HSBC

ऑनलाइन सुरक्षा और सुरक्षित उपयोग संबंधी दिशानिर्देश

आइए, जानिए कि हम आपकी ऑनलाइन बैंकिंग को मिलकर सुरक्षित रखने में कैसे मदद कर सकते हैं.
एक बैंक के रूप में हम सुरक्षा के बारे में सोचने के आदी हैं. इंटरनेट के विकास ने हम सभी के लिए अधिक लचीलेपन की पेशकश की है, लेकिन यह नए जोखिम भी लाता है जिनसे बचाव किया जाना आवश्यक है. एचएसबीसी में, हम आपके खाते को किसी भी अनधिकृत पहुंच से सुरक्षित रखने के लिए तीन प्रमुख क्षेत्रों – गोपनीयता, प्रौद्योगिकी और पहचान पर ध्यान केंद्रित करते हुए, उद्योग मानक सुरक्षा प्रौद्योगिकी और पद्धतियों का उपयोग करते हैं.

आइए, पढ़िए कि हम आपकी ऑनलाइन बैंकिंग की सुरक्षा कैसे करते हैं और आप अपनी ऑनलाइन सुरक्षा को बेहतर बनाने के लिए क्या कदम उठा सकते हैं.

धोखाधड़ी के प्रकार

ऐसे कई तरीके हैं जिनसे धोखेबाज आपको धोखा देकर आपसे आपके व्यक्तिगत और सुरक्षा विवरण प्राप्त करने का प्रयास कर सकते हैं. वे इन विवरणों का उपयोग बैंक के पास आपकी वित्तीय जानकारी तक पहुंचने के लिए करते हैं और आपके खाते से अपने खाते में भुगतान भी सेट कर लेते हैं.

कुछ अधिक सामान्य प्रकार की धोखाधड़ियां निम्निलिखत हैं जिनका आपको सामना करना पड़ सकता है.

क्रेडिट/ डेबिट कार्ड स्किमिंग/ क्लोनिंग:

जालसाज आपके क्रेडिट या डेबिट कार्ड की चुंबकीय पट्टी से जानकारी चुरा सकते हैं. वे एटीएम के कार्ड स्लॉट में या जब आप मर्चेंट भुगतान टर्मिनलों पर ध्यान नहीं दे रहे हैं, तो स्किमिंग डिवाइस छुपाकर ऐसा करते हैं. ये डिवाइस आपके कार्ड के विवरण को स्कैन और भंडारित करते हैं. आपका पिन चुराने के लिए, धोखेबाज एटीएम में या व्यापारिक प्रतिष्ठान में किसी गुप्त स्थान पर कैमरा लगा सकते हैं.

यूपीआई ऐप्स में घोटाला/ भुगतान धोखाधड़ी

जालसाज आपसे क्यूआर कोड को स्कैन करने के लिए या उनके खाते में पैसे ट्रांसफर करने के लिए "Collect Request" को अनुमोदित करने के लिए कहते हुए आपको मैसेजिंग ऐप के जरिए क्यूआर कोड भेज सकते हैं. वे आपको एक झूठी कहानी सुनाकर आपको बरगलाने की कोशिश कर सकते हैं, जैसे कि यह कहना कि वे एक ऐसा उत्पाद खरीदना चाहते हैं जिसे आप बेच रहे हैं. वे आपके लिए रिफंड/ अदावित कैशबैक ऑफर, रिवॉर्ड पॉइंट आदि को प्रोसेस करने की पेशकश करते बैंक या ऑनलाइन शॉपिंग कंपनी के एक्जिक्यूटिव का छद्म रूप धारण कर सकते हैं. असंदेही पीड़ित व्यक्ति क्यूआर कोड को स्कैन कर सकता है या अपने यूपीआई पिन का उपयोग करके "Collect Request" को अनुमोदित कर सकता है जिससे धोखेबाज के खाते में पैसा ट्रांसफर हो जाता है.

व्यावसायिक ईमेल / मैसेजिंग ऐप्स के जरिए भुगतान धोखाधड़ी

जालसाज आपके ईमेल या चैट को हैक कर सकते हैं, या आपके बारे में अधिक जानने के लिए अनएन्क्रिप्टेड संदेशों को इंटरसेप्ट कर सकते हैं. एक बार जब वे आपके बारे में अधिक जान जाते हैं, तो वे हैक की गई / छेड़छाड़ की गई / नकली आईडी से संदेश भेज सकते हैं, जो आपको किसी प्रियजन के अस्पताल में भर्ती होने या किसी बकाया बिल के किसी नए खाते में भुगतान किए जाने जैसे उचित रूप से वैध उद्देश्यों के लिए तत्काल भुगतान करने के लिए कह सकते हैं. पीड़ित व्यक्तियों को अनुरोध की तात्कालिकता के कारण या अनुरोध पर विश्वास करने के कारण भुगतान करने के लिए फंसाया जा सकता है. और चूंकि पीड़ित व्यक्ति ने स्वयं भुगतान किया है, इसलिए वे बैंक द्वारा भेजे गए लेनदेन अलर्ट से चिंतित नहीं होंगे. इस तरह की धोखाधड़ी का पता लगाना मुश्किल होता है.

नकली संपर्क नंबर:

जालसाज बैंकों और सेवा प्रदाता संपर्क केंद्रों के लिए फर्जी संपर्क विवरण प्रदान कर सकते हैं. असंदेही पीड़ित व्यक्ति सर्च इंजन का उपयोग करके संपर्क विवरण ढूंढ सकते हैं और नकली नंबर पर कॉल कर सकते हैं. फिर उन्हें "verification process" से गुजारा जाएगा जहां उन्हें अपने डेबिट/क्रेडिट कार्ड और बैंक खातों के बारे में संवेदनशील जानकारी साझा करने के लिए फंसाया जाता है.

आप यह सुनिश्चित करके अपनी सुरक्षा कर सकते हैं कि आप आवश्यक संपर्क विवरण देखने के लिए हमेशा किसी बैंक या सेवा प्रदाता की आधिकारिक वेबसाइट पर जाएँ. सतर्क रहें और खोज परिणामों में प्रदर्शित होने वाले कॉल नंबरों को पहले जांचे बिना उन कॉल करने से बचें, खासकर यदि वे मोबाइल नंबर हों.

फ़िशिंग/स्पूफ़िंग ईमेल:

जालसाज अधिक से अधिक ईमेल पतों पर ईमेल भेजकर पीड़ित व्यक्तियों के इंटरनेट में सेंध लगा सकते हैं. वे अक्सर बैंक, ऑनलाइन भुगतान सेवा, खुदरा विक्रेता या अन्य समान सेवा जैसे वैध संगठन का हिस्सा होने का नाटक करते हुए ऐसा करते हैं. वे अपनी आईडी को जुल (स्पूफ़) दे सकते हैं ताकि ईमेल ऐसा लगे कि यह स्वयं धोखेबाज के अलावा किसी अन्य व्यक्ति द्वारा भेजा गया है.

आप व्यक्तिगत या वित्तीय जानकारी मांगने वाले ईमेल का जवाब न देकर फ़िशिंग घोटालों से अपनी सुरक्षा कर सकते हैं. आपको कभी भी संदिग्ध ईमेल में लिंक को सिलेक्ट नहीं करना चाहिए.

एचएसबीसी कभी भी आपसे ईमेल द्वारा आपके व्यक्तिगत या सुरक्षा विवरण का खुलासा करने के लिए नहीं कहता है. यदि आपको ऐसा कोई ईमेल प्राप्त होता है, तो उसका उत्तर न दें और ईमेल को तुरंत डिलीट कर दें. और याद रखें, कभी भी अपनी व्यक्तिगत जानकारी जैसे आपका उपयोगकर्ता नाम, पासवर्ड या अन्य सुरक्षा विवरण किसी के साथ साझा न करें.

मनी म्यूल या अतिरिक्त आय ईमेल घोटाला:

मनी म्यूल स्कैम में, धोखेबाज आपसे ट्रांसफर के लिए मदद मांग सकते हैं. वे आपके खाते में रकम ट्रान्सफर करने की पेशकश कर सकते हैं ताकि आप इसे दूसरे खाते में ट्रान्सफर करने में उनकी सहायता कर सकें. बदले में, वे कहते हैं कि वे आपको कमीशन देंगे.

आपको ऐसे अनुरोधों को नज़रअंदाज़ करना चाहिए क्योंकि उनमें अक्सर मनी लॉन्ड्रिंग जैसे अपराध शामिल होते हैं. जानबूझकर भाग लेने वाले किसी भी व्यक्ति को अपराध में शामिल माना जा सकता है और उस पर मुकदमा चलाया जा सकता है. अगर यह सच होने के लिए बहुत अच्छा लगता है, तो शायद यह एक धोखा है!

अग्रिम शुल्क धोखाधड़ी ('419' घोटाले):

जालसाज आम तौर पर अमेरिकी डॉलर में बड़ी मात्रा में धन को ट्रान्सफर करने में मदद करने के लिए एक उदार इनाम की पेशकश करते हुए आपको अवांछित पत्र या ईमेल भेज सकते हैं. ये धोखेबाज वास्तव में आपके बैंकिंग विवरण के पीछे होते हैं. वे आम तौर पर आपसे सौदे को पूरा करने के लिए शुल्क, कुछ कर या रिश्वत देने के लिए कहते हैं – यह अग्रिम शुल्क है. पीड़ित व्यक्ति आमतौर पर इसे धोखेबाजों को खो देते हैं.

यदि आपको संदेह है कि किसी के पास आपका ऑनलाइन बैंकिंग विवरण है, तो आपको ऑनलाइन बैंकिंग में लॉग इन करना चाहिए और अपना पासवर्ड तुरंत बदल लेना चाहिए. हमें सतर्क करने के लिए आप हमें जल्द से जल्द कॉल भी करें. हमारी लाइनें 24x7* खुली हैं. आप हमारे हॉटलाइन नंबरों की सूची यहां पा सकते हैं.

सोशल मीडिया हैक:

जालसाज तुरंत पैसे ट्रांसफर करने के लिए अनुरोध करते हुए फेसबुक, व्हाट्सएप या इंस्टाग्राम जैसे सोशल मीडिया प्लेटफॉर्म पर आपके किसी करीबी दोस्त या रिश्तेदार का रूप धारण कर सकते हैं. आप अपने किसी जानने वाले को कॉल करके या अन्य चैनलों के माध्यम से उनसे संपर्क करके यह जांच सकते हैं कि अनुरोध वैध है या नहीं.

विशिंग कॉल्स (टेलीफोन द्वारा धोखाधड़ी):

जालसाज बैंक कर्मचारी या कस्टमर सर्विस एक्जिक्यूटिव का छद्म रूप धारण कर सकते हैं और संभावित पीड़ितों को उनके बैंक खाते के विवरण जैसी संवेदनशील जानकारी चुराने के लिए कॉल कर सकते हैं. किसी पीड़ित व्यक्ति का विश्वास जीतने के लिए, अपराधी पीड़ित को उसकी कुछ व्यक्तिगत जानकारी प्रदान कर सकते हैं जो सोशल इंजीनियरिंग के माध्यम से चुराई गई होती है. उनके द्वारा कुछ विश्वास उत्पन्न कर लेने के बाद, धोखेबाज कुछ विशेष सेवा या उत्पाद की पेशकश कर सकते हैं, इस उम्मीद में कि वे अपनी गोपनीय जानकारी जैसे कि उनके बैंक विवरण और एकबारगी पासकोड (ओटीपी) प्रदान करेंगे.

ट्रोजन वायरस

जालसाज आपको अवांछित ईमेल भेज सकते हैं जिनमें फाइलें, पेज या अटैचमेंट होते हैं जिन्हें आपको खोलने के लिए कहा जाता है. लेकिन उन्हें खोलने का मतलब है कि आपके कंप्यूटर पर गुप्त रूप से एक प्रोग्राम इंस्टॉल हो जाएगा जो आपकी ऑनलाइन गतिविधि पर नज़र रखता है, और यहां तक कि आप विभिन्न वेबसाइटों पर क्या टाइप करते हैं. इसलिए जब आप ऑनलाइन शॉपिंग करते समय अपने क्रेडिट कार्ड का विवरण दर्ज करते हैं, तो धोखेबाज आपके द्वारा दर्ज की गई जानकारी को देख पाएंगे.

ऑनलाइन सुरक्षा के लिए एचएसबीसी द्वारा उठाए गए कदम

बहु–परतीय लॉगऑन सत्यापन

आपकी वित्तीय जानकारी एक विशिष्ट उपयोगकर्ता नाम और पासवर्ड के परिष्कृत संयोजन और साथ ही आपके भौतिक सुरक्षा उपकरण/डिजिटल सुरक्षित कुंजी द्वारा जनरेट किए गए एकबारगी सुरक्षा कोड द्वारा सुरक्षित है

लेनदेन सत्यापन

कार्ड पर 3D सुरक्षित ट्रांजैक्शन लेनदेन और भुगतान प्रणाली में विश्वास को सुरक्षित करने में मदद करते हैं. लेनदेन के लिए जनरेट हुए ओटीपी को कभी भी किसी के साथ साझा न करें.

128–बिट सिक्योर सॉकेट लेयर (एसएसएल) एन्क्रिप्शन

एचएसबीसी इंटरनेट बैंकिंग सत्र के दौरान प्रसारित जानकारी के लिए 128–बिट सिक्योर सॉकेट लेयर (एसएसएल) एन्क्रिप्शन का उपयोग करता है, जिसे एन्क्रिप्शन के लिए उद्योग मानक के रूप में स्वीकार किया जाता है.

स्वत: 'टाइम–आउट' सुविधा

एक सुरक्षा उपाय के रूप में, आपका इंटरनेट बैंकिंग सत्र उपयोग नहीं किए जाने की अवधि के बाद स्वत: बंद या टाइम–आउट हो जाएगा. जब आप अपना इंटरनेट बैंकिंग कार्य पूरा कर लें तो आपको अपना इंटरनेट बैंकिंग सत्र हमेशा बंद कर देना चाहिए.

सुरक्षा डिवाइस/डिजिटल सुरक्षित कुंजी

आपकी भौतिक सुरक्षा डिवाइस/डिजिटल सुरक्षित कुंजी ऑनलाइन सुरक्षा को उच्च स्तर पर ले जाती है. अपने खाते में लॉग ऑन करने के लिए आपको हमेशा की तरह अपना मौजूदा उपयोगकर्ता नाम और पासवर्ड दर्ज करना होगा, इसके बाद आपकी भौतिक सुरक्षा डिवाइस या आपकी डिजिटल सुरक्षित कुंजी द्वारा उत्पन्न अद्वितीय सुरक्षा कोड दर्ज करना होगा. जब आप अपने इंटरनेट बैंकिंग का उपयोग करते हैं तो यह 2–चरणीय प्रमाणीकरण प्रक्रिया आपको सुरक्षा का एक उन्नत स्तर प्रदान करती है.

ऑनलाइन सुरक्षा में आपकी भूमिका

इंटरनेट बैंकिंग सुरक्षा सुनिश्चित करने के लिए 'क्या करें' और 'क्या न करें' का पालन करें

क्या करें

- सुनिश्चित करें कि आपका कंप्यूटर हर समय नवीनतम एंटी–वायरस और फ़ायरवॉल सुरक्षा सॉफ़्टवेयर से सुरक्षित है. नवीनतम सुरक्षा सुनिश्चित करने के लिए नियमित रूप से अपडेट डाउनलोड करें.
- ऐसा पासवर्ड चुनें जो आपके लिए स्मरणीय हो लेकिन किसी अन्य व्यक्ति के द्वारा अनुमान लगाना आसान न हो. पासवर्ड जिनमें वर्णांकीय (अल्फान्यूमेरिक) संप्रतीकों का संयोजन होता है, आमतौर पर उनका अनुमान लगाना कठिन होता है (उदा. a7g3cy91)
- अपना इंटरनेट बैंकिंग पासवर्ड नियमित रूप से बदलें.
- फ़िशिंग ईमेल से सावधान रहें. हमेशा सभी अक्षरों और संप्रतीकों सहित पूरा ईमेल पता ध्यान से पढ़ें.
- बहुत समान दिखने वाले ईमेल पतों जैसे hsdc.co.in या hsbcbank.com के माध्यम से फ़िशिंग को अंजाम दिया जाता है. उसके वास्तविक गंतव्य को प्रकट करने के लिए अपने माउस पॉइंटर को URL पर घुमाएं; यह आपके ब्राउज़र के निचले बाएँ कोने में प्रदर्शित होता है. अगर कोई बेमेल हो तो लिंक पर क्लिक न करें. URL में वर्तनी की गलतियों, गलत व्याकरण या अव्यवस्थित अक्षरों जैसे संकेतों से सावधान रहें.
- अगर आवश्यकता न रह गई हो तो अपने खाते से जोड़े गए लाभार्थियों को हटा दें.
- लॉगऑन विवरण याद रखने वाले अपने कंप्यूटर या ब्राउज़र पर कार्यात्मकता निष्क्रिय करें.
- अपने सिस्टम और वेब ब्राउज़र को अपडेट रखें. सिस्टमों और ब्राउज़रों में कमजोरियों का पता चलने पर निर्माता नियमित रूप से सुरक्षा पैच जारी करते हैं. इन अपडेटों के लिए अपने सॉफ़्टवेयर प्रदाता से नियमित रूप से संपर्क करते रहें.
- बैंक की वेबसाइट तक पहुंचने के लिए हमेशा ब्राउजर में बैंक का यूआरएल टाइप करें.
- पैडलॉक प्रतीक और साइट सर्टीफिकेट की जाँच करें. जब आप एचएसबीसी ऑनलाइन बैंकिंग में लॉग–इन करते हैं तो यह सुनिश्चित करने के लिए कि साइट सर्टीफिकेट एचएसबीसी से संबंधित है, अपने ब्राउज़र के निचले भाग में पैडलॉक प्रतीक पर डबल–क्लिक करें. यह सुनिश्चित करेगा कि आपको 'फर्जी' साइट पर अपना विवरण दर्ज करने के लिए धोखा नहीं दिया जा रहा है.
- अपने खातों की नियमित रूप से जांच करें. यदि किसी भी लेनदेन के बारे में संदेह है, तो विवरण नोट करें और हमें कॉल करें.
- ऑनलाइन बैंकिंग का उपयोग करने के बाद हमेशा लॉग–आउट करें. बस लॉग–आउट बटन सिलक्ट करें और जब आप सर्विस में लॉगिन हों तो अपने पीसी को कभी भी अरक्षित न छोड़ें.
- यदि आप बैंकों के कस्टमर केयर नंबर, ऑनलाइन शॉपिंग वेबसाइट आदि की तलाश में हैं तो इंटरनेट पर समझदारी से खोजें. जालसाज उनके द्वारा संचालित मोबाइल नंबरों के साथ परिणामों को वापस करने के लिए खोजों में हेरफेर करते हैं. आपको बैंक के कस्टमर केयर नंबर या ई–कॉमर्स वेबसाइट के बजाय धोखेबाज को कॉल करने के लिए धोखा दिया जा सकता है.
- अपने बैंक के संपर्क केंद्र नंबर को अपने डिवाइस पर स्टोर करें या अपने क्रेडिट/डेबिट कार्ड के पीछे लिखा नंबर देखें.
- अपने पर्सनल कंप्यूटर या मोबाइल डिवाइस पर स्क्रीन शेयरिंग एप्लिकेशन से सावधान रहें. जालसाज आपको ऐसे एप्लिकेशन डाउनलोड करने के लिए बरगलाते हैं और आपसे कोड मांगकर एक्सेस हासिल करते हैं. एक बार एक्सेस की अनुमति मिलने के बाद, वे आपके डिवाइस को दूरस्थ रूप से देखते/नियंत्रित करते हैं, यहां तक कि आपके खातों से भुगतान भी निष्पादित कर सकते हैं.
- अपने इंटरनेट कनेक्शन को सुरक्षित करें. हमेशा अपने घर के वायरलेस नेटवर्क को पासवर्ड से सुरक्षित रखें.
- ऐसी योजना/प्रस्तावों के बारे में सतर्क रहें, जिनके लिए आपको अपने खाते में कमीशन या सहायता के लिए भी पैसा मिलता है. वे धोखेबाज आपके खाते में अपराध की आय भेज सकते हैं और आपसे धन ट्रान्सफर करने या उन्हें नकद प्रदान करने के लिए कह सकते हैं. जालसाज खुद को पैसों के जाल में नहीं फंसाना चाहते हैं और आपको मनी म्यूल की तरह इस्तेमाल कर सकते हैं.
- धोखाधड़ी की रिपोर्ट करने के लिए बैंक से तुरंत संपर्क करें.

क्या न करें

- ऐसा पासवर्ड न चुनें जिसका उपयोग आप अन्य सेवाओं के लिए करते हैं. आपका पासवर्ड इंटरनेट बैंकिंग के लिए अद्वितीय होना चाहिए.
- वेबपेजों पर यूजर आईडी, पासवर्ड, कार्ड नंबर, समाप्ति तारीख, सीवीवी आदि जैसे विवरणों का खुलासा न करें, जो अनजाने में ईमेल/एसएमएस में लिंक क्लिक करने पर खुल जाते हैं.
- इस तरह के विवरण मांगने वाले संदेशों का जवाब न दें, भले ही वे बैंक कर्मचारियों या आयकर विभाग, आरबीआई आदि जैसे सरकारी निकायों से होने का दावा कर रहे हों. एचएसबीसी का कोई सदस्य कभी भी आपको फोन नहीं करेगा और आपसे इसके लिए नहीं पूछेगा.
- अपने पासवर्ड के साथ अपना इंटरनेट बैंकिंग यूजरनेम न लिखें. अपना पासवर्ड पहचानने योग्य प्रारूप में न लिखें और अपने लॉगऑन विवरण को अपने भौतिक सुरक्षा डिवाइस/डिजिटल सुरक्षित कुंजी के साथ कभी न छोड़ें.
- अपने मोबाइल बैंकिंग एप्लिकेशन को अपडेट रखें. डाउनलोड और एप्लिकेशन के किसी भी अनुवर्ती अपडेट के लिए प्ले स्टोर पर जाएं.

- अविश्वसनीय स्रोतों से ईमेल में मोबाइल बैंकिंग/भुगतान आवेदन आधार लिंक कभी भी डाउनलोड न करें.
- ऑनलाइन वेबसाइटों पर कार्ड नंबर और समाप्ति तारीखों को स्टोर करने से सावधान रहें. इन विवरणों को शायद ही कभी उपयोग की जाने वाली वेबसाइटों की अविश्वसनीय वेबसाइटों पर स्टोर न करें.
- कभी भी किसी को अपना पिन न बताएं. इसे स्वयं प्रयोग करें. यदि आपको संदेह है कि आपके पिन से छेड़छाड़ की गई है, तो इसे तुरंत बदल दें.

यूपीआई में पिन पूछा जाता है, याद रखें, आप भुगतान कर रहे हैं. भुगतान प्राप्त करने के लिए आपको यूपीआई पिन की आवश्यकता नहीं होती है.

सार्वजनिक कंप्यूटर का उपयोग करते समय सतर्क रहें

हमेशा

- अगर आप कंप्यूटर छोड़ते हैं तो लॉग आउट करें, भले ही वह एक पल के लिए ही क्यों न हो. यदि संभव हो तो लॉग इन रहते हुए कंप्यूटर को अरक्षित न छोड़ें.
- कंप्यूटर से लॉग आउट करने से पहले अपना ब्राउज़िंग इतिहास डिलीट करें: इंटरनेट ब्राउज़र आपके पासवर्ड और आपके द्वारा देखे जाने वाले पृष्ठों के बारे में जानकारी स्टोर करते हैं. इंटरनेट ब्राउजर के टूल्स मेन्यू में जाएं और ऑप्शन्स या इंटरनेट ऑप्शन्स को सिलेक्ट करें. सुनिश्चित करें कि ब्राउज़र में कोई भी स्वत: पूर्ण कार्य बंद हो, किसी भी कुकी को डिलीट कर दें और इतिहास को क्लियर करें.
- अपनी बैंकिंग करने के लिए सार्वजनिक कंप्यूटरों, जिसमें पुस्तकालयों, इंटरनेट कैफे और स्कूलों के कंप्यूटर भी शामिल हैं, के उपयोग से बचें.

संवेदनशील जानकारी टाइप न करें. भले ही आप सभी एहतियातों का पालन करते हों तो भी सार्वजनिक कंप्यूटर में दुर्भावनापूर्ण सॉफ़्टवेयर इंस्टाल हो सकता है, जिसे कीस्ट्रोक लॉगर कहा जाता है. ये प्रोग्राम आपका पासवर्ड, क्रेडिट कार्ड नंबर और बैंक विवरण चुरा सकते हैं. ऐसे वित्तीय लेनदेन करने से बचें जो संवेदनशील जानकारी प्रकट कर सकते हैं.

महत्वपूर्ण: यदि आपको कभी एचएसबीसी होने का दावा करते हुए किसी अविश्वसनीय स्रोत से काई ईमेल प्राप्त होता है या व्यक्तिगत जानकारी मांगने वाला कोई अवांछित ईमेल प्राप्त है तो इसकी रिपोर्ट **phishing@hsbc.com** पर करें ताकि हम आगे की जांच कर सकें.