راهکارهای پیشگیری از فریب‌های اینترنتی

شیوع کرونا تاثیر بسیاری در زمینه رشد کسب وکارهای اینترنتی داشته و استقبال مردم به انجام امور و خریدهای اینترنتی نسبت به دوران قبل از شیوع این ویروس بسیار متفاوت است، اما پیش‌بینی می‌شود پس از پایان همه‌گیری کرونا و بازگشت مردم به زندگی عادی نیز رونق کسب وکارهای اینترنتی حفظ شود، زیرا خرید و انجام امور در بستر فضای مجازی و اینترنت در حال تبدیل به یک فرهنگ در جامعه امروزی است.

با توجه به شرایط کنونی جامعه، اکثر کسب‌وکارها به سوی فضای مجازی و سایت‌های خرید و فروش آنلاین سوق یافته که در این بین کلاهبرداران سایبری با ترفندهای مختلف از کاربران اقدام به کلاهبرداری می‌کنند. بعضی اوقات مشاهده می‌شود که کاربران فضای مجازی و شهروندان برای تهیه لوازم مورد نیاز خود با مراجعه به سایت‌های خرید و فروش، با سهل‌انگاری و زود اعتماد کردن، در دام مجرمان سایبری گرفتار می‌شوند.

۱- بدون شناخت و بی هدف عضو هر گروه یا کانال نشوید و هچنین روی هر لینکی کلیک نکنید: پیامک تسهیلات بانکی، وام مسکن، بسته رایگان اینترنت و...روش خوبی برای فریب می باشد، بنابراین بی جهت کلیک نکنید.

۲- توجه به عبارت https : در صورتی که به درگاه بانکی هدایت شدید، قبل از اینکه شماره کارتتان را وارد کنید در قسمت آدرس‌بار از اعتبار دستگاه مطمئن شوید. یک درگاه مطمئن باید دارای عبارت https باشد.

۳- نمایش قفل: در کنار https در قسمت آدرس‌بار باید یک قفل وجود داشته باشد که علامت تایید کننده سرویس‌دهنده است.

٤- به استوری‌های سلبریتی‌ها شک کنید: عاقبت برخی از تبلیغات سلبریتی‌ها و میکروسلبریتی‌ها معمولا به صفحات تقلبی بانکی می‌رسد. این استوری‌ها معمولا با ویدیوهایی مثل «تخفیف‌های باورنکردنی و قیمت‌های غیرقابل باور» فقط برای فریب دادن افراد طراحی شده‌اند.

٥- توجه به کد امنیتی: معمولا در صفحات فیشینگ این کد امنیتی یک عکس ثابت است که با رفرش کردن صفحه تغییری نمی‌کند.

٦- یک بار اطلاعات غلط وارد کنید: یکی از اطلاعات کارت بانکی‌تان را اشتباه وارد کنید. اگر پیغام خطایی در صفحه کامپیوتر دریافت کردید یعنی به احتمال زیاد این صفحه جعلی نیست.

۷- چک کردن دامنه سایت: در سایت enamad.ir با کلیک و سرچ کردن صفحه بانکی که در آن قرار داریم به ما اعلام می‌شود که در حال استفاده از سایت جعلی هستیم یا نه.

۸- افزونه ضد فیشینگ: یک افزونه یا اکستنشن ضد فیشینگ در سیستم خود نصب کنید که با وارد شدن در سایت مورد نظر به شما اعلام کند این صفحه از امنیت کافی برخوردار است یا نه.

۹- یک کارت بانکی برای خرید آنلاین داشته باشید: یک کارت خالی صرفا برای خرید کردن داشته باشید تا هنگام خرید به اندازه نیازتان ابتدا پول را به آن منتقل کنید.

۱۰- اگر تصمیم دارید تلفن همراه خود را بفروشید حتما تمام اطلاعات موجود در آن را پیش از فروش پاک کنید.

۱۱- سعی کنید دوستان و اعضای خانواده خود را از نکات امنیتی و کلاهبرداری‌های اینترنتی آگاه کنید زیرا در اغلب موارد نداشتن اطلاعات کافی در این زمینه موجب بروز کلاهبرداری می‌شود.

۱۲- اجازه ندهید هر کسی به سیستم شخصی مورد استفاده فلش متصل نماید.