SECURE OUR WORLD

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY — CISA

ਔਨਲਾਈਨ ਧੋਖੇਬਾਜ਼ਾਂ ਨੂੰ ਚਤਰਾਈ ਨਾਲ ਮਾਤ ਦਿਓ

ਤਿੰਨ ਆਸਾਨ ਕਦਮਾਂ ਨਾਲ ਧੋਖਾਧੜੀ ਵਾਲੇ ਘੁਟਾਲਿਆਂ ਤੋਂ ਬਚੋ

ਧੋਖਾਧੜੀ ਵਾਲੇ ਘੁਟਾਲੇ ਔਨਲਾਈਨ ਮੈਸੇਜ ਹੁੰਦੇ ਹਨ ਜਿਨ੍ਹਾਂ ਨੂੰ ਇਸ ਤਰ੍ਹਾਂ ਡਿਜ਼ਾਈਨ ਕੀਤਾ ਜਾਂਦਾ ਹੈ ਜਿਵੇਂ ਕਿ ਕਿਸੇ ਭਰੋਸੇਯੋਗ ਸਰੋਤ ਤੋਂ ਆਏ ਹੋਣ। ਅਸੀਂ ਜਿਸ ਨੂੰ ਸੁਰੱਖਿਅਤ ਈਮੇਲ, ਨੱਥੀ ਜਾਂ ਤਸਵੀਰ ਮੰਨ ਕੇ ਖੋਲ੍ਹਦੇ ਹਾਂ ਅਤੇ ਖੁਦ ਨੂੰ ਮੈਲਵੇਅਰ ਜਾਂ ਸਾਡੇ ਵਿਅਕਤੀਗਤ ਡੇਟਾ ਦੀ ਭਾਲ ਕਰਨ ਵਾਲੇ ਕਿਸੇ ਘੁਟਾਲੇਬਾਜ਼ ਦੇ ਕਬਜ਼ੇ ਵਿੱਚ ਪਾਉਂਦੇ ਹਾਂ।

ਵਧੀਆ ਖ਼ਬਰ ਇਹ ਹੈ ਕਿ ਅਸੀਂ ਆਪਣੇ ਮਹੱਤਵਪੂਰਨ ਡੇਟਾ ਦੀ ਸੁਰੱਖਿਆ ਵਾਸਤੇ ਸਾਵਧਾਨੀ ਵਰਤ ਸਕਦੇ ਹਾਂ। ਡਿਵਾਈਸ ਅਤੇ ਡੇਟਾ ਦੀ ਸੁਰੱਖਿਆ ਵਾਸਤੇ ਧੋਖਾਧੜੀ ਨੂੰ ਪਛਾਣਨਾ ਅਤੇ ਉਸਦੀ ਰਿਪੋਰਟ ਕਰਨਾ ਸਿੱਖੋ।

1 ਆਮ ਸੰਕੇਤ ਪਛਾਣੋ

- ਬਹੁਤ ਜ਼ਿਆਦਾ ਜ਼ਰੂਰੀ ਜਾਂ ਭਾਵਨਾਤਮਕ ਤੌਰ 'ਤੇ ਆਕਰਸ਼ਕ ਭਾਸ਼ਾ
- ਵਿਅਕਤੀਗਤ ਜਾਂ ਵਿੱਤੀ ਡੇਟਾ ਭੇਜਣ ਦੀ ਬੇਨਤੀ
- ਅਣਕਿਆਸੀਆਂ ਨੱਥੀਆਂ
- ਗੈਰ-ਭਰੋਸੇਯੋਗ ਛੋਟੇ URLs
- ਅਜਿਹੇ ਈਮੇਲ ਪਤੇ ਜੋ ਕਥਿਤ ਭੇਜਣ ਵਾਲੇ ਨਾਲ ਮੇਲ ਨਹੀਂ ਖਾਂਦੇ (ਜਿਵੇਂ ਕਿ: fkjsd1102@amazon-yahoo.com)
- ਖ਼ਰਾਬ ਵਿਆਕਰਣ/ਹਿੱਜਿਆਂ ਵਿੱਚ ਗਲਤੀਆਂ (ਘੱਟ ਆਮ)

2 ਆਪਣੇ-ਆਪ ਨੂ ਰੋਕੋ ਅਤੇ ਰਿਪੋਰਟ ਕਰੋ

ਫਿਸ਼ਿੰਗ | ਸਪੈਮ

"ਸਪੈਮ ਦੀ ਰਿਪੋਰਟ ਕਰੋ" ਫੀਚਰ ਦੀ ਵਰਤੋਂ ਕਰਕੇ ਸ਼ੱਕੀ ਸੁਨੇਹਿਆਂ ਦੀ ਰਿਪੋਰਟ ਕਰੋ। ਜੇਕਰ ਮੈਸੇਜ ਕਿਸੇ ਅਜਿਹੇ ਸੰਗਠਨ ਤੋਂ ਆਏ ਵਰਗਾ ਲਗਦਾ ਹੈ ਜਿਸ 'ਤੇ ਤੁਸੀਂ ਭਰੋਸਾ ਕਰਦੇ ਹੋ ਤਾਂ ਸੰਗਠਨ ਨੂੰ ਉਨ੍ਹਾਂ ਦੇ ਵੈੱਬਪੰਨੇ 'ਤੇ ਦਿੱਤੀ ਸੰਪਰਕ ਜਾਣਕਾਰੀ ਦੀ ਵਰਤੋਂ ਨਾਲ ਸਚੇਤ ਕਰਕੇ ਮੈਸੇਜ ਬਾਰੇ ਰਿਪੋਰਟ ਕਰੋ।

3 ਡਿਲੀਟ ਕਰੋ

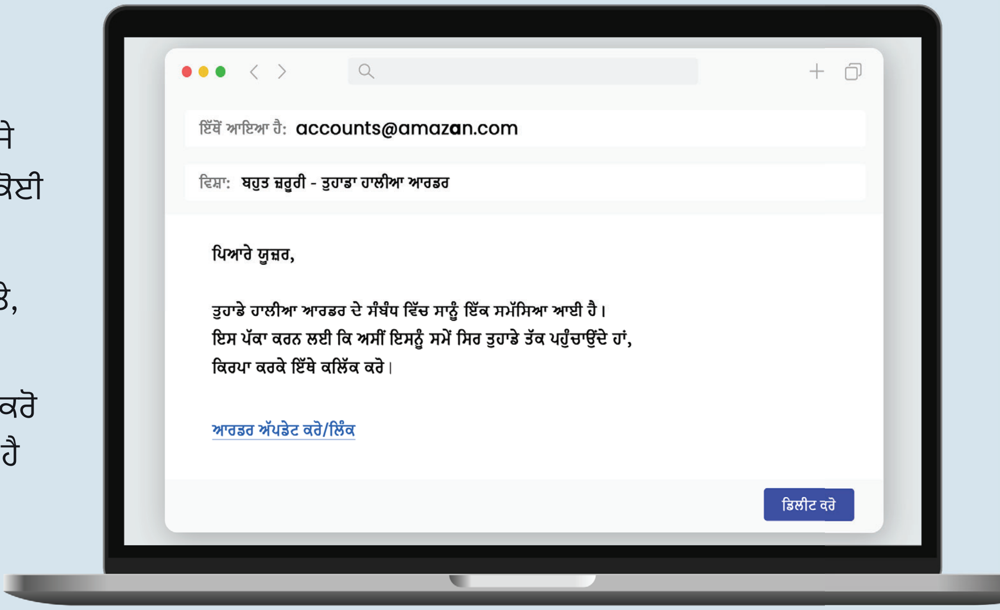
ਮੈਸੇਜ ਨੂੰ ਡਿਲੀਟ ਕਰਾ ਦਿਓ। ਕਿਸੇ ਵੀ ਅਜਿਹੀ ਅਟੈਚਮੈਂਟ ਜਾਂ ਲਿੰਕ ਦਾ ਜਵਾਬ ਨਾ ਦਿਓ ਜਾਂ ਕਲਿੱਕ ਨਾ ਕਰੋ, ਜਿਸ ਵਿੱਚ ਕੋਈ "ਅਣ-ਸਬਸਕ੍ਰਾਈਬ ਕਰੋ" ਲਿੰਕ ਵੀ ਸ਼ਾਮਲ ਹੁੰਦੇ ਹਨ। ਅਣ-ਸਬਸਕ੍ਰਾਈਬ ਕਰੋ ਬਟਨ ਵਿੱਚ ਧੋਖਾਧੜੀ ਵਾਸਤੇ ਵਰਤੋਂ **ਕੀਤਾ ਜਾਣ ਵਾਲਾ ਲਿੰਕ ਸ਼ਾਮਲ ਹੋ ਸਕਦਾ ਹੈ। ਬਸ ਡਿਲੀਟ ਕਰ ਦਿਓ।**

ਡਿਲੀਟ ਕਰੋ

ਜੇਕਰ ਕੋਈ ਮੈਸੇਜ ਸ਼ੱਕੀ ਲੱਗਦਾ ਹੈ ਤਾਂ ਸੰਭਾਵੀ ਤੌਰ 'ਤੇ ਇਹ ਧੋਖਾਧੜੀ ਹੈ।

ਪਰ ਜੇਕਰ ਕੋਈ ਅਜਿਹੀ ਸੰਭਾਵਨਾ ਹੀ ਹੋਵੇ ਕਿ ਇਹ ਅਸਲ ਹੋ ਸਕਦਾ ਹੈ ਤਾਂ ਕਿਸੇ ਵੀ ਲਿੰਕ, ਅਟੈਚਮੈਂਟ 'ਤੇ ਕਲਿੱਕ ਨਾ ਕਰੋ ਜਾਂ ਕਿਸੇ ਨੰਬਰ 'ਤੇ ਕਾੱਲ ਨਾ ਕਰੋ। ਕਿਸੇ ਕੰਪਨੀ ਜਾਂ ਵਿਅਕਤੀ ਨਾਲ ਸਿੱਧਾ ਸੰਪਰਕ ਕਰਨ ਦਾ ਕੋਈ ਦੂਜਾ ਤਰੀਕਾ ਖੋਜੋ:

- ਕਿਸੇ ਕੰਪਨੀ ਦੀ ਸੰਪਰਕ ਜਾਣਕਾਰੀ ਖੋਜਣ ਵਾਸਤੇ, ਉਸ ਦੀ ਵੈੱਬਸਾਈਟ 'ਤੇ ਜਾਓ
- ਉਸ ਵਿਅਕਤੀ ਨੂੰ ਕਿਸੇ ਗਿਆਤ ਨੰਬਰ 'ਤੇ ਕਾੱਲ ਕਰੋ ਅਤੇ ਪੁਸ਼ਟੀ ਕਰੋ ਕਿ ਉਨ੍ਹਾਂ ਨੇ ਉਹ ਮੈਸੇਜ ਭੇਜਿਆ ਹੈ ਜਾਂ ਨਹੀਂ



ਧੋਖਾਧੜੀ ਤੋਂ ਬਚਣਾ **ਸਾਡੀ ਦੁਨੀਆ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖਣ** ਦਾ ਇੱਕ ਤਰੀਕਾ ਹੈ।

ਅਸੀਂ ਸਾਰਿਆਂ ਨੂੰ ਔਨਲਾਈਨ ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਵਿੱਚ ਮਦਦ ਕਰ ਸਕਦੇ ਹਾਂ, ਇਸ ਲਈ ਇਨ੍ਹਾਂ ਸੁਝਾਵਾਂ ਨੂੰ ਪਰਿਵਾਰ ਦੇ ਕਿਸੇ ਮੈਂਬਰ ਜਾਂ ਮਿੱਤਰ ਨਾਲ ਸਾਂਝਾ ਕਰੋ!

cisa.gov/SecureOurWorld