ਐਚ ਡੀ ਐਫ਼ ਸੀ ਬੈਂਕ

SECURE BANKING

ਇਹ ਕਦੇ ਵੀ ਸਾਂਝੇ ਨਾ ਕਰੋ

ਓਟੀਪੀ • ਕਾਰਡ ਨੰਬਰ • ਯੂਪੀਆਈ ਪਿੰਨ • ਬੈਂਕ ਦੇ ਵੇਰਵੇ

• ਕਸਟਮਰ ਆਈਡੀ ਅਤੇ ਪਾਸਵਰਡ

ਫਿਸ਼ਿੰਗ ਅਤੇ ਸਮਿਸ਼ਿੰਗ ਲਿੰਕਸ

ਧੋਖਾਧੜੀ

- ਜਾਲਸਾਜ SMS, ਸੋਸ਼ਲ ਮੀਡੀਆ ਪੋਸ਼ਟ, ਇਨਸਟੈਂਟ ਮੈਸੇਂਜਰ ਆਦਿ ਦੇ ਜ਼ਰੀਏ ਲਿੰਕ ਟ੍ਰਾਂਸਮਿਟ ਕਰਨ ਲਈ ਤੀਜੀ ਪਾਰਟੀ ਵੈਬਸਾਈਟਾਂ ਬਣਾਉਂਦੇ ਹਨ।
- ਜਦੋਂ ਤੁਸੀਂ ਲਿੰਕ ਤੇ ਕਲਿਕ ਕਰਦੇ ਹੋ ਤਾਂ ਤੁਹਾਨੂੰ ਇੱਕ ਅਜਿਹੀ ਵੈਬਸਾਈਟ ਤੇ ਲਿਜਾਇਆ ਜਾਂਦਾ ਹੈ ਜੋ ਦੇਖਣ ਵਿੱਚ ਬਿਲਕੁਲ ਅਸਲੀ ਵਰਗੀ ਲਗਦੀ ਹੈ, ਅਤੇ ਓਥੇ ਤੁਹਾਨੂੰ ਆਪਣੀ ਬੈਂਕ ਜਾਣਕਾਰੀ ਦਰਜ ਕਰਨ ਲਈ ਆਖਿਆ ਜਾਵੇਗਾ।
- ਇੱਕ ਵਾਰ ਜਦੋਂ ਤੁਸੀਂ ਉਹ ਪ੍ਰਕਿਰਿਆ ਪੂਰੀ ਕਰ ਲੈਂਦੇ ਹੋ ਤਾਂ ਜਾਲਸਾਜ ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਦਾ ਗਲਤ ਇਸਤੇਮਾਲ ਕਰ ਸਕਦਾ ਹੈ।

ਸੁਰੱਖਿਆ ਦੇ ਉਪਾਅ

- ਫਿਸ਼ਿੰਗ ਦੇ ਖਿਲਾਫ ਸੁਰੱਖਿਆ ਦਾ ਪਹਿਲਾ ਉਪਾਅ ਹੈ ਇਹ ਜਾਣਨਾ ਕਿ ਤੁਹਾਡਾ ਬੈਂਕ ਕਦੇ ਵੀ ਤੁਹਾਡੇ ਕੋਲੋਂ ਸਬੰਧਿਤ ਜਾਣਕਾਰੀਆਂ ਨਹੀਂ ਮੰਗੇਗਾ ਜਾਂ ਤੁਹਾਨੂੰ ਵੈਬਸਾਈਟ ਤੇ ਲਿੰਕ ਨਹੀਂ ਭੇਜੇਗਾ।
- ਜੋਖਮ ਤੋਂ ਬਚਣ ਦੇ ਲਈ ਤੁਰੰਤ ਆਪਣਾ ਕਾਰਡ ਬਲੌਕ ਕਰੋ ਜਾਂ ਆਪਣਾ ਪਾਸਵਰਡ ਬਦਲੀ ਕਰੋ।

ਵਿਸ਼ਿੰਗ ਕਾਲਸ

ਧੋਖਾਧੜੀ

- ਔਨਲਾਈਨ ਜਾਣਕਾਰੀ ਪ੍ਰਾਪਤ ਕਰ ਕੇ ਕੋਈ ਧੋਖੇਬਾਜ਼ ਇੱਕ ਬੈਂਕਰ, ਕੰਪਨੀ ਦਾ ਕਰਮਚਾਰੀ ਜਾਂ ਬੀਮਾ ਏਜੰਟ ਬਣ ਕੇ ਤੁਹਾਡੇ ਨਾਲ ਸੰਪਰਕ ਕਰ ਸਕਦੇ ਹਨ।
- ਉਹ ਇਸ ਨੂੰ ਬਹੁਤ ਜ਼ਰੂਰੀ ਮਾਮਲਾ ਦੱਸ ਸਕਦੇ ਹਨ ਅਤੇ ਤੁਹਾਡੇ ਅਤੇ ਸ਼ਾਖਾ ਦੇ ਬਾਰੇ ਬੁਨੀਆਦੀ ਗੱਲਾਂ ਨੂੰ ਦੱਸ ਕੇ ਤੁਹਾਡਾ ਭਰੋਸਾ ਜਿੱਤ ਸਕਦੇ ਹਨ।
- ਇੱਕ ਵਾਰ ਧੋਖੇਬਾਜ਼ ਜਦੋਂ ਤੁਹਾਡਾ ਭਰੋਸਾ ਹਾਸਿਲ ਕਰ ਲੈਂਦਾ ਹੈ ਤਾਂ ਉਹ ਤੁਹਾਨੂੰ ਆਪਣਾ KYC ਅਪਡੇਟ ਕਰਨ ਲਈ ਆਖੇਗਾ, ਤੁਹਾਨੂੰ ਆਕਰਸ਼ਕ ਡਿਸਕਾਉਂਟ ਦੇਵੇਗਾ, ਪੈਨਲਟੀ ਤੋਂ ਬਚਣ ਲਈ

ਸੁਰੱਖਿਆ ਦੇ ਉਪਾਅ

- ਆਪਣੇ ਕਾਰਡ ਨੂੰ ਤੁਰੰਤ ਬਲੌਕ ਕਰੋ।
- ਆਪਣਾ ਪਾਸਵਰਡ ਅਕਸਰ ਰੀਸੈਟ ਕਰਦੇ ਰਹੋ।

ਔਨਲਾਈਨ ਸੈਲਿੰਗ ਪਲੈਟਫਾਰਮਸ ਦਾ ਇਸਤੇਮਾਲ ਕਰ ਕੇ ਧੋਖਾਧੜੀ

ਧੋਖਾਧੜੀ

- ਜਾਲਸਾਜ ਔਨਲਾਈਨ ਸੈਲਿੰਗ ਪਲੈਟਫਾਰਮ ਤੇ ਖਰੀਦਦਾਰ ਬਣ ਕੇ ਆਉਂਦੇ ਹਨ ਅਤੇ ਤੁਹਾਡੇ ਪ੍ਰੋਡਕਟ ਵਿੱਚ ਦਿਲਚਸਪੀ ਦਿਖਾਉਂਦੇ ਹਨ।
- ਪੈਸੇ ਦਾ ਭੁਗਤਾਨ ਕਰਨ ਦੇ ਬਦਲੇ, ਉਹ UPI ਐਪਸ ਦੇ ਮਾਧਿਅਮ 'ਪੈਸੇ ਦੀ ਬੇਨਤੀ' ਕਰਦੇ ਹਨ ਅਤੇ ਤੁਹਾਨੂੰ ਕਹਿੰਦੇ ਹਨ ਕਿ ਆਪਣੇ ਖਾਤੇ ਤੋਂ ਪੈਸੇ ਕੱਢਣ ਲਈ ਤੁਸੀਂ ਇਸ ਨੂੰ ਸਵੀਕਾਰ ਕਰੋ।

ਸੁਰੱਖਿਆ ਦੇ ਉਪਾਅ

- ਆਪਣੀ ਵਿੱਤੀ ਸੰਸਥਾ ਨੂੰ ਅਨਅਧਿਕਾਰਤ ਲੈਣ ਦੇਣ ਦੀਆਂ ਘਟਨਾਵਾਂ ਦੀ ਤੁਰੰਤ ਜਾਣਕਾਰੀ ਦਿਓ।
- ਆਪਣੀ ਸ਼ਿਕਾਇਤ ਦਰਜ ਕਰਨ ਲਈ ਰਾਸ਼ਟ੍ਰੀ ਸਾਈਬਰ ਅਪਰਾਧ ਹੈਲਪਲਾਈਨ ਨੰਬਰ 155260 ਨਾਲ ਸੰਪਰਕ ਕਰੋ।

ਤੁਹਾਡੀ ਜਾਣਕਾਰੀ ਦੀ ਚੋਰੀ ਕਰਨ ਲਈ ਜਾਅਲੀ ਹੈਲਪਲਾਈਨ ਅਤੇ ਸਕ੍ਰੀਨ ਸ਼ੇਅਰਿੰਗ ਐਪ

ਧੋਖਾਧੜੀ

- ਗਾਹਕ ਬਿਜ਼ਨੇਸ ਹੈਲਪਲਾਈਨ ਨੰਬਰ ਦੇਖਣ ਦੇ ਲਈ ਸਰਚ ਇੰਜਨ ਦਾ ਇਸਤੇਮਾਲ ਕਰਦੇ ਹਨ, ਜਿੱਥੇ ਧੋਖੇਬਾਜ਼ ਫਰਜ਼ੀ ਨੰਬਰ ਅਪਲੋਡ ਕਰਦੇ ਹਨ ਅਤੇ ਗਾਹਕਾਂ ਨੂੰ ਉਹਨਾਂ ਨੰਬਰਾਂ ਤੇ ਕਾਲ ਕਰਨ ਲਈ ਪ੍ਰੇਰਿਤ ਕਰਦੇ ਹਨ।
- ਧੋਖੇਬਾਜ਼ ਬੈਂਕ ਦਾ ਪ੍ਰਤਿਨਿਧੀ ਹੋਣ ਦਾ ਦਿਖਾਵਾ ਕਰਦਾ ਹੈ ਅਤੇ ਤੁਹਾਡੇ ਕੋਲੋਂ ਐਪ ਡਾਉਨਲੋਡ ਕਰਨ ਅਤੇ ਆਪਣੀ ਸਕ੍ਰੀਨ ਸਾਂਝੀ ਕਰ ਕੇ ਤੁਹਾਡੇ ਡਿਵਾਈਸ ਤੱਕ ਪਹੁੰਚ ਪ੍ਰਾਪਤ ਕਰਦਾ ਹੈ ਜਾਂ ਪੁਸ਼ਟੀ ਦੇ ਲਈ ਤੁਹਾਡੇ ਕਾਰਡ ਦਾ ਵੇਰਵਾ ਮੰਗਦਾ ਹੈ।
- ਅਸੀਂ ਉਹਨਾਂ ਨੂੰ ਸੱਚੇ ਜਾਣ ਕੇ ਆਪਣੀ ਨਿਜੀ ਜਾਣਕਾਰੀ ਉਹਨਾਂ ਨਾਲ ਸਾਂਝੀ ਕਰ ਦੇਂਦੇ ਹਾਂ।
- ਇਸ ਦੀ ਮਦਦ ਨਾਲ ਓਹ ਤੁਹਾਡੀ ਬੈਂਕਿੰਗ ਜਾਣਕਾਰੀ ਤੱਕ ਪਹੁੰਚ ਪ੍ਰਾਪਤ ਕਰ ਲੈਂਦੇ ਹਨ ਅਤੇ ਬਾਅਦ ਵਿੱਚ ਪੇਮੇਂਟ ਐਪ ਜਾਂ ਇੰਟਰਨੈਟ ਬੈਂਕਿੰਗ ਦਾ ਇਸਤੇਮਾਲ ਕਰ ਕੇ ਪੈਸੇ ਕੱਢ ਲੈਂਦੇ ਹਨ।

ਸੁਰੱਖਿਆ ਦੇ ਉਪਾਅ

- ਕਦੇ ਵੀ ਐਪਸ ਡਾਉਨਲੋਡ ਨਾ ਕਰੋ ਅਤੇ ਆਪਣੀ ਸਕ੍ਰੀਨ ਕਿਸੇ ਅਣਪਛਾਤੇ ਵਿਅਕਤੀ ਦੇ ਨਾਲ ਸਾਂਝੀ ਨਾ ਕਰੋ।

ਸੋਸ਼ਲ ਮੀਡੀਆ ਰਾਹੀਂ ਜਾਲਸਾਜ਼ੀ

ਧੋਖਾਧੜੀ

- ਜਾਲਸਾਜ ਮੰਨੇ ਸੋਸ਼ਲ ਮੀਡੀਆ ਪਲੈਟਫਾਰਮਸ ਤੇ ਫਰਜ਼ੀ ਖਾਤੇ ਬਣਾਉਂਦੇ ਹਨ ਅਤੇ ਮੈਡੀਕਲ ਬਿਲ ਜਾਂ ਭੁਗਤਾਨ ਦੇ ਲਈ ਪੈਸੇ ਮੰਗਦੇ ਹਨ।
- ਉਹ ਸਮਾਂ ਪਾ ਕੇ ਤੁਹਾਡਾ ਵਿਸ਼ਵਾਸ ਹਾਸਿਲ ਕਰਦੇ ਹਨ ਅਤੇ ਬਾਅਦ ਵਿੱਚ ਨਿਜੀ ਜਾਣਕਾਰੀ ਦਾ ਇਸਤੇਮਾਲ ਕਰ ਕੇ ਬਲੈਕਮੇਲ ਕਰਦੇ ਹਨ ਅਤੇ ਪੈਸੇ ਕੱਢਣ ਦੇ ਲਈ ਕਹਿੰਦੇ ਹਨ।

ਸੁਰੱਖਿਆ ਦੇ ਉਪਾਅ

- ਹਮੇਸ਼ਾ ਕਿਸੀ ਵੀ ਔਨਲਾਈਨ ਖਾਤੇ ਦੀ ਸੱਚਾਈ ਦੀ ਪੁਸ਼ਟੀ ਕਰੋ ਅਤੇ ਨਿਜੀ ਜਾਣਕਾਰੀ ਦੇ ਬਾਰੇ ਪੁੱਛਣ ਤੇ ਸੰਦੇਹ ਜ਼ਰੂਰ ਕਰੋ।
- ਆਪਣੀ ਸ਼ਿਕਾਇਤ ਦਰਜ ਕਰਨ ਲਈ ਰਾਸ਼ਟ੍ਰੀ ਸਾਈਬਰ ਅਪਰਾਧ ਹੈਲਪਲਾਈਨ ਨੰਬਰ 155260 ਨਾਲ ਸੰਪਰਕ ਕਰੋ।

ਲਾਟਰੀ ਸਬੰਧੀ ਧੋਖਾਧੜੀ

ਧੋਖਾਧੜੀ

- ਜਾਲਸਾਜ ਤੁਹਾਨੂੰ ਈਮੇਲ ਲਿਖ ਸਕਦੇ ਹਨ ਜਾਂ ਤੁਹਾਨੂੰ ਫੋਨ ਕਰ ਸਕਦੇ ਹਨ, ਇਹ ਦਾਅਵਾ ਕਰਦੇ ਹੋਏ ਕਿ ਤੁਸੀਂ ਲਾਟਰੀ ਵਿੱਚ ਇੱਕ ਵੱਡਾ ਇਨਾਮ ਜਿੱਤਿਆ ਹੈ। ਪਰ ਪੈਸੇ ਪਾਉਣ ਦੇ ਲਈ, ਉਹਨਾਂ ਦੀ ਵੈਬਸਾਈਟ ਤੇ ਬੈਂਕ ਖਾਤੇ ਜਾਂ ਕ੍ਰੈਡਿਟ ਕਾਰਡ ਦੁਆਰਾ ਪਛਾਣ ਦੀ ਪੁਸ਼ਟੀ ਕਰਨਾ ਜ਼ਰੂਰੀ ਹੈ, ਜਿੱਥੇ ਡੇਟਾ ਇਕੱਠਾ ਕੀਤਾ ਜਾਂਦਾ ਹੈ।
- ਕੁੱਝ ਹਾਲਾਤਾਂ ਵਿੱਚ, ਧੋਖੇਬਾਜ਼ ਲਾਟਰੀ / ਸਮਾਨ ਪਾਉਣ ਦੇ ਲਈ ਟੈਕਸ, ਸ਼ਿਪਿੰਗ ਫੀਸ, ਪ੍ਰਕਿਰਿਆ ਫੀਸ ਅਤੇ ਹੋਰ ਫੀਸ ਦੇ ਲਈ ਐਡਵਾਂਸ ਭੁਗਤਾਨ ਦੀ ਮੰਗ ਕਰਦੇ ਹਨ।
- ਮੰਗੀ ਹੋਈ ਰਕਮ ਕਿਉਂਕਿ ਲਾਟਰੀ / ਸਮਾਨ ਦਾ ਇੱਕ ਬਹੁਤ ਹੀ ਛੋਟਾ ਹਿੱਸਾ ਹੁੰਦਾ ਹੈ, ਇਸ ਲਈ ਲੋਕ ਧੋਖੇਬਾਜ਼ ਦੀਆਂ ਗੱਲਾਂ ਵਿੱਚ ਆ ਕੇ ਭੁਗਤਾਨ ਕਰ ਸਕਦੇ ਹਨ।

ਸੁਰੱਖਿਆ ਦੇ ਉਪਾਅ

- ਲਾਟਰੀ ਜਿੱਤਣ ਸਬੰਧੀ ਕਾਲ/SMS/ਈਮੇਲ ਦਾ ਕਦੇ ਜਵਾਬ ਨਾ ਦਿਓ।
- ਅਸੁਵਿਧਾ ਤੋਂ ਬਚਣ ਦੇ ਲਈ ਆਪਣੇ ਬੈਂਕ ਜਾਂ ਕ੍ਰੈਡਿਟ ਕਾਰਡ ਦੇ ਜਾਰੀ ਕਰਤਾ ਨੂੰ ਸੂਚਿਤ ਕਰੋ।

ਜਾਲਸਾਜਾਂ ਦੁਆਰਾ ਲੋਨ ਦੇਣ ਦੇ ਲਈ ਫਰਜ਼ੀ ਵਿਗਿਆਪਨ

ਧੋਖਾਧੜੀ

- ਜਾਲਸਾਜ ਬੜੇ ਹੀ ਆਕਰਸ਼ਕ ਵਿਆਜ ਦਰਾਂ, ਅਸਾਨ ਮੁੜ-ਭੁਗਤਾਨ ਵਿਕਲਪਾਂ ਆਦਿ ਦੇ ਨਾਲ ਪਰਸਨਲ ਲੋਨਸ ਦੇ ਲਈ ਨਕਲੀ ਵਿਗਿਆਪਨ ਬਣਾਉਂਦੇ ਹਨ, ਅਤੇ ਫੇਰ ਗਾਹਕਾਂ ਨੂੰ ਉਹਨਾਂ ਨਾਲ ਸੰਪਰਕ ਕਰਨ ਲਈ ਕਹਿੰਦੇ ਹਨ।
- ਇਹ ਈਮੇਲ ਆਈਡੀ ਭੋਲੇ-ਭਾਲੇ ਗਾਹਕਾਂ ਦੇ ਨਾਲ ਭਰੋਸਾ ਬਣਾਉਣ ਲਈ ਅਤੇ ਉਹਨਾਂ ਵਿੱਚ ਭਰੋਸਾ ਜਗਾਉਣ ਲਈ ਸੀਨੀਅਰ ਬੈਂਕ ਅਫਸਰਾਂ ਦੀ ਈਮੇਲ ਆਈਡੀ ਜਹੀ ਦਿਸਣ ਵਾਲੀ ਈਮੇਲ ਆਈਡੀ ਹੁੰਦੀ ਹੈ।
- ਜਦੋਂ ਗਾਹਕ ਲੋਨ ਦੇ ਲਈ ਧੋਖੇਬਾਜ਼ਾਂ ਨਾਲ ਸੰਪਰਕ ਕਰਦੇ ਹਨ ਤਾਂ ਉਹ ਪ੍ਰਕਿਰਿਆ ਫੀਸ, GST, ਇੰਟਰਸਟੇਟ ਲਾਗਤ ਵਰਗੀਆਂ ਅਲੱਗ-ਅਲੱਗ ਐਡਵਾਂਸ ਫੀਸ ਦੀ ਮੰਗ ਕਰਦੇ ਹਨ ਅਤੇ ਫੇਰ

ਸੁਰੱਖਿਆ ਦੇ ਉਪਾਅ

- ਗੱਲ-ਬਾਤ ਕਰਨ ਤੋਂ ਬਚੋ ਅਤੇ ਲੋਨ ਲੈਣ ਦੇ ਲਈ ਆਪਣੇ ਰਿਲੇਸ਼ਨਸ਼ਿਪ ਮਨੇਜਰ ਨਾਲ ਸੰਪਰਕ ਕਰੋ।
- ਸਾਵਧਾਨ ਰਹੋ ਅਤੇ ਕਈ ਅਜਿਹੇ ਸਵਾਲ ਪੁੱਛੋ ਜਿਹਨਾਂ ਦਾ ਜਵਾਬ ਕੇਵਲ ਉਹ ਹੀ ਜਾਣਦੇ ਹੋਣਗੇ।

ਔਨਲਾਈਨ ਨੌਕਰੀ ਸਬੰਧੀ ਧੋਖਾਧੜੀ

ਧੋਖਾਧੜੀ

- ਨਕਲੀ ਜੌਬ ਸਰਚ ਪੋਰਟਲ ਬਣਾ ਲਏ ਜਾਂਦੇ ਹਨ ਅਤੇ ਜਦੋਂ ਜ਼ਰੂਰਤਮੰਦ ਲੋਕ ਰਜਿਸਟ੍ਰੇਸ਼ਨ ਦੇ ਲਈ ਇਹਨਾਂ ਵੈਬਸਾਈਟਾਂ ਤੇ ਗੁਪਤ ਬੈਂਕ ਅਕਾਉਂਟ, ਕ੍ਰੈਡਿਟ ਕਾਰਡ ਜਾਂ ਡੈਬਿਟ ਕਾਰਡ ਸਬੰਧੀ ਜਾਣਕਾਰੀ ਦਰਜ ਕਰਦੇ ਹਨ ਤਾਂ ਉਹਨਾਂ ਦੇ ਅਕਾਉਂਟ ਨਾਲ ਛੇੜਛਾੜ ਕੀਤੀ ਜਾਂਦੀ ਹੈ।
- ਕੁੱਝ ਹਾਲਾਤਾਂ ਵਿੱਚ, ਧੋਖੇਬਾਜ਼ ਇੱਕ ਉੱਘੀ ਕਾਰਪੋਰੇਸ਼ਨ ਦੇ ਅਧਿਕਾਰੀ ਦੇ ਰੂਪ ਵਿੱਚ ਖੁਦ ਨੂੰ ਦੱਸਦਾ ਹੈ ਅਤੇ ਨਕਲੀ ਇੰਟਰਵਿਊ ਕਰਨ ਦੇ ਬਾਅਦ ਤੁਹਾਡੇ ਚੁਣੇ ਜਾਣ ਦੀ ਪੁਸ਼ਟੀ ਕਰਦਾ ਹੈ। ਇਸ ਦੇ ਬਾਅਦ, ਤੁਹਾਡੇ 'ਤੇ ਇੱਕ ਅਹਿਮ ਟ੍ਰੇਨਿੰਗ ਪ੍ਰੋਗਰਾਮ ਲਈ ਭੁਗਤਾਨ ਕਰਨ ਲਈ ਦਬਾਅ ਪਾਇਆ ਜਾਂਦਾ ਹੈ।

ਸੁਰੱਖਿਆ ਦੇ ਉਪਾਅ

- ਹਮੇਸ਼ਾ ਪ੍ਰਮਾਣਿਤ ਜੌਬ ਪੋਰਟਲ ਦਾ ਹੀ ਇਸਤੇਮਾਲ ਕਰੋ।
- ਕਿਸੀ ਅਣਜਾਣ ਕੰਪਨੀ ਦੇ ਈਮੇਲ ਦਾ ਜਵਾਬ ਨਾ ਦਿਓ ਕਿਉਂਕਿ ਇਹ ਇੱਕ ਸਕੈਮ ਹੋ ਸਕਦਾ ਹੈ।

ATM ਕਾਰਡ ਸਕਿਮਿੰਗ

ਧੋਖਾਧੜੀ

- ATM ਮਸ਼ੀਨਾਂ ਵਿੱਚ ਸਕਿਮਿੰਗ ਉਪਕਰਨ ਪਾਏ ਗਏ ਹਨ, ਜਿਸ ਨਾਲ ਧੋਖੇਬਾਜ਼ ਤੁਹਾਡੇ ਕਾਰਡ ਤੋਂ ਡੇਟਾ ਲੈ ਸਕਦੇ ਹਨ ਅਤੇ ਇੱਕ ਡਮੀ ਕਾਰਡ ਅਤੇ ਇੱਕ ਛੋਟਾ / ਪਿਨਹੋਲ ਕੈਮਰਾ ਸਥਾਪਿਤ ਕਰ ਕੇ, ਜੋ ਬੜੀ ਕਾਰੀਗਰੀ ਨਾਲ ਛੁਪਾਇਆ ਗਿਆ ਹੁੰਦਾ ਹੈ, ਤੁਹਾਡਾ ਪਿਨ ਪ੍ਰਾਪਤ ਕਰ ਸਕਦਾ ਹੈ।
- ਕਈ ਵਾਰ, ਧੋਖੇਬਾਜ਼ ਆਮ ਗਾਹਕਾਂ ਦੇ ਰੂਪ ਵਿੱਚ ਸਾਹਮਣੇ ਆ ਸਕਦੇ ਹਨ ਅਤੇ ਜਦੋਂ ਤੁਸੀਂ PIN ਦਰਜ ਕਰ ਰਹੇ ਹੋ ਤਾਂ ਉਸ ਨੂੰ ਵੇਖ ਲੈਂਦਾ ਹੈ। ਫੇਰ ਇਸ ਜਾਣਕਾਰੀ ਦੀ ਵਰਤੋਂ ਡੁਪਲੀਕੇਟ ਕਾਰਡ ਬਣਾਉਣ ਅਤੇ ਗਾਹਕ ਦੇ ਖਾਤੇ ਤੋਂ ਪੈਸ ਕੱਢਣ ਲਈ ਕੀਤੀ ਜਾਂਦੀ ਹੈ।

ਸੁਰੱਖਿਆ ਦੇ ਉਪਾਅ

- ਜਾਂਚ ਕਰੋ ਕਿ ਕਿੱਥੇ ATM ਵਿੱਚ ਕੋਈ ਛੇੜਛਾੜ ਤਾਂ ਨਹੀਂ ਕੀਤੀ ਗਈ ਹੈ।
- ਆਪਣੇ ਇਰਦ ਗਿਰਦ ਸ਼ੱਕੀ ਲੋਕਾਂ ਤੇ ਨਜ਼ਰ ਰੱਖੋ।

SIM ਸਵੈਪ

ਧੋਖਾਧੜੀ

- ਕਿਉਂਕਿ ਤੁਹਾਡਾ ਰਜਿਸਟਰਡ ਮੋਬਾਈਲ ਨੰਬਰ ਤੁਹਾਡੇ ਖਾਤੇ ਦੀ ਜ਼ਿਆਦਾਤਰ ਜਾਣਕਾਰੀ ਅਤੇ ਪੁਸ਼ਟੀ ਨਾਲ ਜੁੜਿਆ ਹੋਇਆ ਹੈ, ਇਸ ਲਈ ਧੋਖੇਬਾਜ਼ ਤੁਹਾਡੇ SIM ਕਾਰਡ ਤੱਕ ਪਹੁੰਚ ਪਾਉਣ ਜਾਂ ਡੁਪਲੀਕੇਟ SIM ਕਾਰਡ ਪ੍ਰਾਪਤ ਕਰਨ ਦਾ ਯਤਨ ਕਰਦਾ ਹੈ ਤਾਂਕਿ ਡੁਪਲੀਕੇਟ ਸਿਮ ਤੇ ਆਏ OTP ਦੀ ਵਰਤੋਂ ਕਰ ਕੇ ਉਹ ਡਿਜਿਟਲ ਲੈਣ ਦੇਣ ਕਰ ਸਕੇ।
- ਜਾਲਸਾਜ ਆਮ ਤੌਰ ਤੇ ਗਾਹਕਾਂ ਨੂੰ ਓਹਨਾਂ ਦੀ ਨੈਟਵਰਕ ਕੰਪਨੀ ਤੋਂ ਹੋਣ ਦਾ ਦਾਅਵਾ ਕਰਦੇ ਹੋਏ ਕਾਲ ਕਰਦੇ ਹਨ, ਜੋ 3G ਤੋਂ 4G ਵਿੱਚ ਮੁਫਤ ਅਪਗ੍ਰੇਡ ਜਾਂ ਸਿਮ ਕਾਰਡ ਤੇ ਬੋਨੱਸ ਦੇ ਬਦਲੇ

ਸੁਰੱਖਿਆ ਦੇ ਉਪਾਅ

- ਜੇ ਤੁਹਾਡੇ ਫੋਨ ਵਿੱਚ ਕਾਫੀ ਸਮੇਂ ਤੋਂ ਮੋਬਾਈਲ ਨੈਟਵਰਕ ਨਹੀਂ ਹੈ ਤਾਂ ਤੁਹਾਨੂੰ ਸ਼ੰਦੇਹ ਹੋ ਜਾਣਾ ਚਾਹੀਦਾ ਹੈ।
- ਤੁਹਾਡੇ SIM ਦੇ ਲਈ ਕੋਈ ਡੁਪਲੀਕੇਟ SIM ਜਾਰੀ ਨਹੀਂ ਕੀਤਾ ਜਾ ਰਿਹਾ ਹੈ ਇਹ ਪੱਕਾ ਕਰਨ ਦੇ ਲਈ ਆਪਣੇ ਮੋਬਾਈਲ ਆਪ੍ਰੇਟਰ ਨਾਲ ਸੰਪਰਕ ਕਰੋ।

ਐਚ ਡੀ ਐਫ ਸੀ ਬੈਂਕ | SECURE BANKING | INTERNATIONAL FRAUD AWARENESS WEEK November 14th - 21st 2021 | ਮੂੰਹ ਬੰਦ ਰੱਖੋ

ਜਾਅਲੀ ਦਸਤਾਵੇਜ਼ਾਂ ਦੇ ਨਾਲ ਧੋਖਾਧੜੀ ਕਰ ਕੇ ਲੋਨ

ਧੋਖਾਧੜੀ

- ਇਹ ਧੋਖਾਧੜੀ ਉਸ ਵੇਲੇ ਹੁੰਦੀ ਹੈ ਜਦੋਂ ਕੋਈ ਵਿਅਕਤੀ ਜਾਂ ਸੰਸਥਾ ਵਲੋਂ ਵਿੱਤੀ ਸੰਸਥਾਵਾਂ ਤੋਂ ਕਿਸੀ ਵੀ ਪ੍ਰਕਾਰ ਦੀਆਂ ਸੇਵਾਵਾਂ ਦਾ ਲਾਭ ਪਾਉਣ ਦੇ ਲਈ ਜਾਅਲੀ ਦਸਤਾਵੇਜ਼ਾਂ ਦੀ ਵਰਤੋਂ ਕੀਤੀ ਜਾਂਦੀ ਹੈ।
- NBFC ਕਰਮਚਾਰੀ/NBFC ਦੀ ਈਮੇਲ ਆਈਡੀ ਦੀ ਪ੍ਰਮਾਣਿਕਤਾ ਦੀ ਪੁਸ਼ਟੀ ਕੀਤੇ ਬਿਨਾ ਵਿੱਤੀ ਸੰਸਥਾਵਾਂ ਦੇ ਨਾਲ KYC ਨਾਲ ਸਬੰਧਿਤ ਦਸਤਾਵੇਜ਼ਾਂ ਨੂੰ ਸਾਂਝਾ ਕਰਦੇ ਸਮੇਂ ਅਜਿਹੀ ਧੋਖਾਧੜੀ ਹੋ ਸਕਦੀ ਹੈ।
- ਪੀੜਤ ਵਿਅਕਤੀ ਦੀ ਨਿਜੀ ਜਾਣਕਾਰੀ, ਜਿਵੇਂ ਪਛਾਣ ਪੱਤਰ, ਬੈਂਕ ਖਾਤੇ ਸਬੰਧੀ ਵੇਰਵਾ, ਆਦਿ ਦੀ ਚੋਰੀ ਕਰ ਕੇ ਧੋਖਾਧੜੀ ਵਾਲੇ ਲੋਨ ਪਾਸ ਕੀਤੇ ਜਾਂਦੇ ਹਨ ਅਤੇ ਇਸ ਜਾਣਕਾਰੀ ਦੀ ਵਰਤੋਂ ਕਿਸੀ ਵਿੱਤੀ ਸੰਸਥਾ ਤੋਂ ਲਾਭ ਪ੍ਰਾਪਤ ਕਰਨ ਵਿੱਚ ਕੀਤੀ ਜਾਂਦੀ ਹੈ।

ਸੁਰੱਖਿਆ ਦੇ ਉਪਾਅ

- ਆਪਣੀ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਹਮੇਸ਼ਾ NBFC ਕਰਮਚਾਰੀ / ਕੰਪਨੀ ਦੀ ਪ੍ਰਮਾਣਿਕਤਾ ਦੀ ਪੁਸ਼ਟੀ ਕਰੋ।
- ਪਛਾਣ ਸਬੰਧੀ ਚੋਰੀ ਤੋਂ ਬਚਣ ਦੇ ਲਈ ਆਪਣੇ ਪਛਾਣ ਪੱਤਰ, ਬੈਂਕ ਖਾਤੇ ਸਬੰਧੀ ਵੇਰਵਾ ਆਦਿ ਸੁਰੱਖਿਅਤ ਰੱਖੋ।

ਆਧਾਰ OTP ਨਾਲ ਸਮਝੌਤਾ

ਧੋਖਾਧੜੀ

- ਆਧਾਰ ਅਧਾਰਤ OTP ਦੇ ਨਾਲ ਡਿਜਿਟਲ ਖਾਤੇ ਖੋਲੇ ਜਾ ਸਕਦੇ ਹਨ।
- ਅਜਿਹੇ ਕਈ ਉਦਾਹਰਨ ਹਨ ਜਿੱਥੇ ਗਾਹਕ ਆਪਣੇ UIDAI OTP ਨੂੰ ਤੀਜੀ ਪਾਰਟੀ ਦੇ ਵੈਂਡਰਾਂ ਨਾਲ ਸਾਂਝਾ ਕਰਦੇ ਹਨ, ਜਿਸ ਨਾਲ ਧੋਖੇਬਾਜ਼ਾਂ ਨੂੰ ਗਲਤ ਖਾਤਾ ਬਣਾਉਣ ਵਿੱਚ ਮਦਦ ਮਿਲਦੀ ਹੈ।

ਸੁਰੱਖਿਆ ਦੇ ਉਪਾਅ

- ਆਪਣੇ ਆਧਾਰ OTP ਨੂੰ ਅਪ੍ਰਮਾਣਿਤ ਸੰਸਥਾਵਾਂ ਨਾਲ ਸਾਂਝਾ ਨਾ ਕਰੋ।
- ਕਿਸੀ ਵੀ ਜਾਣਕਾਰੀ ਨੂੰ ਸਾਂਝਾ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਹਮੇਸ਼ਾ ਵਿਅਕਤੀ ਦੀ ਪਛਾਣ ਦੀ ਪੁਸ਼ਟੀ ਕਰੋ।

ਐਚ ਡੀ ਐਫ਼ ਸੀ ਬੈਂਕ

INDIA'S No.1* BANK

SECURE BANKING

ਵਧੇਰੀ ਜਾਣਕਾਰੀ ਦੇ ਲਈ,
ਐਚਡੀਐਫ਼ਸੀ ਬੈਂਕ ਦੇ ਸਿਕਯੋਰ ਬੈਂਕਿੰਗ ਪੇਜ ਤੇ ਜਾਓ।
https://www.hdfcbank.com/personal/useful-links/security

*ਰੀਟੇਲ ਲੋਨ ਬੁੱਕ ਸਾਈਜ਼ ਉੱਤੇ ਆਧਾਰਿਤ (ਮਾਰਗੇਜੇਜ਼ ਨੂੰ ਛੱਡ ਕੇ)। ਸ੍ਰੋਤ: FY 19-20 ਅਨੁਸਾਰ ਸਾਲਾਨਾ ਰਿਪੋਰਟ।
ਮਾਰਕੀਟ ਕੈਪੀਟਲਾਇਜ਼ੇਸ਼ਨ ਤੇ ਨੰ.1 ਆਧਾਰਿਤ ਹੈ BSE ਅੰਕੜੇ ਤੇ, 31 ਦਸੰਬਰ, 2020 ਦੇ ਦਿਨ।