Your money is safe with your bank, yet....

a little extra care makes your online transactions more secure.

The convenience of online banking can be compared to electricity. It has to be used with care to prevent rude shocks. Which is why one has to be aware of "Phishing". An online method used by fraudsters to steal customers' personal details like User IDs, Passwords, Date of Birth, CVV, IPIN, Credit/ Debit Card No., Card Expiry Date and so on.

UNDERSTAND "PHISHING". PREVENT IT.

- Fraudsters can get personal information from bank's customers through emails or phones. These are very cleverly camouflaged and appear to be originating from the bank itself.
- Information could also get siphoned off while you are logged on to your bank's website. This happens through pop-ups, which appear along side your bank's webpage asking unsuspecting users to disclose confidential information.
- Other requests might draw you to be part of a survey or inform you that your online session has expired and that you need to validate/update/ reveal your account to revive it.
- This could also happen when you download software or files from an unknown source or through threats that your online session will be shut down if reconfirmation of account details is not carried out.

HABITS THAT SAVE YOU FROM "PHISHING"

- Always type the address of your bank URL in the browser bar only.
- Avoid opening of multiple windows during a session.
- Never give your user IDs, Passwords, Date of Birth, CVV, IPIN, Credit/Debit Card No., Card Expiry Date on pop-ups.
- Always log off systematically and reconfirm your status.
- Use proper, updated anti-virus and anti-spyware tools to keep your computer healthy.
- Employ dual security passwords for added protection.
- Update yourself on "Phishing" at regular intervals from authentic sources.

Indian Banks' Association
www.iba.org.in

आपका पैसा आपके बैंक में सुरक्षित है, फिर भी...

ज़रा सी सावधानी आपके ऑनलाइन लेन-देन को बनाए अधिक सुरक्षित।

ऑनलाइन बैंकिंग सुविधा की तुलना हम बिजली से कर सकते हैं। दोनों का ही इस्तेमाल बड़े ध्यान से करना चाहिए, वरना ज़ोरदार झटके सहने पड़ सकते हैं। इसीलिए हमें 'फ़िशिंग' से सतर्क रहने की ज़रूरत है। यह जालसाज़ों द्वारा ग्राहकों की निजी जानकारी, जैसे उपयोगकर्ता की पहचान, पासवर्ड, जन्मतिथि, सी वी वी, आई पी आई एन, क्रेडिट/डेबिट कार्ड नं., कार्ड समाप्ति तिथि इत्यादि चुरा लेने का एक ऑनलाइन तरीक़ा है।

'फ़िशिंग' को समझिए और इसकी रोकथाम कीजिए।

- जालसाज़ ईमेल या फ़ोन द्वारा बैंक के ग्राहकों की निजी जानकारी प्राप्त कर सकते हैं। ये बड़ी ही चालाकी से छिपाई जाती है और ऐसा प्रतीत होता है मानो बैंक से ही मंगवायी गई है।
- आपकी जानकारी तब भी चोरी-छिपे प्राप्त की जा सकती है जब आप अपने बैंक की वेबसाइट पर लॉग ऑन रहते हैं। यह होता है पॉप अप्स के ज़रिये जो आपके बैंक के वेबपेज की बग़ल में आते रहते हैं और भोलेभाले यूज़र्स से उनकी गोपनीय जानकारी बताने का आग्रह करते हैं।
- अन्य प्रकार के निवेदन आपको किसी सर्वेक्षण में शामिल कर सकते हैं अथवा आपको सूचित कर सकते हैं कि आपका ऑनलाइन सैशन समाप्त हो गया है और उसे पुनर्चालित करने के लिए आपको अपना अकाउंट मान्य/अपडेट/प्रदर्शित करना होगा।
- यह तब भी हो सकता है जब आप किसी अनजान स्रोत से जानकारी या फ़ाइल्स डाउनलोड करते हैं अथवा ऐसी चेतावनियों के माध्यम से कि अगर आपने अपने अकाउंट की जानकारी की दोबारा पुष्टि नहीं की तो आपका ऑनलाइन सैशन बंद हो जाएगा।

'फ़िशिंग' से आपका बचाव करने वाली आदतें

- अपने बैंक यूआरएल का पता हमेशा ब्राऊज़र बार में ही टाइप करें।
- एक सैशन में बहुत सारी विन्डोज़ खोलने से बचें।
- कभी भी पॉप अप्स में अपने यूज़र आईडी, पासवर्ड, जन्मतिथि, सीवीवी, आईपीआईएन, क्रेडिट/डेबिट कार्ड नं., कार्ड समाप्ति की तारीख़ न लिखें।
- हमेशा व्यवस्थित तरीक़े से लॉग ऑफ़ हों और अपने स्टेटस की फिर से पुष्टि करें।
- अपने कम्प्यूटर को वायरसरहित रखने के लिए उचित, नवीनीकृत एंटी-वायरस तथा एंटी-स्पायवेयर उपकरणों का इस्तेमाल करें।
- अतिरिक्त सुरक्षा के लिए दोहरी सुरक्षा वाले पासवर्ड्स का प्रयोग करें।
- प्रामाणिक स्त्रोतों द्वारा नियमित रूप से 'फ़िशिंग' के बारे में जानकारी प्राप्त करते रहें।

भारतीय बैंक संघ
www.iba.org.in