ਇੱਥੇ ਸਕੈਮਰ,

ਉੱਥੇ ਸਕੈਮਰ

ਕਿਸੇ ਵੀ ਥਾਂ 'ਤੇ ਫਸ ਨਾ ਜਾਓ!

#BankingDhyaanSe2.0

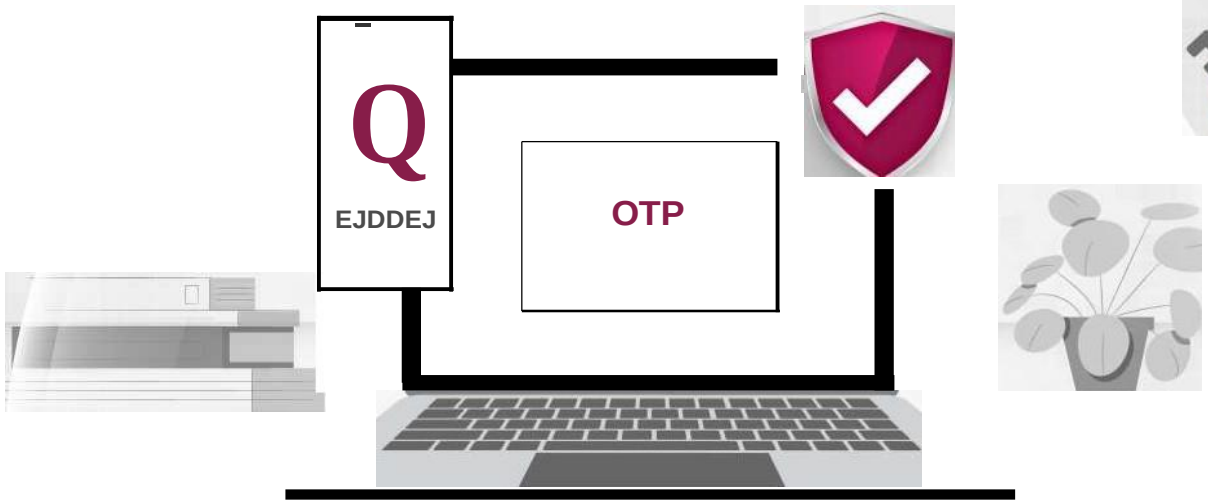
AXIS BANK

ਤੁਸੀਂ ਕਮਾਉਣ ਲਈ ਮਿਹਨਤ ਕਰਦੇ ਹੋ,
ਫਿਰ ਆਪਣੀ ਕਮਾਈ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਿਉਂ ਨਹੀਂ ਰੱਖਦੇ?

ਐਕਸਿਸ ਬੈਂਕ ਫ੍ਰੈਂਡ ਜਾਗਰੂਕਤਾ ਬੁੱਕਲੇਟ #BankingDhyaanSe 2.0, ਵਿੱਚ ਤੁਹਾਡਾ ਸਵਾਗਤ ਹੈ
ਵਿੱਤੀ ਘੁਟਾਲਿਆਂ ਨੂੰ ਸਮਝਣ ਅਤੇ ਰੋਕਣ ਲਈ ਤੁਹਾਡੀ ਕੀ। ਤੇਜ਼ੀ ਨਾਲ ਵਿਕਸਤ ਹੋ ਰਹੇ ਡਿਜੀਟਲ ਯੁੱਗ ਵਿੱਚ, ਗਿਆਨ ਧੋਖੇਬਾਜ਼ਾਂ ਵਿਰੁੱਧ ਤੁਹਾਡੀ ਢਾਲ ਹੈ। ਇਹ ਗਾਈਡਬੁੱਕ ਤੁਹਾਨੂੰ ਸੂਝ, ਅਸਲ-ਜੀਵਨ ਦੀਆਂ ਉਦਾਹਰਣਾਂ ਅਤੇ ਤੁਹਾਡੇ ਮਿਹਨਤ ਨਾਲ ਕਮਾਏ ਪੈਸੇ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਲਈ ਵਿਹਾਰਕ ਸੁਝਾਅ ਪ੍ਰਦਾਨ ਕਰਦੀ ਹੈ।

ਬੈਂਕਿੰਗ ਵਿੱਚ ਤੁਹਾਡੇ ਭਰੋਸੇਮੰਦ ਭਾਈਵਾਲ ਵਜੋਂ, ਐਕਸਿਸ ਬੈਂਕ ਡਿਜੀਟਲ ਲੈਂਡਸਕੇਪ ਨੂੰ ਵਿਸ਼ਵਾਸ ਨਾਲ ਨੇਵੀਗੇਟ ਕਰਨ ਵਿੱਚ ਤੁਹਾਡੀ ਮਦਦ ਕਰਨ ਲਈ ਸਮਰਪਿਤ ਹੈ। ਆਓ ਧੋਖੇ ਤੋਂ ਬਚੀਏ ਅਤੇ ਮਿਲ ਕੇ ਇੱਕ ਉੱਜਵਲ ਵਿੱਤੀ ਭਵਿੱਖ ਸੁਰੱਖਿਅਤ ਕਰੀਏ।

OTP ਸਕੈਮਸ



ਵਨ-ਟਾਈਮ ਪਾਸਵਰਡ ਤੁਹਾਡੇ ਅਭੇਦ ਡਿਜੀਟਲ ਕਿੰਗਡਮ ਤੱਕ ਪਹੁੰਚ ਕਰਨ ਲਈ ਇੱਕ ਗੋਲਡਨ ਕੀ ਹੈ।

ਤੁਹਾਡੀ ਕੀਮਤੀ **ਕੀ** ਨੂੰ ਚਲਾਕ ਠੱਗਾਂ ਤੋਂ ਬਚਾਉਣ ਲਈ, ਤੁਹਾਨੂੰ ਆਪਣੇ ਕਿਲਾ ਦਾ ਰੱਖਵਾਲਾ ਬਣਨਾ ਪਵੇਗਾ !

OTP ਨੂੰ ਗੁਪਤ ਰੱਖੋ: ਕਦੇ ਵੀ ਕਿਸੇ ਨਾਲ ਫੋਨ ਕਾਲਾਂ, ਈ-ਮੇਲਾਂ, ਟੈਕਸਟ ਸੁਨੇਹਿਆਂ ਜਾਂ ਸੋਸ਼ਲ ਮੀਡੀਆ ਰਾਹੀਂ OTP ਸਾਂਝਾ ਨਾ ਕਰੋ ਅਤੇ ਇੱਕ ਚੈਕਸ ਗਾਰਡ ਵਾਂਗ ਸਾਵਧਾਨ ਰਹੋ।

ਬੇਨਤੀਆਂ ਦੀ ਪੁਸ਼ਟੀ ਕਰੋ: ਭਰੋਸਾ ਕਰੋ ਪਰ ਤਸਦੀਕ ਕਰੋ। ਜੇਕਰ ਕੋਈ OTP ਬੇਨਤੀ ਅਚਾਨਕ ਆ ਜਾਂਦੀ ਹੈ ਜਾਂ ਤੁਹਾਨੂੰ ਸ਼ੱਕੀ ਲੱਗਦੀ ਹੈ, ਤਾਂ ਜਲਦਬਾਜ਼ੀ ਨਾ ਕਰੋ। ਇਸ ਨੂੰ ਦੇਣ ਤੋਂ ਪਹਿਲਾਂ ਆਪਣੇ ਜਵਾਬ ਦੀ ਪ੍ਰਮਾਣਿਕਤਾ ਦੀ ਦੋ ਵਾਰ ਜਾਂਚ ਕਰੋ।

ਅਧਿਕਾਰਤ ਵੈੱਬਸਾਈਟਾਂ ਜਾਂ ਐਪਸ ਦੀ ਵਰਤੋਂ ਕਰੋ: OTP ਸਾਂਝੇ ਕਰਦਿਆਂ ਸੁਰੱਖਿਅਤ ਰਹੋ। ਹਮੇਸ਼ਾ ਸਿੱਧੇ ਤੌਰ 'ਤੇ ਅਧਿਕਾਰਕ ਸਾਈਟ ਜਾਂ ਐਪ 'ਤੇ ਜਾਓ - ਕੋਈ ਸ਼ੌਰਟਕਟ ਨਹੀਂ। ਟਾਈਪਿੰਗ ਕਲਿੱਕ ਕਰਨ ਨਾਲੋਂ ਸੁਰੱਖਿਅਤ ਹੈ।

ਜ਼ਰੂਰੀ ਬੇਨਤੀਆਂ ਤੋਂ ਸਾਵਧਾਨ ਰਹੋ: ਸਕੈਮਰ ਅਕਸਰ ਤੁਹਾਡੇ OTP ਨੂੰ ਸਾਂਝਾ ਕਰਨ ਲਈ ਤੁਹਾਡੇ 'ਤੇ ਦਬਾਅ ਪਾਉਣ ਲਈ ਜ਼ਰੂਰੀ ਭਾਵਨਾ ਪੈਦਾ ਕਰਦੇ ਹਨ। ਕਾਰਵਾਈ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਇੱਕ ਕਦਮ ਪਿੱਛੇ ਜਾਓ, ਗੰਭੀਰਤਾ ਨਾਲ ਸੋਚੋ, ਅਤੇ ਸੁਤੰਤਰ ਤੌਰ 'ਤੇ ਬੇਨਤੀ ਦੀ ਪੁਸ਼ਟੀ ਕਰੋ।

ਟੂ-ਫੈਕਟਰ ਪ੍ਰਮਾਣੀਕਰਨ ਨੂੰ ਸਮਰੱਥ ਬਣਾਓ: 2FA (ਟੂ-ਫੈਕਟਰ ਪ੍ਰਮਾਣੀਕਰਨ) ਨਾਲ ਸੁਰੱਖਿਆ 'ਤੇ ਡਬਲ ਡਾਊਨ ਕਰੋ। ਐਪ-ਅਧਾਰਿਤ ਜਾਂ ਹਾਰਡਵੇਅਰ ਟੋਕਨਾਂ ਵਰਗੇ ਰੌਕ-ਸੋਲਿਡ ਵਿਕਲਪ ਚੁਣੋ। ਉਹ ਕਿਸੇ ਵੀ ਦਿਨ SMS OTP ਨੂੰ ਪਛਾੜਦੇ ਹਨ।

ਕਿਰਪਾ ਕਰਕੇ ਯਾਦ ਰੱਖੋ, ਬੈਂਕ ਤੁਹਾਡੇ CVV, OTP, PIN, ਕਾਰਡ ਨੰਬਰ, ਪਾਸਵਰਡ ਆਦਿ ਦੀ ਮੰਗ ਨਹੀਂ ਕਰੇਗਾ। ਇਨ੍ਹਾਂ ਵੇਰਵਿਆਂ ਨੂੰ ਕਿਸੇ ਨਾਲ ਸਾਂਝਾ ਨਾ ਕਰੋ।

ਕ੍ਰੈਡਿਟ ਕਾਰਡ ਸਕੈਮ

ਆਓ ਕ੍ਰੈਡਿਟ ਕਾਰਡ ਸਕੈਮਰ ਨੂੰ ਲੁਕਾਉਣ ਅਤੇ ਲੱਭਣ ਦੀ ਇੱਕ ਗੁੰਝਲਦਾਰ ਖੇਡ ਵਜੋਂ ਕਲਪਨਾ ਕਰੀਏ। ਜਿਵੇਂ ਕਿ ਇੱਕ ਸਕੈਮਰ ਆਪਣੇ ਸੱਚੇ ਇਰਾਦਿਆਂ ਨੂੰ ਲੁਕਾਉਣ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰਦਾ ਹੈ, ਉਹ ਤੁਹਾਨੂੰ ਤੁਹਾਡੀ ਕ੍ਰੈਡਿਟ ਕਾਰਡ ਜਾਣਕਾਰੀ ਦਾ ਖੁਲਾਸਾ ਕਰਨ ਲਈ ਧੋਖਾ ਦੇ ਸਕਦੇ ਹਨ।

ਉਨ੍ਹਾਂ ਦੇ ਜਾਲ ਵਿੱਚ ਫਸਣ ਤੋਂ ਬਚਣ ਲਈ, ਇਹਨਾਂ ਟਿਪਸ ਨੂੰ ਧਿਆਨ ਵਿੱਚ ਰੱਖੋ:

ਫਿਸ਼ਰਾਂ ਦਾ ਧਿਆਨ ਰੱਖੋ: ਸਕੈਮਰ ਤੁਹਾਡੇ ਬੈਂਕ ਜਾਂ ਕਿਸੇ ਜਾਣੀ-ਪਛਾਣੀ ਕੰਪਨੀ ਤੋਂ ਹੋਣ ਦਾ ਦਿਖਾਵਾ ਕਰ ਸਕਦੇ ਹਨ। ਉਨ੍ਹਾਂ ਦੀਆਂ ਚਾਲਾਂ ਵਿੱਚ ਨਾ ਫਸੋ; ਉਨ੍ਹਾਂ ਦੀ ਪਛਾਣ ਦੀ ਪੁਸ਼ਟੀ ਕਰੋ।

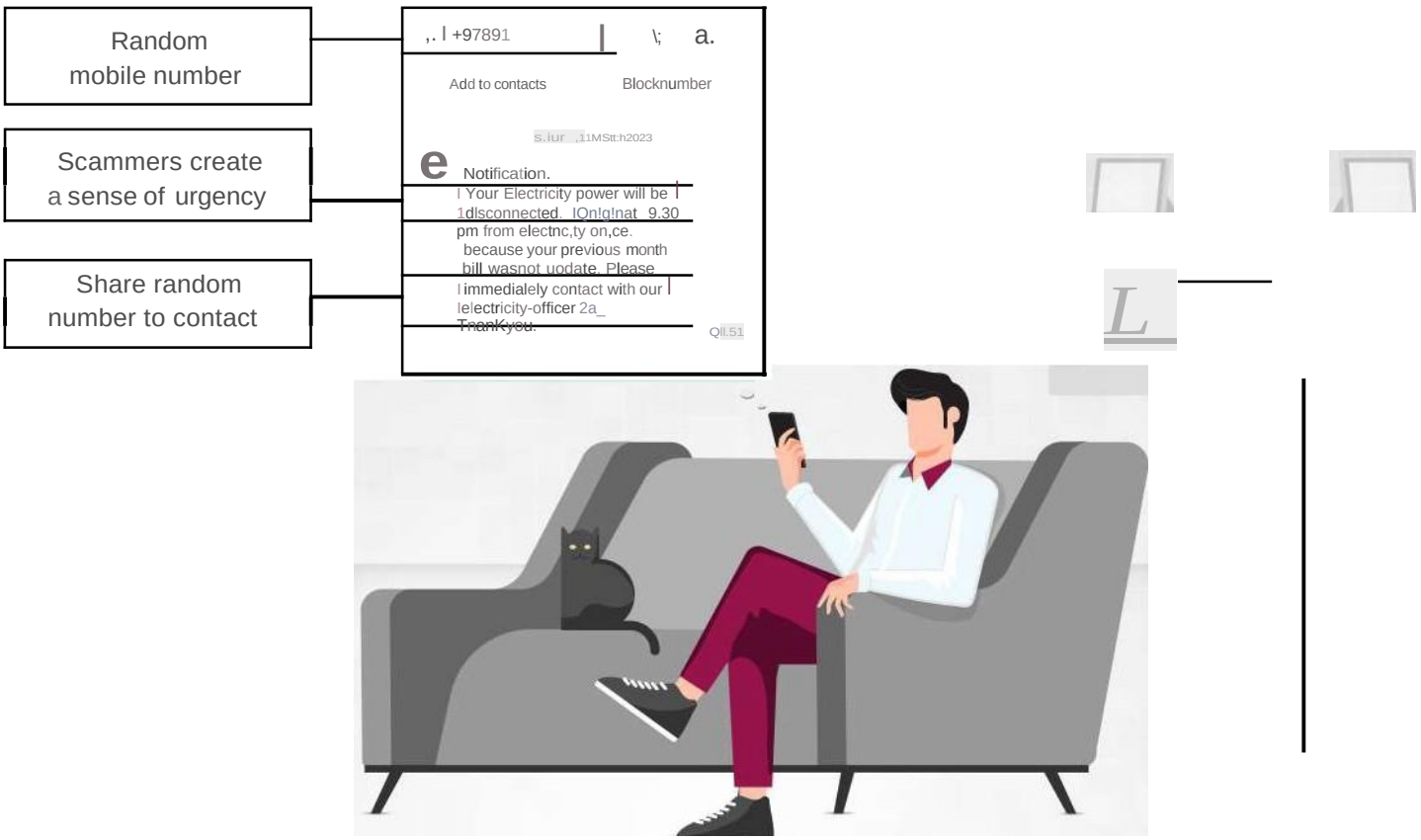
ਆਪਣੇ ਸਟੇਟਮੈਂਟਸ ਦੀ ਜਾਂਚ ਕਰੋ: ਨਿਯਮਤ ਤੌਰ 'ਤੇ ਆਪਣੀਆਂ ਕ੍ਰੈਡਿਟ ਕਾਰਡ ਸਟੇਟਮੈਂਟਸ ਦੀ ਸਮੀਖਿਆ ਕਰੋ। ਜੇਕਰ ਤੁਸੀਂ ਅਣਜਾਣ ਖਰਚੇ ਜਾਂ ਚਾਰਜ ਪਾਈਏ, ਇਹ ਖੇਡ ਵਿੱਚ ਲੁਕਿਆ ਹੋਇਆ ਖਿਡਾਰੀ ਲੱਭਣ ਵਰਗਾ ਹੈ—ਉਹਨਾਂ ਨੂੰ ਤੁਰੰਤ ਪਤਾ ਲਗਾਓ।

ਟ੍ਰਾਂਜੈਕਸਨ ਦੀ ਸੀਮਾਵਾਂ ਸੈੱਟ ਕਰੋ: ਆਪਣੇ ਸਾਰੇ ਭੁਗਤਾਨ ਚੈਨਲਾਂ 'ਤੇ ਟ੍ਰਾਂਜੈਕਸਨ ਦੀਆਂ ਸੀਮਾਵਾਂ ਸੈਟ ਕਰੋ ਅਤੇ 'ਵਰਤੋਂ ਦਾ ਪ੍ਰਬੰਧਨ ਕਰੋ' ਸੈਕਸ਼ਨ ਨੂੰ ਆਪਣੀ ਲੋੜ ਅਨੁਸਾਰ ਅਨੁਕੂਲਿਤ ਕਰੋ।
ਸਿਰਫ ਸੁਰੱਖਿਅਤ ਸਾਈਟਾਂ: ਆਨਲਾਈਨ ਖਰੀਦਦਾਰੀ ਕਰਦੇ ਸਮੇਂ, ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਵੈਬਸਾਈਟ ਸੁਰੱਖਿਅਤ ਹੈ (URL ਵਿੱਚ "https" ਦੀ ਭਾਲ ਕਰੋ)। ਇਹ ਖੇਡ ਲਈ ਇੱਕ ਸੁਰੱਖਿਅਤ ਖੇਡ ਦੇ ਮੈਦਾਨ ਦੀ ਚੋਣ ਕਰਨ ਵਰਗਾ ਹੈ।

ਅੱਪਡੇਟ ਰਹੋ: ਹਮੇਸ਼ਾ ਨਵੇਂ ਸਕੈਮਰ ਦੇ ਤਰੀਕਿਆਂ 'ਤੇ ਨਿਗਾਹ ਰੱਖੋ, ਜਿਵੇਂ ਤੁਸੀਂ ਖੇਡ ਵਿੱਚ ਨਵੀਆਂ ਯੋਜਨਾਵਾਂ ਸਿੱਖਦੇ ਹੋ। ਇਸ ਤਰ੍ਹਾਂ, ਤੁਸੀਂ ਸਕੈਮਰਸ ਨੂੰ ਚਾਲਾਕੀ ਨਾਲ ਹਰਾ ਸਕੋਗੇ।

ਬਿਜਲੀ ਬਿੱਲ ਫਰਾਡ

ਜਾਅਲੀ SMS ਦੀ ਪਛਾਣ ਕਿਵੇਂ ਕਰੀਏ?



ਇਹ ਤਸਵੀਰ ਬਣਾ ਲਓ: ਤੁਸੀਂ ਘਰ ਵਿੱਚ ਆਰਾਮਦਾਇਕ ਸ਼ਾਮ ਬਿਤਾ ਰਹੇ ਹੋ, ਆਪਣੇ ਪਸੰਦਦੇ ਟੀਵੀ ਸ਼ੋ ਨੂੰ ਦੇਖਦੇ ਹੋ, ਜਦੋਂ ਤੁਹਾਡੇ ਫੋਨ 'ਤੇ ਇੱਕ ਆਉਣ ਵਾਲਾ ਸੁਨੇਹਾ ਆਉਂਦਾ ਹੈ। ਇਹ ਤੁਹਾਡਾ ਬਿਜਲੀ ਸਪਲਾਇਰ ਹੈ, ਅਤੇ ਉਹ ਦਾਅਵਾ ਕਰ ਰਹੇ ਹਨ ਕਿ ਤੁਹਾਨੂੰ ਆਪਣੇ ਨਵੇਂ ਬਿਲ ਲਈ ਬਹੁਤ ਜ਼ਿਆਦਾ ਰਕਮ ਦੇਣੀ ਹੈ।

ਘਬਰਾਉਣ ਤੋਂ ਪਹਿਲਾਂ, ਇਸ 'ਤੇ ਵਿਚਾਰ ਕਰੋ: ਬਿਜਲੀ ਦੇ ਬਿੱਲ ਦੀ ਧੋਖਾਧੜੀ, ਕਿਸੇ ਲੁਪਤ ਭੂਤ ਦੀ ਤਰ੍ਹਾਂ, ਬਿਨਾਂ ਕਿਸੇ ਚੇਤਾਵਨੀ ਦੇ ਤੁਹਾਡੀ ਜ਼ਿੰਦਗੀ ਵਿਚ ਦਾਖਲ ਹੋ ਸਕਦੀ ਹੈ।

ਆਪਣੇ ਗੁਪਤ ਵੇਰਵਿਆਂ ਨੂੰ ਕਦੇ ਵੀ ਕਿਸੇ ਨਾਲ ਸਾਂਝਾ ਨਾ ਕਰੋ ਅਤੇ ਨਾ ਹੀ ਅਣਚਾਹੇ ਲਿੰਕਾਂ 'ਤੇ ਕਲਿੱਕ ਕਰੋ।

ਬਿੱਲ ਦੇ ਭੁਗਤਾਨ ਲਈ ਸਿਰਫ਼ ਅਧਿਕਾਰਤ ਅਤੇ ਸੁਰੱਖਿਅਤ ਵੈੱਬਸਾਈਟਾਂ ਦੀ ਵਰਤੋਂ ਕਰੋ।

ਯਾਦ ਰੱਖੋ, ਬਿਜਲੀ ਵਿਭਾਗ ਕਦੇ ਵੀ ਬੇਤਰਤੀਬ/ਅਣਰਜਿਸਟਰਡ ਨੰਬਰਾਂ ਰਾਹੀਂ ਨਿੱਜੀ ਵੇਰਵੇ ਜਾਂ ਭੁਗਤਾਨ ਨਹੀਂ ਮੰਗਦਾ ਹੈ।

ਨੌਕਰੀ ਸਕੈਮ

ਕਲਪਨਾ ਕਰੋ ਕਿ ਤੁਸੀਂ ਨੌਕਰੀ ਦੀਆਂ ਸੂਚੀਆਂ ਨੂੰ ਸਕ੍ਰੋਲ ਕਰ ਰਹੇ ਹੋ, ਅਤੇ ਅਚਾਨਕ ਤੁਸੀਂ ਨੌਕਰੀ ਦੀ ਪੇਸ਼ਕਸ਼ ਕਰਦੇ ਹੋ ਜੋ ਸੱਚ ਹੋਣ ਲਈ ਬਹੁਤ ਵਧੀਆ ਜਾਪਦੀ ਹੈ. ਅਸੀਮਤ ਛੁੱਟੀਆਂ ਦੇ ਦਿਨ, ਪਜਾਮਾ ਵਿੱਚ ਕੰਮ, ਅਤੇ ਡਾਟਾ ਐਂਟਰੀ ਲਈ ਛੇ ਅੰਕਾਂ ਦੀ ਤਨਖਾਹ? ਮੈਨੂੰ ਸਾਈਨ ਅੱਪ ਕਰੋ! "ਹੁਣੇ ਲਾਗੂ ਕਰੋ" ਬਟਨ ਨੂੰ ਦਬਾਉਣ ਤੋਂ ਪਹਿਲਾਂ ਉਡੀਕ ਕਰੋ!

ਕੰਪਨੀ ਦੀ ਖੋਜ ਕਰੋ: ਕੰਪਨੀ ਨੂੰ ਔਨਲਾਈਨ ਵੇਖੋ ਅਤੇ ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਇਹ ਨਾਮਵਰ ਹੈ। ਧੋਖਾਧੜੀ ਕਰਨ ਵਾਲੇ ਅਕਸਰ ਯਕੀਨਯੋਗ ਵੈਬਸਾਈਟਾਂ ਵਾਲੀਆਂ ਜਾਅਲੀ ਕੰਪਨੀਆਂ ਬਣਾਉਂਦੇ ਹਨ।

ਅਗਾਊਂ ਭੁਗਤਾਨ ਨਾ ਕਰੋ: ਜਾਇਜ਼ ਰੁਜ਼ਗਾਰਦਾਤਾ ਤੁਹਾਨੂੰ ਕੰਮ ਸ਼ੁਰੂ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਸਿਖਲਾਈ, ਸਮੱਗਰੀ, ਜਾਂ ਪਿਛੋਕੜ ਦੀ ਜਾਂਚ ਲਈ ਭੁਗਤਾਨ ਕਰਨ ਲਈ ਨਹੀਂ ਕਹਿਣਗੇ।

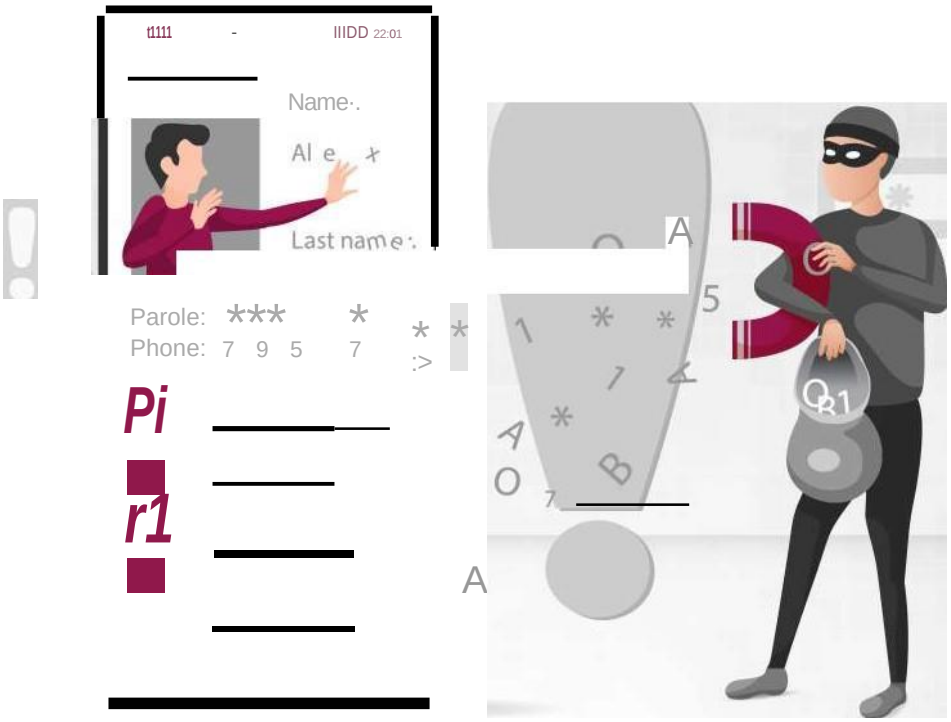
ਲਾਲ ਝੰਡਿਆਂ ਦੀ ਨਿਗਰਾਨੀ ਕਰੋ: ਸਾਵਧਾਨ ਰਹੋ ਜੇ ਨੌਕਰੀ ਲਈ ਤੁਹਾਨੂੰ ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਜਿਵੇਂ ਕਿ ਤੁਹਾਡਾ ਸਮਾਜਿਕ ਸੁਰੱਖਿਆ ਨੰਬਰ ਜਾਂ ਵਿੱਤੀ ਵੇਰਵੇ ਤੁਰੰਤ ਪ੍ਰਦਾਨ ਕਰਨ ਦੀ ਲੋੜ ਹੁੰਦੀ ਹੈ।

ਭਰਤੀ ਕਰਨ ਲਈ ਬਹੁਤ ਜਲਦੀ: ਜੇ ਤੁਹਾਨੂੰ ਇੰਟਰਵਿਊ ਜਾਂ ਬਹੁਤ ਸਾਰੀ ਜਾਣਕਾਰੀ ਦੇ ਆਦਾਨ-ਪ੍ਰਦਾਨ ਤੋਂ ਬਿਨਾਂ ਮੌਕੇ 'ਤੇ ਨੌਕਰੀ ਦੀ ਪੇਸ਼ਕਸ਼ ਕੀਤੀ ਜਾਂਦੀ ਹੈ, ਤਾਂ ਇਹ ਇੱਕ ਸਕੈਮ ਹੋ ਸਕਦਾ ਹੈ।

ਆਪਣੇ ਅਨੁਭਵ 'ਤੇ ਭਰੋਸਾ ਕਰੋ: ਜੇ ਕੁਝ ਗਲਤ ਮਹਿਸੂਸ ਹੁੰਦਾ ਹੈ, ਤਾਂ ਆਪਣੇ ਅਨੁਭਵ 'ਤੇ ਭਰੋਸਾ ਕਰੋ ਅਤੇ ਸਾਵਧਾਨੀ ਨਾਲ ਅੱਗੇ ਵਧੋ ਜਾਂ ਦੂਰ ਚਲੇ ਜਾਓ।

ਯਾਦ ਰੱਖੋ, ਨੌਕਰੀ ਲੱਭਦੇ ਸਮੇਂ ਤੁਹਾਡੀ ਨਿੱਜੀ ਅਤੇ ਵਿੱਤੀ ਜਾਣਕਾਰੀ ਦੀ ਸੁਰੱਖਿਆ ਤੁਹਾਡੀ ਪਹਿਲੀ ਤਰਜੀਹ ਹੋਣੀ ਚਾਹੀਦੀ ਹੈ।

ਕਾਲ ਸਪੂਫਿੰਗ ਸਕੈਮ

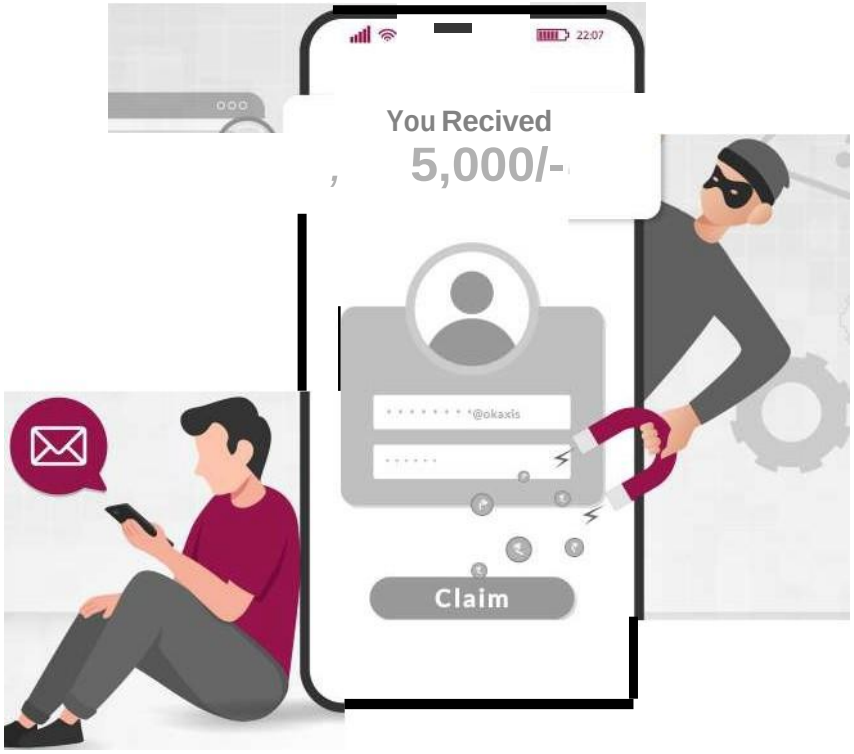


ਜਿਵੇਂ ਕਿ ਇੱਕ ਜਾਦੂਗਰ ਚੀਜ਼ਾਂ ਨੂੰ ਅਸਲ ਵਿੱਚ ਉਨ੍ਹਾਂ ਨਾਲੋਂ ਵੱਖਰਾ ਦਿਖਾ ਸਕਦਾ ਹੈ, ਸਕੈਮਰ ਤੁਹਾਡੀ ਕਾਲਰ ID ਵਿੱਚ ਹੇਰਾਫੇਰੀ ਕਰ ਸਕਦੇ ਹਨ ਤਾਂ ਜੋ ਇਹ ਜਾਪਦਾ ਹੋਵੇ ਕਿ ਉਹ ਕੋਈ ਅਜਿਹਾ ਵਿਅਕਤੀ ਹੈ ਜਿਸਨੂੰ ਤੁਸੀਂ ਜਾਣਦੇ ਹੋ ਜਾਂ ਵਿਸ਼ਵਾਸ ਕਰਦੇ ਹੋ - ਇਸ ਮਾਮਲੇ ਵਿੱਚ, ਤੁਹਾਡਾ ਬੈਂਕ। ਇਹ ਉਨ੍ਹਾਂ ਦੀ ਅਸਲ ਪਛਾਣ ਲਈ ਇੱਕ ਡਿਜੀਟਲ ਭੇਸ ਵਰਗਾ ਹੈ।
ਆਪਣੇ ਆਪ ਨੂੰ ਇਸ ਗੁੰਝਲਦਾਰ ਚਾਲ ਤੋਂ ਬਚਾਉਣ ਲਈ, ਇਹਨਾਂ ਸੁਝਾਵਾਂ ਨੂੰ ਯਾਦ ਰੱਖੋ:

ਸਾਵਧਾਨੀ ਨਾਲ ਪੁਸ਼ਟੀ ਕਰੋ: ਭਾਵੇਂ ਕਾਲਰ ID ਜਾਣੀ-ਪਛਾਣੀ ਲੱਗਦੀ ਹੈ, ਸਾਵਧਾਨ ਰਹੋ। ਜੇ ਕੋਈ ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਮੰਗਦਾ ਹੈ, ਤਾਂ ਹੋਰ ਸਾਧਨਾਂ ਰਾਹੀਂ ਉਸਦੀ ਪਛਾਣ ਦੀ ਦੁਬਾਰਾ ਜਾਂਚ ਕਰੋ।
ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਨਾ ਕਰੋ: ਕਦੇ ਵੀ ਫੋਨ 'ਤੇ ਨਿੱਜੀ ਜਾਂ ਵਿੱਤੀ ਜਾਣਕਾਰੀ ਨਾ ਦਿਓ, ਭਾਵੇਂ ਕਾਲ ਕਰਨ ਵਾਲਾ ਜਾਇਜ਼ ਜਾਪਦਾ ਹੋਵੇ। ਰੁਕੋ ਅਤੇ ਕਿਸੇ ਭਰੋਸੇਮੰਦ ਨੰਬਰ ਦੀ ਵਰਤੋਂ ਕਰਕੇ ਵਾਪਸ ਕਾਲ ਕਰੋ।
ਨਿੱਜੀ ਰਹੋ: ਇਸ ਬਾਰੇ ਸਾਵਧਾਨ ਰਹੋ ਕਿ ਤੁਸੀਂ ਆਨਲਾਈਨ ਜਾਂ ਸੋਸ਼ਲ ਮੀਡੀਆ 'ਤੇ ਕਿਹੜੇ ਨਿੱਜੀ ਵੇਰਵੇ ਸਾਂਝੇ ਕਰਦੇ ਹੋ। ਸਕੈਮਰ ਅਕਸਰ ਇਨ੍ਹਾਂ ਸਰੋਤਾਂ ਤੋਂ ਜਾਣਕਾਰੀ ਇਕੱਠੀ ਕਰਦੇ ਹਨ ਤਾਂ ਜੋ ਉਨ੍ਹਾਂ ਦੀਆਂ ਸਪੂਫ ਕੀਤੀਆਂ ਕਾਲਾਂ ਨੂੰ ਵਧੇਰੇ ਯਕੀਨਯੋਗ ਬਣਾਇਆ ਜਾ ਸਕੇ।
ਕਾਲ ਬਲਾਕਿੰਗ ਦੀ ਵਰਤੋਂ ਕਰੋ: ਆਪਣੇ ਫ਼ੋਨ ਕੈਰੀਅਰ ਦੁਆਰਾ ਪ੍ਰਦਾਨ ਕੀਤੀਆਂ ਕਾਲ-ਬਲਾਕਿੰਗ ਐਪਾਂ ਜਾਂ ਵਿਸ਼ੇਸ਼ਤਾਵਾਂ ਦੀ ਪੜਚੋਲ ਕਰੋ। ਉਹ ਸੰਭਾਵਿਤ ਸਕੈਮ ਕਾਲਾਂ ਨੂੰ ਫਿਲਟਰ ਕਰਨ ਵਿੱਚ ਮਦਦ ਕਰ ਸਕਦੇ ਹਨ।

ਗੂਗਲ ਜਾਂ ਕਿਸੇ ਵੀ ਸਰਚ ਇੰਜਣ 'ਤੇ ਫੋਨ ਨੰਬਰਾਂ ਦੀ ਖੋਜ ਨਾ ਕਰੋ। ਜੇ ਤੁਸੀਂ ਅਜਿਹਾ ਕਰਦੇ ਹੋ, ਤਾਂ ਸੰਸਥਾ ਜਾਂ ਵਪਾਰੀ ਦੁਆਰਾ ਤੁਹਾਨੂੰ ਭੇਜੇ ਗਏ ਕਿਸੇ ਵੀ ਲਿੰਕ 'ਤੇ ਕਲਿੱਕ ਨਾ ਕਰੋ।
ਇਸ ਤੋਂ ਇਲਾਵਾ, ਕਿਰਪਾ ਕਰਕੇ ਇਹ ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਤੁਹਾਡੇ ਕੋਲ ਸਿਰਫ ਅਧਿਕਾਰਤ ਐਪਲੀਕੇਸ਼ਨ ਸਟੋਰਾਂ ਤੋਂ ਤੁਹਾਡੇ ਡਿਵਾਈਸਾਂ 'ਤੇ ਡਾਊਨਲੋਡ ਕੀਤੀਆਂ ਬੈਂਕਿੰਗ ਐਪਲੀਕੇਸ਼ਨਾਂ ਦੇ ਨਵੀਨਤਮ ਸੰਸਕਰਣ ਹਨ।
ਕਿਰਪਾ ਕਰਕੇ ਸਮੇਂ-ਸਮੇਂ 'ਤੇ ਇਸ ਦੀ ਜਾਂਚ ਕਰੋ।
ਯਾਦ ਰੱਖੋ, ਜਿਵੇਂ ਤੁਸੀਂ ਅਸਲ ਜ਼ਿੰਦਗੀ ਵਿਚ ਕਿਸੇ ਨਕਾਬਪੋਸ਼ ਅਜਨਬੀ 'ਤੇ ਭਰੋਸਾ ਨਹੀਂ ਕਰੋਗੇ, ਉਸੇ ਤਰ੍ਹਾਂ ਫੋਨ 'ਤੇ ਨਕਾਬਪੋਸ਼ ਕਾਲਰ 'ਤੇ ਭਰੋਸਾ ਨਾ ਕਰੋ। ਸਾਵਧਾਨ ਰਹੋ!

UPI ਰਿਫੰਡ ਸਕੈਮ

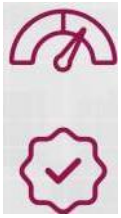


ਕਲਪਨਾ ਕਰੋ ਕਿ ਤੁਸੀਂ ਆਪਣੇ ਫੋਨ ਨੂੰ ਸਲੋਲ ਕਰ ਰਹੇ ਹੋ ਜਦੋਂ ਤੁਸੀਂ ਇੱਕ UPI ਰਿਫੰਡ ਸੂਚਨਾ ਦੇਖਦੇ ਹੋ, ਅਤੇ ਅਚਾਨਕ, ਤੁਸੀਂ ਬਹੁਤ ਖੁਸ਼ ਹੋ ਜਾਂਦੇ ਹੋ! ਪਰ ਥੋੜ੍ਹੀ ਦੇਰ ਲਈ ਰੁਕੋ। ਇਹ ਇੱਕ UPI ਰਿਫੰਡ ਸਕੈਮ ਹੋ ਸਕਦਾ ਹੈ!

UPI ਜਾਂ ਯੂਨੀਫਾਈਡ ਪੇਮੇਂਟਸ ਇੰਟਰਫੇਸ ਸਾਡੀ ਰੋਜ਼ਾਨਾ ਜ਼ਿੰਦਗੀ ਦਾ ਹਿੱਸਾ ਬਣ ਗਿਆ ਹੈ। ਸਥਾਨਕ ਕੀਰਾਣਾ ਸਟੋਰਾਂ 'ਤੇ ਭੁਗਤਾਨ ਕਰਨ ਤੋਂ ਲੈ ਕੇ ਫੋਨ ਰੀਚਾਰਜ ਕਰਨ ਅਤੇ ਫਲਾਈਟ ਦੀਆਂ ਟਿਕਟਾਂ ਬੁੱਕ ਕਰਨ ਤੱਕ, ਅਸੀਂ ਵੱਖ-ਵੱਖ ਚੀਜ਼ਾਂ ਲਈ UPI ਪੇਮੈਂਟ ਦਾ ਉਪਯੋਗ ਕਰਦੇ ਹਾਂ। ਇਸ ਲਈ ਸਕੈਮ ਕਰਨ ਵਾਲੇ ਲੋਕ UPI ਐਪਾਂ ਦੀ ਵਰਤੋਂ ਕਰਕੇ ਲੋਕਾਂ ਨੂੰ ਚਲਾਕੀ ਨਾਲ ਵੰਧਣ ਦੇ ਨਵੇਂ ਤਰੀਕੇ ਅਪਨਾਉਣ ਲੱਗੇ ਹਨ।

ਉਹਨਾਂ ਦੇ ਆਧਿਕਾਰਿਕ ਭਾਸ਼ਾ ਅਤੇ ਪੇਸ਼ਾਵਰ ਬੋਲ-ਚਾਲ ਵਿੱਚ ਨਾ ਆਓ। ਹੇਠ ਲਿਖੇ ਸੁਝਾਅ ਯਾਦ ਰੱਖੋ:

ਲਿੰਕਾਂ ਤੋਂ ਸਾਵਧਾਨ ਰਹੋ: ਠੱਗੇ ਤੁਹਾਨੂੰ ਇੱਕ ਲਿੰਕ ਭੇਜ ਸਕਦੇ ਹਨ, ਜੇਹੜਾ ਤੁਹਾਨੂੰ ਰੀਫੰਡ ਦਾ ਦਾਅਵਾ ਕਰਨ ਲਈ ਰਜਿਸਟਰ ਕਰਨ ਦੀ ਸਲਾਹ ਦੇਵੇਗਾ।



ਉੱਚ ਦਬਾਅ ਵਾਲੇ ਤਰੀਕੇ: ਉਹ ਤੁਹਾਨੂੰ ਤੁਰੰਤ ਪੈਸੇ ਲਈ ਬੈਂਕ ਵੇਰਵੇ ਜਾਂ UPI PIN ਭਰਨ ਲਈ ਦਬਾਅ ਡਾਲਣਗੇ।

ਯੋਗਤਾ ਦੀ ਜਾਂਚ ਕਰੋ: ਯਕੀਨ ਕਰੋ ਕਿ ਤੁਸੀਂ ਰੀਫੰਡ ਲਈ ਯੋਗ ਹੋ। ਜੇ ਹਾਂ, ਤਾਂ ਇੱਕ ਭਰੋਸੇਮੰਦ ਸ੍ਰੋਤ ਦੀ ਜਾਂਚ ਕਰੋ।

ਯਾਦ ਰੱਖੋ, ਬੈਂਕ ਜਾਂ ਹੋਰ ਅਧਿਕਾਰੀ ਕਦੇ ਵੀ ਤੁਹਾਡੇ ਤੋਂ ਇੰਨਾ ਸੰਵੇਦਨਸ਼ੀਲ ਵੇਰਵੇ ਨਹੀਂ ਮੰਗਣਗੇ।.

ਫਿਸ਼ਿੰਗ ਸਕੈਮ

ਕਲਪਨਾ ਕਰੋ ਕਿ ਤੁਸੀਂ ਇੱਕ ਮੱਛੀ ਹੋ ਜੋ ਇੱਕ ਸਾਫ਼ ਤਲਾਬ ਵਿੱਚ ਸ਼ਾਂਤੀ ਨਾਲ ਤੈਰ ਰਹੀ ਹੈ, ਆਪਣੇ ਖੁਦ ਦੇ ਕਾਰੋਬਾਰ ਨੂੰ ਧਿਆਨ ਵਿੱਚ ਰੱਖਦੀ ਹੈ. ਅਚਾਨਕ, ਇੱਕ ਚਮਕਦਾਰ, ਮਨਮੋਹਕ ਚਾਰਾ ਤੁਹਾਡੇ ਸਾਹਮਣੇ ਆ ਉਂਦਾ ਹੈ. ਤੁਸੀਂ ਉਤਸੁਕ ਹੋ ਪਰ ਉਡੀਕ ਕਰੋ - ਕੁਝ ਗੜਬੜ ਹੈ!
ਫਿਸ਼ਿੰਗ ਸਕੈਮ ਨਾਲ ਡਿਜੀਟਲ ਖੇਤਰ ਵਿੱਚ ਬਿਲਕੁਲ ਇਹੀ ਵਾਪਰਦਾ ਹੈ।

ਸਾਈਬਰ ਅਪਰਾਧੀ ਤੁਹਾਨੂੰ ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਦਾ ਖੁਲਾਸਾ ਕਰਨ ਲਈ ਧੋਖਾ ਦੇਣ ਲਈ ਭਰੋਸੇਮੰਦ ਸ਼ਖਸੀਅਤਾਂ ਵਜੋਂ ਪੇਸ਼ ਹੁੰਦੇ ਹਨ, ਜਿਵੇਂ ਕਿ ਮੱਛੀ ਨੂੰ ਚਾਰੇ ਦੁਆਰਾ ਲਾਲਚ ਦਿੱਤਾ ਜਾਂਦਾ ਹੈ। ਉਹ ਜਾਅਲੀ ਈਮੇਲਾਂ, ਸੰਦੇਸ਼, ਜਾਂ ਵੈਬਸਾਈਟਾਂ ਭੇਜਦੇ ਹਨ ਜੋ ਜਾਇਜ਼ ਜਾਪਦੀਆਂ ਹਨ, ਅਕਸਰ ਬੈਂਕਾਂ, ਸੋਸ਼ਲ ਮੀਡੀਆ, ਜਾਂ ਇੱਥੋਂ ਤੱਕ ਕਿ ਤੁਹਾਡੇ ਬੌਸ ਦੀ ਨਕਲ ਕਰਦੇ ਹਨ।

ਇਹਨਾਂ ਡਿਜੀਟਲ ਹੁੱਕਾਂ ਤੋਂ ਬਚਣ ਲਈ, ਇਹਨਾਂ ਸੁਝਾਵਾਂ ਨੂੰ ਯਾਦ ਰੱਖੋ:

ਡਬਲ-ਚੈੱਕ **URL**: ਲਿੰਕਾਂ 'ਤੇ ਹੋਵਰ ਕਰਕੇ ਦੇਖੋ ਕਿ ਉਹ ਕਿੱਥੇ ਜਾਂਦੇ ਹਨ। ।

ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਨਾ ਕਰੋ: ਕਾਨੂੰਨੀ ਸੰਸਥਾਵਾਂ ਈਮੇਲ ਰਾਹੀਂ ਸੰਵੇਦਨਸ਼ੀਲ ਚੀਜ਼ਾਂ ਦੀ ਮੰਗ ਨਹੀਂ ਕਰਨਗੀਆਂ।

rl2J

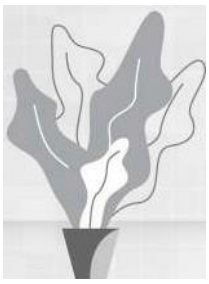
ਸੰਦੇਹੀ ਰਹੋ: ਅਚਾਨਕ ਬੇਨਤੀਆਂ? ਕਾਰਵਾਈ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਹੋਰ ਸਾਧਨਾਂ ਰਾਹੀਂ ਪੁਸ਼ਟੀ ਕਰੋ।

l@l:'"\,.

ਸੁਰੱਖਿਆ ਸਾੱਫਟਵੇਅਰ ਨੂੰ ਅੱਪਡੇਟ ਕਰੋ: ਆਪਣੇ ਡਿਜੀਟਲ ਤਲਾਬ ਨੂੰ ਨਵੀਨਤਮ ਰੱਖਿਆ ਨਾਲ ਸੁਰੱਖਿਅਤ ਰੱਖੋ।

ਇੱਕ ਸਾਵਧਾਨ ਮੱਛੀ ਵਾਂਗ, ਸਾਵਧਾਨ ਰਹੋ ਅਤੇ ਇੰਟਰਨੈਟ ਦੇ ਵਿਸ਼ਾਲ ਸਮੁੰਦਰ ਵਿੱਚ ਸਮਾਰਟ ਤਰੀਕੇ ਨਾਲ ਤੈਰੋ!

ਵਿਸ਼ਿੰਗ ਸਕੈਮ



a

ਤੁਹਾਡੇ ਫ਼ੋਨ ਦੀ ਘੰਟੀ ਵੱਜਦੀ ਹੈ, ਅਤੇ ਇਹ ਤੁਹਾਡਾ ਅਖੌਤੀ ਬੈਂਕ ਹੈ, ਇੱਕ 'ਜ਼ਰੂਰੀ' ਕਾਲ ਕਰਕੇ ਦਾਅਵਾ ਕਰਦਾ ਹੈ ਕਿ ਤੁਹਾਡੇ ਖਾਤੇ ਨਾਲ ਸਮਝੌਤਾ ਹੋ ਗਿਆ ਹੈ, ਜਾਂ ਸ਼ਾਇਦ ਇੱਕ 'ਜੇਤੂ' ਕਾਲ ਜਿਸ ਵਿੱਚ ਦਾਅਵਾ ਕੀਤਾ ਗਿਆ ਹੈ ਕਿ ਇਹ ਤੁਹਾਡਾ ਖੁਸ਼ਕਿਸਮਤ ਦਿਨ ਹੈ, ਅਤੇ ਤੁਸੀਂ ਇੱਕ ਹੈਰਾਨੀਜਨਕ ਜਿੱਤ ਪ੍ਰਾਪਤ ਕੀਤੀ ਹੈ!!
ਫ਼ੋਨ ਫੜੋ (ਸ਼ਾਬਦਿਕ)!

ਅਜਿਹੇ ਸਕੈਮ ਤੋਂ ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਲਈ, ਹੇਠਾਂ ਦਿੱਤੇ ਸੁਝਾਅ ਯਾਦ ਰੱਖੋ:

ਆਪਣੇ ਨਿੱਜੀ ਵੇਰਵਿਆਂ ਨੂੰ ਫੋਨ 'ਤੇ ਕਦੇ ਵੀ ਨਾ ਸਾਂਝਾ ਕਰੋ।.

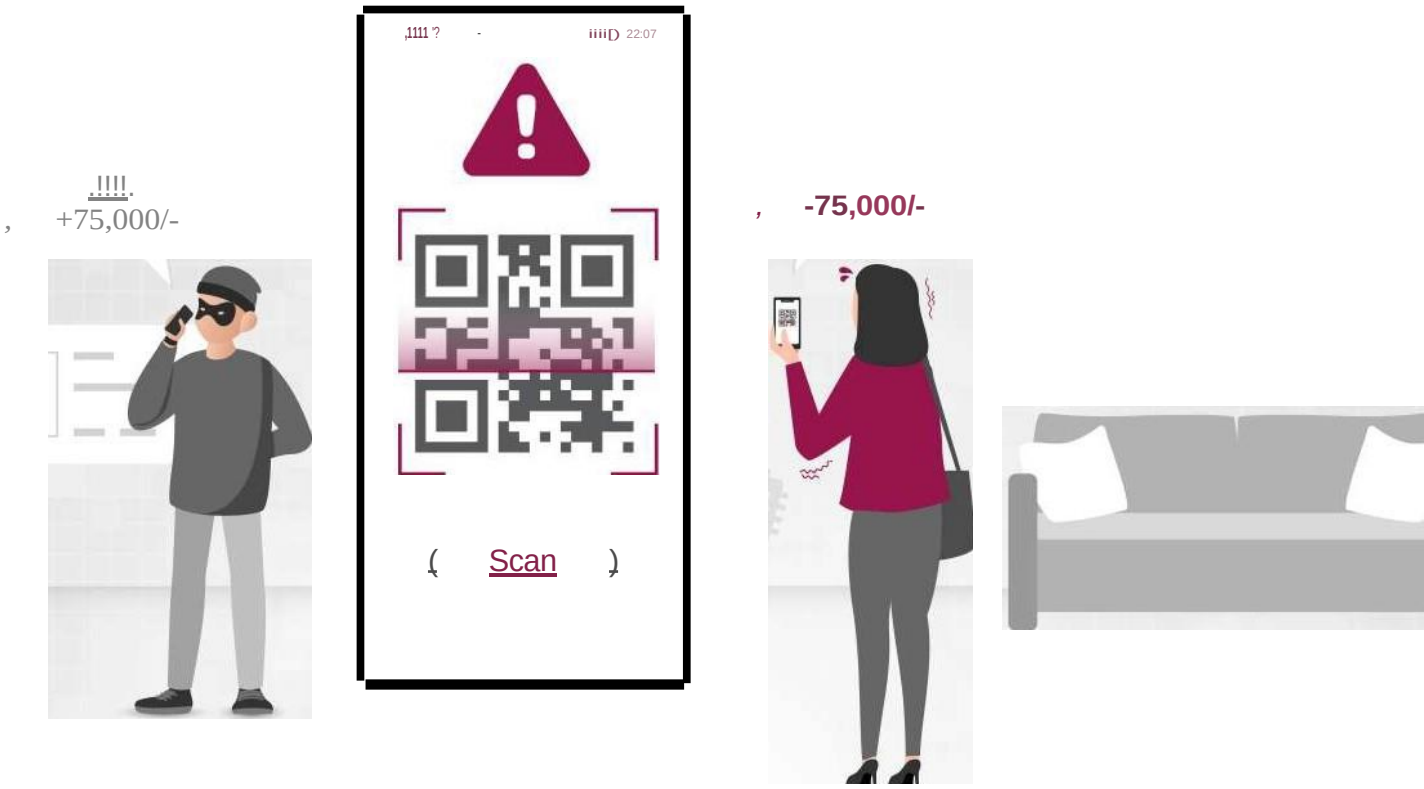
<@)>

ਸ਼ਰਲਾਕ ਹੋਮਜ਼ ਬਣੋ ਅਤੇ ਉਸ ਕਾਲ ਕਰਨ ਵਾਲੇ ਦੀ ਪਛਾਣ ਦੀ ਪੁਸ਼ਟੀ ਕਰੋ।

ਡਰਾਮੇ ਵਿੱਚ ਨਾ ਆਓ! ਜਦੋਂ ਉਹ ਗਰਮੀ ਵਧਾਉਂਦੇ ਹਨ, ਤਾਂ ਠੰਡੀ ਰਹੋ।

ਅਨਜਾਨ ਲੋਕਾਂ ਨਾਲ ਆਨਲਾਈਨ ਜਾਣਕਾਰੀ ਸਾਂਝਾ ਕਰਨ ਵਿੱਚ ਸਾਵਧਾਨ ਰਹੋ - ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਲਈ ਸਮਾਰਟ ਰਹੋ!

UPI ਸਕੈਮ - ਪੈਸੇ ਲਈ ਬੇਨਤੀ ਵਿਕਲਪ



ਸਨੇਹਾ ਨੇ ਇੱਕ ਔਨਲਾਈਨ ਖਰੀਦ ਅਤੇ ਵੇਚਣ ਵਾਲੀ ਐਪ 'ਤੇ ਆਪਣਾ ਫਰਨੀਚਰ ਵਿਗਿਆਪਿਤ ਕੀਤਾ। ਇੱਕ ਖਰੀਦਦਾਰ, ਜੋ ਕਿਹਾ ਕਿ ਉਹ ਪੈਰਾਮਿਲਿਟਰੀ ਕਰਮਚਾਰੀ ਹੈ, ਨੇ ਵਟਸਐਪ 'ਤੇ ਭੁਗਤਾਨ ਲਈ ਇੱਕ QR ਕੋਡ ਭੇਜਿਆ। ਸਨੇਹਾ ਨੇ ਇਸਨੂੰ ਸਕੈਨ ਕੀਤਾ ਅਤੇ 75,000 ਗੁਆ ਦਿਤੇ। ਕੀ ਇਹ ਜਾਣਪਛਾਣ ਵਾਲਾ ਲੱਗਦਾ ਹੈ? ਕੀ ਤੁਸੀਂ UPI ਫ੍ਰੌਡ ਦਾ ਸ਼ਿਕਾਰ ਹੋਣ ਤੋਂ ਡਰਦੇ ਹੋ ਕਿਉਂਕਿ ਤੁਸੀਂ ਅਕਸਰ UPI ਭੁਗਤਾਨ ਪਲੇਟਫਾਰਮਾਂ ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਹੋ?

ਹਮੇਸ਼ਾ ਯਾਦ ਰੱਖੋ:

UPI PIN ਸਿਰਫ ਭੁਗਤਾਨ ਕਰਨ ਲਈ ਲੋੜੀਂਦਾ ਹੈ ਅਤੇ ਕਿਸੇ ਵੀ ਭੁਗਤਾਨ ਨੂੰ ਪ੍ਰਾਪਤ ਕਰਨ ਲਈ ਨਹੀਂ।

ਰੁਕੋ, ਜਿਵੇਂ ਹੀ ਤੁਹਾਨੂੰ ਭੁਗਤਾਨ ਪ੍ਰਾਪਤ ਕਰਨ ਲਈ UPI ਪਿੰਨ ਦੀ ਮੰਗ ਕੀਤੀ ਜਾਂਦੀ ਹੈ! ਇਹ ਅਸਲ ਵਿੱਚ ਇੱਕ ਭੁਗਤਾਨ ਦੀ ਬੇਨਤੀ ਹੋ ਸਕਦੀ ਹੈ, ਇੱਕ ਇਕੱਤਰ ਕਰਨ ਦੀ ਬੇਨਤੀ ਨਹੀਂ।

ਆਪਣੇ OTP, UPI PIN ਜਾਂ ਕਿਸੇ ਵੀ ਗੋਪਨੀਯ ਜਾਣਕਾਰੀ ਨੂੰ ਕਿਸੇ ਨਾਲ ਵੀ ਸਾਂਝਾ ਨਾ ਕਰੋ।

ਕੋਈ ਵੀ ਭੁਗਤਾਨ ਸ਼ੁਰੂ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਹਮੇਸ਼ਾ UPI ਐਪਲੀਕੇਸ਼ਨ ਵਿੱਚ ਮੋਬਾਈਲ ਨੰਬਰ ਅਤੇ ਨਾਮ ਦੀ ਪੁਸ਼ਟੀ ਕਰੋ।

QR ਕੋਡ ਸਕੈਨ ਧੋਖਾਧੜੀ

ਸਾਵਧਾਨੀ ਨਾਲ ਭੁਗਤਾਨ ਐਪਸ 'ਤੇ QR ਕੋਡ ਸਕੈਨ ਕਰੋ; ਪੈਸੇ ਪ੍ਰਾਪਤ ਕਰਨ ਲਈ QR ਕੋਡਾਂ ਨੂੰ ਸਕੈਨ ਨਾ ਕਰੋ; ਫੰਡ ਪ੍ਰਾਪਤ ਕਰ ਉਹਨਾਂ ਵਿੱਚ ਪੈਸੇ ਟ੍ਰਾਂਸਫਰ ਲਈ ਖਾਤੇ ਦੇ ਵੇਰਵੇ ਹੁੰਦੇ ਹਨ। ਲਈ ਲੈਣ-ਦੇਣ ਵਿੱਚ ਬਾਰਕੋਡ/QR ਕੋਡ ਨੂੰ ਸਕੈਨ ਕਰਨਾ ਜਾਂ ਮੋਬਾਈਲ

ਬੈਂਕਿੰਗ ਪਿੰਨ (M-PIN), ਪਾਸਵਰਡ ਆਦਿ ਦਰਜ ਕਰਨਾ ਬੇਲੋੜਾ ਹੈ।

ਇੱਕ ਖਰੀਦਦਾਰ/ਵਿਕਰੇਤਾ ਜੋ ਬੇਲੋੜੀ ਜਲਦਬਾਜ਼ੀ ਜਾਂ ਮੁਸਤੈਦੀ ਦਿਖਾ ਰਿਹਾ ਹੈ ਸ਼ਾਇਦ ਇੱਕ ਧੋਖੇਬਾਜ਼ ਹੈ। ਸ਼ਾਂਤ ਰਹੋ, ਹਮੇਸ਼ਾ ਸਪਸ਼ਟੀਕਰਨ ਮੰਗੋ ਅਤੇ ਜ਼ਰੂਰੀ ਸਵਾਲ ਪੁੱਛੋ।

ਅਣ-ਪ੍ਰਮਾਣਿਤ ਮੋਬਾਈਲ ਐਪ ਫਰਾਡ

ਤੁਹਾਨੂੰ ਇੱਕ SMS, ਇੱਕ ਈਮੇਲ ਜਾਂ ਇੱਥੋਂ ਤੱਕ ਕਿ ਇੱਕ ਲੰਬੇ ਸਮੇਂ ਤੋਂ ਗੁੰਮ ਹੋਏ ਚਚੇਰੇ ਭਰਾ ਤੋਂ ਇੱਕ ਸੁਨੇਹਾ ਪ੍ਰਾਪਤ ਹੁੰਦਾ ਹੈ, ਜਿਸ ਬਾਰੇ ਤੁਸੀਂ ਕਦੇ ਨਹੀਂ ਜਾਣਦੇ ਸੀ, ਇਹ ਸਭ ਇੱਕ ਲਿੰਕ ਨਾਲ ਹੁੰਦਾ ਹੈ ਜੋ ਤੁਹਾਡੀ ਤਰਜੀਹੀ ਅਧਿਕਾਰਤ ਹਸਤੀ ਤੋਂ ਇੱਕ ਜਾਇਜ਼ ਐਪ ਵੱਲ ਜਾਂਦਾ ਹੈ।

ਇੱਕ ਮਿੰਟ ਰੁਕੋ! ਇਹ ਦੋਸਤਾਨਾ ਡਾਊਨਲੋਡ ਨਹੀਂ ਹਨ; ਉਹ ਇੱਕ ਡਿਜੀਟਲ ਪਾਰਟੀ ਲਈ ਇੱਕ ਸੱਦਾ ਹਨ ਜਿਸ ਵਿੱਚ ਤੁਸੀਂ ਯਕੀਨੀ ਤੌਰ 'ਤੇ ਸ਼ਾਮਲ ਨਹੀਂ ਹੋਣਾ ਚਾਹੁੰਦੇ!

ਸਕੈਮਰ SMS, ਈਮੇਲ ਜਾਂ ਸੋਸ਼ਲ ਮੀਡੀਆ ਰਾਹੀਂ ਜਾਅਲੀ ਐਪ ਲਿੰਕ ਭੇਜਦੇ ਹਨ ਜੋ ਜਾਇਜ਼ ਵਾਂਗ ਦਿਖਾਈ ਦਿੰਦੇ ਹਨ। ਉਹ ਉਪਭੋਗਤਾਵਾਂ ਨੂੰ ਉਹਨਾਂ 'ਤੇ ਕਲਿੱਕ ਕਰਨ ਲਈ ਮਨਾਉਂਦੇ ਹਨ, ਜਿਸ ਨਾਲ ਅਣਜਾਣ ਐਪਸ ਨੂੰ ਡਾਊਨਲੋਡ ਕਰਨਾ ਪੈਂਦਾ ਹੈ। ਇੱਕ ਵਾਰ ਸਥਾਪਿਤ ਹੋਣ ਤੋਂ ਬਾਅਦ, ਘੁਟਾਲੇਬਾਜ਼ ਗੁਪਤ ਜਾਣਕਾਰੀ ਅਤੇ OTP ਸਮੇਤ ਡਿਵਾਈਸ ਤੱਕ ਪਹੁੰਚ ਪ੍ਰਾਪਤ ਕਰਦੇ ਹਨ।

ਅਣਜਾਣ ਸਰੋਤਾਂ ਜਾਂ ਅਜਨਬੀਆਂ ਦੀ ਬੇਨਤੀ 'ਤੇ ਐਪਸ ਨੂੰ ਡਾਊਨਲੋਡ ਕਰਨ ਤੋਂ ਬਚੋ।

ਡਾਊਨਲੋਡ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਐਪ ਪ੍ਰਕਾਸ਼ਕਾਂ ਅਤੇ ਉਪਭੋਗਤਾ ਰੇਟਿੰਗਾਂ ਦੀ ਪੁਸ਼ਟੀ ਕਰੋ।

ਅਨੁਮਤੀਆਂ ਅਤੇ ਐਪ ਬੇਨਤੀਆਂ (ਜਿਵੇਂ ਕਿ ਸੰਪਰਕ, ਫੋਟੋਆਂ) ਦੀ ਸਮੀਖਿਆ ਕਰੋ ਅਤੇ ਸਿਰਫ਼ ਲੋੜੀਂਦੀਆਂ ਇਜਾਜ਼ਤਾਂ ਦਿਓ।

ਯਾਦ ਰੱਖੋ, ਬੈਂਕ ਜਾਂ ਹੋਰ ਅਧਿਕਾਰੀ ਕਦੇ ਵੀ ਤੁਹਾਡੇ ਤੋਂ ਅਜਿਹੇ ਸੰਵੇਦਨਸ਼ੀਲ ਵੇਰਵਿਆਂ ਲਈ ਨਹੀਂ ਪੁੱਛਣਗੇ।

ATM ਕਾਰਡ ਸਕਿਮਿੰਗ ਫਰਾਡ

ਡਿਜੀਟਲ ਪਿਕਪਾਕੇਟਿੰਗ ਵਾਂਗ ATM ਸਕਿਮਿੰਗ ਬਾਰੇ ਸੋਚੋ। ਜਦੋਂ ਤੁਸੀਂ ਪੈਸੇ ਕਢਵਾਉਣ ਜਾਂ ਆਪਣਾ ਬਕਾਇਆ ਚੈੱਕ ਕਰਨ ਲਈ ATM ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਹੋ, ਤਾਂ ਧੋਖੇਬਾਜ਼ ਤੁਹਾਡੀ ਕਾਰਡ ਦੀ ਜਾਣਕਾਰੀ ਰਿਕਾਰਡ ਕਰਨ ਲਈ ਮਸ਼ੀਨ 'ਤੇ ਲੁਕਵੇਂ ਯੰਤਰ ਲਗਾ ਦਿੰਦੇ ਹਨ। ਇਹ ਯੰਤਰ ਨਕਲੀ ਕਾਰਡ ਸਲਾਟ ਜਾਂ ਛੋਟੇ ਕੈਮਰਿਆਂ ਵਾਂਗ ਅਦਿੱਖ ਹੋ ਸਕਦੇ ਹਨ।

ATM ਦੀ ਜਾਂਚ ਕਰੋ: ATM ਦੀ ਵਰਤੋਂ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਕਿਸੇ ਵੀ ਅਸਾਧਾਰਨ ਅਟੈਚਮੈਂਟ, ਢਿੱਲੇ ਹਿੱਸੇ ਜਾਂ ਲੁਕਵੇਂ ਕੈਮਰਿਆਂ ਲਈ ਹਮੇਸ਼ਾ ਕਾਰਡ ਸਲਾਟ ਅਤੇ ਕੀਪੈਡ ਦੀ ਜਾਂਚ ਕਰੋ।

ਆਪਣਾ ਪਿੰਨ ਲੁਕਾਓ: ਕੈਮਰਿਆਂ ਜਾਂ ਦਰਸ਼ਕਾਂ ਲਈ ਦੇਖਣਾ ਮੁਸ਼ਕਲ ਬਣਾਉਣ ਲਈ ਆਪਣੇ ਹੱਥ ਜਾਂ ਸਰੀਰ ਨਾਲ ਆਪਣੀ ਪਿੰਨ ਐਂਟਰੀ ਨੂੰ ਲੁਕਾਓ।

ਸਟੇਟਮੈਂਟਾਂ ਦੀ ਨਿਯਮਤ ਤੌਰ 'ਤੇ ਜਾਂਚ ਕਰੋ: ਆਪਣੇ ਬੈਂਕ ਸਟੇਟਮੈਂਟਾਂ ਅਤੇ ਲੈਣ-ਦੇਣ ਦਾ ਧਿਆਨ ਰੱਖੋ। ਕਿਸੇ ਵੀ ਅਣਜਾਣ ਗਤੀਵਿਧੀ ਦੀ ਤੁਰੰਤ ਆਪਣੇ ਬੈਂਕ ਨੂੰ ਰਿਪੋਰਟ ਕਰੋ।

ਕਾਲਾਂ ਤੋਂ ਸਾਵਧਾਨ ਰਹੋ: ਜੇਕਰ ਕੋਈ ਵਿਅਕਤੀ ਤੁਹਾਡੇ ਬੈਂਕ ਤੋਂ ਹੋਣ ਦਾ ਦਾਅਵਾ ਕਰਦਾ ਕਾਲ ਕਰਦਾ ਹੈ ਅਤੇ ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਮੰਗਦਾ ਹੈ, ਤਾਂ ਸਾਵਧਾਨ ਰਹੋ। ਬੈਂਕ ਘੱਟ ਹੀ ਫ਼ੋਨ 'ਤੇ ਪਿੰਨ ਜਾਂ ਪੂਰਾ ਕਾਰਡ ਨੰਬਰ ਮੰਗਦੇ ਹਨ।.

ਸੁਰੱਖਿਅਤ ATM ਦੀ ਵਰਤੋਂ ਕਰੋ: ਚੰਗੀ ਰੌਸ਼ਨੀ ਵਾਲੇ ਖੇਤਰਾਂ ਵਿੱਚ ਜਾਂ ਬੈਂਕ ਸ਼ਾਖਾਵਾਂ ਨਾਲ ਜੁੜੇ ATM ਦੀ ਚੋਣ ਕਰੋ, ਕਿਉਂਕਿ ਉਹਨਾਂ ਨਾਲ ਛੇੜਛਾੜ ਦੀ ਸੰਭਾਵਨਾ ਘੱਟ ਹੁੰਦੀ ਹੈ।

ਅੱਪਡੇਟ ਰਹੋ: ਆਪਣੇ ਆਪ ਨੂੰ ਬਿਹਤਰ ਢੰਗ ਨਾਲ ਸੁਰੱਖਿਅਤ ਕਰਨ ਲਈ ਨਵੀਨਤਮ ਘੁਟਾਲਿਆਂ ਅਤੇ ਧੋਖਾਧੜੀ ਦੀਆਂ ਚਾਲਾਂ ਬਾਰੇ ਜਾਣੂ ਰਹੋ।

ਯਾਦ ਰੱਖੋ, ਸੁਚੇਤ ਰਹਿਣਾ ਅਤੇ ਇਹਨਾਂ ਸੁਝਾਵਾਂ ਦਾ ਪਾਲਣ ਕਰਨਾ ਤੁਹਾਨੂੰ ATM ਕਾਰਡ ਸਕਿਮਿੰਗ ਧੋਖਾਧੜੀ ਦਾ ਸ਼ਿਕਾਰ ਹੋਣ ਤੋਂ ਬਚਣ ਅਤੇ ਆਪਣੇ ਵਿੱਤ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਵਿੱਚ ਮਦਦ ਕਰ ਸਕਦਾ ਹੈ।

ਰਿਮੋਟ ਐਕਸੈਸ ਫਰਾਡ

ਸਕੈਮਰ ਗਾਹਕਾਂ ਨੂੰ ਸਕ੍ਰੀਨ-ਸ਼ੇਅਰਿੰਗ ਐਪਸ ਨੂੰ ਡਾਊਨਲੋਡ ਕਰਨ ਲਈ ਭਰਮਾਉਂਦੇ ਹਨ। ਇਸ ਦੇ ਜ਼ਰੀਏ, ਉਹ ਤੁਹਾਡੀ ਡਿਵਾਈਸ ਵਿੱਚ ਆ ਜਾਂਦੇ ਹਨ, ਤੁਹਾਡੀ ਜਾਸੂਸੀ ਕਰਦੇ ਹਨ ਅਤੇ ਤੁਹਾਡੀ ਵਿੱਤੀ ਜਾਣਕਾਰੀ ਚੋਰੀ ਕਰਦੇ ਹਨ। ਫਿਰ, ਉਹ ਤੁਹਾਡੇ ਪੈਸੇ ਲੈ ਕੇ ਖਰੀਦਦਾਰੀ ਕਰਨ ਜਾਂਦੇ ਹਨ!

ਅਜਿਹੇ **ਸਕੈਮ** ਤੋਂ ਬਚਣ ਲਈ, ਇਹ ਸੁਝਾਅ ਯਾਦ ਰੱਖੋ:

ਕਾਲਰ ਦੀ ਪੁਸ਼ਟੀ ਕਰੋ: ਉਸ ਸੰਸਥਾ ਦੀ ਅਧਿਕਾਰਤ ਸੰਪਰਕ ਜਾਣਕਾਰੀ ਦੀ ਸੁਤੰਤਰ ਤੌਰ 'ਤੇ ਜਾਂਚ ਕਰਕੇ ਕਾਲਰ ਦੀ ਪਛਾਣ ਦੀ ਹਮੇਸ਼ਾਂ ਦੋ ਵਾਰ ਜਾਂਚ ਕਰੋ ਜਿਸਦਾ ਉਹ ਪ੍ਰਤੀਨਿਧਤਾ ਕਰਨ ਦਾ ਦਾਅਵਾ ਕਰਦੇ ਹਨ।

ਜਲਦਬਾਜ਼ੀ ਵਿੱਚ ਫੈਸਲੇ ਨਾ ਲਓ: ਦਬਾਅ ਵਿੱਚ ਆ ਕੇ ਕੋਈ ਫੈਸਲਾ ਨਾ ਲਓ। ਕਿਸੇ ਨੂੰ ਵੀ ਪਹੁੰਚ ਦੇਣ ਜਾਂ ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਕਰਨ ਤੋਂ ਪਹਿਲਾਂ ਸੋਚਣ ਅਤੇ ਪੁਸ਼ਟੀ ਕਰਨ ਲਈ ਸਮਾਂ ਕੱਢੋ।

ਆਪਣੀਆਂ ਡਿਵਾਈਸਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖੋ: ਆਪਣੇ ਡਿਵਾਈਸ ਨੂੰ ਨਵੀਨਤਮ ਸੁਰੱਖਿਆ ਪੈਚਾਂ ਨਾਲ ਅੱਪਡੇਟ ਰੱਖੋ ਅਤੇ ਹਰੇਕ ਖਾਤੇ ਲਈ ਮਜ਼ਬੂਤ, ਵਿਲੱਖਣ ਪਾਸਵਰਡ ਦੀ ਵਰਤੋਂ ਕਰੋ।

ਆਪਣੇ ਆਪ ਨੂੰ ਸਿੱਖਿਅਤ ਕਰੋ: ਆਮ **ਸਕੈਮ** ਅਤੇ ਰਣਨੀਤੀਆਂ ਬਾਰੇ ਜਾਣੋ ਤਾਂ ਜੋ ਤੁਸੀਂ ਉਨ੍ਹਾਂ ਨੂੰ ਪਛਾਣ ਸਕੋ ਜਦੋਂ ਉਹ ਵਾਪਰਦੇ ਹਨ।

ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖੋ: ਫ਼ੋਨ, ਈਮੇਲ, ਜਾਂ ਔਨਲਾਈਨ 'ਤੇ ਨਿੱਜੀ ਜਾਂ ਵਿੱਤੀ ਵੇਰਵਿਆਂ ਨੂੰ ਸਾਂਝਾ ਕਰਨ ਬਾਰੇ ਸਾਵਧਾਨ ਰਹੋ ਜਦ ਤੱਕ ਤੁਸੀਂ ਬੇਨਤੀ ਦੀ ਜਾਇਜ਼ਤਾ ਬਾਰੇ ਨਿਸ਼ਚਤ ਨਹੀਂ ਹੁੰਦੇ।

ਤੁਹਾਡੀ ਡਿਜੀਟਲ ਜ਼ਿੰਦਗੀ ਵਿੱਚ ਘੁਸਪੈਠ ਕਰਨ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰਨ ਵਾਲੇ ਰਿਮੋਟ ਐਕਸੈਸ ਧੋਖੇਬਾਜ਼ਾਂ ਤੋਂ ਵਰਚੁਅਲ ਦਰਵਾਜ਼ੇ ਨੂੰ ਬੰਦ ਰੱਖਣ ਲਈ ਚੌਕਸ ਰਹੋ।

ਕਿਰਪਾ ਕਰਕੇ ਨੋਟ ਕਰੋ - ਜੇ ਤੁਸੀਂ ਕਾਲੀ / ਖਾਲੀ ਸਕ੍ਰੀਨ ਵੇਖਦੇ ਹੋ, ਤਾਂ ਕਿਰਪਾ ਕਰਕੇ ਆਪਣੇ ਸਿਸਟਮ 'ਤੇ ਕਿਸੇ ਵੀ ਕਾਰਵਾਈ ਯੋਗ ਨਾਲ ਅੱਗੇ ਨਾ ਵਧੋ। ਇਹ ਇੱਕ ਸੰਕੇਤ ਹੋ ਸਕਦਾ ਹੈ ਕਿ ਤੁਹਾਡੀ ਸਕ੍ਰੀਨ ਦੂਜਿਆਂ ਨੂੰ ਦਿਖਾਈ ਦੇ ਸਕਦੀ ਹੈ।

ਸਿਮ ਸਵੈਪ ਫਰਾਡ

ਕਲਪਨਾ ਕਰੋ ਕਿ ਇੱਕ ਸਕੈਮਰ ਫ਼ੋਨ ਚੋਰੀ ਕਰ ਰਿਹਾ ਹੈ! ਉਹ ਤੁਹਾਡੇ ਹੋਣ ਦਾ ਦਿਖਾਵਾ ਕਰਦੇ ਹਨ, ਕਹਿੰਦੇ ਹਨ ਕਿ ਉਨ੍ਹਾਂ ਦਾ ਸਿਮ ਕਾਰਡ ਗੁੰਮ ਹੋ ਗਿਆ ਹੈ, ਅਤੇ ਫਿਰ ਉਨ੍ਹਾਂ ਨੂੰ ਤੁਹਾਡਾ ਨੰਬਰ ਮਿਲ ਜਾਂਦਾ ਹੈ। ਨਾਲ ਹੀ, ਉਹ ਤੁਹਾਡੇ ਬੈਂਕ ਜਾਂ ਈਮੇਲ ਵਰਗੇ ਤੁਹਾਡੇ ਔਨਲਾਈਨ ਖਾਤਿਆਂ ਵਿੱਚ ਦਾਖਲ ਹੋ ਜਾਂਦੇ ਹਨ, ਅਤੇ ਤਬਾਹੀ ਮਚਾ ਦਿੰਦੇ ਹਨ!
ਸਵੈਪ ਸਕੈਮ ਨੂੰ ਰੋਕੋ! ਹੇਠਾਂ ਦਿੱਤੇ ਸੁਝਾਅ ਯਾਦ ਰੱਖੋ

ਸਿਮ ਕਾਰਡ ਦੀ ਪਛਾਣ ਦੇ ਵੇਰਵੇ ਸਾਂਝੇ ਨਾ ਕਰੋ।

ਆਪਣੇ ਫ਼ੋਨ ਦੇ ਨੈੱਟਵਰਕ ਐਕਸੈਸ ਦੀ ਨਿਗਰਾਨੀ ਕਰੋ।

ਜੇਕਰ ਕੁਝ ਸਮੇਂ ਲਈ ਕੋਈ ਨੈੱਟਵਰਕ ਨਹੀਂ ਹੈ, ਤਾਂ ਡੁਪਲੀਕੇਟ **ਸਿਮ** ਦੀ ਜਾਂਚ ਕਰਨ ਲਈ ਆਪਣੇ ਆਪਰੇਟਰ ਨਾਲ ਸੰਪਰਕ ਕਰੋ।

ਤੁਹਾਡੀ ਡਿਜੀਟਲ ਜ਼ਿੰਦਗੀ ਵਿੱਚ ਘੁਸਪੈਠ ਕਰਨ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰਨ ਵਾਲੇ ਰਿਮੋਟ ਐਕਸੈਸ ਧੋਖੇਬਾਜ਼ਾਂ ਤੋਂ ਵਰਚੁਅਲ ਦਰਵਾਜ਼ੇ ਨੂੰ ਬੰਦ ਰੱਖਣ ਲਈ ਚੌਕਸ ਰਹੋ।

ਧੋਖਾਧੜੀ ਵਾਲੇ **ਟ੍ਰਾਂਜੈਕਸਨ** ਦੀ ਰਿਪੋਰਟ ਕਿਵੇਂ ਕਰੀਏ?

www.axisbank.com > ਸਹਾਇਤਾ > 'ਤੇ ਜਾਓ 'ਸਾਡੇ ਕੋਲ ਇੱਥੇ ਪਹੁੰਚੋ' ਸੈਕਸ਼ਨ 'ਤੇ ਹੇਠਾਂ ਸਕ੍ਰੋਲ ਕਰੋ > ਸਾਡੇ ਨਾਲ ਗੱਲ ਕਰੋ > 'ਧੋਖਾਧੜੀ ਜਾਂ ਵਿਵਾਦ ਦੀ ਰਿਪੋਰਟ ਕਰੋ' ਚੁਣੋ > ਧੋਖਾਧੜੀ ਦੀ ਰਿਪੋਰਟ ਕਰੋ > ਆਪਣੀ ਪੁੱਛਗਿੱਛ ਦੀ ਡਰਾਪ-ਡਾਊਨ ਸੂਚੀ ਵਿੱਚੋਂ ਸੰਬੰਧਿਤ ਵਿਕਲਪ ਚੁਣੋ> ਕਾਲ 'ਤੇ ਕਲਿੱਕ ਕਰੋ

RBI ਕੋਲ ਸ਼ਿਕਾਇਤ ਦਰਜ ਕਰਵਾਉਣ ਲਈ, https://cms.rbi.org.in 'ਤੇ ਜਾਓ

ਟੋਲ-ਫ੍ਰੀ ਨੰਬਰ 14448 'ਤੇ ਕਾਲ ਕਰੋ (ਸੋਮਵਾਰ ਤੋਂ ਸ਼ੁੱਕਰਵਾਰ, ਸਵੇਰੇ 9:30 ਵਜੇ ਤੋਂ ਸ਼ਾਮ 5:15 ਵਜੇ ਤੱਕ, ਰਾਸ਼ਟਰੀ ਛੁੱਟੀਆਂ ਨੂੰ ਛੱਡ ਕੇ)।).

ਇੱਕ ਭੌਤਿਕ ਸ਼ਿਕਾਇਤ ਭੇਜੋ: 'ਕੇਂਦਰੀਕ੍ਰਿਤ ਰਸੀਦ ਅਤੇ ਪ੍ਰੋਸੈਸਿੰਗ ਸੈਂਟਰ, 4ਵੀਂ ਮੰਜ਼ਿਲ, ਭਾਰਤੀ ਰਿਜ਼ਰਵ ਬੈਂਕ, ਸੈਕਟਰ-17, ਸੈਂਟਰਲ ਵਿਸਟਾ, ਚੰਡੀਗੜ੍ਹ - 160 017' ਨੂੰ ਪੱਤਰ/ਪੋਸਟ। ਲੋੜੀਂਦੇ ਫਾਰਮੈਟ ਬਾਰੇ ਵਧੇਰੇ ਜਾਣਕਾਰੀ ਲਈ ਕਿਰਪਾ ਕਰਕੇ **https://cms.rbi.org.in 'ਤੇ ਜਾਓ।**

ਸਾਈਬਰ ਅਪਰਾਧ ਦੀ ਰਿਪੋਰਟ ਕਰਨ ਲਈ, ਹੈਲਪਲਾਈਨ ਨੰਬਰ **155260 ਜਾਂ 1930** 'ਤੇ ਡਾਇਲ ਕਰੋ ਜਾਂ ਨੈਸ਼ਨਲ ਸਾਈਬਰ ਕ੍ਰਾਈਮ ਰਿਪੋਰਟਿੰਗ ਪੋਰਟਲ **(www.cybercrime.gov.in)** 'ਤੇ ਘਟਨਾ ਦੀ ਰਿਪੋਰਟ ਕਰੋ।