مَجازنامه‌ای برای آموزش حقیقت
مجازی حقیقی
امور فرهنگی و دینی شرکت آبفا اهواز | شماره اول | ۲۷ آبان‌ماه ۱۴۰۰

تهدیدات اقتصادی وب‌سایت‌های دستِ دوم فروشی

در این مطلب آموزشی پیرامون شگردهای کلاهبرداری در فضای مجازی به واسطه خرید و فروش های بدون واسطه با شما صحبت می‌کنیم.

شهروندان برای معامله اجناس، خودرو، ملک، کاریابی و خدمات متنوع دیگر اقدام به انتشار آگهی و یا جستجوی نیازمندی‌ها از طریق وب‌سایت‌هایی مانند دیوار و شیپور می‌نمایند.

در کنار مزایای مطلوب و ارزشمند اینگونه وب‌سایت‌ها، متأسفانه افراد تبهکار و مجرم با بکارگیری شگردهای کلاهبرداری اقدام به فریب کاربران ناآگاه می‌کنند، بنابراین آگاهی شهروندان از ترفندهای مجرمین سایبری بسیار ضروری است، به همین خاطر کالبدشکافی انواع جرائم سایبری باعث هوشیاری کاربران فضای مجازی و پیشگیری از وقوع جرائم می‌شود.

رایج‌ترین روش‌های کلاهبرداری

۱. بیعانه

در این روش شخص کلاهبردار اقدام به انتشار آگهی فروش جنس دست دوم با قیمت و مشخصات کیفی چشم‌نواز می‌نماید، افراد بسیاری با شماره موبایل وی تماس می‌گیرند و به شوق دریافت جنس دست دوم ارزان، اقدام به واریز مبلغ بیعانه به کارت بانکی منتسب به شخص مذکور می‌کنند، لیکن دیگر پاسخی از فروشنده جعلی دریافت نمی‌کنند، شایان ذکر است کلاهبردار از حقه‌های متنوعی مانند اجاره کارت‌های بانکی، سرقت شناسه‌ها و رمز دوم کارت‌های بانکی، همچنین سیم کارت‌های بی‌نام و یا فعال شده با مدارک شناسایی دیگران برای مخفی کردن هویت واقعی خود استفاده می‌کند.

۲. کارت بانکی واسط

در این روش مجرم سایبری به اطلاعات و رمز دوم کارت بانکی دیگران یا کارت‌های اجاره‌ای دسترسی ندارد، در واقع او با بهره‌گیری از تکنیک‌های مهندسی اجتماعی باعث فریب خریدار و فروشنده واقعی می‌شود، برای درک این شیوه مجرمانه، ۳ مثال بیان می‌گردد:

مثال ۱: شخص کلاهبردار به طلافروشی می‌رود، برای خرید طلای انتخابی با مبلغ مشخص، شماره کارت بانکی و تلفن فروشنده را یادداشت می‌کند، سپس در وب سایت دیوار و شیپور جستجو می‌کند تا آگهی فروش یک خودروی با کیفیت را پیدا کند، سپس اقدام به جعل آگهی با قیمت و شرایط بسیار مناسب می‌کند، خریدار تماس می‌گیرد کلاهبردار از او می‌خواهد تا مبلغ بیعانه (مطابق قیمت طلای انتخابی) به شماره کارت بانکی (متعلق به طلافروش) واریز شود به محض

مَجازنامه‌ای برای آموزش حقیقت
مجازی حقیقی
امور فرهنگی و دینی شرکت آبفا اهواز | شماره اول | ۲۷ آبان‌ماه ۱۴۰۰

تهدیدات اقتصادی وب‌سایت‌های دستِ دوم فروشی

واریز پول با فروشنده تماس می‌گیرد و اعلام می کند مبلغ واریز شده است و برای دریافت طلا اقدام می‌کند.

مثال ۲: شخص تبهکار از طریق شبکه‌های اجتماعی مجازی با افرادی که گیفت کارت‌های خارجی عرضه می‌کنند ارتباط و شماره کارت بانکی آن‌ها را می‌گیرد، سپس در اینستاگرام اقدام به راه‌اندازی فروشگاه جعلی با محصولات و قیمت‌های بسیار ارزان می‌کند، سپس به خریدارها می گوید بیعانه (مطابق با قیمت گیفت کارت‌ها) به یکی از شماره کارت‌های مذکور واریز شود، بنابراین به فروشنده واقعی اطلاع می‌دهد که مبلغ را خودش واریز کرده است و اطلاعات گیفت کارت برای شارژ حساب یا فروش به دیگران دریافت می‌گردد.

مثال ۳: شخص فریب‌کار در وب‌سایت دیوار یا شیپور تبلیغ جعلی فروش یک واحد مسکونی با مشخصات مطلوب و قیمت ارزان منتشر می‌کند، خریدارهای زیادی تماس می‌گیرند و شماره آن‌ها برای اعلام نتیجه در گوشی کلاهبردار ذخیره می‌شود، شخص مذکور اقدام به گرفتن خودروی مسافربری از طریق تماس با تاکسی تلفنی یا برنامه‌های اینترنتی می‌کند، پس از پیاده شدن به راننده خودرو می‌گوید که کیف پول و کارت بانکی همراهش نیست، بنابراین شماره کارت بانکی راننده را می‌گیرد، با یکی از خریدارهای واحد مسکونی تماس می گیرد و اعلام می‌کند برای معامله منزل باید بیعانه‌ای به شماره کارت مذکور واریز نماید، سرانجام از طریق خودپرداز و کارت بانکی راننده، اقدام به برداشت بیعانه و همچنین پرداخت مبلغ کرایه می‌کند، به همین ترتیب بیعانه‌های متعددی از خریدارهای دیگر به واسطه تبلیغ صوری و کارت‌های بانکی متعلق به راننده‌های بی‌خبر برداشت می‌گردد.

۳. فیشینگ

در این روش مجرم سایبری تحت عنوان فروشنده به بهانه‌های مختلف اقدام به ارسال لینک درگاه جعلی بانک برای کاربران می‌نماید و با این ترفند به شناسه‌ها و رمز دوم کارت بانکی آنها دسترسی پیدا می‌کند.

مثال ۱: کلاهبردار در نقش فروشنده اقدام به انتشار آگهی فروش جنس دست دوم قابل حمل با قیمت بسیار ارزان در وب سایت دیوار یا شیپور می‌کند، سپس به خریدار می‌گوید از طریق لینک ارسالی ابتدا مشخصات شخصی مطابق فرم ثبت و از طریق درگاه بانکی مختص به پیک موتوری مبلغ ۱۵ هزار تومان واریز کند، سرانجام به محض دریافت جنس دست دوم و اطمینان از صحت

مَجازنامه‌ای برای آموزش حقیقت
مجازی حقیقی
امور فرهنگی و دینی شرکت آبفا اهواز ■ شماره اول ۲۷ آبان‌ماه ۱۴۰۰

تهدیدات اقتصادی وب‌سایت‌های دست دوم فروشی

معامله اقدام به پرداخت هزینه اصلی به پیک موتوری نماید، بنابراین لینک جعلی درگاه بانک ارسال می‌شود، بنابراین اطلاعات و سپس موجودی کارت بانکی خریدار سرقت می‌شود.

مثال ۲: مجرم سایبری اقدام به دسترسی غیرمجاز به پنل پیامکی یا فعال‌سازی آن با مدارک هویتی دیگران می‌کند، سپس در وب‌سایت دیوار یا شیپور شروع به جمع‌آوری شماره‌های موبایل مربوط به آگهی‌های قابل اهمیت می‌کند، سپس برای کاربران مربوطه پیامی با این مضمون منتسب به سایت دیوار ارسال می‌گردد:
"برای عدم منقضی شدن حساب کاربری و آگهی‌های شما در سایت دیوار از طریق لینک ضمیمه، مبلغ ۲ هزار تومان به قید فوریت پرداخت کنید."
بنابراین با هدایت کاربران ساده لوح به درگاه جعلی بانک، اطلاعات و سپس موجودی کارت‌های بانکی فریب خوردگان سرقت می‌شود.

مثال ۳: مجرم سایبری به عنوان کارمند یک سازمان دولتی در وب‌سایت دیوار اقدام به انتشار آگهی مبنی بر فروش امتیاز وام با مبلغ ۵۰ میلیون تومان، اقساط ٦ ساله و بهره ٤ درصد می‌نماید، پس از ارتباط با متقاضی به این بهانه که پیگیری اعطای امتیاز وام به صورت حضوری از طریق بانک عامل ۱۰ روز طول خواهد کشید، بنابراین برای اقدام سریع لینکی ارسال تا متقاضی پس از ثبت شماره موبایل و کد ملی، اقدام به پرداخت مبلغ ٤ هزار تومان جهت دریافت کد اعتبارسنجی نماید تا کارمند مذکور در اسرع وقت یک روز مرخصی گرفته و اقدامات واگذاری وام و دریافت حق امتیاز به مبلغ ۵ میلیون تومان در بانک عامل انجام شود.
متقاضی با هیجان وصف نشدنی از طریق درگاه پرداخت جعلی بانک عامل، اقدام به ثبت شناسه‌های کارت بانکی و رمز دوم می کند پس از تأیید پرداخت این پیام صادر می‌شود:
"بانک شما تراکنش‌های زیر ۵۰.۰۰۰ ریال را پشتیبانی نمی‌کند، لطفا با کارت بانکی دیگری امتحان کنید."
با این ترفند اطلاعات و سپس موجودی کارت‌های بانکی متقاضی سرقت می‌شود.

مثال ٤: جعل رسید پرداخت

تبهکار اینترنتی در نقش خریدار با فروشنده تماس می‌گیرد سپس برای تحویل جنس دست دوم به سمت آدرس مربوطه می‌رود، برای پرداخت هزینه از طریق برنامه آپ یا سکه شماره کارت خریدار ثبت می‌گردد تا نام و نام خانوادگی او مشخص شود، سپس از طریق برنامه رسیدساز اقدام به تکمیل مشخصه‌ها و صدور رسید جعلی می‌کند و رسید تقلبی به فروشنده نشان داده می‌شود، اگر فروشنده

مَجازنامه‌ای برای آموزش حقیقت
مجازی حقیقی
امور فرهنگی و دینی شرکت آبفا اهواز ■ شماره اول ۲۷ آبان‌ماه ۱۴۰۰

تهدیدات اقتصادی وب‌سایت‌های دستِ دوم فروشی

در مورد عدم دریافت پیامک بانکی سوال کند، خریدار صوری می‌گویدَ به احتمال زیاد سیستم پیامک بانکی دچار مشکل شده است و پیامک واریزی حداکثر تا ۳۰ دقیقه دیگر توسط شما دریافت خواهد شد، جنس دست دوم را گرفته و به سرعت از محل خارج می‌شود.

مثال۵: پرداخت با کارت بانکی دیگران

مجرمین سایبری به واسطه کپی‌برداری از کارت‌های بانکی دیگران به وسیله دستگاه اسکیمر، همچنین سرقت شناسه‌ها و رمز دوم اینترنتی کاربران به واسطه درگاه‌های جعلی اقدام به خرید جنس‌های دست دوم با مبالغ موجود در این کارت‌ها می‌کنند به این ترتیب پس از شکایت مالکین کارت‌های بانکی، فروشندگان بی خبر در معرض اتهام قضایی قرار می‌گیرند.

مثال٦: اموال سرقتی

برخی از سارقین به واسطه وب‌سایت‌های دست دوم فروشی اقدام به فروش اموال مسروقه با قیمت های بسیار پایین می‌نمایند، لذا اکثر خریدارها اهمیتی برای بررسی مدارک هویتی فروشنده قائل نیستند، برخی از مالباختگان از طریق این وب‌سایت‌ها متوجه فروش اموال‌شان می‌شوند، به هر حال پس از طی اقدامات قضایی و فنی، سارق توسط پلیس شناسایی و دستگیر می‌شود، سارقین در بازجویی اقدام به معرفی خریداران اموال سرقتی می‌کنند.