HSBC

ऑनलाईन सुरक्षा आणि सुरक्षित वापरासाठी मार्गदर्शक सूचना

तुमचे ऑनलाईन बँकिंग एकत्रितपणे सुरक्षित ठेवण्यासाठी आम्ही तुम्हाला अशा प्रकारे मदत करू शकतो.

एक बँक म्हणून, आम्हाला सुरक्षिततेचा विचार करण्याची सवय आहे. इंटरनेटच्या वृद्धीमुळे आपणा सर्वांनाच जास्त पर्याय मिळवून दिलेली असले, तरी त्यातून नवे धोकेसुद्धा उत्पन्न होत आहेत ज्यांपासून सुरक्षा मिळवायला हवी. एसएचबीसीमध्ये, तुमचे खाते कोणत्याही अनधिकृत वापरापासून सुरक्षित करण्यासाठी आम्ही ह्या उद्योगक्षेत्रातील मानांकित सुरक्षितता तंत्रज्ञान आणि कार्यपद्धतींचा अवलंब करतो व तीन प्रमुख क्षेत्रांवर भर देतो – खासगीपणा, तंत्रज्ञान आणि ओळख.

तुमचे ऑनलाईन बँकिंग सुरक्षित ठेवण्यासाठी आम्ही काय व्यवस्था केली आहे आणि तुमची स्वतःची ऑनलाईन सुरक्षा सुधारण्यासाठी तुम्ही कोणती पावले उचलू शकता ह्या संदर्भात माहिती खालील प्रमाणे

फसवणुकीचे प्रकार

फसवणारी व्यक्ती अनेक प्रकारे तुम्हाला भुलवून अथवा लक्ष विचलीत करून तुमची वैयक्तिक माहिती आणि सुरक्षा तपशील तिला देण्यास प्रवृत्त करू शकते. मग हे तपशील वापरून ती व्यक्ती तुमची बँकेकडे असलेली आर्थिक माहिती प्राप्त करू शकते, आणि तुमच्या खात्यातून गैर व्यवहार करू शकते.

बँक खात्या संदर्भात गैर व्यवहाराचे सर्वसाधारण प्रकार खालील प्रमाणे

क्रेडिट / डेबिट कार्ड स्किमिंग किंवा क्लोनिंग

फसवणाऱ्या व्यक्ती तुमच्या क्रेडिट किंवा डेबिट कार्डवरील चुंबकीय पट्टीवरील माहिती चोरू शकतात. हे करण्यासाठी त्या एटीएमच्या कार्ड स्लॉटमध्ये स्किमिंग यंत्रे दडवून ठेवतात किंवा एखाद्या व्यापाऱ्याच्या दुकानात कार्ड स्वाईप करण्याआधी तुमचे लक्ष नसल्याचा फायदा घेतात. ही यंत्रे तुमच्या कार्डचे तपशील स्कॅन करून जतन करतात. त्याच बरोबर पिन चोरण्यासाठी, फसवणाऱ्या व्यक्ती एटीएममध्ये किंवा व्यापारी आस्थापनामध्ये एखाद्या न दिसणाऱ्या ठिकाणी कॅमेरा दडवून ठेवू शकतात.

युपीआय ॲप्समधील घोटाळा किंवा पेमेंट फसवणूक

फसवणाऱ्या व्यक्ती त्यांच्या खात्यामध्ये पैसे हस्तांतरित करून घेण्यासाठी तुम्हाला मेसेजिंग ॲप्समधून QR कोड्स पाठवून तुम्हाला तो QR कोड स्कॅन करायला सांगू शकतात किंवा तुम्हाला पैसे "स्वीकार करण्याची" एक विनंती संमत करायला सांगू शकतात. ते तुम्हाला एक खोटी कहाणी सांगून भुलवायचा प्रयत्न करू शकतात, उदा. ते असे म्हणतील की तुम्ही विकत असलेले उत्पादन त्यांना विकत घ्यायचे आहे, अथवा ते बँक किंवा कंपनी अधिकारी असल्याचा बनाव करून पैशांचा परतावा करायचा आहे, दावा न केलेल्या कॅशबॅक ऑफर्स किंवा रीवॉर्ड पॉइंट्स तुम्हाला द्यायचा आहे असा आव आणू शकतात. भोळ्या व्यक्ती QR कोड स्कॅन करून किंवा त्यांचा युपीआय पिन वापरून त्यांची "स्वीकार करण्याची" विनंती संमत करून आपले पैसे फसवणाऱ्या व्यक्तीच्या खात्यात पाठवून देऊ शकतात. अशा प्रकारे आपल्या खात्यात पैसे जमा होण्या ऐवजी खात्यातून वजा होतात.

व्यावसायिक ईमेल्स आणि मेसेजिंग ॲप्समार्फत पेमेंट फसवणूक

फसवणाऱ्या व्यक्ती तुमचे ईमेल किंवा चॅट हॅक करून, किंवा एन्क्रिप्ट न केलेले संदेश अंतर्छेदित (हॅक) करून तुमच्याविषयीची माहिती जाणून घेऊ शकतात. ते तुम्हाला हॅक केलेल्या तुमच्या परिचयाच्या व्यक्तीच्या बनावट ईमेल आयडीवरून संदेश पाठवू शकतात, आणि कोणा जिव्हाळ्याच्या व्यक्तीला रुग्णालयात दाखल करून घ्यायचे आहे किंवा एखादे थकित बिल नव्या खात्यामध्ये भरायचे आहे अशा तुम्हाला वरकरणी खऱ्याखुऱ्या वाटणाऱ्या कारणांसाठी घाईघाईने पैसे पाठवायला सांगू शकतात. ह्या मागणीस भुलणारे लोक अशा घाईघाईत केलेल्या विनंतीमुळे किंवा विश्वासातील व्यक्ती मागत आहे असे वाटल्याने पैसे भरण्यास प्रवृत्त होऊ शकतात. आणि अशा व्यक्तीने स्वतःच पैसे भरले/पाठवले असल्याने बँकेने त्यांना पाठवलेल्या व्यवहाराच्या (एसएमएस) संदेशांमुळे ते सावध होत नाहीत. ह्या कारणामुळे अशा प्रकारची फसवणूक ओळखणे कठीण होऊन बसते.

खोटे संपर्क क्रमांक

फसवणाऱ्या व्यक्ती बँकांच्या आणि सेवा पुरवठादारांच्या संपर्क केंद्रांचे खोटे संपर्क तपशील पुरवू शकतात. भोळ्या व्यक्ती सर्च इंजिनचा वापर करून संपर्क तपशील शोधू शकतात आणि चुकीच्या खोट्या क्रमांकावर कॉल करू शकतात. मग त्यांना "पडताळणी प्रक्रियेतून" पार करण्याच्या नावाखाली त्याची व बँक खात्याची गोपनीय माहिती हस्तगत केली जाते आणि बँक खात्यातील संवेदनशील माहिती सांगण्यास भुलवले जाईल.

तुम्ही नेहमी बँकेच्या किंवा सेवा पुरवठादाराच्या अधिकृत संकेतस्थळावर जाऊनच तुम्हाला हवे असलेले संपर्क बँकेचा संपर्क क्रमांक शोधताना सतर्क रहाणे आवश्यक आहे.

फिशींग किंवा स्पुफिंग ई मेल्स

फसवणाऱ्या व्यक्ती त्यांना जमतील तेवढ्या ईमेल ॲड्रेसेसना एक ईमेल पाठवून फिशींग करू शकतात. ते अनेकदा बँक, ऑनलाईन पेमेंट सेवा, विक्रेता किंवा तत्सम एखादी सेवा देणारी अधिकृत संस्था असल्याचा बनाव करतात. ते स्वतःचा बनावट आयडी तयार करू शकतात ज्यामुळे ईमेल पाठवणारी व्यक्ती फसवणारी नसून दुसरीच कोणी आहे असे दिसते.

तुम्ही अशा फिशींग घोटाळ्यांपासून स्वतःला वाचवू शकता, ह्यासाठी वैयक्तिक किंवा आर्थिक माहिती विचारणाऱ्या ईमेल्सना प्रत्युत्तर देऊ नका. तुम्ही संशयास्पद दिसणाऱ्या ईमेल्समधील लिंकसुद्धा कधीही उघडू नका.

एचएसबीसी तुम्हाला कधीही ईमेलमार्फत तुमची वैयक्तिक माहिती किंवा सुरक्षा तपशील उघड करण्याची विचारणा करणार नाही. जर तुम्हाला असा ईमेल आला जो एचएसबीसी कडून असल्याचा दावा करत असेल, तर त्यास प्रतिसाद देऊ नका. तो ईमेल तत्काळ हटवा. आणि लक्षात ठेवा, कधीही तुमची माहिती कोणालाही देऊ नका – उदा. तुमचे युझरनेम, पासवर्ड किंवा इतर सुरक्षा तपशील.

मनी म्युल किंवा जास्तीची कमाई देऊ करणारे ईमेल घोटाळे

मनी म्युल घोटाळ्यामध्ये, फसवणारी व्यक्ती तुम्हाला पैसे हस्तांतरित करण्यासाठी मदत मागू शकते. ते तुमच्या खात्यामध्ये पैसे हस्तांतरित करण्याची विचारणा करू शकतात, व तुम्ही त्यांना ते दुसऱ्या खात्यात हस्तांतरित करण्यास मदत करावी असे सांगतात. त्याबदल्यात, ते म्हणतील की ते तुम्हाला कमिशन देतील.

तुम्ही अशा विनंत्यांकडे दुर्लक्ष करावे कारण हे प्रकार अनेकदा गुन्हेगारी स्वरूपाचे असतात, उदा. मनी लाँडरिंग म्हणजेच काळा पैसा पांढरा करणे. जाणीवपूर्वक ह्यामध्ये सहभाग घेणारी कोणतीही व्यक्ती अशा गुन्ह्यातील साथीदार मानली जाऊ शकते आणि तिच्यावर खटलाही भरला जाऊ शकतो. लक्षात ठेवा, जर एखादा प्रस्ताव खरा वाटणार नाही इतका चांगला असेल, तर बहुधा ती फसवणूकच आहे!

आगाऊ शुल्क फसवणूक ("419" घोटाळे)

फसवणाऱ्या व्यक्ती तुम्हाला अनाहूत पत्रे किंवा ईमेल्स पाठवू शकतात ज्यामध्ये ते तुम्हाला सहसा अमेरिकन डॉलर्समधील अतिशय मोठी रक्कम स्थलांतरित करण्यास त्यांना मदत केल्यास मोठे इनाम देऊ करतात. प्रत्यक्षात ह्या फसवणाऱ्या व्यक्तींना तुमचे बँकेचे तपशील हवे असतात. ते सहसा तुम्हाला व्यवहार पूर्ण करण्यासाठी थोडे शुल्क, काही कर किंवा लाच भरण्यास सांगतात – हे आहे आगाऊ शुल्क. ह्यास बळी पडणारे लोक आपला हा पैसा फसव्या माणसांकडे गमावून बसतात.

जर तुम्हाला संशय असेल की इतर कोणा व्यक्तीकडे तुमचे बँकेचे तपशील आले आहेत, तर तुम्ही ऑनलाईन बँकिंगमध्ये लॉगिन करून तुमचा पासवर्ड तत्काळ बदलावा. तुम्ही आम्हालाही शक्य तितक्या लवकर कॉल करून सावध करावे. आमच्या लाइन्स 24/7* चालू असतात. तुम्हाला इथे आमच्या हॉटलाइन क्रमांकाची यादी मिळेल.

सोशल मीडिया हॅक

फसवणाऱ्या व्यक्ती फेसबुक, व्हॉट्सॲप किंवा इन्स्टाग्राम अशा सोशल मीडिया मंचावर जवळचे मित्र किंवा नातेवाईक असल्याची बतावणी करून तुमच्याकडे पैसे पाठवण्याची विचारणा करू शकतात. अशी मागणी खरी आहे की नाही हे तपासण्यासाठी तुम्ही त्यांना फोन अथवा इतर माध्यमांतून संपर्क साधून खात्री करू शकता.

विशिंग कॉल्स

फसवणाऱ्या व्यक्ती बँक कर्मचारी किंवा ग्राहक सेवा अधिकारी असल्याची बतावणी करून संभाव्यत: बळी पडू शकणाऱ्या लोकांना कॉल करून त्यांच्या बँक तपशिलांसारखी संवेदनशील माहिती चोरू शकतात. अशा बळी पडणाऱ्या लोकांचा विश्वास संपादित करण्यासाठी, गुन्हेगार सहसा त्यांना थोडी अशी वैयक्तिक माहिती सांगतात जी "सामाजिक अभियांत्रिकीमार्फत" चोरलेली असते. थोडा विश्वास संपादित केल्यानंतर, फसवणाऱ्या व्यक्ती कदाचित काही खास सेवा किंवा मोबदला देऊ करतील, व बदल्यात अशी आशा बाळगतील की लोक त्यांना त्यांचे बँक तपशील आणि वन टाइम पासवर्ड्स (ओटीपी) इ. गोपनीय माहिती पुरवतील.

ट्रोजन व्हायरसेस

फसवणाऱ्या व्यक्ती तुम्हाला अनाहूत ईमेल्स पाठवू शकतात ज्यामध्ये अशा फाइल्स, पाने किंवा अटॅचमेंट्स असतात ज्या तुम्हाला उघडण्याची विनंती केली जाते. पण त्या उघडल्यावर गुप्तपणे तुमच्या कम्प्युटरवर एक प्रोग्रॅम इन्स्टॉल होईल जो तुमच्या ऑनलाईन क्रियांवर देखरेख करतो, आणि तुम्ही विविध वेबसाइट्सवर काय टाइप करता हे देखील पाहतो. म्हणजे तुम्ही जेव्हा ऑनलाईन खरेदी करताना तुमचे क्रेडिट कार्ड तपशील प्रविष्ट करता. तेव्हा फसवणाऱ्या व्यक्तींना तुम्ही प्रविष्ट करत असलेली माहिती पाहता येते.

ऑनलाईन सुरक्षेसाठी एचएसबीसीने उचललेली पावले

बहुस्तरीय लॉग ऑन पडताळणी

तुमची आर्थिक माहिती एका जटिल मेळाने सुरक्षित केलेली असते – एक अनोखे युझरनेम आणि पासवर्ड, तसेच तुमच्या भौतिक सुरक्षितता यंत्राद्वारे तयार होणारा एकवेळचा सुरक्षा संकेत किंवा डिजिटल सिक्युअर की.

व्यवहार पडताळणी

कार्ड्सवरील 3डी सुरक्षित व्यवहार हे व्यवहार आणि पेमेंट यंत्रणेमधील विश्वास सुरक्षित करण्यास मदत करतात. व्यवहारासाठी तयार झालेला ओटीपी कोणालाही कधीही देऊ नका.

128-बिट सिक्युअर सॉकेट लेयर (एसएसएल) एन्क्रिप्शन

एचएसबीसी इंटरनेट बँकिंग सत्रादरम्यान पारेषित होणाऱ्या माहितीसाठी 128-बिट सिक्युअर सॉकेट लेयर (एसएसएल) एन्क्रिप्शन वापरते, जे एन्क्रिप्शनसाठी स्वीकृत उद्योगक्षेत्र मानक आहे.

आपोआप "टाइम-आऊट" वैशिष्ट्य

सुरक्षेचा उपाय म्हणून, तुमचे इंटरनेट बँकिंग सत्र काही काळ वापर न झाल्यास आपोआप बंद होईल किंवा टाइम आऊट होईल. तुमचे काम झाले की तुम्ही नेहमी तुमचे इंटरनेट बँकिग सत्र बंद करावे.

सुरक्षा संयंत्र / डिजिटल सिक्युअर की

तुमचे भौतिक सुरक्षा संयंत्र / डिजिटल सिक्युअर की हे ऑनलाईन सुरक्षिततेला नव्या उंचीवर नेऊन ठेवतात. तुमच्या खात्यावर लॉग ऑन करण्यासाठी तुम्ही नेहमीप्रमाणे तुमचे विद्यमान युझरनेम आणि पासवर्ड प्रविष्ट करावे, व त्यानंतर तुमच्या तुमचे भौतिक सुरक्षा संयंत्र किंवा तुमच्या डिजिटल सिक्युअर कीद्वारे तयार झालेला अनोखा सुरक्षा संकेत प्रविष्ट करावा. तुम्ही तुमचे इंटरनेट बँकिंग चालू करता तेव्हा ही 2 पदी अधिस्वीकृती प्रक्रिया तुम्हाला सुरक्षिततेचा वाढीव स्तर मिळवून देते.

ऑनलाईन सुरक्षेतील तुमची भूमिका

इंटरनेट बँकिंग सुरक्षिततेची खात्री करण्यासाठी काय करावे व काय करू नये ह्या बाबी जाणून आचरणात आणा.

काय करावे

- तुमचा कॉम्प्युटर नवीन अँटि व्हायरस आणि फायरवॉल प्रोटेक्शन सॉफ्टवेअरने सर्वकाळ सुरक्षित आहे ह्याची खात्री करा. तुमच्याकडे नवीनतम सुरक्षा असल्याची खात्री करण्यासाठे अद्यतने नियमितपणे डाऊनलोड करत राहा.
- असा पासवर्ड निवडा जो तुमच्या लक्षात राहील पण इतर कोणालाही सहज ओळखता येणार नाही. ज्या पासवर्डमध्ये अक्षरांचा आणि अंकांचा मेळ साधलेला असतो ते सहसा ओळखण्यास कठीण असतात (उदा. a7g3cy91)
- तुमचा इंटरनेट बँकिंग पासवर्ड नियमितपणे बदलत राहा.
- फिशींग ईमेल्सपासून सावध राहा. नेहमी संपूर्ण ईमेलचा पत्ता काळजीपूर्वक वाचा, सर्व अक्षरे आणि चिह्नांसहित.
- फिशींग अगदी सारख्या दिसणाऱ्या ईमेल ॲड्रेसने केले जाते, उदा. hsdc.co.in किंवा hsbcbank.com. तुमचा माऊस पॉइंटर युआरएलवर न्या आणि त्याचे खरे प्रस्थान ठिकाण जाणून घ्या; हे तुमच्या ब्राऊझरच्या डावीकडच्या खालील बाजूस प्रदर्शित होते. जर पत्त्याशी ठिकाण जुळत नसेल तर लिंक उघडू नका. स्पेलिंगमधील चुका, चुकीचे व्याकरण किंवा युआरएलमधील अक्षरांची अदलाबदल अशा खुणांबाबत सावध राहा.
- वापरात नसलेले लाभार्थी जोडलेले असल्यास त्यांना खात्यामधून काढून टाका.
- लॉग ऑन तपशील लक्षात ठेवणारी तुमच्या कॉंप्युटरवरील किंवा ब्राऊझरवरील सुविधा निष्क्रीय करा.
- तुमची सिस्टीम आणि वेब ब्राऊझर अद्ययावत ठेवा. उत्पादक सहसा त्यांच्या सिस्टीम्समध्ये आणि ब्राऊझर्समध्ये कमतरता आढळून आल्या की सिक्युरिटी पॅचेस प्रसृत करतात. तुमच्या सॉफ्टवेअर पुरवठादाराकडून अशी अद्यतने मिळतात का हे नियमितपणे तपासत राहा.
- एचएसबीसीच्या संकेतस्थळावर येण्यासाठी नेहमी तुमच्या ब्राऊझरमध्ये युआरएल टाईप करा.
- बंद कुलुपाचे चिह्न आणि साइट सर्टिफिकेट तपासा. तुम्ही एचएसबीसी ऑनलाईन बँकिंगमध्ये लॉग इन करता तेव्हा तुमच्या ब्राऊझरच्या तळाशी असलेल्या बंद कुलुपाच्या चिह्नावर डबल क्लिक करा साइट सर्टिफिकेट एचएसबीसीच्या मालकीचे आहे ह्याची खात्री करा. ह्यामुळे तुम्ही एका "खोट्या" संकेतस्थळावर तुमचे तपशील प्रविष्ट करून लुबाडले जाणार नाही ह्याची खात्री होईल.
- तुमची खाती नियमितपणे तपासा. जर कोणताही व्यवहार संशयास्पद वाटला, तर तपशील नोंदवा आणि आम्हाला कॉल करा.
- ऑनलाईन बँकिंग केल्यानंतर नेहमी लॉग आऊट करा. फक्त संकेत स्थळावरील वेबपृष्ठ बंद करू नका कधीही सेवेमध्ये लॉग्ड इन असताना तुमचा पीसी दुर्लक्षित ठेवून उठून जाऊ नका.
- तुम्ही बँकांचे, ऑनलाईन खरेदी संकेतस्थळांचे, इ. ग्राहक सेवा क्रमांक शोधत असाल तर इंटरनेटवर सूज्ञपणे शोध घ्या. फसवणाऱ्या व्यक्ती शोध परिणामांमध्ये गडबड करून ते वापरत असलेले मोबाईल क्रमांक परिणामांत दिसतील अशी व्यवस्था करतात. तुम्ही कदाचित ह्यास भुलून बँकेच्या ग्राहक सेवा क्रमांकावर किंवा ई-कॉमर्स संकेतस्थळाला कॉल करण्याऐवजी फसवणाऱ्या व्यक्तीला कॉल कराल.
- तुमच्या बँकेचे संपर्क केंद्र क्रमांक तुमच्या डिव्हायसेसवर जतन करा किंवा तुमच्या क्रेडिट / डेबिट कार्डच्या मागे लिहिलेला क्रमांक पाहा.
- तुमच्या वैयक्तिक कंप्युटरवरील किंवा मोबाईल डिव्हायसेसवरील स्क्रीन शेअर करणारी ॲप्स वापरताना सावध राहा. फसवणाऱ्या व्यक्ती तुम्हाला अशी ॲप्लिकेशन्स डाऊनलोड करण्यास भाग पाडू शकतील आणि दुरून तुमच्या डिव्हाइसवर नियंत्रण ठेवू शकतील, आणि तुमच्या खात्यांमधून पेमेंट्सही करू शकतील.
- तुमचे इंटरनेट कनेक्शन सुरक्षित करा. तुमचे होम वायरलेस नेटवर्क नेहमी पासवर्डने सुरक्षित ठेवा.
- नेहमी अशा योजना / प्रस्तावांपासून सावध राहा ज्यांमध्ये तुम्हाला तुमच्या खात्यामध्ये पैसे जमा करावे लागतात, अगदी कमिशन किंवा मदतीच्या स्वरूपातही. फसवणाऱ्या व्यक्ती गुन्ह्यातून मिळवलेले पैसे तुमच्या खात्यात पाठवून तुम्हाला तो पैसा हस्तांतरित करण्यास किंवा त्यांना रोख स्वरूपात पुरवण्यास सांगू शकतील. फसवणाऱ्या व्यक्तींना ते स्वत: पैशाच्या प्रवाहामधील त्यांच्या सहभागाचा पुरावा नको असतो म्हणून ते तुमचा मनी म्युलसारखा वापर करू शकतात.
- आपल्या संदर्भात झालेल्या फसवणुकीची माहिती देण्यासाठी तत्काळ बँकेशी संपर्क साधा.

काय करू नये

- असा पासवर्ड निवडू नका जो तुम्ही इतर सेवांसाठी वापरता. तुमचा पासवर्ड इंटरनेट बँकिंगसाठी वेगळा ठेवावा.

- ईमेल/एसएमएस मधील लिंक्स चुकून क्लिक झाल्यामुळे उघडणाऱ्या वेबपेजेसवर तुमचा युझरआयडी, पासवर्ड, कार्ड क्रमांक, वैधता समाप्ती दिनांक, सीव्हीव्ही, इ. तपशील देऊ नका. तसे झाल्यास बँकेशी त्वरित संपर्क साधा.
- असे तपशील मागणाऱ्या संदेशांना उत्तर देऊ नका, अगदी ते बँक कर्मचारी असल्याचे सांगत असले तरी किंवा प्राप्तिकर विभाग, आरबीआय इ. शासकीय संस्थांमधून असल्याचे सांगत असले तरीही. एचएसबीसीचा कोणताही कर्मचारी तुम्हाला कॉल करून असे तपशील कधीही मागणार नाही.
- तुमचे इंटरनेट बँकिंग युझरनेम तुमच्या पासवर्डसोबत लिहून ठेवू नका. तुमचा पासवर्ड ओळखता येईल अशा स्वरूपात लिहू नका आणि तुमचे लॉग ऑन तपशील कधीही तुमच्या भौतिक सुरक्षा यंत्रासोबत / डिजिटल सिक्युअर की सोबत ठेवून जाऊ नका.
- तुमचे मोबाईल बँकिंग ॲप्लिकेशन अद्ययावत ठेवा. ते डाऊनलोड करण्यासाठी आणि ते अद्ययावत करण्यासाठी, तुमच्या डिव्हाइसच्या अधिकृत ॲप स्टोरवर जा.
- कधीही अविश्वसनीय स्रोतांकडून आलेल्या ईमेल्समधील लिंक्समधून मोबाईल बँकिंग / पेमेंट ॲप्लिकेशन्स डाऊनलोड करू नका.
- तुमचा कार्ड क्रमांक आणि वैधता समाप्ती दिनांक ऑनलाईन संकेतस्थळांवर जतन करताना खबरदारी बाळगा. हे तपशील अविश्वसनीय संकेतस्थळांवर किंवा क्वचित वापरल्या जाणाऱ्या संकेतस्थळांवर जतन करू नका.
- तुमचा पिन कधीही कोणालाही देऊ नका. तो तुम्ही स्वत: वापरा. जर तुमचा पिन कोणाला कळला असल्याची शंका आली, तर तो लगेच बदलून टाका.
- जर तुमच्याकडे युपीआय पिनची मागणी करण्यात आली, तर लक्षात ठेवा, तुम्ही पैसे भरत आहात. पैसे मिळवण्यासाठी तुम्हाला युपीआय पिन लागत नाही.
- सार्वजनिक कंप्युटर वापरताना सावध राहा.

नेहमी

- तुम्ही कॉम्प्युटर सोडून जात असाल तर लॉग आऊट करा, अगदी काही क्षणांसाठी असेल तरीही, शक्यतो, तुम्ही लॉग्ड इन असताना कॉम्प्युटर नुसता सोडून जाऊ नका.
- तुम्ही कम्प्युटरवरून लॉग आऊट करण्यापूर्वी तुमचा ब्राऊझिंग इतिहास हटवा: इंटरनेट ब्राऊझर्स तुमच्या पासवर्डविषयीची आणि तुम्ही भेट दिलेल्या पानांविषयीची माहिती जतन करून ठेवतात. इंटरनेट ब्राऊझरच्या टूल्स मेन्युवर जा आणि ऑप्शन्स किंवा इंटरनेट ऑप्शन्स हा पर्याय निवडा. ब्राऊझरची कोणतीही ऑटो कम्प्लीट क्रिया बंद केलेली असेल ह्याची खात्री करा, कोणत्याही कूकीज असतील तर त्या हटवा आणि इतिहास साफ करा.
- तुमचे बँकिंग व्यवहार करण्यासाठी शक्यतो सार्वजनिक कंप्युटर वापरणे टाळायचा प्रयत्न करा, अगदी ग्रंथालयांमधील, इंटरनेट कॅफे आणि शाळांमधीलही.

संवेदनशील माहिती टाइप करणे टाळा. तुम्ही सर्व खबरदारी पाळूनही, सार्वजनिक कंप्युटरमध्ये कीस्ट्रोक लॉगर नावाचे धोकादायक सॉफ्टवेअर असू शकते. असे सॉफ्टवेयर तुमचा पासवर्ड, क्रेडिट कार्ड क्रमांक आणि बँक तपशील चोरू शकतात. संवेदनशील माहिती उघड करू शकणारे कोणतेही आर्थिक व्यवहार करणे टाळा.

महत्त्वाचे – जर तुम्हाला अविश्वसनीय स्रोताकडून एचएसबीसी असल्याचा दावा करणारा ईमेल कधीही आला, किंवा वैयक्तिक माहिती मागणारा अनाहूत ईमेल आला, तर त्यांची माहिती **phishing@hsbc.com** ला द्या, आम्ही त्याची पुढे चौकशी करू.