

توصیه های حفاظتی وزارت اطلاعات به شهروندان:

ما در دنیای پر آشوبی زندگی می کنیم. حفظ امنیت خویشتن و اجتناب از آسیب برای هر فردی قابل تصور است. گاهی حتی محتاط ترین و به لحاظ امنیتی آگاه ترین افراد، دچار آسیب های امنیتی می شوند. گرچه امنیت تضمین شدنی نیست ولی به طور خارق العاده ای قابل افزایش است. همه دستگاه های امنیتی کشور از جمله کارکنان وزارت اطلاعات، برای حفظ امنیت ملی، بطور شبانه روزی در حال تلاش هستند. اما این میسر نخواهد شد مگر این که هر یک از شهروندان عزیز ایرانی، نسبت به امنیت خود و سایر هموعان احساس مسئولیت و تلاش نمایند. برای این مقصود، هر شخص باید برای افزایش ایمنی خود، قواعد مربوط به امنیت فردی را بیاموزد. آشنایی هر یک از ما با برخی اقدامات خود حفاظتی، اولین گام برای دفاع و حفاظت شخصی در مقابل خطرات غیرقابل پیش بینی است.

توصیه های حفاظتی در محل سکونت و کار:

- ۱- هرگز نسبت به آن چه که در اطراف شما رخ می دهد، بی اعتنا نباشید.
- ۲- هرگز نسبت به حضور نیروهای خدماتی در محیط زندگی به صورت ناخواسته بی تفاوت نباشید. همواره نسبت به حضور بی موقع، طولانی مدت و خارج از برنامه افرادی با پوشش نیروی خدماتی شهرداری، کارگران سیار و ... در کوچه و خیابان خود حساس باشید. دشمن ممکن است از طریق ارسال نیروهای خدماتی و ... نسبت به شناسایی و آسیب رساندن به شما یا نزدیکانتان اقدام نماید.
- ۳- هرگز فرزندان خردسالتان را حتی لحظه ای در کوچه یا ورودی منزل برای بازی یا هر دلیل دیگر، تنها نگذارید.
- کوچک ترین فرصت می تواند احتمال آسیب رساندن افراد شیاد و آدم ربا را به شما افزایش دهد.
- ۴- هرگز افراد دوره گرد و ناشناس نظیر کارگر، فروشنده سیار و ... با منظوره های مختلف به منزل خود راه ندهید.
- دشمن به منظور جمع آوری اطلاعات با پوشش های مختلف کارگری، در اطراف محیط زندگی شما حضور پیدا کرده تا با این پوشش به داخل منزل شما ورود نماید.
- ۴- هرگز نسبت به پارک طولانی مدت اتومبیل های متفرقه در اطراف محیط کار یا زندگی خود بی تفاوت نباشید.
- اتومبیل هایی که به صورت طولانی و نامعلومی در اطراف محل کار شما پارک شده باشند، می توانند متعلق به یک گروه متخلف، سارق یا حتی جنایت کار باشد.
- ۵- هرگز کلیدهای محل کار، منزل، خودرو و سایر اماکن خود را در اختیار افرادی که اطمینان قطعی از او ندارید، قرار ندهید (حتی نزدیک ترین افراد).
- قرار دادن کلید در اختیار دیگران حتی برای یک لحظه امکان قالب گیری و ساخت کلید یدکی را برای آنها فراهم می سازد.

توصیه های حفاظتی وزارت اطلاعات به شهروندان:

۶- هرگز جهت تعویض یا تعمیر قفل های محیط زندگی و کار خود، از افراد متفرقه استفاده ننمائید. استفاده از افراد متفرقه جهت تعمیر قفل های یک محیط می تواند عواقب جبران ناپذیری در پی داشته باشد. زیرا این گونه افراد مهارت خاصی در باز کردن قفل ها داشته و به راحتی می توانند نمونه هایی از کلیدها برای خود تهیه نمایند. تعویض مغزی داخل قفل کار چندان پیچیده ای نیست، سعی نمایید خودتان آن را تعویض نموده و یا به افراد مطمئن بسپارید.

۷- هرگز محیط کار و زندگی خود را بدون اطمینان از قفل بودن درب ها، رها نکنید.

۸- هرگز از وسایل ایمنی محیط زندگی و کار خود غافل نشوید.

همیشه نسبت به سیستم های ایمنی منزل و محیط کار خود مانند (سیستم های اطفای حریق، سنسورها، راه های اضطراری و) توجه داشته باشید تا خدای ناکرده دچار عواقب آن نگردید.

توصیه های حفاظتی در رابطه با همسایگان:

یکی از روش های ساده و بسیار خوب برای افزایش امنیت، برقراری روابط حسنه با همسایگان است. اغلب گفته می شود حصار خوب همسایگان خوب می سازد، ولی این شامل همه حقایق نیست. زیرا، همسایگان خوب حصارهای خوبی هستند. افرادی که شما را می شناسند احتمالاً وضعیت غیر عادی شما را نیز تشخیص می دهند و به کمکتان می آیند. به طور مثال اگر بدانند شما در مسافرت به سر می برید، با شنیدن صدای مشکوک از منزلتان کنجکاوی نموده، با شما و یا با پلیس تماس خواهند گرفت. همسایگان ما معمولاً خودروهایی که در جلوی خانه مان و یا در کوچه مقابل پارک می نمایند، یا حتی خودروهای برخی از میهمانان و بستگان ما را که به منزل ما تردد دارند، می شناسند. آن ها با شناختی که از وضعیت ما دارند، می توانند نگهبان خوب و مطمئنی برای اماکن ما باشند. بنابراین توصیه های زیر را مد نظر قرار دهید:

۱- هرگز روابط خود با همسایگان را تخریب ننمایید. حتی اگر همسایه ای به شما آزار می رساند، هرگز با او تندی و درگیری فیزیکی ایجاد نکنید. برای حل هر مشکل راه های مختلفی وجود دارد. شما دقت کنید تا بهترین یا کم ضررترین راه را برای حل مشکل خود با همسایه انتخاب نمایید.

۲- اگر به صداقت و امانت داری همسایه ای که قصد دارید او را از سفر خود مطلع نمایید، تردید دارید. هرگز مقصد نهایی و زمان دقیق برگشت خود را آشکار ننمایید. به گونه ای که هر روز تصور کند، به منزل برو خواهید گشت. همسایه ها به سرعت به عدم حضور شما پی می برند، ولی با این وجود، چنان چه شما اطلاعاتی در اختیار آن ها قرار ندهید، از زمان برگشت شما چیزی نخواهند فهمید.

۳- هرگز در مواقعی که قصد سفر طولانی مدت دارید و روابط شما با همسایگان مطلوب نیست، هیچ یک از آن ها را از طولانی بودن سفر خود، مطلع ننمایید. حتی در مواقعی که فقط با برخی یا یکی از همسایه ها، روابط خوبی ندارید، ترجیحاً برای احتیاط در برابر کنجکاوی او و جلوگیری از آسیب احتمالی، فقط اطلاعات ضروری را درباره علت عدم حضور خود، در اختیار همسایه ذی صلاح قرار دهید.

توصیه های حفاظتی وزارت اطلاعات به شهروندان:

توصیه های حفاظتی در برخوردهای اجتماعی و حضور دیگران :

- ۱- هرگز به افرادی که از پیشینه و اصل و نسبش اطلاع دقیقی ندارید، اعتماد نکنید.
- ۲- هرگز به کسانی که بدون دلیل منطقی به شما ابراز علاقه می کنند، به ویژه غریبه ها اعتماد نکنید.
- ۳- اگر با افراد ناشناس قرار ملاقات دارید هرگز با او در مکان های ناآشنا و خصوصی دیدار نکنید. زیرا افراد معمولاً در ملاء عام کم تر مورد حمله واقع می شوند.
- ۴- هرگز دیگران را از اهداف کاری خود مطلع نکنید.
- در صورتی که نیازی به اطلاع دیگران از اهداف کاری نباشد، هرگز اهداف و مراحل کار خود را برای دیگران بازگو نکنید. اطلاع دیگران از اسرار و اهداف کاری شما معمولاً باعث مشکلات لاینحلی خواهد شد که شما را به شدت پشیمان خواهد کرد.
- ۵- هرگز نسبت به کنجکاوی دیگران در امور کاری خود بی تفاوت نباشید.
- کنجکاوی دیگران در امور کاری شما ممکن است موجب درد سرهایی گردد. برخی افراد سودجو پس از اخذ اطلاعات لازم، اقدام به غصب عنوان شغلی و جایگاه اداری شما نموده و با نام شما از اعتماد مردم سوء استفاده نموده و تحت عنوان حل مشکل اداری آن ها، اقدام به کلاهبرداری نماید.
- ۶- هرگز نسبت به اطلاع دیگران از مسائل کاری خود بی تفاوت نباشید.
- در صورتی که متوجه شده اید دیگران از مسائل محرمانه کاری شما مطلع شده اند، آن را جدی بگیرید. زیرا ممکن است به نحوی به اطلاعات شما دسترسی یافته یا اطلاعات شما به سرقت رفته باشد.
- ۷- هرگز نسبت به رفتار غیرعادی دیگران (سردی یا گرمی) نسبت به خود، بی تفاوت نباشید.
- برخوردهای سرد می تواند حاکی از کدورتی باشد که قادر به بیان آن نیست یا شرایط مناسبی برای آشکار کردن آن فراهم نشده است. این کدورت تدریجاً مبدل به دشمنی خواهد شد. لذا قبل از این که بذر کینه و نفرت رشد نماید، سعی کنید از بی ربط بودن رفتار غیرعادی دیگران نسبت به خود مطمئن شوید. گرمی و ابراز عطف و غیرعادی نیز ممکن است ناشی از شکل گیری یک توطئه یا هدفی شوم باشد و ...
- ۸- هرگز در پی برقراری ارتباط با اتباع بیگانه و اعضای سفارتخانه ها نباشید.
- هرگونه ارتباط با اتباع بیگانه بدون اطلاع مسئولین چه در داخل و چه در خارج از کشور، ممکن است شما را اسیر دست اجانب و سرویس های بیگانه نماید.
- ۹- هرگز از وسایل ارتباطی اهدایی از سوی افراد استفاده نکنید.
- یکی از بهترین روش های دسترسی به اطلاعات شخصی یا ورود به حریم خصوصی افراد، اهدای وسایل ارتباطی مانند: دستگاه تلفن، نامبر، مودم، پرینتر، دستگاه کپی، گوشی موبایل و ... می باشد.
- ۱۰- هرگز قفل های رمزار خود را در حضور دیگران باز نکنید.

توصیه های حفاظتی وزارت اطلاعات به شهروندان:

هر قدر سرعت عمل شما در باز کرده قفل های رمز دار بالا باشد، باز هم نمی توان اطمینان داد که ذهن افراد حاضر نمی تواند آن را به خاطر بسپارد. افراد تیزهوش با یکبار نگاه کردن به نحوه باز کردن قفل های رمزدار، می توانند آن را به خاطر بسپارند.

۱۱- هرگز در هنگام باز کردن قفل های رمزدار، رمز قفل ها را به زبان نیاورید. بعضی افراد طبق عادت هنگام بازکردن قفل های رمزدار رمزها را به زبان می آورند. این کار می تواند مخاطرات جدی برای آن ها در برداشته باشد. زیرا در صورتی که افرادی در محیط حضور داشته باشند، به راحتی از اعداد رمز مطلع گردد.

۱۲- هرگز در مکان های عمومی، باز، ساکت و پابت با بستگان، دوستان و همکاران به بحث و گفت و گو نپردازید.

با توجه به متصور بودن دقت و توجه غریبه ها به سخنان شما، هرگونه بحث و گفت و گو در این مکان ها عواقب جبران ناپذیری خواهد داشت. لذا در صورت نیاز و ضرورت بحث به گفت و گو در این اماکن، حتماً در حال حرکت و آهسته تر صحبت کنید.

۱۳- هرگز نیازمندی های شخصی خود را نزد افراد غیر مطمئن بازگو نکنید. بازگو کردن نیازهای شخصی نزد دیگران ارائه نقطه ضعفی از سوی شماست که غریبه ها می توانند از این نقطه ضعف سوء استفاده کرده شما را مدیون خود نموده تا در مواقع نیاز از شما بهره کشی نمایند.

۱۴- هرگز از اعداد مشخص مانند (شماره تلفن، تاریخ تولد، شماره ماشین، سال تولد و ...) به عنوان رمز قفل های رمزدار خود استفاده ننمایید.

معمولاً افراد به منظور سهولت در به خاطر سپردن رمزها از شماره های شناخته شده استفاده می کنند. این امر کمک زیادی به افرادی می کند که می خواهند قفل های رمزدار را باز کنند. پیشنهاد می شود رمز قفل های خود را هر از گاهی تعویض نمایید تا امنیت قفل ها بیش تر گردد.

۱۵- هرگز رمز قفل های خود را در جایی یادداشت نکنید. بعضی از افراد به خاطر عدم اطمینان به حافظه خود رمزهای خود را یادداشت کرده و در جایی نگهداری می کنند. این کار ضریب اطمینان و حفاظت شما را به شدت کاهش می دهد. زیرا ممکن است این رمز بر حسب اتفاق در اختیار دیگران قرار گیرد.

۱۶- هرگز به امید انجام معاملات پرسود، سرمایه گذاری در بورس های خارجی و شرکت های اقتصادی و ... ، پول خود را در اختیار حتی صمیمی ترین دوست خود قرار ندهید.

چه بسا ممکن است دوست صمیمی شما به اشتباه خود واقف نبوده و مغلوب نیرنگ افراد شیاد و گروه های گلدکوئیستی شده باشد.

۱۷- هرگز از به خاطر سپردن شماره تلفن های ضروری غفلت نکنید.

توصیه های حفاظتی وزارت اطلاعات به شهروندان:

همواره سعی کنید شماره تلفن های ضروری خود را مانند (شماره تلفن روابط عمومی وزارت اطلاعات، فوریت های پلیسی، اورژانس، آتش نشانی و) را به خاطر سپرده تا در مواقعی که دچار مشکل شده یا مورد نیازتان شد، به آنها دسترسی داشته باشید.

۱۸- هرگز آمادگی جسمانی خود را از دست ندهید.

کسب آمادگی جسمانی علاوه بر سلامتی و نشاط، شما را در خطرات احتمالی یاری رسانده و در بعضی مواقع جان شما را از بعضی تهدیدات حفظ می نماید.

۱۹- هرگز از مسائل عقیدتی غافل نشوید.

هیچ گاه از ارتباط با خداوند غافل نشده و در کلیه امور از او یاری بجوئید. زیرا زندگی دنیوی بسیار پریچ و خم و مخاطره آمیز بوده و تنها او می تواند شما را در این راه یاری نماید.

توصیه های حفاظتی درخصوص خودرو:

تروریست نمی تواند بدون دسترسی به خودروی شما، بمب یا مواد منفجره را در آن کار بگذارد. به همین دلیل اتخاذ اقدامات حفاظتی در مورد سرقت خودروی شما در جاهایی که احتمال دارد هدف حمله تروریستی قرار بگیرید، کاملاً ضروری است. لذا به توصیه های ذیل توجه کنید:

۱- همواره حتی اگر قصد دارید فقط لحظاتی خودروی خود را ترک کنید (برای خرید یا ...) شیشه هایش را بالا کشیده و درب آن را قفل کنید. در صورت امکان، ماشین را به هنگام شب در خیابان رها نکنید.

۲- چنان چه در محیطی ناامن و پرخطر قرار داشته یا سکونت دارید، درب باک را قفل کرده و درب لوله اگزوز را با سرپوشی ببندید. بدین ترتیب قراردادن مواد منفجره در خودروی شما مشکل تر می شود. نگذارید کسی در نبود شما به صندوق عقب ماشین دسترسی پیدا کند.

۳- وقتی خودرو را در محوطه ای باز پارک می کنید، قبل از خروج از ماشین، مراقب افراد مشکوک حاضر در محل و چشم هایی که شما را می پابند، باشید. در صورت مشاهده افراد مشکوک با ماشین از محل دور شوید.

۴- وقتی ماشین را در محوطه ای ناامن پارک کرده و سپس به طرف ماشین برگشته اید، ابتدا دور ماشین قدم زده و قبل از سوار شدن، اطراف آن را به دقت بررسی کنید. در مناطق پرخطر، شاید بد نباشد در جستجوی هر ردپایی از سیم یا نوار غیرعادی، زیر ماشین را خوب بگردید.

۵- هرگاه متوجه حمله علیه خود شده اید، باید بدون در اختیار داشتن زمان کافی برای سنجش تمامی پیامدهای احتمالی، تصمیمی لحظه ای بگیرید. لذا برای تسریع تصمیم گیری در این زمینه، می توانید از قبل در ذهن خود مشخص کنید که تحت شرایط مختلف و احتمالی، چه واکنشی خواهید داشت.

۶- هرگز در هنگام حوادث رانندگی، خود را با طرف مقابل درگیر نکنید.

توصیه های حفاظتی وزارت اطلاعات به شهروندان:

چنان چه حادثه در مناطق ناامن یا غریب برایتان رخ داده است، از پذیرفتن هرگونه پیش نهاد توسط طرف مقابل امتناع کرده و سعی کنید موضوع را توسط کارشناسان راهنمایی و رانندگی حل کنید. زیرا ممکن است پیش نهادهایی از قبیل تعمیر اتومبیل توسط طرف مقابل، اخذ آدرس منزل و مدارک شناسایی، شماره تلفن و غیره از طرف مقابل درخواست گردد. شما باید هشیارانه به این موضوعات توجه داشته باشید.

۴-هرگز در هنگام رانندگی نسبت به اتومبیل های پشت سر خود بی تفاوت نباشید. هر فرد، ممکن است در معرض سوء قصد افراد ناباب واقع گردد. بنابراین، هوشیاری در هنگام رانندگی می تواند شما را از این موضوع مطلع کند. به خصوص اگر در ساعات مشخصی به محیط کار خود رفته یا آن جا را ترک می کنید.

توصیه های حفاظتی در نگهداری اسناد و مدارک شخصی:

۱- هرگز نسبت به حمل وسایل و اسناد و مدارک شخصی خود از محیط زندگی و کار بی تفاوت نباشید. برخی افراد در جیب، کیف و دیگر وسایل شخصی خود اسناد و مدارک یا کاغذهای یادداشت و ... قرار داده و به همراه خود حمل می کنند. این کار موجب می گردد افراد دیگر به طور تصادفی به این اسناد دسترسی پیدا کنند.

۲- هرگز در محیط های متفرقه کیف اسناد و مدارک را از خود جدا نکنید. بعضاً مشاهده می گردد، برخی افراد کیف و اسناد و مدارک خود را در محیط کار دیگران گذاشته و برای کارهای متفرقه، مانند رفتن برای رفع حاجت و غیره محیط را ترک می کنند. در بعضی مواقع فراموش می کنند که وسایل خود را از اطاق دیگران بردارند. لذا هرگز اسناد و مدارک خود را در هیچ شرایطی از خود جدا نکنید تا دچار عواقب بعدی آن نگردید.

۳- هرگز در مواقع غیرضروری اسناد و مدارک را به همراه خود حمل نکنید. بعضی افراد عادت به حمل اسناد و مدارک غیرضروری داشته و گاهی اوقات آن ها را در داخل اتومبیل گذاشته و به خرید یا کارهای متفرقه می روند. به همراه داشتن اسناد و مدارک همیشه مسئولیت افراد را نسبت به حامل آن ها سنگین تر نموده و خطرات سرقت برای آن ها متصور است. لذا پیش نهاد می گردد، هر روز کیف اسناد و مدارک خود را بازدید کرده و مدارک اضافی را از آن خارج نمایید.

توصیه های حفاظتی در استفاده از تلفن:

۱- هرگز تلفن همراه خود را در اختیار دیگران قرار ندهید. سیم کارت تلفن همراه به راحتی قابل کپی برداری بوده و دیگری به راحتی می تواند از سیم کارت و همچنین اطلاعات ذخیره شده در آن (شماره های ذخیره شده، پیغام ها، قرارها و ...) کپی برداری نماید.

توصیه های حفاظتی وزارت اطلاعات به شهروندان:

از آن جا که اطلاعات ذخیره شده در دستگاه تلفن همراه، بخشی در حافظه دستگاه قرار می گیرد، باید همواره هنگام تعویض و فروش یا تعمیر گوشی تلفن همراه، اطلاعات ذخیره شده در حافظه گوشی را پاک نمایید.

۲- هرگز از تلفن همراه افراد ناشناس برای برقراری ارتباط خود استفاده نکنید.

در بعضی مواقع ممکن است شما نیاز فوری به برقراری تماس تلفنی داشته ولی چون دستگاه تلفن خود را در اختیار نداشته یا امکان تماس با آن وجود ندارد، ممکن است از تلفن همراه دیگران استفاده کنید. از آن جا که شماره تماس در حافظه تلفن همراه او ثبت می گردد. لذا از تلفن های عمومی مخابرات استفاده کنید، یا از تلفن همراه افراد مطمئن، کسبه های ثابت و ... استفاده نموده و حتی المقدور پس از تماس، شماره را حذف نمایید.

۳- هرگز به مکالمات تلفنی افراد ناشناس اعتماد نکنید.

یکی از سریع ترین و ارزان ترین روش جمع آوری اطلاعات تخلیه تلفنی است که برخی افراد با تقلید صدا، غصب عنوان مراکز دولتی و موجه، پوشش های شغلی مختلف و ترفندهای بسیار جالبی اقدام به کسب اطلاعات از دیگران می نمایند. مواظب باشید، حتی برخی افراد حرفه ای نیز ممکن است فریب خورده و ناخواسته اطلاعات ارزشمندی را در اختیار تماس گیرنده قرار دهد.

۴- هرگز منوی «بلوتوث» تلفن همراه را در حالت فعال قرار ندهید.

یکی از امکانات انتقال اطلاعات به صورت بی سیم استفاده سیستم «بلوتوث» می باشد. گوشی های جدید تلفن همراه دارای این قابلیت بوده و از این طریق اطلاعات خود را مبادله می کنند. در صورت فعال بودن این قابلیت در تلفن همراه، افراد ناشناس تا فاصله ۵۰ متری از شما می توانند از اطلاعات دستگاه تلفن همراه شما بهره برداری کرده یا با ارسال ویروس گوشی شما را دچار مشکل کنند.

۵- هرگز از تلفن های بی سیم در ارتباطات تلفنی استفاده نکنید.

فرکانس تلفن های بی سیمی اغلب توسط رادیو موج FM-SW-AM و کانال های تلویزیونی قابل دریافت می باشند. بنابراین، دیگران به ویژه همسایه ها به راحتی می توانند، مکالمات تلفنی شما را شنود کنند. به همین خاطر، هیچ گاه سعی در استفاده بی سیمی نداشته باشید. در صورت لزوم، مطالب سری و مهم خود را از این طریق رد و بدل نکنید.

۶- هرگز شماره تلفن دوستان، آشنایان و همکاران خود را بر روی کاغذ باطله، روزنامه، پشت جعبه دستمال کاغذی و موارد مشابه یادداشت ننمایید.

بارها مشاهده می شود که افراد هنگام مکالمات تلفنی شماره تلفن دیگران را بر روی روزنامه نوشته، نسبت به آن بی توجه می باشند. این در حالی است که در صورت خارج شدن روزنامه های باطله، این گونه اطلاعات نیز خارج می گردد.

توصیه های حفاظتی وزارت اطلاعات به شهروندان:

توصیه های حفاظتی در استفاده از رایانه ها:

- ۱- هرگز از رایانه خود به ویژه در محل کار، بدون رمز عبور (پسورد) استفاده نکنید. همیشه برای رایانه خود رمز عبور تعیین کرده و آن را طوری تنظیم نمایید که در صورت عدم استفاده از آن به مدت (حداکثر) پنج دقیقه از شما اسم رمز عبور درخواست نماید. این کار مانعی برای دسترسی دیگران به رایانه شما خواهد بود و تا حدودی امنیت سیستم شما را افزایش می دهد.
- ۲- هرگز از رمز عبور ساده و مشخص استفاده نکنید. سعی کنید رمز عبورهای سیستم خود را پیچیده و غیرقابل پیش بینی انتخاب کنید. انتخاب رمز عبور با کارکترهای زیاد، با حروف و اعداد، حروف کوچک و بزرگ و یا انتخاب آن به زبان دیگر، می تواند امنیت سیستم شما را افزایش دهد.
- ۳- هرگز اطلاعات محرمانه خود را در فایل های آشکار و سهل الوصول قرار ندهید. فایل های محرمانه خود را می توانید به صورت پنهان و در زیر مجموعه فایل های سیستمی یا زیر مجموعه سایر برنامه های نصبی سیستم قرار دهید تا به راحتی در اختیار افراد بیگانه قرار نگیرد. در غیر این صورت، احتمال دسترسی راحت به این گونه فایل های همواره متصور است.
- ۴- هرگز از کامپیوتری که دارای اطلاعات محرمانه و با اطلاعات خصوصی است، برای متصل شدن به اینترنت استفاده نکنید.
- همیشه در هنگام متصل شدن به اینترنت خطر سرقت اطلاعات، تخریب اطلاعات به صورت جدی وجود داشته و در صورت بی تفاوتی به این مطلب خطرات جبران ناپذیری سیستم و اطلاعات شما را تهدید می کند.
- ۵- هرگز کامپیوتر خود را که حاوی اطلاعات محرمانه یا خصوصی است، جهت تعمیر به افراد متفرقه و ناشناس ندهید. حتماً نسبت به تعمیرکار کامپیوتر خود اطمینان حاصل نموده و سعی کنید شخصاً هنگام تعمیر حضور داشته باشید.
- ۶- هرگز قطعات آسیب دیده سیستم کامپیوتر خود را (مانند: هارد، فلاپی، سی دی و ...) دور نیاندازید. حتماً این گونه لوازم از کار افتاده را منهدم کرده و امکان بهره برداری مجدد را از آنها بگیرید. اغلب کامپیوترهای مستعمل و از رده خارج شده دارای اطلاعات ارزشمندی است که در هنگام تعویض یا فروش بر اثر سهل انگاری در سیستم ها باقی مانده است. همچنین امکان بازیافت اطلاعات از حافظه های پاک شده سیستم وجود داشته و صرف پاک کردن یا فرمت کردن سیستم نمی تواند از پاک شدن صد در صد آنها اطمینان داشت. بنابراین بعضی از افراد تصور می کنند با پاک کردن هاردهای مستعمل تمام اطلاعات آنها از بین رفته و می توانند آنها را دور ریخته یا به فروش برسانند.

توصیه های حفاظتی وزارت اطلاعات به شهروندان:

- ۷- هرگز به تماس های تلفنی از طریق اینترنت اعتماد نداشته باشید.
- امروز اغلب تلفن های خارج از کشور توسط تماس های تلفنی اینترنتی صورت می گیرد که کارت های خدماتی آنها در همه جا قابل دسترس می باشد. از آنجا که شرکت های خدمات اینترنت (آی-اس-پی) و کشورهای سرویس دهنده (بک بن) توانایی استراق سمع تمامی مکالمات تلفنی را دارند. استفاده از این ارتباطات نیز ناامن و غیر مطمئن می باشد.
- ۸- هرگز از مشخصات اصلی خود در محیط اینترنت استفاده نکنید.
- در هنگام حضور افراد در خارج از کشور یکی از راه های به دست آوردن اطلاعات از آنها، مراجعه به فضای اینترنت می باشد. در صورتی که مشخصات شما در یک سایت یا ایمیل یا مشاهده گردد. اطلاعات با ارزشی نسبت به شما می تواند به دست آید.
- ۹- هرگز از کامپیوتر مخصوص اینترنت برای کارهای متفرقه استفاده ننمائید.
- در نظر داشته باشید که مودم، پرینتر، اسکنر و بعضی از اجزای داخلی کامپیوتر «آی-پی» پذیر بوده و می تواند اطلاعات خود را به آدرس برنامه ریزی شده از طریق اینترنت ارسال کنند. بنابراین ممکن است نامه ای که تایپ کرده و پرینت گرفته اید و حتی از کامپیوتر خود را که پاک کرده اید، بعد از آن که به اینترنت متصل می شوید، به آدرس برنامه ریزی شده ارسال گشته بدون آن که شما از آن مطلع گردید.
- ۱۰- هرگز نسبت به محافظت و نگهداری نسخه ذخیره اطلاعات (backup) بی تفاوت نباشید.
- معمولاً به خاطر محافظت از اطلاعات و پیش گیری از تخریب آنها اقدام به تهیه نسخه های ذخیره می نمایند. حفاظت و نگهداری این نسخه ها حتی از اطلاعاتی که در سیستم ها نگهداری می شوند با اهمیت تر می باشد. زیرا این اطلاعات به صورت آماده و بدون درد سر می باشند. سهل انگاری در نگهداری از این نسخه های ذخیره بعضاً معضلات جبران ناپذیری در بر خواهد داشت.
- ۱۲- هرگز در مواقع غیر ضروری سیستم خود را به شبکه اینترنت متصل ننمائید.
- اغلب در ارتباطات لیزلاین و شبکه ای، ارتباط اینترنتی به صورت پیوسته و شبانه روزی است. اما با توجه به تهدیداتی که از این طریق برای سیستم شما متصور است، در مواقعی که نیازی به ارتباط با اینترنت ندارید، آن را قطع نمائید تا از گزند هکرها و جاسوسان اینترنتی و عوامل بیگانه در امان باشید. هکرها توانایی فعال سازی میکروفن و دوربین (وب کم) شما را بدون توافق با شما را دارند. لذا با توجه به متصل بودن بی مورد و طولانی مدت سیستم شما به اینترنت این گونه خطرات همواره متصور است.
- ۱۳- هرگز نسبت به تهیه نسخه ذخیره از اطلاعات درون رایانه خود مسامحه نکنید.
- رایانه ها ابزار قابل اطمینانی نیستند و همواره احتمال صدمه دیدن آنها متصور است لذا همیشه سعی کنید از اطلاعات داخل سیستم خود یک نسخه ذخیره داشته باشید تا در صورت بروز هرگونه اختلالی اطلاعات شما در اختیارتان باشد.

توصیه های حفاظتی وزارت اطلاعات به شهروندان:

۱۴- هرگز به موارد شناخته نشده در اینترنت پاسخ ندهید.

ایمیل های ناشناخته یکی از موارد بوده که هرگز نباید آن ها را گشود، زیرا در مواردی با گشودن ایمیل یا یک تصویر اینترنتی تروجانی از این طریق وارد سیستم شما گشته و مراحل کار جاسوسی و نفوذ به سیستم شما را آغاز می نماید یا پنجره هایی که در خلال کار با اینترنت به صورت ناخواسته ظاهر گشته یا درخواست های اشتراک در سایت، شما را ترغیب به دادن نام کاربر و نام عبور می نماید که از این طریق اطلاعات مربوط به رمز عبور شما را در اختیار گرفته و از آن بهره برداری کنند.

توصیه های حفاظتی در رابطه با مسافرت:

خطر در گوشه و کنار دنیا وجود دارد اما ماهیت و شدت آن در هر کشور یا منطقه متفاوت است. صرف نظر از جایی که می روید شما باید در رابطه با مسافرت خود اقدامات اساسی خاصی را انجام دهید. سطح این اقدام بستگی به مقصد دقیق شما دارد. مع الوصف، برای مسافرت به توصیه های ذیل توجه کنید:

۱- هرگز بدون آشنایی کافی از مقصد و مسیری که برای سفر انتخاب می کنید، به مسافرت نروید. قبل از سفر درباره پاسخ سئوالات زیر تحقیق کنید.

الف. آیا برای سفر به مقصد مورد نظر هشدار خاصی به لحاظ امنیتی، سیل، آتش سوزی، زلزله، برف و بوران و ... داده شده است یا خیر؟

امروزه، با گسترش امکانات ارتباطی، فنی و ماهواره ای، به راحتی می توان از وضعیت راه ها، آب و هوا، حوادث طبیعی خطرناک مثل وقوع سیل و طوفان و ... مطلع شد. حصول اطمینان از ایمنی راه ها و مسیری که باید طی کنیم. هم چنین به همراه داشتن تجهیزات مورد نیاز سفر، ما را در برابر آسیب های احتمالی محفوظ نگاه می دارد.

ب. امنیت جاده ای در چه ساعاتی از شب یا روز کاهش می یابد؟

ج. چه امکانات جاده ای برای حوادث احتمالی وجود دارد؟

د. کدام نقطه از مسیری که طی خواهید کرد، برای اطراق و استراحت بین راهی مناسب و امن تر است؟ کدام منطقه از مسیر سفر، آب آشامیدنی لوله کشی شده دارند و در کدامیک باید از بطری های آب استفاده کرد؟

هـ. چه رستوران هایی را برای صرف غذا باید انتخاب کرد؟

و. مصرف چه غذای بین راهی مناسب تر است؟

۲- در صورت تمایل به صرف غذا در رستوران ها هرگز سالاد (به ویژه در رستوران های ناشناس)، میوه های پوست نکنده و آشامیدنی های همراه با یخ را میل نکنید.

۳- هرگز پول ها و اشیاء ارزشمند خود را در یک کیف یا یک ظرف قرار ندهید.

توصیه های حفاظتی وزارت اطلاعات به شهروندان:

سعی کنید قبل از سفر، وضعیت فرهنگی و اقتصادی ساکنین مناطقی که در مسیرتان قرار خواهند گرفت، اطلاعات لازم را بدست بیاورید. محتویات کیف شما شاید معادل ماه ها حقوق افرادی باشد که در مناطق فقیرنشین زندگی می کنند. معمولاً مسافران پول نقد و اموال ارزشمندتری نسبت به افراد بومی دارند، لذا ممکن است به راحتی هدف دستبرد یا حمله افراد ناشناس قرار بگیرید. به ویژه آن که بومی ها، مناطق امن و ناامن را می شناسند. عدم آشنایی با افراد و محیط یا محدوده ای که تردد می کنید، مطمئناً احتمال آسیب پذیری را افزایش می دهد.

۴- هرگز از مردم رهگذر در خیابان آدرس نپرسید. سعی کنید افسر پلیس یا مسئولی را پیدا کنید. با این کار یک فرد غریبه را از مقصد خود مطلع می کنید. نقشه ای تهیه نموده و از کسانی کمک بگیرید که احتمال بیشتری دارد به شما کمک کند. برای انتخاب بهترین و ایمن ترین مسیر، همیشه از افراد موجه مثل مأمورین راهنمایی و رانندگی و یا افرادی که شناسایی آن ها آسان است، مثل رانندگان تاکسی، مغازه دارها و ... سؤال نمایید. در موارد خاص، وقتی فرد مطمئنی را برای اخذ راهنمایی نیافتید، سعی نمایید در پرسش خود مقصد نهایی خود را بیان نکنید بلکه در شهرهای بین راهی براساس نقشه ای که در اختیار دارید، آدرس نزدیک ترین شهر بعدی مسیر خود را پرسید تا دیگران از مقصد نهایی شما مطلع نگردند.

۵- در مسافرت، هرگز اسناد خود را درون هتل ها جا نگذارید. در مسافرت های به ویژه مسافرت های خارج از کشور سعی کنید هیچ گونه اسناد و مدارکی به همراه خود به داخل هتل ها نبرید و در صورت نیاز هرگز آن ها را در داخل هتل جا نگذارید. زیرا افراد غریبه می توانند در غیاب شما با پوشش نظافت به داخل اتاق های هتل رفته و به اسناد شما دسترسی پیدا کنند.

توصیه های حفاظتی در خصوص اقامت پستی:

۱- هرگز اقامت پستی و نامه های مشکوک و غیرقابل انتظار را از کسی دریافت نکنید. حتماً اعضای خانواده و کارکنان خانه شما باید از پذیرش هرگونه بسته ای در منزل اجتناب کنند. (اگر دارای شغل دیگری نیز هستید) در محل کار خود نیز اطمینان یابید که کارکنان دفتری نحوه برخورد با نامه ها یا بسته های مشکوک را می دانند، به ویژه وقتی در خارج از کشور حضور دارید، با حساسیت بیشتری به این بسته ها توجه کنید.

۲- بسته یا نامه مشکوک را هیچ گاه نباید لمس و جابه جا کرد. وجود چنین اقلامی را فوراً به مقامات امنیتی اطلاع داده و افراد را از آن دور کنید. هرگونه جابه جایی به ویژه برش نوار دور بسته، بست ها، یا هرگونه بسته بندی روی بسته مشکوک، چه بسا موجب انفجار ابزار گردد.

۳- هرگز بسته یا نامه مشکوک را باز نکرده و یا در آب قرار ندهید زیرا شاید موجب انفجار آن گردد.

توصیه های حفاظتی وزارت اطلاعات به شهروندان:

سایر توصیه های حفاظتی:

- ۱- در صورت مشاهده افراد مشکوک، تروریست و خرابکار مراتب را به مراکز امنیتی به ویژه ستاد خبری وزارت اطلاعات به شماره ۱۱۳، اطلاع دهید.
- ۲- چنان چه دارای دوربین عکاسی یا گوشی تلفن همراه دوربین دار هستید، حتی المقدور از آن ها و متعلقاتشان، از جمله خودرو و ... تصویربرداری نمایید.
- ۳- در صورت امکان بدون این که ایجاد حساسیت کنید، آن ها را تعقیب و آدرس محل استقرار آن ها را کشف نمایید.
- ۴- چنان چه شئی مشکوکی را به خودروی دیگران چسبانده یا در مکانی رها نموده اند، به آن نزدیک نشده، بلافاصله به افراد مسئول اطلاع دهید.
- ۵- هرگز به افرادی که خود را مأمور وزارت اطلاعات معرفی نموده و در مراکز غیررسمی با شما قرار ملاقات می گذارند، اعتماد نکنید و بلافاصله به ستاد خبری وزات اطلاعات به شماره ۱۱۳ اطلاع دهید.
- ۶- هرگز در ارزیابی های خود به ظاهر افراد اکتفا نکنید، افراد شیاد هرگز چهره واقعی خود را به شما نشان نخواهند داد.