HSBC

ਔਨਲਾਈਨ ਸੁਰੱਖਿਆ ਅਤੇ ਸੁਰੱਖਿਅਤ ਉਪਯੋਗ ਸਬੰਧੀ ਨਿਰਦੇਸ਼

ਅਸੀਂ ਇਸ ਤਰ੍ਹਾਂ ਇਕੱਠੇ ਮਿਲਕੇ ਤੁਹਾਡੀ ਔਨਲਾਈਨ ਬੈਂਕਿੰਗ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖ ਸਕਦੇ ਹਾਂ।

ਇੱਕ ਬੈਂਕ ਦੇ ਰੂਪ ਵਿੱਚ ਅਸੀਂ ਸੁਰੱਖਿਆ ਬਾਰੇ ਸੋਚਣ ਦੇ ਆਦੀ ਹਾਂ। ਇੰਟਰਨੈਟ ਦੇ ਵਿਕਾਸ ਨੇ ਸਾਡੇ ਸਾਰਿਆਂ ਲਈ ਲਚਕ ਦੀ ਪੇਸ਼ਕਸ਼ ਕੀਤੀ ਹੈ, ਪਰ ਇਹ ਨਵੇਂ ਜੋਖਮ ਵੀ ਲਿਆਉਂਦਾ ਹੈ ਜਿਨ੍ਹਾਂ ਤੋਂ ਬਚਾਅ ਵੀ ਕੀਤਾ ਜਾਣਾ ਚਾਹੀਦਾ ਹੈ। ਐਚਐਚਬੀਸੀ ਵਿੱਚ, ਅਸੀਂ ਤੁਹਾਡੇ ਖਾਤੇ ਨੂੰ ਕਿਸੀ ਵੀ ਅਨਅਧਿਕਾਰਤ ਪਹੁੰਚ ਤੋਂ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਲਈ ਤਿੰਨ ਮੁੱਖ ਖੇਤਰਾਂ – ਗੋਪਨਿਯਤਾ, ਟੈਕਨੋਲੋਜੀ ਅਤੇ ਪਛਾਣ 'ਤੇ ਧਿਆਨ ਕੇਂਦਰਿਤ ਕਰਦੇ ਹੋਏ ਉਦਯੋਗ ਮਿਆਰ ਸੁਰੱਖਿਆ ਟੈਕਨੋਲੋਜੀ ਅਤੇ ਪ੍ਰਥਾਵਾਂ ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਹਾਂ।

ਆਉ ਜਾਣੋ ਕਿ ਐਚਐਚਬੀਸੀ ਤੁਹਾਡੀ ਔਨਲਾਈਨ ਬੈਂਕਿੰਗ ਦੀ ਸੁਰੱਖਿਆ ਦੇ ਲਈ ਕੀ ਕਰਦਾ ਹੈ ਅਤੇ ਆਪਣੀ ਖੁਦ ਦੀ ਔਨਲਾਈਨ ਸੁਰੱਖਿਆ ਨੂੰ ਬੇਹਤਰ ਬਣਾਉਣ ਦੇ ਲਈ ਤੁਸੀਂ ਨਿਜੀ ਰੂਪ ਨਾਲ ਕਿਹੜੇ ਕਦਮ ਚੁੱਕ ਸਕਦੇ ਹੋ।

ਧੋਖਾਧੜੀ ਦੇ ਪ੍ਰਕਾਰ

ਅਜਿਹੇ ਕਈ ਤਰੀਕੇ ਹਨ ਜਿਨ੍ਹਾਂ ਨਾਲ ਇੱਕ ਧੋਖੇਬਾਜ਼ ਤੁਹਾਨੂੰ ਧੋਖਾ ਦੇਕੇ ਤੁਹਾਡਾ ਵਿਅਕਤੀਗਤ ਅਤੇ ਸੁਰੱਖਿਆ ਵੇਰਵਾ ਲੈਣ ਦਾ ਯਤਨ ਕਰ ਸਕਦਾ ਹੈ। ਫੇਰ ਉਹ ਇਹਨਾਂ ਵੇਰਵਿਆਂ ਦੀ ਵਰਤੋਂ ਬੈਂਕ ਦੇ ਕੋਲ ਤੁਹਾਡੀ ਵਿੱਤੀ ਜਾਣਕਾਰੀ ਤੱਕ ਪਹੁੰਚਣ ਲਈ ਕਰਦੇ ਹਨ ਅਤੇ ਤੁਹਾਡੇ ਖਾਤੇ ਤੋਂ ਉਹਨਾਂ ਦੇ ਖਾਤਿਆਂ ਵਿੱਚ ਭੁਗਤਾਨ ਵੀ ਸੈੱਟ ਕਰ ਲੈਂਦੇ ਹਨ।

ਕੁੱਝ ਹੋਰ ਸਧਾਰਨ ਧੋਖਾਧੜੀਆਂ ਜੋ ਪ੍ਰਚਲਿਤ ਹਨ ਉਹ ਇਹ ਹਨ ।

ਕ੍ਰੈਡਿਟ / ਡੈਬਿਟ ਕਾਰਡ ਸਕਿਮਿੰਗ ਜਾਂ ਕਲੋਨਿੰਗ:

ਧੋਖੇਬਾਜ਼ ਤੁਹਾਡੇ ਕ੍ਰੈਡਿਟ ਜਾਂ ਡੈਬਿਟ ਕਾਰਡ ਦੀ ਚੁੰਬਕੀ ਪੱਟੀ ਤੋਂ ਜਾਣਕਾਰੀ ਚੋਰੀ ਕਰ ਸਕਦੇ ਹਨ। ਏਟੀਐਮਾਂ ਵਿੱਚ ਉਹ ਸਕਿਮਰ ਡਿਵਾਈਸ ਨੂੰ ਕਾਰਡ ਸਲਾਟ ਵਿੱਚ ਛੁਪਾ ਦੇਂਦੇ ਹਨ ਜਾਂ ਮਰਚੰਟ ਪੇਮੇਂਟ ਟਰਮੀਨਲ ਤੇ ਜਦੋਂ ਤੁਹਾਡਾ ਧਿਆਨ ਨਹੀਂ ਹੁੰਦਾ ਹੈ ਇਹ ਉਸ ਵੇਲੇ ਅਜਿਹਾ ਕਰਦੇ ਹਨ। ਇਹ ਡਿਵਾਈਸ ਜਾਂ ਉਪਕਰਨ ਤੁਹਾਡੇ ਕਾਰਡ ਦੇ ਵੇਰਵੇ ਨੂੰ ਸਕੈਨ ਕਰਦਾ ਹੈ ਅਤੇ ਜਾਣਕਾਰੀ ਇਕੱਠੀ ਕਰਦਾ ਹੈ। ਤੁਹਾਡੀ ਪਿਨ ਚੋਰੀ ਕਰਨ ਲਈ ਜਾਲਸਾਜ ਏਟੀਐਮ ਜਾਂ ਵਪਾਰਕ ਪ੍ਰਤਿਸ਼ਠਾਨ 'ਤੇ ਅਜਿਹੀ ਥਾਂ ਤੇ ਕੈਮਰਾ ਲਗਾਉਂਦੇ ਹਨ ਜੋ ਅਸਾਨੀ ਨਾਲ ਨਜ਼ਰ ਨਹੀਂ ਆਉਂਦਾ।

ਯੂਪੀਆਈ ਐਪਲੀਕੇਸ਼ਨਾਂ ਵਿੱਚ ਘੋਟਾਲਾ ਜਾਂ ਭੁਗਤਾਨ ਧੋਖਾਧੜੀ

ਧੋਖੇਬਾਜ਼ ਤੁਹਾਨੂੰ ਐਪਲੀਕੇਸ਼ਨ ਦੇ ਮਾਧਿਅਮ ਨਾਲ ਕਿਉਆਰ ਕੋਡ ਭੇਜ ਸਕਦੇ ਹਨ ਅਤੇ ਤੁਹਾਨੂੰ ਕਿਉਆਰ ਕੋਡ ਸਕੈਨ ਕਰਨ ਲਈ ਜਾਂ ਉਹਨਾਂ ਦੇ ਖਾਤੇ ਵਿੱਚ ਫੰਡ ਟ੍ਰਾਂਸਫਰ ਕਰਨ ਲਈ "Collect" ਬੇਨਤੀ ਨੂੰ ਮੰਜੂਰ ਕਰਨ ਲਈ ਆਖਦੇ ਹਨ। ਅਜਿਹੇ ਧੋਖੇਬਾਜ਼ ਤੁਹਾਨੂੰ ਇੱਕ ਝੂਠੀ ਕਹਾਣੀ ਬਣਾ ਕੇ ਵਰਗਲਾਉਂਦੇ ਹਨ, ਜਿਵੇਂ ਕਿ ਇੱਕ ਅਜਿਹਾ ਉਤਪਾਦ ਖਰੀਦਣ ਦਾ ਇਰਾਦਾ ਵਿਅਕਤ ਕਰਨਾ ਜੋ ਤੁਸੀਂ ਵੇਚਦੇ ਹੋ। ਜਾਂ ਉਹ ਬੈਂਕ ਜਾਂ ਸ਼ਾਪਿੰਗ ਕੰਪਨੀ ਦੇ ਐਕਜ਼ਿਕਿਉਟਿਵ ਦੇ ਰੂਪ ਵਿੱਚ ਰਿਫੰਡ, ਕੈਸ਼ਬੈਕ ਆਫਰ, ਰਿਵਾਰਡ ਪੁਆਇੰਟ ਆਦਿ ਨੂੰ ਪ੍ਰੋਸੈਸ ਕਰਨ ਦੀ ਪੇਸ਼ਕਸ਼ ਕਰਦੇ ਹਨ ਜੋ ਤੁਹਾਡੇ ਨਾਮ ਤੇ ਜਮ੍ਹਾ ਹਨ। ਅਸੰਦੇਹੀ ਪੀੜਤ ਵਿਅਕਤੀ ਫੇਰ ਕਿਉਆਰ ਕੋਡ ਨੂੰ ਸਕੈਨ ਕਰ ਸਕਦੇ ਹਨ ਜਾਂ ਆਪਣੀ ਯੂਪੀਆਈ ਪਿਨ ਦੀ ਵਰਤੋਂ ਕਰ ਕੇ "Collect" ਬੇਨਤੀ ਨੂੰ ਮੰਜੂਰ ਕਰਦੇ ਹਨ, ਜਿਸ ਨਾਲ ਧੋਖੇਬਾਜ਼ ਦੇ ਖਾਤੇ ਵਿੱਚ ਪੈਸਾ ਜਮ੍ਹਾ ਹੋ ਜਾਂਦਾ ਹੈ।

ਬਿਜ਼ਨੇਸ ਈਮੇਲ ਅਤੇ ਮੈਸੇਜਿੰਗ ਐਪਸ ਰਾਹੀਂ ਭੁਗਤਾਨ ਧੋਖਾਧੜੀ

ਤੁਹਾਡੇ ਪ੍ਰੋਫਾਈਲ ਨੂੰ ਹੋਰ ਸਮਝਣ ਲਈ ਧੋਖੇਬਾਜ਼ ਈਮੇਲ ਜਾਂ ਚੈਟ ਜਾਂ ਐਨਕ੍ਰਿਪਟੇਡ ਸਨੇਹਿਆਂ ਨੂੰ ਇੰਟਰਸੈਪਟ ਕਰ ਸਕਦੇ ਹਨ। ਇੱਕ ਵਾਰ ਉਹ ਤੁਹਾਡੇ ਬਾਰੇ ਹੋਰ ਜਾਣਕਾਰੀ ਪ੍ਰਾਪਤ ਕਰ ਲੈਣ, ਉਹ ਹੈਕ ਕੀਤੀ ਗਈ ਜਾਂ ਨਕਲੀ ਆਈਡੀ ਤੋਂ ਸਨੇਹੇ ਭੇਜ ਸਕਦਾ ਹੈ ਅਤੇ ਵੈਧ ਉੱਦੇਸ਼ਾਂ ਲਈ ਭੁਗਤਾਨ ਦੀ ਮੰਗ ਕਰ ਸਕਦਾ ਹੈ ਜਿਵੇਂ ਹਸਪਤਾਲ ਵਿੱਚ ਭਰਤੀ ਹੋਣ ਦੇ ਲਈ ਧਨ ਦੀ ਤਤਕਾਲ ਜ਼ਰੂਰਤ ਜਾਂ ਪਿੱਛਲੀਆਂ ਬਕਾਇਆ ਦੇਣਯੋਗ ਰਾਸ਼ੀਆਂ ਦਾ ਭੁਗਤਾਨ ਨਵੇਂ ਖਾਤੇ ਵਿੱਚ ਕਰਨ ਦੀ ਲੋੜ। ਪੀੜਤ ਵਿਅਕਤੀ ਤਤਕਾਲ ਅਵਸਥਾ ਦੀ ਹਾਲਤ ਵਿੱਚ ਧੋਖੇਬਾਜ਼ ਦੇ ਖਾਤੇ ਵਿੱਚ ਭੁਗਤਾਨ ਕਰ ਸਕਦੇ ਹਨ, ਜਾਂ ਉਹਨਾਂ ਨੂੰ ਪ੍ਰਤੀਤ ਹੁੰਦਾ ਹੈ ਕਿ ਉਹ ਉਸ ਬੇਨਤੀ ਤੇ ਵਿਸ਼ਵਾਸ ਕਰ ਸਕਦੇ ਹਨ। ਇਸ ਤਰ੍ਹਾਂ ਦੀ ਧੋਖਾਧੜੀ ਦਾ ਪਤਾ ਲਗਾਉਣਾ ਮੁਸ਼ਕਿਲ ਹੁੰਦਾ ਹੈ ਕਿਉਂਕਿ ਬੈਂਕਾਂ ਤੋਂ ਲੈਣ ਦੇਣ ਅਲਰਟ ਜ਼ਰੂਰੀ ਨਹੀਂ ਕਿ ਸੰਦੇਹ ਪੈਦਾ ਕਰੇ ਕਿਉਂਕਿ ਭੁਗਤਾਨ ਵਾਸਤਵ ਵਿੱਚ ਪੀੜਤ ਵਿਅਕਤੀ ਦੁਆਰਾ ਹੀ ਕੀਤਾ ਜਾਂਦਾ ਹੈ।

ਨਕਲੀ ਸੰਪਰਕ ਨੰਬਰ:

ਜਾਲਸਾਜ ਬੈਂਕਾਂ ਅਤੇ ਸੇਵਾ ਪ੍ਰਦਾਤਾ ਦੇ ਸੰਪਰਕ ਕੇਂਦਰ ਲਈ ਨਕਲੀ ਸੰਪਰਕ ਵੇਰਵਾ ਪ੍ਰਦਾਨ ਕਰ ਸਕਦਾ ਹੈ। ਅਸੰਦੇਹੀ ਵਿਅਕਤੀ ਸਰਚ ਇੰਜਨ ਦੀ ਵਰਤੋਂ ਨਾਲ ਸੰਪਰਕ ਵੇਰਵਾ ਦੀ ਭਾਲ ਕਰਕੇ ਨਕਲੀ ਨੰਬਰ ਤੇ ਕਾਲ ਕਰ ਸਕਦੇ ਹਨ। ਫੇਰ ਉਹਨਾਂ ਨੂੰ ਇੱਕ 'ਪੁਸ਼ਟੀਕਰਨ ਕਿਰਿਆ' ਤੋਂ ਕੱਢਿਆ ਜਾਂਦਾ ਹੈ ਅਤੇ ਉਹਨਾਂ ਦੇ ਡੈਬਿਟ/ਕ੍ਰੈਡਿਟ ਕਾਰਡ ਅਤੇ ਬੈਂਕ ਖਾਤਿਆਂ ਬਾਰੇ ਸੰਵੇਦਨਸ਼ੀਲ ਵੇਰਵਾ ਸਾਂਝਾ ਕਰਨ ਲਈ ਛੱਲ ਕੀਤਾ ਜਾਂਦਾ ਹੈ।

ਖੁਦ ਨੂੰ ਬਚਾਉਣ ਲਈ ਤੁਸੀਂ ਹਮੇਸ਼ਾ ਕਿਸੇ ਬੈਂਕ ਜਾਂ ਸੇਵਾ ਪ੍ਰਦਾਤਾ ਦੀ ਅਧਿਕਾਰਤ ਵੈਬਸਾਈਟ ਤੇ ਹੀ ਜਾਉ ਜੇ ਤੁਸੀਂ ਸੰਪਰਕ ਵੇਰਵਾ ਲੈਣਾ ਚਾਹੁੰਦੇ ਹੋ। ਹਮੇਸ਼ਾ ਸਾਵਧਾਨ ਰਹੋ ਸਰਚ ਨਤੀਜਿਆਂ ਤੇ ਦਿਖਾਈ ਦੇਣ ਵਾਲੇ ਨੰਬਰਾਂ ਤੋਂ, ਖਾਸ ਕਰ ਕੇ ਮੋਬਾਇਲ ਨੰਬਰ ਦੀ ਵਰਤੋਂ ਕਰਨ ਤੋਂ ਬਚੋ।

ਫਿਸ਼ਿੰਗ ਜਾਂ ਸਪੂਫਿੰਗ ਈਮੇਲ:

ਧੋਖੇਬਾਜ਼ ਬਹੁਤ ਸਾਰੇ ਈਮੇਲ ਪਤਿਆਂ ਤੇ ਈਮੇਲ ਭੇਜ ਕੇ ਲੋਕਾਂ ਨੂੰ ਭਰਮਾ ਸਕਦੇ ਹਨ। ਉਹ ਕਿਸੇ ਬੈਂਕ, ਔਨਲਾਈਨ ਭੁਗਤਾਨ ਸੇਵਾ, ਰਿਟੇਲਰ ਜਾਂ ਇਸੇ ਤਰ੍ਹਾਂ ਦੇ ਹੋਰ ਵੈਧ ਸੰਗਠਨਾਂ ਤੋਂ ਆਉਣ ਦਾ ਦਾਅਵਾ ਕਰਦੇ ਹੋਏ ਅਜਿਹਾ ਕਰਦੇ ਹਨ। ਸਪੂਫਿੰਗ ਆਮ ਤੌਰ ਤੇ ਈਮੇਲ ਦੇ ਪ੍ਰਸਾਰ ਨਾਲ ਸਬੰਧਿਤ ਹੈ ਜੋ ਇਸ ਤਰ੍ਹਾਂ ਪ੍ਰਤੀਤ ਹੁੰਦਾ ਹੈ ਜਿਵੇਂ ਕਿ ਧੋਖਾਧੜੀ ਸ੍ਰੋਤ ਦੇ ਇਲਾਵਾ ਕਿਸੇ ਹੋਰ ਵਿਅਕਤੀ ਦੁਆਰਾ ਭੇਜਿਆ ਗਿਆ ਹੈ।

ਫਿਸ਼ਿੰਗ ਤੋਂ ਬਚਾਅ ਲਈ ਤੁਹਾਨੂੰ ਕਦੇ ਵੀ ਵਿਅਕਤੀਗਤ ਜਾਂ ਵਿੱਤੀ ਜਾਣਕਾਰੀ ਦੀ ਬੇਨਤੀ ਕਰਨ ਵਾਲੇ ਈਮੇਲ ਸਨੇਹਿਆਂ ਦਾ ਜਵਾਬ ਨਹੀਂ ਦੇਣਾ ਚਾਹੀਦਾ ਅਤੇ ਕਦੇ ਵੀ ਅਜਿਹੇ ਸੰਦੇਹਜਨਕ ਈਮੇਲ ਦੇ ਲਿੰਕ ਤੇ ਕਲਿਕ ਨਹੀਂ ਕਰਨਾ ਚਾਹੀਦਾ।

ਐਚਐਸਬੀਸੀ ਕਦੇ ਵੀ ਤੁਹਾਡੇ ਤੋਂ ਈਮੇਲ ਦੁਆਰਾ ਤੁਹਾਡੇ ਨਿਜੀ ਜਾਂ ਸੁਰੱਖਿਆ ਵੇਰਵਾ ਦਾ ਖੁਲਾਸਾ ਕਰਨ ਲਈ ਨਹੀਂ ਕਹਿੰਦਾ ਹੈ। ਜੇ ਤੁਹਾਨੂੰ ਐਚਐਸਬੀਸੀ ਤੋਂ ਕੋਈ ਅਜਿਹਾ ਈਮੇਲ ਪ੍ਰਾਪਤ ਹੁੰਦਾ ਹੈ ਤਾਂ ਉਸ ਦਾ ਜਵਾਬ ਨਾ ਦਿਉ। ਉਸ ਈਮੇਲ ਨੂੰ ਤੁਰੰਤ ਡਿਲੀਟ ਕਰ ਦਿਉ। ਅਤੇ ਯਾਦ ਰੱਖੋ – ਕਦੇ ਵੀ ਨਿਜੀ ਜਾਣਕਾਰੀ ਜਿਵੇਂ ਯੂਜ਼ਰ ਨਾਮ, ਪਾਸਵਰਡ ਜਾਂ ਹੋਰ ਸੁਰੱਖਿਆ ਵੇਰਵਾ ਕਿਸੇ ਦੇ ਨਾਲ ਸਾਂਝਾ ਨਾ ਕਰੋ।

ਮਨੀ ਮਿਉਲ ਜਾਂ ਵਾਧੂ ਆਮਦਨੀ ਸਬੰਧਿਤ ਈਮੇਲ ਘੁਟਾਲੇ:

ਮਨੀ ਮਿਉਲ ਸਕੈਮ ਵਿੱਚ ਧੋਖੇਬਾਜ਼ ਪੈਸੇ ਟ੍ਰਾਂਸਫਰ ਕਰਨ ਵਿੱਚ ਤੁਹਾਡੀ ਮਦਦ ਮੰਗ ਸਕਦਾ ਹੈ। ਉਹ ਤੁਹਾਡੇ ਖਾਤੇ ਵਿੱਚ ਧਨ ਰਾਸ਼ੀ ਦਾ ਭੁਗਤਾਨ ਕਰਨ ਦੀ ਪੇਸ਼ਕਸ਼ ਕਰਦਾ ਹੈ ਕਿ ਤੁਸੀਂ ਇਸ ਨੂੰ ਕਿਸੇ ਦੂਜੇ ਖਾਤੇ ਵਿੱਚ ਟ੍ਰਾਂਸਫਰ ਕਰਨ ਲਈ ਮਦਦ ਕਰੋਗੇ। ਬਦਲੇ ਵਿੱਚ, ਉਹ ਤੁਹਾਨੂੰ ਕਮੀਸ਼ਨ ਦੇਣ ਲਈ ਕਹਿਣਗੇ।

ਇਹਨਾਂ ਵਿਚੋਂ ਕਈ ਘੋਟਾਲਿਆਂ ਵਿੱਚ ਅਪਰਾਧ/ ਭੁਗਤਾਨ ਧੋਖਾਧੜੀ ਆਦਿ ਦੀ ਆਮਦਨੀ ਸ਼ਾਮਿਲ ਹੁੰਦੀ ਹੈ ਅਤੇ ਤੁਹਾਨੂੰ ਅਜਿਹੀਆਂ ਬੇਨਤੀਆਂ ਨੂੰ ਅਣਦੇਖਿਆ ਕਰਨਾ ਚਾਹੀਦਾ ਹੈ। ਕੋਈ ਵੀ ਗਾਹਕ ਜੋ ਜਾਣ ਬੁੱਝ ਕੇ ਭਾਗ ਲੈਂਦਾ ਹੈ ਉਹ ਉਸ ਅਪਰਾਧ ਵਿੱਚ ਸ਼ਾਮਿਲ ਹੋ ਜਾਂਦਾ ਹੈ ਜੋ ਤਕਨੀਕੀ ਰੂਪ ਵਿੱਚ ਅਪਰਾਧ ਵਿੱਚ ਇੱਕ ਸਹਿਯੋਗੀ ਹੈ ਅਤੇ ਉਸ ਤੇ ਮੁਕਦਮਾ ਚਲਾਇਆ ਜਾ ਸਕਦਾ ਹੈ। ਜੇ ਇਹ ਸੱਚ ਹੋਣ ਲਈ ਬਹੁਤ ਚੰਗਾ ਲਗਦਾ ਹੈ ਤਾਂ ਸ਼ਾਇਦ ਇਹ ਇੱਕ ਧੋਖਾ ਹੈ!

ਐਡਵਾਂਸ ਫੀ ਧੋਖਾਧੜੀ (‘419’ ਘੋਟਾਲੇ)

ਇਹਨਾਂ ਵਿੱਚ ਧੋਖੇਬਾਜ਼ਾਂ ਦੁਆਰਾ ਅਣਇੱਛਤ ਪੱਤਰ ਅਤੇ ਈਮੇਲ ਸਨੇਹੇ ਸ਼ਾਮਿਲ ਹੁੰਦੇ ਹਨ ਜਿਨ੍ਹਾਂ ਵਿੱਚ ਪ੍ਰਾਪਤ ਕਰਤਾ ਨੂੰ ਆਮ ਤੌਰ ਤੇ ਯੂਐਸ ਡਾਲਰ ਵਿੱਚ ਭਾਰੀ ਮਾਤ੍ਰਾ ਵਿੱਚ ਧਨ ਟ੍ਰਾਂਸਫਰ ਕਰਨ ਵਿੱਚ ਮਦਦ ਦੇ ਲਈ ਇੱਕ ਉਦਾਰ ਇਨਾਮ ਦੀ ਪੇਸ਼ਕਸ਼ ਕੀਤੀ ਜਾਂਦੀ ਹੈ। ਜਾਲਸਾਜ ਦਰਅਸਲ ਤੁਹਾਡੇ ਬੈਂਕਿੰਗ ਵੇਰਵੇ ਦੇ ਪਿੱਛੇ ਹੁੰਦੇ ਹਨ। ਆਮ ਤੌਰ ਤੇ ਉਹ ਤੁਹਾਨੂੰ ਸੌਦਾ ਪੂਰਨ ਕਰਨ ਦੇ ਲਈ ਚਾਰਜ, ਕੁੱਝ ਕਰ ਜਾਂ ਰਿਸ਼ਵਤ ਵਰਗੀ ਕਿਸੇ ਚੀਜ਼ ਦਾ ਭੁਗਤਾਨ ਕਰਨ ਦੀ ਇੱਛਾ ਪ੍ਰਗਟਾਉਂਦਾ ਹੈ। ਇਹ ਐਡਵਾਂਸ ਫੀ ਹੈ। ਅਸੰਦੇਹੀ ਵਿਅਕਤੀ ਅਕਸਰ ਇੱਥੇ ਧੋਖਾ ਖਾ ਜਾਂਦੇ ਹਨ।

ਜੇ ਤੁਹਾਨੂੰ ਸੰਦੇਹ ਹੈ ਕਿ ਕਿਸੇ ਕੋਲ ਤੁਹਾਡੇ ਇੰਟਰਨੈਟ ਬੈਂਕਿੰਗ ਵੇਰਵੇ ਪਹੁੰਚ ਗਏ ਹਨ ਤਾਂ ਆਪਣਾ ਪਾਸਵਰਡ ਬਦਲੀ ਕਰਨ ਲਈ ਝੱਟ ਇੰਟਰਨੈਟ ਬੈਂਕਿੰਗ ਵਿੱਚ ਲੌਗ ਇਨ ਕਰੋ। ਨਾਲ ਹੀ, ਸਾਨੂੰ ਤੁਰੰਤ ਅਲਰਟ ਕਰਨ ਲਈ ਕਾਲ ਕਰੋ। ਸਾਡੀਆਂ ਲਾਈਨਾਂ 24 ਘੰਟੇ, ਹਫਤੇ ਦੇ 7 ਦਿਨ ਖੁੱਲੀਆਂ ਹੁੰਦੀਆਂ ਹਨ। ਸਾਡੇ ਹੌਟਲਾਈਨ ਨੰਬਰਾਂ ਦੀ ਸੂਚੀ ਇੱਥੇ ਮਿਲ ਸਕਦੀ ਹੈ।

ਸੋਸ਼ਲ ਮੀਡੀਆ ਹੈਕ:

ਧੋਖੇਬਾਣ ਸੋਸ਼ਲ ਮੀਡੀਆ ਚੈਨਲ, ਭਾਵੇਂ ਉਹ ਫੇਸਬੁਕ, ਵਟਸਐਪ, ਇਨਸਟਾਗ੍ਰਾਮ ਆਦਿ ਹੋਵੇ, ਦੀ ਵਰਤੋਂ ਦੁਆਰਾ ਤੁਹਾਡੇ ਕਿਸੇ ਕਰੀਬੀ ਦੋਸਤ ਜਾਂ ਰਿਸ਼ਤੇਦਾਰ ਦੇ ਰੂਪ ਵਿੱਚ ਉਹਾਨੂੰ ਤਤਕਾਲ ਮਨੀ ਟ੍ਰਾਂਸਫਰ ਦੀ ਬੇਨਤੀ ਕਰ ਸਕਦਾ ਹੈ। ਤੁਹਾਨੂੰ ਇਸ ਤਰ੍ਹਾਂ ਦੀ ਬੇਨਤੀ ਨੂੰ ਫੋਨ ਕਾਲ ਜਾਂ ਹੋਰ ਤਰੀਕੇ ਨਾਲ ਪੁਸ਼ਟੀ ਕਰਨ ਦੇ ਲਈ ਸਾਵਧਾਨ ਰਹਿਣ ਦੀ ਲੋੜ ਹੈ।

ਵਿਸ਼ਿੰਗ ਕਾਲਸ:

ਧੋਖੇਬਾਜ਼ ਅਕਸਰ ਬੈਂਕ ਕਰਮਚਾਰੀ ਜਾਂ ਕਸਟਮਰ ਸਰਵਿਸ ਐਕਜ਼ਿਕਿਉਟਿਵ ਦਾ ਰੂਪ ਧਾਰਨ ਕਰਦੇ ਹੋਏ ਪੀੜਤ ਵਿਅਕਤੀਆਂ ਨੂੰ ਉਹਨਾਂ ਦੇ ਫੋਨ ਨੰਬਰਾਂ ਤੇ ਕਾਲ ਕਰ ਕੇ ਬੈਂਕ ਖਾਤੇ ਨਾਲ ਸਬੰਧਿਤ ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਚੁਰਾ ਲੈਂਦੇ ਹਨ। ਉਹ ਸੋਸ਼ਿਅਲ ਐਂਜੀਨਿਅਰਿੰਗ ਦੇ ਮਾਧਿਮ ਨਾਲ ਪਹਿਲਾਂ ਤੋਂ ਹੀ ਚੁਰਾਈ ਗਈ ਕੁੱਝ ਨਿਜੀ ਜਾਣਕਾਰੀ ਪੀੜਤ ਵਿਅਕਤੀ ਨੂੰ ਪ੍ਰਦਾਨ ਕਰ ਕੇ ਉਹਨਾਂ ਦਾ ਵਿਸ਼ਵਾਸ ਜਿੱਤਦੇ ਹਨ। ਇੱਕ ਵਾਰ ਵਿਸ਼ਵਾਸ ਸਥਾਪਤ ਹੋ ਜਾਣ ਦੇ ਬਾਅਦ ਉਹ ਪੀੜਤ ਵਿਅਕਤੀਆਂ ਨੂੰ ਕੁੱਝ ਖਾਸ ਪ੍ਰੋਡਕਟ ਜਾਂ ਸੇਵਾ ਪੇਸ਼ ਕਰਦੇ ਹਨ ਇਸ ਉਮੀਦ ਵਿੱਚ ਕਿ ਉਹ ਉਸ ਵੇਲੇ ਬੈਂਕ ਵੇਰਵਾ ਅਤੇ ਵਨ-ਟਾਈਮ ਪਾਸਕੋਡ (ਓਟੀਪੀ) ਸਮੇਤ ਗੋਪਨੀਯ ਵੇਰਵਾ ਸਾਂਝਾ ਕਰ ਦੇਵੇ।

ਟ੍ਰੋਜਨ ਵਾਇਰਸ:

ਧੋਖੇਬਾਜ਼ ਆਮ ਤੌਰ ਤੇ ਉਹਾਨੂੰ ਅਜਿਹੇ ਈਮੇਲ ਭੇਜਦੇ ਹਨ ਜਿਸ ਵਿੱਚ ਫਾਈਲਾਂ, ਪੇਜ ਜਾਂ ਅਟੈਚਮੇਂਟ ਹੋ ਸਕਦੇ ਹਨ ਜਿਨ੍ਹਾਂ ਨੂੰ ਖੋਲਣ ਲਈ ਤੁਹਾਨੂੰ ਕਿਹਾ ਜਾਂਦਾ ਹੈ ਜੋ ਅਕਸਰ ਇੱਕ ਅਣਚਾਹੇ ਜਾਂ ਫਿਸ਼ਿੰਗ ਈਮੇਲ ਦੇ ਰੂਪ ਵਿੱਚ ਪ੍ਰਾਪਤ ਹੁੰਦੇ ਹਨ। ਇੱਕ ਵਾਰ ਖੋਲਣ ਦੇ ਬਾਅਦ, ਉਹ ਤੁਹਾਡੇ ਕੰਪਿਉਟਰ ਵਿੱਚ ਗੁਪਤ ਰੂਪ ਨਾਲ ਇੱਕ ਪ੍ਰੋਗਰਾਮ ਇਨਸਟਾਲ ਕਰ ਸਕਦੇ ਹਨ ਜੋ ਤੁਹਾਡੀ ਔਨਲਾਈਨ ਗਤੀਵਿਧੀ ਦੀ ਨਿਗਰਾਨੀ ਕਰ ਸਕਦਾ ਹੈ, ਇਹ ਵੀ ਕਿ ਤੁਸੀਂ ਅਨੇਕਾਂ ਵੈਬਸਾਈਟਾਂ ਤੇ ਕੀ ਟਾਈਪ ਕਰ ਰਹੇ ਹੋ। ਸੋ ਜਦੋਂ ਤੁਸੀਂ ਔਨਲਾਈਨ ਸ਼ਾਪਿੰਗ ਦੌਰਾਨ ਆਪਣਾ ਕ੍ਰੈਡਿਟ ਕਾਰਡ ਵੇਰਵਾ ਦਰਜ ਕਰਦੇ ਹੋ ਤਾਂ ਧੋਖੇਬਾਜ਼ ਤੁਹਾਡੇ ਦੁਆਰਾ ਟਾਈਪ ਕੀਤੀ ਸਾਰੀਆਂ ਚੀਜ਼ਾਂ ਪ੍ਰਾਪਤ ਕਰਨ ਵਿੱਚ ਸਮਰੱਥ ਹੋ ਜਾਂਦੇ ਹਨ।

ਔਨਲਾਈਨ ਸੁਰੱਖਿਆ ਦੇ ਲਈ ਐਚਐਸਬੀਸੀ ਦੁਆਰਾ ਲਏ ਗਏ ਕਦਮ:

ਬਹੁ-ਪਰਤ ਲੋਗ ਔਨ ਪੁਸ਼ਟੀ

ਤੁਹਾਡੀ ਵਿੱਤੀ ਜਾਣਕਾਰੀ ਇੱਕ ਖਾਸ ਉਪਭੋਗਕਰਤਾ ਨਾਮ ਅਤੇ ਪਾਸਵਰਡ ਦੇ ਸੁਮੇਲ ਅਤੇ ਤੁਹਾਡੇ ਭੌਤਿਕ ਸੁਰੱਖਿਆ ਉਪਕਰਨ ਜਾਂ ਡਿਜਿਟਲ ਸੁਰੱਖਿਅਤ ਕੁੰਜੀ ਦੁਆਰਾ ਜਨਰੇਟ ਕੀਤੇ ਗਏ ਇੱਕ-ਵਾਰ ਦੇ ਸੁਰੱਖਿਆ ਕੋਡ ਦੁਆਰਾ ਸੁਰੱਖਿਅਤ ਹੈ।

ਲੈਣ ਦੇਣ ਪੁਸ਼ਟੀ

ਕਾਰਡ ਤੇ 3ਡੀ ਸੁਰੱਖਿਅਤ ਲੈਣ ਦੇਣ ਭੁਗਤਾਨ ਪ੍ਰਣਾਲੀ ਵਿੱਚ ਵਿਸ਼ਵਾਸ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰਨ ਵਿੱਚ ਮਦਦ ਕਰਦੇ ਹਨ। ਲੈਣ ਦੇਣ ਦੇ ਲਈ ਜਨਰੇਟ ਕੀਤੇ ਓਟੀਪੀ ਨੂੰ ਕਦੇ ਵੀ ਕਿਸੇ ਦੇ ਨਾਲ ਸਾਂਝਾ ਨਾ ਕਰੋ।

128 ਬਿਟ ਸਿਕਯੋਰ ਸਾਕੇਟ ਲੇਅਰ (ਐਸਐਸਐਲ) ਐਨਕ੍ਰਿਪਸ਼ਨ

ਐਚਐਸਬੀਸੀ ਇੰਟਰਨੈਟ ਬੈਂਕਿੰਗ ਸੈਸ਼ਨ ਦੇ ਦੌਰਾਨ ਪ੍ਰਸਾਰਿਤ ਜਾਣਕਾਰੀ ਦੇ ਲਈ 128 ਬਿਟ ਸਿਕਯੋਰ ਸਾਕੇਟ ਲੇਅਰ (ਐਸਐਸਐਲ) ਐਨਕ੍ਰਿਪਸ਼ਨ ਦੀ ਵਰਤੋਂ ਕਰਦਾ ਹੈ। ਜਿਸ ਨੂੰ ਐਨਕ੍ਰਿਪਸ਼ਨ ਦੇ ਲਈ ਉਦਯੋਗ ਮਾਨਕ ਦੇ ਰੂਪ ਵਿੱਚ ਸਵੀਕਾਰ ਕੀਤਾ ਗਿਆ ਹੈ।

ਆਟੋਮੈਟਿਕ 'ਟਾਈਮ-ਆਉਟ' ਸੁਵਿਧਾ:

ਇੱਕ ਸੁਰੱਖਿਆ ਉਪਾਅ ਦੇ ਰੂਪ ਵਿੱਚ, ਤੁਹਾਡਾ ਇੰਟਰਨੈਟ ਬੈਂਕਿੰਗ ਸੈਸ਼ਨ ਉਪਯੋਗ ਨਾ ਕੀਤੇ ਜਾਣ ਦੀ ਮਿਆਦ ਦੇ ਬਾਅਦ ਆਪਣੇ ਆਪ ਬੰਦ ਜਾਂ ਟਾਈਮ-ਆਉਟ ਹੋ ਜਾਵੇਗਾ। ਜਦੋਂ ਤੁਸੀਂ ਆਪਣਾ ਇੰਟਰਨੈਟ ਬੈਂਕਿੰਗ ਕਾਰਜ ਪੂਰਾ ਕਰ ਲਵੋ ਤਾਂ ਤੁਹਾਨੂੰ ਆਪਣਾ ਇੰਟਰਨੈਟ ਬੈਂਕਿੰਗ ਸੈਸ਼ਨ ਹਮੇਸ਼ਾ ਬੰਦ ਕਰ ਦੇਣਾ ਚਾਹੀਦਾ ਹੈ।

ਸੁਰੱਖਿਆ ਉਪਕਰਨ / ਡਿਜਿਟਲ ਸੁਰੱਖਿਅਤ ਕੁੰਜੀ

ਤੁਹਾਡੀ ਭੌਤਿਕ ਸੁਰੱਖਿਆ ਉਪਕਰਨ / ਡਿਜਿਟਲ ਸੁਰੱਖਿਅਤ ਕੁੰਜੀ ਔਨਲਾਈਨ ਸੁਰੱਖਿਆ ਨੂੰ ਉੱਚ ਸਤਰ ਤੇ ਲੈ ਜਾਂਦੀ ਹੈ। ਆਪਣੇ ਖਾਤੇ ਵਿੱਚ ਲੌਗ ਔਨ ਕਰਨ ਦੇ ਲਈ, ਤੁਹਾਨੂੰ ਹਮੇਸ਼ਾ ਦੀ ਤਰ੍ਹਾਂ ਆਪਣਾ ਮੌਜੂਦਾ ਉਪਭੋਗਕਰਤਾ ਨਾਮ ਅਤੇ ਪਾਸਵਰਡ ਦਰਜ ਕਰਨਾ ਹੋਵੇਗਾ, ਇਸ ਦੇ ਬਾਅਦ ਤੁਹਾਡੇ ਭੌਤਿਕ ਸੁਰੱਖਿਆ ਉਪਕਰਨ ਜਾਂ ਤੁਹਾਡੇ ਡਿਜਿਟਲ ਸੁਰੱਖਿਅਤ ਕੁੰਜੀ ਦੁਆਰਾ ਉਤਪੰਨ ਖਾਸ ਸੁਰੱਖਿਆ ਕੋਡ ਦਰਜ ਕਰਨਾ ਹੋਵੇਗਾ। ਇਹ 2-ਚਰਣ ਦੀ ਪ੍ਰਮਾਣੀਕਰਨ ਕਿਰਿਆ ਤੁਹਾਨੂੰ ਆਪਣੇ ਇੰਟਰਨੈਟ ਬੈਂਕਿੰਗ ਤੱਕ ਪਹੁੰਚ ਦੇ ਰੂਪ ਵਿੱਚ ਸੁਰੱਖਿਆ ਦਾ ਇੱਕ ਹੋਰ ਉੱਚ ਸਤਰ ਪ੍ਰਦਾਨ ਕਰਦਾ ਹੈ।

ਔਨਲਾਈਨ ਸੁਰੱਖਿਆ ਵਿੱਚ ਤੁਹਾਡੀ ਭੂਮਿਕਾ

ਇੰਟਰਨੈਟ ਬੈਂਕਿੰਗ ਸੁਰੱਖਿਆ ਪੱਕੀ ਕਰਨ ਲਈ ਹੇਠ ਲਿਖਤ ਕਰੋ ਅਤੇ ਨਾ-ਕਰੋ ਉਪਾਅ ਅਪਣਾਉ:

ਕਰੋ

- ਪੱਕਾ ਕਰੋ ਕਿ ਤੁਹਾਡਾ ਕੰਪਿਉਟਰ ਹਰ ਸਮੇਂ ਨਵੇਂ ਤੋਂ ਨਵੇਂ ਐਂਟੀ-ਵਾਇਰਸ ਅਤੇ ਫਾਇਰਵਾਲ ਸੁਰੱਖਿਆ ਸੌਫਟਵੇਅਰ ਨਾਲ ਸੁਰੱਖਿਅਤ ਹੈ। ਨਵੀਂ ਤੋਂ ਨਵੀਂ ਸੁਰੱਖਿਆ ਪੱਕੀ ਕਰਨ ਲਈ ਨਿੱਤ ਅਪਡੇਟ ਡਾਉਨਲੋਡ ਕਰੋ।
- ਅਜਿਹਾ ਪਾਸਵਰਡ ਚੁਣੋ ਜੋ ਤੁਹਾਨੂੰ ਯਾਦ ਰਹਿ ਸਕੇ ਪਰ ਕਿਸੇ ਹੋਰ ਵਿਅਕਤੀ ਦੁਆਰਾ ਉਸ ਦਾ ਅਨੁਮਾਨ ਲਗਾਉਣਾ ਆਸਾਨ ਨਾ ਹੋਵੇ। ਪਾਸਵਰਡ ਜਿਸ ਵਿੱਚ ਆਲਫਾਨਿਉਮੇਰੀਕਲ ਅੰਕ ਹੋਣ ਕਿਹਨਾਂ ਦਾ ਅਨੁਮਾਨ ਲਗਾਉਣਾ ਮੁਸ਼ਕਿਲ ਹੁੰਦਾ ਹੈ, ਉਦਾਹਰਨ - a7g3cy91).
- ਆਪਣਾ ਇੰਟਰਨੈਟ ਬੈਂਕਿੰਗ ਪਾਸਵਰਡ ਨਿਯਮਿਤ ਰੂਪ ਵਿੱਚ ਬਦਲੀ ਕਰਦੇ ਰਹੋ।
- ਧੋਖੇਧੜੀ ਵਾਲੀਆਂ ਈਮੇਲਾਂ ਤੋਂ ਸਾਵਧਾਨ ਰਹੋ। ਹਮੇਸ਼ਾ ਪੂਰੇ ਈਮੇਲ ਪਤੇ ਨੂੰ ਸਾਰੇ ਅਖਰਾਂ ਅਤੇ ਅੰਕਾਂ ਸਮੇਤ ਧਿਆਨ ਨਾਲ ਪੜ੍ਹੋ।
- ਧੋਖੇਧੜੀ ਵਾਲੀਆਂ ਈਮੇਲਾਂ ਮਿਲਦੇ ਜੁਲਦੇ ਈਮੇਲ ਪਤਿਆਂ ਦੇ ਨਾਮ ਰਾਹੀਂ ਆਉਂਦੀਆਂ ਹਨ ਜਿਵੇਂ hsdc.co.in ਜਾਂ hsbcbank.com. ਆਪਣੇ ਮਾਉਜ਼ ਦੇ ਪਾਈਂਟਰ ਨੂੰ ਯੂਆਰਐਲ ਦੇ ਉਪਰ ਰੱਖੋ ਤਾਂ ਜੋ ਉਸ ਦਾ ਸਹੀ ਟਿਕਾਣਾ ਪਤਾ ਚਲੇ; ਇਹ ਤੁਹਾਡੇ ਬ੍ਰਾਉਜ਼ਰ ਦੇ ਹੇਠਾਂ ਖੱਬੇ ਕੋਨੇ ਤੇ ਦਰਸਾਇਆ ਜਾਂਦਾ ਹੈ। ਜੇ ਮੇਲ ਨਹੀਂ ਖਾਂਦਾ ਹੈ ਤਾਂ ਉਸ ਲਿੰਕ ਤੇ ਕਲਿਕ ਨਾ ਕਰੋ। ਯੂਆਰਐਲ ਵਿੱਚ ਸੰਕੇਤਾਂ ਦਾ ਧਿਆਨ ਰੱਖੋ ਜਿਵੇਂ ਲਿਖਣ ਵਿੱਚ ਗਲਤੀ, ਖਰਾਬ ਵਿਆਕਰਨ ਜਾਂ ਗੁਛਮੁਛ ਅਖਰ।
- ਜੇ ਤੁਹਾਡੇ ਖਾਤੇ ਵਿੱਚ ਅਜਿਹੇ ਲਾਭ ਪ੍ਰਾਪਤਕਰਤਾ ਹਨ ਜਿਨ੍ਹਾਂ ਦੀ ਹੁਣ ਲੋੜ ਨਹੀਂ ਹੈ ਤਾਂ ਉਹਨਾਂ ਨੂੰ ਡਿਲੀਟ ਕਰੋ।
- ਤੁਹਾਡੇ ਕੰਪਿਉਟਰ ਤੇ ਅਜਿਹੇ ਕਾਰਜ ਡਿਸੇਬਲ ਕਰੋ ਜੋ ਲੌਗ ਔਨ ਵੇਰਵਾ ਯਾਦ ਰੱਖਦੇ ਹਨ।
- ਆਪਣਾ ਸਿਸਟਮ ਅਤੇ ਵੈਬ ਬ੍ਰਾਉਜ਼ਰ ਅਪਡੇਟ ਰੱਖੋ। ਨਿਰਮਾਤਾ ਨਿੱਤ ਅਜਿਹੇ ਸੁਰੱਖਿਆ ਸਬੰਧੀ ਵੇਰਵਾ ਭੇਜਦੇ ਹਨ ਜਦੋਂ ਉਹਨਾਂ ਦੇ ਸਿਸਟਮ ਅਤੇ ਬ੍ਰਾਉਜ਼ਰ ਵਿੱਚ ਖਾਮੀਆਂ ਨਜ਼ਰ ਆਉਂਦੀਆਂ ਹਨ। ਨਿਯਮਿਤ ਰੂਪ ਨਾਲ ਆਪਣੇ ਸੌਫਟਵੇਅਰ ਪ੍ਰਦਾਤਾ ਨਾਲ ਅਜਿਹੇ ਅਪਡੇਟਸ ਚੈਕ ਕਰਦੇ ਰਹੋ।
- ਐਚਐਸਬੀਸੀ ਵੈਬਸਾਈਟ ਤੱਕ ਪਹੁੰਚਣ ਲਈ ਬ੍ਰਾਉਜ਼ਰ ਵਿੱਚ ਹਮੇਸ਼ਾ ਸਾਡਾ ਯੂਆਰਐਲ ਟਾਈਪ ਕਰੋ।
- ਪੈਡਲੌਕ ਨਿਸ਼ਾਨੀ ਅਤੇ ਸਾਈਟ ਸਰਟੀਫਿਕੇਟ ਚੈਕ ਕਰੋ। ਜਦੋਂ ਤੁਸੀਂ ਐਸਐਸਬੀਸੀ ਔਨਲਾਈਨ ਬੈਂਕਿੰਗ ਤੇ ਲੌਗ-ਇਨ ਕਰਦੇ ਹੋ ਹਾਂ ਤਾਂ ਬ੍ਰਾਉਜ਼ਰ ਦੇ ਹੇਠਲੇ ਪ ਾਸੇ ਪੈਡਲੌਕ ਨਿਸ਼ਾਨੀ ਉਪਰ ਡਬਲ-ਕਲਿਕ ਕਰੋ, ਇਹ ਪੱਕਾ ਕਰਦਾ ਹੈ ਕਿ ਸਾਈਟ ਸਰਟੀਫਿਕੇਟ ਐਸਐਸਬੀਸੀ ਦਾ ਹੀ ਹੈ। ਇਹ ਪੱਕਾ ਕਰੇਗਾ ਕਿ ਤੁਸੀਂ ਕਿਸੇ 'ਨਕਲੀ' ਸਾਈਟ ਵਿੱਚ ਆਪਣਾ ਵੇਰਵਾ ਦਰਜ ਨਹੀਂ ਕਰਦੇ ਹੋ।
- ਆਪਣੇ ਖਾਤੇ ਨਿੱਤ ਚੈਕ ਕਰਦੇ ਰਹੋ। ਜੇ ਕੋਈ ਸੰਦੇਹ ਹੈ ਤਾਂ ਵੇਰਵਾ ਨੋਟ ਕਰੋ ਅਤੇ ਸਾਨੂੰ ਕਾਲ ਕਰੋ।
- ਔਨਲਾਈਨ ਬੈਂਕਿੰਗ ਦੀ ਵਰਤੋਂ ਦੇ ਬਾਅਦ ਹਮੇਸ਼ਾ ਲੌਗ ਆਉਟ ਕਰੋ। ਲੌਗ ਆਉਟ ਬਟਨ ਚੁਣੋ ਅਤੇ ਕਦੇ ਵੀ ਆਪਣਾ ਕੰਪਿਉਟਰ ਨਾ ਛੱਡੋ ਜਦੋਂ ਤੱਕ ਤੁਸੀਂ ਲੌਗ ਇਨ ਵਿੱਚ ਹੋ।
- ਜੇ ਤੁਸੀਂ ਕਿਸੇ ਬੈਂਕ, ਔਨਲਾਈਨ ਸ਼ਾਪਿੰਗ ਵੈਬਸਾਈਟ, ਆਦਿ ਦੇ ਕਸਟਮਰ ਕੇਅਰ ਨੰਬਰਾਂ ਦੀ ਭਾਲ ਕਰ ਰਹੇ ਹੋ ਤਾਂ ਇੰਟਰਨੈਟ ਤੇ ਸਿਆਣਪ ਨਾਲ ਕੰਮ ਲਵੋ। ਧੋ ਖੇਬਾਜ਼ ਅਜਿਹੇ ਕੰਮਾਂ ਵਿੱਚ ਹੁਸ਼ਿਆਰ ਹਨ ਅਤੇ ਅਜਿਹੇ ਨੰਬਰ ਪ੍ਰਦਾਨ ਕਰ ਸਕਦੇ ਹਨ ਜੋ ਉਹ ਚਲਾ ਰਹੇ ਹਨ। ਤੁਹਾਨੂੰ ਬੈਂਕ ਦੇ ਕਸਟਮਰ ਕੇਅਰ ਨੰਬਰ ਤੇ ਕਾਲ ਕਰਨ ਜਾਂ ਉਹਨਾਂ ਦੀ ਈ-ਕਾਮਰਸ ਵੈਬਸਾਈਟ ਤੇ ਜਾਣ ਦੇ ਬਦਲੇ ਧੋਖੇਬਾਜ਼ ਨੂੰ ਕਾਲ ਕਰਨ ਦਾ ਧੋਖਾ ਹੋ ਸਕਦਾ ਹੈ।
- ਤੁਹਾਡੇ ਬੈਂਕ ਦੇ ਸੰਪਰਕ ਕੇਂਦਰ ਨੰਬਰ ਆਪਣੇ ਉਪਕਰਨਾਂ ਤੇ ਸਟੋਰ ਕਰੋ ਜਾਂ ਤੁਹਾਡੇ ਕ੍ਰੈਡਿਟ/ਡੈਬਿਟ ਕਾਰਡ ਦੇ ਪਿੱਛੇ ਦਿੱਤੇ ਨੰਬਰ ਰੈਫਰ ਕਰੋ।
- ਤੁਹਾਡੇ ਨਿਜੀ ਕੰਪਿਉਟਰ ਜਾਂ ਮੋਬਾਇਲ ਉਪਰ ਸਕ੍ਰੀਨ ਸ਼ੇਅਰਿੰਗ ਐਪਲੀਕਸ਼ਨਾਂ ਦਾ ਧਿਆਨ ਰੱਖੋ। ਧੋਖੇਬਾਜ਼ ਤੁਹਾਨੂੰ ਅਜਿਹੇ ਐਪਲੀਕੇਸ਼ਨ ਡਾਉਨਲੋਡ ਕਰਨ ਵਿੱਚ ਧੋਖਾ ਦੇ ਸਕਦੇ ਹਨ ਅਤੇ ਤੁਹਾਡੇ ਤੋਂ ਕੋਡ ਲੈਕੇ ਉਸ ਤੱਕ ਪਹੁੰਚ ਪਾ ਸਕਦੇ ਹਨ। ਇੱਕ ਵਾਰ ਪਹੁੰਚ ਦੀ ਅਨੁਮਤੀ ਮਿਲ ਜਾਵੇ ਤਾਂ ਉਹ ਤੁਹਾਡੇ ਉਪਕਰਨ ਨੂੰ ਦੂਰੋਂ ਵੀ ਵੇਖ ਸਕਦੇ ਅਤੇ ਉਸ ਤੇ ਨਿਯੰਤ੍ਰਣ ਕਰ ਸਕਦੇ ਹਨ ਅਤੇ ਤੁਹਾਡੇ ਖਾਤਿਆਂ ਤੋਂ ਭੁਗਤਾਨ ਕਰ ਸਕਦੇ ਹਨ।
- ਆਪਣਾ ਇੰਟਰਨੈਟ ਕਨੈਕਸ਼ਨ ਸੁਰੱਖਿਅਤ ਰੱਖੋ। ਹਮੇਸ਼ਾ ਆਪਣੇ ਘਰ ਦੇ ਵਾਇਰਲੇਸ ਨੈਟਵਰਕ ਨੂੰ ਪਾਸਵਰਡ ਦੁਆਰਾ ਸੁਰੱਖਿਅਤ ਰੱਖੋ।

- ਅਜਿਹੀਆਂ ਸਕੀਮਾਂ/ਆਫਰਾਂ ਤੋਂ ਸਾਵਧਾਨ ਰਹੋ ਜਿਸ ਦੀ ਕਿਸੀ ਕਮੀਸ਼ਨ ਜਾਂ ਮਦਦ ਲਈ ਤੁਹਾਡੇ ਖਾਤੇ ਵਿੱਚ ਪੈਸੇ ਜਮ੍ਹਾ ਕਰਨ ਦੀ ਲੋੜ ਹੈ। ਜਾਲਸਾਜ ਕਿਸੀ ਗੁਨਾਹ ਦੇ ਪੈਸੇ ਤੁਹਾਡੇ ਖਾਤੇ ਵਿੱਚ ਪਾਉਣਾ ਚਾਹੁੰਦੇ ਹੋਣ ਅਤੇ ਫੇਰ ਉਹ ਪੈਸਾ ਉਹਨਾਂ ਦੇ ਖਾਤੇ ਵਿੱਚ ਟ੍ਰਾਂਸਫਰ ਕਰਨ ਜਾਂ ਨਕਦ ਦੇ ਰੂਪ ਵਿੱਚ ਦੇਣ ਲਈ ਕਹਿ ਸਕਦੇ ਹਨ। ਜਾਲਸਾਜ ਅਜਿਹੇ ਗੈਰ ਕਾਨੂੰਨੀ ਕੰਮਾਂ ਵਿੱਚ ਨਹੀਂ ਪੈਣਾ ਚਾਹੁੰਦੇ ਤੇ ਤੁਹਾਡੀ ਵਰਤੋਂ ਕਰ ਰਹੇ ਹੋਣ।
- ਕਿਸੇ ਪ੍ਰਕਾਰ ਦੇ ਧੋਖੇ ਨੂੰ ਰਿਪੋਰਟ ਕਰਨ ਲਈ ਤੁਰੰਤ ਬੈਂਕ ਨਾਲ ਸੰਪਰਕ ਕਰੋ।

ਨਾ-ਕਰੋ

- ਅਜਿਹਾ ਪਾਸਵਰਡ ਨਾ ਚੁਣੋ ਜਿਸ ਦੀ ਵਰਤੋਂ ਤੁਸੀਂ ਹੋਰ ਸੇਵਾਵਾਂ ਦੇ ਲਈ ਕਰਦੇ ਹੋ। ਤੁਹਾਡਾ ਪਾਸਵਰਡ ਇੰਟਰਨੈਟ ਬੈਂਕਿੰਗ ਦੇ ਲਈ ਨਵੇਕਲਾ ਹੋਣਾ ਚਾਹੀਦਾ ਹੈ।
- ਆਪਣਾ ਯੂਜ਼ਰ ਆਈਡੀ, ਪਾਸਵਰਡ, ਕਾਰਡ ਨੰਬਰ, ਐਕਸਪਾਇਰੀ ਤਰੀਕ, ਆਦਿ ਵਰਗਾ ਵੇਰਵਾ ਕਦੇ ਵੀ ਵੈਬ ਪੰਨਿਆਂ ਤੇ ਸਾਂਝਾ ਨਾ ਕਰੋ ਜੋ ਖੁੱਲ ਜਾਂਦੇ ਨੇ ਜਦੋਂ ਈਮੇਲ/ਐਸਐਮਐਸ ਤੇ ਕਿਸੇ ਲਿੰਕ ਉਪਰ ਕਲਿਕ ਕੀਤਾ ਜਾਵੇ।
- ਵੇਰਵਾ ਮੰਗਣ ਵਾਲੇ ਅਜਿਹੇ ਸਨੇਹਿਆਂ ਨੂੰ ਜਵਾਬ ਨਾ ਦਿਉ ਭਾਵੇਂ ਉਹ ਦਾਅਵਾ ਕਰਨ ਕਿ ਉਹ ਬੈਂਕ ਜਾਂ ਕਿਸੀ ਸਰਕਾਰੀ ਅਦਾਰਿਆਂ ਤੋਂ, ਜਿਵੇਂ ਆਈ.ਟੀ. ਵਿਭਾਗ, ਆਰ.ਬੀ.ਆਈ. ਆਦਿ, ਤੁਹਾਡੇ ਨਾਲ ਸੰਪਰਕ ਕਰ ਰਹੇ ਹਨ। ਐਚਐਸਬੀਸੀ ਦਾ ਕੋਈ ਵੀ ਸਟਾਫ ਤੁਹਾਨੂੰ ਅਜਿਹੇ ਵੇਰਵੇ ਲਈ ਕਦੇ ਵੀ ਕਾਲ ਨਹੀਂ ਕਰੇਗਾ।
- ਕਦੇ ਵੀ ਆਪਣੇ ਪਾਸਵਰਡ ਨੂੰ ਆਪਣੇ ਇੰਟਰਨੈਟ ਬੈਂਕਿੰਗ ਯੂਜ਼ਰ ਨਾਮ ਦੇ ਨਾਲ ਨਾ ਲਿਖੋ। ਆਪਣਾ ਪਾਸਵਰਡ ਪਛਾਣ-ਯੋਗ ਫਾਰਮੈਟ ਵਿੱਚ ਨਾ ਲਿਖੋ ਅਤੇ ਕਦੇ ਵੀ ਆਪਣੇ ਭੌਤਿਕ ਸੁਰੱਖਿਆ ਉਪਕਰਨ/ਡਿਜਿਟਲ ਸੁਰੱਖਿਆ ਕੁੰਜੀ ਦੇ ਨਾਲ ਆਪਣਾ ਲੌਗ ਔਨ ਵੇਰਵਾ ਨਾ ਛੱਡੋ।
- ਆਪਣਾ ਮੋਬਾਇਲ ਬੈਂਕਿੰਗ ਐਪਲੀਕੇਸ਼ਨ ਅਪਡੇਟ ਰੱਖੋ। ਉਸ ਨੂੰ ਡਾਉਨਲੋਡ ਜਾ ਅਪਡੇਟ ਕਰਨ ਲਈ, ਤੁਹਾਡੇ ਉਪਕਰਨ ਦੇ ਅਧਿਕਾਰਤ ਐਪ ਸਟੋਰ ਤੇ ਜਾਉ।
- ਕਦੇ ਵੀ ਮੋਬਾਇਲ ਬੈਂਕਿੰਗ / ਭੁਗਤਾਨ ਐਪਲੀਕੇਸ਼ਨ ਨੂੰ ਅਣਪਛਾਤੇ ਸ੍ਰੋਤਾਂ ਤੋਂ ਆਏ ਈਮੇਲਸ ਵਿੱਚ ਲਿੰਕ ਤੋਂ ਡਾਉਨਲੋਡ ਨਾ ਕਰੋ।
- ਆਪਣਾ ਕਾਰਡ ਨੰਬਰ ਅਤੇ ਐਕਸਪਾਇਰੀ ਤਰੀਕ ਨੂੰ ਔਨਲਾਈਨ ਵੈਬਸਾਈਟਾਂ ਤੇ ਸਟੋਰ ਨਾ ਕਰੋ। ਅਜਿਹੇ ਵੇਰਵੇ ਨੂੰ ਬਹੁਤ ਹੀ ਘੱਟ ਵਰਤੀਆਂ ਵੈਬਸਾਈਟਾਂ ਦੇ ਸੰਦੇਹਜਨਕ ਵੈਬਸਾਈਟਾਂ ਤੇ ਸਟੋਰ ਨਾ ਕਰੋ।
- ਆਪਣਾ ਪਿਨ ਕਦੇ ਵੀ ਕਿਸੇ ਨਾਲ ਸਾਂਝਾ ਨਾ ਕਰੋ। ਖੁਦ ਹੀ ਉਸ ਨੂੰ ਵਰਤੋ ਜੇ ਤੁਹਾਨੂੰ ਸੰਦੇਹ ਹੈ ਕਿ ਪਿਨ ਕਿਸੇ ਹੋਰ ਕੋਲ ਵੀ ਹੈ ਤਾਂ ਝੱਟ ਉਸ ਨੂੰ ਬਦਲੀ ਕਰੋ।

ਜੇ ਤੁਹਾਡੇ ਕੋਲੋ ਕੋਈ ਯੂਪੀਆਈ ਪਿਨ ਦੀ ਮੰਗ ਕਰਦਾ ਹੈ ਤਾਂ ਯਾਦ ਰੱਖੋ, ਤੁਸੀਂ ਭੁਗਤਾਨ ਕਰ ਰਹੇ ਹੋ। ਕੋਈ ਭੁਗਤਾਨ ਪ੍ਰਾਪਤ ਕਰਨ ਲਈ ਤੁਹਾਨੂੰ ਯੂਪੀਆਈ ਪਿਨ ਦੀ ਲੋੜ ਨਹੀਂ ਹੁੰਦੀ।

ਜਨਤਕ ਕੰਪਿਉਟਰਾਂ ਦੀ ਵਰਤੋਂ ਕਰਦਿਆਂ ਖਿਆਲ ਰੱਖੋ

ਹਮੇਸ਼ਾ

- ਜੇ ਤੁਸੀਂ ਕੰਪਿਉਟਰ ਛੱਡਦੇ ਹੋ ਤਾਂ ਲੌਗ ਆਉਟ ਕਰੋ, ਭਾਵੇਂ ਉਹ ਥੋੜੀ ਦੇਰ ਲਈ ਹੀ ਹੋਵੇ। ਜੇ ਮੁਮਕਿਨ ਹੋਵੇ ਤਾਂ ਜਦੋਂ ਤੱਕ ਤੁਸੀਂ ਲੌਗ ਇਨ ਕੀਤਾ ਹੈ, ਕੰਪਿਉਟਰ ਨੂੰ ਨਹੀਂ ਛੱਡੋ।
- ਕੰਪਿਉਟਰ ਤੋਂ ਲੌਗ ਆਉਟ ਹੋਣ ਤੋਂ ਪਹਿਲਾਂ ਆਪਣਾ ਬ੍ਰਾਉਜ਼ਿੰਗ ਇਤਿਹਾਸ ਡਿਲੀਟ ਕਰੋ: ਇੰਟਰਨੈਟ ਦੇ ਬ੍ਰਾਉਜ਼ਰ ਤੁਹਾਡੇ ਪਾਸਵਰਡ ਅਤੇ ਜੋ ਪੰਨਿਆਂ ਤੇ ਤੁਸੀਂ ਗਏ ਹੋ ਉਸ ਬਾਰੇ ਜਾਣਕਾਰੀ ਸਟੋਰ ਕਰਦੇ ਹਨ। ਇੰਟਰਨੈਟ ਬ੍ਰਾਉਜ਼ਰ ਦੇ ਟੂਲਸ ਮੇਨਿਉ ਤੇ ਜਾਉ ਅਤੇ ਚੁਣੋ ਔਪਸ਼ਨਸ (ਵਿਕਲਪ) ਜਾਂ ਇੰਟਰਨੈਟ ਔਪਸ਼ਨਸ। ਪੱਕਾ ਕਰੋ ਕਿ ਬ੍ਰਾਉਜ਼ਰ ਦਾ ਆਟੋ ਕੰਪਲੀਟ ਕਾਰਜ ਬੰਦ ਹੈ, ਕੋਈ ਵੀ ਕੂਕੀਜ਼ ਨੂੰ ਡਿਲੀਟ ਕਰੋ ਅਤੇ ਹਿਸਟਰੀ ਕਲੀਅਰ ਕਰੋ।
- ਜਿੱਥੇ ਤੱਕ ਹੋ ਸਕਦਾ ਹੈ ਆਪਣੀ ਬੈਂਕਿੰਗ ਲਈ ਜਨਤਕ ਕੰਪਿਉਟਰਾਂ ਦੀ ਵਰਤੋਂ ਨਾ ਕਰੋ, ਲਾਈਬ੍ਰੇਰੀ, ਇੰਟਰਨੈਟ ਕੈਫੇ ਅਤੇ ਸਕੂਲਾਂ ਵਾਲਿਆਂ ਸਮੇਤ।

ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਟਾਈਪ ਕਰਨ ਤੋਂ ਪਰ੍ਹੇਜ਼ ਕਰੋ। ਭਾਵੇਂ ਤੁਸੀਂ ਸਾਰੀਆਂ ਸਾਵਧਾਨੀਆਂ ਦਾ ਪਾਲਨ ਕਰਦੇ ਹੋ, ਹੋ ਸਕਦਾ ਹੈ ਕਿ ਜਨਤਕ ਕੰਪਿਉਟਰਾਂ ਵਿੱਚ ਕੀਸਟ੍ਰੋਕ ਲੌਗਰ ਨਾਮਕ ਦੋਖੀ ਸੌਫਟਵੇਅਰ ਇਨਸਟਾਲ ਕੀਤਾ ਗਿਆ ਹੋਵੇ। ਇਹ ਪ੍ਰੋਗਰਾਮ ਤੁਹਾਡਾ ਪਾਸਵਰਡ, ਕ੍ਰੈਡਿਟ ਕਾਰਡ ਨੰਬਰ ਅਤੇ ਬੈਂਕ ਵੇਰਵਾ ਚੋਰੀ ਕਰ ਸਕਦੇ ਹਨ। ਅਜਿਹੇ ਕੋਈ ਵਿੱਤੀ ਲੈਣ ਦੇਣ ਨਾ ਕਰੋ ਜਿਸ ਨਾਲ ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਹੋ ਰਹੀ ਹੋਵੇ।

ਜ਼ਰੂਰੀ - ਜੇ ਤੁਹਾਨੂੰ ਕਦੇ ਵੀ ਕੋਈ ਸੰਦੇਹਜਨਕ ਸ੍ਰੋਤ ਤੋਂ ਐਚਐਸਬੀਸੀ ਦਾ ਦਾਅਵਾ ਕਰਦਿਆਂ ਕੋਈ ਵੀ ਈ-ਮੇਲ ਆਵੇ ਜਾਂ ਨਿਜੀ ਜਾਣਕਾਰੀ ਮੰਗਦੀ ਬੇਲੋੜੀ ਈਮੇਲ ਆਵੇ; ਉਸ ਨੂੰ ਅੱਗੇ ਹੋਰ ਸਾਡੇ ਵਲੋਂ ਪੜਤਾਲ ਲਈ **phishing@hsbc.com** 'ਤੇ ਰਿਪੋਰਟ ਕਰੋ।