askaribank LIMITED

عسکری
کریڈٹ اور ڈیبٹ کارڈز
کے محفوظ استعمال
کے لیے ہدایات

askaribank LIMITED

عسکری بینک اپنے صارفین کو جدید اور محفوظ الیکٹرانک پیمنٹ سلوشنز فراہم کرنے میں کوشاں ہے۔ فی الحال اے ٹی ایم/ ڈیبٹ کارڈز، انٹرنیٹ بینکنگ، موبائل بینکنگ، کریڈٹ کارڈز، کنٹیکٹ سینٹر آئی وی آر، انٹربینک فنڈز کی منتقلی اور یوٹیلیٹی بلز کی ادائیگیوں کی سہولیات دستیاب ہیں۔ آپ کے کارڈ کا استعمال اب تیز، آسان اور محفوظ تر ہے۔ آپ کے کریڈٹ اور ڈیبٹ کارڈز سے آپ کا بینک اکاؤنٹ اب آپ کی جیب میں ہے۔

جب آپ کو نیا یا تجدید شدہ کارڈ ملتا ہے تو اسے ایکٹیویٹ کرنے کے لیے مندرجہ ذیل ہدایات پر عمل کرنا چاہیئے:

عسکری کریڈٹ کارڈ کی ایکٹیویشن

عسکری بینک لمیٹڈ کے 24/7 ہیلپ لائن 787-000-111 (051) پر کال کریں اور اپنا عسکری ماسٹر کارڈ کریڈٹ کارڈ ایکٹیویٹ کروائیں۔

آپ اپنے عسکری ماسٹر کارڈ کریڈٹ کارڈ کو مختلف چینلز یعنی اے ٹی ایم اور موبائل ایپ/انٹرنیٹ بینکنگ (رجسٹرڈ صارفین کے لیے) کے ذریعے بھی ایکٹیو کرسکتے ہیں۔

عسکری ڈیبٹ کارڈ کی ایکٹیویشن

ڈیبٹ کارڈ کی ایکٹیویشن اے ٹی ایم، انٹرنیٹ بینکنگ سروسز، موبائل ایپلیکیشن، عسکری بینک برانچ اور عسکری بینک کنٹیکٹ سینٹر کے ذریعے کی جاسکتی ہے۔

I. کنٹیکٹ سینٹر کے ذریعے ایکٹیویشن

عسکری بینک 24/7 کنٹیکٹ سینٹر 787-000-111 (051) پر یا عسکری ویزا سگنیچر ڈیبٹ کارڈ کے لیے پرائرٹی بینکنگ ہیلپ لائن (0800-00078) پر کال کریں۔

II. برانچز کے ذریعے ایکٹیویشن

ایکٹیویشن کے لیے اپنی قریبی عسکری بینک کی برانچ پر تشریف لائیں۔

III. آئی نیٹ پورٹل/موبائل ایپ کے ذریعے ایکٹیویشن (رجسٹرڈ صارف کے لیے)

- انٹرنیٹ بینکنگ پر لاگ ان کریں، جہاں کارڈ مینجمنٹ کا آپشن ظاہر ہوگا۔
- کارڈ مینجمنٹ میں تازہ/ نئے کارڈز کو ایکٹیو کرنے کا آپشن موجود ہے۔
- ایکٹیویٹ بٹن پر کلک کرکے کارڈ ایکٹیویشن کا آپشن منتخب کریں۔
- تصدیق کے لیے سسٹم میں اپنے کارڈ نمبر کے 16 ہندسوں کا اندراج کرنا ہوگا۔
- آپ کے رجسٹرڈ موبائل نمبر پر ون ٹائم پاس ورڈ (OTP) بھیجا جائے گا۔
- آپ کو انٹرنیٹ بینکنگ سسٹم میں OTP درج کرنے کی ضرورت ہوگی۔
- کارڈ کو ایکٹیویٹ کرنے کے لیے آپ کو مطلوبہ پن کا اندراج دوبار کرنا ہوگا۔
- کارڈ کو ایکٹیویٹ کرنے کے لیے صارف کی طرف سے رضامندی دی جائے گی۔
- کارڈ کی کامیاب ایکٹیویشن سے متعلق ایک پیغام اسکرین پر ظاہر ہوگا۔

IV. اے ٹی ایم کے ذریعے ایکٹیویشن

- عسکری بینک کے ATM میں اپنا نیا ڈیبٹ کارڈ داخل کریں۔
- ڈیبٹ کارڈ داخل کرنے کے بعد، سسٹم کی طرف سے زبان منتخب کرنے کے بارے میں کہا جائے گا۔
- زبان منتخب کرنے کے بعد، سسٹم CNIC نمبر طلب کرے گا۔
- CNIC مہیا کرنے کے بعد، سسٹم تاریخ پیدائش (DD/MM/YYYY) طلب کرے گا۔

askaribank LIMITED

- تاریخ پیدائش فراہم کرنے کے بعد، آپ کے رجسٹرڈ موبائل نمبر پر ایک OTP ارسال کیا جائے گا۔
- OTP موصول کرنے کے بعد، آپ کو OTP کا اندراج کرنا ہوگا۔
- OTP کا اندراج کرنے کے بعد، آپ کو کارڈ ایکٹیویٹ کرنے کے لیے مطلوبہ نیا ڈیبٹ کارڈ PIN کا دوبار اندراج کرنا ہوگا۔
- کارڈ کی کامیاب PIN جنریشن سے متعلق ایک پیغام اسکرین پر نمودار ہوگا۔

واٹس ایپ بینکنگ کے ذریعے عسکری ڈیبٹ کارڈ کی ایکٹیویشن کا طریقہ:

- عسکری بینک کی واٹس ایپ بینکنگ سروسز چیٹ (گفتگو) کھولیں۔
- گفتگو (Chat) کا آغاز کریں۔
- واٹس ایپ مینو ظاہر ہوگا۔
- کارڈ مینجمنٹ کے لیے *2* پر مشتمل جواب دیں۔
- نئے مینو میں سے ڈیبٹ کارڈ مینجمنٹ کے لیے *1* پر مشتمل جواب دیں۔
- نیا کارڈ ایکٹیویٹ کرنے کے لیے *1* پر مشتمل جواب دیں۔
- اپنا متعلقہ کارڈ منتخب کرنے کے لیے *1* پر مشتمل جواب دیں۔
- سسٹم کی ہدایت پر اپنا مطلوبہ اے ٹی ایم پن (ATM کا PIN) درج کریں۔
- سسٹم کی ہدایت پر تصدیق کے لیے دوبارہ وہی پن درج کریں۔
- اے ٹی ایم پن کی تصدیق کے بعد اپنے MPIN کے تیسرے، پانچویں، چھٹے اور ساتویں حروف کو درج کریں۔
- تفصیلات کی تصدیق کے بعد آپ کا عسکری ڈیبٹ کارڈ ایکٹیویٹ ہوجائے گا۔

پن (PIN) کی تبدیلی:

- عسکری بینک کی واٹس ایپ بینکنگ سروسز چیٹ (گفتگو) کھولیں۔
- گفتگو (Chat) کا آغاز کریں۔
- واٹس ایپ مینو ظاہر ہوگا۔
- کارڈ مینجمنٹ کے لیے *2* پر مشتمل جواب دیں۔
- نئے مینو میں سے ڈیبٹ کارڈ مینجمنٹ کے لیے *1* پر مشتمل جواب دیں۔
- پن تبدیل کرنے کے لیے *2* پر مشتمل جواب دیں۔
- آپ کے کارڈ کی تفصیلات کے ساتھ ایک پیغام ظاہر ہوگا۔ اسے منتخب کرنے کے لیے *1* پر مشتمل جواب دیں۔
- اپنا مطلوبہ 4 ہندسوں والا اے ٹی ایم پن درج کریں۔
- سسٹم کی ہدایت پر دوبارہ وہی 4 ہندسوں والا اے ٹی ایم پن درج کریں۔
- اپنے MPIN کے دوسرے، چوتھے، چھٹے اور ساتویں حروف کو درج کریں۔
- تفصیلات کی تصدیق کے بعد آپ کا عسکری ڈیبٹ کارڈ اے ٹی ایم پن تبدیل ہوجائے گا۔

askaribank LIMITED

کارڈ بلاک کرانا

- عسکری بینک کی واٹس ایپ بینکنگ سروسز چیٹ (گفتگو) کھولیں۔
- گفتگو (Chat) کا آغاز کریں۔
- واٹس ایپ مینو ظاہر ہوگا۔
- کارڈ مینجمنٹ کے لیے *2* پر مشتمل جواب دیں۔
- نئے مینو میں سے ڈیبٹ کارڈ مینجمنٹ کے لیے *1* پر مشتمل جواب دیں۔
- ڈیبٹ کارڈ بلاک کرانے کے لیے نئے مینو میں *3* دبائیں۔
- اپنا متعلقہ کارڈ منتخب کرنے کے لیے *1* پر مشتمل جواب دیں۔
- اپنے MPIN کے تیسرے، چوتھے، پانچویں اور چھٹے حروف درج کریں۔
- تفصیلات کی تصدیق کے بعد، آپ کا ڈیبٹ کارڈ آپ کی درخواست پر بلاک کر دیا جائے گا۔

کارڈ اَن بلاک (Unblock)/دوبارہ ایکٹیویٹ کرانا

- عسکری بینک کی واٹس ایپ بینکنگ سروسز چیٹ (گفتگو) کھولیں۔
- گفتگو (Chat) کا آغاز کریں۔
- واٹس ایپ مینو ظاہر ہوگا۔
- کارڈ مینجمنٹ کے لیے *2* پر مشتمل جواب دیں۔
- نئے مینو میں سے ڈیبٹ کارڈ مینجمنٹ کے لیے *1* پر مشتمل جواب دیں۔
- ڈیبٹ کارڈ اَن بلاک (دوبارہ ایکٹیویٹ) کرانے کے لیے نئے مینو میں *4* دبائیں۔
- اپنا متعلقہ کارڈ منتخب کرنے کے لیے *1* پر مشتمل جواب دیں۔
- اپنے MPIN کے پہلے، تیسرے، چھٹے اور آٹھویں حروف کو درج کریں۔
- تفصیلات کی تصدیق کے بعد آپ کا ڈیبٹ کارڈ آپ کی درخواست پر اَن بلاک/ دوبارہ ایکٹیویٹ کر دیا جائے گا۔

ATM / ڈیبٹ / کریڈٹ کارڈز کے استعمال اور انٹرنیٹ ٹرانزیکشنز کرنے کے لیے ہدایات

ایسے پیمنٹ سلوشنز کی سہولت سے لطف اندوز ہونے کے لیے آپ کو کسی قسم کے خطرے کو کم سے کم کرنے کے لیے احتیاطی تدابیر اپنانی ہوں گی۔ ذیل میں کچھ ہدایات اور احتیاطی تدابیر درج ہیں جو ان سروسز کو استعمال کرتے وقت اپنائی جاسکتی ہیں۔

ذاتی شناخت نمبر (PIN) / پاس ورڈ کا انتخاب

1. اے ٹی ایم PIN، T-PIN اور کریڈٹ کارڈ PIN عام طور پر چار ہندسوں کے کوڈ ہوتے ہیں، جن کی مدد سے آپ اے ٹی ایم اور POS ٹرمینلز اور کنٹیکٹ سینٹر IVR پر ٹرانزیکشن کرتے ہیں۔ پاس ورڈ عام طور پر کم از کم 8 ہندسوں کے حروف اور اعداد پر مشتمل کوڈ ہوتا ہے، جس سے انٹرنیٹ بینکنگ سروسز تک آپ کی رسائی ممکن ہوتی ہے۔
2. PIN / پاس ورڈ کے طور پر ایسا کوئی بھی عدد یا اعداد استعمال نہ کریں، جو با آسانی آپ کی ذات سے منسلک کئے جا سکتے ہوں مثلاً آپ کا ٹیلی فون نمبر، آپ کی تاریخ پیدائش کے اعداد، آپ کی گلی کا نمبر یا ڈرائیونگ لائسنس کا نمبر وغیرہ یا اعداد کا کوئی مقبول عام مجموعہ (جیسے 1111, 2014, 0786)۔
3. بہتر یہ ہوگا کہ اعداد کا کوئی بے ترتیب مجموعہ استعمال کریں (انٹرنیٹ پاس ورڈ کی صورت میں حروف اور اعداد کا مجموعہ) کیونکہ جرائم پیشہ شخص کے لیے اس کا اندازہ لگانا مشکل ہوگا۔
4. ذاتی شناخت نمبر (PIN) اور پاس ورڈ وقتاً فوقتاً تبدیل کرتے رہیں۔
5. QR کوڈ کو اسکین کرتے ہوئے PIN/OTP ہرگز شیئر مت کریں کیونکہ بینک کے مستند QR کوڈ کو کبھی بھی PIN/OTP مطلوب نہیں ہوتے۔ جب بھی QR کوڈ اسکین کرتے ہوئے PIN/OTP مطلوب ہو تو یاد رکھیں کہ یہ دھوکہ دہی پر مبنی ٹرانزیکشن ہو سکتی ہے۔
6. کارڈز کی معلومات کی حفاظت کے لیے اپنے کارڈز کو RFID جیکٹس میں رکھیں۔

اپنے ذاتی شناخت نمبر (PIN) / پاس ورڈ کو خفیہ رکھیں

1. کسی بھی دوسرے شخص کو اپنی لاگ اِن ID / پاس ورڈ، اے ٹی ایم کارڈ نمبر، اے ٹی ایم PIN، سی وی وی کوڈ، ون ٹائم پاس ورڈ (OTP) ہرگز نہ بتائیں۔
2. اپنا ذاتی شناخت نمبر (PIN) / پاس ورڈ اور دیگر سیکورٹی 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 جلدی ممکن ہو اسے تبدیل کر لیں جو آپ با آسانی یاد رکھ سکیں۔ حفاظتی تدابیر کے طور پر اپنے ذاتی شناخت نمبر (PIN) / پاس ورڈ کو لکھ کر کسی ایسی محفوظ جگہ پر رکھیں جہاں تک آپ کے علاوہ کسی دوسرے شخص کی رسائی ممکن نہ ہو۔
3. ہر وقت اپنے کارڈ کو محفوظ اور ذاتی شناخت نمبر (PIN) خفیہ رکھیں۔ آپ کا بینک یا کوئی بھی دیگر ادارہ آپ سے آپ کا ذاتی شناخت نمبر (PIN) / پاس ورڈ پوچھنے کا مجاز نہیں ہے۔
4. اپنا ذاتی شناخت نمبر (PIN) اور سیکورٹی سے متعلقہ دیگر معلومات کو اپنے کارڈ یا ایسی کسی بھی جگہ پر ہرگز درج نہ کریں جو دوسرے لوگوں کے لیے با آسانی قابل رسائی ہو۔
5. اپنے ذاتی شناخت نمبر (PIN) کو فون، موبائل، انٹرنیٹ میسنجر یا کسی دیگر ذرائع سے کسی کو نہ بتائیں۔

ATMs (آٹو میٹڈ ٹیلر مشینز) استعمال کرتے وقت احتیاطی تدابیر

آٹو میٹڈ ٹیلر مشینز (ATMs) آپ کو 24 گھنٹے وسیع خدمات کے ساتھ بینکاری کا ایک تیز رفتار اور آسان متبادل فراہم کرتی ہیں۔ تاہم ATMs پر درج ذیل طریقوں سے نقصان کا خطرہ رہتا ہے:

(الف) اگر آپ کا ATM غیر محفوظ ہے اور کسی دوسرے شخص کو اس کا PIN معلوم ہے تو آپ کے اکاؤنٹ سے غیر قانونی طور پر رقم نکلوانا۔

(ب) رقم نکلواتے وقت لوٹ لینا۔

درج ذیل ہدایات پر عمل کرتے ہوئے نقصان کے خطرے کو کم سے کم کیا جا سکتا ہے:

ATM کا انتخاب

1. کوئی بھی ATM استعمال کرنے سے قبل اپنے ارد گرد 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 کر دیں اور وہ جگہ فوراً چھوڑ دیں۔
2. اگر ATM 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۔
3. رات کا اندھیرا پھیلنے کے بعد ایسے مقامات پر نصب شدہ ATM استعمال کریں جہاں روشنی کا معقول انتظام ہو۔
4. 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۔
5. اگر کسی ATM کے استعمال کے بعد آپ یہ محسوس کریں کہ کوئی آپ کا تعاقب کر رہا ہے تو کسی ایسی جگہ پر پناہ لیں، جہاں لوگوں کی بھیڑ اور چہل پہل ہو تا کہ تحفظ پایا جا سکے۔

ATM کے استعمال کے ضمن میں ہدایات

1. ATM سے اپنے رقم نکلوانے کے منظر کو پوشیدہ رکھنے کے لیے اپنے جسم کا سہارا لیں۔ خصوصی طور پر جب آپ اپنا PIN داخل کر رہے ہوں یا کیش نکال رہے ہوں۔
2. اگر ATM کسی اور کے زیر استعمال ہو تو اسے استعمال کرنے والے کو تنہائی کا وہی موقع دیں، جس کی آپ خود توقع رکھتے ہیں۔ آپ خود اے ٹی ایم مشین تک پہنچنے سے قبل ان لوگوں کو جانے دیں، جو آپ سے پہلے اسے استعمال کر رہے ہیں۔

askari bank LIMITED

3. اجنبی افراد کی مدد قبول نہ کریں اور خود کو کبھی گھبراہٹ یا پریشانی کا شکار نہ ہونے دیں۔

4. متعدد بینکوں نے کسٹمر سپورٹ فراہم کرنے کے لیے کنٹیکٹ سینٹر قائم کئے ہیں۔ اگر آپ کو کوئی مسئلہ درپیش ہو یا کسی مشکوک سرگرمی کا شبہ ہو تو ایسی صورت میں انہیں مطلع کر کے کمپلینٹ نمبر حاصل کریں۔ عسکری بینک کنٹیکٹ سینٹر 787-000-111 (051) پر یا عسکری ویزا سگنیچر ڈیبٹ کارڈ کے لیے پرائرٹی بینکنگ ہیلپ لائن (0800-00078) پر کال کریں۔

5. ATM پر یوٹیلیٹی بلز کی ادائیگی کرتے وقت اچھی طرح 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 جا سکے۔

6. اپنی توجہ ATM کی اسکرین پر مرکوز رکھیں اور بٹنوں کے انتخاب میں مناسب احتیاط برتیں تاکہ مطلوبہ لین دین کی منتقلی کو یقینی بنایا جا سکے۔ Keyboard کا بٹن دبانے / چھونے سے قبل مطلوبہ معلومات احتیاط سے ATM مشین میں درج کریں۔ اگر آپ نے غلط بٹن دبایا / چھولیا 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 ATM چھوڑنے سے قبل اپنی رقم اور کارڈ احتیاط سے اپنی جیب میں رکھ لیں۔

3. اگر ATM آپ کا کارڈ واپس نہ کر رہی ہو تو متعلقہ برانچ جہاں آپ کا اکاؤنٹ ہے یا ہمارے کنٹیکٹ سینٹر 787-000-111 (051) پر کال کرکے اپنا کارڈ بلاک کروائیں۔ آپ اپنا اے ٹی ایم کارڈ اس برانچ (جہاں آپ کا کارڈ کیپچر ہوا تھا) سے 2 ایام کے اندر اپنا اصل شناختی کارڈ دکھا کر حاصل کر سکتے ہیں۔

4. ہر بار جب آپ اے ٹی ایم پر ٹرانزیکشن کرتے ہیں تو آپ رسید کی درخواست کر سکتے ہیں۔ اپنی رسیدیں، ضمنی گوشوارے یا بیلنس انکوائری کی پرچیوں کو ضائع نہ کریں کیونکہ یہ اہم معلومات پر مشتمل ہوتی ہیں۔ اپنی رسیدیں اور ضمنی گوشوارے اور بیلنس انکوائری سے متعلق پرچیاں اچھی طرح تلف کر دیں یا ضائع کر دیں، جب ان کی ضرورت نہ ہو۔

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

1. POS (پوائنٹ آف سیل) پر کارڈ کو dip کرتے وقت اپنے کارڈ پر کڑی نگاہ رکھیں اور PIN کا اندراج خود کریں۔

2. صارفین کے تحفظ اور کسی ممکنہ خطرے سے نمٹنے کے لے بینک عموماً خرید و فروخت کے مراکز پر کارڈ کے ذریعے لین دین پر کڑی نگاہ رکھتے ہیں۔ بعض وجوہات کی بنا پر بینک لین دین کی توثیق اور تصدیق کے سلسلے میں آپ سے رابطہ کر سکتا ہے۔ اپنا ذاتی شناخت نمبر (PIN) اور پاس ورڈ وغیرہ ہرگز ظاہر نہ کریں۔

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

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

1. چائے خانوں اور پبلک مقامات (ایئر پورٹس وغیرہ) پر موجود انٹرنیٹ کو اپنے اکاؤنٹ سے متعلق ذاتی معلومات کے لیے ہرگز نہ استعمال کریں۔

2. Legitimate سافٹ ویئر (آپریٹنگ سسٹم، براؤزرز اور اینٹی وائرس / فائروال کے لیے) استعمال کریں اور مستقل بنیاد پر ان کو اپ ڈیٹ کرتے رہیں۔ ایسا نہ کرنے کی صورت میں دھوکے باز اور بدنیت ہیکرز کو آپ کے سسٹم اور معلومات تک رسائی مل سکتی ہے۔

3. اس بات کو یقینی بنائیں کہ آپ کا براؤزر حفاظتی نوٹیفکیشن اور نگرانی کی بہترین سطح پر ہے۔ جب آپ اپنے کمپیوٹر پر اپنا سافٹ ویئر انسٹال کرتے ہیں تو حفاظتی / سیکورٹی آپشنز ہمیشہ ڈیفالٹ ایکٹیویٹ نہیں ہوتے ہیں۔

4. انٹرنیٹ کے ذریعے خریداری کرتے وقت صرف محفوظ اور قابل اعتماد ویب سائٹس پر خریداری کریں۔ اپنے کارڈ سے متعلق معلومات ارسال کرنے سے قبل اس امر کو یقینی بنائیں کہ آپ کے براؤزر کی نچلی دائیں سطح پر سیکورٹی آئیکون،

مقفل پیڈ لاک یا غیر منقطع کلیدی علامت (Unbroken Key Symbol) ابھر رہی ہو۔ (اشارہ: جب ایک محفوظ کنکشن استعمال کیا جائے تو خوردہ فروش (Retailer) کا انٹرنیٹ ایڈریس "http" کے بجائے "https" سے شروع ہوگا۔

5. حفاظتی آئیکون (Security Icon) کی جانچ پڑتال کر لیں کہ 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 چاہیئے۔ مذکورہ سرٹیفکیٹ کو ویب سائٹس کی شناخت کو یقینی بنانا چاہیئے اور موجودہ دن کی تاریخ اس سرٹیفکیٹ کے مؤثر رہنے کی تاریخوں کے اندر ہونی چاہیئے۔

6. 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 لیے کہا جائے۔مشہور و معروف ریٹیلرز اور بینک وغیرہ کبھی بھی آپ کے متعلق حساس نوعیت کی ذاتی یا خفیہ معلومات بشمول ذاتی شناخت نمبر (PIN) / پاس ورڈ تصدیق کے لیے نہیں کہیں گے۔ اگر آپ کو کوئی شک وشبہ ہو تو سب سے پہلے متعلقہ ادارے کی ہیلپ لائن 787-000-111 (051) پر کال کریں۔

7. غیر ضروری میل (Junk Mail) کے لیے سائن اپ کرنے سے اجتناب کریں کیونکہ اس کے نتیجے میں آپ کو ایک ایسے پتے (Address) پر پہلے سے پر کردہ درخواست فارم ارسال کیے جا سکتے ہیں جہاں سے گئے ہوئے آپ کو بہت مدت گزر چکی ہو۔

8. اپنے آرڈر کا پرنٹ لیں اور اپنا آرڈر اور متعلقہ خوردہ فروش کی شرائط وضوابط، واپسی کی پالیسی، شرائط حوالگی، ڈاک کے پتے (پوسٹ آفس بکس نمبر نہیں) اور فون نمبر (موبائل نمبر نہیں) کی نقول محفوظ رکھیں۔بعض صورتوں میں آپ سے کچھ اضافی اخراجات جیسے مقامی ٹیکسز اور ڈاک کے اخراجات وصول کئے جا سکتے ہیں، بالخصوص جب آپ بیرون ملک سے خریداری کر رہے ہوں۔ اگر ایسی صورت میں آپ کے لیے کچھ مسائل پیدا ہوئے تو آپ کے لیے انہیں حل کرنا مشکل ہو گا 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۔

9. اس امر کو یقینی بنائیں کہ آپ کسی بھی نوع کی جو ادائیگیاں داخل کر رہے ہوں، آپ ان ادائیگیوں کی Commitments سے پوری طرح آگاہ ہیں، آیا کہ آپ کسی واحد ادائیگی کی ہدایت کر رہے ہیں یا متعدد ادائیگیوں کی۔

10. اگر آپ کو اپنے کارڈ سے متعلق تفصیلات فراہم کرنے میں کچھ شکوک وشبہات یا تحفظات ہوں تو ادائیگی کا کوئی دوسرا طریقہ کار تلاش کریں۔

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

12. اپنے پاس ورڈ کو صیغہ راز میں رکھیں۔ چند آن لائن اسٹورز پر آپ کو خریداری سے قبل استعمال کنندہ کے نام اور پاس ورڈ کے ذریعے رجسٹر کرنے کی ضرورت ہو سکتی ہے۔ آن لائن پاس ورڈ، بشمول آپ کو آپ کے جاری کنندہ کی جانب سے تصدیق شدہ پاس ورڈ کو غیر متعلقہ لوگوں / پارٹیوں سے اسی طرح خفیہ رکھیں جس طرح آپ اپنے کارڈ کا ذاتی شناخت کا نمبر خفیہ رکھتے ہیں۔ تمام لاگ اِن (Login) معلومات (Information) کو محفوظ اور خفیہ رکھیں۔

13. 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۔ مشہور و معروف کاروباری سائٹس مرچنٹس انکرپشن ٹیکنالوجیز استعمال کرتے ہیں جو آپ کی جانب سے آن لائن لین دین کرتے وقت آپ کے بارے میں تفصیلات کو دوسرے لوگوں تک پہنچنے کے خطرے سے محفوظ رکھے گی۔

14. ای میلز کے اندر ہائپر لنکس کو کلک نہ کریں۔ اگر آپ کو یقین ہے کہ متعلقہ کمپنی اصلی ہے تو انٹرنیٹ براؤزر ایڈریس بار پر URL براہ راست ٹائپ کریں یا پہلے سے تصدیق شدہ رابطہ نمبر پر یقینی طور پر اصل متعلقہ کمپنی سے رابطہ کریں۔

15. ویب سائٹ اور مرچنٹ اسٹورز کو اپنے کارڈ سے متعلق معلومات اسٹور کرنے کی اجازت نہ دیں۔ ڈیٹابیس پر شناختی معلومات (Identity Information) اسٹور کرنے کی اجازت دینے کے مقابلے میں انکرپٹڈ لین دین کا تبادلہ (Exchange of Encrypted Transactions) بہتر ثابت ہوگا۔

16. اگر آپ بینکاری کی اس اہم سہولت کو استعمال کرتے ہوئے اپنے یوٹیلیٹی بلز کی ادائیگی کر رہے ہیں تو ایسی صورت میں اس امر کو یقینی بنائیں کہ استعمال کنندہ کا نام، صارف کی شناخت 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 کر لیا جائے اور پرنٹ بھی کر لیا جائے، کیونکہ انٹرنیٹ پر لین دین اور اس میں فرق ہو یا پہلے سے ادا شدہ بل، بلوں کے اجراء کے اگلے دورانیہ میں دوبارہ جاری کر دیا جائے تو ایسی صورتوں میں اس رسید کا حوالہ دیا جا سکتا ہے۔

17. اگر آپ فنڈز ٹرانسفر کر رہے ہیں تو اس امر کو یقینی بنائیں کہ آپ نے پہلے سے متعین کردہ فہرست سے درست بینفشری اکاؤنٹ منتخب کیا ہے یا آپ کے بینک کی پیش کردہ سہولت کے مطابق بینفشری کا پورا اکاؤنٹ نمبر درج کیا ہے۔ نیز، اس امر کو بھی یقینی بنائیں کہ لین دین کی تصدیق سے قبل آپ نے صحیح رقم درج کر لی ہے۔ ٹرانزیکشن کی رسید ہارڈ ڈسک میں یا اس کا پرنٹ لے کر بھی محفوظ کی جا سکتی ہے۔

18. سب سے اہم بات یہ کہ آپ کو انٹرنیٹ پر ممکنہ فراڈ سے واقفیت ہونی چاہیے۔ آپ کو ہیکرز کے پھیلائے ہوئے دلفریب اور پرکشش جال میں ہرگز نہیں پھنسنا چاہیے۔

گوشواروں کی جانچ پڑتال کے ضمن میں ہدایات

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

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

آپ کے ڈیبٹ کارڈز پر یومیہ ٹرانزیکشن کی لمٹس

1. آپ عسکری موبائل ایپلی کیشن یا انٹرنیٹ بینکنگ پورٹل میں لاگ اِن کر کے اپنے ڈیبٹ کارڈ سے روزانہ آئی بی ایف ٹی، پی او ایس/ای کامرس اور نقد رقم نکالنے کی لین دین کی لمٹس دیکھ سکتے ہیں۔

2. آپ اپنی ضرورت کے مطابق روزانہ کی لین دین کی لمٹس بھی ایڈجسٹ کر سکتے ہیں۔

دھوکہ دہی اور فریب کاری پر مبنی ای میلز کی پہچان

برائے مہربانی درج ذیل باتوں کو یاد رکھیں اور اس حوالے سے احتیاط برتیں:

1. دھوکہ دہی اور فریب کاری پر مبنی ای میلز پر بھی کمپنی کے مسلمہ ٹریڈ مارکس، لوگوز، گرافکس اور URLs درج ہو سکتے ہیں۔

2. لنک کی پشت پر HTML Tags سے یہ ظاہر ہوگا کہ بنیادی یو آر ایل (Underlying URL) عموماً مستند ڈومین سے منسلک نہیں۔

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

4. اس میں اکاؤنٹ (Account) یا کارڈ کو ایکٹیویٹ رکھنے کے لیے فوری اقدام کی درخواست کی جاتی ہے تا کہ دھوکہ دہی/فریب کاری کے مقاصد کے لیے استعمال کیا جا سکے۔

5. ای میل سے منسلکہ ویب سائٹ (linked Website) محفوظ اور اصل رابطہ فراہم نہ کرے (یعنی یہ ویب براؤزر کی نچلی سطح پر Closed Padlock ظاہر نہ کرے)۔

کارڈز اور ذاتی معلومات کی حفاظت

1. اپنے کارڈ کی مکمل طور پر حفاظت کیجئے کیونکہ اسے سیدھا رکھ کر کیمرے کے ذریعے اس کی تصویر لے کر اہم ڈیٹا چوری کیا جا سکتا ہے۔

askaribank LIMITED

2. کارڈ کو سنبھال کر رکھیں کیونکہ یہ حساس نوعیت کے ہوتے ہیں اوران پر مکینیکل ، برقی کشش (Electromagnetic) اور دھوپ کے اثرات مرتب ہو سکتے ہیں۔

3. کسی لکی ڈرا/قرعہ اندازی میں اپنی ذاتی معلومات فراہم کرنے سے گریز کیجئے، خواہ یہ لکی ڈرا کسی بھی ادارے کی جانب سے ہی کیوں نہ ہوں۔ عام طور پر یہ ادارے ذاتی معلومات چوری ہونے کی صورت میں ذمہ داری قبول نہیں کرتے، جس سے کارڈ ہولڈر کو نقصان پہنچ سکتا ہے۔

4. آپ کا بینک آپ کے مکمل پاس ورڈ کے بجائے صرف آپ کے پاس ورڈ کے مخصوص کیریکٹرز کے بارے میں پوچھ گچھ کرے گا۔ ان سے ان کا فون نمبر طلب کریں اور اس کی جانچ پڑتال کریں اور کال کریں۔ معلومات طلب کرنے کی درخواست پر مبنی ای میلز کے بارے میں بھی محتاط رہیں۔ اگر آپ کسی قسم کے شک وشبہ 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۔

5. جوں ہی آپ کو اپنا نیا کارڈ موصول ہو، اس کی پشت پر فوراً اپنے دستخط کریں۔

6. اپنے پاس صرف چند کارڈ ز رکھیں۔ ایسا کرنے سے ان کی چوری کا خطرہ کم ہوگا۔

7. 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۔

8. کوئی بھی ایسے کارڈز جو آپ کو مطلوب نہ ہوں یا ایسے کارڈز جن کی مدت ختم ہو چکی ہو، ان کو جاری کروانے کے لیے اپنے کارڈ کے جاری کنندہ سے رابطہ قائم کر کے غیر مطلوبہ یا ختم المیعاد کارڈز 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 بینک اور دیگر تمام متعلقہ اداروں کو اپنے نئے پتے سے آگاہ کرنا ہرگز نہ بھولیں۔

10. کارڈ گم ہونے کی وجہ سے ہونے والے نقصانات کی ذمہ داری سے بچنے کے لیے گمشدہ کارڈ کے بارے میں فوری طور پر مطلع کریں۔

بیرون ملک سفر کرتے ہوئے کارڈ کی حفاظت کے ضمن میں ہدایات

1. اپنے کارڈ کے جاری کنندہ کے ہنگامی رابطہ نمبروں کو لکھ کر محفوظ کر لیں اور متعلقہ معلومات اپنے بٹوے کے بجائے کسی اور جگہ بحفاظت رکھیں جہاں آپ کی رسائی باآسانی ممکن ہو۔

2. چیک ان کے دوران ہوائی اڈوں اور دیگر ٹرمینلز پر محتاط رہیں۔ اپنے کارڈ اور دیگر ضروری دستاویزات کی حفاظت یقینی بنائیں۔

کنٹیکٹ سینٹرز/آئی وی آرز کے ذریعے لین دین کے ضمن میں ہدایات

1. فون پر کالز کرنے والے کسی ایسے شخص کو اپنا کارڈ نمبر ہرگز نہ دیں جن سے آپ اچھی طرح سے واقف نہ ہوں۔ ٹیلی فون 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۔ اگر کسی ایسے شخص کی طرف سے کال آتی ہے جو کسی بینک یا کسی بھی مجاز ادارے کی طرف سے ہونے کا دعویٰ کرے تو اس صورت میں خصوصی طور پر محتاط رہیں۔

2. کارڈ اپنے سامنے رکھیں۔ آپ سے آپ کے کارڈ نمبر، میعاد ختم ہونے کی تاریخ، تاریخ اجراء (جہاں قابل اطلاق ہو) اور آپ کے کارڈ پر درج آپ کے نام سمیت معلومات فراہم کرنے کے لیے کہا جا سکتا ہے۔ براہ مہربانی کسی کو بھی PIN/OTP اور CVC (آپ کے کارڈ کی پشت پر موجود 3 ڈجٹ) ہرگز نہ بتائیں۔

3. اگر آپ مارکیٹنگ کے کسی سیلز نمائندے کی جانب سے دباؤ محسوس کریں تو شک وشبہ سے کام لیں۔ اپنا اکاؤنٹ نمبر اس وقت تک نہ بتائیں جب تک آپ خریداری کا فیصلہ نہ کر لیں۔

4. جب بھی آپ اپنا کارڈ استعمال کریں، کوئی بھی ذاتی معلومات اپنے طور پر فراہم نہ کریں ماسوائے اپنے ذاتی شناختی دستاویز کے، جو کہ فراہم کرنے کے سلسلے میں آپ سے درخواست کی جا سکتی ہے۔

5. اگر متعلقہ ریٹیلر آپ کو آرڈر کی تحریری طور پر تصدیق / توثیق ارسال کرے تو اس کے درست ہونے کا یقین کرنے کے لیے بل کی اچھی طرح جانچ پڑتال کریں۔ ایسی رسیدوں کو اپنے پاس رکھیں اور اپنے آئندہ گوشوارے (Statements) سے اس کا موازنہ کر کے اسکی جانچ پڑتال کریں۔
6. اگر آپ کو یہ معلوم ہو کہ آپ کے گوشوارے (Statements) 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 کریں۔ آپ سے عدم دعوے کے ایک فارم (Disclaimer) پر دستخط کرنے کے لیے 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 دھوکہ دہی کا شکار ہو جائیں تو ایسی صورت میں کیا کریں:

اگر آپ کو یہ پتہ چلے کہ آپ کا کارڈ گم یا چوری ہو گیا ہے یا آپ دھوکہ دہی کا شکار ہو گئے ہیں تو ایسی صورت میں فوری طور پر اپنی متعلقہ برانچ کو آگاہ کریں اپنے کارڈ کو بلاک کروانے کے لیے ہمارے کنٹیکٹ سینٹر 787-000-111 (051) پر رابطہ کریں یا عسکری ویزا سگنیچر ڈیبٹ کارڈ کے لیے پرائرٹی بینکنگ ہیلپ لائن (0800-00078) پر کال کریں۔لیکن اگر یہ ثابت ہو جائے کہ کارڈ ہولڈر دھوکہ دہی یا لاپروائی کا مرتکب ہوا ہے، مثلاً اس نے کارڈ پر اپنا ذاتی شناخت نمبر (PIN) لکھ رکھا ہو تو ایسی صورت میں کارڈ ہولڈر تمام نقصانات کا خود ذمہ دار ہو گا۔

آئی ڈی کی چوری اور دھوکہ دہی کی چند انتباہی علامات (Warning Signs)

1. آپ کے بینک اکاؤنٹ یا کریڈٹ کارڈ سے متعلقہ باقاعدہ گوشوارے (Statements) ملنا بند ہو جائیں۔
2. آپ یہ محسوس کریں کہ آپ کی کوئی میل غائب ہو گئی ہے۔
3. آپ کے کریڈٹ کارڈ سے متعلق گوشوارے (Statements) 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 لیے کہا ہو۔
4. قرضے کے حصول پر مامور کوئی ادارہ / ایجنسی آپ سے ان اشیاء کے بارے میں رابطہ قائم کرے جو آپ نے نہ خریدی ہوں یا ایسے کسی اکاؤنٹ (Account) کے بارے میں پوچھ گچھ 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 قرضہ کی درخواست ان وجوہات (جن کے بارے میں آپ کو کوئی علم نہیں) کی بناء پر منظور یا مسترد ہو گئی ہے۔

مسائل کے حل کا طریقہ کار / نظام

عسکری بینک اپنے صارفین کو غلطیوں سے ماورا خدمات فراہم کرنے کی بھرپور کوشش کر رہا ہے۔ تاہم کبھی کبھار غلطیاں سرزد ہو جاتی ہیں۔ صارفین کو رہنمائی فراہم کرنے کے لیے، ہمارے پاس مؤثر نظام / طریقہ کار موجود ہے تا کہ سوالات کے جوابات دیئے جاسکیں اور شکایات کا ازالہ کیا جا سکے۔کسٹمر بینک کے ساتھ درج ذیل ذرائع سے رابطہ کر سکتے ہیں:

1. رہنمائی کے لیے اپنی برانچ کال کریں۔
2. کسی قسم کی مدد کے لیے ہمارے 24/7 کنٹیکٹ سینٹر 787-000-111(051) پر یا عسکری ویزا سگنیچر ڈیبٹ کارڈ کے لیے پرائرٹی بینکنگ ہیلپ لائن (0800-00078) پر کال کریں۔
3. customerservices@askaribank.com.pk یا support@askaribank.com.pk پر ای میل کر کے اپنی شکایات، آراء یا تجاویز یا سوالات درج کریں۔

سیکورٹی کے متعلق آگاہی

سیکورٹی کے متعلق آگاہی کی ہدایات آپ کو ممکنہ دھوکہ دہی کی صورتحال شناخت کرنے میں مدد فراہم کرتی ہیں اور مناسب اور مؤثر انداز میں ان سے نمٹنے میں آپ کی مدد کرتی ہیں۔ اپنے آپ کو دھوکہ دہی سے بچانے کے لیے پہلا قدم خود کو معلومات سے آگاہ رکھنا ہے۔ ایسے امکانات اور دیگر طریقوں کے بارے میں مزید معلومات حاصل کریں جن کا استعمال کر کے دھوکے باز افراد آپ کی ذاتی معلومات حاصل کر سکتے ہیں۔ ذیل میں کچھ عام دھوکہ دہیوں اور ایسے فعال اقدامات کی وضاحت کی گئی ہے جن سے آپ دھوکہ دہی کا شکار ہونے سے بچ سکتے ہیں۔

askari bank LIMITED

چیک کا فراڈ

چیک کا فراڈ مالی فائدے کے مقصد کے لیے چیکوں کا غیر قانونی استعمال (اکاؤنٹ ہولڈر یا غیر مجاز فرد کے ذریعہ) ہے۔ چیک کے فراڈ سے بچنے کے لیے متعدد اقدامات اٹھا سکتے ہیں۔

- جب بھی آپ اپنی چیک بک وصول کریں، تو براہ کرم اس میں چیک لیوز کی تعداد ضرور گنیں۔
- اپنے چیک کو کسی محفوظ مقام پر رکھیں۔
- ماہانہ بینک اسٹیٹمنٹ کا بغور جائزہ لیں اور آن لائن بینکنگ ٹرانزیکشنز کو باقاعدگی سے چیک کریں۔ اگر آپ کو ایسا لگے کہ آپ نے کوئی ٹرانزیکشنز نہیں کیں تو، اس بارے میں اپنے بینک کو فوراً مطلع کریں، بینک اس کی چھان بین کرے گا۔
- اگر آپ نے اپنا اکاؤنٹ بند کروا دیا ہے تو، غیر استعمال شدہ چیکوں کو تلف کردیں۔
- الیکٹرانک ادائیگیوں پر توجہ دیں کیونکہ وہ چیکوں سے زیادہ محفوظ ہیں۔
- جعلی چیک سے محفوظ رہیں۔

کارڈ اسکمنگ (Card Skimming)

اسکمنگ (Skimming) ایک ایسا طریقہ ہے جو جعلساز فنڈز چوری کرنے کے مقصد سے آپ کے پلاسٹک کارڈ سے آپ کی ذاتی یا اکاؤنٹ کی معلومات حاصل کرنے کے لیے استعمال کرتے ہیں۔ اپنے کارڈ کی اسکمنگ (Skimming) سے بچنے کے لیے، درج ذیل حفاظتی اقدامات اپنائیں:

- جب آپ اے ٹی ایم میں ٹرانزیکشن کر رہے ہوں تو اپنے PIN کو ہاتھ، جسم یا پرس کی مدد سے پوشیدہ رکھیں اور پوائنٹ آف سیل پر ٹرانزیکشن کرتے ہوئے اپنے کارڈ پر کڑی نظر رکھیں۔
- کبھی بھی اپنا PIN کسی شخص کے سامنے ظاہر نہ کریں اور نہ ہی قابل فہم انداز میں تحریر کریں۔
- تمام لین دین کی تصدیق کے لیے باقاعدگی سے اپنی بینک اسٹیٹمنٹ اور اکاؤنٹ بیلنس چیک کریں۔
- اگر آپ کا کارڈ گم یا چوری ہوگیا ہے، یا آپ کو Tampering کا شبہ ہے تو اپنا کارڈ تبدیل کریں اور اپنے شبہ کے متعلق بینک کو فوراً اطلاع دیں۔
- اپنے کارڈ کا PIN وقتاً فوقتاً تبدیل کرتے رہیں۔

PIN / پاس ورڈ کی حفاظت

PIN / پاس ورڈ سائبر کرائمز کے خلاف دفاع کی پہلی ڈھال ہیں۔ یہ ضروری ہے کہ آپ اپنے اہم اکاؤنٹس میں سے ہر ایک کے لیے حروف اور اعداد پر مشتمل ایک مضبوط پاس ورڈ منتخب کریں اور پاس ورڈ کو باقاعدگی سے تبدیل کرتے رہیں۔

سائبر کرائم

سائبر کرائم جرائم کی دنیا میں تیزی سے بڑھتا ہوا شعبہ ہے۔ زیادہ تر مجرمان مختلف قسم کی مجرمانہ سرگرمیوں کا ارتکاب کرنے کے لیے انٹرنیٹ کی رفتار، سہولت اور Anonimity کا غلط استعمال کر رہے ہیں، جس کی کوئی حد نہیں۔ انٹرنیٹ پر سرفنگ اور لین دین کرتے وقت مشکوک نظر آنے والی ویب سائٹس سے محتاط رہیں۔ ہمیشہ اچھا اینٹی وائرس اور Malware Detection ایپلی کیشن استعمال کریں، ان کو لازماً اپ ڈیٹ کریں۔

askari bank LIMITED

■ سوشل نیٹ ورکنگ

سوشل میڈیا سماجی رابطے بڑھاتا ہے لیکن مجرموں کے لیے پرکشش خصوصیات بھی پیش کر سکتا ہے۔ جعلساز افراد نام ظاہر نہ کر کے قانونی طریقے سے کم خرچ میں زیادہ لوگوں تک پہنچنے کے لیے سوشل میڈیا کا استعمال کر سکتے ہیں۔ سوشل میڈیا پر اجنبی افراد سے ہمیشہ محتاط رہیں۔

■ فشنگ (Phishing)

اس طریقے سے الیکٹرانک ذرائع سے بات چیت کر کے قابل اعتماد ادارہ ہونے کا بہانہ بنا کر دھوکہ دہی سے حساس معلومات (صارف کا نام، پاس ورڈ، کارڈ کی تفصیلات اور روپے وغیرہ) حاصل کیا جاتا ہے۔ یہ مسئلہ دنیا بھر کے بینکوں کو درپیش ہے۔ عام طور پر اکاؤنٹ سے متعلق معلومات سے بینک کی تفصیلات کو اپ ڈیٹ کرنے یا منافع بخش انعامات کی اسکیموں میں حصہ لینے کی درخواست کی جاتی ہے۔ آپ کو الیکٹرانک ذرائع سے کبھی بھی کوئی ذاتی یا خفیہ معلومات فراہم نہیں کرنی چاہئیں، جب تک کہ آپ کو اس بات کا یقین نہ ہو جائے کہ انکوائری کرنے والا شخص یا ویب سائٹ حقیقی ہے۔

■ اسپوفنگ (Spoofing)

ویب سائٹ کی اسپوفنگ (Spoofing) دھوکہ دہی کی نیت سے جعلی ویب سائٹ بنانے کا عمل ہے۔ Malware (کوڈ کے ذریعے راز داری پر سمجھوتہ کرنا) کے ساتھ آن لائن شاپنگ سائٹس میں نمایاں طور پر اضافہ ہوا ہے۔ آن لائن خریداری کرتے وقت عام فہم کا استعمال کریں اور مندرجہ ذیل محفوظ طریقوں پر عمل کریں:

- سیلر کی ساکھ کے بارے میں معلومات کو یقینی بنائیں۔
- ذاتی معلومات کو بہتر پاس ورڈ سے محفوظ رکھیں۔
- اس امر کو یقینی بنائیں کہ خریداری کی ویب سائٹ محفوظ ہے، یعنی ایڈریس بار میں "https:" موجود ہے۔
- ''کلین'' اور اپ ڈیٹڈ کمپیوٹنگ ڈیوائس کو برقرار رکھیں۔
- ویب سائٹ/پیج ایڈریس ٹائپ کریں۔
- ای میلز میں فراہم کردہ لنکس پر کلک کرنے سے گریز کریں۔

■ وشنگ (Vishing)

یہ ٹیلیفون کا استعمال کر کے دھوکہ دہی سے صارف کی نجی معلومات حاصل کرنے کی کوشش کرنا ہے۔ کال کرنے والا شخص ایک جائز کاروبار ہونے کا ڈھونگ کرتا ہے، اپنے شکار کو بے وقوف بناتا ہے کہ اسے فائدہ ہوگا۔ جب کوئی شخص بینک کے اسٹاف، قانون نافذ کرنے والے اداروں، اسٹیٹ بینک آف پاکستان، بینظیر انکم سپورٹ پروگرام (بی آئی ایس پی) وغیرہ سے تعلق رکھنے کا دعویٰ کرے تو، فون کرنے والے کو کبھی بھی مندرجہ ذیل تفصیلات نہ دیں:

- لاگ اِن آئی ڈی/ پاس ورڈ، اے ٹی ایم کارڈ نمبر، اے ٹی ایم PIN، سی وی وی کوڈ، ون ٹائم پاس ورڈ (او ٹی پی)، اپنے انٹرنیٹ بینکنگ اکاؤنٹ کا پاس ورڈ اور اپنا بینک اکاؤنٹ نمبر۔
- اپنا کریڈٹ/ ڈیبٹ کارڈ نمبر وغیرہ۔

■ سمشنگ (Smishing)

Smishing یا ''ایس ایم ایس فشنگ''، جعلی ٹیکسٹ پیغامات بھیجنے کے لیے ایس ایم ایس سروسز کا استعمال کرنا ہے۔ صارف اپنے موبائل فون یا دوسرے موبائل ڈیوائس پر Malware ڈاؤن لوڈ کر کے دھوکہ دہی کا شکار ہو سکتا ہے۔

askaribank LIMITED

ای میل (E-mail)

عسکری بینک کبھی بھی آپ کو ایسی ای میلز ارسال نہیں کرے گا جن میں خفیہ معلومات طلب کی جاتی ہوں۔ اگر آپ کو کوئی ایسی ای میل موصول ہو جس میں آپ کی انٹرنیٹ بینکنگ کی تفصیلات جیسے کہ آپ کا PIN، پاس ورڈ یا اکاؤنٹ نمبر وغیرہ طلب کیا جائے تو آپ کو کبھی بھی اس کا جواب نہیں دینا چاہیے۔ دھوکہ دہی کی ایسی کوششوں اور ای میلز کی صورت میں، براہ کرم فوری طور پر ہمارے کنٹیکٹ سینٹر 787-000-111(051) پر رابطہ کریں یا عسکری ویزا سگنیچر ڈیبٹ کارڈ کے لیے پرائرٹی بینکنگ ہیلپ لائن (0800-00078) پر کال کریں۔

ترک دعویٰ (Disclaimer)

ان تمام حفاظتی اقدامات کی خلاف ورزی اور عدم تعمیل کی صورت میں نتائج کا ذمہ دار کسٹمر خود ہوگا۔

مزید رہنمائی/معلومات کے لیے،

اپنی قریبی عسکری بینک برانچ تشریف لائیں،

(051)111-000-787 پر یا عسکری ویزا سگنیچر ڈیبٹ کارڈ کے لیے

پرائرٹی بینکنگ ہیلپ لائن (0800-00078) پر کال کریں،