

## کلاهبرداری از طریق شبکه اطلاع رسانی برقی (شارب)



نویسنده: فاتح سامع

شما باید جداً از انتقال پول دیگران از داخل و خارج از طریق حساب بانکی شخصی یا حساب بانکی شرکت خود احتراز کنید، چون این کار غیر قانونی و از جمله ی فعالیت های بازار سیاه شمرده می شود.

امروز از برکت انکشاف فناوری در تمام عرصه های زندگی بشر زمینه دگرگونی های شگرفی رونما شده است.

توسعه خدمات مخابراتی معاملات بانکی دادوستد، خرید و فروش و معاملات بازرگانی را در دورترین نقاط جهان به اسرع وقت ممکن ساخته است. توسعه سریع خدمات شارب (شبکه اطلاع رسانی برقی - Internet)، اجرای معاملات پیچیده و معمول دادوستد را فراهم ساخته، اما چالش ها، کاستی های گزین و احتمالی و مرموزی را در روند اجرای معاملات نیز ایجاد کرده است. تقلب و فریب، خدعه و کلاهبرداری، دغلبازی و دزدی های کوچک و بزرگ در جریان معاملات به انواع گوناگون در طول تاریخ معمول بوده، و به گونه اتفاق افتاده است.



فریبکاری با پیشرفت جوامع بشری و توسعه چشمگیر فناوری اشکال پیچیده به خود گرفته است. در عصر حاضر با گسترش و تعمیم کاربرد از وسایل رایانوی (کامپیوتری) و شارب در معاملات بانکی و تجاری

تقلب و فریبکاری نیز افزایش قابل ملاحظه یافته، و مایه نگرانی مردم و نهاد های ذیربط شده است.

تقلب و چالبازی در حال حاضر بیشتر در معاملات میان افراد شرکت ها و موسسات به طور عمدی و یا مهندسی شده شکل می گیرد. جلوگیری از آن مستلزم آگاهی و هوشیاری لازم و اقدام به موقع می باشد.

هدف از نگارش این مقاله آن است که افراد پیش از آن که شکار دزدهای رایج در فضای شارب شوند، آمادگی کامل داشته باشند، و راه را برای شان با آگاهی تدابیر و اقدام به موقع مسدود و زمینه را محصور سازند.

تقلب کارها بدون استثنا همه مردم را بدون در نظر داشت سن و سال جنس و تبار هدف قرار می دهند تا به گونه مزورانه پول به دست آورند، و بهره ببرند. بنابر آن، افراد مشخص هدف تزویر و خدعه فریبکارها قرار نمی گیرند. تجارب نشان داده است که معمولاً کسانی فریب می خورند که گمان می کنند زرنگ تر از کسانی اند که بخواهند آن ها را فریب بدهند. به طور کلی، فریبکارها از اندیشه ی باطل افراد استفاده می کنند و بنابر دو دلیل موفق هم می شوند. نخست، تقلبکارها از خوش باوری

مردم بهره می برند، و با تبلیغات و حرافی طوری اندیشه های را در ذهن افراد مصور می گردانند که گویا تقاضا و نیاز شان را برآورده می سازند. اما در حقیقت، دامی در کمین گذاشته اند. پس نه باید که معامله مورد نظر بدون بررسی، اندیشه و مشوره ها صورت گیرد. از این لحاظ، نه باید بیشتر از ارزیابی همه جانبه و مشوره لازم در زمینه پیشکش شدن هرگونه خدمات عرضه شده از طریق شارب، با افراد آگاه و مجرب تصمیم نهایی گرفته شود.

دوم، فریبکارها با مهارت و تردستی می خواهند در مدت کوتاه بدون دادن فرصت و مجال تفکر به مشتری معامله را انجام دهند، و مشتری را در برابر یک عمل انجام شده قرار دهند. معلومات محرم مانند شماره حساب بانکی، شماره گذرنامه، شماره جواز رانندگی، تاریخ تولد، نشانی محل کار و بودوباش افراد را به دست می آورند.

تقلبکاران در فضای مجازی با این شیوه به حریم خصوصی اشخاص داخل می شوند. این عمل با زرنگی و پافشاری توأم با ابراز احساس عاطفی، روانی و تامین روابط اجتماعی شکل می گیرد و با سواستفاده سرانجام معامله به فریب و تقلب می انجامد.

برای خودداری و احتمال افتادن به دام متقلب، باید ماهرانه از پاسخ آنی خودداری شود.

### **کدام چیز ها زمینه را برای تقلب کار ها مساعد می سازد.:**

#### **۱. خوش باوری و گمان واهی:**

۱. برخی از افراد گمان می کنند که همه شرکت ها، بنگاه های تجاری، سازمان ها و موسسات قانونی عمل می کنند، و جواز رسمی و قانونی فعالیت دارند، اما در حقیقت چنین نیست، و این باور واهی است. تنها موسسات حمایت از مستهلکین نهادهای اند که در حفظ امنیت مستهلکین از خطر تزویر تقلب کار ها حمایت می کنند، و همواره متوجه هستند که مشتریان را نیرنگ بازها فریب ندهند.

۲. مردم گمان می کنند که همه شبکه های تار نما ها و تارنگارهای برقی یا شارب قانونی اند، و کسی



بدون اجازه نمی تواند خلاف قانون معاملات، خدمات و دادوستد از طریق شارب عمل کند. در حالی که ساختن تارنگار (Website) یا تارنما (Weblog) کار ساده و ارزان است. عرضه کنندگان خدمات تقلبی تارنگار های حرفوی را در خارج از کشوری می سازند که در آن سکونت دارند و از طریق همان تارنگار فعالیت های غیر قانونی خود را انجام می دهند.

### **تارنگارهای کلاهبرداری ( Scam websites )**

۱. تارنگارهای کلاهبرداری طوری ساخته می شود که از لحاظ ساختاری به صورت ساده از تارنگارهای اصلی، رسمی و قانونی تفکیک نمی شوند. تارنگارهای جعلی مانند نهاد قرضه دهنده یا بنگاه تعاونی (Credit Union) برای چند روز محدود فعالیت می کنند. اما گرداننده های چنین بنگاه های تعاونی کلاهبردار پس از فروش اموال و تولیدات تقلبی با بستن آن تارنگارها فرار می کند و دم

به تله نمی دهند، اما آنان اطلاعات محرم مشتریان ساده اندیش شان را، برای سواستفاده در آینده، نزد خود نگه می دارند.

۲. کلاهبرداران گاه از طریق تارنگار های جعلی خویش اسطوره راه کوتاه برای ثروتمند شدن را تبلیغ می کنند، و طوری جلوه می دهند که تنها یک تعداد محدود این راز نهفته و کشف بزرگ را می دانند. اما مشتریان باید از خود سوال کنند که اگر کسی این راه کوتاه را برای ثروتمند شدن می داند پس چرا وقت خود را ضایع می سازد و چه ضرورت دارد که از مردم مزد بگیرد؟

۳. کلاهبرداران حرفوی عرضه کننده خدمات و کالاهای تقلبی از لحاظ روانی مشتریان شان را با چرب زبانی و پیشکش کردن اطلاعات اغواگرآیانه زیر تاثیر می آورند، و حتی برای جذب آنان،



برای شان تحفه های رایگان ارسال می کنند تا در آینده از آنان استفاده ابزاری کنند. پس مشتریان باید عاقلانه عمل کنند و نه باید زیر تاثیر تبلیغات تارنگار های جعلی بروند، چون ارسال تحفه ها و هدایای

ابزاری دامی برای اغفال اذهان آنان است تا از این طریق چنین مشتریان را آماده قربانی شدن در مراحل بعدی روند کلاهبرداری خویش آماده سازند و به کارگیرند.

## **دزدی تارنگار های کلاهبرداری معمول چگونه و با کدام وسایل شکل می گیرد؟**

کلاهبرداری در شارب تا کنون به طرق زیر شکل گرفته است.

### **۱. سرقت هویت (Identity theft):**

یکی از نیرنگ های صاحبان تارنگار های کلاهبرداری و پیشکش کننده خدمات و کالا های تقلبی همانا دسترسی به کارت شناسایی، حساب بانکی (Bank Account)، کارت اعتباری (Credit Card)، جواز رانندگی، است.

### **۲. سرقت رمز حساب بانکی (Bank Account Password Theft):**

کلاهبرداران پس از دستیابی به رمز حساب بانکی مشتریان می توانند پول های آنان را از حساب های بانکی شان بالا کشند.

### **۳. سرقت کیف جیبی و دستیابی به اسناد محرم**

### **(Wallet Theft & Access to Confidential Information):**

یک روش بسیار ماهرانه دستیابی به معلومات محرم توسط کلاهبرداران همانا دستیابی به اطلاعات گزین از میان کاغذهای باطله در زباله دانی ها صورت می گیرد. پیش از باطل ساختن و تصفیة نامه های که دریافت شده باید نام و نشانی محل کار و سکونت و سایر مشخصات از روی پاکت ها محو شود.

از پاسخ به تلفون های ناخواسته اجتناب شود. کلاهبرداران تظاهر می کنند که کارمند بانک، دفتر مالیات، شهرداری و سایر دفاتر دولتی اند و می خواهند در ذهن مخاطبان خویش تشویش ایجاد کنند که در حساب بانکی شان مشکل وجود دارد یا قرضدار دفتر مالیات یا کدام اداره دیگر دولتی هستند و به این منظور از آن افراد برای تشخیص هویت، شماره حساب بانکی و برخی معلومات دیگر را از طریق پیشکش کردن سوال های اغواکننده می به دست آورند. پس هیچگاه اطلاعات خویش را برای هیچ کس از طریق بی سیم یا تلفون ارایه نکنید و باید از ارایه معلومات شخصی به کسانی اجتناب گردد که از طریق بی سیم یا تلفون طالب دریافت چنان اطلاعاتی هستند.

#### **۴. کارت اعتبار جعلی (Credit card scam):**

کلاهبرداران کارت های اعتبار قربانیان جعلکاری های خویش را دزدی می کنند، یا معلومات حساب های بانکی آن را با چال و فریب به دست می آورند تا با استفاده از آن بتوانند حساب های آن قربانیان خویش را خالی کنند

#### **۵. نسخه برداری از کارت بانکی (Bank Card Scamming):**

کلاهبرداران در بانک های خودکار (ATM) دوربین های کوچک را نصب می کنند تا در موقعی انجام معامله بانکی شماره حساب بانکی، کارت اعتبار و رمز آن ها را عکس برداری کنند. پس باید



در موقع کاربرد رمز (Password) حساب بانکی خویش باید دست خود روی صفحه گذاشت تا شماره های رمز توسط آن دوربین ها قابل شناسایی نباشد و امکان عکس برداری از آن شماره میسر نگردد.

کلاهبرداران پس از دستیابی به شماره های حساب بانکی و رمز های کارت های بانک های خودکار، با استفاده از نوار مقناطیسی که در آن مشخصات کارت های مذکور ثبت شده کارت جدید و مشابه می سازند و برای خالی کردن حساب بانکی قربانیان جعل کاری های شان به فعالیت غیر قانونی و تقلبی می پردازند.

#### **۶. انتقال پول برای کس دیگر (Money Transfer for Somebody Else):**

اگر کسی، چه در کشوری شما و چه از یک کشور خارجی، از شما درخواست می کند که پول هایش را از طریق حساب بانکی یا شرکت خویش انتقال دهید، از قبول چنان تقاضای غیر قانونی جداً اجتناب کنید. کسانی هستند که از طرق غیر قانونی و تقلبی پول های هنگفتی را از مدرک فساد، دزدی، قاچاق، رشوت و چپاول دارایی های عامه به دست آورده اند و از طریق ریانامه (Email)، بی سیم یا تلفون از شما تقاضا می کنند که پول ناپاک خود را به حساب بانکی شما انتقال می دهند، و در بدل آن به شما حق العمل (Commission)، انعام یا بخشش پیشنهاد می کنند. این عمل در همه کشور ها جرم قانونی و از جمله فعالیت های پول شویی (Money Laundering) محسوب می گردد. شما باید جداً از انتقال پول دیگران از داخل و خارج از طریق حساب بانکی شخصی یا حساب بانکی

شرکت خود اهتراز کنید، چون این کار غیر قانونی و از جمله ی فعالیت های بازار سیاه شمرده می شود.

### ۷. کار از طریق خانه با پول زیاد و وقت کم (Work from home scam):

امروزه کلاهبرداران از طریق شارب به کاربران فضای مجازی کار تماس می گیرند و به آنان وعده کار از طریق خانه با پول زیاد و وقت کم را پیشکش می کنند. چنین تقلبکارها به شما زنگ می زنند و چنین تبلیغ می کنند که گویا شما می توانید از خانه کار کنید و مزد هنگفت به دست آورید. این کلاهبرداران حتی از شما درخواست می کنند که اشخاص دیگر را برای همکاری با شما برای آنان معرفی کنید و جهت گسترش شبکه همکاران تان مشتری های بیشتری را برای شان معرفی کنید. از قبول همکاری و کار با این فریبکاران باید اجتناب کنید.

### ۸. کلاهبرداری از طریق حراج و پست (Scam Auction & shipping):

به مزایده گذاشتن تولیدات نادرست، غیر قانونی و جعلی از خارج کشور فرمایش ندهید که یا هیچ نمی رسد و یا کاملاً جعلی و خلاف خواست شما ارسال می شود.

### ۹. نرم افزار جاسوسی و کلید وقایع نگار (Spyware & Keylogger):

کلاهبرداران با نصب و کاربرد نرم افزار در رایانه تان پس از دسترسی به خصوصیات و معلومات محرمانه شما را تعقیب می کنند، و به کمک نرم افزار مذکور رمز بانکی و اطلاعات لازم تان را می ربایند، و سپس می توانند پول شما را از حساب های بانکی تان به دست آورند.

### ۱۰. کلاهبرداری پرداخت پول با چک (Cheque over payment scam):

یک روش دیگر کلاهبرداری همانا فرستادن چک از طریق پست در بدل کالای است که فروخته اید. اما فریبکاران به جای درج اصل قیمت کالا در چک مقدار پول بیشتر از مبلغ فروش آن کالا را در چک مذکور درج می کنند، چون آنان مطمئن هستند که شما دوباره آن چک را مسترد می کنید. اما پیش از آن که شما معلومات درج شده در چک ارسالی را ملاحظه کنید، چک مذکور از طرف فرستنده باطل می شود.

### چطور می توان تقلب را کشف کرد؟ (How to detect fraud?):

بر استناد نتایج برانداری (Survey) های که در کشور های آسترالیا و زیلاند جدید انجام شده است، ۴۲ درصد موضوعات کشف شده تقلبی در جریان نظارت و کنترل داخلی پنهان نگهداشته شده است. اما ۲۳ درصد چنین تقلبات از طریق گزارش منابع خارجی و اشخاص خارج از اداره و



۲۲ درصد بر مبنای گزارش کارمندان مربوط شرکت ها و تارنگارهای کلاهبرداری یگانه وسیله بوده که سازمان های ضد تقلب به کشف چنان دزدی ها و تقلبکاری ها اطلاع یافته اند. جالب است که ۴۷ درصد از

تقلبات محل کار را خبررسان ها پس از گذشت یک سال از وقوع آن کلاهبرداری ها افشا می کنند، به دلیل این که در بعضی از سازمان ها فرهنگ و پالیسی اجازه سخن چینی و خبررسانی در مورد همکاران و کارمندان مجاز نیست. بنابراین، افشای تقلب مدتی را در بر می گیرد. در محلات کار از بالا به پایان فرهنگ دوستی و همکاری مشخصه و ممیزه اصلی راز نگهداری را تشکیل می دهد. این اصل عامل بازدارنده برای کشف تقلبات و جلوگیری از وقوع به موقع آن پنداشته می شود.

غالباً در محلات کار کارمندان داخلی و افراد خارج از محلات کاری شاهد نخستین تقلب ها شمرده می شوند. بنابراین این وظیفه کارمندان و متصدیان است تا به خبررسان ها و اشپلاق چی ها قبلاً گوشزد کنند که به مجرد مشاهده تقلب در موقع لازم آن را افشا نمایند. این فرهنگ و شیوه کار وسیله مؤثر برای جلوگیری از تقلبات کوچک می شود، و راه را در آینده برای انجام تقلبات گسترده و کلان مسدود می سازد.

اما، تقلب در نظام های فاسد، دست نشانده و زیر اشغال مانند افغانستان بدون تصفیه کامل و خانه تکانی نظام غیرمحمتمل و ناممکن به نظر می رسد.

فاتح سامع سابق ویرایشگر (Editor) روزنامه کابل تایمز (Kabul Times Daily) و اکنون مترجمی شفایی و کتبی حرفوی و دارنده جواز ترجمه رسمی و قابل اعتبار و تصدیق شده از ناتی (NAATI Accredited and Certified Professional Translator & Interpreter) و عضو هیئت تحریر تارنگار وزین آریایی ([www.ariaye.com](http://www.ariaye.com)) و گزارش گر آزاد (Freelance Journalist).

## منابع برای اطلاعات بیشتر:

1. <https://www.scamwatch.gov.au/>
2. <https://www.forbes.com/sites/franksorrentino/2018/10/19/the-more-technology-changes-the-more-fraud-stays-the-same/#24219be75685>
3. <https://www.scamwatch.gov.au/get-help/protect-yourself-from-scam>