۱. شبکه های اجتماعی

۱۰ نکته امنیتی شبکه های اجتماعی

احتمال موفقیت مجرمان سایبری در شبکه های اجتماعی با توجه به گستردگی مخاطبان و این که افراد هر چیزی را فکر می کنند از سوی دوستانشان ارسال شده است و بر روی آن کلیک می کنند، بالاتر است.

با این شرایط چگونه باید از خود در شبکه های اجتماعی حفاظت کنیم؟ موارد زیر در این می تواند بسیار موثر باشد:

۱. .محدودیت انتشار اطلاعات شخصی

در مورد میزان اطلاعات شخصی که در شبکه های اجتماعی ارائه می دهید، مراقب و محتاط باشید. یک راه معمول مجرمان سایبری برای نفوذ به حساب کاربری شما بوسیله کلیک کردن بر روی لینک "رمز عبور خود را فراموش کرده اید؟" می باشد. با پاسخ به سوال امنیتی می تواند به درون حساب کاربری راه یابد. مجرمان سایبری سعی می کنند پاسخ این سوالات را در پروفایل شخصی و یا در پُست هایی که فرد در صفحه شبکه اجتماعی قرار می دهد، پیدا کنند. در نتیجه اگر شما اطلاعات بیشتری را در پروفایل و یا صفحه خود ارائه کرده باشید کار را برای هکر جهت پیدا کردن جواب سوال های امنیتی و نفوذ به حساب کاربری راحت تر کرده اید.

اگر شبکه های اجتماعی به شما اجازه می دهند که خودتان سوال های امنیتی را ایجاد کنید، سوال هایی مطرح کنید که مطمئن هستید جواب آن ها با یک جستجوی سریع در اینترنت بدست نمی آید.

۲. رعایت احتیاط در مورد کلیک کردن بر روی لینک ها

حتی اگر لینک در پیامی است که از سوی دوست شما فرستاده شده است در هنگام کلیک کردن بر روی آن با احتیاط باشید. به این علت که ممکن است اطلاعات حساب کاربری دوست شما سرقت شده باشد و با استفاده از آن در حال ارسال لینک های مخرب به لیست تماس های او باشند.

۳. در مورد شخصی که به عنوان دوست در شبکه های اجتماعی او را قبول می کنید، بیشتر دقت کنید.

ممکن است سارقان هویت به منظور دریافت اطلاعات شما، پروفایل های جعلی ایجاد کنند. افراد همیشه آن چیزی که می گویند، نیستند.

۴.آدرس سایت شبکه اجتماعی را خودتان به طور مستقیم در مرورگرتایپ نمایید.

اگر شما بر روی لینکی کلیک کنید که شما را به سمت وب سایت شبکه های اجتماعی از طریق یک ایمیل یا دیگر وب سایت ها هدایت کند. ممکن است در حقیقت آن یک مورد فیشینگ باشد که سایت اصلی را جعل کرده است و کاملا شبیه به سایت اصلی به منظور فریب کاربران طراحی شده است تا کلمات عبور و رمز آن ها را بدست آورد.این مسئله نه تنها در مورد شبکه های اجتماعی صدق می کند، بلکه در موارد دیگر نیز باید با احتیاط بود.

۵.مراقب برنامه های جانبی که در شبکه های اجتماعی نصب می کنید، باشید.

بسیاری از سایت های شبکه های اجتماعی به شما اجازه دانلود برنامه های جانبی را می دهند که شما می توانید از طریق آن ها کارهای بیشتری را در صفحات شخصی خود انجام دهید. با این حال، مجرمان سایبری می توانند از این برنامه های جانبی برای سرقت اطلاعات افراد استفاده کنند بدون آن که فرد متوجه شود.

۶. هر آنچه که شما ارسال می کنید دائمی است.

این را بدانید که هر اطلاعاتی که شما در شبکه های اجتماعی ارسال می کنید دائمی است. قبل از آن که هر مطلبی را ارسال کنید به خوبی در مورد آن فکر کنید.

۷.تنظیمات حریم خصوصی

از تنظیمات حریم خصوصی به منظور این که، بتوانید کنترل کنید چه کسانی اطلاعات شخصی شما را مشاهده می نمایند استفاده کنید.

سیاست های حریم خصوصی سایت و شبکه اجتماعی را که از آن استفاده می کنید، مطالعه نمایید و بدانید که آن شبکه اجتماعی از اطلاعات شما چه استفاده هایی می کند.

۸. .هرگز از رمز های یکسان برای چند حساب کاربری استفاده نکنید.

این مسئله فقط مربوط به شبکه های اجتماعی نیست، بلکه برای تمامی حساب ها باید این امر رعایت شود. رعایت این مسئله باعث می شود، در صورتی که به یکی از حساب های شما نفوذ شود،حساب دیگر در معرض خطر قرار نگیرد .

۹.اجازه ندهید سایت شبکه اجتماعی دفترچه آدرس ایمیل شما را اسکن کند.

هنگامی که شما حساب کاربری خود را ایجاد می کنید، ممکن است از شما سوال شود که آیا می خواهید "دوستان خود را پیدا کنید" با ارائه آدرس ایمیل خود، سایت می تواند دفترچه آدرس ایمیل شما را به منظور پیدا کردن دوستان شما اگر در شبکه اجتماعی باشند برسی و اسکن کند. همچنین سایت از این اطلاعات استفاده می کند و اطلاعات را برای تمام افراد لیست تماس می فرستد.

۱۰. استفاده از شبکه های اجتماعی در محل کار، توصیه نمیشود.

دسترسی به سایت های شبکه های اجتماعی در محل کار از طریق سیستم ها و کامپیوترهای محل کار شما را با ریسک حملات ویروسی مواجه می کند. برای مثال، با باز کردن پیوست یک ایمیل و یا با کلیک کردن بر روی لینک دانلود یک برنامه، کامپیوتر محل کار شما می تواند آلوده به بد افزارها و برنامه های مخرب شود و اطلاعات مورد سرقت قرار گیرد

۲. کودکان و شبکه های اجتماعی

۱۰ راهکار برای آنکه از کودکان تان محافظت کنید

۱ .مراقب باشید کودکان کم سن بدون نظارت از شبکه های اجتماعی استفاده نکنند.
۲ .تنظیمات امنیت و حریم خصوصی دستگاههای قابل اتصال و همراه را به طور مرتب بررسی کنید.
۳ .تنظیمات حریم خصوصی حسابهای کاربری را به صورت مداوم بررسی کنید.
۴ .از نرم افزارهای فیلترینگ و مانیتورینگ استفاده کنید.
۵ .برای استفاده از شبکه های اجتماعی و دستگاههای متصل، قانون بگذارید.
۶ .سعی کنید عادتهای کودکان و نوجوانان خود را بشناسید.
۷ .الگوی مناسبی برای کودکانتان باشید.
۸ .سعی کنید در مورد فناوریهای جدید به روز باشید.
۹ .مراقب تصاویر و مطالبی که کودکانتان در شبکه های اجتماعی ارسال می کنند باشید.
۱۰ .اتصال به اینترنت برای کودکان در اتاق خصوصی ممنوع!

۳. کلاهبرداری تلفنی با شگرد شما برنده شدید

مراقب باشید: کلاهبرداری تلفنی با شگرد «شما برنده شده‌اید»

تلفن همراه، اس‌ام‌اس و عابربانک سه ضلع اصلی کلاهبرداری‌های تلفنی است. شیادانی که با سوءاستفاده از ناآگاهی مردم خیلی راحت حساب‌های بانکی آنها را به بهانه‌های مختلف خالی می‌کنند. برنده خوش‌شانس مسابقات رادیویی و تلویزیونی، برنده شدن سفر زیارتی به اماکن مقدس، برنده شدن در قرعه‌کشی بانک‌ها و موسسات مالی مواردی است که کلاهبرداران تلفنی برای فریب مال باختگان از آن استفاده می‌کنند. این شیادان به قدری حرفه‌ای عمل می‌کنند که اقشار مطلع و تحصیلکرده جامعه هم به راحتی فریب می‌دهند.

اما کلاهبرداری‌های تلفنی با ورود تلفن همراه، گسترش عابربانک‌ها و سیستم‌های بانکداری الکترونیکی رنگ بوی جدی‌تری به خود گرفت. در بیشتر موارد این کلاهبرداران با جعل عنوانی فریبنده، از طریق تلفن همراه و پیامک با مالباختگان ارتباط برقرار می‌کنند و پس از جلب اعتماد، با استفاده از شگردهای روحی و روانی خاصی با تحت‌تأثیر

قراردادن فرد مورد نظر آنها را روانه عابربانک‌ها می‌کنند و پس از اجرای عملیاتی پیچیده از پشت تلفن حساب بانکی آن را خالی می‌کنند. تقریبا این شگرد همه کلاهبرداران تلفنی است. کلاهبرداری‌هایی که به نظر می‌رسد با وجود هشدارهای مکرر مقامات انتظامی و سیستم بانکی کشور درخصوص حفظ و حراست از حساب‌های بانکی همچنان در صدر روش‌های کلاهبرداری قرار دارد.

۱۰۰میلیون تومان کلاهبرداری از طریق تلفن همراه

کلاهبرداران تلفنی همواره با استفاده از فضای حاکم برجامعه سعی درفریب مالباختگان دارند. موضوعی که سعید احمدبیگی بازپرس کشیک دادسرای تهران هم به آن اشاره دارد. او درخصوص شگرد جدید کلاهبرداران تلفنی طی روزهای اخیر در تهران به «شهروند» می‌گوید: «اخیراً کلاهبرداری از طریق عابربانک زیاد شده است. این کلاهبرداران با سوءاستفاده از نزدیک‌شدن به ماه محرم و مراسم اربعین، تلفنی با مردم تماس می‌گیرند و به بهانه‌های مختلف حساب‌های بانکی آنها را خالی می‌کنند. فقط درچند ساعت حضور من به‌عنوان بازپرس کشیک چهار کلاهبرداری به شعبه من ارجاع شد. دریکی از همین پرونده‌ها ۱۰۰میلیون تومان و ۳ مورد دیگر به ترتیب ۴۲، ۲۸ و ۹میلیون تومان از این طریق کلاهبرداری شده بود.» او با اشاره به اظهارات این مالباختگان می‌گوید: «پسرجوانی ۱۰۰میلیون تومان پول پدرش را به این طریق از دست داده بود. این پسرجوان به من می‌گفت، نمی‌دانم چطور به پدرم بگویم این اتفاق افتاده. این پول همه سرمایه زندگی‌اش بود.»

احمد بیگی ادامه می‌دهد: «دیروز صبح بازپرس کشیک دادسرای ناحیه ۵ بودم که مرد مالباخته‌ای با مراجعه به دادسرا مدعی شد که ۴۲میلیون تومان پولش را از دست داده است. او در اظهاراتش به من گفت: پنجشنبه عصر وقتی به منزل رسیدم، تلفن همراهم زنگ خورد از پشت تلفن به من گفتند که از رادیوی جوان تماس می‌گیریم و شهردار تهران آقای قالیباف هم صدای شما را می‌شنوند، من هم رفتم عابربانک و ۴۲میلیون تومان پاداش ۲۰ سال کارکردنم را به حساب این مرد کلاهبردار واریز کردم.» اما این شیادان از شگردهای نوین و متفاوتی برای کلاهبرداری و خالی کردن حساب مالباختگان استفاده می‌کنند.

بازپرس کشیک تهران درتوضیح شگردهای این کلاهبرداران می‌گوید: « این شیادان به بهانه‌های مختلفی تماس می‌گیرند و با سوءاستفاده از عنوانی چون حضور مقامات دولتی و رسمی در این برنامه‌ها به مالباختگان می‌گویند، شما برنده خوش‌شانس کمک هزینه سفر به کربلای معلی و دیگر اماکن مقدس شده‌اید. این شیادان با استفاده از این روش مردم را به سمت عابربانک‌ها می‌کشانند.» او ادامه می‌دهد: « این کلاهبرداران پس از جلب اعتماد فرد مورد نظر و هدایت آنها به سمت عابربانک، از طریق تلفن از آنها می‌خواهند که یک‌سری عملیات را انجام دهند و مالباختگان فریب‌خورده ناخواسته موجودی حساب خود را به حساب دیگری منتقل می‌کنند. »

سعید احمد بیگی بازپرس کشیک دادسرای تهران با هشدار نسبت به شگرد جدید کلاهبرداری‌های تلفنی با توجه به نزدیکی ایام محرم و مراسم اربعین تأکید می‌کند: « هیچ پرداخت جایزه‌ای نیاز به رفتن پای عابربانک ندارد. مردم آگاه باشند که اگر فرد ناشناسی از پشت تلفن خواست که به عابربانک بروید، قطعا کلاهبرداری است .»

کلاهبرداران تلفنی

افزایش اطلاعات و پیشرفت فناوری همواره یکی از بزرگ‌ترین وسایل آرامش و آسایش زندگی بشر را رقم زده است .

فناوری‌های پیشرفته روز به روز انسان‌ها را به خود وابسته‌تر کرده و فراگیر شده است تا جایی که بین غنی و فقیر تفاوتی نمی‌بینند و خود را بی‌ادعا در اختیار همه قرار می‌دهد.

همین موضوع باعث می‌شود بسیاری از مجرمان نیز با استفاده از فناوری‌های در دسترس و اضافه کردن کمی چاشنی خلاقیت بتوانند بسیار راحت‌تر از گذشته کلاهبرداری کنند و به مقصود خود برسند.

کلاهبرداری از اطلاعات موجود در فضای پیشرفته ارتباطات انواع مختلفی دارد که یکی از راحت‌ترین کلاهبرداری‌ها، طعمه قرار دادن مردم با استفاده از تلفن است که امروزه بسیار هم رایج شده است.

به دلیل همین رواج و اهمیت کلاهبرداری‌های تلفنی، مستند شوک یکی از برنامه‌های خود را به این نوع کلاهبرداری اختصاص داده که در ادامه قسمت‌هایی از آن را می‌خوانید.

طعمه‌ها چطور شکار می‌شوند؟

در جرایم و کلاهبرداری‌های اینترنتی طعمه‌ها با دلایل مختلف به دام می‌افتند، اما نحوه کلاهبرداری از آنها در نهایت به یک شکل صورت می‌گیرد.

به عنوان مثال در برنامه شوک با عنوان کلاهبرداران تلفنی، افراد به دلایل مختلفی به کلاهبردار اعتماد کرده بودند. یکی از مالباختگان رستوران دار بود و کلاهبردار ضمن تماس با او و ثبت سفارش‌های مختلف به بهانه این که از یک ارگان دولتی تماس گرفته و پول مورد نظر را به صورت حواله به رستوران دار خواهد داد، او را پای عابر بانک کشاند و با دادن اطلاعات اشتباه از او خواست تا کدهای مختلفی را وارد کند، رستوران دار پس از مدت کوتاهی متوجه شد که با کارهایی که انجام داده نه‌تنها پولی به حسابش واریز نشده، بلکه همه موجودی حسابش به کارت دیگری منتقل شده است. مالباخته دیگر نیز به بهانه برنده شدن در برنامه رادیویی و گرفتن مبلغ جایزه، مقابل عابر بانک رفت. وی درباره نحوه اعتمادش به کلاهبردار گفت: زمانی که با من تماس گرفت، اسم و فامیلم را کامل گفت و حتی می‌دانست که چه زمانی و در کدام برنامه رادیویی شرکت کرده و چه چیزهایی گفته‌ام. همه اینها باعث شد به او اعتماد کنم و باور کردم که در این برنامه یک سفر حج برنده شده‌ام.

وی همچنین ادامه داد: همه چیز خیلی طبیعی بود. هم صدای کسی که با من صحبت می‌کرد شبیه صدای گویندگان رادیو بود و هم می‌گفت که چند کارشناس هم در آنجا حضور دارند و من صدایشان را می‌شنیدم. در هر صورت من همه چیز را باور کردم و زمانی که گفت همراه همسرم یک سفر حج برنده شده‌ام، بسیار خوشحال شدم. کلاهبردار به من گفت اگر می‌خواهم کمک هزینه سفر را بگیرم باید به اولین عابربانک مراجعه کنم و از آنجا با او تماس بگیرم تا پس از وارد کردن کدهای مورد نظر، پول جایزه به حسابم واریز شود. من هم قبول کردم و بعد از وارد کردن کدها، متوجه شدم هر چه پول در حسابم بود به صورت خودکار خالی شده است.

هشدارهای مهم قضایی ـ پلیسی

مالباختگان زیادی با روش‌های مختلف توسط کلاهبرداران فریب خورده‌اند، اما حساب همگی آنها از یک راه خالی شده است. همه با اعتماد بی‌جا به فردی که نمی‌شناختند به عابر بانک مراجعه کرده و با وارد کردن کدهای مختلف حسابشان خالی شده است.

اولین نکته‌ای که وجود دارد و کارشناسان مختلف آن را بارها گفته‌اند این که بدون شناخت به دیگران اعتماد نکنید چراکه کلاهبرداران زیادی در کمین هستند تا بتوانند از یک لحظه غفلت افراد جامعه، استفاده کنند. دومین نکته نیز این که در صورت برنده شدن جوایز مختلف نیازی نیست فرد برنده برای گرفتن جایزه خود به عابر بانک مراجعه کند. در ادامه نظر کارشناسان برنامه را درباره پرونده‌های کلاهبرداری تلفنی خواهید خواند.

مقابل عابر بانک نروید

احمد فاضلیان، رئیس کل دادگستری استان البرز در این باره می‌گوید: اگر هر کسی به هر دلیلی به شما گفت پای عابر بانک بردید و جایزه بگیرید، مثلا از طرف روابط عمومی اداره زنگ زد یا برای برنده شدن در مسابقه یا... با شما تماس گرفت و گفت شما چیزی را برنده شده‌اید و باید برای گرفتن جایزه بیاید پای عابر بانک، بدانید که در کارش یک عمل مجرمانه‌ای نهفته است. نکته دیگر این که در هیچ کجا شما برای دریافت مبلغ هدیه لازم نیست پولی به جایی واریز کنید. پس اگر افرادی از شما خواستند برای ارتباط با حسابتان مبلغی به جایی واریز کنید تا پول هدیه به حسابتان واریز شود، این کار یقینا کلاهبرداری است و می‌خواهند شما را در دام بیندازند.

کلاهبرداری با اطلاعات خودتان

سردار محمدیان، رئیس پلیس آگاهی تهران بزرگ در این باره هشدار داد: انواع و اقسام کلاهبرداری ها در جامعه انجام می‌شود که یکی از آنها که مدت‌هاست شایع شده و می‌تواند تعداد زیادی قربانی بگیرد، کلاهبرداری‌های تلفنی است. به عنوان مثال استفاده از فضای مجازی و در پی آن، ارتکاب جرم در فضای واقعی، یکی از جرایم ترکیبی و چنگالی است که کلاهبردار در این جرایم از فضای مجازی اطلاعات لازم را درباره طعمه خود کسب کرده و با استفاده از آن اطلاعات فضا را برای اعتماد کردن طعمه فراهم می‌کند و کلاهبرداری به‌راحتی صورت می‌گیرد.

۴. تشخیص کلاهبرداری تلفنی

چگونه کلاهبرداری تلفنی را تشخیص دهیم

گاهی در برخورد با بعضی از موضوعات تجاری به این فکر می‌کنیم از چه راهی تشخیص دهیم کدام طرح کلاهبرداری است؟ آیا طرح‌های کلاهبرداری و دسیسه‌ها مربوط به آن نشانه‌ای دارد؟ در زیر به برخی از نشانه‌های شناخت یا تشخیص طرح‌های کلاهبرداری اشاره می‌نماییم:

۱- این طرح در ابتدای کار فوق‌العاده جذاب به نظر می‌رسند:

مثلاً می‌گویند:شما برندهٔ جایزه‌ای فوق‌العاده از یک مسابقه شده‌اید، البته شما هیچ‌گاه درآن مسابقه شرکت نکرده‌اید. به شما پیشنهاد می‌دهند در یک موقعیت که در تمام زندگی‌تان فقط یک بار تکرار می‌شود و یک شانس فوق‌العاده برای شما ایجاد می‌نماید و در آن امکان هیچ باخت یا ضرری وجود ندارد شرکت نمایید.

۲-برای دریافت جایزه باید مبلغی پرداخت کنید:

شما برنده شده‌اید، اما باید مبلغی را برای ارسال جایزه، پرداخت مالیات یا دیگر هزینه‌هایی که برای پرداخت جایزه هزینه می‌شود، پرداخت نمایید. حتی برخی اوقات تماس‌گیرنده یک پیک برای دریافت مبلغ از شما می‌فرستد تا مبلغ را از شما بگیرند و برای او ببرند.

۳- از شما می‌خواهند، اطلاعات کاملاً شخصی و محرمانهٔ مالی خود را در اختیارشان قرار دهید:

تماس‌گیرنده از شما می‌خواهد تمام اطلاعات حساب بانکی و یا تمام اطلاعات کارت اعتباری خود را به آن‌ها بدهید. باید بدانید که سیستم‌های تجاری مطمئن و قانونی، هیچ‌گاه نیاز بر جزئیات حساب مالی شما ندارند و حتی اگر قرار باشد پولی یا جایزه‌ای را به شما بدهند، نیاز به رمز عبور کارت شما را ندارند. دادن شمارهٔ حساب یا شمارهٔ کارت کفایت می‌کند.

۴-تماس‌گیرنده بسیار هیجان‌زده‌تر و خوشحال‌تر از شماست:

مثلاً شما برندهٔ دریافت جایزه شده‌اید اما شخص تماس‌گیرنده بسیار هیجان‌زده‌تر و خوشحال‌تر از شماست زیرا کلاهبرداران می‌خواهند شما را هیجان‌زده و ذهن شما را درگیر کنند. قدرت فکر و تصمیم‌گیری عاقلانه را از شما بگیرند.

۵- مدیر تماس می‌گیرد:

شخصی که با شما تماس می‌گیرد ادعا می‌کند از طرف یک دفتر دولتی، مسئول مالیاتی، مرکز رسمی بانکی، یک وکیل یا یک مقام رسمی تماس می‌گیرد. شخص تماس‌گیرنده، در هنگام تماس، نام کوچک شما را به زبان می‌آورد و از شما اطلاعات زیادی در مورد اطلاعات شخصی یا اطلاعات نحوهٔ زندگی شما کسب می‌نماید

۶- شخصی غریبه‌ای که تماس گرفته، سعی می‌کند با شما رابطه صمیمی و دوستانه برقرار کند:

مجرمان می‌خواهند بفهمند که آیا شما تنها هستید و تمایلی به صحبت کردن دارید؟ به محض اینکه فهمیدند، سعی می‌کنند به شما اطمینان دهند که دوست شما هستند، بعد از جلب اطمینان، شما هیچ‌گاه مشکوک نمی‌شوید که چه شخصی که این‌گونه با شما صمیمی است، امکان دارد یک کلاهبردار باشد.

۷- این یک فرصت با مدت زمانی محدود است، اگر عجله نکنید، آن را از دست می‌دهید:

اگر شما تحت فشار قرار گرفتید تا با سرعت یک تصمیم‌گیری در مورد یک خرید بزرگ و گران‌قیمت انجام دهید، یا یک مبلغ زیاد به مؤسسات خیریه پرداخت کنید، مسلماً این یک معاملهٔ قانونی نیست. هر تجارت قانونی یا هر مؤسسه خیریه به شما این فرصت را می‌دهند تا آن‌ها و عملکردشان را بررسی کنید، سپس فکر کنید و بعد تصمیم بگیرید و مبلغ موردنظر را بپردازید.

بعد از آشنایی با این موارد چه‌کارهایی برای محافظت از خود باید انجام دهیم:

- **به هر شکل، مجرمان ممکن است هر چیزی بگویند تا شما را متقاعد کنند که نیاز نیست برای کسب پول، زحمتی بکشند یا کاری انجام دهید.**
- **گاه باشید، شما حق دارید تا در مورد هر شخصی که تلفنی با شما تماس می‌گیرد و به شما پیشنهاد می‌دهد، بررسی‌های لازم را انجام دهید، با نامه‌نگاری از آن‌ها اطلاعات کاری بخواهید، تماس بگیرید، مرجع‌های آن‌ها را استعلام نمایید و زمانی برای فکر کردن و تصمیم‌گیری در مورد پیشنهاد آن‌ها داشته باشید.**

•تمامی افرادی که به‌طور قانونی و به دور از هرگونه دسیسه و کلاهبرداری به‌صورت تلفنی بازاریابی انجام می‌دهند از اینکه اطلاعات فعالیت معقول و منطقی خود را در اختیار شما قرار دهند، خوشحال می‌شوند. همیشه در مورد دادن اطاعات خاص و شخصی خود مخصوصاً اطلاعات حساب بانکی یا کارت‌بانکی خود به دیگران مراقب باشید.

•در آخر هر جایی که احساس کردید مورد متناقضی وجود دارد، یا هرگاه به فرد تماس‌گیرنده شک کردید، بهترین را این است که این تماس قطع کنید. این کار بسیار هوشمندانه است و به هیچ وجه بی‌احترامی محسوب نمی‌شود. همیشه با افراد مورد اطمینان خود، اقوام و پلیس مشورت کنید و از آن‌ها دربارهٔ این موارد پرس‌وجو و تحقیق نمایید. اما فراموش نکنید با قطع کردن تماس می‌توانید از یک کلاهبرداری تلفنی جلوگیری نمایید.

۵. کلاهبرداری تلفنی و کارت به کارت

ترفندهای کلاهبرداری تلفنی و کارت به کارت را می‌شناسید؟

معاون اجتماعی پلیس آگاهی ناجا پنج خطای مطرح مالباختگان در کلاهبرداری تلفنی و کارت به کارت را تشریح کرد. سرهنگ اندرز چمنی در گفت‌وگو با خبرنگار«حوادث» خبرگزاری دانشجویان ایران)ایسنا)، با بیان اینکه عده‌ای کلاهبردار حرفه‌ای با استفاده از تلفن‌های اعتباری همراه با اقشارمختلف ارتباط تلفنی برقرارکرده و در قالب دریافت خدمات، سفارش انجام کار و تعلق جایزه مبادرت به کلاهبرداری از نوع «کارت به کارت» می‌کنند، گفت: در میان اقشار و حرفه‌های مختلف ممکن است که این شیوه کلاهبرداری رخ دهد اما یکی از ایده‌آل‌ترین گروه‌های هدف برای تحقق اهداف مجرمانه، افراد و گروه‌های فعال در حرفه پزشکی هستند.

وی با بیان اینکه در این شیوه، کلاهبرداران با بهانه‌هایی همچون خرید و فروش کالا، اقدام به مذاکره اولیه با فرد می‌کنند که از خطای اول فرد برای توافق با فرد ناشناس استفاده کرده و شماره حساب بانکی فرد را مطالبه می‌کنند تا مبلغی به عنوان پیش پرداخت یا مبلغ کامل جایزه به حساب فرد واریز شود، گفت: در این مرحله مالباخته خطای دوم خود که همان واگذاری شماره حساب بانکی به فرد نادیده و ناشناس است را مرتکب می‌شود و بعد از آن و پیرو همان مذاکره معطوف به درآمدزایی، مجدد با مالباخته در تماس تلفنی اعلام می‌شود که با وجود چندین مرحله تلاش، واریز وجه به حساب وی انجام نشده است.

معاون اجتماعی پلیس آگاهی ناجا با بیان اینکه معمولا افراد کلاهبردار ادبیاتی کاملا جذاب و بر محور درآمدزایی دارند که موجب وسوسه‌شدن مالباخته می‌شود، گفت: بعد از آن و در سومین گام از فرد درخواست می‌شود که برای چک‌کردن واریز وجه به حساب وی به نزدیک‌ترین دستگاه عابربانک مراجعه کند که در اینجا خطای سوم مالباخته که همان مراجعه به دستگاه عابربانک برای واریز وجه به حسابش است، رخ می‌دهد که این در حالی است که مطلقا در فرآیند عملیات صحیح بانکی، گزینه‌ای مربوط به واریز وجه قرار ندارد.

اندرزچمنی با بیان اینکه بعد از مراجعه مالباخته به دستگاه عابربانک، از فرد درخواست می‌شود برای واریز وجه، کارت خود را وارد دستگاه کند، گفت: در این مرحله خطای چهارم مالباخته که واردکردن کارت به دستگاه عابربانک است، انجام می‌گیرد چرا که مطلقا در عملیات صحیح بانکی، برای واریز وجه نباید این حرکت را انجام داد. معاون اجتماعی پلیس آگاهی ناجا با بیان اینکه بعد از آن کلاهبرداران با طرح ادعاهای مختلف شامل تسلط بر سیستم‌های نرم‌افزاری بانک، آشنایی با کارمندان شبکه بانکی و دریافت کدهای مخصوص و ... از فرد می‌خواهند تا برای رفع مانعی ایجاد شده در واریزوجه به حساب بانکی‌اش در صفحه نمایشگر دستگاه عابربانک از دکمه‌های مشخص استفاده کرده و آنها را فشار دهد، گفت: خطای پنجم در این مقطع توسط مالباخته صورت می‌گیرد، چرا که اجابت دستور فرد ناشناس در انجام عملیات روی دکمه‌های صفحه نمایشگر دستگاه عابربانک، عملی نیست که مالباخته بخواهد این مسئله را انجام دهد.

وی با بیان اینکه کلاهبرداران در این شیوه از مالباخته می‌خواهند که عمدتا زبان صفحه نمایشگر را از فارسی به لاتین تغییر دهند، گفت: بعد از تبدیل زبان صفحه نمایشگر به لاتین، پروسه فشاردادن سایر دکمه‌ها که معمولا در قالب یک عدد چند رقمی است، منجر به تخلیه حداکثری موجودی کارت مالباخته و واریز همزمان به کارت فرد ناشناس در حال تماس می‌شود.

اندرز چمنی با بیان اینکه کلاهبرداران حرفه‌ای فعال در این فرآیند مجرمانه معمولا از تلفن‌ها و کارت‌های بانکی فاقد هویت واقعی استفاده می‌کنند، گفت: با انجام ندادن پنج خطای مطرح در این روش و مکالمه، به قربانی جرم در کلاهبرداری‌های تلفنی و کارت به کارت تبدیل نشوند .

۶. کلاهبرداری پیامکی

کلاهبرداری پیامکی

یکی از جرائمی که امروزه در فضای مجازی باب شده و مبالغ بسیاری از هموطنان عزیز کلاهبرداری شده، از طریق ارسال پیامک صورت گرفته، پیامک هایی که جعلی بوده و با متنی بسیار جذاب و اغوا کننده طراحی می شوند و در غالب طرح های مختلف که همگی با استفاده از شیوه های مختلف مهندسی اجتماعی و در ایام و مناسبت های خاص به صورت انبوه برای هموطنان ارسال می شود.

رئیس مرکز تشخیص و پیشگیری پلیس فضای تولید و تبادل اطلاعات ناجا با بیان مطلب فوق گفت: برخی از افراد سودجو و فرصت طلب در موقعیت، شرایط و مناسبت هایی که بتوانند عواطف و احساسات مردم را تحت تأثیر قرار دهند و از طریق سامانه های مختلف اقدام به ارسال پیامک هایی با عناوین مرتبط به مشترکان تلفن همراه کرده و آنها را به قید قرعه در جشنواره های مختلف به عنوان برنده اعلام می کنند و از آنها درخواست ارسال اطلاعات شخصی بانکی دارند. متأسفانه برخی از افراد به علت حسن اعتماد بیش از حد در دام این کلاهبرداران گرفتار شده و مبالغی را از دست می دهند.

وی افزود: در یکی از این شگردها به تازگی پیامک هایی برای مشترکان تلفن همراه ارسال شده که آنها را به عنوان یکی از برندگان جشنواره طرح هزاران لبخند همراه اول معرفی کرده. نمونه متن ارسالی به شرح زیر می باشد:

"مشترک گرامی شما برنده مبلغ ۳/۰۰۰/۰۰۰ ریال در طرح هزاران لبخند همراه اول شده اید. لطفاً جهت کسب اطلاعات بیشتر از نحوه دریافت با شماه ***** تماس حاصل فرمایید".

که پس از برقراری تماس از وی خواسته می شود مشخصات خود را از قبیل نام و نام خانوادگی و شماره ملی و ... را برای آنها ارسال نماید. بعد از ارسال مشخصات پیامکی مبنی بر صحت اطلاعات ارسالی و همسان بودن با اطلاعات فرد برنده برای او ارسال می شود و از وی خواسته می شود جهت واریز مبلغ، شماره حساب، شماره کارت، رمز دوم و دیگر مشخصات بانکی را برای آنها ارسال نماید. در این مرحله است که کلاهبرداری صورت می گیرد. در این زمینه پلیس فتا مکاتباتی با اپراتورهای تلفن همراه انجام داده است که طی آنها مشخص شده این اپراتورها برندگان خود را فقط از طریق سایت اعلام نمایند. در این راستا اپراتورها پیامک هایی را در مورد چگونگی و نحوه اعلام برندگان برای تمامی کاربران ارسال کرده اند. لذا به تمامی هموطنان عزیز توصیه می شود هرگز برای دریافت وجه نیازی به ارسال اطلاعات حساب بانکی نمی باشد.

در نهایت پلیس فتا از هموطنان درخواست می کند در صورت مواجه با موارد مشکوک آن را از طریق سایت پلیس فتا به آدرس Cyberpolice.ir بخش تماس با ما گزارش نمایند و هشدار های پلیس را جدی بگیرید.

منبع :

پایگاه اطلاع رسانی پلیس فتا