اگر می خواهید گرفتار کلاهبرداری اینترنتی نشوید این کتاب را حتماً بخوانید

چگونه در اینترنت سَرمان کلاه نرود !

(همه چیز درباره کلاهبرداری های اینترنتی)

مجموعه ای از اطلاعات مفید و کاربردی شامل :

- نکته ها ، هشدارها و مثال ها در مورد کلاهبرداری های اینترنتی
- روش های کلاهبرداری رایج اینترنتی در ایران ...
- کلاهبرداری از طریق ترفندهای افزایش شارژ...
- روش های کلاهبرداری در شبکه‌های اجتماعی...
- کلاهبرداری از افراد جویای کار ...
- کلاهبرداری فیشینگ چیست؟
- چگونه یک سایت فیشینگ را بشناسیم؟ تصویری
- چگونه یک فروشگاه اینترنتی قابل اعتماد را تشخیص دهیم؟
- برخی معیارهای اعتبار سنجی برای فروشگاه های اینترنتی
- خرید از فروشگاه های اینترنتی
- امنیت در خریدهای اینترنتی
- اگر از کافی نت استفاده می کنید این نکات را به خاطر بسپارید
- ۶۹ نکته امنیتی بانک مرکزی برای استفاده از خدمات بانکداری الکترونیک
- و مطالب مفید دیگر ...

گردآوری و تنظیم کننده : رضا فریدون نژاد
WWW.DZBOOK.IR

سلام ؛

کتاب شماره ۱۵ از **مجموعه دانش و زندگی** ، با عنوان **چگونه در اینترنت،سَرمان کلاه نرود!** را تقدیم به شما خواننده محترم می نمایم .امیدوارم این کتاب مورد استفاده شما قرار بگیرد.

" کتابهای الکترونیکی دانش و زندگی را به دوستانتان معرفی کنید "

" کاربر محترم ، هر زمان که کتابهای دانش و زندگی را دانلود و مطالعه نمودید نظر خود را درباره همان کتاب و یا دیگر کتابها به من اعلام نمایید (از نظر مفید بودن مطالب ارائه شده،موضوعات انتخاب شده،داشتن طراحی جلد مناسب،روان و قابل فهم بودن متن کتاب و ...) ، **منتظر نظرات ، پیشنهادات و انتقادات سازنده شما عزیزان هستم"**

نظر شما در مورد این کتاب و دیگر کتابهای ارائه شده چیست؟

www.dzbook.ir

rezaf1390@gmail.com

با آرزوی موفقیت و سلامتی برای شما

رضا فریدون نژاد

مقدمه

در این کتاب قصد دارم شما را با پدیده شوم **کلاهبرداری های اینترنتی** بوسیله آگهی های کاذب ، خرید از فروشگاه های کلاهبردار ، پرداخت های اینترنتی ، صفحات جعلی و موارد مشابه آشنا نمایم ، بحث کلاهبرداری اینترنتی موردی است که متاسفانه اکثر ما آن را جدی نمی گیریم و یا تصور میکنیم این اتفاق فقط برای دیگران رخ می دهد ! ولی اینطور نیست ، اگر کوچکترین غفلتی بکنیم قربانی بعدی کلاهبرداری اینترنتی خودمان هستیم ، پس این کتاب را فقط نخوانید ، بلکه به هشدارها و نکته های ارائه شده توجه نمایید و آنها را به کار بگیرید تا **در اینترنت سرتان کلاه نرود !**

در کنار گسترش روز افزون کاربران اینترنت و همچنین تسهیل شدن امور عادی بشر بواسطه استفاده از اینترنت، همواره مجرمین با سوء استفاده از اعتماد عمومی مردم و گاهی ساده لوحی افراد و با تطبیق خود با ویژگی‌های محیط و ابزار روز، در جهت اقدامات و اهداف مجرمانه حرکت می‌کنند. در کنار سو استفاده ها و جرایم سایبری در حوزه اجتماعی و سیاسی، جرایم سایبری در حوزه اقتصادی پیشرفت‌های قابل توجهی به خود دیده است .بهترین راهی که می توان از کلاهبرداری و ضررهای دیگر در امان ماند **آگاهی و دانش بیشتر برای استفاده از تکنولوژی‌های روز دنیا است** .همانطور که می‌دانیم روز به روز شمار افرادی که قربانی فریب‌های اینترنتی می شوند افزایش می یابد. **فقط کافیست نگاهی به عناوین زیر بیندازید :**

سوءاستفاده دختر جوان از حساب اینترنتی پدرش ، سوءاستفاده از اعتماد با دزدی از حساب بانکی اینترنتی ، سرقت ۹۶ میلیونی برای پرداخت قبوض دیگران ، سرقت میلیاردی از حساب برای خرید طلا ، سرقت اینترنتی عروس از پدرشوهرش ، برداشت از حساب مادر برای خرید و فروش شارژ ، طلبکاری که سارق اینترنتی شد، کلاهبرداری اینترنتی با وعده ازدواج ، خرید شارژ از حساب بانکی دیگران ، کلاهبرداری یک مرکز خدمات اینترنتی از مشتری ، سارق اینترنتی به حساب پدرش هم رحم نکرد، متصدی کافی‌نت سارق اینترنتی از آب درآمد ، کلاهبرداری اینترنتی با وعده استخدام ، کلاهبرداری اینترنتی با وعده سی دی کسب درآمد کلان و . . . این عناوینی که خواندید فقط نمونه های کوچکی بودند که متاسفانه روزانه اکثر این اتفاقات را می شنویم یا می خوانیم و شاید خودمان قربانی بعدی این اتفاقات باشیم ! روز به روز بر قربانیان فریب‌های اینترنتی افزوده می‌شود و تعداد بیش‌تری پول‌های خود را از دست می‌دهند ،تمام این اتفاقات به دلیل غفلت ، سادگی ، اعتماد بیش از حد و ناآگاهی افراد ، پیش می آید.

با توجه به اهمیت موضوع، هشدارهای نهادهای مسئول به خصوص پلیس فضای تولید و تبادل اطلاعات (پلیس فتا) درباره انواع جرایم سایبری، می تواند به هشیاری افراد کمک نماید.

فضای مجازی نیز مانند فضای واقعی، آدم ها و شگردهای خاص خودش را دارد، این فضا همان قدر که با ابزارهایش به آسان تر انجام شدن کارها کمک می کند، با همین ابزارها نیز می تواند باعث شود عده ای در این فضا کلاهبرداری با شیوه های جدید انجام دهند و ما را در دام بیندازند!این چیزی است که خواه ناخواه

در دنیا وجود دارد، اما فایده های فضای مجازی آنقدر زیاد است که نمی توانیم حتی با وجود خطر کلاهبرداری در این فضا از آن صرف نظر کنیم. پس هر کدام از ما باید برای مراقبت از خود شیوه های این افراد را تا حدودی بشناسیم تا در دام آنها گرفتار نشویم.اولین کاری که یک کلاهبردار اینترنتی انجام می دهد، جلب اعتماد است. او سعی می کند طوری برخورد یا شرایط را مهیا کند که شما به او اطمینان کنید و مطابق نقشه او پیش بروید.

حتما قبل از اتصال به اینترنت این نکات را به یاد داشته باشید

۱.معمولا کلاهبرداری ها با تماس کلاهبردار آغاز می شود، مثلا برای شما ایمیل یا پیامک می فرستند یا حتی ممکن است به شما زنگ بزنند. در این موارد فرد با جعل یا شبیه سازی اطلاعات خود از ایمیلی که متعلق به او نیست یا آدرس های بسیار مشابه استفاده می کند و از شما درخواست هایی مانند واریز پول به یک شماره حساب یا دادن شماره کارت بانکی یا رمز حساب یا اطلاعات مشابهی را می نمایند. در این موارد حتما شما مجدد با اطلاعاتی که خودتان دارید با تماس گیرنده ارتباط برقرار کنید و هویت تماس گیرنده را بررسی کنید و به یاد داشته باشید بانک ها و شرکت های معتبر از ایمیل های عمومی مانند yahoo و gmail برای ارسال ایمیل استفاده نمی کنند. شماره های موبایل اعتباری و در بعضی مواقع ایرانسل نیز معمولا نشانه خوبی نیستند.

۲.مواظب آدرس های مشابه باشید، بسیاری از کلاهبرداری ها، با استفاده از آدرس های بسیار مشابه آدرس های اصلی انجام می شود. پس حتما آدرس سایت هایی را که در آنها اطلاعات وارد می کنید، با دقت بررسی کنید مخصوصا اگر لینک آنها را با ایمیل برای شما فرستاده اند

۳.گول ایمیل هایی که ادعا می کنند شما برنده جایزه شده اید و برای دریافت جایزه خود باید مبلغی را به شماره حسابی واریز کنید را نخورید.

۴.اگر شما با کسانی کار می کنید و آنها از طریق ایمیل برای شما فاکتورهایشان را ارسال می کنند، بسیار در معرض خطر هستید! حتما اطلاعات حساب فروشنده را هر بار با او از طریق دیگری غیر از ایمیل هم کنترل کنید.

۵.هیچ فایلی را از ایمیل بدون داشتن یک آنتی ویروس مطمئن و به روز شده دریافت نکنید، زیرا بسیاری از کلاهبردارها، با جعل ایمیل های دوستان شما یا با عنوان هایی بسیار فریب دهنده، فایلی را برای شما می فرستند و از شما می خواهند آن را اجرا کنید. با اجرا کردن این برنامه ها، رایانه شما کاملا در دستان کلاهبردارها خواهد بود و به این روش شما همه اطلاعات شخصی خود را تقدیم کلاهبرداران خواهید کرد

۶. اگر مجبور شدید در مکان های عمومی یا کافی نت ها به اینترنت متصل شوید، اگر امکانش را دارید حتما از لپ تاپ خودتان استفاده کنید، رایانه ای که متعلق به شما نیست، ممکن است تمام فعالیت های شما را ذخیره کند و در اختیار دیگران قرار دهد.

۷. اگر لپ تاپ، رایانه یا حتی گوشی موبایل کارکرده خریده اید، حتما قبل از شروع به استفاده از آن، تمام درایوهای آن را فرمت کنید و برنامه ها را از نو روی آن نصب کنید و اگر امکانش را دارد، تنظیمات آن را به حالت پیش فرض اولیه برگردانید. شاید این کار در ابتدا کمی زمانبر باشد، اما به دردسرهایی که در آینده ممکن است ایجاد کند، می ارزد.

۸.اگر از فروشگاه های اینترنتی خرید می کنید، مطمئن شوید که پشت این فروشگاه شخصی وجود دارد، از قسمت "تماس با ما" فروشگاه ها، شماره تلفن آنها را بردارید و با آنها تماس بگیرید، در هنگام خرید به این فکر کنید که اگر کالا دیر به دست شما رسید، اگر کالای رسیده معیوب بود یا اگر پس از خرید نیاز به استفاده از گارانتی و تعمیر داشت، چه باید بکنید؟ این سوال ها را از فروشنده بپرسید و پس از اطمینان خرید کنید

۹.اطلاعات کارت های بانکی خود را در هیچ سایتی به غیر از سایت اصلی بانک های کشور وارد نکنید. هیچ فروشنده ای اجازه ندارد اطلاعات کارت شما را داشته باشد. همچنین مطمئن شوید سایتی که در آن اطلاعات را وارد می کنید سایت بانک باشد و نه سایتی که شبیه سایت اصلی شبیه سازی شده است.

۱۰.اگر با لحاظ تمام جوانب باز هم گرفتار کلاهبرداری اینترنتی شدید، با پلیس تماس بگیرید. پلیس فتا رسته ای از نیروی انتظامی است که تخصص آنها جرایم رایانه ای است.

آیا اختفاء در اینترنت ممکن است؟

بسیاری از کاربران اینترنتی بر این باورند که توانایی مخفی ماندن از طریق نرم افزارها و برخی روشهای موجوددر فضای مجازی را دارند.در این خصوص کارشناس معاونت تشخیص و پیشگیری پلیس فتا عنوان نمود : عده ای با استفاده از نرم افزارهای موجود در فضای مجازی مانندVPN و نیز با تغییراتی درhttpsو یا با داشتن IP های داینامیکی به تصور، در اینترنت اقدام به اختفاء می نمایند و همانطور که خیلی از متخصصان در این حوزه به این علم واقف هستند چنین امری یک تصور باطل می باشد.

وی خاطر نشان کرد : حضور در فضای مجازی بصورت کاملا پنهانی همیشه میسر نبوده و بسیاری از کاربران به دلیل عدم شناخت با پرداخت هزینه های زیادی در این زمینه صرفاً کمک به کسب درآمد عده ای سودجو می‌نمایند که متاسفانه این امر به صورت متوالی صورت می پذیرد.

این کارشناس در ادامه بیان داشت : امروزه یکی از دلایل اصلی افشاء اطلاعات اشخاص در فضای مجازی مک آدرس مربوط به سیستم های سخت افزاری آنان و همچنین تصور اشتباه آنان در مخفی کردن هویت اصلی خود در فضای مجازی است .

وی در پایان اشاره نمود کاربران گرامی باید دقت لازم را به منظور حفظ و نگهداری از اطلاعات حساس و کلیدی خود داشته و به تکنیک هایی که به آن اشاره شد اکتفاء نکنند و مواردی را که سبب احساس ناامنی برای آنان در این فضا می شود را سریعاً از طریق وب‌سایت پلیس فتا به این پلیس اطلاع دهند .

کلاهبرداری اینترنتی ، کلاهبرداری امروزی!

اصطلاح کلاهبرداری اینترنتی عبارت است از هر طرح کلاهبرداری که در یک یا چند قسمت مختلف تشکیل دهنده اینترنت نظیر اتاقهای گفتگو Chat rooms ، پست الکترونیک , بردهای پیغام یا وب سایتها برای ارائه در خواستهای ساختگی به قربانی مورد نظر داده می شود و یا معاملات ساختگی (جعلی) و یا انتقال درآمد حاصل از کلاهبرداری به موسسات مالی و یا موسسات وابسته به این طرح بکار برده می شود.

اگر شما از اینترنت استفاده می کنید , به زودی خواهید دید که افراد و اشیائی که آنلاین هستند در حال جابجائی اند . این ضرب المثل که می گوید : " دوره دوره فن آوری اطلاعات است = دوره اینترنت است " . برای عده زیادی از مردم به این معنی است که تمام چیزها در اینترنت مثل تصمیمات تجاری , جستجوی اطلاعات و ارتباطات خصوصی خیلی سریع ظرف چند ثانیه اتّفاق می افتد . در حالیکه قبلاً مثل آب در هاون کوبیدن بود و ساعت ها طول می کشید . متأسفانه افرادی که به کلاهبرداری می پردازند در دوره تکنولوژی و فن آوری هم اغلب مؤثرند . آنهابه دنبال استفاده از قابلیت های منحصر به فرد اینترنت هستند , برای مثال با فرستادن نامه الکترونیکی (E-mail) در عرض چند ثانیه و یا با فرستادن اطلاعات صفحات شبکه (Web sites) که در سرتاسر جهان آماده و قابل دسترس است از قابلیت های اینترنت استفاده می کنند .امروزه انواع مختلف طرحهای کلاهبرداری سریعتر از طرحهای کلاهبرداری در گذشته انجام می شود.

برای پی بردن به اهداف سایتهای کلاهبرداری در اینترنت باید دو عامل را در نظر داشت یکی شناخت کلاهبرداران و دیگر بستر کلاهبرداری که، اینترنت می‌باشد. همیشه **افراد فرصت طلب و سودجو برای رسیدن به اهداف نامشروع و ثروتهای بادآورده** با شگردهای خاص و فریب افراد ناآگاه اقدام به اعمال کلاهبرداری می‌نمایند. برای این بزهکاران عملکردی که منجر به کسب درآمد زیاد میشود دارای اهمیت است.

بزهکاران حرفه‌ای با مدد پول و استفاده از ابزارهای پیشرفته به قدرتهای مافیایی تبدیل شده و روز به روز حوزه کاری خود را گسترش می‌دهند. گره خوردن گروههای مافیایی با سیاستمداران به عبارتی تعامل این دو گروه برای بقا و استمرار و تقویت قدرت وجه دیگر این عده از افراد است.

اما عامل دوم که اینترنت است. با گستردگی حوزه فعالیت اینترنت، بستری امن برای فعالیت کلاهبرداران فراهم می باشد. کلاهبرداران در اینترنت اهداف مختلفی را دنبال می‌کنند؛ **به عبارتی کلاهبرداران اینترنتی به دسته‌های مختلفی تقسیم می‌شوند:**

گروه اول: عده‌ای در سطح حرفه‌ای با صرف هزینه و بکارگیری افراد متخصص در زمینه‌های مختلف کامپیوتری با هدفهای بزرگ اقدام به کلاهبرداری در سطح بین المللی می‌نمایند.

گروه دوم: کلاهبرداران به اصطلاح خرده پا هستند که برای کسب درآمد اقدام به این عمل می‌کنند.

گروه سوم: کسانی هستند که مشکل مالی ندارند ولی با کسب تخصصی برای تفنن، سرگرمی، ماجراجویی و پرکردن خلاءهای روانی اقدام به کلاهبرداری در اینترنت می‌کنند.

گروه چهارم: شرکتها، کارتلها، سازمان‌های جاسوسی هستند که برای از میدان بدرکردن رقبای تجاری و یا اختلال در ثبات اقتصادی و سیاسی یک کشور با مصرف هزینه‌های کلان دراین راستا فعالیت می‌کنند.

به هر حال آنچه که مهم می باشد این است که همیشه در تمامی این موارد این کاربران اینترنت هستند که در معرض تهدید این سایتها قرار می‌گیرند.

راههای پیشگیری از کلاهبرداری:

۱.کاربران در دنیای مجازی می توانند خود را با شخصیت‌ها و اسامی گونان و غیرواقعی معرفی کنند و در شبکه های اجتماعی ،چت‌روم‌ها، سایت ها و ... فعالیت کنند پس هرگز به افراد در دنیای مجازی اعتماد نکنید زیرا این امکان وجود دارد که با هویت دروغین خود را به شما معرفی کرده باشند.

۲. از ارائه اطلاعات کارت بانکی خود حتی به افراد نزدیک خودداری کنید.

۳.از نوشتن رمز کارت بانکی در کنار کارت بپرهیزید و کارت بانکی خود را به شخص دیگری ندهید و اگر این امر صورت گرفت در اسرع وقت نسبت به تغییر رمز کارت خود اقدام نمائید.

۴. برای اینکه اطلاعات شخصی ما ربوده نشود یا کمتر آسیب پذیر باشد، باید اطلاعات مالی و شخصی خود را به خاطر بسپاریم و بطور مرتب آنرا را کنترل نمائیم و از آنها بدقت نگهداری کنیم.

۵. کلاهبرداری از طریق سایت های اینترنتی توسط اتباع کشور نیجریه و سنگال و یا تحت عنوان افراد تبعه این کشورها مسبوق سابقه است.

۶. هرگز به ایمیل هایی با عناوین؛ شرکت در قرعه کشی، برنده شدن در مزایده یا مسابقه، خرید اقلام کم یاب، انواع کمک های مالی، مشارکت در سودهای معاملاتی مختلف و ... اطمینان نکرده و هیچ مبلغی را به حساب اشخاص خارج از کشور واریز نکنید.

۷. فریب های اینترنتی معمولاً از یک الگوی مشابه پیروی می کنند که تماس اولیه از طریق ایمیل یا شبکه های اجتماعی انجام می شود و ابتدا از قربانیان خواسته می شود از طریق ایمیل، تلفن، فاکس و ... به این تماس پاسخ دهند و بعد از اینکه در اولین گام طعمه به دام شکارچیان افتاد، آنان سعی می کنند اعتماد قربانی را جلب کرده و در انتها به بهانه ای از او در خواست پول می کنند پس همیشه در هنگام روبرو شدن با موضوعاتی از این قبیل شباهت الگوهای کلاهبرداری اینترنتی را مدنظر قرار داده تا به دام ترفندهای آنها قرار نگیرید.

۸.از جمله کلاهبرداری های اینترنتی، کلاهبرداری نیجریه ای است که با رتبه نخست فریب اینترنتی، همچنان پرطرفدارترین شیوه کلاهبرداری است. در این حقه به قربانی قول یک جایزه یا ارائه درصدی از پول کلانی داده می شود که قرار است آن را از کشور نیجریه خارج کنند و معمولاً ابتدا از کاربر خواسته می شود یک مبلغ اولیه برای پوشش هزینه های بانکی ارائه دهد و به محض ارسال نخستین پول، کلاهبرداران غیب می شوند، لذا در مواجهه با این نوع کلاهبرداری ها که به اشکال مختلف و مختص کشورهای آفریقایی است، هیچگونه توجهی به ترفندهای آنان نکرده و هیچ ارتباطی از طریق ایمیل یا تلفن و ... حاصل نکنید.

۹. برای انجام انواع عملیاتهای بانکی اعم از پرداخت قبوض، پرداخت شهریه دانشگاه، انتقال وجه به حساب های دیگر، انواع خریدهای اینترنتی و ... حتی المقدور از کافی‌نت استفاده نکنید و در صورتی که به اجبار از کافی‌نت جهت عملیات بانکی استفاده نمودید بلافاصله بعد از انجام عملیات فوق با مراجعه به دستگاههای خودپرداز، در بانک خود اقدام به تعویض رمز دوم کارت نمایید.

۱۰. در صورتی که خودتان به هر دلیلی نتوانستید عملیات بانکی مورد نظرتان را انجام دهید و نیاز به کمک دیگران در انجام عملیات بانکی داشتید، کارت و رمز کارت خود را دراختیار افراد ذیصلاح و مطمئن قرار دهید و بعد از دریافت کارت خود سریعاً حساب خود را چک کرده و اقدام به تعویض رمز خود کنید.

۱۱. برای پرداخت ها و خریدهای اینترنتی تنها شماره روی کارت، رمز دوم، تاریخ انقضای کارت و شماره ۳ یا ۴ رقمی پشت کارت (cvv2) کافی است پس در صورت افشای رمز دوم کارت خود سریعاً با مراجعه به نزدیک ترین عابر بانک مربوطه اقدام به تعویض رمز دوم خود کنید.

۱۲. از انتخاب رمزها و پسوردهای ساده و رند مانند تارخ تولد، شماره شناسنامه و ... جداً خودداری نمائید.

آشنایی با برخی از روش های کلاهبرداری اینترنتی در ایران

اگر کاربران به طور مرتب اطلاعات خود را از منابع تائید شده را به روز کنند، می‌توانند مجرمان دنیای مجازی را در اجرای نقشه‌های خود ناکام بگذارند.

در این قسمت روش هایی را که در کشورمان کلاهبرداران اینترنتی از آن بهره می‌برند تا سر کاربران اینترنت کلاه بگذارند، با هم مرور می‌کنیم ، تا آگاهی و هوشیاری شما نسبت به این افراد بیشتر شود :

حقه نیجریه‌ای

این شگرد که باعث شد افراد ساده‌لوح زیادی قربانی حرص و طمع خود شوند به این علت حقه نیجریه‌ای لقب گرفته است که در آن فرد تبهکار از طریق پست الکترونیکی ایمیل‌های فراوانی برای طعمه خود ارسال کرده و ادعا می‌کند شاهزاده بخت‌برگشته‌ای در نیجریه است که از بد ماجرا از سمت خود خلع شده و از آنجا که بدخواهان و دشمنان زیادی دارد می‌خواهد به صورت پنهانی مبلغ زیادی پول از کشور خارج کند، این شاهزاده تقلبی در ایمیل‌هایی که برای طعمه خود می‌فرستد وعده‌های وسوسه‌کننده و سرخرمن زیادی به قربانی خود می‌دهد. در این روش فرد کلاهبردار بعد از این‌که طعمه خود را وسوسه کرد از او می‌خواهد از طریق تلفن یا فکس با او تماس بگیرد تا اعتمادش بیشتر جلب شود. بعد از این‌که کلاهبردار مطمئن شد طعمه به دام افتاده، از قربانی خود می‌خواهد برای انجام مقدمات کار مبلغی به او بدهد تا کارهای اولیه انجام شود، قربانی‌ها در این روش از ۵۰۰ تا هزاران دلار خود را از دست می‌دهند.

برنده خیالی یا بازنده واقعی

در این روش کلاهبردار به وسیله ارسال ایمیل یا تماس در شبکه‌های اجتماعی به طعمه‌هایش وعده برنده شدن در قرعه‌کشی را می‌دهد، به این ترتیب او از قربانیان خود می‌خواهد مبلغی پول به حسابش بریزند تا او جایزه را برایشان پست کند، اما گرفتن پول همان و کلاهبرداری هم همان.

در یکی از پرونده‌های کلاهبرداری اینترنتی با وعده برنده‌شدن، تبهکاری با فرستادن ایمیل برای قربانی‌های خود به آنها وعده می‌داد در قرعه‌کشی گرین‌کارت آمریکا برنده شده‌اند و کافی است برای گرفتن مدارک و انجام کارهای اولیه مبلغی را به عنوان هزینه پست و مالیات پرداخت کنند تا گرین کارت به دستشان برسد.در این شگرد قربانی از همه جا بی‌خبر هم پول را به حساب کلاهبردار واریز می‌کرد تا پولش را از دست داده و کلاه گشادی به سر بگذارد.

کلاهبرداری با وعده ازدواج

در این روش از کلاهبرداری اینترنتی که مجرمان، طعمه‌های خود را در شبکه‌های اجتماعی و چت‌روم‌ها شکار می‌کنند با دادن وعده‌هایی مانند ازدواج، اطلاعات شخصی کاربران را به دست آورده و با تهدید به انتشار آنها از طعمه‌های خود اخاذی می‌کنند. مدتی قبل با شکایت دختر جوانی کلاهبردار جوانی به دام افتاد که از دختران زیادی با این روش اخاذی کرده بود.

یکی از شاکیان این پرونده درباره شگرد مرد کلاهبردار به ماموران پلیس گفت: بعد از این‌که با مرد جوانی در اینترنت دوست شدم، او ادعا کرد قصد دارد با من ازدواج کند. به همین علت در دنیای مجازی بیشتر با هم در ارتباط بودیم. مدتی به این شکل گذشت و یک روز این فرد گفت کامپیوتر مرا هک کرده و اگر به حسابش پول واریز نکنم، او عکس‌های شخصی مرا در اینترنت منتشر خواهد کرد.

به این ترتیب، ماموران با شکایت دختر جوان و اطلاعاتی که او در اختیارشان گذاشته بود، متهم را دستگیر کردند.

کلاهی برای جویندگان کار

مثال : ما یک کار عالی برای شما در نظر گرفته ایم. از همین الان می توانید این کار را شروع کنید.

هدف: بدست آوردن اطلاعات شخصی، شماره حساب بانکی یا شماره بیمه و. . . . . .

نتیجه: قربانیان فریب خورده بدون تحقیقات، به امید ورود به شغل ایده آل خود، اطلاعات در خواستی را در اختیار کلاهبرداران قرار می دهند، بدون اینکه نتیجه ای برای آنها داشته باشد. در نهایت شغلی هم نصیب آنها نمی شود.

با توجه به آمار زیاد بیکاران در جامعه، گروهی از کلاهبرداران دنیای مجازی برای دست یافتن به اطلاعات طعمه‌های خود از این شگرد استفاده می‌کنند؛ آنها در پوشش بنگاه کاریابی ایمیلی برای قربانی خود ارسال کرده و به او می‌گویند شغل ایده‌آلی را برایش پیدا کرده‌اند.

کلاهبرداران که نیتی جز به دست آوردن اطلاعات سوژه خود ندارند، به همراه ایمیل، فایلی را برای فرد مورد نظر ارسال کرده و از او می‌خواهند فرم را پر کند. به این ترتیب قربانی بدون این‌که بویی ببرد، اطلاعاتی مانند شماره حساب، شماره بیمه و مشخصات خود را در اختیار سارقان اینترنتی قرار می‌دهد.

فروش کالای تقبلی

با همه‌گیر شدن استفاده از اینترنت، کار خرید و فروش اینترنتی هم رونق گرفته است. امروز سایت‌های زیادی را در دنیای مجازی می‌توان دید که انواع و اقسام محصولات موجود در بازار را می‌فروشند؛ از کالاهای لوکس گرفته تا خدماتی مانند تورهای مسافرتی.

در بین این فروشندگان می‌توان کلاهبرداران دنیای مجازی را هم دید، گروهی از این تبهکاران با فروش اجناس تقلبی به جای اجناس اصل سر مشتری های خود کلاه می‌گذارند، برای همین توصیه می‌کنیم از فروشگاه‌های اینترنتی معتبر و خوشنام خرید کرده و قبل از هر چیز با شماره تلفن ثابتی که به دفتر فروش سایت اینترنتی مربوط می‌شود تماس بگیرید تا حداقل مطمئن شوید می‌توانید نام و آدرسی از فروشنده در اختیار داشته باشید.

کلاهبرداری به بهانه فروش وسایل دست دوم

مدتی پیش فردی دستگیر شد که به بهانه فروش لوازم دست دوم در دنیای مجازی سر صدها نفر کلاه گذاشته بود.

مرد کلاهبردار به این شکل عمل می‌کرد؛ او پس از طراحی سایت خوش آب و رنگی برای خود، از تعداد زیادی وسیله دست دوم عکاسی کرده و تصاویر را روی سایت خود قرار داده بود.در حالی که همه اجناس به نظر تمیز و سالم می‌آمدند مرد جوان برای آنها قیمت‌های پایینی را در نظر گرفته بود تا از این راه مشتریان را وسوسه کند.مرد جوان از خریداران خود می‌خواست برای انجام معامله بهای اجناس را برایش کارت به کارت کنند تا او از طریق پست کالای مورد نظر مشتری‌هایش را برایشان ارسال کند.جالب اینجا بود که او هزینه پست کردن وسایل را هم از مشتریان خود می‌گرفت، اما بعد از واریز شدن پول به حسابش دیگر شخصی را به عنوان خریدار نمی‌شناخت.

کلاهبرداری با ایمیل جعلی

این گروه از کلاهبرداران دنیای مجازی سراغ تاجرهایی می‌روند که در دنیای مجازی فعال هستند. آنها بعد از شناسایی طعمه‌های خود برای آنها ایمیل‌هایی ارسال کرده و از این طریق از قربانیان می‌خواهند به حساب آنها پول واریز کنند.

کلاهبردارهای دنیای مجازی به این شکل عمل می‌کنند؛ آنها وقتی به اطلاعات بازگانان دست پیدا کردند، ایمیلی مشابه ایمیل طرف قرارداد بازرگانان می‌سازند و با ارسال نامه از طریق ایمیل جعلی به قربانیان خود می‌گویند شماره حساب شرکت تغییر کرده و بهتر است برای ادامه داد و ستد آنها مبلغ باقیمانده از قرارداد

را به شماره حساب جدیدی که برایشان ارسال کرده‌اند، واریز کنند تا هر چه سریع‌تر اجناس خود را دریافت کنند اما راز کلاهبرداری این سارقان اینترنتی زمانی برملا می‌شود که تاجر بخت‌برگشته هر چه انتظار می‌کشد، جنسی به دست او نمی‌رسد.

فیس بوک / هات‌میل / جی میل / یاهو میل و ...

کلاهبردان اطلاعات نام کاربری و کلمه عبور فیس بوک، هات میل و دیگر وب سایت‌های مشابه را سرقت کرده و رمز عبور شما را تغییر می‌دهند. سپس برای همه دوستان شما ای‌میلی را ارسال می‌کنند که در آن آمده است در حالی که در مسافرت بوده‌اید همه پول‌های شما به سرقت رفته است و در حال حاضر نیازمند پول برای پرداخت هزینه‌های هتل هستید.

غرامت

اخیراً فریبی هوشمندانه بر پایه فریب نیجریه ایجاد شده است که در آن ای‌میلی برای شما ارسال می‌شود مبنی بر اینکه مبلغی برای دلجویی از قربانیان کلاهبرداری نیجریه در نظر گرفته شده است و شما یکی از قربانیان خوش‌شانس هستید. سپس کلاهبرداران برای ارسال غرامت، از شما درخواست ۱۰۰۰ دلار پول می‌کنند!

اشتباه

در این فریب شایع، کلاهبرداران در صورتی که شما فروشنده چیزهای با ارزشی همچون خانه، ماشین و غیره باشید، با شما تماس می‌گیرند. آن‌ها کالای مذکور را از طریق چک خریداری می‌کنند ولی چکی با مبلغی بالاتر را برای شما ارسال می‌کنند، سپس درخواست می‌کنند تا باقیمانده پول آن‌ها را برایشان ارسال کنید. چک مذکور تقلبی بوده و یا برگشت می‌خورد و شما همه پولی را که نقداً پرداخت کرده‌اید، از دست خواهید داد.

کلاهبرداری از طریق دریافت هزینه جهت اخذ وام

مثال : ما قابلیت اخذ وام در مبالغ بالا و با کمترین تعهدات و صرف زمان کم را برای شما داریم.

هدف: دریافت مبلغی تحت عنوان کارمزد و. . . . (درحقیقت نزول) از فردی که فریب خورده است.

هدف: دریافت مبلغی تحت عنوان کارمزد یا حق واسطه گری از متقاضی می باشد.

نتیجه: شرکت و یا اشخاص فریب خورده مبلغ مورد توافق را پرداخت می کنند اما هیچ وقت وامی را دریافت نمی کنند.

بزرگ نمایی تورهای مسافرتی

مثال : یک مسافرت ایده ال با امکانات رفاهی و هزینه مناسب در انتظار شماست و البته با مقایسه ی قیمت با سایر تورهای مسافرتی متوجه می شوید این یک پیشنهاد مناسب است.

هدف: اخذ مبلغ از متقاضیان خرید تور مسافرتی.

نتیجه: در زمان مسافرت متوجه می شوید شرایط متفاوت می باشد و امکاناتی نظیر هتل های چند ستاره نوع خطوط هوایی و امکانات اقامتی و ... که به شما وعده داده شده بود محقق نشده است در حالی که شما مبلغ را پرداخت کرده اید و چاره ای جز قبول شرایط ندارید .

کلاهبرداری با وعده استخدام ، فرصتهای شغلی کار در خانه ، فروش محصولات کسب درآمد کلان و ... از دیگر موارد هستند.

کلاهبرداری از طریق ترفندهای افزایش شارژ

با توجه به مکانیزمهایی که در سیستمهای نرم افزاری اپراتورهای تلفن همراه وجود دارد و بعضاً به عنوان باگ های این سیستمها شناخته می شود، این امکان وجود دارد که افراد سودجو با پی بردن به این گونه مطالب اقدام به کلاهبرداری و کسب مال نامشروع کنند.

کلاهبرداری از طریق ترفندهای افزایش شارژ

در برخی وب سایتها، عناوین و تیترهایی تحت عنوان ترفندهای افزایش شارژ آورده شده، به عنوان نمونه در یکی از این ترفندها پیشنهاد شده بود که با استفاده از یک کد و وارد کردن آن، کاربران افزایش شارژ **سه برابری را تجربه کنند.**

در این ترفندها پیشنهاد شده اگر شماره شارژ را وارد می کردید تمام مبلغ شارژ شما برای شماره تلفن فرد کلاهبردار که از راست به چپ نوشته شده بود، ارسال می شد و هیچ گونه افزایش شارژی را برای کاربر به همراه نداشت.

با توجه به فضاهای خالی و باگ های موجود در برخی اپراتورهای تلفن همراه افراد بعضاً وسوسه می شوند تا با پرداخت هزینه کمتر از مکالمات و امکانات بیشتری استفاده کنند که در بسیاری از موارد منجر به متضرر شدن کاربر می شود.

مردم باید از مراجعه به سایتهای اینترنتی که تبلیغ شارژ ارزان سیم کارت یا خریداران می کنند، خودداری کنند زیرا این سایتها اغلب کاربران را به سایتهای **جعلی بانکها** وصل کرده و رمز اینترنتی حساب بانکی آنها را سرقت می کنند.

از این رو توصیه می کنم، به دنبال دورزدن سیستمهای مخابراتی به منظور به دست آوردن فرصت مکالمه بیشتر نباشیم تا افراد سودجو نتوانند از این میل و اشتیاق به نفع خود بهره برداری کنند.

روش های کلاهبرداری در شبکه‌های اجتماعی

هر سرویسی که بزرگ می‌شود، به همان اندازه برای کلاهبرداران و هکرها هم ارزشمند می‌شود و لقمه‌ای چرب برای کسب درآمد به حساب می‌آید. فیس‌بوک نیز از این قاعده مستثنا نیست .

جرایم سایبری همیشه در جریان هستند اما در مورد شبکه‌های اجتماعی باید گفت این جرایم را بسیار آسان تر می توان مرتکب شد مثلا در شبکه‌های اجتماعی کاربران بدون اینکه یکدیگر را به خوبی بشناسند با یکدیگر دوست می‌شوند و اطلاعات خود را در اختیار هم قرار می‌دهند .

هیچ کدام از شبکه‌های اجتماعی موجود به اندازه **فیس‌بوک** پتانسیل اجرای جرایم سایبری را ندارند به خصوص اینکه فیس‌بوک بیش از صدها میلیون کاربر دارد و امکان اجرای هر سواستفاده‌ای از آن بسیار ساده تر است برای آشنایی با جرایمی که از طریق فیس‌بوک انجام می‌شوند .

چند نمونه از رایج ترین آنها را برایتان انتخاب کرده‌ایم :

۱.هک کردن حساب‌های کاربری : این ابزارها اصولا گرد رمزهای عبور رایج می‌گردند و برخلاف ایمیل‌ها، معمولا از نام ها و تاریخ‌ها استفاده می‌کنند. به محض هک کردن یک اکانت، هکر می‌تواند از آن به عنوان یک وسیله مطمئن برای ارسال اسپم استفاده کند یا اطلاعات آن حساب کاربری را بفروشد. فروختن اطلاعات در مقابل دریافت پول رایج ترین روش کلاهبرداران و هکرهای اینترنتی است. در دنیای مجازی، اطلاعات کاربران ارزش و بهای بسیاری دارند .

۲.استفاده از حساب‌های کاربری: یکی از روش‌های مستقیم دزدی هویت، زمانی است که هکر با استفاده از شناسه کاربری و رمز عبور دزدیده شده وارد اکانت کاربر می‌شود. به محض اینکه هکرها آنلاین می‌شوند، تمام فهرست دوستان کاربر و اطلاعات آنها را در اختیار دارند. در این‌گونه مواقع کلاهبردار می‌تواند با استفاده از هویت فرد قربانی، طرح‌های فریب کارانه خود را مانند حیله «لندن» اجرا کند .

۳. شبیه سازی پروفایل: شبیه سازی پروفایل صفحات اجتماعی روشی است که در آن با استفاده از اطلاعات و عکس‌های محافظت نشده فرد، می‌توان اکانتی جدید با نام و مشخصاتی بسیار شبیه به کاربر ساخت. یعنی کپی پروفایل موجود، یک پروفایل جعلی درست کرد .کلاه‌بردارها با این روش و استفاده از پروفایل جعلی برای همه قربانیان خود درخواست دوستی ارسال می‌کنند کاربر قربانی به خیال اینکه که فرستنده تقاضای دوستی را می‌شناسد، درخواستش را قبول می‌کند غافل از اینکه این پروفایل جعلی دامی برای سو استفاده از اطلاعات او خواهد بود .

۴. استخراج اطلاعات محافظت نشده: برخی از وب‌سایت‌ها، در مقایسه با صفحات اجتماعی منابع بسیار آسان تری برای ربودن اطلاعات شخصی هستند. با همه اینها، با اینکه در آنها می‌توان از اطلاعات شخصی خود محافظت کرد، اما بسیاری از کاربران اطلاعاتی همچون ایمیل، شماره تلفن، نشانی، تاریخ تولد و بسیاری از اطلاعات شخصی خود را در معرض دید همگان قرار می دهند.

افراد جویای کار مراقب باشند

کارشناس پلیس فتا گفت: اخیراً تعدادی از افراد سود جو با راه اندازی سایت‌هایی جهت استخدام اقدام به کلاه برداری از هم وطنان می‌نمایند. این افراد با دادن آگهی های استخدام در شرکت ها و موسسات مختلف، افراد بی کار را تشویق به ثبت نام می کنند. این افراد سعی می کنند با دادن توضیحاتی همچون حمایت دولت از آنان و.... اعتماد افراد را به دست آورند. معمولاً در این سایتها زمان و مکان برگزاری آزمون متعاقباً و از طریق سایت اعلام میشود ولی در عمل اینگونه نخواهد بود در ادامه و بعد از جلب اعتماد کاربران، کلاه بردار از فرد قربانی می خواهد که مبلغ در خواستی را از طریق پرداخت اینترنتی و وارد کردن رمز دوم و ccv2 به حساب شرکت واریز نماید. در حالی که فرد کلاه بردار بعد از دریافت مبلغی قابل توجه و یا برداشت وجه از حساب کاربران دیگر پاسخگوی افراد نخواهد بود.

کارشناس پلیس فتا افزود : ازهم وطنان درخواست می شود قبل از تکمیل فرم ثبت نام شرکت ها و موسسات ابتدا از معتبر بودن سایت مطمئن شوند.

در نهایت پلیس فتا از کلیه کاربران می خواهد در صورت مواجه با موارد مشکوک آن را از طریق سایت پلیس فتا به آدرس Cyberpolice.irبخش وب‌سایت‌های متخلف گزارش نمایند

یک راهکار ساده برای اینکه سرمان کلاه نرود !

انگلیسی ها یک ضرب المثل بسیار جالب دارند؛ مفهوم این ضرب المثل آن است که" **هیچ چیز گرانی بی حکمت نیست و هیچ ارزانی بی علت**" . اما متاسفانه عدم توجه ما به همین مفهوم ساده برای بسیاری از افراد مشکلات جبران ناپذیری به بار آورده است.

یکی از ساده ترین راه هایی که کلاهبرداران به ویژه کلاهبرداران اینترنتی از آن سود می برند، استفاده از طمع کسانی است که قصد کلاهبرداری از آنها را دارند.

در هر کلاهبرداری اینترنتی دو مقصر وجود دارد:

۱. کلاهبرداران

کسانی هستند که کلاهبرداری می کنند ، مجرمینی که همواره در پی دستیابی به خواسته های خویش اند تا از کوچکترین غفلت ما نهایت سود را ببرند.

۲.کسانی که سرشان کلاه می رود(فریب خوردگان)

افرادی هم که موقعیت سودجویی و سرقت اموالشان را فراهم می کنند به اندازه هکرها مقصر اند. بیشتر این افراد با مشاهده عرضه و فروش کالاهایی با قیمت بسیار پایین تر از قیمت های واقعی، طمع کرده و به راحتی اطلاعات و رموز بانکی شان را تقدیم هکرها می کنند.

به عنوان مثال خیلی واضح است که یک کارت شارژ ۵ هزارتومانی تلفن همراه زمانی که ۴ هزار تومان به فروش برسد یا فروشنده دیوانه شده و چوب حراج به اموالش زده و یا اینکه حتما کلکی در کار است! چراکه خود اپراتور های تلفن همراه و نمایندگی ها یشان هم تنها با ۲۰۰ تومان سود مبادرت به فروش کارت شارژ می کنند.

این در حالی است که بسیاری از خریداران با دیدن قیمت ۴ هزار تومان به اصطلاح" ذوق زده" شده و دیگر به عواقب کار فکر نمی کنند و همین امر سبب از دست رفتن اموالشان می شود.

"خرید اینترنتی" هم در هزینه ها صرفه جویی می کند و هم در وقت، اما این امر زمانی محقق می شود که کلیه نکات ایمنی را رعایت کرده باشیم در غیر اینصورت حتما نمی توان از یک خرید آسان و مطمئن سود برد.

مجرمین همواره در پی سودجویی از سهل انگاری ما هستند.از این روی به آنها نمی توان خرده گرفت, این ما هستیم که همواره می بایست با پرهیز از طمع کاری مراقب اموالمان باشیم.

راه هایی برای اجتناب از غارت های اینترنتی

اجازه ندهید کلاهبرداران به سیستم شما نفوذ کنند. اگر چند نکته امنیتی زیر را رعایت کنید، خرید و بانکداری اینترنتی کار بی خطری خواهد بود .

اگر در حال خرید اینترنتی هستید، به دنبال نشانه های مشهود و معتبری باشید که نشان دهند در حال خرید از یک شرکت معتبر هستید:

•آیا آنها در دنیای واقعی نیز فعالیت می کنند؟ آیا می توانید آدرس و شماره تلفن آنها را ببینید؟

•آیا وب سایت آنها امن و مطمئن است؟ وقتی که در حال ارائه جزییات (کارت اعتباری) یا اطلاعات شخصی برای هر نوع پرداختی هستید، در صفحه ای که در حال ارائه این اطلاعات هستید، به دنبال علائم انسداد (padlock) و https:// باشید .

•آیا آنها یک سیاست حفظ حریم شخصی روشن و مشخص دارند؟ آیا سیاست آنها برای بازپرداخت وجوه واضح و روشن است؟

•اگر شما (نسبت به اعتبار واقعی بودن فعالیت های آنها) متقاعد نشده اید، در اینترنت در مورد شرکت تحقیق کنید و اعتبار آنها را بررسی کنید. با آنها تماس بگیرید. به قضاوت منطقی خود اعتماد کنید و در صورت لزوم از جای دیگری خرید نمایید. اگر در حال کار با سایتی هستید که اجناس را به قیمت مزایده ای می فروشد)سایت حراجی)، مانندeBay ، انجام چند کار ساده زیر می تواند به انجام یک فعالیت ایمن تر و مطمئن تر در این سایت ها کمک کند .

•قبل از این که شروع به کار کنید، روند مزایده، قوانین سایت و توصیه های امنیتی شرکت مزایده گذار را به خوبی درک کرده و متوجه شوید.

•خریدار یا فروشنده را بشناسید. سوالات خود را مطرح کنید. باز خورد (پاسخ) آنها را بررسی کنید.

•گذر واژه (رمز عبور) و یا اطلاعات شخصی خود را در اختیار کسی قرار ندهید .

در زمان تحویل دادن پول، از راه های مطمئن مانند درگاه های بانکی (یک سایت اینترنتی برای نقل و انتقال پول) یا کارت اعتباری استفاده نمایید.

چگونگی کشف نشانه های بارز از مهندسی اجتماعی را یاد بگیرید:

•آنها جوایز نفیسی را وعده خواهند داد: بردن جوایز قرعه کشی

•یک حس تصنعی از فوریت (خصوصاً در هنگاه پرداخت وجوه) وجود دارد.

•جزئیات اضافی و غیر عادی را از شما می خواهند.

•از شما می خواهند هزینه های جانبی را پرداخت کنید یا اطلاعات شخصی خود را در اختیار آنها قرار دهید.

احتیاط کنید و در مورد این مسائل از منطق خود استفاده کنید. این مسئله به پول شما مربوط می شود. بنابراین اگر به شما احساس ناخوشایندی دست داد یا احساس راحتی نکردید، از این سایت خارج شوید. با عجله کاری را انجام ندهید .قبل از این که تصمیمات اساسی و بزرگی بگیرید، با هر شخصی که به او اعتماد دارید، صحبت کنید. به یاد داشته باشید اگر شرایط به گونه ای بیش از انتظار ،عالی به نظر رسید، احتمالاً حقه ای در کار است.

کلاهبرداری اینترنتی را جدی بگیرید

برای پرداخت مبالغ خرید اینترنتی، درگاه های اینترنتی بانکی در صفحات وب را با دقت بررسی کنید.

با گسترش مبادلات اینترنتی و افزایش استفاده از این فناوری برای صرفه جویی در میزان و هزینه روشهای سوء استفاده از این فناوری نیز گسترش یافته است .کاربران اینترنتی که از سایت های اینترنتی اکانت، شارژ یا هر جنس را خریداری می کنند دقت کنند وقتی که به طور خودکار از صفحه خرید سایت به صفحه پرداخت بانک مربوطه وارد می شوند، آدرس بالای صفحه را در نوار آدرس مرورگر چک کرده تا حتما نشانی، مربوط به بانک مربوطه باشد.

دزدهای اینترنتی با ایجاد صفحات جعلی بانکی و تعیین فیلدهای خالی می توانند با دریافت شماره کارت یا حساب و رمز نسبت به دستبرد اینترنتی از حسابهای بانکی اقدام کنند.

برای حفظ اطلاعات حساب خود، این مورد را حتما دقت کنید که اگر آدرس موجود در مرورگر حتی یک نقطه هم با نشانی اصلی اینترنتی بانک تفاوت داشت، سریعا از صفحه خارج شوید؛ فقط باید از نشانی اینترنتی بانک مورد نظرخود آگاه باشد.

آشنایی با توصیه‌های پلیس فتا در خصوص کلاهبرداری اینترنتی

استفاده از کارت اعتباری برای سهولت در مبادلات مالی، در بین اقشار مختلف مردم رواج گسترده‌ای پیدا کرده است.

برای کاهش وقوع جرایم در فضای سایبر، پلیس فتا توصیه‌هایی را به شهروندان ارائه کرده و همواره توصیه شده که تحت هیچ عنوان مشخصات کامل کارت اعتباری خود را در اختیار دیگران قرار ندهید.

توصیه‌های پلیس فتا در این خصوص عبارتند از:

- اطلاع داشته باشید برای واریز و انتقال هر مبلغی به حساب شما به جز شماره حساب یا شماره کارت اعتباری نیاز به هیچ مشخصات دیگری نیست.
- در حفاظت از مشخصات کامل کارت اعتباری خود نهایت دقت کنید.
- در تاریخ‌های مختلف نسبت به تغییر رمز اول و دوم کارت اعتباری خود اقدام کنید.
- ترجیحاً آدرس سایت را مستقیماً در قسمت کادر آدرس وارده و از جست‌وجو گرهای اینترنتی استفاده نکنید.
- دقت داشته باشید در ابتدای قسمتی از صفحه سایت اینترنتی بانک که آدرس سایت درج شده عبارت https:// ذکر شده باشد.
- برای استفاده از اینترنت در نقل و انتقالات مالی از صفحه کلید مجازی استفاده کنید.
- در جهت ایمنی بیشتر از کافی نت‌ها برای نقل و انتقالات مالی استفاده نکنید.

توصیه کارشناس : چطور از کلاهبرداری اینترنتی جلوگیری کنیم؟

کلاهبرداری های اینترنتی، از خالی کردن حساب بانکی شما گرفته تا هک کردن ایمیل و رایانه، این روزها بیشتر از هر زمان دیگری تهدید کننده شده اند. تهدیدی که عضو انجمن علمی تجارت الکترونیک ایران می گوید با انجام کارهای ساده زیر می‌توانید از آن در امان بمانید

جلوگیری از هک شدن اطلاعات در فضای مجازی کار سختی نیست. کافیست در اولین قدم، آنتی‌ویروس‌ها را روی رایانه نصب کنید. متاسفانه از آنجا که بیشتر این آنتی‌ویروس‌ها خارجی است و کاربران ایرانی باید آن‌ها را خریداری کنند، کاربران، این آنتی‌ویروس‌ها را از اینترنت به طور رایگان دانلود می‌کنند.
او می گوید حدود ۹۹ درصد آنتی‌ویروس‌هایی که از این طریق بر رایانه‌ها نصب می‌شوند، نه تنها ایمن نبوده بلکه خود حاوی ویروس هستند که باعث آلودگی سیستم می‌شوند. برخی از سایت‌ها، آنتی‌ویروس‌ها را به صورت رایگان در اختیار کاربران قرار می‌دهند که بهتر است از این آنتی‌ویروس‌ها هم استفاده نشود چون در آن‌ها هم تغییراتی ایجاد شده و ایمن نیستند.
استفاده از آنتی‌ویروس‌های رایگانی مطمئن است که از طریق سایت‌های سازنده در اختیار کاربران قرار می‌گیرد. آنتی‌ویروس کومودو (comodo) و فایروال جزو پیشهادهای عضو انجمن تجارت الکترونیک ایران است تا از نصب بدافزارها بر رایانه جلوگیری شود.

دومین اقدام برای ایمن سازی رایانه در مقابل کلاهبردارها، باز نکردن ایمیل‌های ناشناس یا انجام عمل گزارش اسپم (report spam) در مورد این ایمیل‌ها است.

راهکار سوم هم باز نکردن لینک‌های ناشناس در مسنجرها و عدم اشتراک‌گذاری عکس‌های شخصی در فضای مجازی است ، لینک‌های ناشناس ممکن است حاوی بدافزار باشند و اطلاعات شخصی شما را هک کنند. همچنین از طریق عکس‌ها هم می‌توان ویروس را منتقل کرد.همچنین نرم‌افزارها و مرورگرهای به روز و جدید استفاده کنید چرا که برای هر نسخه جدید این‌ها، ویروس خاصی طراحی می‌شود.

دزدی اطلاعات شخصی وکلاهبرداری

بعضی از طرحهای کلاهبرداری اینترنتی شامل دزدی اطلاعات شخصی وبه دست آوردن آن به صورت غیر قانونی واستفاده از آن است .این اطلاعات معمولا" با تقلب وکلاهبرداری بدست می آید و سود اقتصادی دارد. گاهی نام وشماره بیمه اجتماعی افراد را از یک Web site بدست می آورند و از این نامها و شماره ها از طریق اینترنت سوء استفاده می کنند. گاهی اطلاعات شخصی افراد را از یک Web site بدست می آورند و واز آن سوء استفاده می کنند.

برای مقابله با دزدی اطلاعات و کلاهبرداری اینترنتی چه کار کنیم ؟برای اینکه قربانی دزدی اطلاعات و کلاهبرداری اینترنتی نشویم وظیفه مااینست که اطلاعات مالی و شخصی خود را به یاد داشته باشیم. متأسفانه ضربه ای که مجرمان به ما می زنند بیشتر یک دزدی اطلاعات است. برای کم کردن و کاهش خطر دزدی اطلاعات و کلاهبرداری اینترنتی چند مرحله وجود دارد که شما باید آنرا انجام دهید . برای دادن اطلاعات شخصی تان به دیگران خسیس (ناخن خشک) باشید مگر اینکه به آنها اعتماد داشته باشید.

راهکارهای مقابله با سرقت‌های اینترنتی

۱.هنگام خرید از مغازه‌ها، رمز بانکی خود را شخصا وارد دستگاه کارتخوان کنید و از گفتن آن به فروشنده و دیگران خودداری کنید.
۲.کارت بانکی خود را به شخص دیگری ندهید و اگر دادید بعد از دریافت، رمز کارت و رمز دوم را تعویض کنید.

۳.از نوشتن رمزهای کارت بانکی در کنار کارت بانکی خود خودداری کنید.

۴.کارت بانکی خود را کاملا شخصی بدانید و از ارائه اطلاعات آن حتی به افراد نزدیک خودداری کنید (مثلا نگویید بابا ماکه این حرفا رو نداریم!). بسیار پیش آمده که افرادی که مرتکب دزدی اینترنتی شده‌اند، از کارت‌های بانکی افراد خانواده خود یا آشنایان و همکاران استفاده کرده‌اند. پس بهتر است هر کسی خودش مراقب اموال خویش باشد تا از اتفاقات ناخواسته جلوگیری شود.
۵.خریدهای اینترنتی خود را از سایت‌های معتبر انجام دهید و قبل از خرید از سایت، هویت و اعتبار سایت را بررسی کنید. این کار را می‌توانید با جست‌وجو در اینترنت انجام دهید یا از دوستان و آشنایان خود بپرسید.
۶.در هنگام خرید اینترنتی و زمان وارد کردن اطلاعات بانکی، حتما به آدرس سایت بانک دقت شود. زیرا افراد سودجو با راه‌اندازی سایت‌های فیشینگ و شبیه‌سازی آن به سایت بانک‌ها، اقدام به دزدیدن اطلاعات بانکی افراد می‌کنند. بسیاری از جرائم اینترنتی با همین روش انجام می‌شود.
۷.اگر به هر نحوی مطلع شدید که تمام یا بخشی از اطلاعات کارت بانکی شما درز کرده است باید سریعا اقدام به تغییر این اطلاعات کنید.
۸.به هیچ‌وجه پرداخت‌های اینترنتی و استفاده از اینترنت بانک را در کافی‌نت‌ها و کامپیوترهای عمومی انجام ندهید. حتی مشاهده شده که در مرکز کامپیوتر دانشگاه‌ها نیز، اطلاعات کارت‌های بانکی سرقت شده و مورد سوءاستفاده قرار گرفته است. در صورت اجبار به این کار، بلافاصله رمز دوم کارت خود را تغییر دهید.
۹.به قدیمی‌ها کمک کنید. پدران و مادران ما یا پدربزرگ‌ها و مادربزرگ‌های ما که حالا بازنشسته شده‌اند و حقوقشان را به وسیله کارت‌های عابربانک دریافت می‌کنند هدف‌های سارقانند زیرا آنها کمتر از من و شما با اینترنت و روش‌های الکترونیک آشنا هستند. ممکن است به بهانه کمک کردن سارقان به سراغشان بیایند یا از کندی حرکت آنها در عملیات بانکی استفاده کنند و شماره رمز آنها را پیدا کنند پس به آنها کمک کرده و یا آنکه روش صحیح استفاده را به آنها یاد بدهید.

۱۰توصیه برای مقابله با کلاهبرداران اینترنتی

اولین کاری که یک کلاهبردار اینترنتی انجام می‌دهد، جلب اعتماد است. او سعی می‌کند طوری برخورد یا شرایط را مهیا کند که شما به او اطمینان کنید و مطابق نقشه او پیش بروید. حتما قبل از روشن کردن رایانه خود و اتصال به اینترنت این نکات را به یاد داشته باشید:

۱ـ معمولا کلاهبرداری‌ها با تماس کلاهبردار آغاز می‌شود، مثلا برای شما ایمیل یا پیامک می‌فرستند یا حتی ممکن است به شما زنگ بزنند. در این موارد فرد با جعل یا شبیه‌سازی اطلاعات خود از ایمیلی که متعلق به او نیست یا آدرس‌های بسیار مشابه استفاده می‌کند و از شما درخواست‌هایی مانند واریز پول به یک شماره حساب یا دادن شماره کارت بانکی یا رمز حساب یا اطلاعات مشابهی را می‌نمایند. در این موارد حتما شما مجدد با اطلاعاتی که خودتان دارید با تماس‌گیرنده ارتباط برقرار کنید و هویت تماس‌گیرنده را بررسی کنید و به یاد داشته باشید بانک‌ها و شرکت‌های معتبر از ایمیل‌های عمومی مانند yahoo و gmail برای ارسال ایمیل استفاده نمی‌کنند. شماره‌های موبایل اعتباری نیز معمولا نشانه خوبی نیستند.

۲ـ مواظب آدرس‌های مشابه باشید، بسیاری از کلاهبرداری‌ها، با استفاده از آدرس‌های بسیار مشابه آدرس‌های اصلی انجام می‌شود. پس حتما آدرس سایت‌هایی را که در آنها اطلاعات وارد می‌کنید، با دقت بررسی کنید مخصوصا اگر لینک آنها را با ایمیل برای شما فرستاده‌اند.

۳ـ گول ایمیل‌هایی که ادعا می‌کنند شما برنده جایزه شده‌اید و برای دریافت جایزه خود باید مبلغی را به شماره حسابی واریز کنید را نخورید.

۴ـ اگر شما با کسانی کار می‌کنید و آنها از طریق ایمیل برای شما فاکتورهایشان را ارسال می‌کنند، بسیار در معرض خطر هستید! حتما اطلاعات حساب فروشنده را هر بار با او از طریق دیگری غیر از ایمیل هم کنترل کنید.

۵ ـ هیچ فایلی را از ایمیل بدون داشتن یک آنتی‌ویروس مطمئن و به‌روز شده دریافت نکنید، زیرا بسیاری از کلاهبردارها، با جعل ایمیل‌های دوستان شما یا با عنوان‌هایی بسیار فریب‌دهنده، فایلی را برای شما می‌فرستند و از شما می‌خواهند آن را اجرا کنید. با اجرا کردن این برنامه‌ها، رایانه شما کاملا در دستان کلاهبردارها خواهد بود و به این روش شما همه اطلاعات شخصی خود را تقدیم کلاهبرداران خواهید کرد.

۶ـ اگر مجبور شدید در مکان‌های عمومی یا کافی‌نت‌ها به اینترنت متصل شوید، اگر امکانش را دارید حتما از لپ‌تاپ خودتان استفاده کنید، رایانه‌ای که متعلق به شما نیست، ممکن است تمام فعالیت‌های شما را ذخیره کند و در اختیار دیگران قرار دهد.

۷ـ اگر لپ‌تاپ، رایانه یا حتی گوشی موبایل کارکرده خریده‌اید، حتما قبل از شروع به استفاده از آن، تمام درایوهای آن را فرمت کنید و برنامه‌ها را از نو روی آن نصب کنید و اگر امکانش را دارد، تنظیمات آن را به حالت پیش‌فرض اولیه برگردانید. شاید این کار در ابتدا کمی زمانبر باشد، اما به دردسرهایی که در آینده ممکن است ایجاد کند، می‌ارزد.

۸ ـ اگر از فروشگاه‌های اینترنتی خرید می‌کنید، مطمئن شوید که پشت این فروشگاه شخصی وجود دارد، از قسمت «تماس با ما» فروشگاه‌ها، شماره تلفن آنها را بردارید و با آنها تماس بگیرید، در هنگام خرید به این فکر کنید که اگر کالا دیر به دست شما رسید، اگر کالای رسیده معیوب بود یا اگر پس از خرید نیاز به استفاده از گارانتی و تعمیر داشت، چه باید بکنید؟ این سوال‌ها را از فروشنده بپرسید و پس از اطمینان خرید کنید.

۹ـ اطلاعات کارت‌های بانکی خود را در هیچ سایتی به غیر از سایت بانک‌های کشور وارد نکنید. هیچ فروشنده‌ای اجازه ندارد اطلاعات کارت شما را داشته باشد. همچنین مطمئن شوید سایتی که در آن اطلاعات را وارد می‌کنید سایت بانک باشد و نه سایتی که شبیه سایت اصلی شبیه‌سازی شده است.

۱۰ـ اگر با لحاظ تمام جوانب باز هم گرفتار کلاهبرداری اینترنتی شدید، با پلیس تماس بگیرید. پلیس فتا رسته‌ای از نیروی انتظامی است که تخصص آنها جرایم رایانه‌ای است.

۸ توصیه ی پلیسی در برای کار با ایمیل !

اداره اجتماعی پلیس آگاهی ناجا در واحد مبارزه با جرایم رایانه‌ای به کاربران اینترنت در هنگام کار با ایمیل هشدار داد:

۱. از باز کردن فایل‌های ارسال شده (attachment) توسط ایمیل‌های ناشناس خودداری کنید، زیرا ممکن است فایل‌ها حاوی برنامه‌های مخرب جهت سرقت اطلاعات شخصی یا از کار انداختن رایانه شما باشد.

۲. بهترین راه برخورد با نامه‌های الکترونیک ناشناس حذف نامه‌ها و پیوست آنها است.

۳. اگر پیام الکترونیکی از دوست یا همکار خود دریافت کردید که در بازکردن ضمیمه فایل تاکید دارد، حتما قبل از باز کردن ضمیمه با فرستنده آن هماهنگی کنید.

۴. از ذخیره کردن گذر واژه پست الکترونیکی خود، خودداری کنید.

۵. از باز کردن نامه‌های پست الکترونیک با عناوین نامشروع خودداری و سعی کنید از دادن اطلاعات شخصی و عضویت در این نوع گروه‌ها اجتناب کنید.

۶. در اینترنت (فضای مجازی) سایت‌هایی هستند که با عضویت در آن تعدادی نامه الکترونیکی مشخصی را به فرد عضو شده می‌فرستد که فرد با باز کردن آن نامه‌های الکترونیک که حاوی پیغام‌های تبلیغاتی است و در ازای خواندن آن مبلغی از پنج سنت تا دو دلار در یک حساب تجاری که خود شرکت معرفی کرده واریز می‌کنند، اما از هویت و چگونگی برداشت از حساب معرفی شده دارای وجود خارجی نیست. لذا نتیجه کار تنها اتلاف وقت کاربران و صرف هزینه‌های مربوط به اتصال اینترنت است.

۷. فضای مجازی اینترنت سرشار از تبلیغات فریبنده است که کاربران را به پولدارشدن از راه‌های جدید در پوشش عناوینی همچون بازاریابی شبکه‌ای و تجارت الکترونیک وسوسه می‌کند، بدون شک ورود کاربران به این بازی‌ها یک دسیسه هرمی بیش نیست که به پولدارشدن بازیگردانان منتهی می‌شود.

۸. به نامه‌های الکترونیک ارسالی ناشناس که خبر برنده شدن مبالغ قابل توجهی پول را به شما می‌دهند، توجه نکنید، این روش دامی برای کلاهبرداری از شماست.

۲۵ توصیه "پلیس فتا" به کاربران اینترنت

استفاده از اینترنت، پیامدهای مثبت و منفی متعددی را درپی دارد. اگر چه نباید فرصت‌های مثبتی را که از طریق اینترنت ایجاد شده نادیده گرفت، اما از طرفی نمی‌توان از کنار معضلات، ناهنجاری‌ها، بزهکاری‌ها و ... به وجود آمده از این طریق نیز به سادگی و با بی‌توجهی گذر کرد.

پایگاه اطلاع رسانی پلیس فتا، برای پیشگیری از وقوع جرائم اینترنتی و سرقت اطلاعات کاربران اینترنتی و والدین هشدارهایی را به کاربران داده است که کاربرد آنها بسیار مفید خواهد بود. این موارد به شرح زیر است:

۱. از پسوردهای متعدد برای امور مختلف استفاده کنید تا از لو رفتن آنها جلوگیری شود.

۲. در زمان استفاده از اینترنت در مکان‌های عمومی حتماً از محل‌های معتبر استفاده کنید.

۳. کامپیوترهای خانگی را در محلی از منزل قرار دهید که در مقابل دید اعضاء خانواده باشد

۴. ساعاتی را که بچه‌ها با کامپیوتر کار می‌کنند، محدود کنید.

۵. از ذخیره و نگهداری اطلاعات شخصی در سیستم‌های رایانه و گوشی‌های تلفن همراه جدا" خودداری کنید.

۶. از ارسال اطلاعاتی در اینترنت که هویت شما را آشکار می‌کند، خودداری کنید.

۷. هیچگونه اطلاعاتی را با افراد غریبه که بصورت آنلاین معرفی می‌شوند، به اشتراک نگذارید

۸. هرگز ضمایم همراه ایمیل‌های افراد ناشناس را باز نکنید.

۹. حتما از نصب نرم‌افزارهای امنیتی که از سیستم شما دربرابر حملات ویروسی، هکرها و جاسوسی محافظت کنند، اطمینان حاصل کنید.

۱۰. از کلمات عبور طولانی، شامل اعداد، حروف و نشانه‌ها استفاده کنید.

۱۱. کلمات عبور و پسورد خود را در فواصل زمانی معین تغییر دهید.

۱۲. از وجود سه نرم افزار امنیتی - آنتی‌ویروس، ابزار ضدجاسوسی و فایروال در سیستم خود اطمینان حاصل کنید.

۱۳. تهدیدات و آسیب‌های اینترنتی را به فرزندان خود گوشزد کنید.

۱۴. در زمان خرید اینترنتی حتما" از واقعی بودن وب‌سایت‌ها اطمینان حاصل کنید.

۱۵. در زمان استفاده از اینترنت در محل‌های عمومی حتما قبل از خروج از محل، نسبت به خروج کامل از سیستم اطمینان حاصل کنید.

۱۶. در زمان خرید تجهیزات رایانه‌ای، حتما از محل‌های فروش معتبر و شناخته شده خرید کنید.

۱۷. فریب تبلیغات و آگهی‌های فریبنده که هیچگونه برند مشهوری از آن پشتیبانی نمی‌کند را نخورید.

۱۸. از قرار دادن آی پی (آدرس خود) در اختیار دیگران خودداری کنید.

۱۹. از پاسخ گویی به ایمیل‌های مشکوک که از سوی افراد ناشناس برایتان ارسال می‌شود خودداری کنید.

۲۰. از شرکت کردن در وب‌سایت‌های هرمی تحت عنوان سرمایه گذاری خودداری کنید.

۲۱. سیستم‌های معیوب خود را نزد مهندسین تعمیرکار آشنا و مورد اطمینان ببرید و از تحویل سیستم معیوب به هر تعمیرکاری خودداری کنید.

۲۲. از اسکن کردن مدارک و اسناد قانونی خود در سیستم‌های رایانه‌ای شخصی جدا" خودداری کنید.

۲۳. از واریز وجه به حساب اشخاص و شرکت‌هایی که آگهی فروش با قیمت مناسب زده‌اند قبل از بررسی اصالت و هویت واقعی شرکت یا شخص آگهی دهنده جدا خودداری گردد.

۲۴. در هر زمان قبل از ورود به اینترنت از نرم‌افزارهای فایروال و آنتی‌ویروس‌های به روز استفاده کنید.

۲۵.در هنگام اتصال به اینترنت از طریق گوشی‌های تلفن همراه، مراقب نامه‌های الکترونیکی مشکوک و وب‌سایت‌های اینترنتی فریبنده باشید.

کلاهبرداری فیشینگ چیست؟

فیشینگ راهی است که تبهکاران، اطلاعاتی نظیر کلمه کاربری، رمز عبور، شماره ۱۶ رقمی عابر بانک، رمز دوم و CVV2 را از طریق ابزارهای الکترونیکی ارتباطات به سرقت می برند. شبکه های اجتماعی، سایت های حراجی و درگاه های پرداخت آنلاین نمونه ای از ابزار های الکترونیکی ارتباطات می باشند.

کلاهبرداری فیشینگ از طریق ایمیل ها و پیامها صورت می پذیرد و قربانیان به صورت مستقیم اطلاعات حساس و محرمانه خود را در **وب سایت های جعلی** که در ظاهر کاملا شبیه وب سایت های سالم و قانونی می باشد وارد می نمایند. حقه ی فیشینگ یکی از تکنیک های مهندسی اجتماعی برای فریب کاربران می باشد که علی‌القاعده از ضعف امنیتی یک وب سایت برای انجام عملیات مجرمانه خود استفاده می کنند. برای اولین بار حقه ی فیشینگ در ۱۹۸۷ تعریف شد و اولین باری که واژه فیشینگ برای نام گذاری این واژه استفاده گردید، سال ۱۹۹۶ بود.

انواع تکنیک هایی که در حقه فیشینگ مورد استفاده قرار می گیرد:

دستکاری و تقلب در لینکها و آدرس ها

یکی از شیوه های متداول و رایج در فیشینگ ارسال لینک ها و آدرس های متعلق به سازمانهای غیر واقعی و جعلی از طریق ایمیل می باشد. آدرس هایی که تنها تفاوت آنها با آدرس اصلی یک یا دو حرف است یا از دامین های فرعی گمراه کننده برای ایجاد آنها استفاده گردیده است.

دور زدن فیلتر

فیشرها با استفاده کردن از عکس به جای متن، کار فیلترهای ضد فیشینگ را که برای شناسایی متن هایی که عموماً در ایمیل های حاوی آدرس های جعلی یافت می شوند، را سخت می کنند.

وب سایت جعلی

تنها با ورودو بازدید یک قربانی به سایت جعلی عمل کلاهبرداری صورت نمی پذیرد . در برخی از روش های فیشینگ از دستورات جاوا اسکریپت استفاده می شود تا نوار آدرس را اصلاح کند و تغییر دهد. این کار با قرار دادن تصویر یک آدرس اینترنتی قانونی و موجه در نوار آدرس یا بستن نوار آدرس اصلی و باز کردن یک نوار آدرس جدید که حاوی آدرس اینترنتی قانونی و موجه است، انجام می شود.

یک فیشر(مهاجم) حتی می تواند از نقایص موجود در برنامه جاوا اسکریپت یک سایت معتبر و قانونی علیه قربانیان خوداستفاده نمایند. این نوع حمله ها) که به کراس سایت اسکریپتینگ معروف هستند) به طور خاص سخت و پیچیده هستند، چون آنها قربانی را به صفحه اینترنتی ثبت نام خدمات بانکی خود ارجاع می دهند. صفحه ای که در آن همه چیز از آدرس سایت گرفته تا گواهی امنیتی، همه درست و صحیح به نظر می رسند. در حقیقت لینک دادن به صفحه اصلی حقه ای برای به ثمر رساندن سرقت و انجام دادن حمله است. با انجام این کار کشف این حمله برای افرادی که دانش لازم را ندارند، کار بسیار سختی است. در سال ۲۰۰۶ چنین حمله ای علیه سایت Pay Pal انجام شد.

یک برنامه فیشینگ در سطح جهانی با عنوانMan-in-the-middle ، که در سال ۲۰۰۷ کشف شد، از یک رابط ساده استفاده می کرد که به فیشر (مهاجم) اجازه می داد به دون هیچ مشکلی سایت هایی خاصی را مجدداً ایجاد کند و جزئیات اطلاعات ورود یا لاگین افراد (نام کاربری و رمز عبور) وارد شده در وب سایت جعلی را برای ورود به سایت های اصلی ثبت و ضبط کند.

برای از کار انداختن تکنیک ها و برنامه هایی که وب سایت ها را با هدف پیدا کردن متون و علائم مرتبط با فیشینگ اسکن و بررسی می کنند، فیشرها به تازگی شروع به استفاده از وب سایت هایی کرده اند که با برنامه های فلش ،ساخته شده اند. این گونه سایت ها بسیار واقعی به نظر می رسند اما در واقع در این سایت ها متون و علائم مرتبط با فیشینگ پشت ظاهر برنامه های فلش پنهان شده اند.

فیشینگ از طریق تلفن

تمامی حملات فیشینگ نیاز به استفاده از یک وب سایت جعلی و ساختگی ندارند .این نوع حملات شامل پیام هایی هم می شوند که ادعا می کند از طرف بانک هستند و از مشتری ها (استفاده کنندگان خدمات بانکی) می خواهند با توجه به مشکلی که برای حساب های آنها به وجود آمده است، با یک شماره تماس

بگیرند. به محض این که مشتری با این شماره تلفن (که متعلق به مهاجم است و یک سرویس تلفن اینترنتی است) تماس بگیرد، دستوراتی به مشتری داده می شود تا شماره حساب و رمز خود را وارد کند. فیشرهایی که از سرویس تلفن اینترنتی استفاده می کنند، گاهی اوقات از داده های جعلی برای آی دی کالر استفاده می‌نمایند تا برای مشتریان این گونه به نظر برسد که این تماس از طرف یک سازمان مطمئن و معتبر انجام می شود.

سایر روش ها

- نوع دیگری از حمله که موفقیت آمیز بودنش ثابت شده است، ارجاع دادن قربانی به وب سایت اصلی بانک است. سپس یک پنجره پاپ آپ در بالای صفحه سایت به نمایش در می آید و به شکلی که به نظر برسد این صفحه و این سایت متعلق به بانک است، اطلاعات حساس قربانی را درخواست می کنند.

- یکی از جدیدترین روش های فیشینگ تب نبینگ است. این برنامه از صفحاتی که کاربر باز کرده استفاده می کند و به طور آهسته کاربر را به سایت ساختگی ارجاع میدهد.

- دوقلوهای شر یا Evil twins روشی است که شناسایی و کشف آن کار بسیار سختی است. یک فیشر یک شبکه بی سیم (وایرلس) ساختگی ایجاد می کند. این شبکه همانند شبکه های معتبر عمومی و قانونی می تواند در مکان هایی مانند فرودگاه ها، هتل ها و کافی شاپ ها وجود داشته باشد. وقتی که یک نفر وارد شبکه جعلی می شود، کلاهبرداران سعی می کنند رمزهای عبور و یا سایر اطلاعات مرتبط با کارت اعتباری او را ثبت و ضبط کنند.

قانون طلایی برای جلوگیری از فریب خوردن توسط فیشینگ این است که هرگز بر روی لینک‌های موجود در متن نامه کلیک نکنیم و همواره چنین ای- میلی را بلافاصله پاک کرده و پس از آن قسمت trash را هم خالی کنیم تا از کلیک اتفاقی بر روی آن جلوگیری کنیم.

فیشینگ چه عواقب و خساراتی برای قربانیان دارد؟

خسارت هایی که فیشینگ به بار آورده است، مشکلات زیادی از عدم دست یابی به ایمیل گرفته تا زیان های مالی قابل توجه را شامل می شود. عواقب، متعدد و چندگانه است. برای مثال ایمیل شما را جعل می‌کنند تا از آشنایانتان کلاهبرداری و از آنها پول درخواست کنند. این عمل می‌تواند خطرناک باشد چون شاید شما اطلاعات بانکی خود را داده باشید و هکر می‌تواند مبلغ زیادی پول از شما بدزد. در این نوع از فیشینگ، در سامانه «پی پال (PAYPAL) «که یک شرکت تجارت الکترونیکی است، در بخش آدرس ایمیل آن نوشته شده است «کیو پال دات آی تی (qpal. it) «که اصلا ربطی به پی پال ندارد. اگر بر روی لینک فشار دهیم صفحه سامانه پی پال جعلی باز می‌شود که خیلی خوب طراحی شده است. در این سامانه از ما می‌خواهند ثبت نام و آدرس ای میل و گذرواژه خود را تایید کنیم. ولی وقتی به نشانی وب نگاه کنیم، اصلا مطابقت نمی‌کند. این وب سایتی است که از **طریق فیشینگ جعل شده است.**

چگونه یک سایت فیشینگ را بشناسیم؟ تصویری

فیشینگ یا سرقت آنلاین در عمل به صورت کپی دقیق رابط گرافیکی یک وبسایت معتبر مانند بانک‌های آنلاین انجام می‌شود.

به عبارت ساده تر اینکه سارقان نوین یا همان هکر ها یک سایت که از نظر ظاهری کاملا مشابه سایت های بانک هاست طراحی کرده و ضمن فریب افراد اطلاعاتشان را سرقت میکنند و به طبع آن حساب فریب خوردگان خالی می شود.

به دو تصویر زیر دقت کنید کاملا مشابه می باشد و کمتر کسی می تواند حدس بزند که یکی از آنها توسط سارقات طراحی شده. تصویر اول متعلق به دروازه پرداخت بانک ملت می باشد و تصویر دوم توسط یک هکر حرفه ای و با هدف سرقت اطلاعات بانکی طراحی شده است.

دروازه پرداخت بانک ملت

سایت طراحی شده توسط یک هکر که به بهانه فروش دیش ماهواره اطلاعات بانکی افراد را سرقت می کرد!!

به تشابه این دو تصویر نیز دقت کنید. به قدری ماهرانه طراحی شده که کمتر کسی تصور می کند که یکی از آنها هیچ ارتباطی به بانک پاسارگاد ندارد و تنها اطلاعات شما را به دست هکرها می دهد.

دروازه پرداخت بانک پاسارگاد

این سایت فیشینگ به بهانه فروش کارت شارژ به سرقت اطلاعات می پرداخت

پس از اینکه فریب خوردگان کلیه اطلاعات خودشان را تقدیم سارق می کردندبدون اینکه شارژی دریافت کنند با پیغام بالا روبرو می شدند

لازم نیست بترسید. هکر ها هر چقدر هم بامهارت باشند بازهم تشخیص سایت های تقلبی چندان دشوار نیست کافی است آدرس پرداخت الکترونیک بانک خود را به درستی بشناسید . چراکه هیچ هکری نمی تواند آن را سرقت نماید.

آدرس صحیح برخی از دروازه های پرداخت بانک ها از این قرار است:

آدرس پرداخت اینترنتی بانک سامان sb24.com
آدرس پرداخت اینترنتی بانک پارسیان pec24.com
آدرس پرداخت اینترنتی بانک پاسارگاد BankPasargad.com
آدرس پرداخت اینترنتی بانک ملت bankmellat.ir
آدرس پرداخت اینترنتی بانک سین esinabank.com
آدرس پرداخت اینترنتی بانک ملی bankmelli-iran.com

دومین راه تشخیص سایت های فیشینگ هم در قسمت URL سایت کاملا واضح است. حتما دقت داشته باشید که در کنار آدرس سایت عبارت https://ذکر شده باشد.

کارشناسان وجود علامت قفل مانند در کنار صفحات آدرس ایترنتی را هم در تشخیص اعتبار سایت موثرمی دانند.

پس تنها در صورتی که به این دونکته ساده (آدرس پرداخت الکترونیک بانک و درجhttps در آدرس سایت دقت کنید)با خیالی راحت می توانید از یک خرید اینترنتی لذت ببرید.

راه درست: مهم ترین نکته ای که در این مورد باید در نظر داشته باشید این است که روی آدرس سایت دقیق شوید و اطمینان حاصل کنید. هنگام استفاده از این سایت ها سعی کنید ایمیل یا فیلترشکن روی دستگاه باز نباشد.

چگونه می‌توانیم از خود در مقابل فیشینگ محافظت کنیم؟

اول از همه باید به همه ایمیل‌های دریافتی شک کرد. در واقع ما می‌توانیم ایمیل‌هایی از اشخاص ناآشنا و همچنین دوستانی که ایمیلشان هک شده دریافت کنیم. باید به این نکته مهم توجه کنیم که هیچ شرکت معتبری اطلاعات شما را توسط ایمیل درخواست نمی‌کند.

پس هرگز نباید گذرواژه ایمیل خود را ارائه کنیم.

دقیقا. هرگز نباید اطلاعات شخصی مانند آدرس ایمیل، گذرواژه یا شناسه کاربری را ارائه کرد. چون همچنانکه گفتم، هکرها می‌توانند از دوستان، خانواده و همکارانتان از طریق فیشینگ یا شیوه‌ای دیگرکلاهبرداری کنند.

پیشنهادی دیگر...

اگر مورد مشکوکی مشاهده می‌کنید از گزارش آن به شرکت ارائه کننده خدمات اینترنت، سرویس‌های مبارزه با جرایم سایبری در اداره پلیس یا گروه های ایمنی تردید نکنید. این وظیفه آنهاست و برای این کار در دسترس هستند.

و آخرین پیشنهاد؟

هرگز نباید فایل پیوستی ایمیلی را که فرستنده آن را نمی‌شناسیم باز کنیم. چون شاید حاوی ویروس، پیام‌های فیشینگ یا چیزهای دیگر باشد. برای اطمینان بیشتر هرگز فایل‌های پیوستی را که از طرف دوستان، خانواده یا همکارانتان دریافت کرده‌اید باز نکنید.

پس چه موقعی می‌توانیم فایل پیوستی را با خیال راحت باز کنیم؟

وقتی واقعا از هویت فرستنده مطمئنیم و قبلا با او ایمیل رد و بدل کرده‌ایم، به او زنگ زده‌ایم یا حتی یک اس ام اس به هم فرستاده‌ایم.

ناگفته نماند که ایمیل‌های فیشینگ معمولاً دارای لوگوها و تیترهای رسمی از بانک‌ها یا موسسات مالی معتبر هستند و حاوی درخواست ارائه اطلاعات شخصی و حساس هستند.سازندگان این ایمیل‌ها معمولاً برای رسمی جلوه دادن بیشتر فعالیت‌های خود، لینکی از سایتی با ظاهری آراسته و رسمی به ایمیل‌های خود اضافه می‌کنند.

برای ایمن کردن خود در برابر حملات فیشینگ بهترین و کامل‌ترین راه، استفاده از ویروس‌یاب‌ها و برنامه‌های امنیتی به روز است ادامه داد:"بعضی از ایمیل‌های فیشینگ حاوی فایل‌ها و برنامه‌های مخرب نیز هستند به همین دلیل یکی از بهترین راه‌ها برای مقابله با آن‌ها به روز سازی نرم‌افزارهای امنیتی است..

جمع بندی : برای جلوگیری از حقه های فیشینگ به نکات زیر توجه فرمایید:

در مورد ایمیل های ناخواسته ای که از شما اطلاعات شخصی تان را درخواست می کنند، محتاط باشید.
فرم هایی را که در ایمیل ها فرستاده می شوند، پر نکنید.
همواره لینکی را که در ایمیل موجود است، با لینکی که واقعاً به آن ارجاع داده شده اید، مقایسه کنید.
به جای آن که روی لینک موجود در ایمیل ناخواسته کلیک کنید، مستقیماً به وب سایت رسمی مراجعه کنید.
برای آن که بررسی کنید ایمیل دریافتی معتبر و قانونی است، با شرکتی که گمان می کنید ایمیل را ارسال کرده است، تماس بگیرید.

در حملات فیشینگ به عنوان مثال صفحه‌ای مشابه یکی از سایت‌ها همچون بانک می‌سازند و با جابجا کردن یک حرف از سایت مورد نظر لینکی را درون ای میل قرار می‌دهند با این مضمون که برای تایید یا فعال‌سازی حساب خود بر روی آن کلیک کنید و در بعضی موارد تهدیداتی نیز انجام می‌دهند، مانند اینکه در صورت عدم تایید حساب از سوی لینک زیر، حساب شما به مدت یک‌ماه مسدود خواهد شد!هنگامی که کاربر روی لینک تقلبی کلیک کند، وارد سایت جعلی که از سوی نفوذگر ساخته شده می‌شود که کاملا شبیه سایت اصلی بانک است.

چگونه می توانیم از امن بودن یک وب سایت اطمینان حاصل کنیم؟

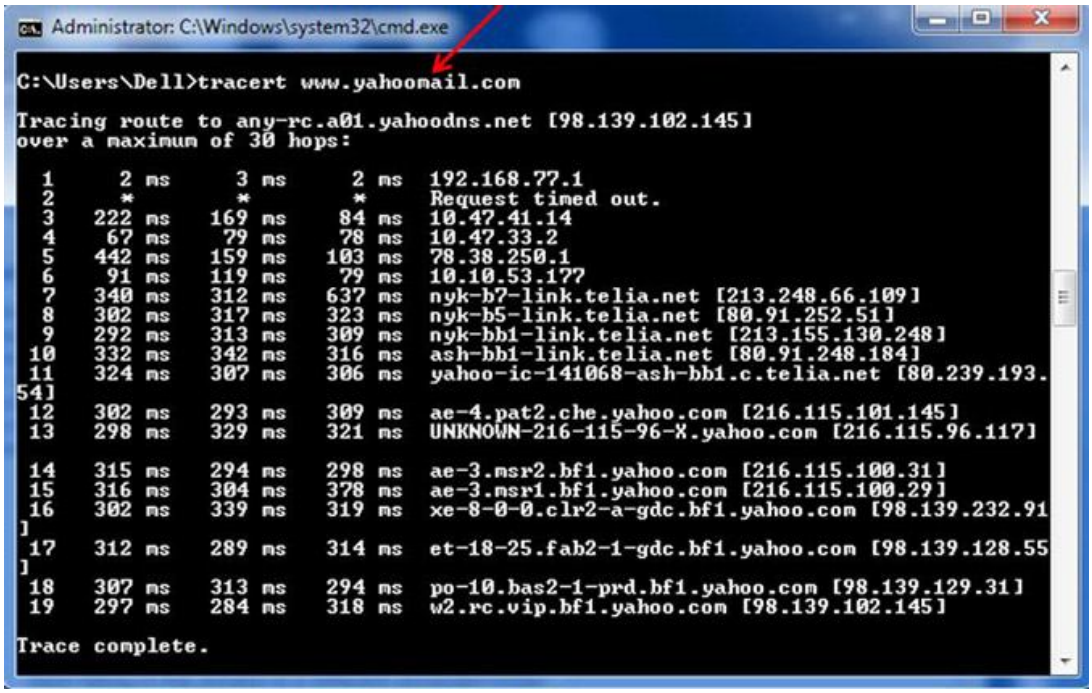
هرگاه یک وب سایت از شما اطلاعات حساسی را درخواست کرد، لازم است که آن را از جهت امن بودن مورد بررسی قرار دهید. توانایی تشخیص امن بودن یک وب سایت جهت جلوگیری از سوء استفاده و کلاهبرداری، بسیار حائز اهمیت می باشد.

زمانی که شما از یک وب سایت بازدید می کنید، اطلاعاتی از سوی کامپیوتر شما به وب سایت ارسال می گردد و همچنین بالعکس اطلاعاتی از سوی وب سایت برای کامپیوتر شما فرستاده می شود. این تبادل اطلاعات به صورت یک فایل دارای متن صورت می پذیرد و بدین معناست که شما قادر به خواندن آن می باشید.
نکته ی دیگری که شما لازم است در اینجا بدانید این است که هر قسمت از اطلاعات ارسالی شما از کامپیوتر ها و سرورهای زیادی عبور می کند تا به مقصد برسد.

در صورتی که شما تمایل دارید بدانید اطلاعات ارسالی شما از چه دستگاه هایی برای رسیدن به مقصد عبورمی کند، می توانید مراحل زیر را انجام دهید:

1. به منو استارت بروید.
2. در قسمت Run یا جستجو کلمه CMD را تایپ نمایید.
3. در پنجره CMD جمله روبرو را تایپ نماییدTracertwww.yahoomail.ir.
4. دکمه enter را فشار دهید.

در تصویر زیر شما می توانید سایت یاهو میل را مشاهده نمایید.



اطلاعاتی که در سایت یاهو میل نظیر کلمه کاربری و رمز عبور وارد می کنید از ۱۹ سرور یا گره عبور می کند تا به مقصد نهایی برسد. این اطلاعات در تمامی قسمت های زیر می تواند ذخیره گردد و قابل دسترس باشد. در بعضی موارد شما تا ۳۰ گره را مشاهده خواهید نمود.

شاید شما با فهمیدن این موضوع کمی در وارد کردن رمز دوم عابر بانک خود در سایت ها محتاط تر شده اید. راه حل برطرف کردن این ترس کد گذاری و به رمز درآوردن اطلاعات انتقالی می باشد. لایه درگاه امن یا همان SSL برای این موضوع طراحی و تعبیه گردیده است.

SSLاز یک سیستم پیچیده تغییر کلمات و رمزگذاری بین مرورگر اینترنتی شما و سرور استفاده می نماید. و زمانی که یک سایت از یکSSL فعال استفاده می نماید می توانیم بگوییم که آن سایت امن می باشد.

هر سایتی که از شما اطلاعات حساس و مهمی نظیر رمز عابر بانک را دریافت می نماید باید از SSL استفاده نماید!!

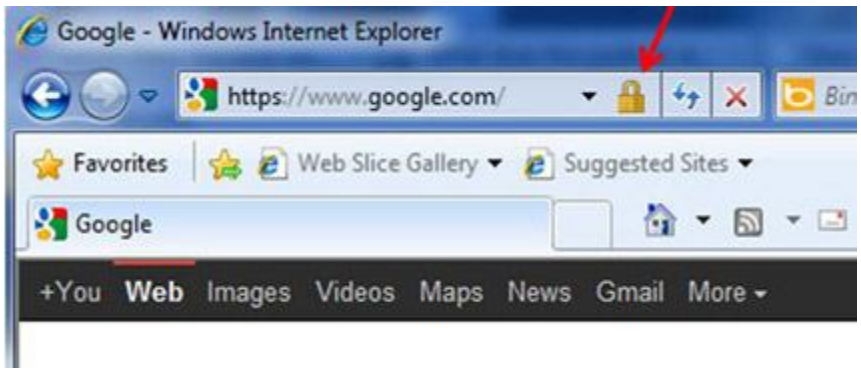
به طور کلی دو شاخص برای امن بودن یک وب سایت وجود دارد:

۱.در ابتدا آدرس وب سایت را بررسی نمایید.

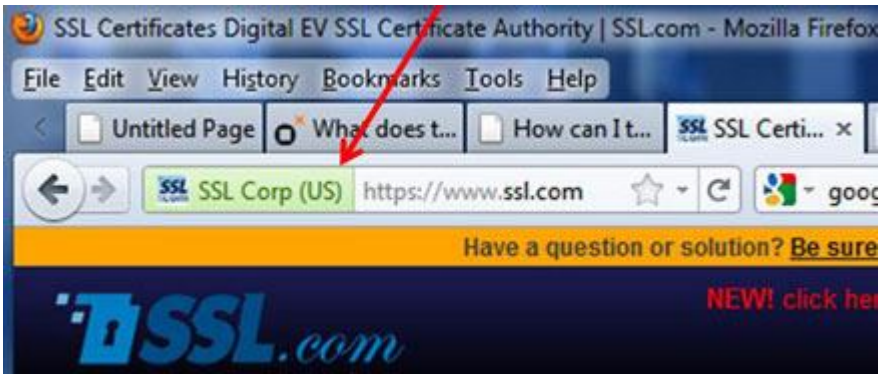
به طور معمول زمانیکه شما صفحه یک سایت را در مرورگر خود باز می کنید، آدرس آن وب سایت با "HTTP" آغاز می گردد و این بدان معناست که سایتی که شما وارد آن شده اید یک سایت امن نمی‌باشد. زمانی می توان از امن بودن یک وب سایت مطمئن شد که آدرس آن سایت با کلمه HTTPS آغاز گردد.

۲.بررسی نشان "قفل" بر روی سایت

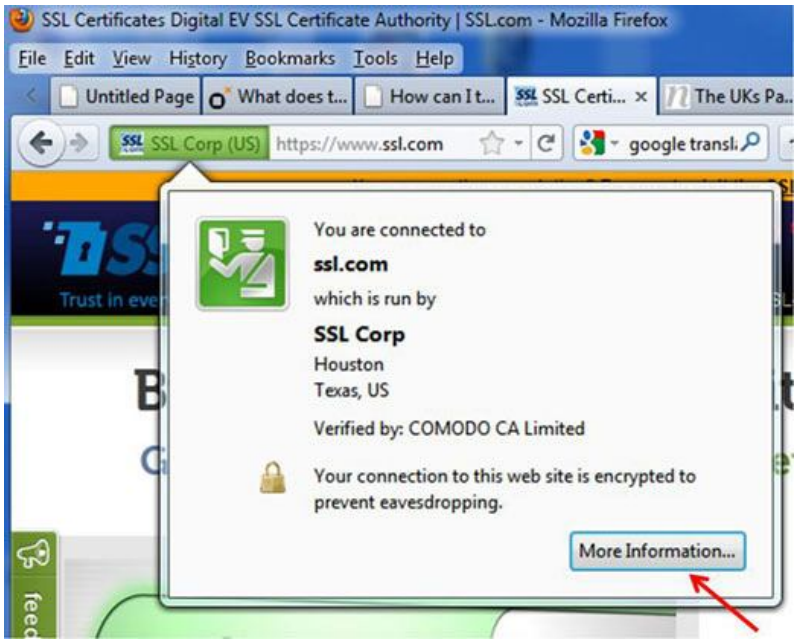
به عنوان مثال شما هنگامی که وارد سایت های www.gmail.com یا www.yahoomail.comمی شوید در قسمت آدرس مشاهده می کنید که بعد از "HTTP" حرف "S" قرار دارد و این بدان معناست که تمامی اطلاعاتی که شما وارد می کنید به صورت رمز و کدگذاری شده برای شخص مقابل ارسال می گردد. همچنین شما می توانید به صورت دستی حرف "S"را بعد از کلمه HTTP وارد نمایید و درصورت برخورداری این سایت از این پروتکل، وب سایت برای شما بصورت امن بارگذاری مجدد می گردد. در صورتی که آدرس وب سایت به صورت HTTPS بازگشایی گردید به عنوان مثال در مرورگرهای شرکت مایکروسافت شما علامت کوچکی به شکل یک قفل در قسمت انتهایی آدرس بار همانند تصویر زیر مشاهده خواهید کرد.



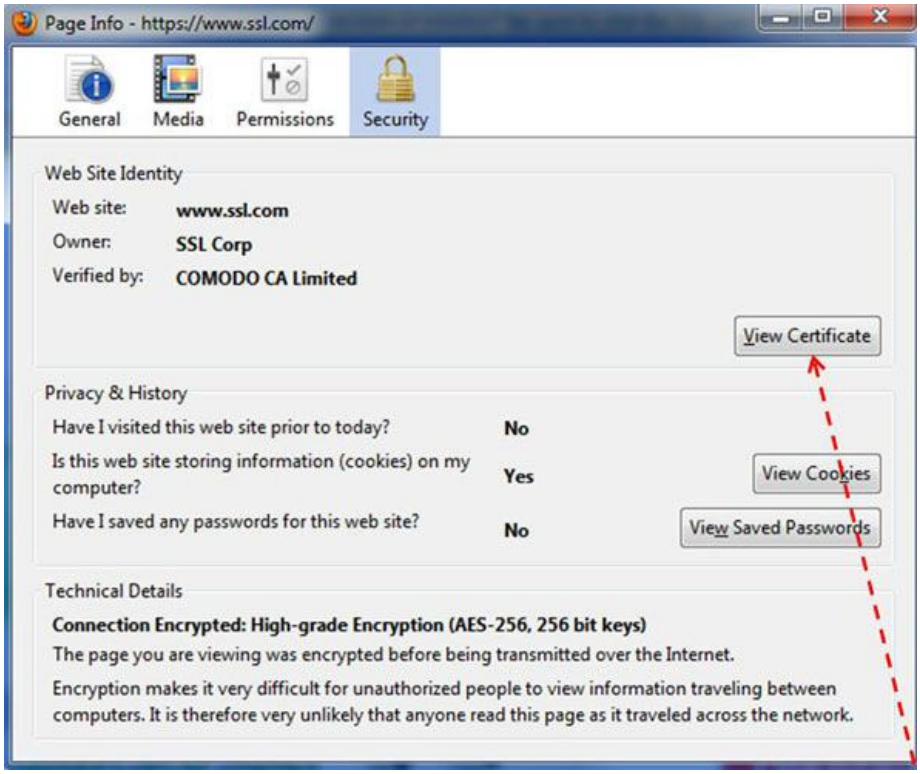
در مرورگرهایی نظیر فایر فاکس نشان امنیت سایت در قسمت نمایش داده شده در زیر قرار دارد.



با کلیک بر روی قسمت نشان داده شده در بالا کادر زیر نمایش داده می شود:



در صورت کلیک روی دکمه more information کادر زیر به نمایش درمی آید.



با کلیک بر روی قسمت view certificate کادر زیر که نشان دهنده گواهی اعتبار سایت می باشد، به نمایش درمی آید.

شاخص های دیگری که نشان دهنده امن بودن یک وب سایت می باشند

بسیاری از شرکت های ارائه دهنده گواهی SSL نظیر Verisign,Geotrust,,SSL.comنمادهای اعتمادی را برای دارندگان سایت فراهم می آورند برخی از خصوصیات این نمادها عبارتند از:

•به خوبی در معرض دید قرار دارند: صاحبان فروشگاه های آنلاین تمایل دارند که این نشان را به خوبی در معرض دید بازدیدکنندگان سایت قرار دهند .آنها با این عمل می‌خواهند احساس اعتماد و اطمینان را در بین مشتریان خود ایجاد نمایند.

•به سختی قابل تکثیر می باشند: این نشان ها بگونه ای طراحی می گردند که به سختی توسط کلاهبرداران و مجرمین اینترنتی قابل تکثیر باشد. این نمادها همچنین در تاریخ مشخصی که ذکر گردیده است منقضی می گردد.

•اتصال تائید کننده: با کلیک بر روی تمامی این نشان ها صفحه جدیدی به آدرس سایت صادر کننده گواهی باز می گردد که حاوی اطلاعاتی در مورد سایت مورد نظر می باشد.

پرداخت اینترنتی چیست؟

پرداخت اینترنتی به پرداختن پول از طریق اینترنت، در قبال دریافت کالا یا خدمات اطلاق می شود به طوری که این پرداخت بدون نیاز به حضور فیزیکی در بانک یا فروشگاه و از طریق اینترنت انجام شود. در واقع خریدار با استفاده از کارت بانکی خود می تواند از اینترنت خرید کند و پول آن را همان موقع و یا پس از دریافت کالا پرداخت نماید.

فرآیند پرداخت اینترنتی

مدیران سایت های اینترنتی با بانک ها قراردادی می بندند و به این ترتیب پول با همکاری بانک از طریق اینترنت از حساب مشتری به حساب مدیر سایت واریز می شود.

در حال حاضر بانکهای ملت، سامان، پارسیان، ملی، اقتصاد نوین و پاسارگاد این امکان را فراهم آورده اند که افراد بتوانند با استفاده از کارت های بانکی تحت شتاب، خرید اینترنتی انجام دهند. یعنی این بانک ها به عنوان دروازهٔ پرداخت یا درگاه پرداخت یا در اصطلاح Gateway عمل می کنند.

این به این معنی نیست که فقط کارت های همین ۵ بانک قابلیت خرید اینترنتی را دارد، بلکه به این معناست که این بانکها امکاناتی را فراهم کرده اند که بتوان با کارت سایر بانک ها نیز خرید اینترنتی کرد و این امکانات خود را در اختیار فروشگاههای اینترنتی قرار داده اند.

به این ترتیب شما پس از اطمینان از کالا یا سرویس سایت مورد نظر خود می توانید پول آن را به صورت آنلاین پرداخت نمایید.

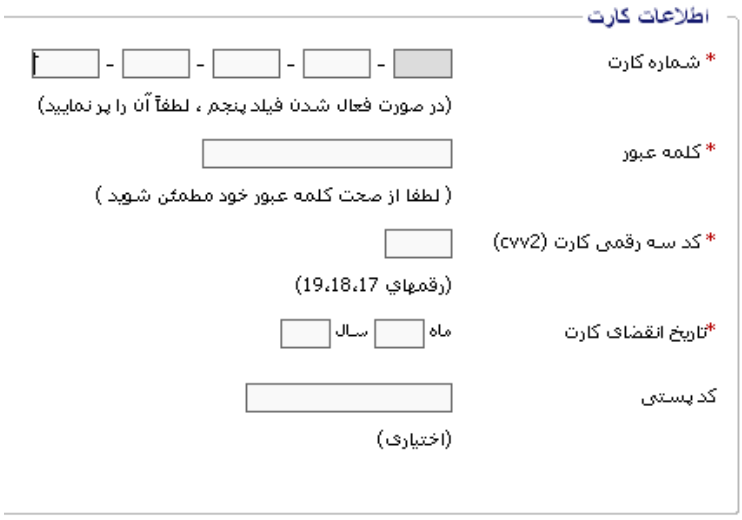
با چه کارت هایی می توان خرید اینترنتی کرد

کارت بانک های ملی، صادرات، پارسیان، سامان، اقتصاد نوین، پاسارگاد، ملت، کشاورزی، توسعه صادرات و صنعت و معدن و بانک سینا امکان خرید اینترنتی دارند.

کارت بانک های پست بانک، تجارت رفاه، سپه، مسکن، کارآفرین و سرمایه فعلاً قابلیت خرید اینترنتی ندارند.

پارامتر های لازم برای خرید اینترنتی

در هنگام خرید اینترنتی ۴ پارامتر کارت بانکی از شما پرسیده می شود که در عکس زیر کنارشان ستاره قرمز زده شده است.



در ادامه به بررسی تک تک این پارامترها می پردازیم:

۱- شماره ۱۶ رقمی درج شده بر روی کارت

این شماره در کارت همه بانک ها، بر روی کارت درج شده است. نمونه شماره کارت درج شده بر روی کارت های بانک ملی در عکس زیر آمده است.

۲- رمز خرید اینترنتی یا رمز دوم

رمز خرید اینترنتی، با رمزی که شما هنگام استفاده از دستگاههای خود پرداز ATM وارد می نمائید متفاوت می باشد. حتی این رمز با رمز اینترنت بانک که حساب خود را از طریق اینترنت چک می کنید، نیز متفاوت است.

در اکثر بانک ها زمانی که کارت خود را تحویل می گیرید، رمز خرید اینترنتی ندارید. برای فعال کردن رمز خرید اینترنتی یکی از کارهای زیر را انجام دهید:

۱- اکثر بانک ها امکان تعریف رمز خرید اینترنتی را در دستگاههای ATM خود قرار داده اند. به دستگاه خودپرداز بانک خود مراجعه کنید. کارت خود را وارد کنید و بخش عملیات رمز را انتخاب کنید. در بخش رمز دوم یا رمز اینترنتی، رمز خود را تعریف کنید.

۲- به شعبه بانک خود مراجعه کنید و بگویید می خواهم رمز خرید اینترنتی دریافت کنم. اگر بانکتان بانک خوبی باشد حتماً راهنمایی می شوید.

۳- کد CVV2

کد CVV2 به صورت یک عدد ۳رقمی (و به ندرت ۴رقمی) مانند شمارهٔ ۱۶رقمی حک شده روی کارت، بر روی اکثر کارت ها حک شده است. مثلاً روی کارت های بانک های ملت، صادرات، پاسارگاد، سامان، پارسیان و... به صورت یک عدد ۳رقمی حک شده است. یا در برخی کارت های بانک ملی ۴ رقمی است و عکس آن را در زیر مشاهده می نمایید.

در برخی کارت های بانک تجارت، کد CVV2 به صورت رقم ۱۷، ۱۸ و ۱۹ بعد از ۱۶رقم شماره کارت حک شده است.

۴- تاریخ انقضاء

تاریخ انقضاء هم روی اغلب کارت های بانکی حک شده است. اگر روی کارت شما تاریخ انقضاء وجود ندارد، نگران نباشید. از عدد ۱۲ به جای ماه و از ۹۹ به جای سال انقضای کارت استفاده نمایید.

مشکلات احتمالی پرداخت اینترنتی

سیستم پرداخت اینترنتی توسط بانک های عامل به گونه ای طراحی شده است که هم ایمن باشد و هم ساده و کمترین نیاز به راهنمایی را برای خریدار ایجاد نماید. اما با این وجود برخی اوقات ممکن است مسائلی در هنگام خرید اینترنتی به وقوع بپیوندد.

مثلاً ممکن است در هنگام پرداخت شبکه بانکی قطع شود و پرداخت ناموفق انجام شود.

معمولاً بدترین حالتی که ممکن است به وقوع بپیوندد این است که پول از حساب شما کسر شود، ولی به حساب فروشنده واریز نشود. اما نگران نباشید. در این حالت معمولاً پول شما در حساب های حد واسط بانک است.

نهایتاً خود بانک می باید مغایرت ها را رفع کند. منتظر بمانید و اگر تا ۴۸ ساعت پول به حسابتان برگشت نخورد، آنگاه با پشتیبانی سایت فروشنده و یا بانک عامل پرداخت اینترنتی تماس بگیرید تا مغایرت برطرف شود.

در صورتیکه تمایل به استفاده از این مطالب در سایت یا وبلاگ خود دارید، ترجیحاً از لینک به این صفحه استفاده کنید. چون این راهنماها خیلی زود قدیمی می شود و مفید بودن خود را از دست می دهد. این مطالب توسط سایت بانکی در همین صفحه به روز می شود.

۱۸ نکته امنیتی جهت استفاده از سیستم های پرداخت اینترنتی

بانک ملی ایران با هدف آگاهی بخشی به عموم مردم ، نکات لازم جهت استفاده ایمن از سیستم های پرداخت اینترنتی را اعلام کرد.

یکی از حربه های اصلی کلاه برداران اینترنتی، هدایت کاربران پرداخت های الکترونیکی به سمت سایت های مشابه سایت اصلی و ذخیره کردن اطلاعات شخصی کاربر و سوء استفاده بعدی از این اطلاعات است.

بر این اساس لازم است هنگام استفاده از درگاه های پرداخت الکترونیکی، کاربران از طریق کنترل محتوای آدرس بار (Address Bar) مرورگر (Browser)خود مطمئن شوند از پروتکل امن https به جای پروتکل ناامن http استفاده می شود و در عین حال کاربران حتماً از صفحه کلید مجازی موجود در سایت برای ورود اطلاعات بهره برند.

همچنین سیستم های مورد استفاده در تراکنش های مالی، حتماً باید دارای نرم افزارهای ضد ویروس (Anti virus) و ضد جاسوسی (Anti Spy)بوده، ضمن اینکه سیستم عامل و نرم افزارهای مذکور باید به روز باشند.

بر اساس این گزارش کاربران برای پرداخت های الکترونیکی بهتر است از رایانه های شخصی به جای رایانه های موجود در اماکن عمومی و کافی نت ها استفاده کنند.

حفظ اطلاعات محرمانه شخصی کاربری به شرح نام کاربری(User Name) ، کلمه عبور (Password) ، رمز دوم کارت و cvv2 و پرهیز از ارسال آنها به صورت نامه الکترونیکی و پیام کوتاه، تعویض فوری کلمه عبور و رمز دوم کارت در صورت افشای عمدی یا غیرعمدی آن ها و تعویض کلمات عبور در فواصل

حداکثر یک ماهه از دیگر تأکیدات بانک ملی ایران است.

ضمناً لازم است کاربران در انتخاب کلمه عبور و رمز دوم کارت دقت کافی را داشته باشند، بدین صورت که کلمات عبور به صورت ترکیبی از حروف کوچک و بزرگ و اعداد و علائم مجازی انتخاب شوند.

لازم به ذکر است خدمات الکترونیکی بانک ملی ایران صرفاً بر روی آدرس های www.bmi.ir و www.bankmelli-iran.com ارائه می گردد.

از رمزهای ساده استفاده نکنید. رمزهای خود را ترجیحاً به صورت ترکیبی از حروف کوچک و بزرگ و اعداد و علامتها انتخاب نمایید. توصیه می شود: از انتخاب شماره شناسنامه، کد ملی و تاریخ تولد خود و یا خانواده ، پلاک خانه و شماره تلفن خودداری نمایید.

نکات امنیتی

-رمز خود را جایی یادداشت نکنید و در صورت یادداشت نمودن، آن را در جیب یا کیف پول به همراه کارت قرار ندهید.

-رمزهای عبور خود را به صورت دوره ای تغییر دهید.

-رمز خود را در اختیار سایر افراد قرار ندهید.

-اطلاعات حساس از جمله رمز خود را از طریق تلفن برای دیگران بازگو نکنید.

-در صورت فاش شدن رمز خود، در کوتاهترین زمان ممکن آن را عوض نمایید.

-کارت و رمز خود را به هیچ وجه در اختیار دیگران قرار ندهید. بعضاً افراد سود جو به بهانه کمک کردن و راهنمایی ضمن اخذ کارت و رمز شما پس از انجام عملیات، کارت شما را با کارت دیگری (سرقتی ، مفقودی ، باطله و...) معاوضه نموده و حساب شما را مورد سوء استفاده قرار می دهند.

-در صورت انجام انتقال وجه و عملیات اینترنتی برروی حساب خود در مرورگرهای اینترنت گزینه ی به خاطرسپردن رمز را انتخاب نکنید. این گزینه با نام کلی Remember Password شناخته می شود، از این قابلیت استفاده نکنید.

-برای ارسال اطلاعات حساس خود از پست الکترونیکی استفاده ننمایید.

-همواره سعی کنید برای ورود رمز خود از امکان Virtual Keyboard بجای کیبورد فیزیکی کامپیوتر استفاده کنید. این امکان در سیستم عامل ویندوز و همچنین در برخی از سایتهای پرداخت آنلاین وجود دارد.

-شناسه عبور و رمز خود را بر روی کامپیوترهای خارج از اختیار و کنترل خود وارد نکنید.

-هنگام ورود به وب سایتها به ویژه وب سایتهایی که در آن اطلاعات محرمانه وارد می گردد، آدرس سایت مورد بازدید را در کادر نوار آدرس کنترل نمایید. بسیاری از کلاهبردارهای اینترنتی بواسطه استفاده از سایتهای جعلی و مشابه، جهت دریافت اطلاعات حساس کابران رخ می دهد.

-در صفحاتی که سایت مورد بازدید از شما درخواست ورود شماره کارت، رمز کارت، رمز دوم و CVV2 می نماید، حتماً مطمئن شوید که از پروتکل SSL استفاده شده است. بدین منظور آدرس صفحه می بایست با عبارت https بجای http آغاز گردد.

-همواره از نرم افزارهای آنتی ویروس معتبر و بروزشده استفاده نمایید.

-سیستم عامل کامپیوتر خود را همواره بروزرسانی کرده و آخرین وصله های امنیتی را دریافت نمایید.

-در صورتی که احتمال وجود برنامه های مخرب را بر روی کامپیوتر خود می دهید از انجام هرگونه تراکنش مالی آنلاین خودداری نمایید.

-پس از انجام کار مورد نیاز در وب سایتهایی که نیاز به رمز ورود دارند، به طور کامل Log out کنید.

-به مطالب نوشته شده در پنجره هایی که اتوماتیک نمایش داده می شوند توجه نموده و بلافاصله بر روی Ok یا Yes کلیک نکنید. بسیاری از برنامه های مخرب به همین شیوه بر روی کامپیوترها نصب می گردند.

-ایمیلهای دریافتی از منابع ناشناس را باز نکنید. به لینکهای ارائه شده در ایمیلها اعتماد نکنید، به عنوان نمونه بانکها و موسسات اعتباری هیچ گاه از طریق نامه های الکترونیکی اطلاعات محرمانه شما را درخواست نمی کنند. بنابراین هرگاه در صندوق پستی خود نامه هایی از این دست را مشاهده کردید به سرعت آن را حذف کنید. از داده های حساس خود نسخه پشتیبان تهیه نموده و در جایی امن نگهداری کنید.

نماد اعتما الکترونیکی

یکی از عوامل مهم توسعه تجارت الکترونیکی، ایجاد اعتماد و اطمینان در میان کاربران خدمات الکترونیکی می باشد.با توجه به بررسی های انجام گرفته ، مهمترین عوامل مراجعه و اعتماد خریداران به فروشگاه های مجازی به شرح ذیل می باشند :

۱. شناسایی مالک فروشگاه و امکان مراجعه در صورت بروز اشکال .
۲. کامل و صحیح بودن اطلاعات کالا یا خدمات ارائه شده .
۳. گارانتی محصولات و ارائه خدمات پس از فروش .
۴. واضح بودن روند برگرداندن کالا و بازپس گیری پول .
۵. محفوظ ماندن اطلاعات شخصی و مالی خریداران .
۶. تایید امنیت سایت توسط یک موسسه و مرکز ملی اعتماد .

طبق مطالعات انجام شده تائید فروشگاه مجازی توسط یک موسسه و مرکز ثالث ، بیشترین تاثیر در مراجعه و اعتماد خریداران به فروشگاه مجازی را دارد . در این حالت خریدار از محفوظ ماندن اطلاعات خود احساس امنیت بیشتری دارد و اگر از اطلاعات شخصی وی سوء استفاده شو د ، می تواند برای شکایت از فروشگاه مجازی متخلف به مراجع قانونی مراجعه نماید .

در ایران مرکز توسعه تجارت الکترونیکی مسئولیت ایجاد زیر ساخت های امنیت و اعطای نماد اعتماد الکترونیکی به فروشگاه های مجازی را برعهده دارد .

اعطای نماد اعتماد الکترونیکی برای وب‌سایت های تجاری با هدف قانونمند کردن و چارچوب دهی به فعالیت فروشگاه‌های مجازی در حال انجام می باشد. نماد اعتماد الکترونیکی به شکل یک علامت در بالای سایت‌هایی که از نظر قانونی فعالیت آنان مورد تائید است به نمایش در می آید. ساماندهی سایت‌های تجاری در کشور موثرترین گام برای ایجاد فضای تجارت الکترونیکی به‌خصوص B2C خواهد بود. به نحوی‌که مردم در هنگام خرید از طریق اینترنت با اطمینان از این‌که سایت‌ها به تعهدات خود در قبال آنان عمل خواهند کرد و حقوق مصرف کنندگان را به رسمیت می‌شناسند، اقدام به خرید می کنند.

خریداران می باید با جستجو در فهرست وب سایت های مورد تایید، از صحت "نماد اعتماد الکترونیکی" به نمایش درآمده در وب سایت ها اطمینان حاصل کنند.

چرا باید تا حد امکان از فروشگاه اینترنتی که نماد اعتماد الکترونیکی (Enamad) دارد، خرید نمائیم ؟

چون مرکز توسعه ی تجارت الکترونیک پس از بررسی فروشگاه اینترنتی و تطابق نحوه عملکرد آن با قوانین ،اقدام به اعطای نماد اعتماد الکترونیکی(اینماد) می نماید. همچنین به صورت مداوم تحت بررسی این سازمان قرار دارد و ملزم به رعایت قانون حمایت از مصرف کننده می باشد و در صورت تخطی از قوانین، نماد اعتمادش سلب خواهد شد.فروشگاه دارای نماد اعتماد الکترونیکی (اینماد) موظف است اگر شما در خریدتان با مشکلی مواجه شدید پاسخگوی سؤالات و مشکلات شما باشد، ضمن اینکه خطر ربوده شدن رمز دوم کارت و یا ارسال نشدن محصول و یا مشکلات دیگر وجود ندارد .

فروشگاه اینترنتی چیست ؟

به زبان ساده ، فروشگاه اینترنتی به وب سایتی گفته می شود که تعدادی کالا یا خدمات را در ویترین خود از طریق اینترنت عرضه می کند. مشتریان برای استفاده از آن خدمات یا کالاها می توانند به فروشگاه سفارش بدهند و حتی هزینه خدمات یا کالا را به صورت آنلاین و یا در محل پرداخت نمایند.

جهت اطلاع از فروشگاه های اینترنتی دارای نماد اعتماد الکترونیکی اینجا کلیک کنید

چگونه یک فروشگاه اینترنتی قابل اعتماد را تشخیص دهیم؟

پلیس فضای تولید و تبادل اطلاعات ناجا خطاب به کاربرانی که قصد دارند از طریق اینترنت خرید کنند تاکید کرد: این پلیس هیچ فروشگاه اینترنتی یا وب سایتی را به طورخاص تائید نکرده، بنابراین استفاده از لوگوی این پلیس درصفحات وب سایت‌ها به هرعنوان از قبیل توصیه پلیس فتا و ... صحت نداشته و اقدام غیرقانونی است.

معاونت اجتماعی پلیس فضای تولید وتبادل اطلاعات ناجا درگزارشی با بیان اینکه درچند سال اخیر شاهد تبلیغات زیادی درفضای مجازی هستیم اعلام کرد: درحالی که خرید آنلاین کالا و خدمات، از با ارزش‌ترین خدماتی است که برروی اینترنت ارائه می‌شود اما متاسفانه بعضی مجرمان با استفاده از فضای سایت‌هایی که محل ارائه تبلیغات رایگان هستند اقدام به تبلیغ انواع کالاها کرده و پس از فریب افراد و واریزکردن وجوه توسط مشتری از ارسال کالا خودداری می‌کنند.

پلیس فتا علاوه برکنترل و نظارت بر سایت‌های ارائه‌دهنده خدمات تبلیغ رایگان و فروشگاه‌های اینترنتی، توصیه‌هایی را نیز برای پیشگیری به کاربران اعلام می‌کند.

*هنگام خرید آنلاین از معتبربودن فروشگاه الکترونیکی موجود مطمئن شده و حدالامکان کالای مورد نظرتان را از وب‌سایت‌های معتبرکه توسط وزارت بازرگانی تائید شده‌اند یا قبلاً دوستان وآشنایان از آن خرید کردند،خریداری کنید.

*به فروش ارزان یک کالا در فروشگاهی نسبت به سایر فروشگاه‌ها اعتماد نکرده و حتما تحقیق کنید.

*اگر یک فروشگاه اینترنتی از آرم‌هایی که توسط بعضی ارگان‌ها برای اعتبار یک وب‌سایت به آن اعطا می‌کنند، استفاده کرده حتما اعتبار آن را بسنجید تا از جعلی نبودن آن اطمینان حاصل کنید.

*فروشگاه‌های اینترنتی موظف به درج مشخصات کامل فنی و عکس واقعی کالا و ارائه ضمانت نامه‌های معتبر هستند و نباید از عکس‌های عمومی آن کالا برای معرفی طرح‌های مختلف کالای مورد نظر استفاده کنین و نیز اگر برای فروش بیشتر کالا اقدامات تشویقی از قبیل تخفیف یا اعطای هدایای رایگان مثل سی‌دی آموزشی و ... در نظرگرفته‌اند باید بطور کامل به تعهدات تشویقی خود عمل کنند.

*درهنگام پرداخت وجوه، آدرس صفحه درگاه بانک الکترونیکی، متعلق به همان بانکی باشد که آرم و لوگوی آن را در صفحه مشاهده می‌کنند و این نکته که در نوار آدرس کنار آدرس اینترنتی صفحه پرداخت بانک، نماد یک قفل یا عبارت https:// درج شده باشد، درغیر این صورت قطعاً صفحه جعلی است و قصد کلاهبرداری دارد.
*پلیس فضای تولید و تبادل اطلاعات در ادامه این گزارش عنوان کرد که این پلیس هیچ فروشگاه اینترنتی یا وب سایتی را بطورخاص تائید نکرده و بنابراین استفاده از لوگوی این پلیس در صفحات وب سایت‌ها به هرعنوان از قبیل توصیه پلیس فتا و ... صحت نداشته و اقدام غیرقانونی است.
در پایان این گزارش آمده است که بدیهی است؛ رعایت نکردن هریک از این موارد مصداق کلاهبرداری بوده و ضمن خرید نکردن، موارد را ازطریق وب‌سایت پلیس فتا به آدرس www.cyberpolice.ir به این پلیس گزارش کنند.

چگونه با اطمینان خاطر،خرید خود را از طریق اینترنت انجام دهیم؟

چگونه در اینترنت به خرده فروشان اعتماد کنیم و در دام دسیسه های کلاهبرداری نیافتیم؟ هر روز میلیون ها نفر بدون هیچ گونه مشکلی در اینترنت خرید می کنند. با داشتن کمی شجاعت و دانش، شما می توانید از ایجاد مشکلات مربوط به تجارت الکترونیکی جلوگیری نمائید .

خطرات:

- خرید کالاهایی که تحویل داده نمی شوند.
- ارائه کالاهایی که با خصوصیات گفته شده در سایت مطابقت ندارند.
- تاخیر ها و زحمت هایی که خرید آنلاین دارد.
- خدمات ضعیف پس از فروش
- سوء استفاده از کارت های اعتباری شما

با فروشندگان مطمئن و معروف معامله کنید:

- فروشندگان دارای اعتبار را انتخاب کنید. مخصوصاً زمانی که از اشخاص خاصی خرید می کنید.
- در جستجوی مدارک واقعی مانند جزئیات آدرس و شماره تلفن برای برقراری ارتباط باشید.
- فقط با بازدید از وب سایت افراد یا شرکت ها در مورد آنها قضاوت نکنید.
- وقتی که در حال خرید از شرکت های خارجی هستید، به طور خاص خیلی حساس باشید.
- سیاست فروشندگان در حفظ حریم شخصی و بازپرداخت مبلغ کالا را بررسی نمائید.
- از روش های مناسب و ایمن برای پرداخت پول در اینترنت استفاده کنید تا در صورت عدم تحویل کالا از اطلاعات مالی و بانکی شما تا حدی محافظت شود.

از یک وب سایت مطمئن استفاده کنید.

- اطمینان حاصل کنید که از یک وب سایت مطمئن برای وارد کردن اطلاعات کارت اعتباری خود استفاده می کنید. در گوشه پایین سمت راست پنجره مرورگر خود به دنبال نشانه ای از قفل (Padlock) باشید و اطمینان حاصل کنید که آدرس وب سایت با (https://) آغاز می شود.
- اگر شما از آخرین نسخه مرورگر خود استفاده می کنید و وب سایت اینترنتی فروشگاه از جدیدترین تکنولوژی امنیتی مانند نسخه جدید و معتبر شناسه امنیتی SSL استفاده می کند، ممکن است وقتی که از یک وب سایت مطمئن بازدید می کنید، نوار آدرس شما سبز شود.

•اگر اخطاری در ارتباط با شناسه امنیتی سایت دریافت کردید، خیلی حساس و محتاط باشید. در هر حال، قفل (Padlock) نشانه ای دقیق از وجود امنیت در سایت نیست و هیچ ارتباطی با اصول اخلاقی مورد استفاده صاحبان سایت ندارد .

•بر روی قفل (Padlock) کلیک کنید تا بتوانید ادعای فروشنده در مورد هویتش را ببینید و بررسی کنید که آیا شناسه امنیتی آنها در آدرس درست و واقعی ثبت شده است یا خیر.

•اطلاعاتی که توسط قفل (Padlock) روی صفحه ظاهر می شود، نباید شما را فریب دهد. برای صاحبان اصلی سایت کپی کردن تصویر یک قفل (Padlock)کار آسانی است. شما باید به دنبال قفلی (Padlock) باشید که در پنجره اصلی خود مرورگر وجود دارد .

از دسیسه های کلاهبرداری بر حذر باشید.

•اگر شرایط (یک معامله) خیلی بیشتر از حد واقعی ،عالی به نظر برسد، احتمالاً حقه ای در کار است. در اینترنت به بررسی اطلاعات راجع به این شرکت بپردازدید و بررسی کنید که آیا شخصی قبلاً با این مشکل مواجه شده است .

•از طرح های کار در خانه که وعده می دهند به راحتی می توانید درآمد کسب کنید و هیچ وقت هزینه ای نپردازید، اجتناب کنید .

•از شرکت های معتبر خرید کنید.

•به شدت از هر چیزی که در پیام های ناخواسته یا هرزنامه ها (Spam) ارائه و تبلیغ می شود، اجتناب و دوری کنید .

فروش آنلاین

اگر شما شرکتی دارید که بخش فروش آنلاین دارد،:

•مشتریان و عرضه کنندگان جدید را از طریق اطلاعات منتشر شده در مورد آنها (مانند شماره تلفن یا آدرس) شناسایی کنید.

•قبل از ارسال هر نوع کالایی به صورت نسیه، گزارشی از وضعیت اعتباری مشتریان خود تهیه کنید.

•شرکت های تجارت الکترونیک در قبال هر نوع کلاهبرداری از کارت های اعتباری مسئول هستند.

•استفاده از سیستم های بررسی هویت و اعتبار آدرس (AVS) و شماره امنیتی کارت (CSC) می تواند به گونه ای موثر خطرات تقلب و کلاهبرداری در تجارت الکترونیک را کاهش دهد.

•تایید اعتبار مشتری پرداخت مبلغ پول را تضمین نمی کند و بنابراین شرکت ها باید تمامی بررسی ها برای تایید اعتبار مشتری و آدرس مشتری برای تحویل کالا را انجام دهند.

برخی معیارهای اعتبار سنجی برای فروشگاه های اینترنتی

نکته کاملاً روشن و واضح در مطالعه قوانین و دستوالعمل های کشورها در زمینه فروشگاه های اینترنتی این است که در اکثر موارد مفاد یکسانی برای کنترل و نظارت در این زمینه لحاظ گردیده است. در همین راستا مؤسسات خصوصی و نیمه خصوصی، استانداردهایی را برای اعتبار سنجی فروشگاه های اینترنتی لحاظ کرده اند.

درمطلب زیر به برخی از این مفاد و استانداردهای مشترک اشاره می کنیم:

۱.تعیین مدت زمان باز پسگیری کالا (حداقل تا اتمام مدت هفت روز کاری پس از دریافت کالا(

۲.بازگشت کامل هزینه خرید، پس از اطلاع از مرجوعی، بدون کسر هزینه برای حمل اولیه و دیگر هزینه ها

۳.ارائه سیاست های قیمت گذاری ثابت و مشخص

۴.دسترسی آسان به شرایط و ضوابط

۵.دسترسی به اطلاعات و مشخصات کامل واسطه از قبیل: آدرس، شماره تلفن و...

۶.ارائه اطلاعاتی از قبیل نام، ویژگی های اصلی کالا یا خدمات، هزینه ارسال، مدت زمان اعتبار و...توسط فروشنده یا بنکدار

۷.ارائه اطلاعاتی خاص توسط فروشنده به صورت کتبی از طریق (ایمیل ،نامه ،فکس) که این نامه کتبی باید حداکثر در زمان سفارش دادن یا ارسال سفارش یا شروع خدمات، به خریدار برسد.

۸.اطلاعات کتبی باید شامل زمان و نحوه انصراف از سفارش ،آدرس کامل ،جزئیات هر گونه گارانتی، و مشخص کردن اینکه هزینه پس فرستادن کالا با خریدار است یا فروشنده، باشد.

۹.پس از گذاشتن سفارش، خریدار حق دارد که سفارش خود را به هر دلیلی کنسل نماید. ولی چند استثناء وجود دارد که شامل موارد زیر می باشد:

- ♦کالایی که دارای تاریخ انقضای زودرس است.
- ♦نرم افزار ،دی وی دی و غیره که پلمپش باز شده است.
- ♦روزنامه، نشریات یا مجلات
- ♦قیمتی که با نوسانات بازار مرتبط باشد.
- ♦کالاهای فصلی

۱۰.در صورتی که تمام اطلاعات داده شده در مورد کالا تا سه ماه محقق نشود خریدار می تواند سفارش را کنسل نماید. اگر فروشنده این اطلاعات را دیر به فرد بدهد ولی هنوز سه ماه تمام نشده باشد، هفت روز از زمان اطلاعات وقت دارد که سفارش خود را کنسل نماید.

۱۱.خریدار باید انصراف خود را به صورت کتبی، از طریق نامه، فکس یا ایمیل به اطلاع فروشنده برساند.

۱۲.اگر خریدار قبلا پولی بابت کالا یا خدمات پرداخته است، فروشنده باید نهایتاً تا ۳۰ روز پس از توافق بر سر انصراف، پول را بازگرداند.

۱۳.خریدار در زمان های مشخص شده در زیر می تواند خرید خود را کنسل نماید.

- ●هفت روز کاری پس از دریافت کالا
- ●هفت روز کاری پس از آنکه فروشنده موافقت کرد تا خدماتش را شروع کند .

۱۴.رعایت استاندارد های خاص توسط شرکت ارائه دهنده خدمات از قبیل:

- ●حفاظت از حریم خریدار
- ●دقت در امنیت پرداخت
- ●اطلاع رسانی درست در خصوص موارد توافق شده

چرا مردم در فضای آنلاین خرید می‌کنند؟

رضایت خاطر یکی از مهمترین عوامل است بر اساس نظر سنجی های صورت گرفته یکی از دلایل اصلی خرید اینترنتی رضایت خاطر افراد می باشد این رضایت خاطر در مواردی نظیر دستیابی راحت به کالاها و توانایی پیدا کردن هر آنچه می خواهند می باشد. یکی دیگر از عوامل بسیار مهم در رضایت خاطر مشتریان این است که خریداران می توانند از خطرات و زحمات خرید به صورت غیر مجازی(سنتی) مانند حمل کالاها جلوگیری کنند. در نظر سنجی که اخیراً صورت گرفته است بسیاری از افراد جلوگیری از رفت و آمد را به عنوان یکی از اصلی ترین عوامل رغبت برای خرید اینترنتی ذکر کرده اند .در همین نظر سنجی شخص اظهار داشته که من می توانم راحت در خانه خود بنشینم و جزئیات کالایی را که می خواهم وارد نمایم و مجبور نیستم به دنبال جای پارک بگردم و در صف مغازه ها بایستم .

انتخاب یکی دیگر از عوامل مهم در روی آوردن مردم به خرید اینترنتی، تنوع کالاها در فضای اینترنت می باشد. در نظر سنجی های صورت گرفته افراد انتخاب بیشتر و مقایسه ی قیمت ها را از عوامل اصلی خرید خود در اینترنت ذکر کرده اند. به خصوص افرادی که در مناطق روستایی و دور افتاده زندگی می کنند و در منطقه خود به یکسری از کالاها دسترسی ندارند، می توانند از طریق خرید اینترنتی و بدون مراجعت به شهر کالا خود را خریداری کرده و آن را در محل زندگی خود دریافت کنند.

مشاهده قیمت های پایین تر به عنوان یک عامل مالی در روی آوردن مردم به خرید اینترنتی بسیار مهم می باشد. در نظر سنجی های صورت گرفته افراد بسیاری دستیابی به قیمت های پایین تر را از دلایل اصلی برای انجام خرید اینترنتی ابراز کرده اند .

اطلاعات و دسترسی جامع به آن در فضای اینترنت از عوامل دیگری است که موجب تشویق افراد به خرید از اینترنت می گردد. قسمت اعظم این اطلاعات از راه مقایسه سایت ها برای خریداران فراهم می گردد.

آیا شما هم از فروشگاه‌های الکترونیکی خرید می‌کنید؟

کارشناس پلیس فتا گفت: با توجه به رشد روز افزون فعالیت‌های اقتصادی در حوزه فضای مجازی امروزه شاهد استفاده از فروشگاه الکترونیکی به منظور تأمین نیازهای کاربران در سطح اینترنت هستیم .

متأسفانه مردم به هشدارهای پلیس فتا در این خصوص توجه نکرده‌اند و همچنان از فروشگاه‌هایی که دارای اعتبار لازم نیستند خرید کرده و بسیاری از آنها با مشکلات عدیده‌ای مواجه شده‌اند.

عدم توجه به تذکر پلیس فتا در خصوص خریدهای اینترنتی موجب شده تا بعد از اینکه فرد از یک وب‌سایت غیر معتبر خرید کرده و وجه را از طریق درگاه الکترونیک یکی از بانک‌های عضو شتاب پرداخت می‌نماید حتی بعد از گذشت ماه‌ها موفق به دریافت کالا و یا خدمات خریداری شده نگردیده و با پیگیری‌های وی وجه پرداختی نیز مسترد نشده است، از این رو پلیس فتا به کلیه کاربران اینترنتی که قصد خرید الکترونیکی را دارند توصیه اکید می‌کند تا از فروشگاه‌هایی که دارای نماد اعتماد الکترونیک از مرکز توسعه تجارت الکترونیک وزارت صنعت و معدن تجارت هستند خرید نمایند.

کلیه کاربران می توانند لیست فروشگاه‌هایی که دارای نماد الکترونیکی از مرکز توسعه تجارت الکترونیک وزارت بازرگانی می‌باشند را از سایت enamad.ir دریافت نمایند.

در نهایت پلیس فتا از کلیه کاربران می خواهد در صورت مواجه با موارد مشکوک آن را از طریق وب‌سایت پلیس فتا به آدرس Cyberpolice.irبخش گزارش تخلف فروشگاه‌های اینترنتی با ما گزارش نمایند.

نکاتی قبل از خرید از فروشگاه های اینترنتی که باید بدانید

پیشنهاد می نمائیم قبل از مبادرت به خرید کالا یا خدمات رعایت این موارد را بررسی نمایید:

مصرف کنندگان در زمان خرید از فروشگاه های اینترنتی باید حداقل به مدت ۷ روزکاری از تاریخ قبول و تحویل کالا یا خدمات حق انصراف داشته باشند و بابت درخواستی که برای انصراف در خرید دارند به همراه ارائه دلیل هیچ هزینه ای را به عنوان جریمه پرداخت ننمایند.

اعمال حق انصراف از جانب مصرف کننده به ترتیب زیر خواهد بود:

♦در خصوص خرید کالا از زمان تحویل کالا و در امور خرید خدمات از روز انعقاد لحاظ خواهد شد.

♦بعد از درخواست مصرف کننده جهت استفاده از حق انصراف، فروشنده مکلف است بدون مطالبه ی هیچگونه وجهی عین مبلغ دریافتی را در اسرع وقت به مصرف کننده مسترد نماید.

♦در هر حال آغاز اعمال حق انصراف مصرف کننده پس از ارائه اطلاعاتی خواهد بود که فروشنده طبق مواد (۳۳) و (۳۴) قانون تجارت الکترونیکی موظف به ارائه آن است.

در موارد زیر به علت شرایط خاص کالا و خدمات، حق انصراف ۷ روزه اعمال نمی شود و ادعای بازگشت هزینه به استناد حق انصراف از سوی مصرف کننده پذیرفته نخواهد شد. مگر اینکه طرفین به نحو دیگری توافق نمایند:

♦درمورد ارائه خدمات، در صورتی که با توافق مصرف کننده ارائه آن قبل از پایان هفت روز کاری شروع شده باشد. همچنین خدماتی که برای تحویل مواد غذایی یا سایر کالاهایی که مورد مصرف روزانه قرار می گیرند.

♦کالا یا خدماتی که قیمت آنها وابسته به نوسانات بازار مالی می باشند و خارج از اختیار فروشنده است.

♦کالاهایی که به درخواست شخصی مصرف کننده و با مشخصات فردی وی ساخته می شوند و یا اینکه به دلیل طبیعت آنها قابل بازپس گیری نیستند و نیز در مدت کوتاهی قابلیت فاسد شدن و خرابی دارند.

♦نوارهای صوتی و تصویری و نرم افزارهای رایانه ای بسته بندی شده که به وسیله مصرف کننده باز شده و یا مورد استفاده قرار گرفته باشند.

♦روزنامه، نشریه و مجلات مطابق تعریف قانون مطبوعات.

مصرف کننده باید نسبت به صحت نشانی وب سایت تجاری و آدرس تجاری طرف قرارداد خود اطمینان حاصل نموده و اسناد و مدارک تأیید کننده سفارش خود در وب سایت را برای جلوگیری از بروز مشکل یا پیگیرهای آتی به نحو مقتضی حفظ نماید.

قبل از پرداخت قیمت کالا یا خدمات درخواستی، از متناسب بودن قیمت مطمئن شوید. همچنین از وجود کالای عینی یا خدمات ارائه شده در بازار سنتی ،علاوه بر فضای اینترنت، اطمینان حاصل کنید و توجه داشته باشید کالا یا خدمات مورد نظر صوری و یا به صورت مجازی نباشد.
از آنجا که به استناد بند «د» ماده ۴۲ قانون تجارت الکترونیکی، خرید از حراجی ها تحت پوشش قواعد حمایت از مصرف کننده قرار نگرفته و متولی حراجی علی القاعده، مسئولیتی نسبت به مشکلات احتمالی ناشی از خرید ندارد، لازم است مصرف کننده توجه و دقت لازم را در زمان خرید از این فروشگاه ها از حیث رابطه قراردادی و حدود مسئولیت میزبان حراجی و پیشنهاد دهنده ی فروش و نیز اعتبار پیشنهاد ارائه شده و شخص پیشنهاد دهنده به عمل آورد.
به منظور جلوگیری از بروز مشکل در اجرای مواد ۳۷ و ۳۸ قانون تجارت الکترونیکی لازم است، مصرف کننده انصراف خود را از انعقاد یا ادامه قرارداد از طریق نامه، فکس یا ایمیل به اطلاع فروشنده رسانده و تأئیدیه ی اطلاع مخاطب از قصد خود را نیز دریافت نماید. به نحوی که ابزار مورد استفاده برای ارسال قصد مصرف کننده و تأئیدیه ی دریافتی از سوی ایشان قابلیت استناد و اثبات اعمال حق انصراف وی را داشته باشد.
در هنگام خرید هرگز شماره رمز عبور کارت خود را اعلام ننمائید، مگر اینکه مطمئن شوید درخواست کننده به نمایندگی از بانک عامل شما این درخواست را

نموده است. در این صورت نیز بلافاصله در فرصت مناسب نسبت به تغییر رمز خود اقدام نمایید.کالا و خدمات ارائه شده نباید مشمول منع تبلیغات عمومی طبق قوانین کشور باشد. همچنین کالا و خدمات ارائه شده باید دارای مجوز فروش طبق قوانین داخلی کشور باشد .هیچ گاه نسبت به انجام خرید اجباری اقدام ننموده و هنگام خرید از پرداخت هزینه حق عضویت خودداری نمایید.

هنگام پرداخت الکترونیک مراقب هکرها باشید!

سارقان نوین یا همان هکرها، یک سایت که از نظر ظاهری کاملا مشابه سایت های بانکهاست طراحی کرده و ضمن فریب افراد اطلاعاتشان را سرقت میکنند و به طبع آن حساب فریب خوردگان خالی می شود.

امنیت در خرید اینترنتی

اگر قصد خرید اینترنتی از یک فروشگاه الکترونیکی را دارید باید با چشمانی باز این کار را انجام دهید. ما نمی خواهیم خرید اینترنتی را یک کار عجیب و سخت جلوه دهیم اما وقتی شما به صورت فیزیکی هم خرید می کنید مطمئنا از یک مکان معتبر خرید خود را انجام می دهید. خرید اینترنتی شاید ساده ترین و لذت بخش ترین کاری باشد که شما در اینترنت می توانید انجام دهید به شرطی که به یک سری نکات مهم توجه داشته باشید.

خرید اینترنتی از فروشگاه های معتبر

قبل از خرید اینترنتی در مورد فروشگاهی که می خواهید از آن خرید کنید تحقیق کنید. فروشگاه های معتبر عموما آدرس پستی، تلفن و مشخصات خود را به طور دقیق در وب سایت شان درج می کنند. دقت کنید که فروشگاهی که از آن خرید می کنید یک فروشگاه فعال است یا یک وب سایت رها شده. در نظر داشته باشید تعداد زیادی وب سایت رها شده در اینترنت وجود دارند که روزی به مشتریان خود سرویس دهی می کردند اما به علل مختلف بی استفاده مانده اند اگر از طریق تبلیغات با فروشگاه آشنا شدید تقریبا می توان اطمینان داشت که فروشگاه مورد نظر فعال است، اما اگر به طور اتفاقی وارد فروشگاه شدید باید بررسی بیشتر نمایید. معمولا وب سایت های فعال بخش اخبارشان به روز است به عنوان یکی از نشانه های به روز بودن فروشگاه می توان در نظر گرفت است و یا اینکه بررسی کنید اطلاعات تکمیلی در مورد کالا به همراه قیمت و شرایط و هزینه های ارسال درج شده باشد. معمولا فروشگاه هایی که یک شعبه ی فیزیکی دارند بسیار مطمئن تر از فروشگاه هایی هستند که فقط به صورت مجازی پایه گذاری شده اند و آمارها نیز نشان می دهد اعتماد افراد به فروشگاه هایی که شعبه ی فیزیکی دارند بیشتر است. زیرا احتمال کلاهبرداری و یا این که کالای خریداری شده به دست شما نرسد کمتر است و اگر مشکلی پیش بیاید می توانید به آدرس فروشگاه مربوطه مراجعه کنید.

انتخاب روش خرید مناسب

وقتی از یک فروشگاه مجازی معتبر خرید می کنید معمولا انتخاب های متعددی برای نحوه خرید و دریافت کالا برای شما وجود خواهد داشت. از جمله پرداخت وجه به صورت آنلاین، خرید به صورت پستی، واریز به حساب و .... همیشه سعی کنید روشی برای خرید خود انتخاب کنید که کمترین ریسک پذیری را داشته باشد.

خرید به صورت آنلاین

معمولا فروشگاه هایی که ارائه دهنده سرویس های آنلاین هستند خدمات پرداخت اینترنتی خود را از یکی از بانکهای کشور دریافت می کنند و بانک ها نیز معمولا بابت ارائه این نوع سرویس از فروشگاه ها مبالغی بابت ضمانت دریافت می کنند. تا در مواردی که از فروشگاه مربوطه شکایتی صورت گرفت مورد اجرا قرار دهند. استفاده از این سیستم بیشتر در مواقعی مناسب است که شما محصول خود را می خواهید به صورت الکترونیکی دریافت کنید مانند خرید کارت اینترنت و .... در پرداخت های آنلاین همیشه وقتی می خواهید مرحله پرداخت وجه را از طریق کارت انجام دهید وارد سایت دومی خواهید شد که سایت بانک دریافت کننده وجه است که عموما سایت های بانک سامان به آدرس sb14.com و یا سایت بانک پارسیان به آدرس pec.ir و یا سایت معتبر دیگر بانک ها

می باشد. دقت کنید بسیاری از سارقان اینترنتی با راه اندازی سایت هایی شبیه به سایت های بانکها و آدرس های شبیه به آنها اقدام به کلاهبرداری نموده اند. اگر از مرورگر IE اسفتاده می کنید، بعد از ورود به صفحه پرداخت بانک، تصویر یک قفل زرد رنگ پایین صفحه مشاهده می شود روی آن قفل دو بار کلیک کنید تا گواهینامه سایت باز شود. در قسمت Issuedto آدرس بانک نوشته شده است . مثلا اگر وارد سایت بانک پارسیان شده باشید باید www.pec.ir نوشته شده باشد. ولی اگر وارد قسمت پرداخت شدید و این قفل زرد رنگ را مشاهده نکردید، یا نام داده شده در قسمت Issuedto درست نبود، شماره کارت رمز خود را وارد نکنید چون نشان دهنده ی این است که این سایت از نظر امنیتی تایید نشده است و یا اصلا سایت بانک نمی باشد و اطلاعات شما در اختیار افراد دیگری قرارخواهد گرفت.

شیوه خرید از طریق واریز به حساب

در این روش برای خرید اینترنتی یک کالا باید ساعت ها در صف بانک بایستید تا مبلغ را به حساب فروشگاه واریز کرده سپس شماره فیش را در وب سایت وارد کنید تا محصول مورد نظر را برای شما ارسال کنند. این شیوه یکی از بدترین شیوه های خرید اینترنتی است و حتی شاید نتوان آن را یک خرید اینترنتی قلمداد کرد. زیرا استفاده از تجارت الکترونیک باید باعث سرعت وسهولت در خرید گردد، اما در این روش شما دردسر بیشتری نسبت به خرید فیزیکی خواهید داشت. از نظر امنیتی هم استفاده از این روش خرید غیر عاقلانه است. در پرداخت های الکترونیکی تمام سوابق تراکنش های مالی شما در سیستم ثبت می شود و حتی مشخص است که این کالا در چه تاریخی و از چه فروشگاهی و با چه قیمتی خریداری شده است. اما در حالتی که شما به حساب فردی مبلغی واریزمی کنید ممکن است هیچ وقت چیزی به دست شما نرسد و چون شما مبلغ را در بانک واریز کرده اید و این فروشگاه اینترنتی برای بانک شناخته شده نیست و فروشگاه ضمانتی هم به بانک نداده است. اثبات این که شما مبلغی را بابت خرید محصول خاصی که در اینترنت وجود داشته پرداخت کرده این مشکل تر است و ردیابی آن سخت تر و یا اگر بر فرض فیش بانکی را گم کنید که اوضاع وخیم تر خواهد شد. بسیاری از سارقان از این روش نیز برای کلاهبرداری های اینترنتی خود استفاده می کنند و با راه اندازی یک سایت و رائه یک محصول با قیمت وسوسه انگیز و ارائه شماره حساب از مشتریان می خواهند مبالغ را واریز کنند. معمولا این افراد درخواست مبالغ اندکی از مشتریان می کنند، به طور مثال ۳ تا ۵ هزار تومان. به همین خاطر بیشتر افراد وقتی چیزی به دستشان نمی رسد در پی شکایت نمی روند، اما در نظر بگیرید این افراد از هزاران نفر به این شیوه کلاهبرداری می کنند و مبالغ کلانی به جیب می زنند.

خرید پستی

شاید بتوان امن ترین روش برای خرید اینترنتی استفاده از سیستم خرید پستی باشد که امروزه اغلب فروشگاه ها نیز از این سرویس استفاده می کنند. شما با استفاده از این روش می توانید محصول مورد نظر را سفارش دهید و محصول موردنظر توسط شرکت پست برای شما ارسال شده و سپس مبلغ کالا را به مامور پست تحویل می دهید. می بینید که در این روش شما با اطمینان خاطر و بدون اینکه پولی را از پیش پرداخت کرده باشید می توانید محصول خود را خریداری کنید. استفاده از این روش برای کالاهایی که ماهیت فیزیکی دارند بسیار مناسب است. همیشه سعی کنید در فروشگاهی که امکان خرید پستی وجود دارد از این روش استفاده کنید البته از این شیوه در محصولاتی که ماهیت فیزیکی ندارند مانند کارت اینترنتی و اطلاعات و حق عضویت و .... نمی توان استفاده کرد و باید شیوه پرداخت آنلاین استفاده شود.

خرید و فروش آنلاین

با یک کلیک وارد فروشگاه می‌شوید، با حرکت موس گشتی در فروشگاه می‌زنید و اجناس را برانداز می‌کنید و با کلیک دیگری مشخصات کالای مورد نظرتان را مشاهده می‌کنید. برای پرداخت پول از کارت اعتباری الکترونیکی‌تان استفاده می‌کنید و در مدت زمان مشخصی که در سایت به اطلاعتان رسیده است کالا یا خدمت مورد نظرتان را در منزل دریافت می‌کنید .فکرش را بکنید؛ به همین راحتی همان طور که پشت رایانه نشسته‌اید، می‌توانید خرید کنید.

برای خرید در دنیای مجازی علاوه بر اینکه لازم است شرکت یا فروشگاه موردنظر مجهز به سیستم خرید الکترونیکی باشد ، مصرف کنندگان و خریداران هم لازم است به رایانه دسترسی و امکان اتصال به شبکه اینترنت را داشته باشند. شمار کاربران اینترنت در کشور روز به روز در حال افزایش است و پیش بینی می‌شود به شمار این افراد هر ساله اضافه گردد.

این تعداد کاربر می‌تواند دلگرمی‌خوبی برای فروشندگانی باشد که چند سالی است پایه‌گذار تجارت الکترونیک در ایران شده‌اند. تجارت الکترونیک و فروشگاه‌های اینترنتی در کشور ما هرچند هنوز کوچه پس کوچه‌های منتهی به یک بزرگراه پهن را می‌پیماید اما با توسعه بانکداری الکترونیک و کارت‌های خرید اینترنتی، بهبود بازار کامپیوتر و تجهیزات فناوری اطلاعات، می‌تواند حرکت سریع‌تر و بهتری داشته باشد.

مزایای خرید اینترنتی

آنهایی که فرصت چندانی برای خریدهای حضوری ندارند یا به دلیل کهولت سن، بیماری یا معلولیت خرید کردن برایشان دشوار است از خریدهای اینترنتی استقبال می‌کنند. برای چنین افرادی نشستن پای یک کامپیوتر و سفارش دادن کالای مورد نیاز و تحویل گرفتن آن در منزل یک امتیاز محسوب می‌شود. کاهش ترافیک و آلودگی هوا، ایجاد اشتغال، راحتی بیشتر و کاهش استرس ناشی از تردد در خیابان‌های شلوغ، امنیت خرید و جلوگیری از سرقت یا گم شدن پول، مدیریت زمان و صرفه جویی در وقت و نیز صرفه جویی در هزینه‌های رفت و آمد از مزایای خرید در دنیای مجازی است .

به طور مثال یک دانش آموز ممکن است برای خرید یک کتاب کمک درسی ساعت‌ها وقت صرف کند، در حالی که با صرف زمان کوتاهی می‌تواند در حالی که به خواندن درس‌هایش مشغول است منتظر رسیدن سفارشش باشد .

برای مسافری که بلیت اتوبوس، قطار یا هواپیما را از طریق اینترنت خریداری می‌کند، هتل محل اقامتش را از این طریق رزرو می‌کند این شیوه بسیار مناسب است. همچنین برای محققی که روی یک موضوع در حال تحقیق است و می‌تواند به راحتی نیازهای اطلاعاتی اش را از آن سوی دنیا و از طریق اینترنت خریداری کند، فایل‌های مربوط به مقاله‌ها یا کتاب‌های مورد نیاز خود را از فروشگاه‌های الکترونیکی دانلود کند یا یک موسسه تبلیغاتی که مناسب‌ترین عکس‌های مرتبط با موضوع خود را از این طریق به دست می‌آورد، هیچ چیزی به اندازه توسعه تجارت الکترونیک مفید نیست.

برخی از خدمات الکترونیک مانند پرداخت‌های آنلاین مانند قبوض آب، برق، تلفن و ثبت نام اینترنتی دانشگاه‌ها که موجب کاهش زمان تلف شده ناشی از ایستادن در صف‌های طولانی در بانک و باجه‌های پست می‌شود، تمایل مردم را نسبت به استفاده از این خدمات بیشتر کرده است که با توسعه کارت‌های پرداخت اینترنتی به وسیله سیستم بانکداری و نیز توسعه تجهیزات فناوری اطلاعات و نرم افزارهای مربوط به طراحی سایت و به خصوص امنیت شبکه‌های مجازی، این امر با استقبال بیشتری مواجه خواهد شد .

کمبود کارت‌های اعتباری، ضعف تجهیزات و امکانات در زمینه فناوری اطلاعات، عدم آموزش و آشنایی کافی مردم با این روش از موانع خرید اینترنتی است.

مراقب باشید

هم‌زمان با توسعه تکنولوژی و فن‌آوری، شگردهای کلاه‌برداری هم پیشرفت کرده است. امروزه فروشگاه‌های اینترنتی گوناگونی به تبلیغ نوعی کالا می‌پردازند و از افراد می‌خواهند مبلغ کالا را به یک شماره حساب واریز کنند و منتظر دریافت کالا باشند در حالی که هیچ کالایی وجود ندارد یا کالا آن چیزی نیست که در فروشگاه اینترنتی تبلیغ شده است.

گاهی نیز برخی فروشگاه‌های اینترنتی، سایت خود را با نام‌هایی شبیه فروشگاه‌هایی معتبر تاسیس می‌کنند و حتی شکل ظاهری سایت را نیز مشابه سایت فروش همان فروشگاه طراحی می‌کنند تا مراجعه کنندگان را فریب دهند. این کار بیشتر در مورد بانک‌ها و سازمان‌هایی که خدمات مالی ارایه می‌دهند مشاهده می‌شود.

برای جلوگیری از چنین سوء استفاده‌هایی توصیه می‌شود آدرس سایت هر فروشگاه، بانک و سازمانی را مستقیم از خود آن بانک یا سازمان دریافت کنید و به آدرس‌های اینترنتی که از طریق موتورهای جستجوگر معرفی یا ایمیل‌هایی که برای شما ارسال می‌شود، اعتماد نکنید.

کلمات و رمزهای عبور هنگام ورود به سبد خرید یا پرداخت وجه مهم است و باید نسبت به مخفی نگه داشتن آنها حساس بود. همچنین استفاده از کامپیوترهای همگانی مثل کافی‌نت‌ها برای خریدهای اینترنتی توصیه نمی‌شود.

نکته‌های خرید اینترنتی:

•هرچند مزایای خرید اینترنتی بر کسی پوشیده نیست اما هنوز عده کمی‌از مردم حاضر به انجام چنین خریدهایی هستند. به جز عدم اعتماد نسبی که برخی از مردم به فروشگاه‌های اینترنتی دارند، شاید ریشه اصلی استقبال کم در این خصوص، لذتی است که انسان از خرید کردن حضوری و تماشای اجناس می‌برد. بسیاری از مردم، از تماشای ویترین‌های رنگارنگ فروشگاه‌ها، اجناس و لوازم خانگی و صوتی تصویری، فروشگاه‌های پرزرق و برق لباس و کفش لذت می‌برند .

•از همه مهم‌تر اینکه مقایسه یک کالا در فروشگاه‌ها و دخالت احساسات و سلیقه‌ها در مدل، رنگ و اندازه که در فروشگاه‌های الکترونیکی این امکان کمتر وجود دارد موجب می‌شود افراد رنج رفتن به مراکز خرید و قدم زدن‌های طولانی را بر نشستن پای رایانه ترجیح دهند. همچنین خریدهای حضوری برای خیلی‌ها نوعی تفریح به حساب می‌آید .

•نکته دیگر اینکه در دنیای امروز که به دلیل مشاغل نشسته ، مصرف غذاهای آماده و کم تحرکی ، چاقی اپیدمی شده است و این موضوع سلامت افراد را به مخاطره انداخته است. شاید همین قدم زدن در فروشگاه و فعالیت بدنی اندکی که هنگام خرید انجام می‌شود برای حفظ سلامت آدم‌های کم‌تحرک این روزگار غنیمت باشد.

مقایسه کالاها قبل از خرید در اینترنت

اگر قصد خرید در اینترنت را دارید قبل از خرید کمی تحقیق کنید؛ حتی اگر بدانید که قصد خرید چه نوع کالایی را دارید، انتخاب کالا بین هزاران محصول، برند و وب‌سایت کار ساده‌ای نخواهد بود. از نکات زیر استفاده کنید تا بتوانید بهترین کالا را انتخاب کنید و در دام پیشنهادهای ساختگی افراد کلاهبردار قرار نگیرید.

قبل از خرید کمی فکر کنید

قبل از خرید کمی در مورد هدف خود فکر کنید. آیا به دنبال کالای خاصی هستید؟ می‌خواهید از برند خاصی خرید کنید؟ کالای مد نظر شما باید چه ویژگی‌های مهمی داشته باشد؟ بودجه خرید شما چقدر است؟ توجه کنید، اگر شما بر مبنای آن چیزی که برایتان مهم است، تصمیم به خرید بگیرید، احتمال آن‌که به‌صورت ناگهانی خرید کنید و از خرید خود پشیمان شوید، کم خواهد بود.

در مورد کالاهایی که در یک رده قرار می‌گیرند، اطلاعات لازم را کسب کنید.

در اغلب موارد ویژگی‌های اصلی یک کالای ساده با برترین کالای تولید شده توسط همان تولید کننده مشترک است و به دلیل ویژگی‌های جدید و برخی خصوصیات خاص، قیمت کالاهای جدید بالاتر است. برای مثال، ممکن است، شما مبلغ بیشتری برای خرید یک توستر که ساعت دارد، بپردازید. در حالی که مدل ارزان‌تر این دستگاه فقط نان را تبدیل به تُست می‌کند. در اغلب موارد سازندگان در سایت‌هایشان بیشترین اطلاعات در مورد ویژگی‌های محصولاتشان را در اختیار بازدیدکنندگان قرار می‌دهند.

از موتورهای جستجو استفاده کنید

اگر فکر می‌کنید که شرایط خرید اینترنتی خوب و منصفانه است، اما با کالا و شرکت تولید کننده آن آشنا نیستید، کمی بیشتر تحقیق کنید. در موتور جستجوی مورد علاقه خود نام شرکت یا کالا را همراه با کلماتی چون «بررسی»، «شکایت» و «کلاهبرداری» تایپ کنید. اگر اخبار بدی دریافت کردید، شما باید تصمیم بگیرید که آیا پذیرفتن شرایط معامله ارزش پذیرفتن ریسک و خطرهای ناشی از آن را دارد یا نه. در نهایت، اگر شما یک کالای خوب دریافت کردید، این معامله یک معامله خوب و منصفانه است.

سایت‌هایی که کالاها را مقایسه می‌کنند، بررسی کنید.

این سایت‌ها امکان برقراری ارتباط شما با بسیاری از خرده‌فروشان که همان کالا را می‌فروشند، برقرار می‌کنند. در برخی از موارد، اختلاف قیمت‌ها فاحش و چشمگیر است. در هنگام مقایسه به جای آن‌که فقط به قیمت فروش توجه کنید، قیمت کلی خرید را که شامل هزینه‌های ارسال، راه اندازی و مالیات است، مقایسه کنید. سایت‌های مختلف سیاست‌های مختلفی برای بازگرداندن کالا دارند. این سیاست‌ها را بررسی کنید تا بدانید که آیا شما باید هزینه‌های ارسال و نگهداری را پرداخت کنید. برخی از سایت‌ها امکاناتی را در اختیار دارند که در صورت ثبت‌نام در زمانی که قیمت‌ها افزایش پیدا کند، اطلاعات لازم را در اختیار کاربران قرار می‌دهند.

برگه‌های تخفیف را در نظر بگیرید

برخی از شرکت‌ها برای کسانی که از طریق اینترنت خرید می‌کنند، برگه‌های تخفیف را از طریق ایمیل ارسال می‌کنند. سایر سایت‌ها نیز مجموعه قوانینی برای هزینه‌های ارسال و سایر تخفیفات دارند. به خاطر داشته باشید که صرف وجود تخفیف در قیمت، همیشه به معنی خرید مناسب نیست.

اگر می‌خواهید وضعیت تخفیف‌ها در یک شرکت را بررسی کنید، همراه با اسم وب‌سایت یا شرکت کلماتی چون «تخفیف»، «اوراق تخفیف» یا «ارسال رایگان» را در یک موتور جستجو تایپ کنید. اگر سایتی از شما خواست که نرم افزاری را دانلود کنید یا اطلاعات مالی خود را وارد کنید تا به دستورالعمل‌های مربوط به انواع تخفیفات دسترسی داشته باشید، به هیچ وجه اطلاعات خود را وارد نکنید و از آن سایت خریدی انجام ندهید.

نظرهای کاربران را بخوانید؛ ولی زیاد به آن‌ها اعتماد نکنید

وقتی که بخش نظرها را مطالعه می‌کنید، دربارهٔ منبع اطلاعات فکر کنید. آیا منبع این اطلاعات یک سازمان حرفه‌ای و بی‌طرف، یک مشتری، چند مشتری خاص یا یک مقاله‌نویس است؟ همیشه این امکان را بدهید که شاید نظرها ساختگی و از جانب خود فروشنده باشد.

با خواندن نظراتی که کاربران در سایت‌های خرید یا سایت‌های مقایسه کالا می‌نویسند، شما می‌توانید تصویر مناسبی از کیفیت کارایی یک محصول به دست آورید؛ اما ممکن است، این نظرها منعکس کننده تجربه واقعی تمام خریداران نباشد. شما همچنین می‌توانید به سایت‌هایی مراجعه کنید که به‌صورت تخصصی به بررسی کالاها می‌پردازند. در این سایت‌ها کالاها به فروش نمی‌رسند؛ اما شما می‌توانید نظرهای افراد حرفه‌ای و مقایسه کالاها به صورت حرفه‌ای را در این سایت‌ها پیدا کنید.

هر چیزی را که در سایت‌های خرده فروشی می‌بینید، بررسی کنید

برخی از کلاهبردارها سایت‌هایی را راه‌اندازی می‌کنند که به‌صورت خاص اقدام به فروش نوع خاصی از کالاها می‌کنند. این گونه سایت‌ها مملو از نظرهای مثبت و اغراق آمیز افرادی است که خود را مانند افراد عادی نشان می‌دهند. آن‌ها برای نوشتن این گونه نظرها پاداش دریافت می‌کنند. در این گونه سایت‌ها نمی‌توانید نظرهای متوسط و منفی پیدا کنید؛ چون مسئولین سایت این گونه نظرها را حذف کرده‌اند.

شما در مورد عکس چه چیزی می‌دانید؟

عکس کالا روشی برای ایجاد بهترین تصویر از کالا است؛ اما امکان دست‌کاری در آن وجود دارد و ممکن است، کالایی را که درب منزل دریافت می‌کنید با مشخصات ارائه شده و عکس آن به هیچ وجه مطابقت نداشته باشد.

از خودتان چند سوال بپرسید

- شرکت تولید کننده از نظر ارائه کالای با کیفیت و خدمات پس از فروش اعتبار و شهرت دارد؟

• زمان تعیین شده برای تحول کالا چه زمانی است؟

• اگر مشکلی پیش بیاید، چگونه می‌توانید با فروشنده در تماس باشید؟

• آیا شرکت کالای معیوب را خواهد پذیرفت؟

اگر جواب‌هایتان به این سوال‌ها معقول است، می‌توانید با اطمینان خاطر بیشتری اقدام به خرید کنید.

۷ نکته برای یک خرید امن آنلاین

اگر قصد دارید امنیت را تا آن‌جا که ممکن است در فرآیند خرید برقرار کنید، با ما همراه باشید تا هفت نکته‌ی مفید و کاربردی این حوزه را فرا بگیرید.

۱.استفاده از آخرین نسخه‌ی مرورگر

شرکت‌های ارائه‌دهنده‌ی مرورگرهای اینترنتی با انتشار نسخه‌ی جدیدی از محصول خود، قابلیت‌های امنیتی بیشتری به آن اضافه می‌کنند تا فضایی امن‌تر نسبت به نسخه‌های قبلی برای کاربر به وجود آید. این که شما از کدام مرورگر اینترنتی استفاده می‌کنید خیلی مهم نیست، مهم این است که از آخرین نسخه‌ی آن مرورگر استفاده کنید. البته در بین مرورگرهای مختلف می‌توان گفت Mozilla Firefox و Goole Chromeبالاترین میزان امنیت برای کاربران را فراهم می‌کنند.

۲. خرید از سایت‌های شناخته‌شده

سایت‌های بسیاری وجود دارند که می‌توان از آن‌ها برای تلفن همراه خود شارژ خریداری کنید اما تنها تعداد محدودی از آن‌ها توسط اپراتورهای تلفن همراه تایید شده‌اند. همین مورد در حوزه‌های مختلف نیز وجود دارد، پس بهتر است که به آن توجه کرد.

۳.اطلاع از وضعیت امنیت سایت

یکی از پروتکل‌هایی که از آن جهت تبادل اطلاعات به صورت رمزنگاری شده استفاده می‌شود HTTPS نام دارد. فروشگاه‌های اینترنتی با استفاده از این پروتکل، فرآیند خرید را در فضایی امن پیاده‌سازی می‌کنند. پس اگر برای خرید آنلاین خود به سایتی مراجعه کردید و در نشانی آن خبری از این پروتکل نبود بلافاصله از خرید خود منصرف شوید. معمولا تمام بانک‌های کشور در صفحه‌ی پرداخت خود نکاتی را جهت بررسی این وضعیت به کاربر گوشزد کرده‌اند.

۴. استفاده از کارت‌های اعتباری

در کشور ما اکثر بانک‌ها کارت‌های خرید نقدی (debit) ارائه می‌دهند و تعداد محدودی نیز کارت‌های خرید اعتباری .(credit) تفاوت این دو کارت در نحوه‌ی پرداخت است، به این معنی که در کارت‌های نقدی تا زمانی که پول در حساب نباشد امکان خرید وجود ندارد اما در مورد کارت‌های اعتباری این مورد صادق نیست. پس اگر کارت اعتباری و نقدی دارید توصیه می‌شود از کارت اعتباری جهت خرید آنلاین استفاده کنید.

۵.حفاظت از اطلاعات شخصی

اطلاعاتی از جمله رمزدوم کارت، CVV2و تاریخ انقضا را نباید در هیچ سایتی ذخیره کنید. حتی اگر در حال وارد کردن این اطلاعات در سایت بانک خود هستید و مرورگر از شما درخواست می‌کند که این اطلاعات را در حافظه‌ی خود ذخیره سازد، بهتر این است که شما این کار را نکنید چرا که طی مرور زمان نگهداری این اطلاعات در مرورگر دردسرساز خواهد شد.

۶. گذرواژه امن

هنوز از ۱۲۳۴ یا کلمه‌ی password استفاده می‌کنید؟ درست است که به یاد داشتن چنین ترکیب‌های ساده‌ای برای کاربر ساده است اما به یاد داشته باشید که حدس زدن این موارد برای هکر یا فرد ناشناسی که قصد دارد اطلاعات شما را به سرقت ببرد، بسیار آسان است. پس بهتر است از گذرواژه‌های ترکیبی با طول حداقل ۶ که از حروف کوچک، بزرگ، نمادها و اعداد تشکیل شده‌اند استفاده کنید.

۷. بررسی حساب بانکی

بهتر است پس از انجام خرید آنلاین حساب بانکی خود را بررسی کنید تا از میزان مبلغ پرداختی اطمینان حاصل شود. این مورد آخر نسبت به قبلی‌ها خیلی به امنیت ربط ندارد اما رعایت کردن آن باعث می‌شود که کاربر از تکمیل فرآیند خرید اطمینان پیدا کند.

۹نکته عمومی درمورد خرید اینترنتی

نکات ارائه شده در قسمت ذیل می تواند به اشخاص در زمان خرید اینترنتی کمک کند تا به راحتی و با امنیت بیشتر اقدام به خرید اینترنتی نمایند.

۱. شخصی که با او معامله می کنید، را بشناسید.

● قبل از این که خریدی انجام دهید، آدرس و شماره تلفن واقعی فروشنده اینترنتی را بررسی کنید و نسبت به صحت آن اطمینان حاصل نمایید. به این منظور که اگر بعداً برای شما سوالی پیش بیاید و یا به مشکلی برخورد کنید، این آدرس و شماره تلفن در دست شما است و می توانید به آنها مراجعه کنید.

۲. کالائی را که در حال خرید آن هستید، بشناسید.

●یک نسخه نهایی از شرایط و ویژگی های محصول را که فروشنده تهیه کرده است، را به دقت مطالعه کنید حتی اگر این کار برای شما خسته کننده و ملال آور باشد.

●شرایط و ویژگی ها را به دقت بررسی کنید. اگر شما از محصول راضی نیستید، آیا می توانید آن را برگردانده و پول خود را دریافت کنید؟ هر نوع اطلاعات ثبت شده که مربوط به این معامله است و شامل تمامی نامه های الکترونیک ارسالی به فروشنده و دریافتی از فروشنده است، را ذخیره کرده و از آنها پرینت بگیرید .

●کارت های هدیه را از مراکزی که می شناسید و به آنها اعتماد دارید، تهیه کنید. از خرید کارت از سایت هایی که مانند یک حراجی کار می کنند، خودداری کنید. زیرا این کارت ها می توانند تقلبی باشند .

۳.در حفاظت از اطلاعات شخصی خود حساس باشید.

●اطلاعات کارت اعتباری خود یا سایر اطلاعات مالی خود را در ازای خرید و دریافت جدیدترین اسباب بازی، کارت هدیه رایگان، یک شغل فصلی و یا اجاره (یک محل) برای تعطیلات در اختیار شخصی که نمی شناسید، قرار ندهید .

●اطلاعات مالی خود را از طریق نامه الکترونیک ارسال نکنید. نامه الکترونیک روشی مطمئن برای انتقال شماره کارت اعتباری، شماره حساب بانکی و یا شماره تامین اجتماعی نیست .

●بر روی لینک موجود در نامه الکترونیک کلیک نکنید. شرکت هایی که فعالیت آنها مشروع و قانونی است، اطلاعات مالی شما را از طریق نامه الکترونیک یا پیام های پاپ آپ درخواست نمی کنند.

۴. سیاست حفظ اسرار را به دقت مطالعه و بررسی کنید .

●سیاست حفظ اسرار ممکن است طولانی باشد و خواندن آن زمان بر باشد، اما می تواند اطلاعات مهمی را در اختیار شما قرار دهد. برای مثال وب سایت چه نوع اطلاعات شخصی را جمع آوری می کند، صاحبان و اپراتورهای سایت چگونه قصد دارند از این اطلاعات استفاده کنند. اگر نمی توانید سیاست حفظ اسرار سایت را پیدا کنید و یا آن را درک نمی کنید و مفاد آن را متوجه نمی شوید، به فکر انجام معاملات تجاری خود در جای دیگری باشید و بگذارید که سایت (صاحبان سایت) بداند شما چه فکر و نظری دارید .

۵.حواشی خرید

●با دانستن نام سازنده یک کالا و شماره مدل، شما می توانید ویژگی های این کالا را به صورت جز به جز با سایر کالاهای مشابه مقایسه کنید. بعضی از خرده فروشان کالا را به قیمتی که سایر رقبا عرضه می کنند، وارد بازار می کنند و یا حتی قیمت آن را پایین تر هم می آورند. بسیاری از بازرگان ها، نه همه آنها، امسال هزینه ای بابت خرید کالا پرداخت نمی کنند. پس بنابر این هزینه ارسال کالا را نیز در مجموع هزینه ها در نظر بگیرید. اگر شما در اینترنت سفارش خرید می دهید و محل فروشگاه را انتخاب می کنید، هزینه پارکینگ و حمل و نقل عمومی را نیز در نظر بگیرید.

۶.آیا باید خرید خود را از طریق شبکه WiFi عمومی (شبکه ای که رمز ندارد) انجام دهید؟

●فکر نکنید که نقاط دسترسی WiFi عمومی امن هستند. تا زمانی که مطمئن نشوید که یک نقطه دسترسی ابزارهای امنیتی موثر و کافی دارد، ممکن است نخواهید اطلاعات حساس خود مانند شماره کارت اعتباری تان را از طریق آن شبکه ارسال کنید .

۷. مبالغ را از طریق کارت اعتباری یا کارت هزینه پرداخت کنید.

این ابزارها از بهترین و اثر گذارترین روش ها برای محافظت و حمایت از استفاده کننده می باشد.

●ارسال پول از طریق سیستم مخابراتی می تواند ریسک داشته باشد. همانند ارسال وجه نقد، اگر یک بار ارسال شود، دیگر ارسال شده است. شما نمی توانید آن را برگردانید.

●خرید در اینترنت و استفاده از ابزارهای شبه نقد مانند چک شخصی و.... می تواند ریسک داشته باشد. تنها زمانی از این ابزارها استفاده کنید که شخصی که با او معامله می کنید، را می شناسید .

۸.محصولات رایگان می توانند هزینه زا باشند.

● محافظ صفحه، کارت های الکترونیک و سایر دانلودها در فضای اینترنت می توانند، حامل ویروس های خطرناک باشند. نرم افزارهای ضد ویروس و ضد جاسوسی خود را همراه با نرم افزار دیواره آتش همواره به روز و فعال نگه دارید .

۹. حساب های مالی خود را به دقت بررسی کنید.

●به صورت روزانه و مستمر حساب های خود را بررسی کنید تا مطمئن شوید تمامی برداشت های پول از حساب مطابق نظر خودتان صورت گرفته است.

۹ نکته مهم امنیتی در خریدهای آنلاین

ترس از نبود امنیت مهم‌ترین دلیل مردم در عدم اقبال به خریدهای آنلاین است. در حالی که تامین امنیت در خریدهای آنلاین به اندازه رعایت چند نکته معمولی ساده است. در ادامه ۹ نکته امنیتی که باید در خریدهای آنلاین رعایت کنید بیان می‌شود.

مرورگرهای خود را به روزرسانی کنید

شرکت‌های ارائه‌دهنده‌ی مرورگرهای اینترنتی با انتشار نسخه‌ی جدیدی از محصول خود، قابلیت‌های امنیتی بیشتری به آن اضافه می‌کنند تا فضایی امن‌تر نسبت به نسخه‌های قبلی برای کاربر به وجود آید. این که شما از کدام مرورگر اینترنتی استفاده می‌کنید خیلی مهم نیست، مهم این است که از آخرین نسخه‌ی آن مرورگر استفاده کنید. البته در بین مرورگرهای مختلف می‌توان گفت Mozilla Firefox و Google Chrome بالاترین میزان امنیت برای کاربران را فراهم می‌کنند.

خرید از سایت‌های شناخته‌شده

به تجربه سایت‌ها در ارائه سرویس توجه کنید. معمولا یک محصول را می‌توان از سایت‌های مختلف خریداری کرد و یا از افرادی که قبلا از سایت خرید کرده‌اند، پرس‌وجو کنید.

اطلاع از وضعیت امنیت سایت‌ها

خرید را از سایت‌هایی که مجهز به درگاه HTTPS هستند، انجام دهید. این پروتکل اطلاعات را به صورت امن رمز نگاری و تبادل می‌کند. یکی از پروتکل‌هایی که از آن جهت تبادل اطلاعات به صورت رمزنگاری شده استفاده می‌شود HTTPS نام دارد. در حال حاضر سایت تمام بانک‌های کشور از این درگاه برای مبادلات مشتریان استفاده می.کنندفروشگاه‌های اینترنتی با استفاده از این پروتکل، فرآیند خرید را در فضایی امن پیاده‌سازی می‌کنند.

استفاده از کارت‌های اعتباری

در کشور ما اکثر بانک‌ها کارت‌های خرید نقدی (debit) ارائه می‌دهند و تعداد محدودی نیز کارت‌های خرید اعتباری (Credit) تفاوت این دو کارت در نحوه‌ی پرداخت است، به این معنی که در کارت‌های نقدی تا زمانی که پول در حساب نباشد امکان خرید وجود ندارد اما در مورد کارت‌های اعتباری این مورد صادق نیست. پس اگر کارت اعتباری و نقدی دارید توصیه می‌شود از کارت اعتباری جهت خرید آنلاین استفاده کنید.

حفاظت از اطلاعات شخصی

اطلاعاتی از جمله رمزدوم کارت، CVV2 و تاریخ انقضا را نباید در هیچ سایتی ذخیره کنید. حتی اگر در حال وارد کردن این اطلاعات در سایت بانک خود هستید.

انتخاب گذر واژه امن

گذر واژه امن هنوز برای خیلی‌ها مفهوم روشنی ندارد. با چند نکته ساده می‌توان رمز خود را امن کنید از جمله:

از ایجاد رشته‌های پشت‌سرهم در رمز مانند ۱۲۳، qwer، abcdeو غیره پرهیز کنید.

در رمز خود حتما از کاراکترهایی مانند! ، @، #، %، ^، &، *استفاده کنید.

می‌توان رمز خود را براساس کاراکترهای اول یک جمله که در ذهنتان است انتخاب کنید.

به بزرگ و کوچک بودن حروف استفاده شده حتما دقت کنید. این روش در امن کردن رمز شما بسیارکمک خواهد کرد.

تعداد کاراکترهای رمز باید بالای ۶ باشد.

توصیه می‌شود که هر شش ماه یکبار رمز خود را تغییر دهید.

از ترکیب‌های روتین که اطرافیانتان نیز از آنها با خبرند پرهیز کنید.

اگر هم ایده‌ی خوبی برای ساختن رمز ندارید می‌توانید از سایت‌های زیر کمک بگیرید. البته پیشنهاد می‌کنیم بازهم رمز گرفته شده از این سابت‌ها را تغییر دهید:

بررسی حساب بانکی

منطقی‌تر است پس از انجام خرید آنلاین حساب بانکی خود را بررسی کنید تا از میزان مبلغ پرداختی اطمینان حاصل نمایید. (تصور نکنید چون مبلغ قابل توجهی وجه در حساب بانکی تان ندارید هدف مناسبی برای سارقان اینترنتی نیستید چرا که تمام کاربران اینترنت به یک میزان در معرض خطر تهاجم هکر ها هستند پس در هر شرایطی امنیت را جدی بگیرید.)

از کامپیوتر شخصی خرید کنید

حتی‌الامکان در محیط‌های عمومی مانند کافی نت نه وارد اینترنت بانک خود شوید ، نه وارد حسابهای کاربری و نه خرید اینترنتی انجام دهید ،

نکاتی برای حفظ امنیت اطلاعات در کافی نت ها

سرویس های عمومی همواره با آسیب پذیری بیشتری نسبت به سیستم های شخصی مواجه هستند. همین وضع برای کافی نت ها که ارائه دهنده خدمات اینترنتی هستند نیز برقرار است. به طور کلی یک سیستم شخصی چون با تعداد موارد تهدیدزای کمتری مواجه است از امنیت بهتری برخوردار است. ولی در شرایطی ممکن است به هر دلیلی ناچار شویم ازرایانه هایی که متعلق به خودمان نیست مثلا رایانه های موجود در کافی نت ها چنین استفاده کنیم. در ادامه نکاتی در مورد حفاظت از داده های خود در این شرایط را توضیح می دهیم.

ابتدا سیستم را ریست کنید

همان طور که می دانید افراد زیادی در طول یک روز ازیک کافی نت استفاده می کنند و اغلب آنها دارای حافظه های قابل حملی هستند که می توانند در صورت آلوده بودن آن، سیستم ها و حافظه های قابل حمل دیگر را نیز آلوده کنند. راه حلی که معمولا در کافینت ها استفاده می شود نصب نرم افزاری از قبیل DeepFreez است که پس از ریست شدن سیستم آن را به حالت اول برگردانیده و درنتیجه ویروس ها یا تغیرات انجام گرفته را خنثی خواهد نمود. اگر شما اولین نفری باشد که از چنین سیستمی استفاده می کنید نگرانی وجود ندارد. ولی اغلب موارد این طور نیست و ممکن است با سیستم از قبل آماده واحتمالا ویروسی مواجه شوید. وضعیتی که اکنون می تواند وجود داشته باشد این است که اکنون رایانه ی در مقابل شما به نوعی ویروس، تروجان یا جاسوس افزارآلوده شده باشد. با این توضیحات راه حلی که به نظر می رسد این است که کلا قبل از اتصال حافظه فلش یا ورود به وبسایت هایی که مجبور به وارد کردن نام کاربری خودهستید سیستم را یک بار ریست کنید.همچنین بعد از استفاده نیزتوصیه می شود این را برای حذف ردپای خود تکرار کنید. زیرا ممکن است در صورت ورود به ایمیل یا حساب کاربری خود در هر وب سایت دیگری اولا کوکی های شما در مرورگر سیستم ذخیره شوند وثانیا ممکن است جاسوس افزارها کلماتی که در حین وارد کردن نام کاربری و پسورد خود بوده اید را ضبط کرده باشند.

تاریخ وساعت آخرین ورود را چک کنید

معمولا وب سایتها پس از لوگین شدن درآنها، تاریخ و آخرین ساعت ورود به حساب کاربری را نمایش می دهند. در حین لوگین نمودن با خواندن این تاریخ و ساعت، آن را با آخرین ورود خود به سیستم که در ذهن شماست مقایسه کنید. در صورتی که با هم منطبق نبودند می توان گفت در این فاصله شخص دیگری به حساب شما دسترسی داشته است. در این موارد باید هرچه سریع تر پسورد و سوالاتی را که در حین ثبت نام به آنها پاسخ داده اید را عوض نمایید.

به خاطرسپاریها و کوکی ها را رد کنید

در حین کاربا مرورگرها آنها ممکن است پیغام هایی مبتنی بر ذخیره کوکی ها و به یاد آوردن تنظیمات لوگین شما شما سوال نماید. در این حالت همیشه گزینه هایی را انتخاب کنید که این کار را متوقف می کنند. همچنین در برخی از وب سایت ها از فعال نمودن گزینه هایی از قبیل مرا به خاطر بسپار خودداری کنید.

فایل های خود را جا نگذارید

از لحاظ روان شناسی ثابت شده است که افراد معمولا پس از انجام کاری که در ذهن خود دارند و رسیدن به هدف اصلی خود جزییات مربوط به آن را فراموش می کنند. مثلا در از پریز در آوردن دستگاه پس از استفاده از آن را فراموش می کنند. پس مراقب باشد بعد از اتمام کار فایل های خود را در رایانه مورد استفاده جا نگذارید.

از حساب خود خارج شوید

بستن مرورگر برای خارج شدن از حساب کافی نیست. زیرا مرورگرها پس از لوگین شدن شما کوکی هایی را برای نگهداری حساب کاربری و تنظیمات هر سایت در سیستم ذخیره می کنند تا با باز کردن مرورگر بدون وارد کردن مجدد شناسه کاربری به حساب خود دسترسی داشته باشید. همیشه گزینه هایی مثل خروج از حساب یا Log Out را بدین منظور بزنید. در پایان در تنظیمات مرورگر رفته و کوکی های خود را پاک کنید.

ابتدا حافظه فلش را اسکن کنید

اطلاعات شخصی و مهم را در حافظه فلش ذخیره نکنید. اگر متوجه شدید که داده های موجود در حافظه فلش شما پاک شده است، ممکن است واقعا این طور نباشد. به طور خلاصه ویروس ها معمولا فایل ها را به صورت مخفی در می آورند و به جای آن یک میانبر ایجاد می کنند تا با باز کردن آن ابتدا ویروس و سپس فایل مورد نظر اجرا شود. می توانید اولا فایل های مخفی شده را با فعال کردن نمایش آنها درکنترل پانل ویندوز نجات دهید. پیشنهاد می شود این کار قبل از استفاده از آنتی ویروس و به طور دستی انجام دهید. چون ممکن است آنتی ویروس فایل شما را هم ناچارا از بین ببرد. سپس می توانید فلش خود را اسکن یا فرمت کنید. پس از فرمت کردن وارد فلش شوید در صورتی که پس از چند لحظه، فایل های ناخواسته ای مثل میانبرها در فلش ظاهر شد، سیستم فعلی آلوده است و تنها می توان پس از حذف دستی این فایلها حافظه فلش را سریعا از سیستم جدا نمود. یک توصیه کلی دیگر غیر فعال نمودن اتوران ها در ویندوز است. دراینجا مهمترین نکته ای که پیشنهاد می شود، استفاده از نرم افزار Panada USB است که با واکسینه کردن فایل Autorun.inf کار را برای ورود و گسترش فایل های مخرب دشوار می کند، در حقیقت بسیاری از بدافزارها به منظور آلوده ساختن حافظه فلش به محض اتصال آن به کامپیوتر، فایل اجرایی مخرب را در درایو حافظه فلش کپی می کنند و فایل Autorun را نیز تغییر می دهند. نرم افزار Panda USB قابلیت اجرایی خودکار تمام برنامه های موجود در CD، USB و DVD را غیر فعال می کند، این نرم افزار را می توانید از آدرس http://www.pandasecurity.com/usa دریافت کنید، روش دیگر استفاده ازآنتی ویروس های قابل حمل است که مهمترین آن ها AntiVir، ClamWin Portable و Portable Ad-Aware هستند.

سخن آخر

همواره توصیه می شود تا جای ممکن از استفاده از کامپیوترهای عمومی و وارد کردن اطلاعات مهم و شخصی پرهیز کنید، اما اگر مجبور به استفاده شدید، روش هایی که عنوان شده اند در عین سادگی بسیار کارآمد هستند، در عین حال توجه داشته باشید که همواره تمام حساب های کاربری خود را پس اتمام کارتان Log Out خارج کنید و به گزینه های هشدار به خاطر سپردن رمز عبور نیز توجه داشته باشیدو در چنین مکان هایی هرگز آن ها را تایید نکنید و از همه مهمتر اسناد مهم خود را پس از ویرایش در این کامپیوتر ها جا نگذارید.

هشدار معاونت اجتماعی پلیس فتا ناجا در مورد استفاده از کافی نت ها : به هموطنان هشدار داده می‌شود که در هنگام استفاده از سیستم‌های کافی نت در هنگام ثبت نام و یا مواردی مشابه هیچ گاه رمز بانکی خود را در اختیار دیگران قرار ندهید و اگر احتمال لو رفتن رمز خود را می‌دهید سریعاً رمز را تغییر داده و مراتب را با پلیس فتا در میان گذارید.همچنین مدیران دفاتر خدمات اینترنتی ، موظفند شرایطی را فراهم کنند که اطلاعات کاربر پیشین (شامل سایت‌ها ، صفحات دیده شده، فعالیت‌ها، IDها ، آدرس‌های ایمیل و ...) به محض قطع استفاده کاربر، از بین رفته و برای کاربران بعدی که از آن رایانه استفاده می‌کنند قابل بازیابی نباشد و همینطور رایانه‌های استفاده شده در مراکز خدمات اینترنت (کافی‌نت) بایستی الزاماً در حالت کاربر محدود (Limited User) در اختیار کاربران قرار گرفته و درگاه‌های ورودی سیستم رایانه‌ای شامل درگاه‌هایUSB ، کارت خوان‌ها و سایر درگاه‌هایی که امکان اتصال حافظه‌های جانبی به آن‌ها وجود دارد، به صورت نرم افزاری مسدود شود.در صورت نیاز کاربر به استفاده یا ارسال فایل رایانه‌ای باید انتقال از طریق متصدی اجرایی دفتر خدمات اینترنت و از طریق شبکه داخلی دفتر روی سیستم رایانه‌ای کاربر و پس از اطمینان از آلوده نبودن فایل رایانه‌ای به بدافزارها انجام شود

اینترنت بانک چیست ؟

اینترنت بانک یکی از خدمات بانکداری الکترونیک است که این روزها تقریبا همه بانک ها و بعضی از موسسات مالی در غالب آن خدماتی را به مشتریان خود ارائه می دهند. اگرچه این خدمات نقش بسیار موثری را در تسهیل عملیات بانکی و کاهش هدر رفت زمان بر عهده دارد اما اگر نکات امنیتی به هنگام استفاده از این خدمات به درستی بکار گرفته نشود سبب خواهد شد تا شما زمینه سرقت اموالتان را با دستان خودتان فراهم آورید.

هشدار

ا گر قصد خرید اینترنتی دارید این توصیه‌ها را جدی بگیرید. اولین پیش‌فرض برای حقیقی و سالم بودن خدمات یک فروشگاه الکترونیک این است که کالاهای مجاز ارائه می‌کند. بنابراین فروشگاه‌هایی که کالاهای غیرمجاز می‌فروشند، به احتمال بسیار بالا، قصد کلاهبرداری دارند.
هنگام تصمیم به خرید، از تجربه دوستان و آشنایان خود درخصوص خریدهای آنلاین استفاده و از فروشگاه هایی که سابقه مطلوب دارند، خرید کنید.
بدانید صفحاتی که ناخواسته در برابر شما باز می شوند و حاوی تبلیغات فروش کالاها و ارائه خدمات هستند، ممکن است تقلبی باشند. هنگام خرید آنلاین و در زمانی که پس از انتخاب کالا به درگاه پرداخت الکترونیکی بانک راهنمایی می شوید، دقت کنید حتما آدرس صفحه درگاه پرداخت الکترونیکی، متعلق به همان بانکی باشد که آرم و لوگوی آن را در صفحه مشاهده می کنید.

نکاتی جهت استفاده از خدمات بانکی در فضای اینترنتی

چند نکته هنگام استفاده از رایانه در زمان اتصال به اینترنت جهت استفاده ازخدمات بانکی در فضای اینترنتی :

برای جلوگیری از دسترسی غیرمجاز به رایانه شخصی خود از فایروال استفاده کنید.

همواره از نرم افزارهای آنتی ویروس در سیستم خود استفاده نمایید و آن را به روز نگه دارید.

ایمیل های حاوی پیوست که از منابع ناشناس به شما ارسال می شود را بدون بازکردن فایل حذف کنید.

مطمئن شوید که هنگام وارد کردن شناسه کاربری و پسورد، شخص دیگری صفحه کلید شما را مشاهده نمی کند اگر از

کافی نت استفاده می کنید، توجه کنید که دوربین های مخفی رمزهای عبوری شما را ثبت نکنند.

دقت کنید، بانکها نیازی به اطلاعات محرمانه حساب شما ندارند. به ایمیل هایی که با عنوان ارسال از جانب بانک این اطلاعات را از شما درخواست می کنند، توجه نکنید.

برای استفاده از خدمات بانکی در فضای اینترنت هرگز از طریق رایانه های عمومی (مانند کافی نت ها)، و هر سیستمی که

به امن بودن آن اطمینان ندارید، اطلاعات خود را ارسال نکنید.

هوشیار باشید و به تقاضاهایی که از طریق پنجره های POP- UP برای شما ارسال می شود، پاسخ ندهید.

۶۹ نکته امنیتی بانک مرکزی برای استفاده از خدمات بانکداری الکترونیک

بانک مرکزی جمهوری اسلامی ایران با ابلاغ اطلاعیه‌ای نکاتی مهم امنیتی را برای استفاده از خدمات بانکداری الکترونیک برای اطلاع عموم شهروندان اعلام کرد.در این اطلاعیه آمده است که این نکات با هدف جلوگیری از سوءاستفاده‌های افراد سودجو از ناآگاهی شهروندان گرامی کشورمان حین استفاده از دستگاه‌های خودپرداز و خدمات بانک الکترونیکی اعلام شده است.

بنابراین گزارش، نکاتی مهم امنیتی اعلام شده توسط بانک مرکزی جمهوری اسلامی ایران برای پیشگیری از وقوع جرم در ارایه خدمات بانکداری الکترونیک به این شرح است :

۱ -هنگام دریافت پاکت رمز کارت بانک خود از شعبه به سلامت و عدم پارگی پاکت دقت کنید .

۲ -به محض وصول رمز کارت صادره، به دستگاه خودپرداز شعبه مراجعه و رمز خود را تغییر دهید .

۳ -به محض دریافت کارت‌بانک، نسبت به یادداشت کردن شماره ۱۶ رقمی آن اقدام نمایید. به خاطر داشته باشید برای مسدود کردن حساب هنگام سرقت یا مفقود شدن کارت به این شماره نیاز دارید.

۴ -شماره چهار رقمی که به عنوان رمز استفاده می‌کنید، به سادگی برای دیگران قابل حدس زدن نباشد. برای مثال از سال تولد، سال ازدواج یا شماره تلفن خود استفاده نکنید .

۵ -رمز جدید را به خاطر بسپارید و از یادداشت کردن رمز کنار کارت و قرار دادن برگه رمز در کیف کارت جدا خودداری کنید .

۶ -هنگام وارد کردن رمز در دستگاه خودپرداز، به گونه‌ای جلوی دستگاه بایستید که کسی امکان دیدن صفحه کلید را نداشته باشد .

۷ -رمز خود را هر سه تا چهار ماه تغییر دهید .

۸ -در فروشگاه‌ها و هنگام خرید از پایانه فروش، خودتان رمز را وارد دستگاه کنید و از اعلام آن به فروشنده خودداری نمایید .

۹ -در صورتی که در فروشگاهی مجبور به اعلام رمزتان شدید، حتی‌المقدور به سرعت نسبت به تغییر رمز خود اقدام نمایید .

۱۰ -از سپردن کارت خود به دیگران خودداری نمایید. در صورت لزوم، بلافاصله نسبت به تغییر رمز خود اقدام نمایند .

۱۱ -رسید دریافتی از دستگاه خودپرداز و کارتخوان را در محل رها نکنید .

۱۲ -در صورت بروز اشکال در عملیات بانکی، از توسل به افراد غریبه جدا خودداری کنید .

۱۳ -هنگام انجام عملیات انتقال وجه، فرد دریافت‌کننده فقط شماره ۱۶ رقمی کارت خود را اعلام می‌کند و نیازی به ارایه سایر اطلاعات کارت یا مراجعه به دستگاه خودپرداز ندارد .

۱۴ -از پایانه فروش فقط برای خرید، مانده‌گیری و پرداخت قبض استفاده کنید .

۱۵ -برای انتقال وجه به سایر حساب‌های خود یا دیگران به هیچ‌وجه از پایانه فروش استفاده نکنید .

۱۶ -برای انتقال وجه از دستگاه‌های خودپرداز، پایانه شعب یا خدمات ساتنا و پایا که در داخل شعبه ارایه می‌شود، بهره‌برداری کنید .

۱۷ -سقف انتقال وجه دستگاه خودپرداز سه میلیون تومان در هر روز است .

۱۸ -با مراجعه به شعبه و استفاده از پایانه شعبه می‌توانید تا سقف پانزده میلیون تومان به صورت آنی به سایر کارت‌های خود یا دیگران انتقال وجه دهید .

۱۹ -با مراجعه به شعبه و استفاده از سامانه پایا می‌توانید به هر حسابی در هر بانک تا سقف پانزده میلیون تومان در همان روز انتقال وجه دهید .

۲۰ -با مراجعه به شعبه و استفاده از سامانه ساتنا می‌توانید به هر حسابی در هر بانک به صورت نامحدود در همان روز انتقال وجه دهید .

۲۱ -برای انجام عملیات انتقال وجه از طریق پایا و ساتنا دانستن شماره شبای حساب مقصد الزامی است .

۲۲ -یک راه اطلاع از شماره شبا، مراجعه به شعبه یا سایت اینترنتی بانک افتتاح‌کننده حساب است .

۲۳ -هرگز برای دریافت شماره شبای بانک الف به سایت بانک ب مراجعه نکنید .

۲۴ -بانک مسوولیتی برای جبران خسارت مشتریانی که شماره شبای مقصد را اشتباه ثبت کرده‌اند، نخواهد داشت .

۲۵ -با داشتن کارت‌بانک می‌توانید قبوض خود را بدون مراجعه به شعب بانک‌ها پرداخت کنید .

۲۶ -مراجعه به دستگاه خودپرداز هریک از بانک‌ها یک راه پرداخت سریع قبض شماست .

۲۷ -مراجعه به پایانه فروش نصب شده در فروشگاه محل سکونت شما، یک راه پرداخت سریع قبض شماست .

۲۸ -مراجعه به پایانه شعبه هریک از بانک‌ها یک راه پرداخت سریع قبض شماست .

۲۹ -مراجعه به سایت هریک از بانک‌ها یک راه پرداخت سریع قبض شماست .

۳۰ -برای خریدهای اینترنتی داشتن رمز دوم الزامی است .

۳۱ -برای دریافت رمز دوم کارت به دستگاه خودپرداز بانک خود مراجعه کنید .

۳۲ -رمز اول و دوم کارت شما محرمانه است. از ارایه اطلاعات محرمانه کارت خود به دیگران خودداری کنید .

۳۳ -کدCVV ۲ کارت شما محرمانه است. از ارایه اطلاعات محرمانه کارت خود به دیگران خودداری کنید .

۳۴ -به محض اطلاع از مفقود شدن کارت خود، نسبت به مسدود کردن آن اقدام کنید .

۳۵ -به محض اطلاع از به سرقت رفتن کارت خود، نسبت به مسدود کردن آن اقدام کنید .

۳۶ -یک راه مسدود کردن کارت بانک، مراجعه به شعب بانک صادرکننده کارت است .

۳۷ -یک راه مسدود کردن کارت بانک، مراجعه به سایت اینترنتی بانک صادرکننده کارت است .

۳۸ -یک راه مسدود کردن کارت بانک، تماس با میز امداد بانک صادرکننده کارت است .

۳۹ -برای مسدود کردن کارت بانک داشتن رمز دوم کارت الزامی است .

۴۰ -هرگز برای پرکردن حساب جاری از پایانه فروش استفاده نکنید .

۴۱ -انتقال وجه از طریق اینترنت بانک، فقط با داشتن رمز مخصوص اینترنت بانک امکان‌پذیر است .

۴۲ -برای انجام عملیات انتقال وجه شتابی از همراه بانک استفاده نکنید .

۴۳ -در صورت عدم پرداخت اقساط کارت‌های اعتباری، کارت اعتباری شما به مدت شش ماه مسدود خواهد شد .

۴۴ -برای بهره‌برداری موثر از خدمات بانکداری الکترونیکی و ایمن ماندن از ریسک‌های احتمالی، هنگام افتتاح حساب و درخواست کارت بانک بروشورهای مربوطه را به دقت مطالعه کنید .

۴۵ -سایت بانک‌ها منبع مفیدی برای دریافت نکات ایمنی هنگام بهره‌برداری از خدمات بانکداری الکترونیکی است .

۴۶ -سایت پلیس فتا www.cyberpolice.ir منبع مفیدی برای دریافت آخرین اطلاعات مربوط به تهدیدات امنیتی است .

۴۷ -شماره تلفن ۲۹۹۱۱ راهی آسان برای ثبت مغایرت‌های شماست .

۴۸ -مامورین تعمیر پایانه فروش شرکت شما دارای کارت شناسایی از شرکت مربوطه هستند. از سپردن دستگاه خود به افراد ناشناس خودداری کنید .

۴۹ -رسید تراکنش‌های ناموفق خود را تا حصول اطمینان از کسر نشدن وجه از حساب‌تان نگهداری کنید .

۵۰ -استفاده از صفحه کلید مجازی سایت راهی مطمئن برای وارد کردن رمز .

۵۱ -هنگام انجام خرید یا پرداخت قبض در اینترنت، حتما از صفحه کلید مجازی برای وارد کردن رمز خود استفاده کنید .

۵۲ -شب‌ها از مراجعه به خودپردازهایی که در محل‌های کم رفت و آمد و تاریک قرار دارند، خودداری کنید .

۵۳ -توجه داشته باشید آدرس سایت سیستم اینترنت بانک و یا پرداخت اینترنتی در مرورگر باید با https آغاز شود .

۵۴ -برای ورود به سیستم اینترنت بانک و یا پرداخت اینترنتی هرگز از مکان‌های عمومی مانند کافه‌نت‌ها استفاده نکنید .

۵۵ -در انتخاب نام کاربری و کلمه عبور خود دقت نمایید تا دیگران نتوانند آن را حدس بزنند .

۵۶ -بدون خروج قطعی از اینترنت بانک، کامپیوتر را ترک نکنید .

۵۷ -فقط کلاهبرداران وانمود می‌کنند که برای انتقال وجه، باید از کارت ارزی خود استفاده کنند و شما را ترغیب به استفاده از منوی انگلیسی می‌کند .

۵۸ -با وارد کردن آدرس پست الکترونیکی هنگام پرداخت قبض یا خرید اینترنتی، بانک رسید عملیات را برای شما ارسال می‌کند که برای اطلاع و بهره‌برداری آتی بسیار مفید خواهد بود .

۵۹ -از انجام پرداخت‌های اینترنتی از طریق سایت‌های متعلق به موسسات غیرمعتبر و ناشناس در اینترنت خودداری کنید .

۶۰ -هیچ بانکی به اطلاعات محرمانه کارت شما (نظیر رمز اول یا دوم، کدCVV ۲ و تاریخ انقضای کارت) نیاز ندارد. به ایمیل‌ها و پیامک‌هایی که به عنوان بانک این اطلاعات را از شما می‌خواهند، هرگز پاسخ ندهید .

۶۱ -هرگز به تقاضاهایی که از طریق ایمیل یا پنجره‌های pop-up اطلاعات شخصی شما را می‌خواهند پاسخ ندهید .

۶۲ -از کامپیوتر افراد ناشناس یا کافه‌نت‌ها برای انجام عملیات بانکی خود استفاده نکنید .

۶۳ -روش‌های متعدد مسدودی کارت عبارتند از: اینترنت بانک، تلفنبانک، موبایل، خودپرداز، شعبه، مرکز تماس. به نحوه مسدودی کارت در بانک صادرکننده کارت خود را در ساعات کاری و ایام تعطیل توجه کنید .

۶۴ -برای انتقال وجه نیازی به استفاده از منوی انگلیسی نیست. منوی انگلیسی برای بهره‌برداری مسافران خارجی ایجاد شده است .

۶۵ -مراقب باشید: فقط کلاهبرداران شما را به استفاده از منوی انگلیسی ترغیب می کنند .

۶۶ -لطفا به محض اطلاع از مفقودی یا سرقت کارت خود، حساب خود را مسدود کنید .

۶۷ -هنگام دریافت کارت خود از شعبه بانک، شماره ۱۶ رقمی کارت و شماره تماس خدمات مشتریان بانک را از پشت کارت برای موارد ضروری یادداشت کنید .

۶۸ -برای دریافت رمز دوم به دستگاه خودپرداز بانک صادرکننده کارت خود مراجعه کنید .

۶۹ -درخواست ارسال پیامک در انجام تراکنش‌ها و ورود به خدمات غیرحضوری مانند اینترنت بانک، تلفنبانک و غیره باعث آگاهی مشتری از سوءاستفاده احتمالی و جلوگیری از سوءاستفاده بیشتر است. به محض دریافت چنین پیامکی در صورتی که خودتان تراکنشی انجام نداده‌اید، نسبت به تعویض رمز خود اقدام کنید ".

۱۰ پاسخ به ده اشتباه در مورد استفاده از اینترنت بانک

در ایران، اینترنت بانکها امکاناتی از قبیل دریافت موجودی به صورت آنلاین، انتقال وجه بین کلیه حساب ها در بانک ، مشاهده صورتحساب و ... را دراختیار مشتریان هربانک قرار می دهند. همچنین با استفاده از این خدمات، امکان مسدود نمودن کارت های مفقودی یا سرقتی میسر می باشد.

اما برخی از مشتریان بانک ها در استفاده از خدمات اینترنت بانک ها تردید دارند و از زیر استفاده کردن این خدمات شانه خالی می کنند. در این گزارش شما را با ۱۰ اشتباه رایج که مانع استفاده از اینترنت بانک می شود، آشنا می کنیم .

۱. رمز اینترنت بانک

برای ورود به سامانه اینترنت بانک بانک های کشور می بایست رمز اینترنتی جهت ورود به این سامانه را در اختیار داشته باشید. برخی این رمز را با رمز کارت بانک و یا حتی شماره حساب خود اشتباه می گیرند.

برای تهیه رمز اینترنت بانک می بایست به یکی از شعب بانک عامل خود مراجعه کنید و در خواست رمز اینترنتی کنید. خوشبختانه این روزها اغلب بانک ها هنگام افتتاح حساب نحوه استفاده از اینترنت بانک را به مشتریان خود آموزش داده و رمز اینترنت بانک را هم در اختیار ایشان می گذارند .

۲.اشتباه گرفتن خرید اینترنتی و اینترنت بانک

موضوع بعدی خرید و یا پرداخت اینترنتی است .خیلی ها خرید اینترنتی را با اینترنت بانک اشتباه می گیرند. شما با داشتن اینترنت بانک نمی توانید اقدام به خرید اینترنتی کنید و یا پرداخت وجه (مثل قبوض ...) را انجام بدهید و برای این کار نیاز به کارت خرید اینترنتی یکی از بانک ها دارید .به عبارتی کارت بانکی شما درصورتی که رمز دوم داشته باشید برای خرید اینترنتی قابل استفاده است .

۳.نگرانی از گم شدن وجه

یکی از نگرانی های بسیار رایجی که مانع استفاده افراد از اینترنت بانک می شود این است که نگرانند پولشان در جریان مبادلات بین بانکی گم بشود. اما لازم است بدانید هیچ تراکنشی در سیستم بانکداری الکترونیک مفقود و یا ناپدید نمی گردد. اگر هم به هر دلیل تراکنش شما با موفقیت انجام نگیرد پس از گذشت ۴۸ ساعت وجه به حساب شما باز می گرددو حتی اگر به هر دلیلی این امر هم محقق نشود با کمک شماره پیگیری که بانکتان در اختیار شما می گذارد می توانید روند انتقال وجه را پیگیری نمایید .

۴.استفاده از اینترنت بانک خطرناک است

عده ای بر این تصورند که استفاده از اینترنت بانک خطرناک است و از لحظه ای که وارد اینترنت خواهند شد دزدان و هکر ها در پی سرقت اموال ایشان هستند.درحالی که اغلب بانک ها سیستم های امنیتی پیچیده ای را جهت پیشگیری از سرقت های اینترنتی طراحی کرده اند و در صورتی که کاربران کلیه نکات امنیتی را رعایت کنند و رمز خود را در اختیار سایر افراد قرار ندهند امکان سرقت اینترنتی موجودیشان بسیار کمتر از امکان سرقت فیزیکی پولهایشان خواهد بود .

۵.در صورتی که از اینترنت بانک استفاده کنم حساب پولهایم را از دست می دهم

نگرانی از ولخرجی و خارج شدن حساب و کتاب خرج ها یکی دیگر از نگرانی هایی است که مانع از استفاده افراد از اینترنت بانک می شود. در حالی که به دلیل دقت بالای محاسبات سیستم بانکی به ویژه اینترنت بانک شما هر لحظه از شبانه روز قادر خواهید بود میزان موجودی خودتان را چک کنید و در خصوص میزان استفاده از پس انداز هایتان تصمیم گیری کنید. به این ترتیب پول کمتری را هدر خواهید داد.

۶.اگر از پرداخت الکترونیک استفاده کنم نمی توانم دیگران را متقاعد به پرداخت کنم

برخی هم از این نگرانند که اگر از پرداخت الکترونیک استفاده کنند به دلیل در اختیار نداشتن قبض رسید بانک قادر نخواهند بود شرکت ها و نهاد ها را متقاعد کنند؛به این ترتیب حتی از پرداخت الکترونیک قبوض هم شانه خالی می کنند، در حالی که تمامی وجوه انتقال داده شده در این سیستم به دقت ثبت می شود و پیگری پرداخت مبالغ با استفاده از این سیستم حتی از پیگیری شماره پرداخت رسید های بانکی هم راحت تر است و همانطور که پیشتر هم اشاره شد هیچ وجهی در این سیستم مفقود نمی گردد .

۷.بانک در ازای استفاده از اینترنت بانک کارمزد دریافت می کند

کسر کارمزد از دیگر دغدغه هایی است که سبب می شود افراد برای استفاده از اینترنت بانک و به طور کلی خدمات بانکداری الکترونیک به خود تردید راه بدهند،درصورتی که نه تنها کارمزدی از آنها کسر نمی شود بلکه اغلب بانک ها برای استفاده مشتریانشان از سیستم اینترنت بانک و یا هر یک از خدمات بانکداری الکترونیک مثل دستگاه های POSجوایزی را هم در نظر گرفته اند .

۸.اگر چه استفاده از اینترنت بانک در وقت صرفه جویی می کند، اما اگر مشکلی پیش بیاید باید زمان بیشتری صرف کرد

عده ای هم که نمی توانند سرعت و دقت استفاده از اینترنت بانک و سایرخدمات الکترونیک بانک ها را انکار کنند، نگران آن هستند که بروز هر مشکلی در پرداخت الکترونیک باعث به هدر رفتن وقت و انرژی آنها شود.

در صورتی که هنگام بروز هر گونه مشکل در هر یک از مراحل بانکداری الکترونیک به حضور فیزیکی مشتری نیازی نیست و اغلب اشکالات احتمالی از طریق استفاده از پشتیبانی تلفنی بانک ها و استفاده از شماره های پیگیری که در اختیار مشتریان قرار می گیرد قابل پیگیری است .

۹.اگر پولم اینترنتی سرقت شود دستم هیچ جابند نیست

این تصور غلط سبب می شود که افراد فکر کنند محیط اینترنت یک محیط کاملا باز است که هیچ نظارتی بر آن نیست و در صورتی که هکر ها اموال ایشان را سرقت کنند، دستشان به هیچ جا بند نیست.

همانطور که پیشتر هم اشاره شد، اگر هر فردی کلیه نکات امنیتی را رعایت کند، امکان سرقت اینترنتی بسیار کاهش می یابد .اگر هم خدای ناکرده سرقتی بروز کند پلیس اینترنتی (فتا) جهت کمک به هم میهنان راه اندازی شده و این ماموران با استفاده از امکاناتی که به آن دسترسی دارند مثل کد هایی IP که شماره منحصر به فردی است و برای تمامی کاربران اینترنت وجود دارد می توانند سارقان را شناسایی و دستگیر نمایند .

۱۰.هنگام استفاده از اینترنت بانک هیچ راهنمایی نیست

برخی با این تصور که وقتی به بانک مراجعه می کنند کارمندان بانک آنها را راهنمایی می کنند و در صورت بروز هر مشکلی راهکار را به آنها ارائه می کنند ترجیح می دهند به بانک مراجعه کنند و از اینترنت یا سایر خدمات الکترونیک استفاده نکنند.

در صورتی که اغلب بانک ها راهنماهای الکترونیک جامعی را برای استفاده از اینترنت بانک ها فراهم کرده اند و سیستم های پشتیبانی ومشاوره آنها هم در اغلب ساعات شبانه روز آمادگی پاسخگویی به تمامی سوالات شما را دارند .

۸گام موثر پس از سرقت اطلاعات بانکی

همیشه سود جویانی هستند که برای کسب پول بدون زحمت به دزدی روی می آورند این افراد از هر بستری برای سرقت استفاده می کنند ازخیابان های شلوغ و پر رفت آمد گرفته تا محیط گسترده اینترنت.

۸ گام موثر را که پس از سرقت اینترنتی باید بپیماییم که اگر اطلاعات شما سرقت شد می بایست انجام دهید :

۱.پیش از هر کاری کلیه رمزهای کارتتان (اعم از رمز کارت و رمز اینترنتی) را تغییر بدهید.

برای انجام این کار کافی است به یکی از(ATM) خود پرداز های بانک خود مراجعه کنید و با انتخاب گزینه تغییر رمز ,رمز جدیدی انتخاب کنید.

از انتخاب تاریخ تولد,شماره شناسنامه , سال تولد و ترکیب هایی که به راحتی قابل حدس زدن هستند پرهیز کنید.

در مواردی که مبلغ قابل توجهی در حساب بانکی تان موجود است آن را به یک حساب دیگر منتقل کنید یا حسابتان را خالی کنید.

۲.با مراجعه به شعبه ای که در آن حساب دارید پرینتی از آخرین تراکنش های بانکی تان دریافت کنید .

به این ترتیب از جزئیات سرقت مطلع می شوید. مثلا این که در چند مرحله و در هر مرحله چه میزان وجه از حسابتان کسر شده است.

۳.به دادسرا یاآگاهی جرائم رایانه ای مراجعه کنید و شکایت تنظیم نمایید.

هنگام مراجعه به داد سرا یک کارت شناسایی معتبر(کارت ملی یا شناسنامه) و پیرینت آخرین گردش های مالی حساب مورد سرقت قرار گرفته را به همراه داشته باشید.

پلیس فتا به طور تخصصی به بررسی جرائم اینترنتی و سرقت های انجام شده در محیط سایبر می پردازد.

۴. نامه ای از پلیس و دادسرا دریافت نمایید تا بتوانید درگاهی که از طریق آن از کارت شما خرید شده مشخص کنید و به این ترتیب فروشگاه یا هر مرکزی که از طریق اطلاعات کارت شما از آن خرید انجام شده باشد مشخص می گردد.

۵. مراجعه به مجموعه ای که با کارت شما از آنها خرید شده است.

با مراجعه به مجموعه هایی که با کارت شما از آنها خرید شده و ارائه نامه رسمی دادگستری یا پلیس سایبری کشور می توانید) IP آدرس آی پی ، شماره شناسایی هر کامپیوتر متصل به شبکه اینترنت است. بنابر این می توان گفت که آی پی، شماره شناسایی هر کاربر اینترنتی است.) هر مکانی که از طریق آن خرید ها انجام شده را مشخص نمایید.

۶. شرکت موظف است کلیه اطلاعات در خواستی را به پلیس اعلام نماید.

IP.۷ از طریق مخابرات شناسایی می شود و به این ترتیب می توان محل سرقت را پیدا کرد.

۸. پلیس با مراجعه حضوری به محل, سارق را شناسایی و دستگیر می نماید.

در بسیاری موارد اگر شانس داشته باشید به پولتان دست پیدا خواهید کرد اما هیچ گاه تضمینی نیست که اموالتان را بدست بیاورید بنا بر این توصیه می شود پیش از هر اقدامی در نگهداری و حفظ اطلاعات کارت خود دقت کافی را به عمل آورید.

چگونه از اطلاعاتمان محافظت کنیم ؟

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.

مفاد مرتبط با حمایت از مصرف کنندگان در قانون تجارت الکترونیکی

فصل اول- حمایت از مصرف کننده(consumer protection)

ماده ۳۳- فروشندگان کالا و ارائه دهندگان خدمات بایستی اطلاعات مؤثر در تصمیم گیری مصرف کنندگان جهت خرید و یا قبول شرایط را از زمان مناسبی قبل از عقد در اختیار مصرف کنندگان قرار دهند. حداقل اطلاعات لازم، شامل موارد زیر می‌باشد:

الف- مشخصات فنی و ویژگی‌های کاربردی کالا و یا خدمات.

ب- هویت تأمین کننده، نام تجاری که تحت آن نام به فعالیت مشغول می‌باشد و نشانی وی.

ج- آدرس پست الکترونیکی، شماره تلفن و یا هر روشی که مشتری در صورت نیاز بایستی از آن طریق با فروشنده ارتباط برقرار کند.

د- کلیه هزینه هایی که برای خرید کالا بر عهده مشتری خواهد بود (از جمله قیمت کالا و یا خدمات، میزان مالیات، هزینه حمل، هزینه تماس.(

ه- مدت زمانی که پیشنهاد ارائه شده معتبر می‌باشد.

و- شرایط و فرایند عقد از جمله ترتیب و نحوه پرداخت، تحویل و یا اجرا، فسخ، ارجاع، خدمات پس از فروش.

ماده ۳۴- تأمین کننده باید به طور جداگانه ضمن تأیید اطلاعات مقدماتی، اطلاعات زیر را ارسال نماید:

الف- آدرس محل تجاری یا کاری تأمین کننده برای شکایت احتمالی.

ب- اطلاعات راجع به ضمانت و پشتیبانی پس از فروش.

ج- شرایط و فراگرد فسخ معامله به موجب مواد (۳۷) و (۳۸) این قانون.

د- شرایط فسخ در قراردادهای انجام خدمات.

ماده ۳۵- اطلاعات اعلامی و تأییدیه اطلاعات اعلامی به مصرف کننده باید در واسطی با دوام، روشن و صریح بوده و در زمان مناسب و با وسایل مناسب ارتباطی در مدت معین و براساس لزوم حسن نیت در معاملات و از جمله ضرورت رعایت افراد ناتوان و کودکان ارائه شود.

ماده ۳۶- در صورت استفاده از ارتباط صوتی، هویت تأمین کننده و قصد وی از ایجاد تماس با مصرف کننده باید به طور روشن و صریح در شروع هر مکالمه بیان شود .

ماده ۳۷- در هر معامله از راه دور مصرف کننده باید حداقل هفت روز کاری، وقت برای انصراف (حق انصراف) از قبول خود بدون تحمل جریمه و یا ارائه دلیل داشته باشد. تنها هزینه تحمیلی بر مصرف کننده هزینه باز پس فرستادن کالاخواهد بود.

ماده ۳۸- شروع اعمال حق انصراف به ترتیب زیر خواهد بود:

الف- در صورت فروش کالا، از تاریخ تسلیم کالا به مصرف کننده و در صورت فروش خدمات، از روز انعقاد.

ب- در هر حال آغاز اعمال حق انصراف مصرف کننده پس از ارائه اطلاعاتی خواهد بود که تأمین کننده طبق مواد(۳۳) و (۳۴) این قانون موظف به ارائه آن است.

ج- به محض استفاده مصرف کننده از حق انصراف،تأمین کننده مکلف است بدون مطالبه هیچ گونه وجهی عین مبلغ دریافتی را در اسرع وقت به مصرف کننده مسترد نماید.

د- حق انصراف مصرف کننده در مواردی که شرایط خاصی بر نوع کالا و خدمات حاکم است اجرا نخواهد شد. موارد آن به موجب آیین‌نامه‌ای است که در ماده (۷۹ (این قانون خواهد آمد.

ماده ۳۹- در صورتی که تأمین کننده در حین معامله به دلیل عدم موجودی کالا و یا عدم امکان اجرای خدمات، نتواند تعهدات خود را انجام دهد، باید مبلغ دریافتی را فوراً به مخاطب برگرداند، مگر دربیع کلی و تعهداتی که برای همیشه وفای به تعهد غیر ممکن نباشد و مخاطب آماده صبر کردن تا امکان تحویل کالا و یا ایفای تعهد باشد. در صورتی که معلوم شود تأمین کننده از ابتدا عدم امکان ایفای تعهد خود را می‌دانسته، علاوه بر لزوم استرداد مبلغ دریافتی، به حداکثر مجازات مقرر در این قانون نیز محکوم خواهد شد.

ماده ۴۰- تأمین کننده می‌تواند کالا یا خدمات مشابه آنچه را که به مصرف کننده وعده کرده تحویل یا ارائه نماید مشروط بر آن که قبل از معامله یا در حین انجام معامله آن را اعلام کرده باشد.

ماده ۴۱- در صورتی که تأمین کننده، کالا یا خدمات دیگری غیر از موضوع معامله یا تعهد را برای مخاطب ارسال نماید، کالا و یا خدمات ارجاع داده میشود و هزینه ارجاع به عهده تأمین کننده است. کالا یا خدمات ارسالی مذکور چنانچه به عنوان یک معامله یا تعهد دیگر از سوی تأمین کننده مورد ایجاب قرار گیرد، مخاطب می تواند آن را قبول کند.

ماده ۴۲- حمایت‌های این فصل در موارد زیر اجرا نخواهد شد:

الف- خدمات مالی که فهرست آن به موجب آیین‌نامه‌ای است که در ماده (۷۹) این قانون خواهد آمد.

ب- معاملات راجع به فروش اموال غیر منقول و یا حقوق مالکیت ناشی از اموال غیرمنقول به جز اجاره.

ج- خرید از ماشین‌هایی فروش مستقیم کالا و خدمات.

د- معاملاتی که با استفاده از تلفن عمومی (همگانی) انجام می‌شود.

ه- معاملات راجع به حراجی ها.

ماده ۴۳- تأمین کننده نباید سکوت مصرف کننده را حمل بر رضایت وی کند.

ماده ۴۴- در موارد اختلاف و یا تردید مراجع قضایی رسیدگی خواهند کرد.

ماده ۴۵- اجرای حقوق مصرف کننده به موجب این قانون نباید بر اساس سایر قوانین که حمایت ضعیفتری اعمال میکنند متوقف شود.

ماده ۴۶- استفاده از شروط قراردادی خلاف مقررات این فصل و همچنین اعمال شروط غیرمنصفانه به ضرر مصرف کننده، مؤثر نیست.

ماده ۴۷- در معاملات از راه دور آن بخش از موضوع معامله که به روشی غیر از وسایل ارتباط از راه دور انجام میشود مشمول مقررات این قانون نخواهد بود.

ماده ۴۸- سازمان‌های قانونی و مدنی حمایت از حقوق مصرف کننده می‌توانند به عنوان شاکی اقامه دعوی نمایند. ترتیب آن به موجب آیین نامه ای خواهد بود که به پیشنهاد وزارت بازرگانی و تصویب هیأت وزیران میباشد.

ماده ۴۹- حقوق مصرف کننده در زمان استفاده از وسایل پرداخت الکترونیکی به موجب قوانین و مقرراتی است که توسط مراجع قانونی ذیربط تصویب شده و یا خواهد شد.

فصل دوم- در قواعد تبلیغ(marketing) -

ماده ۵۰- تأمین کنندگان در تبلیغ کالا و خدمات خود نباید مرتکب فعل یا ترک فعلی شوند که سبب مشتبه شدن و یا فریب مخاطب از حیث کمیت و کیفیت شود.

ماده ۵۱- تأمین کنندگانی که برای فروش کالا و خدمات خود تبلیغ میکنند نباید سلامتی افراد را به خطر اندازند.

ماده ۵۲- تأمین کننده باید به نحوی تبلیغ کند که مصرف کننده به طور دقیق، صحیح و روشن اطلاعات مربوط به کالا و خدمات را درک کند.

ماده ۵۳- در تبلیغات و بازاریابی باید هویت شخص یا بنگاهی که تبلیغات به نفع اوست روشن و صریح باشد.

ماده ۵۴- تأمین کنندگان نباید از خصوصیات ویژه معاملات به روش الکترونیکی جهت مخفی نمودن حقایق مربوط به هویت یا محل کسب خود سوء استفاده کنند .

ماده ۵۵- تأمین کنندگان باید تمهیداتی را برای مصرف کنندگان درنظر بگیرند تا آنان راجع به دریافت تبلیغات به نشانی پستی و یا پست الکترونیکی خود تصمیم بگیرند.

ماده ۵۶- تأمین کنندگان در تبلیغات باید مطابق با رویه حرفه‌ای عمل نمایند .ضوابط آن به موجب آیین‌نامه‌ای است که در ماده (۷۹) این قانون خواهد آمد.

ماده ۵۷- تبلیغ و بازاریابی برای کودکان و نوجوانان زیر سن قانونی به موجب آیین‌نامه ای است که در ماده (۷۹) این قانون خواهد آمد.

فصل سوم- حمایت از «داده‌پیام»های شخصی

)حمایت از داده(data protection -

ماده ۵۸- ذخیره، پردازش و یا توزیع «داده‌پیام»های شخصی مبین ریشه‌های قومی یا نژادی، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و

«داده‌پیام»های راجع به وضعیت جسمانی، روانی و یا جنسی اشخاص بدون رضایت صریح آنها به هر عنوان غیر قانونی است.

ماده ۵۹- در صورت رضایت شخص موضوع «داده‌پیام» نیز به شرط آن که محتوای داده‌پیام وفق قوانین مصوب مجلس شورای اسلامی باشد ذخیره، پردازش و توزیع »داده‌پیام»های شخصی در بستر مبادلات الکترونیکی باید با لحاظ شرایط زیر صورت پذیرد:

الف- اهداف آن مشخص بوده و به طور واضح شرح داده شده باشند.

ب- «داده‌پیام» باید تنها به اندازه ضرورت و متناسب با اهدافی که در هنگام جمع‌آوری برای شخص موضوع «داده‌پیام» شرح داده شده جمع آوری گردد و تنها برای اهداف تعیین شده مورد استفاده قرار گیرد.

ج- «داده‌پیام» باید صحیح و روزآمد باشد.

د- شخص موضوع «داده‌پیام» باید به پرونده‌های رایان‌های حاوی »داده‌پیام»های شخصی مربوط به خود دسترسی داشته و بتواند «داده‌پیام»هایی ناقص و یا نادرست را محو یا اصلاح کند.

ه- شخص موضوع «داده‌پیام» باید بتواند در هر زمان با رعایت ضوابط مربوطه در خواست محو کامل پرونده رایانه‌ای «داده‌پیام»های شخصی مربوط به خود را بنماید.

ماده ۶۰- ذخیره، پردازش و یا توزیع «داده‌پیام»های مربوطه به سوابق پزشکی و بهداشتی تابع آیین‌نامه‌ای است که در ماده (۷۹) این قانون خواهد آمد.

ماده ۶۱- سایر موارد راجع به دسترسی موضوع «داده‌پیام» از قبیل استثنائات، افشای آن برای اشخاص ثالث، اعتراض، فراگردهای ایمنی، نهادهای مسئول دیدبانی و کنترل جریان «داده‌پیام»های شخصی به موجب مواد مندرج در باب چهارم این قانون و آیین نامه مربوطه خواهد بود.

از "پلیس فتا" چه می دانید ؟

پلیس فضای تولید و تبادل اطّلاعات کشور با نام اختصاری فتا در سال ۱۳۸۹ تشکیل شد.

توسعه روزافزون زیرساخت‌های فناوری اطلاعات و ارتباطات در کشور و افزایش کاربران و استفاده‌کنندگان از اینترنت و سایر فناوری‌های اطلاعاتی، ارتباطی و مخابراتی نظیر خطوط تلفن‌های ثابت و همراه، شبکه‌های دیتای کشوری و محلی، ارتباطات ماهواره‌ای از جمله دلایلی است که لزوم ایجاد و توسعه سازوکاری برای برقراری امنیت در فضای تولید و تبادل اطلاعات جمهوری اسلامی ایران را توجیه می‌کند.

همچنین توسعه خدمات الکترونیک در کشور نظیر دولت الکترونیک، بانکداری الکترونیک، تجارت الکترونیک، آموزش الکترونیک و سایر خدمات از این دست نیز لزوم ایجاد پلیسی تخصصی در مجموعه نیروی انتظامی جمهوری اسلامی ایران را برای تأمین امنیت و مقابله با جرایمی که در این فضا به وقوع می‌پیوندند را آشکار می‌کند.

از سوی دیگر، رشد قارچ‌گونه جرایم در حوزه فضای تولید و تبادل اطّلاعات کشور (فتا) مثل کلاهبرداری‌های اینترنتی، جعل داده‌ها و عناوین، سرقت اطّلاعات، تجاوز به حریم خصوصی اشخاص و گروه‌ها، هک و نفوذ به سامانه‌های رایانه‌ای و اینترنتی، هرزه‌نگاری و جرایم اخلاقی و برخی جرایم سازمان‌یافته اقتصادی، اجتماعی و فرهنگی ایجاب می‌کند که پلیس تخصّصی که توان پی‌جویی و رسیدگی به جرایم سطح بالای فناورانه داشته باشد، به وجود آید.

از سوی دیگر با توجه به تصویب قانون جرایم رایانه‌ای در مجلس شورای اسلامی و لزوم تعیین ضابط قضایی برای این قانون و نیز مصوبات کمیسیون افتای

دولت جمهوری اسلامی ایران مبنی بر تشکیل پلیس فضای تولید و تبادل اطلاعات، این پلیس در بهمن‌ماه سال ۱۳۸۹ به دستور سردار فرماندهی محترم نیروی انتظامی جمهوری اسلامی ایران، تشکیل گردید.

سخن پایانی

در پایان یادآوری می نمایم که افراد کلاهبردار ، صرفاً افرادی باهوش و نابغه ای نیستند ، بلکه مهارت آنها استفاده از نقطه ضعف ، ناآگاهی و سادگی افراد می باشد ، پس تا می توانید سطح دانش ، آگاهی و هوشیاری خود را بالا ببرید و بدانید که ، کلاهبرداران اینترنتی از راه های مختلف، دست به تخلف می زنند و شگردهای خود را پیوسته تغییر می دهند. این من و شما هستیم که باید بیشتر مراقب باشیم. در پرداخت های اینترنتی خود بسیار دقت کنید و کنجکاو باشید ، به راحتی گول تبلیغات محصولات ارزان را نخورید ، همانطور که خواندید هر ارزانی بی دلیل نیست ... از فروشگاه های اینترنتی خرید کنید که حداقل امکان پرداخت پستی در آن فراهم باشد ، یعنی اول کالا را تحویل بگیرید و سپس مبلغ را بپردازید ، به این شکل حداقل مطمئن هستید کالا به دستتان خواهد رسید ، حالا چقدر این کالا از نظر کیفیت با تبلیغاتش هماهنگی دارد، قضاوتش با خودتان است ! هر زمان که قصد خرید کالایی از فروشگاه اینترنتی را داشتید در مورد درستی و صحت فعالیت آن فروشگاه از طریق جستجوگرها تحقیق کنید و از تجربیات و نظرات دیگر کاربران در مورد همان سایت بهره ببرید ، متاسفانه فروشگاه های اینترنتی زیادی هستند که مشتریانی ناراضی دارند و بعضاً در بین آنها فروشگاه های معروف و مشهوری هم وجود دارد !! (با کمی جستجو در اینترنت متوجه این موضوع خواهید شد) در پرداخت اینترنتی به هیچ فردی ، خصوصاً در مکان های عمومی اعتماد نکنید (متاسفانه بیشتر کلاهبرداری ها و ضررهای وارده به ما ایرانیان از اعتمادهای بی جاست) . کمی صبر و دقت کنید و هر زمان که پرداخت اینترنتی خود را نهایی کردید و به دروازه پرداخت بانک هدایت شدید ، در قسمت آدرس ، دقت کنید که دقیقاً همان آدرس دروازه پرداخت بانک مورد نظر باشد ، چرا که در غیر اینصورت با صفحه جعلی روبرو هستید ، در نهایت اگر در اینترنت هر مشکلی برایتان پیش آمد آن را سریعاً به پلیس فتا و مراجع مربوطه اطلاع دهید .

امیدوارم این کتاب و مطالبش برای شما کاربر محترم ، آموزنده و مفید بوده باشد ، آرزو می کنم با بکارگیری دانش و هوشیاری تان در فضای مجازی ، مجال سوء استفاده به افراد کلاهبردار را ندهید ، مجدداً یادآوری میکنم علاوه بر اینکه این کتاب را خوانده اید ، نکته ها و هشدارهای آن را جدی بگیرید تا هیچگاه در **اینترنت سرتان کلاه نرود !**

پایان

موفق و سلامت باشید

رضا فریدون نژاد

مجموعه کتابهای الکترونیکی

دانش و زندگی

کتابهایی مختصر ، مفید و کاربردی

دانلود کاملاً رایگان

WWW.DZBOOK.IR

گردآوری و تنظیم : رضا فریدون نژاد

منابع :

پلیس فتا (http://www.cyberpolice.ir)

بانکی دات آی آر (http://www.banki.ir)

همشهری آنلاین (www.hamshahrionline.ir)

ایران هشدار (http://www.iranhoshdar.ir)

اینماد (http://www.enamad.ir)

با احترام

رضا فریدون نژاد

rezaf1390@gmail.com