DCB BANK

সংযুক্তি 7: গ্রাহক সচেতনতা - সাইবার থ্রেটস এবং প্রতারণা

এটি লক্ষ্য করা গেছে যে অসাধু ব্যক্তিগণ সোশ্যাল মিডিয়া কৌশল, মোবাইল ফোন কল ইত্যাদি সহ উদ্ভাবনী পদ্ধতি ব্যবহার করে জনসাধারণকে প্রতারণা ও বিভ্রান্ত করছে। এর পরিপ্রেক্ষিতে, ডিসিবি ব্যাঙ্ক জনসাধারণকে প্রতারণামূলক বার্তা, ভুয়ো কল, অপরিচিত লিঙ্ক, মিথ্যা বিজ্ঞপ্তি, অননুমোদিত কিউআর কোড ইত্যাদি সহ যে কোনো উপায়ে ব্যাঙ্ক এবং আর্থিক পরিষেবা প্রদানকারীদের কাছ থেকে ছাড় / দ্রুত প্রতিক্রিয়া নিশ্চিত করতে সাহায্য করার প্রতিশ্রুতি প্রদানকারীদের থেকে সচেতন হওয়ার জন্য সতর্ক করে।

প্রতারকরা গোপন তথ্য যেমন ব্যবহারকারী আইডি, লগ-ইন / লেনদেনের পাসওয়ার্ড, ওয়ান টাইম পাসওয়ার্ড (ওটিপি), ডেবিট / ক্রেডিট কার্ডের বিবরণ যেমন পিন, সিভিভি, মেয়াদ শেষ হওয়ার তারিখ এবং অন্যান্য ব্যক্তিগত তথ্য প্রাপ্ত করার চেষ্টা করে থাকে। প্রতারকদের দ্বারা ব্যবহৃত সাধারণ পদ্ধতিগুলি হল:

- ভিশিং – কেওয়াইসি-আপডেট করা, অ্যাকাউন্ট / সিম কার্ড আনব্লক করা, ডেবিট করা অর্থরাশি ক্রেডিট করা ইত্যাদির অজুহাতে গ্রাহকদের গোপন তথ্য শেয়ার করতে প্রলুব্ধ করার জন্য ব্যাঙ্ক / নন-ব্যাঙ্ক ই-ওয়ালেট প্রদানকারী / টেলিকম পরিষেবা প্রদাকারীদের কাছ থেকে আসা ফোন কলগুলি।
- ফিশিং – প্রতারণামূলক ইমেল এবং / অথবা এসএমএস যা গ্রাহকদের প্রতারিত করার জন্য এইরকমভাবে ডিজাইন করা হয়েছে যে যেন যোগাযোগটি তাদের ব্যাঙ্ক / ই-ওয়ালেট প্রদানকারীর কাছ থেকে এসেছে এবং তাতে গোপন তথ্য বের করার জন্য লিঙ্ক থাকে।
- রিমোট অ্যাক্সেস – গ্রাহকদের তাদের মোবাইল ফোন / কম্পিউটারে একটি অ্যাপ্লিকেশন ডাউনলোড করার জন্য প্রলুব্ধ করে যা গ্রাহকের ডিভাইসে থাকা তথ্য উপলব্ধ করতে পারে।
- টাকা পাওয়ার জন্য 'আপনার ইউপিআই পিন লিখুন'-এর মত বার্তা বা মেসেজ সহ জাল অর্থপ্রদানের অনুরোধ পাঠিয়ে ইউপিআই-এর 'সংগ্রহ অনুরোধ' বৈশিষ্ট্যের অপব্যবহার করা।
- ওয়েব পেজ / সোশ্যাল মিডিয়াতে ব্যাঙ্ক / ই-ওয়ালেট প্রদানকারীদের জাল যোগাযোগ নম্বর এবং সার্চ ইঞ্জিন ইত্যাদি দ্বারা দর্শানো হয়।

ডিসিবি ব্যাঙ্ক যে কোনো ডিজিটাল (অনলাইন / মোবাইল) ব্যাঙ্কিং / পেমেন্ট লেনদেন পরিচালনা করার সময় সকল যথাযথ সতর্কতা অবলম্বন করে নিরাপদ ডিজিটাল ব্যাঙ্কিং প্র্যাক্টিস করার জন্য জনসাধারণকে অনুরোধ করে। এই সতর্কতা আর্থিক এবং / অথবা অন্যান্য ক্ষতি প্রতিরোধে সাহায্য করবে।

নিরাপদ ডিজিটাল ব্যাঙ্কিং প্র্যাক্টিস

- আপনার অ্যাকাউন্টের বিবরণ যেমন, অ্যাকাউন্ট নম্বর, লগ-ইন আইডি, পাসওয়ার্ড, পিন, ইউপিআই-পিন, ওটিপি, এটিএম / ডেবিট কার্ড / ক্রেডিট কার্ডের বিশদ বিবরণ কারোর সাথে শেয়ার করবেন না, একনকি ব্যাঙ্কের কর্মকর্তাদের সাথেও নয়, তারা যদি প্রকৃত ব্যক্তির মত আচরণ করেন তাও।
- কেওয়াইসি আপডেট না করার অজুহাতে আপনার অ্যাকাউন্ট ব্লক করার হুমকি প্রদানকারী ফোন কল / ইমেল এবং এটি আপডেট করার জন্য লিঙ্কে ক্লিক করার পরামর্শ দেওয়া প্রতারকদের সাধারণ একটি পদ্ধতি। কেওয়াইসি আপডেট করার / ত্বরান্বিত করার জন্য অফারগুলিতে কোনো প্রতিক্রিয়া জানাবেন না বা উত্তর দেবেন না। সবসময় আপনার ব্যাঙ্ক / এনবিএফসি / ই-ওয়ালেট প্রদানকারীর অফিসিয়াল ওয়েবসাইট অ্যাক্সেস করুন বা শাখায় যোগাযোগ করুন।
- আপনার ফোন বা ডিভাইসে অজানা বা অপরিচিত কোনো অ্যাপ ডাউনলোড করবেন না। অ্যাপটি গোপনে আপনার গোপন তথ্য উপলব্ধ করতে পারে।
- অর্থের প্রাপ্তি সম্পর্কিত লেনদেনের জন্য বারকোড বা কিউআর কোড স্ক্যান করা বা এমপিন প্রদান করার প্রয়োজন হয় না। তাই যদি এগুলি কেউ করতে বলে তাহলে সতর্কতা অবলম্বন করার উচিত।
- যোগাযোগের বিশদ বিবরণের জন্য সর্বদা ব্যাঙ্ক / এনবিএফসি / ই-ওয়ালেট প্রদানকারীর অফিসিয়াল ওয়েবসাইট অ্যাক্সেস করুন। ইন্টারনেট সার্চ ইঞ্জিনে যোগাযোগের নম্বরগুলি প্রতারণামূলক হতে পারে।
- বানানের ত্রুটির জন্য ইমেল এবং এসএমএস-এ প্রাপ্ত ইউআরএল এবং ডোমেন নামগুলিকে পরীক্ষা করুন। অনলাইন ব্যাঙ্কিংয়ের জন্য কেবলমাত্র যাচাইকৃত, সুরক্ষিত এবং বিশ্বস্ত ওয়েবসাইট এবং অ্যাপ ব্যবহার করুন, অর্থাৎ, ''https'' দিয়ে শুরু হওয়া ওয়েবসাইট। একটি সন্দেহজনক ইউআরএল বা ওয়েবসাইট সম্বন্ধে অবিলম্বে স্থানীয় পুলিশ কর্তৃপক্ষ / সাইবার ক্রাইম ব্রাঞ্চকে অবহিত করা উচিত।

- যদি আপনি শুরু করেননি এইরকম একটি লেনদেনের জন্য আপনার অ্যাকাউন্ট থেকে ডেবিট করার জন্য একটি ওটিপি পান, তাহলে অবিলম্বে আপনার ব্যাঙ্ক / ই-ওয়ালেট প্রদানকারীকে জানান। আপনি যদি লেনদেন না করার জন্য একটি ডেবিট এসএমএস পান, তাহলে অবিলম্বে আপনার ব্যাঙ্ক / ই-ওয়ালেট প্রদানকারীকে জানান এবং ইউপিআই সহ ডেবিটের সমস্ত মোড ব্লক করুন। আপনি যদি আপনার অ্যাকাউন্টে কোনো প্রতারণামূলক কার্যকলাপ সন্দেহ করেন, তাহলে ইন্টারনেট / মোবাইল ব্যাঙ্কিংয়ের জন্য সক্রিয় সুবিধাভোগী তালিকায় যোগ আছে কিনা দেখে নিন।
- আপনার ব্যাঙ্ক / ই-ওয়ালেট অ্যাকাউন্টের সাথে লিঙ্ক করা আপনার ইমেল-এর পাসওয়ার্ড করবেন না। ই-কমার্স / সোশ্যাল মিডিয়া সাইট এবং আপনার ব্যাঙ্ক অ্যাকাউন্ট এবং আপনার ব্যাঙ্ক অ্যাকাউন্টের সাথে লিঙ্ক করা ইমেল-এর সাধারণ পাসওয়ার্ড রাখবেন না। পাবলিক, ওপেন বা ফ্রি ওয়াই-ফাই বা ইন্টারনেট নেটওয়ার্কের মাধ্যমে ব্যাঙ্কিং করা থেকে বিরত থাকুন।
- ইউজার আইডি হিসাবে আপনার ইমেল-এর সাথে কোনও ওয়েবসাইট / অ্যাপ্লিকেশনে নিবন্ধন করার সময় আপনার ইমেল পাসওয়ার্ডটিকে ''পাসওয়ার্ড'' শব্দটি হিসাবে সেট করবেন না। আপনার ইমেল অ্যাক্সেস করার জন্য ব্যবহৃত পাসওয়ার্ড, বিশেষ করে যদি আপনার ব্যাঙ্ক অ্যাকাউন্টের সাথে লিঙ্ক করা থাকে, তা অদ্বিতীয় এবং কেবলমাত্র ইমেল অ্যাক্সেসের জন্য ব্যবহার করা উচিত এবং অন্য কোনো ওয়েবসাইট বা অ্যাপ্লিকেশন অ্যাক্সেস করার জন্য নয়।
- বিদেশ থেকে প্রেরিত অর্থরাশি, কমিশন প্রাপ্তি বা লটারি জেতার জন্য আরবিআই-এর কাছে আপনার তরফে টাকা জমা দেওয়ার পরামর্শ সম্বন্ধে বিভ্রান্ত হবেন না।
- আপনার আর্থিক পরিষেবা প্রদানকারীর কাছ থেকে সতর্কতার জন্য নিয়মিতরূপে আপনার ইমেল এবং ফোন মেসেজগুলি যাচাই করুন। আপনার অ্যাকাউন্টে যে কোনো অননুমোদিত লেনদেন আপনার ব্যাঙ্ক / এনবিএফসি / পরিষেবা প্রদানকারীকে অবিলম্বে কার্ড, অ্যাকাউন্ট, ওয়ালেট ব্লক করে আরও বেশি ক্ষতি বা লোকসান রোধ করার জন্য রিপোর্ট করুন।
- আপনার এটিএম, ডেবিট এবং ক্রেডিট কার্ডগুলিকে সুরক্ষিতভাবে রাখুন এবং লেনদেনের জন্য দৈনিক সীমা সেট করুন। আপনি সীমা সেট করতে পারেন এবং আন্তর্দেশীয় / আন্তর্জাতিক ব্যবহারের জন্য সক্রিয় / নিষ্ক্রিয় করতে পারেন। এটি জালিয়াতির কারণে হওয়া ক্ষতি বা লোকসানকে সীমিত করতে পারে।