✓کارنیل، بزرگترین شبکه موفقیت ایرانیان می باشد، که افرادی زیادی توانسته اند با آن به موفقیت برسند، فاطمه رتبه ۱۱ کنکور کارشناسی، محمد حسین رتبه۶۸ کنکور کارشناسی، سپیده رتبه ۳ کنکور ارشد، مریم و همسرش راه اندازی تولیدی مانتو، امیر راه اندازی فروشگاه اینترنتی،کیوان پیوستن به تیم تراکتور سازی تبریز، میلاد پیوستن به تیم صبا، مهسا تحصیل در ایتالیا، و..... این موارد گوشه از افرادی بودند که با کارنیل به موفقیت رسیده اند، شما هم می توانید موفقیت خود را با کارنیل شروع کنید.

برای پیوستن به تیم کارنیلی های موفق روی لینک زیر کلیک کنید.

www.karnil.com

همچنین برای ورود به کانال تلگرام کارنیل روی لینک زیر کلیک کنید.

https://telegram.me/karnil

ویژه پنجمین نمایشگاه رسانه های دیجیتال

هر آنچه که لازم است از توصیه‌های پلیس فتا به خاطر داشته باشید

پلیس فضای تولید و تبادل اطلاعات ناجا

هر آنچه که لازم است از توصیه‌های پلیس فتا به خاطر داشته باشید

یکی از دارایی‌های ارزش‌مند شما، اطّلاعاتی است که آن را مدیریت می‌کنید. چه اطّلاعات محرمانه‌ی سازمانی شما باشد یا اطّلاعات شخصی شما، هکرها می‌خواهند که به آن دست یابند. کار آن‌ها را آسان نکنید.

- هر اطّلاعاتی ارزشمند است و باید محافظت شود.
- به یاد داشته باشید که باید اطّلاعات خود را طبقه‌بندی کنید تا بتوانید سطح امنیتی مورد نیاز هر طبقه را مشخّص نمایید.
- اطّلاعات الکترونیک خود را با توزیع مناسب، رمزنگاری اطّلاعات، و استفاده از تدابیر امنیتی مناسب، حفاظت کنید.
- همان‌طور که برای امحاء کاغذهای حاوی اطّلاعات محرمانه، آن‌ها به دستگاه‌های خردکن می‌سپارید، اطّلاعات رایانه‌ای حسّاس را نیز با نرم‌افزارهای امحاء (شردر) از بین ببرید.

ارزیابی محرمانگی، تمامیت و دسترس‌پذیری اطّلاعات به شما کمک می‌کند تا تعیین کنید که چه سطحی از حفاظت مورد نیاز شماست.

- پیش از آن که وارد گفتگو پیرامون اطّلاعات محرمانه با شریک یا مشتریان خود شوید و این اطّلاعات را برای آن‌ها ارسال کنید، مطمئن شوید که شما یک قرارداد امضای شده‌ی عدم افشا دارید.
- هر فردی، نقش مهمّی در محافظت از اطّلاعات حسّاس دارد.
- انتشار اطّلاعات محرمانه در شبکه‌های اجتماعی اینترنتی، حتّی با رعایت سیاست‌های محرمانگی، باز هم به منزله‌ی افشای اطّلاعات است.
- جاسوس‌افزارها، در رایانه‌ها به دنبال اطّلاعات حسّاس می‌گردند. نرم‌افزارهای امنیتی را برای کاهش آسیب آن‌ها به کار گیرید.

هر آنچه که لازم است از توصیه‌های پلیس فتا به خاطر داشته باشید

امنیت پست الکترونیکی

پیام‌های با ارزش خود را حفظ کنید

پست الکترونیکی یک ابزار قوی و راحت برای تبادل اطّلاعات است. اطّلاعاتی که در یک پست الکترونیکی تبادل می‌شود، ممکن است دارای ارزش زیادی باشد که آن را به یک هدف برای هکرها تبدیل می‌کند. این توصیه‌ها را برای وقتی که از پست الکترونیکی استفاده می‌کنید به خاطر بسپارید.

- مطمئن شوید که پست الکترونیکی را برای افراد واقعی ارسال می‌کنید. قبل از آن که بر روی «ارسال» کلیک کنید، دوباره آدرس گیرنده را بازبینی کنید.
- وقتی از گزینه‌ی «ارسال به همه» استفاده می‌کنید، احتیاط کنید. مطمئن باشید که شما می‌خواهید همه‌ی کسانی که در لیست ارسال شما قرار دارند، پیام شما را دریافت کنند.
- مراقب کلاهبرداری‌های از طریق فیشینگ باشید. اگر شما پست الکترونیکیی دریافت کردید که از شما، شماره‌ی حساب، رمز عبور، پین یا رمز دوّم شما را درخواست کرد، از طریق سازمانی که به ظاهر ارسال‌کننده‌ی آن پست الکترونیکی است، فرستنده را احراز هویّت کنید. این‌گونه اطّلاعات را هرگز از طریق پست الکترونیکی ارسال نکنید.
- آنتی ویروس خود را به روز کنید و آن را طوری تنظیم نمایید که فایل‌های پیوست پست الکترونیکی را به صورت خودکار اسکن کند.
- همواره در هنگام ارسال پست الکترونیکی، آدرس گیرنده را دوباره کنترل کنید تا مطمئن شوید که اطّلاعات حسّاس را به افراد مربوطه ارسال می‌کنید.
- در موقع انتخاب سرویس‌دهنده‌ی پست الکترونیکی، سرویس‌دهنده‌ای را انتخاب کنید که به شما کمک می کند از دریافت پست الکترونیکی‌های ناخواسته (اسپم) جلوگیری کنید.
- هرگز به پست الکترونیکی‌های ناخواسته (اسپم) پاسخ ندهید و پست الکترونیکی‌هایی که حاوی ویروس هستند را بازفرست (فوروارد) نکنید. آن‌ها را پاک کرده و به دور اندازید.
- هرگز اطّلاعات محرمانه را در زمانی که از سرویس‌های رایگان پست الکترونیکی یا سرویس‌های عمومی مبتنی بر وب استفاده می‌کنید ارسال یا ذخیره نکنید. با استفاده از این پست الکترونیکی‌های مبتنی بر وب ممکن است به اندازه‌ی کافی در امنیت نباشید.

CYBER POLICE
پلیس فتای تولید و تبادل اطلاعات ناجا

هر آنچه که لازم است از توصیه‌های پلیس فتا به خاطر داشته باشید

امنیت پیام‌رسان‌ها (مسنجرها)

از آسودگی خود لذّت ببرید، امّا احتیاط کنید

پیام‌رسان‌های فوری (مسنجرها) یک ابزار پرطرفدار برای ایجاد ارتباطات سریع هستند. با این‌حال برخی از تهدیدها در استفاده از پیام‌رسان‌ها وجود دارد. این تهدیدها را به یاد سپارید:

- ارتباطات پیام‌رسان‌ها، رمزنگاری نمی‌شوند. از پیام‌رسان‌ها برای ارسال اطّلاعات محرمانه استفاده نکنید. زیرا ممکن است دیگران قادر به شنود مکالمه متنی یا صوتی و تصویری شما باشند.
- در رابطه با هرگونه فایلی که از طریق پیام‌رسان‌ها دریافت می‌کنید، احتیاط کنید. تنها دریافت فایل از کسانی را بپذیرید که آن‌ها را می‌شناسید و همیشه فایل‌ها را پیش از گشودن، با آنتی ویروس اسکن کنید.
- از رمزهای عبور قوی برای حساب کاربری پیام رسان خود استفاده کنید.
- اطّلاعات شخصی زیادی را در پروفایل حساب کاربری پیام‌رسان خود قرار ندهید. دیگران ممکن است از این اطّلاعات برای هدف قراردادن شما استفاده کنند.
- مطمئن شوید که از آخرین نسخه‌ی نرم‌افزار پیام‌رسان خود استفاده می‌کنید.
- هیچ‌گاه از پیام‌رسان‌ها برای بحث پیرامون موضوعات محرمانه، شخصی یا کاری استفاده نکنید.
- از کدهای مخرّب و مهندسین اجتماعی در زمانی که از نرم‌افزارهای پیام‌رسان استفاده می کنید برحذر باشید.
- از اکانت پیام‌رسان و رمز عبور خود مراقبت کنید. همیشه نرم‌افزار پیام‌رسان خود را به روز نگه‌دارید و به صورت مرتّب رمز عبور خود را تغییر دهید.
- هرگز برنامه‌های نرم‌افزاری را از منابع غیرقابل اعتماد دریافت نکنید و همیشه آنتی‌ویروس خود را به روز نگه دارید.
- هرگاه که فعّالیّت خود در پیام‌رسان را به پایان بردید، از آن خارج شوید (لوگ آف کنید).

هر آنچه که لازم است از توصیه‌های پلیس فتا به خاطر داشته باشید

مهندسی اجتماعی

فریب اطّلاعات آشکار را نخورید

مهندسین اجتماعی، فریب‌کاران هنرمندی هستند که می‌خواهند شما را فریب دهند تا اطّلاعات شخصی یا محرمانه‌ی خود را در اختیار آن‌ها بگذارید. بیاموزید که چگونه ترفندهای مشترک مهندسین اجتماعی را شناسایی کنید تا به دام آن‌ها نیافتید.

- مهندسی اجتماعی، هنر دستکاری در اختیارات افراد برای گرفتن اطّلاعات یا انجام کارهایی است که آن‌ها به طور عادّی انجام نمی‌دهند.
- مهندسین اجتماعی با استفاده از غفلت انسان‌ها (عدم اطّلاع)، ساده‌لوحی، تمایل به دوستی و تمایل آن‌ها به کمک به دیگران، طعمه‌های خود را انتخاب می‌کنند.
- درباره‌ی آن‌چه به غریبه‌ها می‌گویید احتیاط کنید. ممکن است آن‌ها، همان کسانی نباشند که ادّعا می کنند.
- از افرادی که تلاش می‌کنند تا بدون نشان وارد ساختمان شما شوند، برحذر باشید. هر غریبه‌ای را که در محیط‌های صرفاً اداری خود مشاهده کردید، بیرون کنید.
- در برابر ایمیل‌هایی که از شما اطّلاعات صحیح شخصی یا محرمانه‌تان را سوال می‌کند، احتیاط کنید، اگر شک کردید، منبع ارسال را چک کنید.
- اطّلاعات ضبط شده در ایمیل یا ایمیل صوتی خود که در خارج از محیط اداری ضبط کرده‌اید را محدود کنید. مهندسین اجتماعی می‌توانند از این اطّلاعات استفاده کرده، با فریب هم‌کلاسی‌ها یا همکاران شما، اطّلاعات محرمانه را کسب کنند.
- اگر مشکوک به این هستید که اطّلاعات شخصی شما به خطر افتاده است، سریعاً با بانک یا شرکت صادرکننده‌ی کارت اعتباری خود تماس بگیرید.
- از غریبه‌هایی که اطّلاعات با جزئیاتی از کار شما را سؤال می‌کنند، بر حذر باشید. ممکن است آن‌ها در پی فریب‌دادن شما برای کسب اطّلاعات محرمانه‌ی شما باشند.

هر آنچه که لازم است از توصیه‌های پلیس فتا به خاطر داشته باشید

امنیت مرورگرهای وب

در وب گسترده جهانی در امنیت باشید

مرورگرهای وب شما را قادر می‌سازند که به وب گسترده‌ی جهانی دسترسی داشته باشید تا به مقادیر زیادی از اطّلاعات دست یابید. امّا همه‌ی وب‌سایت‌ها سالم نیستند. دانستن برخی از تهدیدهای ذاتی وب گسترده‌ی جهانی، به شما کمک خواهد کرد تا از سرقت هویّت یا استفاده‌ی غیرمجاز از رایانه‌تان در امان باشید:

- مطمئن شوید که از آخرین نسخه‌ی مرورگر وب خود استفاده می‌کنید و تنظیمات حسّاس امنیتی و محرمانه را فعّال ساخته‌اید. همچنین آخرین به روزرسانی‌ها و اصلاحیه‌ها را اعمال کرده‌اید.
- کوکی‌ها و زبان‌های اسکریپت‌نویسی را بدون آن‌که هدف آن‌ها را بدانید، تایید نکنید.
- از نام‌های کاربری و رمزهای عبور متفاوت برای سایت‌های مختلف یا حساب‌های کاربری خود استفاده کنید. این امر کمک می‌کند تا اطمینان حاصل کنید که اگر یک حساب کاربری شما به خطر افتاد، بر روی سایر حساب های کاربری شما، تاثیری نخواهد گذاشت.
- بیانیه‌ی محرمانگی وب سایت را پیش از آن‌که اطّلاعات شخصی‌تان را در اختیار آن بگذارید، وارد کنید چرا که در این صورت می‌دانید که وب‌سایت با اطّلاعات شما چه خواهد کرد.
- قبل از این که اطّلاعات حسّاس را در وب‌سایتی وارد کنید، به دنبال آیکن قفل یا عبارت https:// در نوار آدرس بگردید تا امنیت آن را احراز کنید.
- تمام فایل‌های دانلود شده را قبل از بازکردن آن، اسکن کنید.

هر آنچه که لازم است از توصیه‌های پلیس فتا به خاطر داشته باشید

رمز عبور، خطّ مقدّم دفاعی شما در حفاظت از اطّلاعات ذخیره‌شده است. مطمئن شوید که از رمزهای عبور قوی استفاده می‌کنید و با هوشیاری آن را حفظ کنید.

- رمز عبور مکانیزم احراز هویّت و اعتبار کاربر است.
- رمز عبور، شناسه‌ی الکترونیکی شخصی شماست که باید محافظت شود.
- از رمزهای عبوری استفاده کنید که حدّاقل شامل ۸ کاراکتر بوده و ترکیبی از حروف کوچک و بزرگ، اعداد، کاراکترهای ویژه و سمبل‌ها باشند.
- از رمزهای عبور پیش‌گزیده و تکراری استفاده نکنید.
- هیچ‌وقت رمزهای عبور خود را در جایی یادداشت نکنید. اگر نیاز به ذخیره‌سازی آن‌ها دارید، به نحوی رمزها را پنهان‌نگاری کنید که غیر قابل دسترس باشند.
- رمز عبور خود را با دیگران به اشتراک نگذارید. هرگز رمز عبور خود را به هیچ کس واگذار نکنید.
- از عباراتی که به شما کمک می‌کنند تا رمزهای عبور قوی‌ای که ساخته‌اید را به خاطر بسپارید، استفاده کنید.
- رمز عبور خود را به طور مرتّب تغییر دهید. حدّاقل هر ۹۰ روز یک‌بار این کار را انجام دهید.

هر آنچه که لازم است از توصیه‌های پلیس فتا به خاطر داشته باشید

با ظهور وب ۲.۰ و توسعه‌ی سرویس‌های جدید، سیستم‌هایی برای به اشتراک‌گذاری اطّلاعات شخصی و گروهی به وجود آمده است. شبکه‌های اجتماعی، سیستم‌های اشتراک گذاری (Sharing) عکس، ویدئو و سایر محتواها، دائرةالمعارف‌ها (ویکی‌ها)، سیستم‌های اشتراک‌گذاری فایل Peer2Peer، تورنت‌ها، سرویس های جانمایی مثل گوگل ارت، ویکی‌مپیا و بسیاری دیگر از سرویس‌های اینترنتی مبتنی بر به اشتراک گذاری اطّلاعات، این امکان را به شما می‌دهند که منابع مشترکی را با دیگران ایجاد کنید. در صورتی که مسائل و الزامات امنیتی و اصول محرمانگی در این اشتراک‌گذاری‌ها رعایت نشود، متاسّفانه آسیب‌های جدّی در حوزه‌های فردی، اجتماعی و خانوادگی به وقوع خواهد پیوست. موارد ذیل را در به اشتراک‌گذاری اطّلاعات و منابع به خاطر بسپارید:

- عکس‌ها، ویدئوها و سایر اطّلاعات شخصی را تنها با کسانی به اشتراک بگذارید که درجه‌ی اعتماد بالایی به آن‌ها دارید. در صورتی که در شبکه‌های اجتماعی، این موارد را به اشتراک می‌گذارید، نسبت به تنظیمات محرمانگی (Privacy) خود اقدام کنید.
- اطّلاعات مکانی شما، مورد علاقه‌ی سارقان است. زمانی که از دستگاه‌های رایانه‌ای همراه مجهّز به GPS، نظیر برخی از تلفن‌های همراه و تبلت‌ها استفاده می‌کنید و در مکانی خارج از محلّ کار یا محلّ زندگی، مثلاً در مسافرت هستید، اطّلاعات مکانی خود را در سیستم‌های جانمایی مثل گوگل‌مپ یا گوگل‌ارت به اشتراک نگذارید. در غیر این صورت، سارق یا سارقان به خالی بودن منزل یا محلّ کار شما پی می‌برند.
- سیستم‌های به اشتراک گذاری اطّلاعات مکانی نظیر گوگل‌ارت و ویکی‌مپیا می‌توانند مورد استفاده‌ی سیستم‌های جاسوسی دشمن نیز قرار گیرند. جانمایی اماکن حیاتی و حسّاس نظیر اماکن سیاسی و نظامی، خدماتی، فرهنگی، اقتصادی و اجتماعی، اطّلاعات ذی‌قیمتی را برای دشمن فراهم می‌کند و فرد را بی‌آن که خود بخواهد به یک جاسوسِ خائن تبدیل می‌کند.
- برای تبه‌کارانی که از مهندسی اجتماعی برای مقاصد مجرمانه خود استفاده می‌کنند، هیچ اطّلاعاتی ارزشمندتر از اطّلاعات دسته اوّلی که خود کاربران به اشتراک گذاشته‌اند نیست.
- بسیاری از فایل‌هایی که در سیستم‌های تورنت و Peer2Peer به اشتراک گذاشته می‌شوند به انواع ویروس‌ها، تروجان‌ها و سایر بدافزارها آلوده‌اند. در صورت دانلود این گونه فایل‌ها، آن‌ها را با نرم‌افزارهای امنیتی چک کنید.
- عکس‌ها و ویدئوهای شخصی و خانوادگی را در سایت‌های به اشتراک‌گذاری منتشر نکنید. زیرا در این صورت دیگر شما صاحب آن‌ها نیستید. این‌گونه محتواها به سرعت توسّط مجرمین اخلاقی منتشر می‌شوند.

هر آنچه که لازم است از توصیه‌های پلیس فتا به خاطر داشته باشید

هک و نفوذ به سامانه‌های رایانه‌ای و مخابراتی با نیّت و قصد مجرمانه‌ای که در قانون جرایم رایانه‌ای تعریف شده‌است، جرم تلقّی می‌شود و مجازات دارد. امّا بسیاری از افراد خصوصاً نوجوانان و جوانان، از روی کنجکاوی و با استفاده از برخی نرم‌افزارها و تکنیک‌ها، به این امر اقدام می‌کنند. این افراد بایستی بدانند که در بیشتر موارد اقدام آنان جرم تلقّی شده و در صورت شناسایی پلیسی و برخورد قضایی مجازاتی را برای آنان در پی دارد، و از آن پس یک فرد «سابقه‌دار» محسوب شده و در آینده از بسیاری از امتیازات اجتماعی نظیر ادامه تحصیل، اشتغال و ... محروم خواهند بود. نکات ذیل تذکّراتی به این قبیل ماجراجویان و نیز سایر کسانی است که ممکن است قربانی این کنجکاوی‌ها شوند.

- ورود به سامانه‌های رایانه‌ای و مخابراتی به منظورهای مختلف، نخست عملی غیر اخلاقی محسوب می‌شود. همانطور که بالارفتن از دیوار خانه‌ی مردم و سرقت در فضای واقعی مذموم است، سرقت دارایی‌های رایانه‌ای نیز جرم اخلاقی و جرم قانونی محسوب می‌شود.
- خرید و فروش باگ‌ها و اطّلاعات منافذ کشف شده‌ی سایت‌های اینترنتی، خصوصاً سایت‌های مهم و حسّاس و ارائه‌ی راهنمایی در این خصوص در انجمن‌ها، اطاق‌های گفتگو و شبکه‌های اجتماعی، خرید و فروش نرم‌افزارهای غیرقانونی هک و کرک و استخدام افراد برای اقدام به هک و کرک، جرم محسوب شده و پلیس با شناسایی این دسته از افراد با آنان برخورد قانونی خواهد کرد.
- بسیاری از والدین تصوّر می‌کنند که بزه و تخلّف اجتماعی جوانان و نوجوانان، جایی خارج از چارچوب خانه و خانواده اتّفاق می‌افتد و بنابر این اگر فرزند نوجوان کنجکاو آن‌ها در خانه و با رایانه و اینترنت نسبت به هک و نفوذ اقدام کند، مجرم نیست و از این رو در برابر اقدامات پلیس و تصمیمات دستگاه قضایی مقاومت می‌کنند. لذا بایسته است والدین نسبت به فعّالیّت های خانگی درخانه‌ی فرزندانشان حسّاسیّت بیشتری به خرج دهند.
- افزایش امنیت سخت‌افزاری و نرم‌افزاری رایانه و سیستم‌های رایانه‌ای و اینترنتی یک اصل اساسی در فضای مجازی است. لذا برای جلوگیری از آسیب‌های ناشی از هک و نفوذ، مدیران سامانه‌های رایانه‌ای و مخابراتی و افراد بایستی با استفاده از تدابیر امنیتی مناسب نسبت به حفظ سامانه‌های خود اقدام کنند. شایان ذکر است که قانون بر «تدابیر امنیتی» تاکید ویژه ای دارد و از این رو مدیران سامانه‌هایی که تدابیر امنیتی را لحاظ نکرده باشند، نیز باید در برابر قانون پاسخگو باشند.
- تدابیر امنیتی شامل کلّیه‌ی اقدامات فنّی مثل استفاده از آنتی‌ویروس‌ها و فایروال‌ها، سرورهای بک‌آپ و نیز تعیین سطح دسترسی کاربران و اقدامات محیطی در ایمن‌سازی و به‌سازی مکانی محل نصب و خدمات‌دهی سامانه‌های رایانه‌ای است.

هر آنچه که لازم است از توصیه‌های پلیس فتا به خاطر داشته باشید

امنیت خریدهای آنلاین

لذّت خرید آنلاین با دقّت و احتیاط

خرید آنلاین کالاها و خدمات، از با ارزش‌ترین خدماتی است که بر روی اینترنت ارائه می‌شود. این امر علاوه بر صرفه‌جویی در وقت کاربران، مزایایی چون افزایش امنیت در جابجایی پول، کاهش هزینه‌های بازاریابی، صرفه‌جویی اقتصادی و افزایش فرصت‌های شغلی و کارآفرینی را به دنبال دارد. امّا در عین حال کلاهبرداران فضای مجازی نیز با استفاده از عدم اطّلاع یا کم‌دقّتی خریداران و مشتریان، آن را با تهدیدها و آسیب‌هایی مواجه ساخته‌اند. نکات ذیل را در هنگام خریدهای الکترونیکی در نظر داشته باشید.

- اوّلین پیش‌فرض برای حقیقی و سالم بودن خدمات یک فروشگاه الکترونیک، این است که کالاهای مجاز ارائه می‌کند. بنابر این فروشگاه‌هایی که کالاهای غیرمجاز به فروش می‌رسانند، با احتمال بسیار بالا، به قصد کلاهبرداری به وجود آمده‌اند.
- در هنگام تصمیم به خرید از فروشگاه‌های الکترونیکی، از تجربه‌ی دوستان و آشنایان نزدیک در خصوص خریدهای آنلاین استفاده کنید و از فروشگاه‌هایی که سابقه‌ی ارائه‌ی خدمات مطلوب دارند، خرید کنید.
- صفحاتی که ناخواسته در برابر شما باز می‌شوند و حاوی تبلیغات فروش کالاها و ارائه‌ی خدمات هستند، ممکن است تقلّبی بوده و قصد کلاهبرداری داشته باشند.
- سعی کنید در هنگام خرید آنلاین، با روش‌هایی نظیر گرفتن Who is از دامنه‌ی سایت اینترنتی فروشگاه، یا جستجو در انجمن هایی که اعضای آن‌ها، تجربیات خرید آنلاین خود را برای اطّلاع سایر اعضا می‌نویسند، از مدیر و گردانندگان فروشگاه، احراز هویّت کنید.
- در هنگام خرید آنلاین و در زمانی که پس از انتخاب کالا به درگاه پرداخت الکترونیکی بانک رهنمون می‌شوید، دقّت کنید که حتماً آدرس صفحه‌ی درگاه پرداخت الکترونیکی، متعلّق به همان بانکی باشد که آرم و لوگوی آن را در صفحه مشاهده می‌کنید.
- در بعضی از مواقع کلاهبرداران با جعل صفحات درگاه پرداخت الکترونیکی بانک‌ها، شما را به صفحاتی هدایت می‌کنند که آدرسی بسیار شبیه آدرس بانک اصلی دارند. در صورت عدم دقّت خریدار و ورود اطّلاعات کارت بانکی خود شامل شماره‌ی کارت، رمز عبور، CVV2 و تاریخ انقضای کارت، این اطّلاعات را در سیستم خود ثبت کرده و عملاً امکان هرگونه اقدامی را با حساب و موجودی قربانی دارند.
- سیستم پرداخت الکترونیکی همه‌ی بانک‌ها از SSL و روش‌های مطمئن رمزنگاری استفاده می‌کند. دقّت کنید که در نوار آدرس کنار آدرس اینترنتی صفحه‌ی پرداخت بانک، نماد یک قفل یا عبارت https:// درج شده باشد. در غیر این صورت قطعاً صفحه جعلی است و قصد به سرقت بردن اطّلاعات کارت بانکی شما را دارد.
- مرکز توسعه‌ی تجارت الکترونیکی وزارت بازرگانی، با همکاری نیروی انتظامی جمهوری اسلامی ایران در جهت افزایش امنیت خدمات تجارت الکترونیک، اعطای نماد اعتماد الکترونیکی به فروشگاه‌های الکترونیک را آغاز کرده‌است تا خریداران به راحتی و با آسودگی خاطر خرید خود را انجام دهند. ترجیحاً از فروشگاه‌هایی که دارای این نماد هستند، خرید کنید.

هر آنچه که لازم است از توصیه‌های پلیس فتا به خاطر داشته باشید

امنیت تلفن‌های همراه

به همراه خود به سادگی اعتماد نکنید

امروزه تلفن همراه، همگانی‌ترین ابزار رایانه‌ای و ارتباطی است به نحوی که تقریباً همه‌ی افراد، لااقل یک گوشی تلفن همراه را با خود دارند. گوشی‌های تلفن همراه در سال‌های گذشته از یک گوشی صرف، به رایانه‌ای با امکانات فراوان ارتباطی در اندازه‌ای کوچک تبدیل شده‌اند. همین ویژگی‌های ممتاز و جالب توجّه تلفن‌های همراه، آن را به هدفی تازه برای مجرمان و تبه‌کاران تبدیل کرده است. رعایت نکات ذیل، می‌تواند استفاده از تلفن همراه را برای شما، به تجربه‌ای سودمند و جذّاب تبدیل کند.

- تمام نکات امنیتی که برای رایانه‌ها ذکر می‌شود، تقریباً برای تلفن‌های همراه هم کاربرد دارد. بیشتر تلفن‌های همراه از سیستم‌های عامل مخصوص ابزارهای همراه استفاده می‌کنند و تقریباً فرمت بیشتر فایل‌های رایانه‌ای را تشخیص می‌دهند. بنابر این برخی ویروس‌ها و بدافزارها نیز در تلفن‌های همراه اثر می‌کنند. دقّت در انتقال فایل‌های رایانه‌ای و استفاده از آنتی‌ویروس های مخصوص موبایل برای در امان ماندن از آسیب‌ها و تهدیدها را جدّی بگیرید.
- گوشی‌های تلفن همراه مجهّز به امکانات ارتباطی متنوّعی مثل وای‌فای، بلوتوث و اینفرارد هستند. در هنگامی که از این امکانات ارتباطی استفاده نمی‌کنید، آن‌ها را غیر فعّال کنید. مجرمان قادر هستند تا با هک و نفوذ به گوشی شما، اختیار آن را در دست گرفته، ضمن برقراری تماس‌های تلفنی به حساب شما، اطّلاعات و محتواهای درون گوشی شما را به سرقت برند.
- اطّلاعات محرمانه، عکس‌ها و ویدئوهای شخصی و خانوادگی خود را بر روی گوشی خود نگه‌داری نکنید.

  در هنگام خرابی گوشی تلفن همراه خود، حتّی‌الامکان پس از تخلیه‌ی کامل اطّلاعات و محتواهای موجود در آن، برای تعمیر به تعمیرکاران مجرّب و قابل اعتماد مراجعه کنید.
- احتمال گم شدن یا به سرقت رفتن تلفن‌های همراه، بیشتر از سایر ابزارهای رایانه‌ای است. از این رو، اطّلاعات و محتواهای ذخیره‌ی شما در آن، در معرض خطر و آسیب‌های جدّی ناشی از دسترسی سارق به آن‌ها قرار دارد.
- تلفن‌های همراه دارای قابلیت‌هایی هستند که می‌توانند به عنوان ابزارهای جاسوسی مورد استفاده قرار بگیرند. بنابراین در اماکن مهم و حسّاس، به توصیه‌های امنیتی مبنی بر عدم استفاده از تلفن‌های همراه توجّه کنید.
- به پیامک‌هایی که به شیوه‌های مختلف مثل اعلام برنده‌شدن شما در مسابقات و قرعه‌کشی‌ها، امور خیریه و مواردی از این دست، اطّلاعات شما نظیر اطّلاعات کارت بانکی شما را درخواست می‌کنند، اعتماد نکرده و به آن‌ها پاسخ ندهید.

هر آنچه که لازم است از توصیه‌های پلیس فتا به خاطر داشته باشید