DCB BANK

ਅਨੁਬੰਧ 7: ਖਪਤਕਾਰ ਜਾਗਰੂਕਤਾ–ਸਾਈਬਰ ਧਮਕੀਆਂ ਅਤੇ ਧੋਖਾਧੜੀ

ਇਹ ਦੇਖਿਆ ਗਿਆ ਹੈ ਕਿ ਬੇਈਮਾਨ ਤੱਤ ਸੋਸ਼ਲ ਮੀਡੀਆ ਤਕਨੀਕਾਂ, ਮੋਬਾਈਲ ਫੋਨ ਕਾੱਲਾਂ ਆਦਿ ਸਮੇਤ ਨਵੀਨਤਾਕਾਰੀ ਢੰਗ ਨਾਲ ਲੋਕਾਂ ਨੂੰ ਧੋਖਾ ਦੇ ਰਹੇ ਹਨ ਅਤੇ ਗੁੰਮਰਾਹ ਕਰ ਰਹੇ ਹਨ, ਇਸ ਦੇ ਮੱਦੇਨਜ਼ਰ, ਡੀਸੀਬੀ ਬੈਂਕ ਨੇ ਲੋਕਾਂ ਨੂੰ ਧੋਖਾਧੜੀ ਵਾਲੇ ਸੰਦੇਸ਼ਾਂ, ਜਾਅਲੀ ਕਾੱਲਾਂ, ਅਣਜਾਣ ਕਾਲਾਂ ਤੋਂ ਸੁਚੇਤ ਰਹਿਣ ਲਈ ਸਾਵਧਾਨ ਕੀਤਾ ਹੈ। ਲਿੰਕ, ਗਲਤ ਸੂਚਨਾਵਾਂ, ਅਣਅਧਿਕਾਰਤ ਕਿਊਆਰ ਕੋਡ, ਆਦਿ, ਕਿਸੇ ਵੀ ਤਰੀਕੇ ਨਾਲ ਬੈਂਕਾਂ ਅਤੇ ਵਿੱਤੀ ਸੇਵਾ ਪ੍ਰਦਾਤਾਵਾਂ ਤੋਂ ਰਿਆਇਤਾਂ / ਤੁਰੰਤ ਜਵਾਬ ਦੇਣ ਵਿੱਚ ਮਦਦ ਦਾ ਵਾਅਦਾ ਕਰਦੇ ਹਨ।

ਧੋਖੇਬਾਜ਼ ਗੁਪਤ ਵੇਰਵੇ ਜਿਵੇਂ ਕਿ ਯੂਜ਼ਰ ਆਈਡੀ, ਲੌਗਇਨ/ਟ੍ਰਾਂਜੈਕਸ਼ਨ ਪਾਸਵਰਡ, ਵਨ ਟਾਈਮ ਪਾਸਵਰਡ (ਓਟੀਪੀ), ਡੇਬਿਟ/ਕ੍ਰੇਡਿਟ ਕਾਰਡ ਦੇ ਵੇਰਵੇ ਜਿਵੇਂ ਕਿ ਪਿਨ, ਸੀਵੀਵੀ, ਮਿਆਦ ਪੁੱਗਣ ਦੀ ਮਿਤੀ ਅਤੇ ਹੋਰ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਪ੍ਰਾਪਤ ਕਰਨ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰਦੇ ਹਨ। ਧੋਖੇਬਾਜ਼ਾਂ ਦੁਆਰਾ ਵਰਤੇ ਜਾ ਰਹੇ ਆਮ ਢੰਗ ਹਨ:

• ਕੇਵਾਈਸੀ ਦਾ ਪ੍ਰੀਟੈਕਸਟ ਅਪਡੇਟ ਕਰਨ, ਖਾਤਾ/ਸਿਮ ਕਾਰਡ ਅਨਬਲੱਾਕ ਕਰਨ, ਡੇਬਿਟ ਕੀਤੀ ਰਾਸ਼ੀ ਕ੍ਰੇਡਿਟ ਕਰਨ ਆਦਿ ਦੇ ਤਹਿਤ ਗੁਪਤ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਕਰਦੇ ਹੋਏ ਗਾਹਕਾਂ ਨੂੰ ਲੁਭਾਉਣ ਲਈ ਬੈਂਕ/ਗੈਰ-ਬੈਂਕ ਈ-ਵੱਲੇਟ ਪ੍ਰਦਾਤਾਵਾਂ/ਟੈਲੀਕਾਮ ਸੇਵਾ ਪ੍ਰਦਾਤਾਵਾਂ ਤੋਂ ਹੋਣ ਦਾ ਦਿਖਾਵਾ ਕਰਦੇ ਹੋਏ ਵਿਸ਼ਿੰਗ-ਫੋਨ ਕਾੱਲਾਂ।

• ਫਿਸ਼ਿੰਗ – ਧੋਖਾਧੜੀ ਵਾਲੀਆਂ ਈਮੇਲਾਂ ਅਤੇ/ਜਾਂ ਐਸਐਮਐਸ ਗਾਹਕਾਂ ਨੂੰ ਇਹ ਸੋਚਣ ਲਈ ਮਜ਼ਬੂਰ ਕਰਨ ਕਿ ਸੰਚਾਰ ਉਹਨਾਂ ਦੇ ਬੈਂਕ/ਈ-ਵੱਲਟ ਪ੍ਰਦਾਤਾ ਤੋਂ ਸ਼ੁਰੂ ਹੋਇਆ ਹੈ ਅਤੇ ਇਸ ਵਿੱਚ ਗੁਪਤ ਵੇਰਵਿਆਂ ਨੂੰ ਐਕਸਟਰੈਕਟ ਕਰਨ ਲਈ ਲਿੰਕ ਸ਼ਾਮਲ ਹੋਣ।

• ਰਿਮੋਰਟ ਐਕਸੈਸ – ਗਾਹਕਾਂ ਨੂੰ ਉਨ੍ਹਾਂ ਦੇ ਮੋਬਾਈਲ ਫੋਨ/ਕੰਪਿਊਟਰ 'ਤੇ ਇੱਕ ਐਪਲੀਕੇਸ਼ਨ ਡਾਊਨਲੋਡ ਕਰਨ ਲਈ ਲੁਭਾਉਣਾ ਜੋ ਗਾਹਕ ਦੇ ਡਿਵਾਈਸ ਵਿੱਚ ਡੇਟਾ ਤੱਕ ਪਹੁੰਚ ਕਰ ਸਕਦੀ ਹੈ।

• ਪੈਸੇ ਪ੍ਰਾਪਤ ਕਰਨ ਲਈ 'ਆਪਣਾ ਯੂਪੀਆਈ ਪਿਨ ਦਾਖਲ ਕਰੋ' ਵਰਗੇ ਸੰਦੇਸ਼ਾਂ ਨਾਲ ਫਰਜ਼ੀ ਭੁਗਤਾਨ ਬੇਨਤੀਆਂ ਭੇਜ ਕੇ ਯੂਪੀਆਈ ਦੀ ‘‘ਕੁਲੈਕਟ ਬੇਨਤੀ' ਵਿਸ਼ੇਸ਼ਤਾ ਦੀ ਦੁਰਵਰਤੋਂ ਕਰਨਾ।

• ਬੈਂਕਾਂ/ਈ-ਵੱਲੇਟ ਪ੍ਰਦਾਤਾਵਾਂ ਦੇ ਜਾਅਲੀ ਸੰਪਰਕ ਨੰਬਰ ਵੈੱਬਪੇਜਾਂ/ਸੋਸ਼ਲ ਮੀਡੀਆ 'ਤੇ ਅਤੇ ਸਰਚ ਇੰਜਣਾਂ ਆਦਿ ਦੁਆਰਾ ਪ੍ਰਦਰਸ਼ਿਤ ਕਰਨਾ।

ਡੀਸੀਬੀ ਬੈਂਕ ਜਨਤਾ ਨੂੰ ਕਿਸੇ ਵੀ ਡਿਜੀਟਲ (ਔਨਲਾਈਨ/ਮੋਬਾਈਲ) ਬੈਂਕਿੰਗ/ਭੁਗਤਾਨ ਲੈਣ-ਦੇਣ ਕਰਦੇ ਸਮੇਂ ਸਾਰੀਆਂ ਉਚਿਤ ਸਾਵਧਾਨੀ ਵਰਤ ਕੇ ਸੁਰੱਖਿਅਤ ਡਿਜੀਟਲ ਬੈਂਕਿੰਗ ਦਾ ਅਭਿਆਸ ਕਰਨ ਦੀ ਅਪੀਲ ਕਰਦਾ ਹੈ। ਇਹ ਵਿੱਤੀ ਅਤੇ/ਜਾਂ ਹੋਰ ਨੁਕਸਾਨ ਨੂੰ ਰੋਕਣ ਵਿੱਚ ਮਦਦ ਕਰਨਗੇ।

ਸੁਰੱਖਿਅਤ ਡਿਜੀਟਲ ਬੈਂਕਿੰਗ ਅਭਿਆਸ

• ਆਪਣੇ ਖਾਤੇ ਦੇ ਵੇਰਵੇ ਜਿਵੇਂ ਕਿ, ਖਾਤਾ ਨੰਬਰ, ਲੌਗਇਨ ਆਈ.ਡੀ., ਪਾਸਵਰਡ, ਪਿਨ, ਯੂਪੀਆਈ-ਪਿਨ,ਓਟੀਪੀ, ਏਟੀਐ/ਡੇਬਿਟ ਕਾਰਡ/ਕ੍ਰੇਡਿਟ ਕਾਰਡ ਦੇ ਵੇਰਵਿਆਂ ਨੂੰ ਕਦੇ ਵੀ ਕਿਸੇ ਨਾਲ ਸਾਂਝਾ ਨਾ ਕਰੋ, ਬੈਂਕ ਅਧਿਕਾਰੀਆਂ ਨਾਲ ਵੀ ਨਹੀਂ, ਭਾਵੇਂ ਉਹ ਸਹੀ ਕਿਉਂ ਨਾ ਹੋਵੇ।

• ਕੇਵਾਈਸੀ ਨੂੰ ਅਪਡੇਟ ਨਾ ਕਰਨ ਦੇ ਬਹਾਨੇ ਤੁਹਾਡੇ ਖਾਤੇ ਨੂੰ ਬਲੱਾਕ ਕਰਨ ਦੀ ਧਮਕੀ ਦੇਣ ਵਾਲੀ ਕੋਈ ਵੀ ਫ਼ੋਨ ਕਾਲ/ਈਮੇਲ ਅਤੇ ਉਸ ਨੂੰ ਅਪਡੇਟ ਕਰਨ ਲਈ ਲਿੰਕ 'ਤੇ ਕਲਿੱਕ ਕਰਨ ਦਾ ਸੁਝਾਅ ਧੋਖਾਧੜੀ ਕਰਨ ਵਾਲਿਆਂ ਦਾ ਇੱਕ ਆਮ ਤਰੀਕਾ ਹੈ। ਕੇਵਾਈਸੀ ਅਪਡੇਟ ਕਰਨ/ਤੇਜ਼ ਕਰਵਾਉਣ ਲਈ ਪੇਸ਼ਕਸ਼ਾਂ ਦਾ ਜਵਾਬ ਨਾ ਦਿਓ। ਹਮੇਸ਼ਾ ਆਪਣੇ ਬੈਂਕ/ਐਨਐਫਬੀਸੀ/ਈ-ਵੱਲੇਟ ਪ੍ਰਦਾਤਾ ਦੀ ਅਧਿਕਾਰਤ ਵੈੱਬਸਾਈਟ ਤੱਕ ਪਹੁੰਚ ਕਰੋ ਜਾਂ ਸ਼ਾਖਾ ਨਾਲ ਸੰਪਰਕ ਕਰੋ।

• ਆਪਣੇ ਫੋਨ ਜਾਂ ਡਿਵਾਈਸ 'ਤੇ ਕੋਈ ਵੀ ਅਣਜਾਣ ਐਪ ਡਾਊਨਲੋਡ ਨਾ ਕਰੋ। ਐਪ ਤੁਹਾਡੇ ਗੁਪਤ ਡੇਟਾ ਨੂੰ ਗੁਪਤ ਰੂਪ ਵਿੱਚ ਐਕਸੈਸ ਕਰ ਸਕਦੀ ਹੈ।

• ਪੈਸਿਆਂ ਦੀ ਰਸੀਦ ਵਾਲੇ ਲੈਣ-ਦੇਣ ਲਈ ਬਾਰਕੋਡਾਂ ਜਾਂ ਕਿਊਆਰ ਕੋਡਾਂ ਨੂੰ ਸਕੈਨ ਕਰਨ ਜਾਂ ਐਮਪੀਆਈਐਨ ਦਾਖਲ ਕਰਨ ਦੀ ਲੋੜ ਨਹੀਂ ਹੁੰਦੀ ਹੈ। ਇਸ ਲਈ, ਜੇਕਰ ਅਜਿਹਾ ਕਰਨ ਲਈ ਕਿਹਾ ਜਾਵੇ ਤਾਂ ਸਾਵਧਾਨੀ ਵਰਤੋ।

• ਸੰਪਰਕ ਵੇਰਵਿਆਂ ਲਈ ਹਮੇਸ਼ਾਂ ਬੈਂਕ/ਐਨਬੀਐਫਸੀ/ਈ-ਵਾਲੇਟ ਪ੍ਰਦਾਤਾ ਦੀ ਅਧਿਕਾਰਤ ਵੈੱਬਸਾਈਟ ਤੱਕ ਪਹੁੰਚ ਕਰੋ। ਇੰਟਰਨੈੱਟ ਖੋਜ ਇੰਜਣਾਂ 'ਤੇ ਸੰਪਰਕ ਨੰਬਰ ਧੋਖਾਧੜੀ ਵਾਲੇ ਹੋ ਸਕਦੇ ਹਨ।

• ਸਪੈਲਿੰਗ ਗਲਤੀਆਂ ਲਈ ਈਮੇਲਾਂ ਅਤੇ ਐਸਐਮਐਸ ਵਿੱਚ ਪ੍ਰਾਪਤ ਯੂਆਰਐਲ ਅਤੇ ਡੋਮੇਨ ਨਾਮਾਂ ਦੀ ਜਾਂਚ ਕਰੋ। ਔਨਲਾਈਨ ਬੈਂਕਿੰਗ ਲਈ ਸਿਰਫ਼ ਪ੍ਰਮਾਣਿਤ, ਸੁਰੱਖਿਅਤ ਅਤੇ ਭਰੋਸੇਯੋਗ ਵੈੱਬਸਾਈਟਾਂ ਅਤੇ ਐਪਸ ਦੀ ਵਰਤੋਂ ਕਰੋ, ਯਾਨੀ ' ਹਟਟਪਸ ਨਾਲ ਸ਼ੁਰੂ ਹੋਣ ਵਾਲੀਆਂ ਵੈੱਬਸਾਈਟਾਂ। ਇੱਕ ਸ਼ੱਕੀ ਯੂਆਰਐਲ ਜਾਂ ਵੈੱਬਸਾਈਟ ਨੂੰ ਤੁਰੰਤ ਸਥਾਨਕ ਪੁਲਿਸ/ਸਾਈਬਰ ਕ੍ਰਾਈਮ ਬ੍ਰਾਂਚ ਨੂੰ ਸੂਚਿਤ ਕੀਤਾ ਜਾਣਾ ਚਾਹੀਦਾ ਹੈ।

• ਜੇਕਰ ਤੁਹਾਨੂੰ ਤੁਹਾਡੇ ਦੁਆਰਾ ਸ਼ੁਰੂ ਨਹੀਂ ਕੀਤੇ ਗਏ ਟ੍ਰਾਂਜੈਕਸ਼ਨ ਲਈ ਆਪਣੇ ਖਾਤੇ ਨੂੰ ਡੇਬਿਟ ਕਰਨ ਲਈ ਇੱਕ ਓਟੀਪੀ ਪ੍ਰਾਪਤ ਹੁੰਦਾ ਹੈ, ਤਾਂ ਤੁਰੰਤ ਆਪਣੇ ਬੈਂਕ/ਈ-ਵਾੱਲੇਟ ਪ੍ਰਦਾਤਾ ਨੂੰ ਸੂਚਿਤ ਕਰੋ। ਜੇਕਰ ਤੁਹਾਨੂੰ ਕਿਸੇ ਲੈਣ-ਦੇਣ ਲਈ ਇੱਕ ਡੈਬਿਟ ਐਸਐਮਐਸ ਪ੍ਰਾਪਤ ਹੁੰਦਾ ਹੈ, ਤਾਂ ਤੁਰੰਤ ਆਪਣੇ ਬੈਂਕ/ਈ- ਵਾੱਲੇਟ ਪ੍ਰਦਾਤਾ ਨੂੰ ਸੂਚਿਤ ਕਰੋ ਅਤੇ ਯੂਪੀਆਈ ਸਮੇਤ ਡੇਬਿਟ ਦੀਆਂ ਸਾਰੀਆਂ ਵਿਧੀਆਂ ਨੂੰ ਬਲੌਕ ਕਰੋ। ਜੇਕਰ ਤੁਹਾਨੂੰ ਆਪਣੇ ਖਾਤੇ ਵਿੱਚ ਕਿਸੇ ਧੋਖਾਧੜੀ ਦੀ ਗਤੀਵਿਧੀ ਦਾ ਸ਼ੱਕ ਹੈ, ਤਾਂ ਇੰਟਰਨੈਟ/ਮੋਬਾਈਲ ਬੈਂਕਿੰਗ ਲਈ ਯੋਗ ਲਾਭਪਾਤਰੀ ਸੂਚੀ ਵਿੱਚ ਜੋੜਨ ਦੀ ਜਾਂਚ ਕਰੋ।

• ਆਪਣੇ ਬੈਂਕ/ਈ-ਵਾੱਲੇਟ ਖਾਤੇ ਨਾਲ ਲਿੰਕ ਕੀਤੇ ਆਪਣੇ ਈਮੇਲ ਦਾ ਪਾਸਵਰਡ ਸਾਂਝਾ ਨਾ ਕਰੋ।ਈ-ਕਾਮਰਸ/ਸੋਸ਼ਲ ਮੀਡੀਆ ਸਾਈਟਾਂ ਅਤੇ ਆਪਣੇ ਬੈਂਕ ਖਾਤੇ ਅਤੇ ਆਪਣੇ ਬੈਂਕ ਖਾਤੇ ਨਾਲ ਲਿੰਕ ਕੀਤੇ ਈਮੇਲ ਦਾ ਕੌਮਨ ਪਾਸਵਰਡ ਨਾ ਰੱਖੋ।ਜਨਤਕ, ਖੁੱਲ੍ਹੇ ਜਾਂ ਮੁਫ਼ਤ ਵਾਈ-ਫਾਈ ਜਾਂ ਇੰਟਰਨੈੱਟ ਨੈੱਟਵਰਕ ਰਾਹੀਂ ਬੈਂਕਿੰਗ ਕਰਨ ਤੋਂ ਬਚੋ।

• ਕਿਸੇ ਵੀ ਵੈੱਬਸਾਈਟ/ਐਪਲੀਕੇਸ਼ਨ ਵਿੱਚ ਆਪਣੀ ਈਮੇਲ ਨੂੰ ਯੂਜ਼ਰ ਆਈਡੀ ਵਜੋਂ ਰਜਿਸਟਰ ਕਰਦੇ ਸਮੇਂ ਆਪਣੇ ਈਮੇਲ ਪਾਸਵਰਡ ਨੂੰ ਸ਼ਬਦ "ਪਾਸਵਰਡ" ਵਜੋਂ ਸੈਟ ਨਾ ਕਰੋ। ਤੁਹਾਡੀ ਈਮੇਲ ਤੱਕ ਪਹੁੰਚ ਕਰਨ ਲਈ ਵਰਤਿਆ ਜਾਣ ਵਾਲਾ ਪਾਸਵਰਡ, ਖਾਸ ਤੌਰ 'ਤੇ ਜੇਕਰ ਤੁਹਾਡੇ ਬੈਂਕ ਖਾਤੇ ਨਾਲ ਲਿੰਕ ਕੀਤਾ ਗਿਆ ਹੋਵੇ, ਵਿਲੱਖਣ ਹੋਣਾ ਚਾਹੀਦਾ ਹੈ ਅਤੇ ਸਿਰਫ਼ ਈਮੇਲ ਪਹੁੰਚ ਲਈ ਵਰਤਿਆ ਜਾਣਾ ਚਾਹੀਦਾ ਹੈ ਨਾ ਕਿ ਕਿਸੇ ਹੋਰ ਵੈੱਬਸਾਈਟ ਜਾਂ ਐਪਲੀਕੇਸ਼ਨ ਤੱਕ ਪਹੁੰਚ ਕਰਨ ਲਈ।

• ਵਿਦੇਸ਼ੀ ਪ੍ਰੇਸ਼ਣ, ਕਮੀਸ਼ਨ ਦੀ ਪ੍ਰਾਪਤੀ, ਜਾਂ ਲਾਟਰੀ ਜਿੱਤਣ ਲਈ ਭਾਰਤੀ ਰਿਜਰਵ ਬੈਂਕ ਵੱਲੋਂ ਧਨ ਦੀ ਜਮ੍ਹਾਂ ਕਰਨ ਦੀ ਸੂਚਨਾ ਦੇਣ ਵਾਲੀ ਸਲਾਹ ਨਾਲ ਗੁੰਮਰਾਹ ਨਾ ਹੋਵੋ।

• ਆਪਣੇ ਵਿੱਤੀ ਸੇਵਾ ਪ੍ਰਦਾਤਾ ਤੋਂ ਚੇਤਾਵਨੀਆਂ ਲਈ ਨਿਯਮਿਤ ਤੌਰ 'ਤੇ ਆਪਣੇ ਈਮੇਲ ਅਤੇ ਫ਼ੋਨ ਸੁਨੇਹਿਆਂ ਦੀ ਜਾਂਚ ਕਰੋ। ਆਪਣੇ ਖਾਤੇ ਵਿੱਚ ਕਿਸੇ ਵੀ ਗੈਰ-ਅਧਿਕਾਰਤ ਲੈਣ-ਦੇਣ ਦੀ ਰਿਪੋਰਟ ਤੁਰੰਤ ਆਪਣੇ ਬੈਂਕ/ਐਨਬੀਐਫਸੀ/ਸੇਵਾ ਪ੍ਰਦਾਤਾ ਨੂੰ ਹੋਰ ਨੁਕਸਾਨ ਨੂੰ ਰੋਕਣ ਲਈ ਕਾਰਡ, ਖਾਤੇ, ਵੱਲੇਟ ਨੂੰ ਬਲੌਕ ਕਰਨ ਲਈ ਕਹੋ।

• ਆਪਣੇ ਏਟੀਐਮ, ਡੇਬਿਟ ਅਤੇ ਕ੍ਰੇਡਿਟ ਕਾਰਡਾਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰੋ ਅਤੇ ਲੈਣ-ਦੇਣ ਲਈ ਰੋਜ਼ਾਨਾ ਸੀਮਾ ਨਿਰਧਾਰਤ ਕਰੋ। ਤੁਸੀਂ ਘਰੇਲੂ/ਅੰਤਰਰਾਸ਼ਟਰੀ ਵਰਤੋਂ ਲਈ ਸੀਮਾਵਾਂ ਵੀ ਨਿਰਧਾਰਤ ਕਰ ਸਕਦੇ ਹੋ ਅਤੇ ਸਕ੍ਰਿਅ/ਅਕ੍ਰਿਅ ਕਰ ਸਕਦੇ ਹੋ। ਇਹ ਧੋਖਾਧੜੀ ਕਾਰਨ ਹੋਏ ਨੁਕਸਾਨ ਨੂੰ ਸੀਮਤ ਕਰ ਸਕਦਾ ਹੈ।