بینک دولت پاکستان

(Payment Systems Department)

کریڈٹ/ ڈیبٹ/ اسمارٹ کارڈ استعمال کرنے والے کھاتیداروں کے لئے ہدایات/ رہنما خطوط (Guidelines)

نوٹ:

ٹیکنالوجی سے فائدہ اٹھاتے وقت براہ کرم اپنے تحفظ کی خاطر مندرجہ ذیل ہدایات/ رہنما خطوط پر عمل کریں۔ یہ ہدایات چونکہ عمومی ہیں لہٰذا ٹیکنالوجی اور حالات کے تقاضے کے مطابق خصوصی احتیاطی اقدامات کئے جاسکتے ہیں۔

ذاتی شناخت نمبر (PIN) کا انتخاب

(1) ایسا کوئی بھی عدد یا اعداد استعمال نہ کریں، جو با آسانی آپ کی ذات سے منسلک کئے جاسکتے ہوں، مثلاً، آپ کا ٹیلیفون نمبر، آپ کی تاریخ پیدائش کے اعداد، آپ کی گلی کا نمبر یا ڈرائیونگ لائسنس کا نمبر یا اعداد کا کوئی مقبولِ عام مجموعہ (جیسے 786 یا 2005 یا 1111)۔

(2) بہتر تو یہ ہوگا کہ اعداد کا کوئی بے ترتیب مجموعہ استعمال کریں کیونکہ کسی بھی جرائم پیشہ شخص کے لئے اس کا اندازہ لگانا بہت مشکل ہوتا ہے۔ اگر آپ کے لئے اعداد کے اس بے ترتیب مجموعے کو ذہن نشین کرنا مشکل ہو تو پھر ایسے دو اعداد، جو آپ کے لئے کوئی مفہوم و معنی رکھتے ہوں، ان کے ساتھ دو اعداد کا مجموعہ مثلاً، 99 استعمال کریں۔

(3) ذاتی شناخت نمبر (PIN) تھوڑی مدت کے وقفے سے تبدیل کرتے رہیں۔

اپنے ذاتی شناخت نمبر (PIN) کو خفیہ رکھیں

(1) کسی بھی دوسرے شخص کو اپنا کارڈ، ذاتی شناخت نمبر (PIN) اور دیگر کارڈ سے متعلق معلومات استعمال نہ کرنے دیں۔

(2) اپنا ذاتی شناخت نمبر (PIN) اور دیگر معلومات ہمیشہ ذہن نشین رکھیں۔ آپ کو جو ذاتی شناخت نمبر (PIN) فراہم کیا گیا ہے، اگر آپ کو اسے یاد رکھنا مشکل ہو تو جتنی جلد ممکن ہو، آپ اسے کسی دوسرے نمبر سے تبدیل کرلیں، جو آپ کو کیش مشین پر با آسانی یاد رہ سکے۔

(3) ہر وقت اپنے کارڈ کو محفوظ اور ذاتی شناخت نمبر (PIN) خفیہ رکھنے کے لئے مناسب اقدامات کریں۔ آپ کا بینک یا کوئی بھی دیگر ادارہ آپ سے آپ کا ذاتی شناخت نمبر (PIN) پوچھنے کا مجاز نہیں ہے۔

(4) اپنا ذاتی شناخت نمبر (PIN) اور متعلقہ معلومات اپنے کارڈ یا ایسی کسی بھی جگہ پر ہرگز درج نہ کریں، جو دوسرے لوگوں کے لئے با آسانی قابلِ رسائی ہو۔

ATM استعمال کرتے وقت احتیاطی تدابیر

آٹومیٹڈ ٹیلرمشین (ATM) کھاتیداروں کو بینکاری کا ایک تیز رفتار اور آسان متبادل فراہم کرتی ہیں۔ آپ جب اور جہاں چاہیں بینک کی سہولت حاصل کرسکتے ہیں کیونکہ جن مقامات پر یہ مشینیں نصب ہیں، ان تک رسائی بہت آسان ہے۔ چوری اور دھوکا دہی کے خطرات سے نمٹنے کے لئے ہم آپ کو ATMs کے محفوظ استعمال سے متعلق چند نکات بتارہے ہیں تاکہ آپ اور آپ کے کھاتے کی حفاظت میں مدد مل سکے۔

یہ بات یادرکھیں کہ ATMs پر چوری کی واردات دو طریقوں سے ہوسکتی ہے:

(الف) کسی کھاتے سے غیر قانونی طور پر رقم نکلوانا.....یا.....

(ب) کسی شخص کا لین دین مکمل ہوتے ہی اسے لوٹ لینا۔

کیش مشینیں استعمال کرنے والے کارڈ کے حاملین اگر مندرجہ ذیل ہدایات پر عمل کریں تو انہیں ایسے حادثات کا شکار بننے سے محفوظ رہنے میں بڑی مدد ملے گی۔

ATM کا انتخاب

(1) کوئی بھی ATM استعمال کرنے سے قبل اپنے اردگرد کے ماحول پر نظر رکھیں۔ اگر آپ کو کوئی شخص یا کوئی چیز مشکوک محسوس ہو تو آپ ATM سے رقم نکلوانے کا ارادہ ملتوی کردیں اور وہ جگہ فوراً چھوڑ دیں۔ اگر کیش مشین سے متعلق کوئی چیز خلاف معمول ہو یا اس میں تحریف (Tampering) کی علامات محسوس ہوں تو یہ مشین استعمال نہ کریں اور متعلقہ بینک کو فی الفور اس کے متعلق مطلع کریں۔

(2) رات کا اندھیرا پھیلنے کے بعد صرف ایسے مقامات پر نصب شدہ ATMs استعمال کریں، جہاں روشنی کا معقول انتظام ہو۔

(3) اگر ممکن ہو تو کسی مصروف مقام پر نصب شدہ ATM استعمال کریں۔ لوگوں کے بہت زیادہ رش والے مقام کا مطلب اضافی تحفظ ہے۔

(4) اگر کسی ATM کے استعمال کے بعد آپ یہ محسوس کریں کہ کوئی آپ کا تعاقب کررہا ہے تو کسی ایسی جگہ پر پناہ لیں، جہاں لوگوں کی بھیڑ اور، چہل پہل ہو تاکہ تحفظ پایا جاسکے۔

ATM کے استعمال کے ضمن میں ہدایات

(1) ATM سے اپنے رقم نکلوانے کے منظر کو پوشیدہ رکھنے کے لئے اپنے جسم کا سہارا لیں خصوصی طور پر جب آپ اپنا PIN داخل کررہے ہوں یا کیش نکال رہے ہوں۔ اگر ضروری ہو تو اُس شخص کو جانے کے لئے کہہ دیں، خواہ وہ شخص کتنا ہی متجسس کیوں نہ ہو۔

اگر ATM کسی اور کے زیر استعمال ہو تو اسے استعمال کرنے والے کو تنہائی کا وہی موقع فراہم کریں، جس کی آپ خود توقع رکھتے ہیں۔ خود اے ٹی ایم مشین تک پہنچنے سے قبل ان لوگوں کو جانے دیں، جو آپ سے پہلے اسے استعمال کررہے تھے۔

(2) اجنبی افراد کی مدد قبول نہ کریں اور خود کو کبھی گھبراہٹ یا پریشانی کا شکار نہ ہونے دیں۔

(3) متعدد بینکوں نے صارفین کی مدد کے لئے مراکز قائم کئے ہیں۔ اگر آپ کو کوئی مسئلہ درپیش ہو تو ایسی صورت میں متعلقہ شکایتی مرکز کو مطلع کرکے شکایت نمبر حاصل کریں۔

(4) ATM پر یوٹیلیٹی بلز کی ادائیگی کرتے وقت اچھی طرح یہ جانچ پڑتال کرلیں کہ اے ٹی ایم مشین کے ذریعے لین دین کی تفصیلات اصل بل پر درج بل کی رقم اور صارف کی شناخت سے ہم آہنگ ہیں۔ لین دین کی رسید کو بحفاظت اپنے پاس رکھیں تاکہ ادا شدہ رقم کے اگلے بل میں بقایا جات ظاہر ہونے کی صورت میں اس کا حوالہ دیا جاسکے۔

(5) اپنی توجہ ATM کے اسکرین پر مرکوز رکھیں اور بٹنوں کے انتخاب میں مناسب احتیاط برتیں تاکہ مطلوبہ لین دین/رقم کی منتقلی کو یقینی بنایا جاسکے۔ Keyboard کا بٹن دبانے/چھونے سے قبل مطلوبہ معلومات احتیاط سے اے ٹی ایم مشین میں داخل کریں۔ اگر آپ نے غلط بٹن دبایا/چھوا ہو تو مطلوبہ لین دین کا پلٹ کر واپس آنا ممکن نہیں ہے۔

ATM چھوڑنے کے ضمن میں ہدایات

(1) لین دین مکمل ہونے کے بعد اپنا کارڈ واپس لینا نہ بھولیں۔

(2) کوئی بھی لین دین مکمل کرنے کے بعد کیش مشین چھوڑنے سے قبل اپنی رقم اور کارڈ احتیاط سے اپنی جیب میں رکھ لیں۔ اے ٹی ایم مشین پر رقم نہ گنیں۔

(3) اگر کیش مشین آپ کا کارڈ واپس نہ کررہی ہو تو متعلقہ بینک کو اس کی گمشدگی کی فوری طور پر اطلاع دیں۔

(4) اپنی رسیدیں اور ضمنی گوشوارے یا کھاتے میں موجود بقیہ رقم کا پتہ لگانے سے متعلق پرچیاں وہاں نہ چھوڑیں کیونکہ ان پر اہم معلومات درج ہوتی ہیں۔ ATM کے ذریعے ہر دفعہ

لین دین کرتے وقت ہمیشہ رسید ضرور حاصل کریں۔

(5) جب بھی آپ کیش مشین سے متعلق اپنی رسیدیں ضمنی گوشوارے یا کھاتے میں موجود بقیہ رقم کی معلومات سے متعلق پرچیوں کو تلف کرنا ہو تو انہیں اچھی طرح ضائع کردیں۔

خرید وفروخت کے مراکز پر Point of Sale(POS) استعمال کے ضمن میں ہدایات

(1) صارفین کے تحفظ اور کسی ممکنہ خطرے سے نمٹنے کے لئے بینک عموماً خرید وفروخت کے مراکز پر نصب شدہ مشینوں سے کارڈ کے ذریعے لین دین پر کڑی نگاہ رکھتے ہیں۔ایسی صورت حال میں آپ کا متعلقہ بینک آپ کے لین دین کی توثیق اور تصدیق کے سلسلے میں آپ سے رابطہ قائم کرسکتا ہے۔آپ اپنے حقیقی لین دین کی تصدیق ضرور کریں لیکن اپنا ذاتی شناخت نمبر (PIN) اور پاس ورڈ وغیرہ ظاہر نہ کریں۔دونوں جانب سے اس احتیاط کی بدولت برقی بینکاری (e-banking) کے حفاظتی انتظامات کو مؤثر بنانے میں بڑی مدد ملے گی۔

(2) خریداری کے بعد ہمیشہ جب بھی آپ کو آپ کا کارڈ واپس کیا جائے تو اس کی جانچ پڑتال ضرور کریں۔

انٹرنیٹ (Internet) کے ذریعے محفوظ لین دین / اپنے کارڈز کے ذریعے خریداری کے ضمن میں ہدایات

(1) صارفین کو سب سے پہلے تو انٹرنیٹ پر ممکنہ دھوکا دہی کے بارے میں آگہی حاصل ہونی چاہئے۔انہیں ہیکرز (Hackers) کے پھیلائے ہوئے دلفریب اور پُرکشش جال میں ہرگز نہیں پھنسنا چاہئے۔

(2) سوفٹ ویئر (Operating Systems and Browsers) کی ہمیشہ تجدید کرتے رہیں کیونکہ دھوکے باز اور بدنیت ہیکرز بہت چالاک ہوتے ہیں اور وہ سوفٹ ویئر (Widows and Browsers) میں کمزوریوں/ خامیوں کا پتہ چلالیتے ہیں۔متعلقہ بینکوں/ مالیاتی اداروں اور صارفین، دونوں ہی کو اس امر کو یقینی بنانا چاہئے کہ نظام کار اور قانونی فروخت کنندگان کی جانب سے جاری کردہ قانونی اپ گریڈز اور پیچز (Upgrades & Patches) کے استعمال کے ذریعے سوفٹ ویئر کی مسلسل تجدید کی جائے۔

(3) اس امر کو یقینی بنائیں کہ آپ کے کمپیوٹر میں جدید اینٹی وائرس سوفٹ ویئر (Up-to-date anti-virus) اور ایک فائروال (Fire Wall) نصب ہے۔فائروال انٹرنیٹ پر قائم کئے جانے والے دوطرفہ رابطوں کی نگرانی کرسکتی ہے اور اینٹی وائرس سوفٹ ویئر آپ کے کمپیوٹر کو بڑے اور چھوٹے وائرس، دونوں کے حملوں سے محفوظ رکھے گا۔

(4) اس امر کو یقینی بنائیں کہ آپ کا براؤزر نہایت محفوظ ہے۔جب آپ اپنے کمپیوٹر میں اپنے سوفٹ ویئرز نصب کررہے ہوں تو یہ بات یاد رکھیں کہ Safety Options اکثر کوتاہی کی وجہ سے فعال نہیں ہوتے۔

(5) مائکروسوفٹ انٹرنیٹ ایکسپلورر اور نیٹس کیپ نیوی گیٹر دو مقبول ترین براؤزرز ہیں۔یہ ضرور دیکھ لیں کہ آپ جدید ترین ورژن (Recent Version) استعمال کررہے ہیں یا نہیں۔آپ عام طور سے ان براؤزرز کی ویب سائٹس سے جدید ترین ورژن ڈاؤن لوڈ کرسکتے ہیں۔

(6) صرف محفوظ ویب سائٹس پر خریداری کریں۔اپنے کارڈ سے متعلق تفصیلات ارسال کرنے سے قبل اس امر کو یقینی بنائیں کہ آپ کے براؤزرز کی نچلی دائیں سطح پر سیکیورٹی آئیکون مقفل پیڈلاک یا غیر منقطع کلیدی علامت (Unbroken key symbol) ابھر رہی ہے۔

(7) جب ایک محفوظ کنیکشن استعمال کیا جائے گا تو خوردہ فروش (Retailer) کا انٹرنیٹ ایڈریس "http" کے بجائے "https" سے شروع ہوگا۔

(8) ایسی سائٹس استعمال کریں، جن پر آپ اعتماد کرسکتے ہوں، مثلاً، جن سائٹس سے آپ واقف ہوں یا جن کے استعمال کی آپ کو تجویز دی گئی ہو یا ایسی سائٹس، جن کا نام ہی اعتماد کی علامت (Trust Logo) ہو۔

(9) حفاظتی آئیکون (Security Icon) کی جانچ پڑتال کرلیں تاکہ آیا خوردہ فروش ایک مؤثر Encryption سرٹیفکیٹ کا حامل ہے۔اس سرٹیفکیٹ پر درج پتے کو ایڈریس بار پر ابھرنے والے پتے سے ہم آہنگ ہونا چاہئے۔مذکورہ سرٹیفکیٹ کو ویب سائٹس کی شناخت کو یقینی بنانا چاہئے اور موجودہ دن کی تاریخ اس سرٹیفکیٹ کے مؤثر رہنے کی تاریخوں کے اندر ہونی چاہئے۔

(10) اپنی ذاتی معلومات کو محفوظ رکھیں۔ایسی ای میلز سے ہمیشہ ہوشیار رہیں، جن میں آپ سے کسی پتے/ رابطے (Link) کو کلک کرنے یا آپ سے آپ کے متعلق معلومات کی تصدیق کرنے کے لئے کہا جائے۔مشہور ومعروف خوردہ فروش اور بینک وغیرہ آپ سے کبھی بھی آپ کے متعلق حساس نوعیت کی ذاتی یا خفیہ معلومات، بشمول ذاتی شناخت نمبر (PIN) کی تصدیق کے لئے نہیں کہیں گے۔اگر آپ کو کوئی شک وشبہ ہو تو سب سے پہلے متعلقہ ادارے کو فون کریں۔

(11) غیرضروری (Junk Mail) کے لئے Click کرنے سے اجتناب کریں کیونکہ اس کے نتیجے میں آپ کوایک ایسے پتے (Address) پر پہلے سے پرکردہ درخواست فارم ارسال کئے جاسکتے ہیں، جہاں سے گئے ہوئے آپ کو بہت مدت گزر چکی ہو۔

(12) اپنا آرڈراور متعلقہ خوردہ فروش کی شرائط وضوابط، واپسی کی پالیسی (Returns Policy)، شرائط حوالگی (Delivery Conditions) ڈاک کے پتے (ناکہ پوسٹ آفس بکس نمبر، فون نمبر، موبائل نمبر) کی نقول محفوظ رکھیں۔ بعض صورتوں میں آپ سے کچھ اضافی اخراجات وصول کئے جاسکتے ہیں، بالخصوص جب آپ بیرون ملک سے خریداری کررہے ہوں۔ بیرون ملک سے خریداری کرتے وقت ہمیشہ یادرکھیں کہ اگر ایسی صورت میں آپ کے لئے کچھ مسائل پیدا ہوئے تو آپ کے لئے انہیں حل کرنا مشکل ہوگا لیکن مذکورہ بالا تمام معلومات حاصل ہونے کی صورت میں آپ کا کارڈ جاری کرنے والے کو آپ کا مسئلہ حل کرنے میں مدد ملے گی۔

(13) اس امر کو یقینی بنائیں کہ آپ کسی بھی نوع کی جو ادائیگیاں داخل کررہے ہوں، آپ ان ادائیگیوں کی Commitments سے پوری طرح آگاہ ہیں، آیا آپ کسی واحد ادائیگی کی ہدایت کررہے ہیں یا متعدد ادائیگیوں کی۔

(14) اگر آپ بینکاری کی اس اہم سہولت کو استعمال کرتے ہوئے اپنے یوٹیلٹی بلز کی ادائیگی کررہے ہوں تو ایسی صورت میں اس امر کو یقینی بنائیں کہ استعمال کنندہ (User)، صارف کی شناخت (Customer ID) اور بل کی رقم ہو بہو وہی ہے، جو آپ کی کمپنی کی جانب سے آپ کو ارسال کردہ بل پر درج ہے۔ اس لین دین کی رسید کو ہارڈ ڈسک پر محفوظ کرلیا جائے اور پرنٹ بھی کرلیا جائے کیونکہ اگر انٹرنیٹ پر لین دین اور اس میں فرق ہو یا پہلے سے ادا شدہ بل، بلوں کے اجراء کے اگلے دورانیے (Next Billing Cycle) میں دوبارہ جاری کردیا جائے تو ایسی صورتوں میں اس رسید کا حوالہ دیا جاسکتا ہے۔

(15) اگر آپ کو اپنے کارڈ سے متعلق تفصیلات فراہم کرنے کے سلسلے میں کچھ شبہات یا تحفظات ہوں تو ادائیگی کا کوئی دوسرا طریق کار تلاش کریں۔

(16) اگر آپ انٹرنیٹ پر باقاعدگی سے لین دین کرتے ہیں تو آپ کریڈٹ کارڈ کا ایک الگ کھاتہ (Account) کھولنے پر غور کریں، جو صرف اس لین دین کے لئے مخصوص ہو۔

(17) اپنے پاس ورڈز (Passwords) کو صیغۂ راز میں رکھیں۔ چند آن لائن اسٹورز آپ کو خریداری سے قبل استعمال کنندہ کے نام اور پاس ورڈ کے ذریعے رجسٹر کرنے کی ضرورت ہوسکتی ہے۔ آن لائن پاس ورڈز، بشمول آپ کو آپ کے جاری کنندہ (Issuer) کی جانب سے تصدیق شدہ پاس ورڈز کو غیر متعلقہ لوگوں/ پارٹیوں سے بالکل اسی طرح خفیہ رکھیں، جس طرح آپ اپنے کارڈ کا ذاتی شناخت کا نمبر (PIN) خفیہ رکھتے ہیں۔ تمام Login Information کو محفوظ اور خفیہ رکھیں۔

(18) ادائیگی سے متعلق معلومات کبھی بھی ای میلز کے ذریعے ارسال نہ کریں۔ انٹرنیٹ پر جانے والی معلومات (مثلاً: ای میل) پوری طرح محفوظ نہیں ہوتی ہے اور غیر متعلقہ لوگوں/ پارٹیوں کی جانب سے اسے پڑھے جانے کا خدشہ موجود رہتا ہے۔ نہایت مشہور ومعروف کاروباری سائٹس (Merchant Sites) انکرپشن ٹیکنالوجیز (Encryption Technologies) استعمال کرتے ہیں، جو آپ کی جانب سے آن لائن لین دین کرتے وقت آپ کے بارے میں نجی تفصیلات کو دوسرے لوگوں تک پہنچنے کے خطرے سے محفوظ رکھیں گی۔

(19) ای میلز کے اندر کبھی بھی ہائپر لنکس (Hyper Links) کو کلک نہ کریں۔ اگر آپ کو یقین ہے کہ متعلقہ کمپنی اصلی ہے تو انٹرنیٹ براؤزرز ایڈریس بار (Internet browsers address bar) پر URL میں براہ راست ٹائپ کریں یا پہلے سے تصدیق شدہ رابطہ نمبر پر یقینی طور پر اصل متعلقہ کمپنی سے رابطہ قائم کریں۔

(20) ویب سائٹس اور مرچنٹ اسٹورز کو اپنے کارڈ سے متعلق معلومات اسٹور کرنے کی اجازت نہ دیں۔ ڈیٹا بیس پر شناختی معلومات (Identity Information) اسٹور کرنے کی اجازت دینے کے مقابلے میں انکرپٹڈ لین دین کا تبادلہ (Exchage of Encrypted Transactions) بہتر ثابت ہوگا۔

گوشواروں کی جانچ پڑتال کے ضمن میں ہدایات

(1) اپنے بینک کی جانب سے گوشواروں کی باقاعدگی سے وصولی کو یقینی بنائیں۔ اگر آپ کو گوشوارہ موصول نہ ہو تو ایسی صورت میں بینک اسٹیٹمنٹ کی نقل حاصل کرنے کے لئے اپنے بینک سے رجوع کریں۔

(2) لین دین کی مطابقت کے لئے یہ تجویز کیا جاتا ہے کہ ضمنی گوشوارے (Mini-statements) باقاعدگی سے حاصل کئے جائیں۔

(3) اپنے لین دین کے گوشواروں (بینک اسٹیٹمنٹ یا ضمنی گوشوارے) کے ساتھ باقاعدگی سے مطابقت کریں۔

دھوکا دھی اور فریب کاری پر مبنی ای میلز

(1) دھوکا دہی اور فریب کاری پر مبنی ای میلو پر بھی کمپنی کے مسلمہ ٹریڈ مارکس، لوگوز (Logos)، گرافکس اور URLs درج ہو سکتے ہیں۔

(2) لنک کی پشت پر ایچ ٹی ایم ایل ٹیگز (HTML Tags) سے یہ ظاہر ہوگا کہ بنیادی یو آر ایل (Underlying URL) عموماً مستند حلقے (Authentic Domain) سے منسلک نہیں۔

(3) اس طرح کی ای میل میں خفیہ یا ذاتی معلومات، ذاتی شناخت نمبر (PIN)، اکاؤنٹ نمبر وغیرہ فراہم کرنے کی درخواست کی جاتی ہے۔

(4) اس میں کھاتے (Accounts) یا کارڈز کو قابلِ استعمال (Activated) رکھنے کے لئے فوری اقدام کی درخواست کی جاتی ہے تا کہ اسے دھوکا دہی/فریب کاری کے مقاصد کے لئے استعمال کیا جا سکے۔

(5) ای میل سے منسلکہ ویب سائیٹ (Linkedwebsite) محفوظ اور اصل رابطہ فراہم نہ کرے یعنی یہ ویب براؤزر کی نچلی سطح پر Closed Pedlock ظاہر نہیں کرتی۔

صرف ایسی ای میلز کھولیں اور ان کا جواب دیں جو
بعض بنیادی آزمائشوں پر پورا اترتی ہوں، مثلاً:

(1) کیا یہ ای میل کسی ایسے شخص کی جانب سے بھیجی گئی ہے، جسے آپ جانتے ہیں؟

(2) کیا یہ ای میل بھیجنے والے کی جانب سے آپ کو اس سے قبل بھی ای میلز موصول ہوئی ہیں؟

(3) کیا آپ یہ ای میل بھیجنے والے کی جانب سے منسلکہ (Attachment) کے ہمراہ ای میل کی توقع کر رہے تھے؟

(4) کیا اس ای میل بھیجنے والے کی جانب سے بھیجی گئی ای میل اور عنوان کے خانے (Subject Line) میں بیان کردہ مندرجات اور منسلکہ کے نام کے کوئی مفہوم و معنی ہیں؟

(5) کیا اس ای میل کے ساتھ وائرس تو نہیں؟

کارڈز اور ذاتی معلومات کی حفاظت

(1) اپنے کارڈ کی مکمل طور پر حفاظت کیجئے اور اس ضمن میں اس کے کچھ بنیادی اصولوں پر عمل کیجئے۔ کارڈز حساس نوعیت کے ہوتے ہیں اور اگر انہیں کھلا چھوڑ دیا جائے تو ان پر میکینکل، برقی کشش (Electromagnetic) اور دھوپ کے اثرات مرتب ہو سکتے ہیں اور کیمروں کے ذریعے ان کی تصویر بھی اتاری جا سکتی ہے۔

(2) لکی ڈراز (Lucky Draws) کے لئے ذاتی معلومات فراہم کرنے سے گریز کیجئے، خواہ یہ لکی ڈراز کسی بھی ادارے کی جانب سے ہی کیوں نہ ہوں۔ عام طور پر یہ ادارے ذاتی معلومات چوری ہونے کی صورت میں کوئی ذمہ داری قبول نہیں کرتے، جس سے کارڈ کے حامل (Card Holder) کو نقصان پہنچ سکتا ہے۔

(3) آپ کا متعلقہ بینک آپ کے مکمل پاس ورڈ کے بجائے صرف آپ کے پاس ورڈ کے مخصوص کیریکٹرز کے بارے میں استفسار کرے گا۔ آپ کے متعلقہ بینک کی جانب سے جب بھی آپ سے اس سلسلے میں کوئی استفسار کیا جائے، آپ ان کا فون نمبر پوچھیں، اس کی تصدیق کر کے دوبارہ ان سے فون پر رابطہ قائم کریں۔ ایسی میلو کا جواب دینے کے سلسلے میں بھی احتیاط برتیں، جن میں آپ سے معلومات فراہم کرنے کی درخواست کی گئی ہو۔ اگر آپ کسی شک و شبے میں مبتلا ہوں تو شناخت کا ثبوت طلب کریں یا پھر اپنے طور پر جانچ پڑتال کریں۔ اپنا ذاتی شناخت نمبر (PIN) کبھی بھی کسی پر ظاہر نہ کریں۔

(4) جونہی آپ کو اپنا نیا کارڈ موصول ہو، اس کی پشت پر فوراً اپنے دستخط کریں۔

(5) اپنے پاس صرف چند کارڈز رکھیں کیونکہ ان کی چوری کا خطرہ بہت کم ہوگا۔

(6) متعدد کارڈز رکھنے کی صورت میں اپنے تمام کارڈز اور ان کے نمبروں کی ایک فہرست مرتب کریں اور انہیں کسی محفوظ جگہ پر رکھیں۔

(7) چونکہ کارڈ کے ذریعے آپ آسانی سے لین دین کر سکتے ہیں لہٰذا گھر میں بڑی رقم نہ رکھیں۔ اس مقصد کے لئے آپ کا بینک محفوظ مقام ہے۔

(8) کوئی بھی ایسے کارڈز، جو آپ کو مطلوب نہ ہوں یا ایسے کارڈز جن کی مدت ختم ہو چکی ہو، ان کو منسوخ کرانے کے لئے اپنے کارڈ کے جاری کنندہ (Card-Issuer) سے رابطہ قائم کر کے غیر مطلوبہ یا ختم المیعاد (Expired) کارڈ کو کم از کم دو حصوں میں کاٹ کر منسوخ کرا دیں۔

(9) اگر آپ اپنے موجودہ گھر سے کہیں اور منتقل ہو رہے ہوں تو ایسی صورت میں اپنے متعلقہ بینک اور دیگر تمام متعلقہ اداروں کو اپنے نئے پتے سے آگاہ کرنا ہرگز نہ بھولیں۔

(10) جو حالات کارڈز کے حاملین کے بس سے باہر ہوں، ایسے حالات کے نتیجے میں کارڈ گم ہونے کی وجہ سے ہونے والے نقصانات کی ذمہ داری عام طور پر کارڈز کے حاملین پر عائد نہیں

ہوتی ہے، مذکورہ حالات میں مندرجہ ذیل حالات اگر چہ شامل ہیں، تاہم یہ ان ہی تک محدود نہیں ہیں:

(الف) فنی مسائل(Technical Problems)، کارڈ کے جاری کنندہ کی غلطیاں اور سسٹم کی دیگر خرابیاں۔

(ب) ایسی صورت میں کسی کارڈ یا ذاتی شناخت نمبر (PIN) کا غیر قانونی استعمال، جہاں ایسے استعمال کی روک تھام کی ذمہ داری کارڈ کے جاری کنندہ پر عائد ہوتی ہے، مثلاً: کارڈ کی گمشدگی یا چوری کی رپورٹ درج کرانے کے بعد، کارڈ منسوخ ہو چکا ہو یا اس کی مدت ختم ہو چکی ہو یا کارڈ کے حامل نے رپورٹ درج کرا دی ہو کہ ذاتی شناخت نمبر (PIN) کارڈ کے حامل کے علاوہ کسی اور کو بھی معلوم ہو سکتا ہے۔

بیرون ملک جاتے ہوئے کارڈز کی حفاظت کے ضمن میں ہدایات

(1) اپنے کارڈ کے جاری کنندہ کے ہنگامی رابطہ نمبروں (Emergency Contact Numbers) لکھ کر محفوظ کر لیں اور متعلقہ معلومات اپنے بٹوے کے بجائے کسی اور جگہ بحفاظت رکھیں۔

(2) چیکنگ کے دوران ہوائی اڈوں اور دیگر ٹرمینلز پر محتاط رہیں۔

کال سینٹرز/آئی وی آرز (Call Centers/IVRs) کے ذریعے لین دین کے ضمن میں ہدایت

(1) ایسے ٹیلی فون کالز کرنے والوں کو اپنا کارڈ نمبر نہیں دیجئے، جن سے آپ اچھی طرح سے واقف نہ ہوں۔ ٹیلیفون کالز کے ذریعے صرف اس وقت لین دین کیجئے، جب آپ نے خود ٹیلیفون کال کی ہو اور آپ متعلقہ کمپنی سے بخوبی واقف ہوں۔ اس وقت خاص طور پر محتاط رہیں، جب کوئی نامعلوم شخص آپ کو فون کر کے کسی بینک یا غیر مجاز ادارے وغیرہ سے وابستہ ہونے کا دعویٰ کرے۔

(2) کارڈ اپنے سامنے رکھیں۔ آپ سے آپ کے کارڈ نمبر، اس کے ختم ہونے کی مدت، دستخط کی پٹی پر کارڈ کا چار عددی خفیہ کوڈ (آپ کا خفیہ ذاتی شناخت نمبر (PIN) نہیں) تاریخ اجراء (جہاں کہیں قابل اطلاق ہو) اور آپ کے کارڈ پر کسی بھی نمونے سے درج آپ کے نام سمیت معلومات فراہم کرنے کے لئے کہا جا سکتا ہے۔

(3) اگر آپ مارکیٹنگ کے کسی سیلز نمائندے کی جانب سے دباؤ محسوس کریں تو تامل سے کام لیں۔ اپنا اکاؤنٹ نمبر اس وقت تک نہ بتائیں، جب تک کہ آپ خریداری کا فیصلہ نہ کر لیں۔

(4) جب بھی آپ اپنا کریڈٹ/ڈیبٹ کارڈ استعمال کریں، کوئی بھی ذاتی معلومات اپنے طور پر فراہم نہ کریں، ماسوائے اپنی ذاتی شناختی دستاویز (ID Document) کے، جو فراہم کرنے کے سلسلے میں آپ سے درخواست کی جا سکتی ہے۔

(5) اگر متعلقہ خوردہ فروش آپ کو آرڈر کی تحریری طور پر تصدیق/توثیق ارسال کرے تو اس کے درست ہونے کا یقین کرنے کے لئے بل کی اچھی طرح جانچ پڑتال کریں۔ ایسی رسیدوں کو اپنے پاس رکھیں اور اپنے آئندہ گوشوارے سے اس کا موازنہ کر کے اس کی جانچ پڑتال کریں۔

(6) اگر آپ کو یہ معلوم ہو کہ آپ کے گوشوارے پر کوئی ایسا لین دین درج ہے، جس کے بارے میں آپ کو یقین ہو کہ آپ نے یہ لین دین نہیں کیا ہے تو ایسی صورت میں فوری طور پر اپنے متعلقہ بینک سے رابطہ قائم کریں۔ آپ سے عدم دعوے کے ایک فارم (Disclaimer) پر دستخط کرنے کے لئے کہا جا سکتا ہے تا کہ اس امر کی تصدیق ہو جائے کہ آپ نے مذکورہ لین دین نہیں کیا ہے۔

اگر آپ کارڈ کے ضمن میں عام دھوکا دھی کا شکار ہوجائیں تو ایسی صورت میں کیا کریں؟

اگر آپ کو یہ پتہ چلے کہ آپ کا کارڈ گم یا چوری ہو گیا ہے یا آپ دھوکا دہی کا شکار ہو گئے ہیں تو ایسی صورت میں فوری طور پر اپنے متعلقہ بینک کو آگاہ کریں۔ لیکن اگر یہ ثابت ہو جائے کہ کارڈ کا حامل دھوکا دہی یا لاپروائی کا مرتکب ہوا ہے، مثلاً اس نے اپنے کارڈ پر اپنا ذاتی شناخت کارڈ (PIN) لکھ رکھا ہو تو ایسی صورت میں کارڈ کے حامل تمام نقصانات کا خود ذمہ دار ہوگا۔

آئی ڈی کی چوری اور دھوکادھی کی چند انتباھی علامات(Warning Signs)

(1) آپ کے بینک اکاؤنٹ یا کریڈٹ کارڈ سے متعلق باقاعدہ گوشوارے (Statements) ملنا بند ہوجائیں۔

(2) آپ یہ محسوس کریں کہ آپ کی کوئی میل (Mail) غائب ہوگئی ہے۔

(3) آپ کے کریڈٹ کارڈ سے متعلق گوشوارے میں ان اشیاء کی خریداری کے ضمن میں وصولیاں شامل ہوں، جو آپ نے نہ تو خریدی ہوں اور نہ ہی ان کی خرید کے لئے کہا ہو۔

(4) قرضے کی وصولی پر مامور کوئی ادارہ/ایجنسی آپ سے ان اشیاء کے بارے میں رابطہ قائم کرے جو آپ نے نہ خریدی ہوں یا ایسے کسی کھاتے کے بارے میں استفسار کرے، جو کہ آپ نے کھولا ہی نہ ہو۔

(5) آپ کو کوئی ایسی ٹیلیفون کال یا ایسا کوئی خط موصول ہو، جس میں یہ کہا جائے کہ آپ کی قرضے کی درخواست ان وجوہات (جن کے بارے میں آپ کو کوئی علم نہیں) کی بنا پر منظور یا مسترد ہوگئی ہے۔

مسائل کے حل کا طریق کار/نظام

(1) بینک کو غلطیوں سے ماورا خدمات فراہم کرنے کی بھرپور کوشش کرنی چاہئے تاکہ دن بدن بڑھتے ہوئے مالی لین دین کو محفوظ بنایا جاسکے۔تاہم کبھی کبھار غلطیاں سرزد ہوجاتی ہیں،جنہیں مکمل طور پر درست کرلیا جانا چاہئے۔خطرے کے امکانات کو کم سے کم کرنے اور صارفین کا اعتماد بحال کرنے کے لئے ہر ایک بینک کے پاس مؤثر نظام/طریق کار موجود ہونا چاہئے تاکہ استفسارات کے جوابات دئے جاسکیں اور شکایات کا ازالہ کیا جاسکے۔

(2) کسی مسئلے/الجھن کی صورت میں سب سے پہلے اس معاملے کا بھرپور جائزہ لیں۔اس مسئلے کی نوعیت پر غور وخوض کریں تاکہ لوگوں کو اس کا حوالہ دیا جاسکے۔ممکن ہے کہ آپ کا یہ مسئلہ فون پر ہی حل ہوجائے۔

☆☆☆