشند.



شکل (۱): تجهیزات شخصی کاربران

[1] Bring your own device (BYOD)

این روزها کاربران، بسیاری از کارهای مربوط به پیام‌رسانی، چندرسانه‌ای، مسیریابی، شبکه‌های اجتماعی، خرید الکترونیکی، بانکداری، فعالیت‌های کسب و کار، کارهای سازمانی، دبیرخانه الکترونیکی و غیره را با تکیه بر تجهیزات شخصی خود انجام می‌دهند. پیشرفت تجهیزات همراه و افزایش وابستگی کاربران به آن‌ها به مهاجمان این امکان را می‌دهد تا با سوءاستفاده از این فناوری‌ها به راحتی بتوانند در زمینه‌های مختلف مانند نقض حریم خصوصی، فریب و کلاهبرداری، سرقت و انتشار اطلاعات، مسائل ضدفرهنگی، حملات سایبری و غیره فعالیت کنند. بنابراین با به خطر افتادن امنیت این تجهیزات به معنای به خطر افتادن امنیت اطلاعات شخص، شرکت، سازمان یا حتی کشور است. از این رو کاربران مختلفی که تجهیزات شخصی را در محل کار و سازمان مورد استفاده قرار می‌دهند و حتی به شبکه سازمانی متصل میشوند باید علاوه بر حفاظت از اطلاعات شخصی، مهم و حساس‌شان با حفاظت از دارایی‌های سازمان نیز آشنا شوند. بنابراین به نظر می‌رسد سیاست‌گذاری صحیح، آموزش کافی، مسئولیت‌پذیری، پایش دقیق بهترین راه دفاع سایبری و حفاظت از داده‌ها، اطلاعات و سرمایه‌های سازمان است.

در این بخش به طور وسیع به آسیب‌پذیری‌های "به آتش" نخواهیم پرداخت، زیرا تعدد تجهیزات همراه افراد و نیز تجهیزات یا شبکه‌های سازمانی به تعداد زیاد آسیب‌پذیری دارند و در بخش‌های مختلف این کتاب به بعضی از آن‌ها پرداخته شده است ولی در زیر اهم آن‌ها را مطرح می‌کنیم.

آسیب‌پذیری‌های به‌آتش

در یک تعریف رایج آسیب‌پذیری به هر گونه ضعف که قابل سوءاستفاده باشد، گفته می‌شود. در واقع، تهدیدات از آسیب‌پذیری‌ها بهره‌برداری می‌کنند و برای انجام این کار یک حمله‌کننده باید دست کم یک ابزار یا روش کاربردی داشته باشد تا بتواند از ضعف "به آتش"ها سوءاستفاده کند.

عدم آگاهی کاربر: کاربران به آگاهی نیاز دارند تا بتوانند تهدیدات و خطرات به کارگیری "به آتش"ها را کاهش دهند.

ضعف در رمزنگاری: ضعف در استفاده از رمزنگاری مناسب اطلاعات و داده‌ها یا ارتباطات امن موجب آشکارشدن اطلاعات برای دشمنان در استفاده از "به آتش"ها می‌گردد. در بحث "به آتش"ها دو مسأله مطرح است، رمزنگاری شدن داده‌های کاربر بر روی "به آتش"ها در جهت حفاظت از آن‌ها و رمزنگاری داده‌های سازمانی مورد استفاده توسط "به آتش"ها در راستای حفاظت از داده‌های سازمانی.

عدم حفاظت از حریم خصوصی: با توجه به اینکه اطلاعات خصوصی زیادی روی "به آتش"ها وجود دارد و ممکن است این اطلاعات با اطلاعات سازمانی مخلوط یا ترکیب شوند و یا دسترسی‌های خاص یا حملات و نفوذ از طریق شبکه‌های سازمانی به "به آتش"ها انجام شود، لذا در صورت کنترل‌نکردن نکات مربوطه، حریم خصوصی افراد به شدت به خطر می‌افتد.

ضعف در احراز اصالت: احراز اصالت به معنای آن است که با استفاده از سازوکار خاصی از هویت یک موجود اطمینان حاصل شود. در واقع، احراز اصالت روشی است که تشخیص می‌دهد اطلاعات هویتی یک موجود درست است یا خیر. بنابراین برای اتصال "به آتش" در شبکه‌های سازمانی، باید مطمئن شد که آن‌ها همانی هستند که ادعا می‌کنند یا اجازه دسترسی به منابع سازمان را دارند.

نصب و راه‌اندازی برنامه‌های نرم‌افزاری مخرب در "به آتش": نصب و وجود برنامه‌های نرم‌افزاری مخرب مختلف بر روی "به آتش" می‌تواند آسیب جدی به سازمان وارد نماید.

سهولت دسترسی به "به آتش": ممکن است "به آتش"ها در خانواده‌ها مورد استفاده اعضای خانواده باشند. این تجهیزات عموماً از رمز عبور ضعیف برخوردارند و یا رمز عبور آن‌ها در اختیار تعداد زیادی از افراد است. این موضوع می‌تواند موجب مخاطرات مختلفی برای شخص و سازمان شود.

دسترسی "به آتش": "به آتش"ها به شبکه یا تجهیزات سازمان متصل می‌شوند ولی سطح دسترسی آن‌ها چه میزان باشد تا آسیب‌پذیری آن‌ها را بتوان مهار نمود.

پایش و مانیتورینگ ضعیف "به آتش": در صورتی که سامانه‌های دقیق پایش و مانیتورینگ سازمانی "به آتش"ها و سطح دسترسی آن‌ها را به طور دائم رصد نکنند، شبکه و سازمان می‌تواند با مخاطرات جدی روبرو شود.

ذخیره‌سازی "به آتش": در اتصال "به آتش" به شبکه‌های سازمانی، داده‌ها و اطلاعات زیادی بر روی آن‌ها به جای می‌ماند که می‌تواند منجر به مخاطرات جدی برای سازمان شود.

تهدیدات و مخاطرات به‌آتش

نشت داده‌ها بر اثر سرقت یا گم‌شدن تجهیزات: به معنای دسترسی یا انتقال غیرمجاز داده‌ها و اطلاعات به صورت عمدی است. در صورت نبود کنترل‌های فنی برای جلوگیری از نشت داده‌ها، آن‌ها فاش خواهند شد. نشت داده‌ها از داده‌های ذخیره‌شده در حافظه‌ی دائمی "به آتش"ها یا داده‌های در حال انتقال (ایمیل، پیام‌رسان‌ها و دیگر کانال‌های اینترنتی مختلف) رخ می‌دهد.

مخلوط یا ترکیب‌شدن اطلاعات شخصی و سازمانی و افشای ناخواسته‌ی اطلاعات: استفاده از "به آتش"ها در سازمان موجب مخلوط شدن اطلاعات شخصی و سازمانی می‌شود. به عبارت دیگر، بعضی اطلاعات شخصی وجود دارند که افراد هیچ تمایلی به افشای آن‌ها ندارند. همین‌طور اطلاعات سازمانی بر روی "به

آتش"ها وجود دارد که سازمان تمایل به افشای آنها ندارد. خطراتی که ممکن است در زمینه‌ی افشای اطلاعات برای کاربران و سازمان پیش آید، شامل افشای هویت افراد، باج گیری، توهین و تهدید سازمان است.

مخاطره سه، امحای نامناسب: به معنی دسترسی یا انتقال اطلاعات به صورت عمدی یا غیرعمدی در زمان امحا است. کاربران باید در مورد امنیت "به آتش"ها دقت و وسواس زیادی داشته باشند تا اطلاعات خود و سازمان به خاطر امحای نادرست و نامناسب فاش نشود. هدف از امحای "به آتش"ها، حذف داده‌ها از روی آن است؛ به گونه‌ای که داده‌های مذکور قابل بازگرداندن نباشند.

مخاطره چهار، حملات فیشینگ: به طور کلی، ‹‹فیشینگ›› به معنی فریب کاربران برای دسترسی یا انتقال اطلاعات آن‌ها با استفاده از ابزارهای فریبنده‌ی مبتنی بر تجهیزات همراه است. مهاجمان برای افزایش احتمال مؤفقیت در حملات فیشینگ، سعی می‌کنند خود را نمایندگان قانونی مراکز معتبر مانند بانک‌ها جابزنند تا کاربران به آنان اعتماد کرده و قبولشان کنند. رمز مؤفقیت این حملات فیشینگ قدرت جلب اعتماد مردم است و مهاجمان از هر چیزی که آنان را موجه‌تر جلوه دهد، استقبال می‌کنند. مهاجمان پس از جلب اعتماد کاربران، اطلاعات حساس و مهمی را مانند شماره‌ی کارت اعتباری از آنان درخواست می‌کنند. بیش‌تر عملیات اشاره شده به صورت خودکار انجام می‌شود. با توجه به این که کاربران بسیاری هدف اولیه‌ی حمله‌ی فیشینگ قرار می‌گیرند و درصد بسیار زیادی از آنان از راه‌های تشخیص و مقابله با این نوع حملات آگاهی ندارند، شانس مؤفقیت مهاجمان به اندازه‌ی کافی بالاست.

مخاطره پنج، جاسوس‌افزارها: به طور کلی، ‹‹جاسوس‌افزارها›› شامل برنامه‌هایی هستند که به جمع‌آوری یا انتقال اطلاعات مربوط به کاربران و فعالیت‌های آن‌ها می‌پردازند. "به آتش"ها با توجه به کاربرد دوگانه استفاده شخصی و سازمانی بهترین ابزار برای طعمه‌شدن توسط هکرها و دشمنان هستند.

مخاطره شش، حملات جعل شبکه: از آنجا که "به آتش"ها عموماً به صورت بی‌سیم به شبکه‌ها وصل می‌شوند، لذا یکی از راه‌های نفوذ به "به آتش"ها، جعل شبکه و ایجاد دستگاه‌های هرز و مخربی است که سعی دارند نقاط دسترسی واقعی را جعل و شبیه‌سازی کنند. این کار راه را برای شنود ترافیک اینترنت قربانیان از سوی سوءاستفاده‌ی نفوذگران هموار می‌سازد. اغلب کاربران، "به آتش"های خود را به گونه‌ای تنظیم می‌کنند که به طور خودکار به شبکه‌ی بی‌سیم منزل یا سازمان وصل شود؛ ولی زمانی که دو شبکه‌ی بی‌سیم مشابه با نام و آدرس یکسان در دسترس آن قرار گیرد، بیش‌تر این "به آتش"ها به طور خودکار به شبکه‌ای که آنتن‌دهی (سیگنال) قوی‌تری دارد، متصل می‌شوند. جعل نام و آدرس نقاط دسترسی برای نفوذگران کار آسانی است و در نتیجه، آنان می‌توانند به راحتی "به آتش"ها را وادار کنند تا به شبکه‌ی جعلی وصل شود.

مخاطره هفت، بدافزارها: «بدافزارها» به زبان ساده نوعی برنامه‌هایی هستند که برای اقدامات مخرب ساخته می‌شوند و اطلاعات مختلف درباره‌ی کاربران "به آتش"ها را جمع‌آوری می‌کنند یا باعث تخریب "به آتش"ها یا تجهیزات سازمان می‌شوند. بدافزارها شامل ویروس‌ها، ردگم‌کن‌ها، شماره‌گیرها، اسب تراواها، بدافزارهای مالی و غیره هستند.

مخاطره هشت، ازدحام شبکه: وجود بار اضافی در منابع شبکه هنگام استفاده از "به آتش"ها، باعث عدم دسترسی کاربران "به آتش"ها به شبکه می‌شود. ازدحام شبکه زمانی روی می‌دهد که تقاضا برای یک منبع بیش از ظرفیت آن باشد. در واقع وقتی شبکه در حال حمل داده‌هایی بیش از توان خود است، کیفیت خدمات شبکه کاهش می‌یابد.

توصیه‌های پدافندی و مکانیزم‌های دفاعی در مواجه با "به آتش"

۱. برای همه "به آتش" باید سیاست امنیتی و راهنمای روشن و شفافی تهیه شود و با توجه به تنوع "به آتش"ها سالانه به روز شود. برای نمونه:

- مشخص نمایید چه نوع تجهیزاتی از "به آتش" اجازه استفاده در سازمان را دارند.
- باید مشخص شود "به آتش" چه نوع سیستم عاملی می‌توانند داشته باشند.
- اجبار شود که سیستم عامل یا برنامه‌های نصب شده روی "به آتش" باید آخرین نسخه با وصله‌های امنیتی لازم باشند.
- سیاست‌های سخت‌گیرانه برای "به آتش" باید در نظر گرفت، مثلاً کاربران "به آتش" ها باید رمزعبورهای پیچیده مورد استفاده قرار دهند.
- مشخص نمایید چه کسی صاحب برنامه‌ها یا داده‌ها و اطلاعات است.
- دارایی‌های سازمان را که "به آتش" به آن‌ها دسترسی خواهند داشت شناسایی و تحلیل مخاطره کنید.
- داده‌های طبقه‌بندی مرتبط با کسب و کار سازمان که "به آتش" به آن‌ها دسترسی خواهند داشت مشخص شوند.
- مشخص نمایید چه برنامه‌های کاربردی بر روی "به آتش" اجازه استفاده دارند و چه برنامه‌هایی ممنوع هستند.
- سیاست‌های خود در خصوص "به آتش" را با سایر سیاست‌های موجود امنیتی سازمان تلفیق یا هماهنگ سازید. مثلاً استفاده از VPNها برای "به آتش" و سایر تجهیزات موجود سازمان باید باید سیاست گمراه‌کننده یا مشکل‌زایی نداشته باشند. همچنین سیاست‌های حفاظت از داده‌ها و اطلاعات و مدیریت برنامه‌های کاربردی باید با سیاست‌های "به آتش" هماهنگ باشد.
- استراتژی‌های سازمان برای پایش و مانیتورینگ "به آتش" مشخص نمایید.
- استراتژی سازمان برای کارمندان مستعفی یا جدا شده از سازمان و "به آتش" آن‌ها داشته باشید.

- کاربر باید مسئولیت حفاظت از "به آتش" خود، داده‌های روی آن‌ها و سایر موارد را از هر نظر بپذیرد.
- نحوه احراز هویت متقابل و مدیریت هویت دیجیتال "به آتش" و صاحبان آن‌ها را تعیین کنید.
- میزان دسترسی صاحبان "به آتش" را به داده‌ها یا اطلاعات سازمانی را مشخص کنید.
- سازمان مسئول گم شدن داده‌های شخصی یا آسیب دیدن "به آتش" کارمندان نیست.
- مدت زمان اتصال "به آتش" به شبکه سازمانی باید تعیین و کنترل شوند.
- در صورت رخداد امنیتی باید محل مشخصی برای این موضوع برای اطلاع‌رسانی یا دریافت اطلاعات از صاحبان "به آتش" مشخص شود.
- اتصال "به آتش" به شبکه سازمان و حضور آن‌ها در فضای سازمان باید از نظر به روز بودن و امنیت آن‌ها پایش و مانیتور شود و در صورت وجود مشکل از راه دور ارتباط آن‌ها قطع شود.
- در صورت نیاز سازمان به جهت حفظ اطلاعات یا در جهت حفظ امنیت یا کنترل یک رخداد امنیتی باید بتواند سریعاً ارتباط "به آتش" را قطع نماید.
- در صورت ایجاد رخداد امنیتی توسط صاحب "به آتش"، باید به حراست سازمان موضوع منعکس شود.
- سازمان نباید در مانیتورینگ و پایشی که انجام می‌دهد، اطلاعات شخصی و خصوصی کاربران و صاحبان "به آتش" را مانیتور و شنود نماید.
- مسأله حق مؤلف و عدم نقض آن توسط "به آتش" در سازمان مورد توجه باشد.
- مسأله دزدیده شدن یا گم شدن داده‌های سازمانی توسط "به آتش" مدنظر باشد.
- هر گونه ذخیره‌سازی، تکثیر، ارسال، چاپ و دسترسی به محتوای غیراخلاقی باید ممنوع شود.

- نصب برنامه‌های ممنوعه از طرف سازمان باید به اطلاع صاحبان "به آتش" رسانیده شود.
- هر گونه ماسکینگ و تغییر هویت در استفاده از "به آتش" و ارتباط با دیگران به صورت ناشناس یا ماسکینگ باید ممنوع شود.
- تلاش برای قطع ارتباط یا مانیتورینگ شبکه توسط "به آتش" باید ممنوع شده و با جریمه و تنبیه همراه باشد.
- اشاعه عمدی هر گونه بدافزار باید ممنوع شده و شامل جریمه باشد.
- اجاره کنترل از راه دور "به آتش" را تعیین کنید.
- آموزش و آگاهی رسانی برای صاحبان "به آتش" در دستور کار باشد.
- قرارداد عدم افشای اطلاعات سازمان با صاحبان "به آتش" انجام شود.

۲. سرویس‌ها و خدمات شفافی برای پشتیبانی از "به آتش" ارائه نمایید.
   - مشخص نمایید چه پشتیبانی از "به آتش" شکسته شده (هک شده) ارائه خواهید داد.
   - پشتیبانی از برنامه‌های کاربردی نصب شده بر روی "به آتش" را در برنامه کار خود قرار دهید.
۳. برای حفاظت از "به آتش" و اطلاعات ذخیره شده در آن، یک برنامک ضد سرقت معتبر انتخاب، و بر روی آن‌ها نصب و استفاده کند.
۴. نصب آخرین نسخه از ضد بدافزارهای مورد تأیید سازمان بر روی "به آتش" باید رعایت شود.
۵. گم شدن "به آتش" را باید به سازمان اطلاع داد.
۶. نشت اطلاعات صورت گرفته توسط "به آتش" خود را باید به سازمان اطلاع دهید.
۷. شما مسئول حفاظت از داده‌ها بر روی "به آتش" خود هستید.

۸. اگر اهل مسافرت‌های بین‌المللی هستید "به آتش" شما باید توسط سازمان یا کنترل‌های مرزی مورد بررسی قرار گیرد.

۹. برای پیدا کردن موقعیت جغرافیایی "به آتش" گم شده یا دزدیده شده‌ی خود، حساب کاربری تعریف کنید.

۱۰. در انتخاب سیستم عامل "به آتش" خود، ویژگی ‹‹حذف خودکار از راه دور اطلاعات›› را در نظر بگیرید.

۱۱. برای ورود "به آتش" یا برنامه‌ها و فایل‌های حساس در آن‌ها از قفل استفاده کنید.

۱۲. برای حفظ حریم خصوصی و امنیت خود در "به آتش" فایل‌های شخصی را رمزگذاری کنید.

۱۳. برای حفظ حریم خصوصی خود، برنامه‌های مخفی کننده‌ی فایل‌ها و برنامه‌ها را در "به آتش" انتخاب کنید.

۱۴. سیستم عاملی برای "به آتش" خود انتخاب نمایید که از رمزگذاری پشتیبانی کند.

۱۵. قابلیت رمزگذاری اطلاعات ذخیره شده را در سیستم عامل "به آتش" فعال کنید.

۱۶. هنگام انتخاب "به آتش" به قابلیت‌های امنیتی زیست‌سنجی توجه کند.

۱۷. پیش از اتصال "به آتش" به شبکه‌های سازمانی سیاست‌های حفظ حریم خصوصی سازمان را بررسی و مطالعه و رعایت کنید.

۱۸. کاربر از نصب برنامه‌های غیرضروری روی "به آتش" خود پرهیز کند.

۱۹. هنگام استفاده از ایمیل در "به آتش"، احراز اصالت دومرحله‌ای ایمیل فعال شود.

۲۰. هنگام ایجاد حساب کاربری برای برنامه‌های شخصی و سازمانی، حساب کاربری و کلمه‌ی عبور یکسان برای آن‌ها در "به آتش" ایجاد نشود.

۲۱. روش‌های مهندسی اجتماعی در حمله به "به آتش" را بیاموزید.

۲۲. در سازمان "به آتش" خود را به شبکه‌های اجتماعی غیرسازمانی متصل نکنید.

۲۳. در زمان اتصال به شبکه‌های تحت نظارت، استفاده از برنامه‌های شخصی که از طریق اینترنت اطلاعات را تبادل می‌کنند، محدود شوند.

۲۴. "به آتش" خود را در اختیار دیگران قرار ندهید.

۲۵. هنگام استفاده از "به آتش" خود، از محیط اطراف خود و دوربین‌های مداربسته و غیره آگاه باشید.

۲۶. یک مرکز تعمیر مطمئن و مجوزدار برای "به آتش" خود انتخاب کنید.

۲۷. پیش از تعمیر "به آتش"های خود، سیم‌کارت و کارت حافظه‌ی SD یا سایر ابزارهای ذخیره‌سازی را خارج کنید.

۲۸. در پشتیبان‌گیری، تنظیمات لازم را برای تهیه‌ی نسخه‌ی پشتیبان از اطلاعات ذخیره شده در "به آتش" خود در فواصل دوره‌ای منظم انجام دهد.

۲۹. هنگام پشتیبان‌گیری از اطلاعات "به آتش" خود، از رمزنگاری استفاده کنید.

۳۰. پیش از استفاده از سرویس‌های ابری برای پشتیبان‌گیری اطلاعات "به آتش" خود، اطلاعات را به روش مناسب رمزگذاری کنید.

۳۱. پیش از امحای "به آتش" خود و کنارگذاشتن آن، اطلاعات شخصی یا سازمانی، مهم و حساس خود در کارت حافظه‌ی SD را بررسی کند.

۳۲. پیش از امحای "به آتش" خود و کنارگذاشتن آن، روش‌های ایمن حذف اطلاعات از گوشی را بررسی کند.

۳۳. پیش از امحای "به آتش" خود و کنارگذاشتن آن، اطلاعات آن را رمزنگاری کنید.

۳۴. پیش از امحای "به آتش" و کنارگذاشتن آن‌ها، اطلاعات موجود در حافظه‌ی داخلی را با استفاده از گزینه‌ی «تنظیم مجدد کارخانه‌ای» حذف کنید.

۳۵. کاربر پیش از امحای گوشی هوشمند و کنارگذاشتن آن، سیم کارت را خارج کند.

۳۶. "به آتش" خود را نفروشید.در صورت نیاز به فروش باید سازمان "به آتش" را از نظر عدم وجود اطلاعات سازمانی بر روی آن‌ها بررسی و تأیید نماید.

۳۷. اگر اجازه دانلود فایل‌های سازمانی بر روی "به آتش" خود را ندارید، حتماً این موضوع را مسئولانه رعایت کنید.

۳۸. برای انتخاب یک برنامه و نصب آن روی "به آتش" خود، به اعتبار، اصالت و رسمی بودن تولیدکننده‌ی آن برنامه توجه کنید.

۳۹. درباره‌ی نصب برنامه‌های ناخواسته که بدون اطلاع شما بر روی "به آتش" انجام می‌شود، دقت کنید.

۴۰. با تنظیم "به آتش" خود، جلوی بارگیری برنامه‌ها از سایت‌های نامعتبر را بگیرید.

۴۱. از نصب برنامه‌های غیرضروری و کرک شده روی "به آتش" خود پرهیز کنید.

۴۲. هنگام نصب یا به روز رسانی برنامه روی "به آتش" خود، به مجوزهای درخواستی برنامه توجه کنید.

۴۳. هنگام استفاده از برنامه‌ها به اجزای غیرضروری "به آتش" خود اجازه‌ی دسترسی ندهید.

۴۴. با پوشاندن لنز دوربین "به آتش"های خود از عکس‌برداری مخفی در سازمان جلوگیری کنید.

۴۵. هنگام خرید "به آتش" و قطعات جانبی آن از نو بودن "به آتش"، حافظه‌ی داخلی و کارت حافظه‌ی SD مطمئن شوید.

۴۶. از به کارگیری "به آتش" اهدایی یا دست دوم در سازمان پرهیز کنید.

۴۷. در صورت root یا jailbreak بودن "به آتش" دست دوم، آن را unroot کنید.

۴۸. پیش از به کار بردن "به آتش" اهدایی، آن را پاک‌سازی کنید.

۴۹. کارت دست دوم حافظه‌ی SD را فرمت و پاک‌سازی کنید.

۵۰. سیستم عامل "به آتش" خود را root و یا jailbreak نکنید.

۵۱. هنگام انتخاب شبکه‌ی وای–فای، از اتصال "به آتش" خود به شبکه‌های عمومی و ناشناخته پرهیز کنید.

۵۲. برای اتصال "به آتش" به شبکه‌های مخابراتی و اپراتوری، ملاحظات امنیتی لازم را از جهات مختلف انتقال امن مالتی مدیا، دسترسی به اینترنت و سایر موارد را رعایت کنید.

۵۳. با تهدیدات VPNها آشنا باشد و صرفاً از VPNهای مجاز استفاده نماید.

۵۴. در صورت عدم استفاده از شبکه‌ی وای–فای "به آتش" خود، آن را خاموش کنید.

۵۵. کاربر هنگام اتمام کار با شبکه‌های وای–فای (شبکه‌های دارای زمان اتصال کم)، گزینه‌ی ‹‹Forget›› را انتخاب کنید.

۵۶. برنامه‌های روشن و خاموش کردن خودکار وای–فای برای مکان‌های خاص جغرافیایی تنظیم شود.

۵۷. GPS "به آتش" خاموش باشد، همچنین مکان‌یابی تمام برنامه‌های "به آتش" خود را غیرفعال نمایید.

۵۸. از نام‌های غیرقابل شناسایی برای نقطه‌ی دسترسی استفاده کنید.

۵۹. هنگام استفاده از نقطه‌ی دسترسی، SSID یا نام نقطه‌ی دسترسی را مخفی کنید.

۶۰. از یک کلمه‌ی پیچیده‌ی عبور برای نقطه‌ی دسترسی خود استفاده کنید.

۶۱. کاربر هنگام استفاده از نقطه‌ی دسترسی، کلمه‌ی عبور آن را به صورت دوره‌ای تغییر دهید.

۶۲. هنگام استفاده از نقطه‌ی دسترسی از رمزنگاری قوی مانند WPA۲ در شبکه‌های بی سیم استفاده شود.

۶۳. هنگام استفاده از نقطه‌ی دسترسی، قابلیت فیلترینگ آدرس مک را فعال کنید.

۶۴. از قابلیت WPS در نقاط دسترسی استفاده نکنید.

۶۵. در صورت عدم استفاده از نقطه‌ی دسترسی، کاربر از خاموش بودن آن مطمئن شوید.

۶۶. از نامی غیرقابل شناسایی برای هات اسپات "به آتش" خود استفاده کنید.

۶۷. کاربر هنگام استفاده از هات اسپات "به آتش" خود، کلمه‌ی پیش فرض عبور را تغییر دهد.

۶۸. در صورت عدم استفاده از هات اسپات، از خاموش بودن آن مطمئن شوید.

۶۹. تنظیمات پیش فرض بلوتوث "به آتش" را تغییر دهید.

۷۰. نامی ناشناس برای "به آتش" یا بلوتوث خود انتخاب کنید.

۷۱. ‹‹مدت قابل مشاهده بودن بلوتوث›› "به آتش" خود را محدود کنید.

۷۲. دستگاه‌های بلوتوث را به صورت غیرقابل مشاهده پیکربندی کنید، مگر این که برای جفت شدن به آن‌ها نیاز باشد.

۷۳. در مدت معین، کلید جفت بلوتوث را عوض کنید.

۷۴. کاربر هنگام انجام تنظیمات بلوتوث، مراقب دسترسی دستگاه‌های جفت شده به امکانات "به آتش" خود باشید.

۷۵. نقل و انتقال بلوتوث را که از طرف دستگاه‌های ناشناخته یا مشکوک است، نپذیرد.

۷۶. در صورت امکان بلوتوث گوشی هوشمند خود را به روز رسانی کنید.

۷۷. پس از اتمام کار با بلوتوث، دستگاه را از حالت جفت شده با دستگاه‌های بلوتوثی دیگر خارج کنید.

۷۸. در زمانی که از بلوتوث "به آتش" خود استفاده نمی‌کنید، آن را غیرفعال کنید.

۷۹. در زمان انتخاب شبکه، از پروتکل‌های ارتباطی ایمن استفاده کنید.

۸۰. پیش از کار با شبکه، از برنامه‌های رمزگذار روی تنظیمات شبکه‌ی گوشی هوشمند استفاده کنید.

۸۱. کلمه‌ی پیچیده عبور برای تنظیمات شبکه‌ی "به آتش" خود استفاده کنید.

۸۲. برای ارتباطات شبکه‌ای حساس از پروتکل HTTPS استفاده کنید.

۸۳. سرویس NFC را در "به آتش" خود غیرفعال کنید.

۸۴. کاربر هنگام انتخاب "به آتش"، به روز بودن آن و امکان به روزرسانی سیستم عامل را در نظر بگیرید.

۸۵. از شارژ "به آتش" توسط شارژرهای متفرقه و یا با اتصال به سیستم‌های مختلف صوتی، تصویری و سیستمی پرهیز کنید.

۸۶. سیاست‌های امنیتی سازمان خود در زمینه نحوه استفاده از "به آتش" را مطالعه نموده و مسئولانه به توصیه‌ها عمل نماید.

۸۷. در استفاده از "به آتش" در سازمان و منزل از مرورگرهای متفاوت استفاده نمایید.

منبع : کتاب مباحث عمومی پدافند سایبری

اداره کل پدافند غیرعامل استان قم