বাংলাদেশ কৃষি ব্যাংক
প্রধান কার্যালয়, ঢাকা
আইসিটি সিস্টেমস্, কার্ড ও মোবাইল ব্যাংকিং বিভাগ

ফোন ঃ ৯৫৭৬৬৫৩
৯৫৬০০২১- ৩৩৫
ই-মেইল : cbs@krishibank.org.bd
ওয়েবসাইট: www.krishibank.org.bd

২২

প্রকা/আইসিটি (সিস্টেমস্)/গাইডলাইনস/১৩(১)/২০১৮-২০১৯/ ২৪২ তারিখ ঃ ৩০/০৮/২০১৮

উপ-মহাব্যবস্থাপক
বাংলাদেশ কৃষি ব্যাংক
স্থানীয় মুখ্য কার্যালয়/ সকল কর্পোরেট শাখা
ও
ব্যবস্থাপক
বাংলাদেশ কৃষি ব্যাংক
সকল অনলাইন শাখা।

বিষয় ঃ ব্যাংকের লেনদেনের ব্যবস্থায় সম্ভাব্য সাইবার আক্রমন সংক্রান্ত সতর্কতা প্রসংগে।

প্রিয় মহোদয়,

উপর্যুক্ত বিষয়ে বাংলাদেশ ব্যাংক, পেমেন্ট সিস্টেমস্ ডিপার্টমেন্টের পিএসডি সার্কুলার নং-০১/২০১৮, তারিখ ঃ ১৬/০৮/২০১৮ এর প্রতি দৃষ্টি আকর্ষণ করা যাচ্ছে।

০২। বাংলাদেশ ব্যাংক, পেমেন্ট সিস্টেমস্ ডিপার্টমেন্টের সার্কুলার অনুযায়ী সম্প্রতি বিভিন্ন পত্র-পত্রিকা গণমাধ্যমে আমাদের পাশ্ববর্তী দেশের ব্যাংকিং ব্যবস্থা হ্যাকিংয়ের মাধ্যমে বিপুল পরিমাণ অর্থ আত্নৎ-এর খবর প্রকাশিত হয়েছে। এ ক্ষেত্রে সাইবার অপরাধীরা পেমেন্ট সিস্টেমস্ হ্যাক করে দেশের ভেতরে এবং দেশের বাইর থেকে এ অর্থ হাতিয়ে নেয়। উদীয়মান অর্থনীতির দেশ হিসেবে বাংলাদেশও এ ধরণের সাইবার সিকিউরিটি এবং হ্যাকিং সংক্রান্ত নিরাপত্তা হুমকিতে রয়েছে। সম্ভাব্য সাইবার আক্রমনের ঝুঁকি মোকাবেলায় তথ্য প্রযুক্তি ব্যবস্থার নিরাপত্তা বৃদ্ধিকল্পে নিম্নোক্ত ব্যবস্থা গ্রহণ করার জন্য বিশেষভাবে অনুরোধ করা হলো।

বিভিন্ন পেমেন্ট চ্যানেলের মাধ্যমে সম্পাদিত কার্ড-ভিত্তিক লেনদেনের ক্ষেত্রে ঃ

১. SMS এলার্ট সার্ভিসের মাধ্যমে কার্ড-ভিত্তিক সকল লেনদেনের তথ্য তাৎক্ষণিকভাবে গ্রাহককে অবহিত করার লক্ষ্যে গ্রাহকদের SMS সার্ভিসের আওতায় আনয়নের ব্যবস্থা গ্রহণ করতে হবে।
২. লেনদেনের সময় অন্য ব্যাংকের ATM-এ কার্ড আটকে গেলে কার্ড সংশ্লিষ্ট শাখা-কে অবহিত করতঃ ডুপ্লিকেট কার্ডের জন্য আবেদন করার জন্য গ্রাহককে অবহিত করতে হবে।
৩. গ্রাহকদের কার্ড-ভিত্তিক লেনদেনে উৎসাহিত করার জন্য কার্ড ব্যবহারের সুবিধাসমূহ সম্পর্কে গ্রাহকদের জানাতে হবে এবং দৃশ্যমান স্থানে প্রদর্শনের ব্যবস্থা করতে হবে।
৪. কার্ড-ভিত্তিক লেনদেনের ঝুঁকি হ্রাসকল্পে সকল লেনদেনের ক্ষেত্রে যথাযথ সতর্কতা/গোপনীয়তা অবলম্বনসহ সঠিক উপায়ে কার্ড ব্যবহার বিধি সংক্রান্ত নির্দেশনা গ্রাহকদের অবহিত করতে হবে এবং দৃশ্যমান স্থানে প্রদর্শনের ব্যবস্থা করতে হবে।
৫. ATM লেনদেন-সংক্রান্ত সকল ধরনের ফি/চার্জ দৃশ্যমান স্থানে প্রদর্শনের ব্যবস্থা করতে হবে।
৬. POS লেনদেনের ক্ষেত্রে কার্ডধারী-কে স্বহস্তে পিন প্রদান করার জন্য উৎসাহিত করতে হবে।
৭. বুথে কোন ধরনের নতুন যন্ত্র সংস্থাপন/মেরামত কালে ATM বুথে কর্মরত সিকিউরিটি গার্ড এ বিষয়ে ব্যাংকের ক্ষমতাপ্রাপ্ত কর্মকর্তার সাথে যোগাযোগ করে আগন্তুক ব্যক্তি/ব্যক্তিগণের পরিচয় নিশ্চিত করবেন। প্রয়োজনে সংশ্লিষ্ট ব্যাংক কর্মকর্তা ATM বুথে স্বশরীরে উপস্থিত হয়ে এরূপ ব্যক্তি/ব্যক্তিগণের পরিচয় নিশ্চিত করবেন।
৮. ATM বুথসমূহে নিয়োজিত গার্ডদের প্রতারণা-জালিয়াতি প্রতিরোধে করণীয় সম্পর্কে প্রয়োজনীয় প্রশিক্ষণ প্রদান করতে হবে। এছাড়া সানগ্লাস পরিধানকারী, ব্যাগ বহনকারী এবং অন্যান্য সন্দেহজনক গ্রাহকদের ক্ষেত্রে বিশেষ সতর্কতা অবলম্বন করতে হবে।
৯. গ্রাহকদেরকে নগদ লেনদেনে নিরুৎসাহিত করার জন্য ইতোমধ্যে চালুকৃত স্বয়ংক্রিয়/ডিজিটাল (Automated/Digital) পদ্ধতিসমূহ যথা- কার্ড(Card), BEFTN, RTGS ইত্যাদি বিষয়ে যথাযথভাবে অবহিতকরণর এবং শাখার দৃশ্যমান স্থানে স্বয়ংক্রিয় পদ্ধতিসমূহ সম্পর্কে নোটিশ ঝুলানোর ব্যবস্থা গ্রহণ করতে হবে।
১০. BACH, BEFTN, RTGS, SWIFT অপারেশন পরিচালনার সময় যথাযথ সাবধনতা অবলম্বন করতে হবে। এ ক্ষেত্রে সকল নীতিমালা ও গাইডলাইন অনুসরণ করতে হবে।
১১. ফোন, ইমেইল বা ভয়েস এসএমএস এর অনুরোধের প্রেক্ষিতে কোনরুপ গোপনীয় তথ্য প্রদান করা যাবে না। পিন, User Name, Password শেয়ার বা হস্তান্তর করা যাবে না।

নগদ লেনদেনের ক্ষেত্রে ঃ

১. অনলাইন শাখায় কিছু অসাধুচক্র টেলিফোন/মোবাইলের মাধ্যমে বিকেবি প্রধান কার্যালয়ের উর্ধতন কর্মকর্তাদের (GM, AGM, DGM ও অন্যান্য কর্মকর্তা) রেফারেন্স দিয়ে বিভিন্ন ধরনের অযাচিত লেনদেন (অনলাইন ক্যাশ ট্রান্সফার ইত্যাদি) করার চেষ্টা করছে। শাখা ব্যবস্থাপকসহ কর্মকর্তা/কর্মচারীদের অসর্তকতার দরুণ শাখা পর্যায়ে এ ধরণের অনাকাঙ্খিত লেনদেন সংঘঠিত হচ্ছে, যা কোনো অবস্থাতেই কাম্য হতে পারে না। টেলিফোনের মাধ্যমে কোনো ধরণের লেনদেন সংঘটিত না করা (যাহা ব্যাংক বিধি বহির্ভূত ) এবং বিষয়টি সন্দেহজনক হলে তাৎক্ষনিকভাবে কর্তৃপক্ষকে অবহিত পূর্বক যথাযথ আইনানুগ ব্যবস্থা গ্রহন করতে হবে।
২. বিকেবি প্রধান কার্যালয়ের আইসিটিসহ অন্যান্য বিভাগের উর্ধতন কর্মকর্তাদের (GM, AGM, DGM ও অন্যান্য কর্মকর্তা) রেফারেন্স দিয়ে এবং ভয়-ভীতি প্রদর্শন করে যে কোন ধরণের লেনদেন যেমন, ড্যামি লেনদেন বা অনলাইন লেনদেন বন্ধ হয়ে যাবে অথবা সিস্টেম বন্ধ হয়ে যাবে ইত্যাদি অযাচিত কথা বলে কিছু করাতে চাইলে তা থেকে সম্পূর্ন বিরত থাকতে হবে এবং তাৎক্ষনিকভাবে নিয়ন্তনকারী কর্তৃপক্ষকে অবহিত করতে হবে।
৩. শাখার প্রত্যেক এন্ট্রি ইউজার এবং অথোরাইজ ইউজারগণ তাদের দৈনন্দিন সকল কর্মকান্ড দিনশেষে ভাউচারসহ পরীক্ষা করে কার্যালয় ত্যাগ করবেন।
৪. শাখা ব্যবস্থাপক দিনের সকল লেনদেন শেষে ভাউচারসহ ইউজার আইডি ভিত্তিক পরীক্ষা করে সঠিকতা নির্ণয় পূর্বক স্বাক্ষর করবেন।
৫. শাখার প্রত্যেক ইউজারগণ (এন্ট্রি এবং অথোরাইজ ) তাদের আইডি এবং পাস ওয়ার্ড নিজ দায়িত্বে গোপনীয় ভাবে ব্যবহার করবেন যাতে করে একজন ইউজারের পাসওয়ার্ড অন্যজন জানতে না পারেন।
৬. Core Banking Solution (CBS) –এ Login অবস্থায় অথবা Log out না হয়ে User তাঁর Desk ত্যাগ করতে পারবে না।
৭. শাখা ব্যবস্থাপক নিয়মিত শাখার Audit Trail Report Check করবেন। কোন ধরণের অসঙ্গতি প্রতিয়মান হলে প্রয়োজনীয় ব্যবস্থা গ্রহণ করবেন।

৮. Authorization ব্যতিত Cash Counter এর মাধ্যমে Payment করা যাবে না।
৯. Cheque বই যথাযথভাবে সংরক্ষণের জন্য গ্রাহককে সচেতন করতে হবে।
১০. CBS সংশ্লিষ্ট কম্পিউটারে পেনড্রাইভ/ইন্টারনেট ব্যবহার করা যাবে না।
১১. কোন কর্মকর্তা/কর্মচারী বদলি/চাকুরি থেকে ইস্তফা/অবসর গ্রহণ করলে কার্যকরের তারিখেই User ID বন্ধ করার জন্য ই-মেইলের (cbs@krishibank.org.bd) মাধ্যমে অত্র বিভাগ-কে অবহিত করতে হবে।
১২. Online/ Bearer Cheque Payment এর ক্ষেত্রে গ্রাহকের সাথে ফোনালাপ নিশ্চিত করতে হবে।
১৩. প্রতিটি শাখা Day Close Register চালু করবেন এবং Day Close করার পর তথ্যাদি Register এ লিপিবদ্ধ করবেন।
১৪. একই কর্মকর্তা/কর্মচারী একাধিক User এর জন্য আবেদন করতে পারবে না।
১৫. Cash Receive/Payment সংশ্লিষ্ট কাজ ক্যাশিয়ার স্ব User ID ও Password ব্যবহার পূর্বক যথাযথ যাচাই করে সম্পন্ন করবেন।
১৬. User Creation/ Password Reset এর জন্য ই-মেইলের মাধ্যমে অত্র বিভাগ-কে অবহিত করতে হবে।

নেটওয়ার্কের ক্ষেত্রে ঃ

১. শাখার সকল Network Device ও Equipment এর নিরাপত্তা বিধানকল্পে শাখা ব্যবস্থাপক ও কম্পিউটার ইনচার্জ বা ক্ষমতা প্রাপ্ত কর্মকর্তা কর্তৃক নিয়মিত তা পর্যবেক্ষণ করতে হবে। উল্লেখিত যন্ত্রপাতি কোন অবস্থায় খোলা ও অরক্ষিত জায়গা, জানালার পাশে, পানি গড়িয়ে পড়ে এমন স্থানে বা মেঝের উপর রাখা যাবে না।
২. শাখার IP Address সহ অন্যান্য যাবতীয় তথ্যাদির গোপনীয়তা রক্ষা করতে হবে। সংশ্লিষ্ট নহে এমন কারো কাছে কোনঅবস্থায় এতদসংক্রান্ত তথ্য প্রকাশ করা যাবে না।
৩. অননুমোদিত Wireless Device, Network Switch ইত্যাদি সংযোগের মাধ্যমে Network Structure এর কোনরুপ পরিবর্তন বা পরিবর্ধন করা যাবে না।
৪. ব্যক্তিগত বা অননুমোদিত pc/ Laptop TAB, PDA, Mobile Phone, Modem, Pendrive শাখার নেটওয়ার্কে সংযুক্ত করা যাবে না।

০৩। সাইবার নিরাপত্তা ও লেনদেন ঝুঁকি সম্পর্কে নিজস্ব সকল কর্মকর্তা-কর্মচারীকে সচেতন ও প্রশিক্ষিত করার লক্ষ্যে বাংলাদেশ ব্যাংক কর্তৃক জারিকৃত " Guidelines on ICT Security for Banks and Non Financial Institutions " বিষয়ক পলিসি ও পিএসডি সার্কুলার-০১/২০১৮, ০৪/২০১৭, ০২/২০১৬ এবং বাংলাদেশ কৃষি ব্যাংক কর্তৃক জারিকৃত " ICT Security Policy "ও আইসিটি পরিপত্র-০২/২০১৭, অনুসরণ করতে হবে।

০৪। আইসিটি সিকিউরিটি সংক্রান্ত নীতিমালা পরিপালন না করার ফলে শাখা পর্যায়ে যদি কোনো ধরনের অনাকাঙ্খিত পরিস্থিতির সৃষ্টি হয়,তবে তাঁর দায়দায়িত্ব সংশ্লিষ্ট শাখার ইউজার, অথোরাইজড ইউজার ও শাখা ব্যবস্থাপকের উপর বর্তাবে। বিষয়টি সর্বাধিক গুরুত্ব সহাকারে বিবেচনা করতে হবে।

আপনার বিশ্বস্ত

Rashid 20.8.17

(মোঃ মামুনুর রশীদ)
উপ-মহাব্যবস্থাপক

সদয় অবগতি ও প্রয়োজনীয় ব্যবস্থা গ্রহণের জন্য অনুলিপি ঃ

০১। স্টাফ অফিসার, মহাব্যবস্থাপক মহোদয়ের দপ্তর, সকল বিভাগীয় কার্যালয়, বাংলাদেশ কৃষি ব্যাংক।
০২। মুখ্য আঞ্চলিক/ আঞ্চলিক ব্যবস্থাপক, সকল মুখ্য আঞ্চলিক/ আঞ্চলিক কার্যালয়, বাংলাদেশ কৃষি ব্যাংক ।
০৩। নথি/ মহানথি।