نکات امنیتی ویژه استفاده از درگاه‌های پرداخت اینترنتی

[ad_1]

به گزارش خبرنگار روابط عمومی گروه تجاری ققنوس، توسعه اکوسیستم تجارت الکترونیک و پیدایش کسب و کارهای جدید در قالب کسب و کارهای اینترنتی و ارائه خدماتی در بستر معاملات نیاز به خرید اینترنتی و استفاده از درگاه‌های پرداخت اینترنتی را افزایش داده است و بر همین اساس این درگاه ها از حدود ۱۰ سال گذشته تا به امروز مورد توجه کلاهبرداران سایبری بوده و آن‌ها توانستند با روش فیشینگ و جعل درگاه‌های پرداخت و سرقت اطلاعات کارت بانکی کاربران مخاطرات زیادی را در بستر تراکنش‌های اینترنتی ایجاد کنند.

از سویی دیگر، توجه به نکات امنیتی درگاه‌های پرداخت اینترنتی می‌تواند کاربران را از کلاهبرداری فیشینگ در امان نگاه دارد و تراکنش‌های بانکی در این بستر به صورت امن و بدون خطر انجام بپذیرد.

اصول مهم امنیتی استفاده از درگاه های پرداخت اینترنتی

از مهمترین نکات امنیتی که کاربران در هنگام ورود به درگاه‌های پرداخت اینترنتی باید به آن توجه کنند، آدرس صفحه در نوار URL مرورگر اینترنتی است؛ در این نوار ابتدا باید صفحه با کلمه https آغاز شود و صرفا کلمه shaparak.ir (دات شاپرک دات آی آر) به پایان می‌رسد و در صورت هر گونه مغایرت در این عبارت از جمله کلماتی مانند «shaaparak.ir و «shaparakk.ir شما وارد صفحه‌ی درگاه پرداخت اینترنتی تقلبی شده‌اید که توسط کلاهبرداران سایبری و فیشرها به منظور سرقت پول و اطلاعات کارت بانکی کاربران ساخته شده است؛ در واقع کاربران صرفا باید به درگاه‌هایی با شکل آدرس است توجه کنند که به جای مقدار xxx حتما باید نام یکی از psp ها (شرکت های پرداخت الکترونیک) مطرح درج شده باشد.

آدرس درگاه‌های پرداخت مجاز

بر اساس این گزارش، درگاه های پرداخت مجاز شامل «آسان پرداخت پرشین» به آدرس https://asan.shaparak.ir، به پرداخت ملت

https://bpm.shaparak.ir، تجارت الکترونیک پارسیان
https://pec.shaparak.ir، تجارت الکترونیک پارسیان
https://pecco.shaparak.ir، پرداخت الکترونیک سامان
https://sep.shaparak.ir، پرداخت الکترونیک سامان
https://sep۲.shaparak.ir، پرداخت الکترونیک پاسارگاد
https://pep.shaparak.ir، پرداخت نوین آرین
https://pna.shaparak.ir، پرداخت الکترونیک سداد
https://sadad.shaparak.ir، کارت اعتباری ایران کیش
https://ikc.shaparak.ir، فن‌آوا کارت
https://fanava.shaparak.ir، فن‌آوا کارت
https://fcp.shaparak.ir، مبنا کارت آریا
https://mabna.shaparak.ir، الکترونیک کارت دماوند
https://ecd.shaparak.ir، سایان کارت https://sayan.shaparak.ir
هستند.

نکات مهم جلوگیری از کلاهبرداری و فیشنگ

یکی از راه‌های بسیار آسان و مهم برای جلوگیری از کلاهبرداری و فیشنگ از کاربران در فضای سایبری خودداری از وارد کردن اطلاعات کارت در شبکه‌های اجتماعی، ربات‌ها، پیام رسان‌ها، اپلیکیشن‌های غیر معتبر و سامانه‌های پیامکی است.

از راه‌های شناسایی در گاه‌های پرداخت جعلی رفرش کردن صفحه اینترنتی درگاه پرداخت و عدم تغییر وضعیت کیبورد موجود در صفحه به عنوان کیبورد امن و کد امنیتی است که نشان از صفحه جعلی و طراحی شده برای فیشینگ دارد.

اغلب مرورگرهای اینترنتی در کنار آدرس درگاه‌های مجاز و معتبر اینترنتی دارای مجوز بانک مرکزی و شرکت شاپرک تصویر زیر را دارند:

عدم نمایش تصویر قفل، یا نمایش قفل به رنگ قرمز یا با خط قرمز، یا پیغام خطا با مضمون خطای امنیتی و خطای SSL هنگام بارگزاری صفحه درگاه پرداخت، از نشانه های درگاه‌های غیرمجاز و ناامن است.

[ad_2]