فصلنامه داخلی خبری و آموزشی

رصد

سال اول | پیش شماره ۱ | تابستان ۱۳۹۸

نخبگی و دسترسی به اطلاعات

دو ویژگی مهم برای سرویس های جاسوسی

یکی از رویکردها و راهبردهای اعلامی معاونت ضدجاسوسی وزارت اطلاعات، راهبرد صیانت و پیشگیری است.
وزارت اطلاعات در کنار مقابله با تهدیدات امنیتی اقدامات گسترده‌ای را برای پیشگیری از وقوع تهدیدات اتخاذ می‌کند. یکی از این اقدامات برپایی نمایشگاه توجیهی و آموزشی برای مخاطبینی است که محتمل است در معرض آسیب و یا تهدیدات امنیتی قرار گیرند.

شهریورماه امسال معاونت ضدجاسوسی وزارت اطلاعات ضمن برگزاری نمایشگاهی با هدف صیانت و پیشگیری به تشریح برخی از اقدامات سرویس های بیگانه برای جاسوسی از دستگاه ها، نهادها و وزارتخانه های کشور پرداخت.
در این نمایشگاه تخصصی ضدجاسوسی تلاش شده تا ضمن افشای روش‌های سازمان های اطلاعاتی، مخاطبین نسبت به تهدیدات اطلاعاتی هشیار و یا به عبارتی واکسینه شوند. برای همین یکی از مهمترین فعالیت‌های معاونت ضدجاسوسی ارتقاء سواد امنیتی، مهارت افزایی جامعه به‌ویژه نخبگان و مدیران کشور است.

این نمایشگاه موضوعاتی از جمله تکنیک‌های ارتباطی و رفتاری سازمان‌های جاسوسی در فرآیند فریب افراد، اقدامات نرم آمریکا برای «نفوذ» فرهنگی، جاسوسی تلفنی، سوءاستفاده از هویت‌های جعلی، دام ویزا، روش‌های جذب نخبگان، اهداف و روش‌های نفوذ در عرصه‌های سیاسی و اجتماعی و موضوعات متنوع دیگری تبیین و به تصویر کشیده است.

◈ نخبگی و دسترسی به اطلاعات
دو ویژگی مهم برای سرویس های جاسوسی

خبرآنلاین درباره بازدید ۱۰۰ نفره جمعی از اهالی رسانه از این نمایشگاه نوشت: به وضوح مشهود بود که زبان کارشناسان ضدجاسوسی در بیان جزئیات پرونده ها بسته است و گاه که یک همکار رسانه ای با ۲-۳سوال متوالی قصد گودبرداری! و کسب اطلاعات بیشتر را داشت با کوچه علی چپ مواجه می شد و گاه نیز به وضوح می شنید که به دلیل طبقه بندی حفاظتی، حرف بیشتری نمی تواند بشنود. آن گونه که این رسانه گزارش داده، برابر آن چه

کارشناسان ضدجاسوسی در این نمایشگاه مطرح کردند، عوامل نفوذی یا چهره‌هایی که فریب سازمان‌های اطلاعاتی را خورده بودند، گرچه به قشر خاصی محدود نمی‌شدند اما ویژگی مشترکشان، نخبگی و دسترسی‌شان به اطلاعات بود. همچنین نفوذی‌ها، هم در لباس روحانیت بودند و هم پزشک، مهندس، دانشجو، کارمند نظامی، غیرنظامی و ... .

آن‌گونه که خبرآنلاین روایت کرده است، نکته مهمی که در لابه‌لای حرف‌های کارشناسان به اشاره‌ای اکتفا شد، اطلاعاتی است که حریف، بدون هیچ هزینه‌ای آن‌ها را از دست‌مان می‌قاپد. این بر می‌گردد به اظهار نظرهای برخی مسئولان کشور در رده‌های مختلف مدیریتی که گاه و بی‌گاه در یک دعوای سیاسی، نه پته همدیگر، که منافع ملی کشور را روی آب می‌ریزند و برای این که در مشاجره، دست بالا را داشته باشند، اطلاعات طبقه‌بندی شده را فاش می‌کنند. براساس گزارش انصاف‌نیوز، در بخش دیگری از این بازدید، فیلمی از برخی افراد دستگیر شده که در سازمان‌ها، نهادها و وزارتخانه‌های مختلف، اطلاعاتی را به سرویس‌های بیگانه منتقل کرده بودند، نمایش داده شد.

◈سیا: ایرانیان عاطفی هستند، با هدیه مدیونشان کنید!

براساس گزارش فارس، یکی از بخش‌های جالب توجه و قابل تامل در این نمایشگاه، آسیب‌شناسی فرهنگی جامعه ایران توسط سازمان اطلاعاتی آمریکاست. در این بررسی که سند پنهان آن توسط معاونت ضدجاسوسی کشف شده است، این سازمان طی ابلاغ رسمی به افسران اطلاعاتی فعال در موضوع ایران توصیه کرده که ایرانیان مردمانی عاطفی و احساسی هستند بنابراین تلاش کنید تا در تعاملات خود آن‌ها را با دادن هدیه، تسهیلات، دعوت به یک رستوران و... مدیون کنید چرا که آنان در این شرایط تلاش خواهند کرد تا محبت شما را جبران کنند و در این فرآیند است که می‌توان یک ایرانی را از طریق ارتباط دوستانه با خود همراه و به تدریج تبدیل به خائن و جاسوس کنید.

◈عملیات تله عسل

به گزارش اصناف‌نیوز در این نمایشگاه راه‌های مختلف جذب عامل از سوی سرویس‌های مختلف و فرایندی که آنها برای ایجاد ارتباط و همکاری طی می‌کنند نمایش داده شد؛ از جمله راه‌هایی که به ایجاد همکاری میان این سرویس‌ها و فرد مورد استفاده قرار گرفته شده، منتهی می‌شود، می‌توان به ایجاد ارتباط در طول پروسه صدور ویزا، ایجاد ارتباط از طریق پیشنهاد همکاری و کارهای اقتصادی، از طریق آنچه به آن عملیات تله عسل می‌گویند و در آن از پرستوها استفاده می‌شود و... اشاره کرد. در این مورد آخر ضمن بر شمردن برخی مواردی که تاکنون سرویس‌های بیگانه در آنها از این شیوه استفاده کرده‌اند، فیلمی کوتاه نیز نمایش داده شد از زنی خارجی، تقریبا مسلط به زبان فارسی که از سوی سرویس امنیتی یکی از کشورها بکارگیری شده بود برای برقراری ارتباط با کارکنان کنسولگری ایران؛ در خانه‌اش از سوی سرویس امنیتی کشور بیگانه دوربین و میکروفون نصب شده و کارفرماهای او اصرار داشته‌اند که بزودی افراد مورد نظر را به خانه‌اش بکشاند.

◈تخلیه تلفنی منافقین ادامه دارد...

مورد دیگری که مورد اشاره در این نمایشگاه بود موضع تخلیه‌تلفنی سازمان تروریستی مجاهدین خلق (منافقین) بود. تلفن‌هایی در این نمایشگاه تعبیه شده بود که برخی مکالمات واقعی منافقان با بعضی از افراد در گوشی این تلفن‌ها پخش می‌شد. صداهایی معمولی، با لحنی اداری، که هربار خود را کسی و منتسب به جایی معرفی کرده بودند و در برخی موارد هم موفق شده بودند که فرد مورد نظر را بصورت تلفنی تخلیه اطلاعاتی کنند

بنا بر گزارش انصاف نیوز، نکته جالب توجه دیگر در این بازدید این بود که محدودیتی در قشری که سرویس‌های امنیتی کشورهای دیگر تلاش به برقراری ارتباط با آنها می‌کردند وجود نداشت. افراد متعددی برای این کار انتخاب می‌شدند، از کسی با پوشش روحانی تا راننده تاکسی و رایزن فرهنگی و دیپلمات و کارمندان و شاغلان نهادهای نظامی و... از همگی مثالی با نام و نشان وجود داشت که به اشکال مختلف با سرویس‌های امنیتی دیگر کشورها به همکاری پرداخته بودند و در برخی موارد اطلاعاتی موثر و مهم را به دست آنها رسانده بودند. تا آنجا که در یکی از این موارد فرد موردنظر غیر از اینکه اطلاعاتی مهم در زمینه نظامی را خارج کرده بود، حتی به‌شکلی، اطلاعاتی درباره برخی دانشمندان هسته‌ای ترور شده – از جمله شهید علی‌محمدی - از سوی این فرد به سرویس‌هایی چون موساد داده شده بود که در نهایت دستگیر شد.

◈جاسوسان بیخ گوش ما!

در فقره دیگری دیپلماتی با سابقه بود که از سال ۷۲ وارد وزارت خارجه شده و در سال ۸۴ ماموریتی ثابت در یکی از کشورهای اروپای مرکزی به او داده شده است و سه سال بعد از آن آغاز همکاری‌اش با سیا بوده است. او سال ۸۸ به ایران بازمی‌گردد و در وزارت امور خارجه به عنوان دستیار یکی از معاونین مشغول به کار می‌شود و همچنان ارتباطش با CIA از طریق راه‌های امن ادامه داشته و در ازای اطلاعات سری مربوط به جلسات و همکاری با این سازمان امنیتی جاسوسی، پولی هنگفت دریافت می‌کرده است. او از زمانی که متوجه می‌شود که رد داخل به او مشکوک شده‌اند به سرعت متواری شده و تا امروز هم اطلاعی از او در دست نیست.

◈نخبگان علمی در معرض طعمه‌شدن

اما در میان سوژه‌های کشف شده از سوی وزارت اطلاعات با عنوان جاسوس، برخی نخبگان علمی نیز دیده می‌شوند. یکی از این افراد که مشخصاتش در این مراسم نمایش داده شده بود، فردی بود که به لحاظ علمی سطحی بالایی داشته است. بعد از روشن شدن همکاری‌اش با سرویس‌های امنیتی بیگانه، دستگیر شده و به‌خاطر حساسیت اطلاعات نظامی که منتقل کرده، به اعدام محکوم شده است. اما مدیرکل ضد جاسوسی وزارت اطلاعات با تاکید براینکه جرم جاسوسی ۵ الی ۱۰ سال حبس دارد و تنها در صورت جاسوسی در شرایط جنگ و یا در موضوع اطلاعات نظامی به تشخیص قاضی پرونده ممکن است حکم اعدامی صادر شود، می‌گوید که به‌دنبال این هستیم که در مورد نخبگان بتوان از علم و دانسته‌های آنها استفاده کرده و به شکل دیگری کیفر کاری که انجام داده‌اند را ببینند تا جامعه بتواند از علمشان منتفع شود.

◈ منابع:
◆روزنامه‌خراسان،
خبرگزاری‌فارس،خبرآنلاین، اصناف نیوز

زنگ تلفن همیشه زنگ خبر نیست

یک تماس تلفنی ساده با صدایی گرم، صمیمی و گاه جدی شما را با نامتان مورد خطاب قرار می دهد. و این آغازی است برای کسب اطلاعات دلخواه .
موضوعی به ظاهر کم اهمیت و ساده که در صورت بی‌توجهی به آن می‌تواند پازل اطلاعاتی دشمن (تماس گیرنده) را کامل کند.

برخی (بویژه مدیران جوان امروز) تصور می کنند تخلیه تلفنی روشی کهنه و "سوخته" است. در حالیکه اطلاعات موجود نشان می‌دهد دشمن و عوامل آن نظیر منافقین همچنان بخشی از اطلاعات خود را از این طریق بدست می آورند.

يكي از آسان‌ترين و كم خطرترين شيوه‌هاي طرف متخاصم براي كسب اطلاعات به صورت مخفيانه، استفاده از ابزار فني و مخابراتي مثل تلفن، فاكس، تلكس و اينترنت است و ساده ترين و كم هزينه ترين آن استفاده از تلفن مي‌باشد. جمع آوري از طريق تلفن را جاسوسي تلفني و به نوعي ديگر كه همراه با فريب باشد تخليه تلفني مي گويند. از آنجا كه گروهك‌هاي ضدانقلاب مثل منافقين و برخي عناصر خود فروخته همواره در پي كسب اطلاعات از مراكز دانشگاهي و فعاليت‌هاي علمي كشور هستند، جهت اطلاع همگان برخي نكات بارز دربرخورد با اين افراد ذكر مي گردد.

◈اولین سئوالی که در این خصوص مطرح است این‌که به نظر شما چند درصد از اطلاعات و اخبار کشور توسط تخلیه تلفنی به دست دشمنان ایران زمین می‌افتد؟

◆پاسخ : نزديك به ۸۰ درصد اطلاعات كشور توسط تخليه تلفني از تمامي اقشار جامعه به دست دشمنان اين مرز و بوم مي‌افتد.

دشمن در تخلیه تلفنی به دنبال اطلاعاتی است که از نظر ما ارزش چندانی ندارند

◈سئوال بعدی که مطرح می گردد این که دشمن در تخلیه تلفنی به دنبال چیست و چه کسانی در معرض تخلیه تلفنی هستند؟

◆پاسخ : دشمن در تخليه تلفني به دنبال اطلاعاتي است كه از نظر ما ارزش چنداني ندارند، ولي در واقع براي آن‌ها ارزشمند محسوب مي گردد و اطلاعات ما به واقع تكميل كننده پازل اطلاعاتي آن‌هاست و دشمنان براي اين كار هيچ محدوديت سني اعمال نكردند و از كودكان ٦ ساله تا سال خوردگان ٩٠ ساله را مورد تخليه قرار داده‌اند.

◈اصولاً تخلیه تلفنی به دو صورت انجام می گیرد:

۱) كنترل تلفن همراه افراد با استفاده از وسائل و روش هاي مخصوص، كه بيش‌تر جنبه جاسوسي و اطلاعاتي دارد.
۲) تماس تلفني با اشخاص و گرفتن مستقيم اطلاعات از آن‌ها.

◈نکات مهم جهت مقابله با تخلیه تلفنی

◆هرگونه اطلاعات درون سازماني كه دانستن آن براي عموم جايز نيست، داراي ارزش است و نمي بايست فاش گردد.
◆دادن اطلاعات به تماس گيرنده را موكول به تماس تلفني خودتان كنيد كه ضمن اخذ شماره تلفن و چك كردن آن برقرار خواهيد كرد.
◆صرف اينكه طرف تماس، به شما يك شماره داد، دليل صحت او نيست بلكه بايد شماره داده شده را بررسي كنيد.
◆از دادن شماره تلفن هاي غير عمومي به افراد ناشناس خودداري كنيد.

ادامه در صفحه ٤

ادامه از صفحه۳

◆در صورتي كه تماس‌گيرنده به موارد ضعف شما اشاره كند، يا در صورت ندادن اطلاعات تهديد به از دست دادن شغل يا گزارش به رده هاي بالاتر نمايد، اعتنا نكنيد.
◆بعضي وقتها تماس گيرنده، اتفاق مدنظر را به صورتي تعريف مي‌نمايد تا مخاطب تحريك شده و اطلاعات جزئي‌تري بدهد.
◆اگر فردي تماس گرفته و اطلاعات آشكاري راجع به موضوع دارد، دليل صاحب نظر بودن او نيست، پس به او اعتماد نكنيد.
◆ جاسوس‌ها از علاقه نيروهاي يك سازمان در جهت راه اندازي كار سازمان‌هاي ديگر استفاده كرده و در ساعات غير اداري تماس گرفته، خود را مسئول سازمان ديگر معرفي مي كنند، پس با سوال و جواب زيركانه ادعاي او را بررسي كنيد.
◆ اساس تخليه تلفني بر غفلت و فريب است، مواظب غفلت خود و فريبكاري دشمن باشيد.

◈روش تماس با افراد نخبه و علمی

برخي روش هايي كه منافقين، اخيراً از آنها در تماس با افراد نخبه و علمي كشور بهره برده اند، جهت بهره برداري اعلام مي شود:

◆ تماس گيرنده خود را با هويت فردي ديگر از مراكز علمي و پژوهشي يا رياست جمهوري يا وزارت علوم معرفي مي نمايد.
◆موضوع صحبت در محور برگزاري سمينار يا نشست علمي، ارائه مقاله، مصاحبه مطبوعاتي بوده و خواستار اطلاعات از مخاطب پيرامون افراد و پروژه هاي علمي و اداري مي گردند.
◆ مشخصات و شماره تماس افراد مختلف و اساتيد و پژوهشگران مرتبط با علوم فوق الذكر را خواستار مي گردند.
◆ مشخصات و شماره تماس افراد مرتبط با صنايع نظامي و يا دانشجويان دوره دكتري يا كارشناسي ارشد نظامي، شاغل به تحصيل در محيط هاي وزارت علوم را درخواست مي‌نمايند.
◆ مشخصات پروژه هاي مرتبط با پيشرفت هاي علمي و افراد فعال در آن را درخواست مي نمايند.
◆ فرد تماس گيرنده، نامه اي رسمي و جعلي به امضاي مقامي مسئول مي فرستد و خواستار ارسال اطلاعات خاص مي شود.

◈منبع: سايت وزارت اطلاعات

تلفن همراه | عابربانک | پیامک
سه‌ضلع کلاهبرداری

تلفن همراه، اس‌ام‌اس و عابربانک سه ضلع اصلی کلاهبرداری تلفنی است. برنده خوش‌شانس مسابقات رادیویی و تلویزیونی، برنده شدن سفر زیارتی به اماکن مقدس، برنده شدن در قرعه‌کشی بانک‌ها و موسسات مالی مواردی است که کلاهبرداری تلفنی برای فریب مال باختگان از آن استفاده می کنند.
شیادانی که با سوءاستفاده از ناآگاهی مردم خیلی راحت حساب‌های بانکی آنها را به بهانه‌های مختلف خالی می‌کنند. این شیادان به قدری حرفه‌ای عمل می‌کنند که اقشار مطلع و تحصیلکرده جامعه را هم به راحتی فریب می‌دهند.

◈طمع

حتما با تبلیغاتی نظیر برنده‌شدن در یک جشنواره ، زیر مجموعه‌گیری در شرکت های هرمی ، سرمایه گذاری با سود های رویایی آشنا هستید و حداقل یک بار راجع به آنها شنیده اید. اگر به طور مفصل تر همه این موارد را بررسی کنید متوجه خواهید شد که همه آنها از نقطه ضعف طمع در انسان‌ها استفاده می‌کنند. نقطه ضعفی که اگر به درستی تحریک شود می‌تواند میلیون ها تومان پول را فقط در عرض چند ثانیه به امید بدست آوردن چند هزارتومان به باد دهد!
پس بر طمع خود غلبه و آن را مدیریت کنید.

کسب و کار های زیادی بر پایه این طمع در دنیا بوجود آمده اند کسب و کارهایی نظیر کازینوها، لاتاری‌ها، شرکت‌های بازاریابی شبکه‌ای و ...، و اکثر این کلاهبرداران بر پایه طمع و با تحریک این ضعف انسان از آن کسب درآمد می کنند. و کلاهبرداری های تلفنی نیز از این امر مستثنا نیست.
بنابر این اگر نتوانید روی این حس به خوبی کار کنید، حتی در معامله و خرید و فروش هم به مشکل خواهید خورد!

◈روش کلاهبرداران

اصلی‌ترین روش این کلاهبرداران استفاده از عنوان‌های مختلف از جمله برنده شدن در مسابقات و قرعه‌کشی‌ها و یا معرفی خود بعنوان یکی از پرسنل مالی دانشگاه یا یک سازمان و ارگان دولتی می‌باشد. که در همه این موارد از افراد خواسته می‌شود که در کنار دستگاه عابر بانک حاضر شوند. حتی در برخی از موارد فرد کلاهبردار در ابتدای کار با ارائه شماره کارت سازمان های دولتی سعی در جلب اعتماد فرد می‌نماید که بایستی در این خصوص دقت شود.

اگر خوشبختانه تا بحال گرفتار این کلاهبرداران نشده اید، ابتدا فایل صوتی زیر را بشنوید (کدQR زیر را اسکن کنید) تا ببینید یک کلاهبرداری تلفنی تا چه حد می تواند دقیق انجام شود.

◈همه چیز زیر سر عابر بانک است!

اکثر کلاهبرداران تلفنی با همکاری خود فرد اقدام به کلاهبرداری می‌کنند! بنابراین توجه داشته باشید که اگر فردی می خواهد مبلغی را برای شما واریز کند به هیچوجه نیازی به حضور صاحب کارت و حساب در کنار دستگاه خودپرداز نیست.

> اگر فردی می خواهد مبلغی را برای شما واریز کند به هیچوجه نیازی به حضور صاحب کارت یا حساب در کنار دستگاه خودپرداز نیست.

◈فقط شماره حساب یا کارت

برای اینکه وجهی به حساب یا کارتتان واریز شود نیاز به ارائه اطلاعاتی بیش از شماره کارت یا حساب به افراد تماس گیرنده نیست، این موضوع را جدی بگیرید.

کلاهبرداری‌ها هرروزه شکل جدیدی به خود می گیرند. پس شما باید به شدت حواستان را جمع کنید، هر کجا مواردی نظیر قیمت ارزان‌تر، پول زیاد، برنده شدن، جایزه‌های میلیونی، قرعه کشی‌هایی با جایزه‌های رویایی، چندبرابر کردن تضمینی سرمایه و...، مواردی از این قبیل مشاهده کردید و از آن فاصله نگرفتید، آماده از دست دادن سرمایه خود باشید.

لذا ضروری است ضمن حفظ هوشیاری کامل در این خصوص از هرگونه همکاری با کلاهبرداران جدا خودداری نموده و مراتب را سریعا به مدیریت حراست دانشگاه اعلام نمایید.

جهت آشنایی با روش های این کلاهبرداران پیشنهاد می کنیم با اسکن کد QR زیر حتما داستان های واقعی بخش کلاهبرداری سایت مدیریت حراست را مطالعه کنید.

◈منابع:
◆سایت مدیریت حراست دانشگاه فردوسی
◆سایت ارزپلاس

چگونه امنیت گوشی هوشمند خود را بالا ببریم؟

امروزه اغلب تمام اطلاعات ارزشمند و غیرقابل جایگزین ما در همین دستگاه کوچک یعنی تلفن‌همراه ذخیره و نگهداری می‌شوند. با توجه به گسترش استفاده از تلفن‌همراه و نیاز به حفظ امنیت آن کمی از وقت خود را صرف یادگیری موارد ساده و در عین حال مهم مطرح شده در متن زیر کنید تا بتوانید به راحتی به حفاظت از گوشی خود بپردازید.

◈از رمزی ایمن برای قفل صفحه نمایش خود استفاده کنید

هنگامی که مجبورید گوشی خود را برای چند لحظه روی میز کارتان ترک کنید یا اگر گوسی‌تان به سرقت رفته است و یا آن را گم کرده اید؛ داشتن یک پسورد پیچیده برای قفل صفحه نمایش آن، ساده‌ترین راه برای محدود کردن دسترسی به تلفن همراه‌تان است. به طور کلی، داشتن یک پین‌کد تصادفی شش رقمی که شامل حروف و اعداد است، نیاز به دانش و ابزار مخصوصی برای دور زدن پسورد آن بدون فعال‌سازی تنظیمات خود تخریب تلفن دارد.

◈فقط برنامه‌های قابل اعتماد را نصب کنید

اگر شما از منبع دیگری جز نرم افزارهای مطمئن همچون کافه بازار یا گوگل‌پلی برای دانلود نرم افزار استفاده می‌کنید باید حتما گزینه «دانلود از منابع ناشناخته» در قسمت تنظیمات امنیت گوشی خود را فعال کنید البته گاهی گوگل پلی هم اجازه دانلود بدافزار ها را می دهد و باید مراقب باشید.
هرگز از سایت‌های جعلی و غیرمعتبر برنامه‌ای را دانلود نکنید و در هنگام دانلود حتما به آدرس منبع و لینک(URL) آن دقت کنید.

◈غیر فعال کردن اشکال زدایی USB

اشکال زدایی USb یا USB Debugging مربوط به کاربران پیشرفته می‌شود. در صورتیکه شما آشنایی کامل به این مورد دارید و به عنوان کاربر حرفه‌ای شناخته می شود این قسمت را فعال می کنید در غیر اینصورت لطفا این قسمت را غیر فعال کنید. که با این کار شما گوشی خود را از سوءاستفاده‌های بیرونی حفظ خواهید کرد. شما در کل نیازی فعال کردن این بخش از تنظیمات گوشی خودنیستید.

◈به درخواست مجوزهای برنامه‌ها هنگام نصب دقت کنید!

به عنوان مثال چرا باید برنامه چراغ قوه نیاز به دسترسی به فهرست دوستان شما داشته باشد؟ یا اینکه چرا برنامه ماشین حساب باید هنگام نصب از شما بخواهد تا امکان دسترسی به فیلم ها و عکس‌های گوشی شما داشته باشد؟ برنامه و نرم افزارهای مشکوک تلاش می‌کنند تا به لیست دوستان و مکان شما دسترسی پیدا کند. شما باید هنگام نصب برنامه‌ها دقت لازم را داشته باشید و در صورت انجام این کار سریعا برنامه‌های نصب شده غیر فعال و حذف شوند.

◈ اطلاعات خود را رمزنگاری کنید

شما می‌توانید حساب کاربری، تنظیمات، برنامه‌ها و داده‌های خود، آهنگ و دیگر فایل‌ها و برنامه‌های خود را رمزگذاری کنید. سیستم عامل اندروید این اجازه را در تنظیمات گوشی به شما می دهد. البته هیچ کس بدون داشتن اطلاع در مورد قفل صفحه اصلی و پسورد گوشی شما نمی تواند رمزگشایی برنامه های شما را انجام دهد به همین خاطر سعی کنید هیچوقت پسورد خود را فراموش نکنید.

◈از Wi-Fi های عمومی بپرهیزید

در مکان‌های عمومی که قصد استفاده از Wi-Fi را دارید جهت امنیت بیشتر از VPN استفاده‌کنید.
هکرها و کلاهبرداران اینترنتی با استفاده از اینترنت (Wi-Fi) محل‌های عمومی می‌توانند به اطلاعات گوشی شما دسترسی پیدا کنند. برخی از نرم‌افزارهای موبایل‌سکیوریتی به شما این امکان را می دهد که اطلاعات ورودی و خروجی گوشی همراه خود را با یک VPN مطمئن، قابل رمزگذاری و براحتی محافظت کنید.

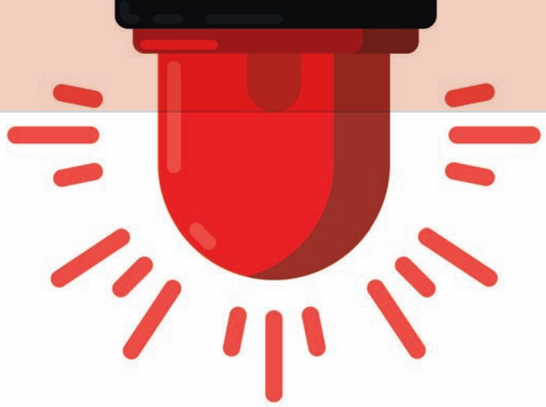
◈ از احراز هویت دو مرحله ای برای حساب های مجازی استفاده کنید

از احراز هویت دو مرحله ای برای حفاظت از حساب های کاربری خود در فضای مجازی استفاده کنید. همه حساب های آنلاین نیاز به استفاده از رمز عبوری قوی و احراز هویت دو مرحله‌ای در صورت ارائه دارند. هیچگاه از یک رمز عبور مشابه در چندین سایت یا حساب کاربری استفاده نکنید، بلکه یک نرم افزار مدیریت رمز عبور برای نگه‌داری آنها داشته باشید. استفاده از یک حساب متمرکز برای سایر حساب‌های اعتباری شما، کار خطرناکی است مگر اینکه که رمز عبوری قوی داشته باشید.

◈مراقب پیام های ناشناس باشید

هرگز یک لینک ناشناس یا پیام حاوی فایل‌های مشکوک را باز نکنید. پیش از این در سیستم عامل اندروید از فیلم‌های دستکاری شده برای نفوذ و رخنه امنیتی استفاده شده است. این فایل‌های آلوده قابلیت دسترسی به مجوزهای سطح بالای فایل‌های سیستمی را داشته اند، همچنین اسکریپتی شناسایی شده که می‌توانست نرم‌افزارهای مخرب را به راحتی نصب کند. دیده شده است که یک فایل JPG یا PDF، همین کار را در iPhone انجام داده است. هرچند رخنه‌های امنیتی مذکور به سرعت شناسایی و مسدود شده اند، اما نمی‌توان مطمئن بود که دیگر سوءاستفاده مشابهی صورت نگیرد.

◈منابع:
سایت نت نوشت، سایت آی‌پی پروتکت



هر جایی از جهان که باشید دسترسی به خدمات اضطراری مانند کمک‌های پزشکی، آتش‌نشانی و پلیس امکان‌پذیر است. مکان‌های مختلف در جهان شماره تماس‌های اضطراری مختلفی هم دارند.

به جای اینکه شماره های اضطراری را حفظ کنید و یا به شماره‌گیری بپردازید می‌توانید با ذخیره کردن آن و زدن یک دکمه به طور مستقیم ارتباط برقرارکنید.
نام این قابلیت Emergency SOS یا همان «تماس اضطراری» است. که امیدواریم هیچوقت از آن استفاده نکنید، اما به شما کارایی و نحوه استفاده از آن را توضیح میدهیم تا در زمان اضطراری و خطر از آن استفاده‌کنید.
در گوشی‌های همراه مختلف از جمله برندهایی همچون آیفون و سامسونگ این امکان برای مواقع اضطراری دیده شده است و با تنظیمات اولیه و درج شماره تلفن های دلخواه (به عنوان مثال مرکز پیام دانشگاه) در مواقع اضطراری و اتفاقات با فشردن چند باره کلید پاور امکان ارسال مختصات جغرافیایی و ارسال پیام تقاضای کمک وجود دارد.

با ذخیره کردن شماره مرکز پیام دانشگاه ۰۹۲۰۸۸۰۴۹۵۹ در بخش SOS گوشی خود، در موقع خطر ما را مطلع نمایید

حتی در برخی از برندها امکان ارسال تصویری از فرد با استفاده از دوربین جلو و عقب و همچنین ارسال صوت نیز وجود دارد و همه این پیام ها بصورت خودکار و فقط با فشردن یک کلید خاص امکان پذیر است و گوشی بصورت اتومات با فعال کردن GPS، عکس برداری و ضبط صدا و ارسال پیامک به شماره های ازپیش تعیین شده دیگران را از احوالات و موقعیت مکانی فرد مطلع می کند. ضمن اینکه در صورتیکه این امکان بر روی گوشی شما با برندهای مختلف وجود نداشت می‌توانید از نرم افزارهای مشابه کمک‌رسان با قابلیت‌های بسیار خوب بصورت رایگان استفاده نمایید. این نرم افزارها بصورت اتوماتیک مختصات جغرافیایی فرد را از GPS گوشی می‌گیرد و در صورت نداشتن قابلیت GPS، بصورت اتوماتیک از نزدیکترین دکل BTS یا شبکه های مخابراتی همراه اطراف، مختصات فرد را برای شماره‌هایی که در این نرم افزار از پیش تعیین شده است با استفاده از دیتای گوشی یا پیامک ارسال می کند. حتی در صورت نداشتن آنتن یا اعتبار سیم کارت، بصورت اتوماتیک با ۱۱۲ تماس می گیرند.

پیشنهاد می کنیم با اسکن کد QR زیر با نحوه فعال کردن این امکان در گوشی های دارای سیستم عامل اندروید و آی‌اواس در سایت مدیریت حراست آشنا شوید.

در مواقع اضطراری و خطر

چگونه مرکز پیام دانشگاه را مطلع کنیم؟

فصلنامه داخلی خبری و آموزشی

رصد

سال اول | پیش شماره ۱ | تابستان ۱۳۹۸

فصلنامه داخلی خبری و آموزشی «رصد»

سال اول - پیش شماره ۱ - مهرماه ۱۳۹۸

صاحب امتیاز: **مدیریت حراست دانشگاه فردوسی مشهد**

زیرنظر شورای سردبیری

با تشکر از: همکاران مدیریت حراست و اداره حفاظت فیزیکی و انتظامات

گرافیک و صفحه آرایی: مؤسسه صهبا رسانه

راه‌های ارتباطی: **رایانامه:** herasat@um.ac.ir **وبگاه:** herasat.um.ac.ir **تلفن:** ۰۵۱۳۸۸۰۲۲۹۸

اخبار

در پنج ماه نخست سال ۱۳۹۸؛

◈برقراری نظم و امنیت آزمون های علمی

برقراری نظم و امنیت توسط همکاران انتظامات جهت برگزاری ۲۸ مورد آزمون های علمی و استخدامی در تمامی دانشکده های دانشگاه با شرکت حدود ۴۹۱۰۰ داوطلب.

در پنج ماه نخست سال ۱۳۹۸؛

◈اعزام بیمار به مراکز پزشکی

هماهنگی جهت اعزام ۱۸۹ مورد بیمار به مراکز پزشکی به علت افت فشار و آسیب دیدگی جسمی، تنگی نفس، حمله عصبی، مسمومیت ، دل درد،سرماخوردگی، مصدومیت و غیره که از این تعداد ۱۵۵ مورد از مجموعه خوابگاهها و مابقی از دانشکده ها و مجموعه های دیگر دانشگاه بوده است. ضمن اینکه تعداد ٦٤ مورد از بیماران توسط اورژانس ۱۱۵ به مراکز درمانی سطح شهر اعزام شدند.

در پنج ماه نخست سال ۱۳۹۸؛

◈پیگیری رفع نواقص فنی

۳۳ مورد پیگیری رفع نواقص فنی در اتصال سیستم های اعلام سرقت، مشکلات قطعی برق، ترکیدگی لوله، خرابی آسانسور و غیره در سطح پردیس دانشگاه توسط همکاران اداره حفاظت فیزیکی و انتظامات که با حضور عوامل فنی مرتبط در اسرع وقت مشکل مرتفع گردیده است.

در پنج ماه نخست سال ۱۳۹۸؛

◈رسیدگی به سرقت‌ها

رسیدگی به ۲۷ مورد گزارش سرقت شامل اموال شخصی و اداری توسط اداره انتظامات که از این تعداد ۱۹ مورد کشف، سارق نیز شناسایی و اموال سرقتی تحویل مالکان گردید.

در پنج ماه نخست سال ۱۳۹۸؛

◈رسیدگی به تصادفات

وقوع ٤٤ فقره تصادف در سطح پردیس که در این خصوص ضمن حضور سریع و به موقع واحد های گشتی اداره انتظامات در محل، اطلاع رسانی لازم به عوامل راهور جهت بررسی صحنه تصادف نیز صورت پذیرفته است.

آیین‌نامه اجرایی قانون پیشگیری و مقابله با تقلب در آثار علمی تصویب شد

هیأت وزیران در جلسه روز چهارشنبه ۲۳ مرداد ۱۳۹۸ به ریاست حجت الاسلام والمسلمین حسن روحانی رئیس‌جمهوری، آیین‌نامه اجرایی قانون پیشگیری و مقابله با تقلب در تهیه آثار علمی را تصویب کرد.

بر اساس این تصویب نامه، تهیه، عرضه و یا واگذاری آثاری از قبیل رساله، پایان نامه، مقاله، طرح پژوهشی، کتاب، گزارش یا سایر آثار مکتوب پژوهشی - علمی و یا هنری اعم از الکترونیکی و غیرالکترونیکی توسط هر شخص به قصد انتفاع و به عنوان حرفه یا شغل - با هدف ارائه کل اثر و یا بخشی از آن توسط دیگری به عنوان اثر خود، جرم بوده و مرتکب یا مرتکبان علاوه بر واریز وجوه دریافتی به خزانه دولت مشمول مجازات می‌شود.

آیین‌نامه فوق با هدف برخورد با مراکز فروش پایان‌نامه، مقالات علمی و امثال آن و نیز با رویکرد پیشگیری و مقابله با تقلب علمی در سطح مؤسسه تهیه و تدوین شده است.

همچنین به موجب آیین نامه مذکور، افرادی که با ارائه پایان نامه جعلی موفق به دریافت مدرک تحصیلی شده‌اند، حتی پس از فراغت از تحصیل، مدرک تحصیلی حاصل از تقلب آنان بلااثر خواهد شد.

لازم به ذکر است در اجرای اصل ۱۲۳ قانون اساسی جمهوری اسلامی ایران «قانون پیشگیری و مقابله با تقلب در تهیه آثار علمی» در مورخ ۱۳۹۶/۰۵/۳۱ مجلس شورای اسلامی تصویب و در تاریخ ۱۳۹۶/۶/۸ به تایید شورای نگهبان رسیده بود.