

بخش اول: کلاهبرداری اینترنتی و فیشینگ (سرقت اطلاعات مالی)

۱. پیامک‌های حاوی لینک با عناوین «سامانه ثنا»، «سهام عدالت» یا «یارانه»، شگرد کلاهبرداران است؛ هرگز روی آن‌ها کلیک نکنید.
۲. بانک‌ها هیچ‌گاه از طریق تماس یا پیامک «رمز پویا» یا «اطلاعات کارت» شما را مطالبه نمی‌کنند؛ اطلاعات محرمانه خود را افشا نکنید.
۳. پیش از هر پرداخت اینترنتی، از صحت آدرس درگاه شاپرک (`shaparak.ir`) و نماد اعتماد الکترونیکی (اینماد) اطمینان حاصل کنید.
۴. پیام‌ها و تماس‌های «شما برنده شده‌اید»، ترفند کلاهبرداران برای ترغیب به انتقال وجه است؛ فریب نخورید.
۵. در صورت دریافت درخواست فوری پول از حساب دوستان، پیش از واریز حتماً تلفنی با آن‌ها گفتگو کنید؛ حسابشان ممکن است هک شده باشد.
۶. در خریدهای اینترنتی، تا زمان دریافت و بررسی کالا، از پرداخت هرگونه وجه تحت عنوان «بیعانه» خودداری فرمایید.
۷. وعده‌های سودهای نجومی و تضمینی در فضای مجازی و بازار ارز دیجیتال، دامی برای غارت سرمایه شماست.
۸. نرم‌افزارهای بانکی را صرفاً از وبسایت رسمی بانک‌ها بارگیری (دانلود) کنید؛ بدافزارها در کمین موجودی شما هستند.

بخش دوم: اسکیم (کپی‌برداری از کارت‌های بانکی)

۹. هنگام خرید، کارت بانکی را شخصاً در دستگاه کارت‌خوان بکشید و رمز را خودتان وارد نمایید.
۱۰. اعلام بلند رمز کارت در فروشگاه‌ها، نقض امنیت مالی شماست؛ از این رفتار پرخطر پرهیز کنید.

بخش سوم: هتک حیثیت، حریم خصوصی و جرایم سایبری

۱۱. طبق قانون جرایم رایانه‌ای، انتشار تصاویر، ویدیوها یا اسرار خصوصی دیگران در فضای مجازی، مجازات حبس و جزای نقدی دارد.
۱۲. توهین و هتک حیثیت در فضای مجازی علاوه بر پیگرد قانونی، آسیب‌های شدید و جبران‌ناپذیر روانی برای قربانی به همراه دارد.
۱۳. بازنشر پیام‌های توهین‌آمیز و شایعات بی‌اساس، مشارکت در چرخه تخریب روانی جامعه است؛ از بازنشر آن‌ها خودداری کنید.
۱۴. ساخت حساب کاربری با نام و تصویر دیگران، مصداق جعل رایانه‌ای و جرم دارای مجازات است.

۱۵. مراقب اشتراک‌گذاری عکس‌ها و داده‌های شخصی باشید؛ سوءاستفاده‌کنندگان سایبری از این محتواها برای اخاذی و تهدید استفاده می‌کنند.

بخش چهارم: مسئولیت‌های کیفری و راه‌های ارتباطی*

۱۶. اجاره دادن کارت، حساب بانکی یا درگاه پرداخت، شراکت در جرم کلاهبرداری و پول‌شویی است و عواقب کیفری دارد.
۱۷. سیم‌کارت‌های به نام خود را مدیریت کنید؛ مسئولیت هرگونه سوءاستفاده از سیم‌کارت ثبت‌شده متوجه مالک آن است.
۱۸. قابلیت «تأیید دومرحله‌ای» را در تمامی شبکه‌های اجتماعی و پیام‌رسان‌های خود فعال نمایید تا مانع دسترسی غیرمجاز شوید.
۱۹. اگر قربانی کلاهبرداری اینترنتی شدید، بلافاصله از طریق همراه بانک یا تماس با بانک، کارت خود را مسدود کنید.
۲۰. مرکز فوریت‌های سایبری پلیس فتا به شماره ۰۹۶۳۸۰ به صورت ۲۴ ساعته آماده دریافت گزارش‌ها و راهنمایی شماست.