ਨਿੱਜੀ ਸੁਰੱਖਿਆ ਬਾਰੇ ਵਿਚਾਰਨਯੋਗ ਗੱਲਾਂ ਸੰਬੰਧੀ ਕਾਰਵਾਈ ਗਾਈਡ ਮਹੱਤਵਪੂਰਨ ਬੁਨਿਆਦੀ ਢਾਂਚੇ ਦੇ ਕਰਮਚਾਰੀ

ਜਾਣ-ਪਛਾਣ

ਅੱਜ ਦੇ ਮੌਜੂਦਾ ਖ਼ਤਰੇ ਭਰੇ ਮਾਹੌਲ ਵਿੱਚ, ਚੌਕਸ ਰਹਿਣਾ ਅਤੇ ਆਪਣੀ ਨਿੱਜੀ ਸੁਰੱਖਿਆ ਦੀ ਜ਼ਿੰਮੇਵਾਰੀ ਲੈਣਾ ਸਾਰੇ ਮਹੱਤਵਪੂਰਨ ਬੁਨਿਆਦੀ ਢਾਂਚੇ ਦੇ ਕਰਮਚਾਰੀਆਂ ਲਈ ਬਹੁਤ ਜ਼ਰੂਰੀ ਹੈ—ਕਾਰਜ-ਸਥਾਨ 'ਤੇ ਅਤੇ ਕਾਰਜ-ਸਥਾਨ ਤੋਂ ਬਾਹਰ, ਦੋਵੇਂ ਥਾਵਾਂ 'ਤੇ। ਮਹੱਤਵਪੂਰਨ ਬੁਨਿਆਦੀ ਢਾਂਚਾ ਕਰਮਚਾਰੀ ਬਹੁਤ ਤਰ੍ਹਾਂ ਦੀਆਂ ਸੇਵਾਵਾਂ ਪੂਰੀਆਂ ਕਰਦੇ ਹਨ ਜੋ ਆਧੁਨਿਕ ਅਮਰੀਕੀ ਜੀਵਨ ਲਈ ਜ਼ਰੂਰੀ ਪ੍ਰਣਾਲੀਆਂ ਅਤੇ ਸੰਪਤੀਆਂ ਨੂੰ ਸੰਚਾਲਿਤ ਕਰਦੇ ਹਨ, ਚਲਾਉਂਦੇ ਹਨ ਅਤੇ ਸੰਭਾਲਦੇ ਹਨ। ਤੁਹਾਡੇ ਕੰਮ ਨਾਲ ਜੁੜੇ ਕਿਸੇ ਵੀ ਖ਼ਤਰੇ ਜਾਂ ਖ਼ਤਰਿਆਂ ਨੂੰ ਧਿਆਨ ਵਿੱਚ ਰੱਖਣਾ ਅਤੇ ਸਾਰੀਆਂ ਸੁਰੱਖਿਆ ਪ੍ਰਕਿਰਿਆਵਾਂ ਦੀ ਪਾਲਣਾ ਕਰਨਾ ਤੁਹਾਡੀ, ਤੁਹਾਡੇ ਨਜ਼ਦੀਕੀ ਲੋਕਾਂ ਅਤੇ ਉਸ ਬੁਨਿਆਦੀ ਢਾਂਚੇ, ਜਿਸ ਨੂੰ ਤੁਸੀਂ ਸੇਵਾ ਦਿੰਦੇ ਹੋ, ਦੀ ਰੱਖਿਆ ਕਰਨ ਵਿੱਚ ਮਦਦ ਕਰੇਗਾ। ਨਿੱਜੀ ਸੁਰੱਖਿਆ ਨੂੰ ਤਿੰਨ ਮੁੱਖ ਹਿੱਸਿਆਂ ਵਿੱਚ ਵੰਡਿਆ ਜਾ ਸਕਦਾ ਹੈ—ਭੌਤਿਕ ਸੁਰੱਖਿਆ, ਸਥਿਤੀ ਸੰਬੰਧੀ ਜਾਗਰੂਕਤਾ ਅਤੇ ਔਨਲਾਈਨ ਸੁਰੱਖਿਆ। ਇਹ ਗੈਰ-ਸੰਪੂਰਨ ਕਾਰਵਾਈ ਗਾਈਡ ਤੁਹਾਡੀ ਸੁਰੱਖਿਆ ਸਥਿਤੀ ਦਾ ਮੁਲਾਂਕਣ ਕਰਨ ਵਿੱਚ ਤੁਹਾਡੀ ਮਦਦ ਕਰ ਸਕਦੀ ਹੈ ਅਤੇ ਖ਼ਤਰਿਆਂ ਨੂੰ ਘਟਾਉਣ 'ਤੇ ਵਿਚਾਰ ਕਰਨ ਲਈ ਵਿਕਲਪ ਮੁਹੱਈਆ ਕਰ ਸਕਦੀ ਹੈ।[1]

ਮਹੱਤਵਪੂਰਨ ਬੁਨਿਆਦੀ ਢਾਂਚਾ ਕਰਮਚਾਰੀਆਂ ਵਾਸਤੇ ਸੁਰੱਖਿਆ ਦੇ ਉਚਿਤ ਪੱਧਰ ਦਾ ਮੁਲਾਂਕਣ ਕਰਨਾ

ਇਹ ਗਾਈਡ ਘਰ ਵਿੱਚ, ਕਾਰਜਸਥਾਨ 'ਤੇ, ਜਨਤਕ ਸਥਾਨਾਂ 'ਤੇ ਅਤੇ ਔਨਲਾਈਨ ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਦੇ ਤਰੀਕਿਆਂ ਬਾਰੇ ਇੱਕ ਵਿਆਪਕ ਜਾਣਕਾਰੀ ਮੁਹੱਈਆ ਕਰਦੀ ਹੈ। ਇਹ ਫੈਸਲਾ ਕਰਨਾ ਤੁਹਾਡੇ 'ਤੇ ਨਿਰਭਰ ਕਰਦਾ ਹੈ ਕਿ ਤੁਹਾਡੀ ਜੀਵਨਸ਼ੈਲੀ, ਸੁਰੱਖਿਆ ਸੰਬੰਧੀ ਕਮਜ਼ੋਰੀਆਂ ਅਤੇ ਉਨ੍ਹਾਂ ਸਥਿਤੀਆਂ ਜੋ ਸ਼ਾਇਦ ਤੁਹਾਡੇ ਸਾਹਮਣੇ ਆ ਸਕਦੀਆਂ ਹਨ, ਲਈ ਕਿਹੜੇ ਉਪਾਅ ਸਭ ਤੋਂ ਢੁਕਵੇਂ ਹਨ—ਉਦਾਹਰਨ ਲਈ, ਕੁਝ ਕਾਰਕ ਕੰਮ ਵਾਲੀ ਥਾਂ 'ਤੇ ਹਿੰਸਾ ਦੀ ਸੰਭਾਵਨਾ ਨੂੰ ਵਧਾ ਸਕਦੇ ਹਨ:

- **ਇਕੱਲੇ** ਜਾਂ ਅਲੱਗ-ਥਲੱਗ ਖੇਤਰਾਂ ਵਿੱਚ ਕੰਮ ਕਰਨਾ।
- **ਵਿਅਕਤੀਗਤ ਮੌਜੂਦਗੀ ਵਾਲੀਆਂ ਸੇਵਾਵਾਂ** ਜਾਂ ਦੇਖਭਾਲ ਮੁਹੱਈਆ ਕਰਨਾ।
- **ਖ਼ਤਰਨਾਕ ਸਮੱਗਰੀ ਨਾਲ** ਜਾਂ ਰਾਸ਼ਟਰੀ ਸੁਰੱਖਿਆ ਪ੍ਰਤੀ ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਨਾਲ ਕੰਮ ਕਰਨਾ।
- ਸਥਾਨਕ ਜਾਂ ਰਾਸ਼ਟਰੀ ਮਹੱਤਵਪੂਰਨ ਬੁਨਿਆਦੀ ਢਾਂਚੇ ਦੀ **ਸੁਰੱਖਿਆ ਲਈ ਜ਼ਿੰਮੇਵਾਰੀ**।

ਤੁਹਾਡੀਆਂ ਸੁਰੱਖਿਆ ਸੰਬੰਧੀ ਲੋੜਾਂ ਦਾ ਮੁਲਾਂਕਣ ਕਰਦੇ ਸਮੇਂ, ਹੇਠਾਂ ਦਿੱਤੀਆਂ ਗੱਲਾਂ 'ਤੇ ਵਿਚਾਰ ਕਰੋ:

- **ਤੁਹਾਡਾ ਪੇਸ਼ਾ ਅਤੇ ਪੇਸ਼ੇਵਰ ਭੂਮਿਕਾ**। ਕੀ ਤੁਹਾਡੀ ਨੌਕਰੀ ਜਾਂ ਕਰੀਅਰ ਤੁਹਾਨੂੰ ਇੱਕ ਆਕਰਸ਼ਕ ਨਿਸ਼ਾਨਾ ਬਣਾਉਂਦਾ ਹੈ?
- **ਖਾਸ ਖ਼ਤਰੇ**। ਕੀ ਕੋਈ ਭਰੋਸੇਯੋਗ ਸਬੂਤ ਹੈ ਜੋ ਤੁਹਾਡੇ ਲਈ ਖ਼ਤਰੇ ਦਾ ਸੰਕੇਤ ਦਿੰਦਾ ਹੈ?
- **ਤੁਹਾਡਾ ਨਿੱਜੀ ਇਤਿਹਾਸ**। ਕੀ ਬੀਤੇ ਸਮੇਂ ਵਿੱਚ ਤੁਹਾਨੂੰ ਨਿਸ਼ਾਨਾ ਬਣਾਇਆ ਗਿਆ ਹੈ ਜਾਂ ਧਮਕੀ ਦਿੱਤੀ ਗਈ ਹੈ?
- **ਤੁਹਾਡੇ ਨਿੱਜੀ ਦਿੱਸਣ ਵਾਲੇ ਪਛਾਣਕਰਤਾ**। ਕੀ ਤੁਸੀਂ ਕਿਸੇ ਵੀ ਸਮੂਹ ਨਾਲ ਸਬੰਧ ਪ੍ਰਦਰਸ਼ਿਤ ਕਰਦੇ ਹੋ ਜੋ ਤੁਹਾਨੂੰ ਆਕਰਸ਼ਕ ਨਿਸ਼ਾਨਾ ਬਣਾਉਂਦੇ ਹਨ?

ਅੱਜ, ਮਹੱਤਵਪੂਰਨ ਬੁਨਿਆਦੀ ਢਾਂਚੇ ਦੇ ਕਰਮਚਾਰੀਆਂ ਨੂੰ ਸੰਭਾਵੀ ਤੌਰ 'ਤੇ ਕਈ ਤਰ੍ਹਾਂ ਦੇ ਖ਼ਤਰਿਆਂ ਦਾ ਸਾਹਮਣਾ ਕਰਨਾ ਪੈਂਦਾ ਹੈ—ਆਮ ਅਪਰਾਧਕ ਗਤੀਵਿਧੀ ਤੋਂ ਲੈ ਕੇ ਹਿੰਸਕ ਕੱਟੜਪੰਥੀਆਂ ਦੀਆਂ ਸਾਜ਼ਿਸ਼ਾਂ ਤੱਕ। ਜੇ ਤੁਸੀਂ ਉਪਰੋਕਤ ਕਿਸੇ ਵੀ ਜਾਂ ਸਾਰੇ ਸਵਾਲਾਂ ਦਾ ਜਵਾਬ ਹਾਂ ਵਿੱਚ ਦਿੱਤਾ ਹੈ, ਤਾਂ ਇਹ ਇਸ ਗੱਲ ਦਾ ਸੰਕੇਤ ਹੋ ਸਕਦਾ ਹੈ ਕਿ ਤੁਸੀਂ ਅਤੇ ਸੰਭਾਵੀ ਤੌਰ 'ਤੇ ਹੋਰ ਮਹੱਤਵਪੂਰਨ ਬੁਨਿਆਦੀ ਢਾਂਚੇ ਦੇ ਕਰਮਚਾਰੀ ਜਿਨ੍ਹਾਂ ਨਾਲ ਤੁਸੀਂ ਕੰਮ ਕਰਦੇ ਹੋ, ਜੋਖਮ ਵਿੱਚ ਹੋ ਅਤੇ ਤੁਹਾਨੂੰ ਆਪਣੀਆਂ ਸੁਰੱਖਿਆ ਸੰਬੰਧੀ ਲੋੜਾਂ ਦਾ ਮੁਲਾਂਕਣ ਕਰਨਾ ਚਾਹੀਦਾ ਹੈ। ਜਦੋਂ ਤੁਸੀਂ ਆਪਣੀ ਨਿੱਜੀ ਸੁਰੱਖਿਆ ਦਾ ਮੁਲਾਂਕਣ ਕਰਦੇ ਹੋ, ਤਾਂ ਇਹ ਮਹੱਤਵਪੂਰਨ ਹੈ ਕਿ ਤੁਸੀਂ ਇੱਕ ਸੰਤੁਲਿਤ ਪਹੁੰਚ ਨੂੰ ਅਪਣਾਓ ਅਤੇ ਯਾਦ ਨਾਲ ਆਪਣੇ ਘਰ ਅਤੇ ਕਾਰਜ-ਸਥਾਨ, ਦੋਵਾਂ ਸਥਾਨਾਂ 'ਤੇ ਜੀਵਨ ਨੂੰ ਧਿਆਨ ਵਿੱਚ ਰੱਖੋ—**ਆਪਣੀਆਂ ਨਿੱਜੀ ਸੁਰੱਖਿਆ ਸੰਬੰਧੀ ਵਿਧੀਆਂ, ਆਦਤਾਂ ਵਿੱਚ ਸੁਚੇਤ ਰਹੋ ਅਤੇ ਆਪਣੇ ਆਲੇ-ਦੁਆਲੇ ਦਾ ਲਗਾਤਾਰ ਮੁਲਾਂਕਣ ਕਰੋ**। ਤੁਹਾਡੇ ਦੁਆਰਾ ਚੁੱਕੇ ਜਾਣ ਵਾਲੇ ਉਪਾਅ ਮੰਨੀਆਂ ਜਾਣ ਵਾਲੀਆਂ ਧਮਕੀਆਂ ਲਈ ਉਚਿਤ ਹੋਣੇ ਚਾਹੀਦੇ ਹਨ। ਬਹੁਤ ਜ਼ਿਆਦਾ ਸੁਰੱਖਿਆ ਕਾਰਵਾਈਆਂ ਬੇਲੋੜੇ ਤਣਾਉ ਅਤੇ ਅਸੁਵਿਧਾ ਦਾ ਕਾਰਨ ਬਣ ਸਕਦੀਆਂ ਹਨ; ਹਾਲਾਂਕਿ, ਨਾਕਾਫ਼ੀ ਕੋਸ਼ਿਸ਼ਾਂ ਤੁਹਾਨੂੰ ਜੋਖਮ ਵਿੱਚ ਪਾ ਸਕਦੀਆਂ ਹਨ।

ਅਸੁਰੱਖਿਅਤ ਸਥਿਤੀਆਂ ਨੂੰ ਪਛਾਣਨ ਦੀ ਯੋਗਤਾ ਉਨ੍ਹਾਂ ਤੋਂ ਬਚਣ ਜਾਂ ਜਦੋਂ ਉਹ ਵਾਪਰਦੀਆਂ ਹਨ ਤਾਂ ਉਸ ਸਮੇਂ ਲਈ ਤਿਆਰ ਰਹਿਣ ਲਈ ਬਹੁਤ ਮਹੱਤਵਪੂਰਨ ਹੈ। ਅਸੁਰੱਖਿਅਤ ਹੋਣਾ ਇੱਕ ਭੌਤਿਕ ਵਿਸ਼ੇਸ਼ਤਾ ਜਾਂ ਸੰਚਾਲਨ ਸੰਬੰਧੀ ਗੁਣ ਹੈ ਜੋ ਕਿਸੇ ਇਕਾਈ, ਸੰਪਤੀ, ਸਿਸਟਮ, ਨੈੱਟਵਰਕ ਜਾਂ ਭੂਗੋਲਿਕ ਖੇਤਰ ਨੂੰ ਸ਼ੋਸ਼ਣ ਲਈ ਖੁੱਲ੍ਹਾ ਜਾਂ ਕਿਸੇ ਦਿੱਤੇ ਖ਼ਤਰੇ ਲਈ ਸੰਵੇਦਨਸ਼ੀਲ ਬਣਾਉਂਦਾ ਹੈ।[2] ਜਦੋਂ ਹਮਲਾਵਰ ਵਿਅਕਤੀਆਂ ਨੂੰ ਨਿਸ਼ਾਨਾ ਬਣਾਉਂਦੇ ਹਨ ਤਾਂ ਉਹ ਰਚਨਾਤਮਕ ਹੋ ਸਕਦੇ ਹਨ। ਹਮਲਾ ਕਰਨ ਵਾਲੇ ਦਾ ਟੀਚਾ ਸ਼ਰਮ, ਅਸੁਵਿਧਾ, ਪਰੇਸ਼ਾਨੀ ਪੈਦਾ ਕਰਨਾ ਹੋ ਸਕਦਾ ਹੈ ਜਾਂ ਉਹ ਸ਼ਾਇਦ ਉਸਦਾ ਇਰਾਦਾ ਸਰੀਰਕ ਸੱਟ, ਤੰਦਰੁਸਤੀ ਵਿੱਚ ਵਿਘਨ ਪਾਉਣ ਜਾਂ ਮਨੁੱਖੀ ਜੀਵਨ ਨੂੰ ਖ਼ਤਰਾ ਵਿੱਚ ਪਾਉਣਾ ਹੋ ਸਕਦਾ ਹੈ।

1 ProtectUK. 2022. Publicly accessible locations (PALs) guidance: Personal security. 8 ਅਗਸਤ, 2023 ਨੂੰ ਪਹੁੰਚ ਕੀਤੀ ਗਈ। protectuk.police.uk/personal-security.

2 U.S. Department of Homeland Security. Risk Steering Committee. 2010. DHS Risk Lexicon 2010 Edition. ਅਗਸਤ 8, 2023 ਨੂੰ ਪਹੁੰਚ ਕੀਤੀ ਗਈ। cisa.gov/resources-tools/resources/dhs-risk-lexicon.

ਭੌਤਿਕ ਸੁਰੱਖਿਆ

ਤੁਹਾਡੇ ਘਰ ਦੀ ਰੱਖਿਆ ਕਰਨੀ

ਵਿਚਾਰ ਕਰਨ ਲਈ ਕਈ ਵੱਖ-ਵੱਖ ਤਰ੍ਹਾਂ ਦੇ ਸਧਾਰਨ ਉਪਾਅ ਹਨ ਜੋ ਤੁਹਾਡੀ ਅਤੇ ਤੁਹਾਡੇ ਘਰ ਦੀ ਰੱਖਿਆ ਕਰਨ ਵਿੱਚ ਮਦਦ ਕਰ ਸਕਦੇ ਹਨ। ਤੁਹਾਡੇ ਨਿਵਾਸ ਜਾਂ ਸੰਪਤੀ ਦੇ ਆਲੇ ਦੁਆਲੇ ਸੁਰੱਖਿਆ ਪ੍ਰਣਾਲੀਆਂ ਨੂੰ ਸਥਾਪਤ ਕਰਨ ਜਾਂ ਸੁਧਾਰਨ ਨਾਲ ਸ਼ੁਰੂਆਤ ਕਰੋ। ਕਿਸੇ ਵੀ ਦਰਵਾਜ਼ੇ ਜਾਂ ਖਿੜਕੀਆਂ ਨੂੰ ਤਾਲਿਆਂ, ਚਾਬੀਆਂ, ਅਲਾਰਮ, ਲਾਈਟਾਂ ਨਾਲ ਸੁਰੱਖਿਅਤ ਕਰੋ ਅਤੇ ਕਲੋਜ਼-ਸਰਕਟ ਟੈਲੀਵਿਜ਼ਨ (CCTV) ਸਿਸਟਮ ਦੀ ਲੋੜ ਦਾ ਮੁਲਾਂਕਣ ਕਰੋ। ਦਾਖਲ ਹੋਣ ਦੇ ਤਰੀਕਿਆਂ ਅਤੇ ਖਿੜਕੀਆਂ ਲਈ ਕਿਸੇ ਉੱਨਤ ਲਾਕਿੰਗ ਸਿਸਟਮ ਦੀ ਵਰਤੋਂ ਕਰਨ 'ਤੇ ਵਿਚਾਰ ਕਰੋ ਜਿਸ ਵਿੱਚ ਨਿਗਰਾਨੀ ਵਾਲੀ (ਮਲਟੀ-ਦ੍ਰਿਸ਼ ਸਮਰੱਥ) ਵੀਡੀਓ ਚੌਕਸੀ ਪ੍ਰਣਾਲੀ ਹੋਵੇ।

ਜਾਇਦਾਦ ਦੇ ਬਾਹਰੀ ਢਾਂਚਿਆਂ, ਜਿਵੇਂ ਕਿ ਕੰਧਾਂ ਅਤੇ ਵਾੜਾਂ ਦੀ ਸਾਂਭ-ਸੰਭਾਲ ਕਰੋ ਅਤੇ ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਤੁਹਾਡੇ ਘਰ ਤੱਕ ਪਹੁੰਚਣ ਲਈ ਵਰਤੇ ਜਾ ਸਕਣ ਵਾਲੇ ਕੋਈ ਵੀ ਔਜ਼ਾਰਾਂ ਜਾਂ ਪੌੜੀਆਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਢੰਗ ਨਾਲ ਸਟੋਰ ਕੀਤਾ ਜਾਵੇ। ਕਿਸੇ ਵੀ ਅਜਿਹੀ ਚੀਜ਼ ਨੂੰ ਹਟਾਉਣ 'ਤੇ ਵਿਚਾਰ ਕਰੋ ਜਿਸ ਨੂੰ ਨੁਕਸਾਨ ਪਹੁੰਚਾਉਣ ਲਈ ਵਰਤਿਆ ਜਾ ਸਕਦੀ ਹੈ, ਜਿਵੇਂ ਕਿ ਖੁੱਲੀਆਂ ਇੱਟਾਂ, ਵੱਡੇ ਪੱਥਰ ਅਤੇ ਬਗੀਚੇ ਵਿੱਚ ਸਜਾਵਟੀ ਚੀਜ਼ਾਂ। ਇਹ ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਝਾੜੀਆਂ, ਘਾਹ-ਫੂਸ ਆਦਿ ਦੀ ਕਟਾਈ ਅਤੇ ਸਾਂਭ-ਸੰਭਾਲ ਕੀਤੀ ਜਾਂਦੀ ਹੈ ਤਾਂ ਜੋ ਪੱਤੇ:

- **ਘੁਸਪੈਠੀਆਂ ਦੁਆਰਾ ਲੁਕਣ ਜਾਂ** ਘਰ ਅੰਦਰ ਦਾਖਲ ਹੋਣ ਲਈ ਨਾ ਵਰਤੇ ਜਾ ਸਕਣ।
- **ਘਰ ਦੇ ਅੰਦਰੋਂ ਬਾਹਰ** ਦੇ ਦ੍ਰਿਸ਼ ਵਿੱਚ ਰੁਕਾਵਟ ਨਾ ਬਣਦੇ ਹੋਣ।

ਬਾਹਰੀ ਦਰਵਾਜ਼ਿਆਂ ਅਤੇ ਖਿੜਕੀਆਂ ਨੂੰ ਢੁਕਵੇਂ ਤਾਲਾਬੰਦ ਡਿਵਾਈਸਾਂ ਨਾਲ ਸੁਰੱਖਿਅਤ ਕਰੋ, ਜਿਨ੍ਹਾਂ ਵਿੱਚ ਇਲੈਕਟ੍ਰਾਨਿਕ ਅਤੇ ਕੋਡ ਵਾਲੀਆਂ ਲਾਕਿੰਗ ਵਿਧੀਆਂ ਸ਼ਾਮਲ ਹੋ ਸਕਦੀਆਂ ਹਨ। ਐਮਰਜੈਂਸੀ ਦੌਰਾਨ ਵਰਤਣ ਲਈ ਚਾਬੀਆਂ ਜਾਂ ਐਂਟਰੀ ਕੋਡਾਂ ਦਾ ਇੱਕ ਵਾਧੂ ਸੈੱਟ ਸੁਰੱਖਿਅਤ ਕਰਨਾ ਸਭ ਤੋਂ ਵਧੀਆ ਹੈ। ਐਂਟਰੀ ਕੋਡਾਂ ਨਾਲ ਛੇੜਛਾੜ ਕੀਤੇ ਜਾਣ ਜਾਂ ਚਾਬੀਆਂ ਗੁੰਮ ਹੋਣ ਦੀ ਸੂਰਤ ਵਿੱਚ ਪੂਰੇ ਲਾਕਿੰਗ ਸਿਸਟਮ ਨੂੰ ਬਦਲਣ 'ਤੇ ਵਿਚਾਰ ਕਰੋ।

ਅਜਿਹੀ ਬਾਹਰੀ ਰੋਸ਼ਨੀ ਵਿੱਚ ਨਿਵੇਸ਼ ਕਰੋ ਅਤੇ ਉਸਦੀ ਸਾਂਭ-ਸੰਭਾਲ ਕਰੋ ਜੋ ਬਾਹਰੀ ਦਰਵਾਜ਼ਿਆਂ, ਪਾਰਕਿੰਗ ਖੇਤਰਾਂ ਅਤੇ ਘਰ ਦੇ ਆਲੇ ਦੁਆਲੇ ਤੁਰ ਵਾਲੇ ਰਸਤਿਆਂ ਨੂੰ ਰੋਸ਼ਨ ਕਰੇ। ਦਰਵਾਜ਼ਿਆਂ ਅਤੇ ਖਿੜਕੀਆਂ ਦੇ ਦ੍ਰਿਸ਼ਾਂ ਵਾਲੇ ਕੈਮਰੇ ਲਗਾਉਣ ਬਾਰੇ ਵਿਚਾਰ ਕਰੋ। ਇਨ੍ਹਾਂ ਲਾਈਟਾਂ ਅਤੇ ਕੈਮਰਿਆਂ ਨੂੰ ਰਣਨੀਤਕ ਤਰੀਕੇ ਨਾਲ ਕਿਸੇ ਵੀ ਅਜਿਹੇ ਸਥਾਨਾਂ ਨੂੰ ਖਤਮ ਕਰਨ ਲਈ ਲਗਾਓ ਜਿੱਥੇ ਕੋਈ ਵਿਅਕਤੀ ਦਿਖਾਈ ਦੇਣ ਤੋਂ ਬਚ ਸਕਦਾ ਹੈ।

ਜੇ ਤੁਹਾਡੇ ਕੋਲ ਵਾਹਨ ਹੈ ਅਤੇ ਤੁਸੀਂ ਇਸਨੂੰ ਗੈਰੇਜ ਜਾਂ ਤਾਲਾਬੰਦ ਖੇਤਰ ਵਿੱਚ ਸੁਰੱਖਿਅਤ ਨਹੀਂ ਕਰ ਸਕਦੇ ਹੋ, ਤਾਂ ਇਸਨੂੰ ਜਨਤਕ ਸਥਾਨ 'ਤੇ ਛੱਡਣ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰੋ। ਕਿਸੇ ਚੰਗੀ ਰੋਸ਼ਨੀ ਵਾਲੇ ਖੇਤਰ, CCTV ਕੈਮਰੇ ਦੀ ਨਜ਼ਰ ਵਿੱਚ ਜਾਂ ਸਟਾਫ਼ ਵਾਲੀ ਪਾਰਕਿੰਗ ਵਿੱਚ ਪਾਰਕ ਕਰੋ। ਕਿਸੇ ਵੀ ਖਿੜਕੀਆਂ ਨੂੰ ਹਮੇਸ਼ਾ ਬੰਦ ਕਰੋ, ਕੀਮਤੀ ਸਮਾਨ ਨੂੰ ਨਜ਼ਰ ਤੋਂ ਦੂਰ ਰੱਖੋ ਅਤੇ ਆਪਣੀ ਕਾਰ ਨੂੰ ਲਾਕ ਕਰੋ, ਭਾਵੇਂ ਤੁਸੀਂ ਕੁਝ ਮਿੰਟਾਂ ਲਈ ਦੂਰ ਜਾ ਰਹੇ ਹੋਵੋ। ਸਮਝੋ ਕਿ ਤੁਹਾਡੇ ਵਾਹਨ ਦੇ ਅੰਦਰ ਜਿਸ ਕਿਸਮ ਦਾ ਚੋਰੀ ਰੋਕਣ ਵਾਲਾ ਅਲਾਰਮ ਸਿਸਟਮ ਲੱਗਾ ਹੈ, ਉਸ ਨੂੰ ਕਿਵੇਂ ਵਰਤਣਾ ਹੈ। ਪੁਲਿਸ ਦੀ ਪ੍ਰਤਿਕਿਰਿਆ ਨੂੰ ਤੇਜ਼ ਕਰਨ ਵਿੱਚ ਸਹਾਇਤਾ ਕਰਨ ਲਈ ਵਾਹਨ ਲੋਕੇਟਰ ਸੇਵਾਵਾਂ ਤੋਂ ਇਲਾਵਾ ਅਜਿਹੇ ਸਿਸਟਮ ਹਨ ਜਿਨ੍ਹਾਂ ਵਿੱਚ ਸੁਣਾਈ ਅਤੇ ਦਿਖਾਈ ਦੇਣ ਵਾਲੀਆਂ ਸੂਚਨਾਵਾਂ ਸ਼ਾਮਲ ਹੁੰਦੀਆਂ ਹਨ।

ਪਹਿਲਾਂ ਤੋਂ ਯੋਜਨਾ ਬਣਾਓ

ਪਰਿਵਾਰਕ ਐਮਰਜੈਂਸੀ ਕਾਰਵਾਈ ਯੋਜਨਾ ਤਿਆਰ ਕਰਨ ਅਤੇ ਐਮਰਜੈਂਸੀ ਦੀ ਸਥਿਤੀ ਵਿੱਚ ਕੀ ਕਰਨਾ ਹੈ, ਇਸਦਾ ਅਭਿਆਸ ਕਰਨ 'ਤੇ ਵਿਚਾਰ ਕਰੋ। ਯੋਜਨਾ ਤਿਆਰ ਕਰਨ ਵਿੱਚ ਮਦਦ ਲਈ, ਇੱਥੇ ਜਾਓ:

fema.gov/blog/have-emergency-plan-your-family.

ਗੋਲੀ ਚਲਾਉਣ ਵਾਲੇ ਹਥਿਆਰਾਂ ਨਾਲ ਹਮਲੇ

ਕਿਰਿਆਸ਼ੀਲ ਸ਼ੂਟਰ ਦੀ ਪਰਿਭਾਸ਼ਾ ਹੈ ਇੱਕ ਜਾਂ ਵੱਧ ਵਿਅਕਤੀ ਜੋ ਕਿਸੇ ਆਬਾਦੀ ਵਾਲੇ ਖੇਤਰ ਵਿੱਚ ਲੋਕਾਂ ਨੂੰ ਮਾਰਨ ਜਾਂ ਮਾਰਨ ਦੀ ਕੋਸ਼ਿਸ਼ ਵਿੱਚ ਸਰਗਰਮੀ ਨਾਲ ਰੁੱਝੇ ਹੋਏ ਹਨ।[3] ਕਿਰਿਆਸ਼ੀਲ ਸ਼ੂਟਰ ਦੀਆਂ ਘਟਨਾਵਾਂ ਦਾ ਅਕਸਰ ਅਨੁਮਾਨ ਨਹੀਂ ਲਗਾਇਆ ਜਾ ਸਕਦਾ ਹੈ ਅਤੇ ਇਹ ਤੇਜ਼ੀ ਨਾਲ ਵਿਕਸਤ ਹੋ ਜਾਂਦੀਆਂ ਹਨ। ਹਫੜਾ-ਦਫੜੀ ਵਿੱਚ, ਕੋਈ ਵੀ ਵਿਅਕਤੀ ਕਿਸੇ ਕਿਰਿਆਸ਼ੀਲ ਸ਼ੂਟਰ ਵਾਲੀ ਘਟਨਾ ਦੇ ਪ੍ਰਭਾਵਾਂ ਨੂੰ ਘਟਾਉਣ ਵਿੱਚ ਇੱਕ ਮਹੱਤਵਪੂਰਨ ਭੂਮਿਕਾ ਨਿਭਾ ਸਕਦਾ ਹੈ।

ਕਿਉਂਕਿ ਕਿਰਿਆਸ਼ੀਲ ਸ਼ੂਟਰ ਵਾਲੀਆਂ ਸਥਿਤੀਆਂ ਅਕਸਰ 10 ਤੋਂ 15 ਮਿੰਟਾਂ ਦੇ ਅੰਦਰ - ਕਾਨੂੰਨ ਲਾਗੂ ਕਰਨ ਵਾਲਿਆਂ ਦੇ ਘਟਨਾ ਸਥਾਨ 'ਤੇ ਪਹੁੰਚਣ ਤੋਂ ਪਹਿਲਾਂ - ਖਤਮ ਹੋ ਜਾਂਦੀਆਂ ਹਨ, ਵਿਅਕਤੀਆਂ ਨੂੰ ਕਿਸੇ ਕਿਰਿਆਸ਼ੀਲ ਸ਼ੂਟਰ ਵਾਲੀ ਘਟਨਾ ਵਿੱਚ ਪ੍ਰਤਿਕਿਰਿਆ ਕਰਨ ਲਈ ਮਾਨਸਿਕ ਅਤੇ ਸਰੀਰਕ ਤੌਰ 'ਤੇ ਤਿਆਰ ਹੋਣਾ ਚਾਹੀਦਾ ਹੈ।

ਸ਼ੂਟਰ ਦੇ ਹਮਲੇ ਵਾਲੀ ਘਟਨਾ ਦੀ ਸਥਿਤੀ ਵਿੱਚ, ਆਪਣੇ ਸੰਗਠਨ ਦੀਆਂ ਸੁਰੱਖਿਆ ਨੀਤੀਆਂ ਦੇ ਅਨੁਸਾਰ ਕਿਸੇ ਅਭਿਆਸ ਕੀਤੀ ਗਈ ਜਵਾਬੀ ਰਣਨੀਤੀ—ਜਿਵੇਂ ਕਿ ਦੌੜੋ, ਲੁਕ ਜਾਓ, ਲੜੋ ਪ੍ਰਕਿਰਿਆ—ਲਾਗੂ ਕਰਨ ਬਾਰੇ ਵਿਚਾਰ ਕਰੋ। ਵਾਧੂ ਜਾਣਕਾਰੀ ਅਤੇ ਸਰੋਤ ਕਿਰਿਆਸ਼ੀਲ ਸ਼ੂਟਰ ਲਈ ਤਿਆਰੀ ਬਾਰੇ CISA ਦੇ ਹੋਮਪੇਜ 'ਤੇ ਮਿਲ ਸਕਦੇ ਹਨ।

ਅੱਗ ਨੂੰ ਹਥਿਆਰ ਵਜੋਂ ਵਰਤਣਾ

ਅੱਗਜ਼ਨੀ ਦੀ ਪਰਿਭਾਸ਼ਾ ਹੈ ਕਿਸੇ ਰਿਹਾਇਸ਼ੀ ਘਰ, ਜਨਤਕ ਇਮਾਰਤ, ਮੋਟਰ ਵਾਹਨ, ਹਵਾਈ ਜਹਾਜ਼ ਜਾਂ ਹੋਰ ਨਿੱਜੀ ਜਾਇਦਾਦ ਨੂੰ—ਧੋਖਾਧੜੀ ਦੇ ਇਰਾਦੇ ਨਾਲ ਜਾਂ ਬਿਨਾਂ—ਜਾਣ-ਬੁਝ ਕੇ ਜਾਂ ਮੰਦਭਾਵਨਾ ਨਾਲ ਸਾੜਨ ਜਾਂ ਸਾੜਨ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰਨੀ।[4] ਅੱਗ ਲਗਾਉਣ ਵਾਲੇ ਦੀ ਪ੍ਰੇਰਣਾ ਵਿੱਚ ਹੋਰ ਗੱਲਾਂ ਸਮੇਤ, ਬਦਲਾ, ਮਾਰ-ਧਾੜ, ਧੋਖਾਧੜੀ ਜਾਂ ਅਪਰਾਧ ਨੂੰ ਛੁਪਾਉਣਾ, ਸ਼ਾਮਲ ਹੋ ਸਕਦੇ ਹਨ। ਅੱਗ ਸ਼ੁਰੂ ਕਰਨ ਲਈ ਅੱਗ ਵਧਾਉਣ ਵਾਲੇ ਪਦਾਰਥ ਅਤੇ ਲਾਟਾਂ ਜਾਂ ਕਿਸੇ ਕਿਸਮ ਦੇ ਸੁਧਾਰੇ ਗਏ ਅੱਗ ਲਗਾਉਣ ਵਾਲੇ ਡਿਵਾਈਸ (IID) ਦੀ ਵਰਤੋਂ ਕੀਤੀ ਜਾ ਸਕਦੀ ਹੈ।

ਜਦੋਂ ਤੱਕ ਹਮਲਾ ਸ਼ੁਰੂ ਨਹੀਂ ਹੋ ਜਾਂਦਾ, ਹਥਿਆਰ ਵਜੋਂ ਅੱਗ ਦੇ ਖ਼ਤਰੇ ਦਾ ਪਤਾ ਲਗਾਉਣਾ ਮੁਸ਼ਕਲ ਹੋ ਸਕਦਾ ਹੈ। ਜੇ ਤੁਹਾਨੂੰ ਧੁੰਏਂ ਦੀ ਗੰਧ ਆਉਂਦੀ ਹੈ ਜਾਂ ਕੋਈ ਚੀਜ਼ ਸੜਦੀ ਹੋਈ ਦਿਖਾਈ ਦਿੰਦੀ ਹੈ, ਤਾਂ ਤੁਹਾਨੂੰ ਇਹ ਸਮਝਣ ਦੀ ਲੋੜ ਹੁੰਦੀ ਹੈ ਕਿ ਤੁਸੀਂ ਕਿਹੜੇ ਕਦਮ ਚੁੱਕਣੇ ਹਨ।

3 Federal Bureau of Investigation, n.d. Active Shooter Safety Resources. 1 ਦਸੰਬਰ 2023 ਨੂੰ ਪਹੁੰਚ ਕੀਤੀ ਗਈ, fbi.gov/how-we-can-help-you/active-shooter-safety-resources.

4 Cybersecurity and Infrastructure Security Agency. 2021. Fire as a Weapon Action Guide. ਅਗਸਤ 8, 2023 ਨੂੰ ਪਹੁੰਚ ਕੀਤੀ ਗਈ। cisa.gov/resources-tools/resources/fire-weapon-action-guide.

ਅੱਗ ਦੇ ਹਮਲੇ ਦੀ ਸਥਿਤੀ ਵਿੱਚ, 9-1-1 ਨੂੰ ਕਾੱਲ ਕਰੋ ਅਤੇ ਐਮਰਜੈਂਸੀ ਕਰਮਚਾਰੀਆਂ ਦੀਆਂ ਹਿਦਾਇਤਾਂ ਦੀ ਪਾਲਣਾ ਕਰੋ। ਅੱਗ ਦੀ ਗਤੀਵਿਧੀ ਵਾਲੇ ਖੇਤਰ ਤੋਂ ਤੁਰੰਤ ਚਲੇ ਜਾਓ ਅਤੇ ਜੇ ਸੰਭਵ ਹੋਵੇ ਤਾਂ ਦੂਜਿਆਂ ਨੂੰ ਸੁਚੇਤ ਕਰੋ। ਅਜਿਹੇ ਖੇਤਰਾਂ ਤੋਂ ਬਚੋ ਜਿੱਥੇ ਤੁਹਾਨੂੰ ਧੁੰਏਂ ਦੀ ਗੰਧ ਆਉਂਦੀ ਹੈ ਜਾਂ ਅੱਗ ਦਿਖਾਈ ਦਿੰਦੀ ਹੈ। ਅੰਦਰੂਨੀ ਇਮਾਰਤਾਂ ਨੂੰ ਖਾਲੀ ਕਰੋ; ਅੱਗ ਨੂੰ ਕਾਬੂ ਕਰਨ ਲਈ ਆਪਣੇ ਪਿੱਛੇ ਸਾਰੇ ਦਰਵਾਜ਼ੇ ਬੰਦ ਕਰ ਦਿਓ। ਜੇ ਤੁਸੀਂ ਬਾਹਰ ਨਹੀਂ ਨਿਕਲ ਸਕਦੇ ਹੋ, ਤਾਂ ਖ਼ਤਰੇ ਤੋਂ ਜਿੰਨਾ ਸੰਭਵ ਹੋ ਸਕੇ ਦੂਰ ਚਲੇ ਜਾਓ ਅਤੇ ਲੋੜ ਅਨੁਸਾਰ ਅੱਗ ਬੁਝਾਉਣ ਵਾਲੇ ਯੰਤਰਾਂ ਦੀ ਵਰਤੋਂ ਕਰੋ। ਸਥਿਤੀ ਸੰਬੰਧੀ ਜਾਗਰੂਕਤਾ ਬਣਾਈ ਰੱਖੋ ਅਤੇ ਸ਼ੱਕੀ ਗਤੀਵਿਧੀ ਜਾਂ ਵਾਧੂ ਖ਼ਤਰਿਆਂ 'ਤੇ ਨਜ਼ਰ ਰੱਖੋ।

ਅੱਗ ਨੂੰ ਹਥਿਆਰ ਵਜੋਂ ਵਰਤੇ ਜਾਣ ਦੀਆਂ ਘਟਨਾਵਾਂ ਨੂੰ ਘਟਾਉਣ ਬਾਰੇ ਹੋਰ ਸੁਝਾਵਾਂ ਲਈ CISA ਦੀ ਅੱਗ ਨੂੰ ਹਥਿਆਰ ਵਜੋਂ ਵਰਤਣਾ ਸੰਬੰਧੀ ਕਾਰਵਾਈ ਗਾਈਡ 'ਤੇ ਜਾਓ।

ਸੋਧੇ ਗਏ ਵਿਸਫੋਟਕ ਡਿਵਾਈਸ (IED)

IED ਅਜਿਹਾ ਡਿਵਾਈਸ ਹੁੰਦਾ ਹੈ ਜਿਸ ਨੂੰ ਵਿਨਾਸ਼ਕਾਰੀ, ਘਾਤਕ, ਹਾਨੀਕਾਰਕ, ਆਤਿਸ਼ਬਾਜੀ ਜਾਂ ਅੱਗ ਲਗਾਉਣ ਵਾਲੇ ਰਸਾਇਣਾਂ ਨੂੰ ਸ਼ਾਮਲ ਕਰਦੇ ਹੋਏ ਸੋਧੇ ਗਏ ਢੰਗ ਨਾਲ ਰੱਖਿਆ ਜਾਂ ਬਣਾਇਆ ਜਾਂਦਾ ਹੈ ਅਤੇ ਤਬਾਹ ਕਰਨ, ਅਸਮਰਥ ਬਣਾਉਣ, ਪਰੇਸ਼ਾਨ ਕਰਨ ਜਾਂ ਧਿਆਨ ਭਟਕਾਉਣ ਲਈ ਤਿਆਰ ਕੀਤਾ ਜਾਂਦਾ ਹੈ।[5] ਬੰਬ ਬਣਾਉਣ ਵਾਲੇ ਲਈ ਉਪਲਬਧ ਟੀਚਿਆਂ ਅਤੇ ਸਮੱਗਰੀਆਂ ਦੇ ਆਧਾਰ 'ਤੇ, IEDs ਵਿੱਚ ਛੋਟੇ, ਖਰ੍ਹਵੇਂ ਡਿਵਾਈਸਾਂ, ਜਿਵੇਂ ਕਿ ਓਵਰਪ੍ਰੈਸ਼ਰ ਡਿਵਾਈਸ ਜਾਂ ਪਾਈਪ ਬੰਬ ਜੋ ਅਕਸਰ ਵਿਸਫੋਟਕ ਪਾਊਡਰਾਂ ਨਾਲ ਭਰੇ ਹੁੰਦੇ ਹਨ, ਤੋਂ ਲੈ ਕੇ ਵੱਡੀ ਮਾਤਰਾ ਵਿੱਚ ਵਿਸਫੋਟਕਾਂ ਵਾਲੇ ਵਾਹਨ ਡਿਵਾਈਸਾਂ ਤੱਕ ਸ਼ਾਮਲ ਹੁੰਦੇ ਹਨ।

ਖ਼ਤਰੇ ਵੱਖ-ਵੱਖ ਰੂਪ ਲੈ ਸਕਦੇ ਹਨ। ਜੇ ਤੁਸੀਂ ਕਦੇ ਵੀ ਕਿਸੇ ਸਥਿਤੀ ਜਾਂ ਸ਼ੱਕੀ ਵਸਤੂ ਬਾਰੇ ਚਿੰਤਤ ਹੋਵੋ, ਤਾਂ ਤੁਰੰਤ ਆਪਣੇ ਸਥਾਨਕ ਕਾਨੂੰਨ ਲਾਗੂਕਰਨ ਵਾਲਿਆਂ ਨੂੰ ਕਾੱਲ ਕਰੋ। ਬੰਬ ਦਾ ਸੰਕੇਤ ਦੇਣ ਵਾਲੀਆਂ ਉਦਾਹਰਨਾਂ ਵਿੱਚ ਅਸਪਸ਼ਟ ਤਾਰਾਂ ਜਾਂ ਇਲੈਕਟ੍ਰਾਨਿਕਸ, ਹੋਰ ਦਿਖਾਈ ਦਿੰਦੇ ਬੰਬ ਵਰਗੇ ਹਿੱਸੇ, ਅਤੇ ਅਸਧਾਰਨ ਆਵਾਜ਼ਾਂ, ਭਾਫ਼, ਧੁੰਦ ਜਾਂ ਗੰਧ ਸ਼ਾਮਲ ਹਨ। ਸੋਧੇ ਗਏ ਵਿਸਫੋਟਕ ਡਿਵਾਈਸ ਵਾਲੀਆਂ ਅਜਿਹੀਆਂ ਘਟਨਾਵਾਂ ਲਈ, ਜਿਨ੍ਹਾਂ ਵਿੱਚ ਕੋਈ ਸ਼ੱਕੀ ਡਿਵਾਈਸ ਸ਼ਾਮਲ ਹੁੰਦਾ ਹੈ, ਬੰਬ ਦਸਤੇ ਦੁਆਰਾ ਪ੍ਰਤਿਕਿਰਿਆ ਕੀਤੇ ਜਾਣ ਅਤੇ ਵਿਸਫੋਟਕ ਡਿਵਾਈਸਾਂ ਦਾ ਪਤਾ ਲਗਾਉਣ ਅਤੇ ਉਨ੍ਹਾਂ ਨੂੰ "ਸੁਰੱਖਿਅਤ" ਕਰਨ ਦੀ ਸਮਰੱਥਾ ਦੀ ਲੋੜ ਹੁੰਦੀ ਹੈ।

ਸ਼ੱਕੀ ਵਸਤੂਆਂ ਦੀ ਪਛਾਣ ਕਰਨ ਬਾਰੇ ਵਧੇਰੇ ਜਾਣਕਾਰੀ ਲਈ, ਅਣਪਛਾਤੀ ਚੀਜ਼ ਬਨਾਮ ਸ਼ੱਕੀ ਚੀਜ਼ ਲਈ ਪੋਸਟਕਾਰਡ ਅਤੇ ਪੋਸਟਰ ਦਾ ਹਵਾਲਾ ਲਵੋ ਅਤੇ ਵੀਡੀਓ “ਕੀ ਕੀਤਾ ਜਾਏ: ਸ਼ੱਕੀ ਜਾਂ ਅਣਪਛਾਤੀ ਚੀਜ਼” ਦੇਖੋ।

ਵਿਰੋਧ ਅਤੇ ਪ੍ਰਦਰਸ਼ਨ

ਜੇ ਤੁਹਾਡੇ ਘਰ, ਕਾਰੋਬਾਰ ਦੇ ਸਥਾਨ ਜਾਂ ਇੱਥੋਂ ਤੱਕ ਕਿ ਤੁਹਾਡੀ ਪ੍ਰਾਪਰਟੀ 'ਤੇ ਕੋਈ ਜਨਤਕ ਵਿਰੋਧ ਜਾਂ ਪ੍ਰਦਰਸ਼ਨ ਹੁੰਦਾ ਹੈ, ਤਾਂ ਮਿਸ਼ਨ ਜਾਂ ਇਰਾਦੇ ਦੀ ਪਰਵਾਹ ਕੀਤੇ ਬਿਨਾਂ, ਸ਼ਾਂਤ ਰਹੋ। ਵਿਰੋਧ-ਪ੍ਰਦਰਸ਼ਨ ਡਰਾਉਣੇ ਲੱਗ ਸਕਦੇ ਹਨ ਪਰ ਇਨ੍ਹਾਂ ਤੋਂ ਕੋਈ ਸਰੀਰਕ ਖ਼ਤਰਾ ਪੈਦਾ ਹੋਣ ਦੀ ਸੰਭਾਵਨਾ ਨਹੀਂ ਹੁੰਦੀ। ਭਾਵੇਂ ਸਥਿਤੀ ਅਸਥਿਰ ਹੋ ਜਾਵੇ, ਸ਼ਾਂਤ ਰਹੋ। ਅੰਦਰ ਰਹੋ, ਆਪਣੇ ਦਰਵਾਜ਼ੇ ਅਤੇ ਖਿੜਕੀਆਂ ਨੂੰ ਬੰਦ ਕਰਕੇ ਤਾਲਾਬੰਦ ਕਰੋ, ਅਤੇ ਆਪਣੇ ਪਰਦੇ/ਬਲਾਇੰਡ ਲਗਾ ਦਿਓ। ਜੇ ਤੁਸੀਂ ਅਸੁਰੱਖਿਅਤ ਮਹਿਸੂਸ ਕਰਦੇ ਹੋ ਜਾਂ ਸਥਿਤੀ ਵੱਧ ਜਾਂਦੀ ਹੈ, ਤਾਂ ਆਪਣੇ ਸਥਾਨਕ ਕਾਨੂੰਨ ਲਾਗੂਕਰਨ ਵਾਲਿਆਂ ਨੂੰ ਕਾੱਲ ਕਰੋ।

ਜੇ ਜ਼ਰੂਰੀ ਹੋਵੇ, ਮੌਜੂਦ ਵਿਅਕਤੀਆਂ ਅਤੇ ਵਾਹਨਾਂ ਦੇ ਵੇਰਵੇ ਨੋਟ ਕਰੋ। ਪੁਲਿਸ ਨੂੰ ਕੋਈ ਵੀ ਵੀਡੀਓ ਨਿਗਰਾਨੀ ਫੁਟੇਜ, ਸੈਲ ਫ਼ੋਨ ਵੀਡੀਓ ਜਾਂ ਫੋਟੋਆਂ ਪ੍ਰਦਾਨ ਕਰੋ, ਕਿਉਂਕਿ ਇਸ ਨਾਲ ਜਾਂਚ ਹੋਣ ਦੀ ਸਥਿਤੀ ਵਿੱਚ ਮਦਦ ਮਿਲ ਸਕਦੀ ਹੈ।

CISA ਦੀ ਜਨਤਕ ਪ੍ਰਦਰਸ਼ਨਾਂ ਦੌਰਾਨ ਬੁਨਿਆਦੀ ਢਾਂਚੇ ਦੀ ਰੱਖਿਆ ਕਰਨਾ ਤੱਥ ਸ਼ੀਟ ਅਜਿਹੇ ਕਾਰੋਬਾਰਾਂ ਲਈ ਸੁਰੱਖਿਆ ਸਿਫ਼ਾਰਿਸ਼ਾਂ ਦੀ ਪੇਸ਼ਕਸ਼ ਕਰਦੀ ਹੈ ਜੋ ਜਨਤਕ ਪ੍ਰਦਰਸ਼ਨਾਂ ਦੌਰਾਨ ਗੈਰ-ਕਾਨੂੰਨੀ ਕਾਰਵਾਈਆਂ ਦਾ ਨਿਸ਼ਾਨਾ ਬਣ ਸਕਦੇ ਹਨ।

ਸਥਿਤੀ ਸੰਬੰਧੀ ਜਾਗਰੂਕਤਾ

ਸਥਿਤੀ ਸੰਬੰਧੀ ਜਾਗਰੂਕਤਾ ਦਾ ਮਤਲਬ ਹੈ ਤੁਹਾਡੇ ਆਲੇ ਦੁਆਲੇ ਕੀ ਹੋ ਰਿਹਾ ਹੈ ਉਸ ਬਾਰੇ ਜਾਗਰੂਕ ਬਣਨਾ, ਹਰ ਚੀਜ਼ ਨੂੰ ਧਿਆਨ ਵਿੱਚ ਰੱਖਣਾ ਅਤੇ ਤੁਹਾਨੂੰ, ਤੁਹਾਡੇ ਪਰਿਵਾਰ ਜਾਂ ਤੁਹਾਡੇ ਸਹਿਕਰਮੀਆਂ ਨੂੰ ਸੱਟ ਲੱਗਣ ਦੇ ਜੋਖਮ ਨੂੰ ਘਟਾਉਣ ਲਈ ਆਪਣੇ ਵਿਹਾਰ ਨੂੰ ਅਨੁਕੂਲ ਬਣਾਉਣਾ।

ਮੁਲਾਕਾਤੀ

ਮੁਲਾਕਾਤੀਆਂ ਨੂੰ ਆਪਣੇ ਘਰ ਦੇ ਅੰਦਰ ਆਉਣ ਦੇਣ ਤੋਂ ਪਹਿਲਾਂ ਹਮੇਸ਼ਾਂ ਉਨ੍ਹਾਂ ਦੀ ਪਛਾਣ ਕਰੋ। ਦਰਵਾਜ਼ੇ ਦੇ ਦੂਜੇ ਪਾਸੇ ਕੌਣ ਹੈ, ਇਸਦੀ ਪਛਾਣ ਕਰਨ ਵਿੱਚ ਤੁਹਾਡੀ ਮਦਦ ਕਰਨ ਲਈ ਬੰਦ ਦਰਵਾਜ਼ੇ ਵਿੱਚੋਂ ਦੇਖਣ ਵਾਲੀ ਮੋਰੀ (ਪੀਪਹੋਲ) ਜਾਂ ਦਰਵਾਜ਼ੇ ਦਾ ਕੈਮਰਾ ਲਗਾਉਣ ਕਰਨ ਬਾਰੇ ਵਿਚਾਰ ਕਰੋ। ਆਪਣਾ ਦਰਵਾਜ਼ਾ ਖੋਲ੍ਹਣ ਤੋਂ ਪਹਿਲਾਂ ਅਣਜਾਣ ਮੁਲਾਕਾਤੀਆਂ ਨੂੰ ਆਪਣੀ ਪਛਾਣ ਦੱਸਣ ਲਈ ਕਹੋ। ਇੱਕ ਵਾਰ ਤੁਹਾਡੇ ਨਿਵਾਸ ਦੇ ਅੰਦਰ ਆਉਣ 'ਤੇ, ਉਨ੍ਹਾਂ ਨੂੰ ਆਪਣੇ ਨਜ਼ਦੀਕ ਰੱਖੋ, ਤਰਜੀਹੀ ਤੌਰ 'ਤੇ ਤੁਹਾਡੇ ਸਾਹਮਣੇ ਜਾਂ ਅਜਿਹੀ ਸਥਿਤੀ ਵਿੱਚ ਜਿੱਥੇ ਉਨ੍ਹਾਂ 'ਤੇ ਨਜ਼ਰ ਰੱਖੀ ਜਾ ਸਕਦੀ ਹੈ। ਹਰ ਸਮੇਂ ਆਪਣੇ ਕੋਲ ਮੋਬਾਈਲ ਫ਼ੋਨ ਰੱਖਣ ਬਾਰੇ ਸੋਚੋ।

ਸੰਵੇਦਨਸ਼ੀਲ ਸਮੱਗਰੀ

ਗੁਪਤ ਸਮੱਗਰੀ ਦਾ ਹਮੇਸ਼ਾ ਸਹੀ ਢੰਗ ਨਾਲ ਨਿਪਟਾਰਾ ਕਰੋ ਜਾਂ ਉਸ ਨੂੰ ਨਸ਼ਟ ਕਰੋ ਜਿਸ ਵਿੱਚ ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਂ ਨਿੱਜੀ ਤੌਰ 'ਤੇ ਪਛਾਣਯੋਗ ਜਾਣਕਾਰੀ (PII) ਹੋ ਸਕਦੀ ਹੈ। PII ਵਿੱਚ ਅਜਿਹੀ ਕੋਈ ਵੀ ਜਾਣਕਾਰੀ ਸ਼ਾਮਲ ਹੁੰਦੀ ਹੈ ਜੋ ਵਿਅਕਤੀਗਤ ਪ੍ਰਕਿਰਤੀ ਦੀ ਹੁੰਦੀ ਹੈ ਅਤੇ ਜਿਸ ਨੂੰ ਤੁਹਾਡੀ ਪਛਾਣ ਕਰਨ ਲਈ ਵਰਤਿਆ ਜਾ ਸਕਦਾ ਹੈ।

ਪੈਦਲ ਚਲਣ ਵਾਲਿਆਂ ਦੀ ਸੁਰੱਖਿਆ

ਜਨਤਕ ਥਾਵਾਂ 'ਤੇ ਯਾਤਰਾ ਕਰਨ, ਸੈਰ ਕਰਨ ਜਾਂ ਜੌਗਿੰਗ ਕਰਨ ਵੇਲੇ ਆਪਣੀ ਨਿੱਜੀ ਸੁਰੱਖਿਆ ਨੂੰ ਤਰਜੀਹ ਦਿਓ। ਢੁਕਵੀਆਂ ਸਾਵਧਾਨੀਆਂ ਵਰਤਣ ਨਾਲ ਤੁਹਾਨੂੰ ਅਸੁਰੱਖਿਅਤ ਸਥਿਤੀਆਂ ਅਤੇ ਹਿੰਸਾ ਜਾਂ ਹਮਲਾਵਰਤਾ ਦਾ ਸਾਹਮਣਾ ਕਰਨ ਦੇ ਜੋਖਮ ਨੂੰ ਘਟਾਉਣ ਵਿੱਚ ਮਦਦ ਮਿਲ ਸਕਦੀ ਹੈ। ਸਾਧਾਰਨ ਉਪਾਵਾਂ 'ਤੇ ਵਿਚਾਰ ਕਰੋ ਜਿਵੇਂ ਕਿ ਪਹਿਲਾਂ ਹੀ ਸੁਰੱਖਿਅਤ ਰੂਟ ਦੀ ਯੋਜਨਾ ਬਣਾਉਣੀ, ਨਿਯਮਿਤ ਥਾਵਾਂ 'ਤੇ ਜਾਣ ਵੇਲੇ ਆਪਣਾ ਰਸਤਾ ਬਦਲਣਾ, ਅਤੇ ਸੰਭਾਵੀ ਖ਼ਤਰੇ ਵਾਲੇ ਬਿੰਦੂਆਂ, ਜਿਵੇਂ ਕਿ ਸ਼ਾਂਤ ਜਾਂ ਮਾੜੀ ਰੋਸ਼ਨੀ ਵਾਲੀਆਂ ਗਲੀਆਂ, ਉਜਾੜ ਪਾਰਕਿੰਗ ਗੈਰੇਜ ਅਤੇ ਰਿਮੋਟ ਪਾਰਕਿੰਗ ਸਥਾਨਾਂ ਤੋਂ ਬਚਣਾ।

5 U.S. Department of Homeland Security. Federal Bureau of Investigation. n.d. *Security and Resiliency Guide: Counter-Improvised Explosive Device (C-IED) Concepts, Common Goals, and Available Assistance*. 8 ਅਗਸਤ, 2023 ਨੂੰ ਪਹੁੰਚ ਕੀਤੀ ਗਈ। ਪੰਨਾ 4. cisa.gov/resources-tools/resources/security-and-resiliency-guide-srg-and-annexes.

ਜਦੋਂ ਵੀ ਤੁਸੀਂ ਜਨਤਕ ਸਥਾਨ 'ਤੇ ਹੋਵੋ, ਵਿਵੇਕ ਦੀ ਵਰਤੋਂ ਕਰੋ ਅਤੇ ਸਾਵਧਾਨੀਆਂ ਵਰਤ ਕੇ ਕੋਈ ਵੀ ਕੰਮ ਸੰਬੰਧੀ ਵੇਰਵਿਆਂ ਜਾਂ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਨੂੰ ਲੁਕੋ ਦਿਓ। ਜਨਤਕ ਥਾਵਾਂ 'ਤੇ ਬੈਜ ਪਹਿਨਣ ਜਾਂ ਪਾਸਵਰਡ ਦਾਖਲ ਕਰਨ ਵੇਲੇ ਧਿਆਨ ਰੱਖੋ। ਹੋਰ ਤੱਥਾਂ ਅਤੇ ਸੁਝਾਵਾਂ ਲਈ, ਨੈਸ਼ਨਲ ਹਾਈਵੇਅ ਟ੍ਰੈਫ਼ਿਕ ਸੇਫਟੀ ਪ੍ਰਸ਼ਾਸਨ ਦੀ ਪੈਦਲ ਤੁਰਨ ਵਾਲਿਆਂ ਦੀ ਸੁਰੱਖਿਆ ਬਾਰੇ ਵੈੱਬਸਾਈਟ 'ਤੇ ਜਾਓ।

ਸਥਿਤੀ ਸੰਬੰਧੀ ਜਾਗਰੂਕਤਾ ਬਣਾਈ ਰੱਖੋ

ਜੇ ਤੁਸੀਂ ਕਿਸੇ ਜਨਤਕ ਖੇਤਰ/ਮਾਹੌਲ ਵਿੱਚ ਹੁੰਦੇ ਹੋਏ ਚਿੰਤਤ ਹੋ ਜਾਂਦੇ ਹੋ ਜਾਂ ਅਸੁਰੱਖਿਅਤ ਮਹਿਸੂਸ ਕਰਨਾ ਸ਼ੁਰੂ ਕਰਦੇ ਹੋ, ਤਾਂ ਲੋਕਾਂ ਦੇ ਸਮੂਹ ਦੇ ਨੇੜੇ ਚਲੇ ਜਾਓ। ਜੇ ਇਹ ਸੰਭਵ ਨਹੀਂ ਹੈ, ਤਾਂ ਆਪਣੀਆਂ ਹਰਕਤਾਂ ਨੂੰ ਵਿਵਸਥਿਤ ਕਰੋ ਜਿਸ ਨਾਲ ਤੁਸੀਂ ਆਪਣੀ ਸਥਿਤੀ ਸੰਬੰਧੀ ਜਾਗਰੂਕਤਾ ਨੂੰ ਵੱਧ ਤੋਂ ਵੱਧ ਕਰ ਸਕੋ ਅਤੇ ਹੇਠਾਂ ਦਿੱਤੀਆਂ ਸਾਵਧਾਨੀਆਂ ਵਰਤੋ:

- **ਆਪਣੇ ਮੋਬਾਈਲ ਫ਼ੋਨ** ਨੂੰ ਅਜਿਹੀ ਸਥਿਤੀ ਵਿੱਚ ਰੱਖੋ ਕਿ ਐਮਰਜੈਂਸੀ ਕਾੱਲ ਕੀਤੀ ਜਾ ਸਕੇ।
- **ਸੁਚੇਤ ਰਹੋ** ਅਤੇ ਆਪਣੇ ਸਟੀਕ ਸਥਾਨ ਅਤੇ ਆਲੇ-ਦੁਆਲੇ ਬਾਰੇ ਜਾਗਰੂਕ ਰਹੋ।
- **ਕਿਸੇ ਵੀ** ਗਹਿਣੇ ਜਾਂ ਕੀਮਤੀ ਚੀਜ਼ਾਂ **ਨੂੰ ਦਿਖਾਉਣ ਤੋਂ ਬਚੋ**।
- **ਖੇਤਰ ਦੀ ਰੋਸ਼ਨੀ, ਟਿਕਾਣੇ ਅਤੇ** ਹੋਰ ਸਥਾਨਕ ਕਾਰੋਬਾਰਾਂ **ਤੋਂ ਨੇੜਤਾ ਬਾਰੇ ਵਿਚਾਰ ਕਰੋ**।
- ਪਿੱਛੋਂ ਆਉਣ ਵਾਲੇ ਵਾਹਨਾਂ ਤੋਂ ਬਚਣ ਲਈ **ਪੈਦਲ ਤੁਰਦੇ ਸਮੇਂ ਟ੍ਰੈਫ਼ਿਕ ਤੋਂ ਉਲਟੀ ਦਿਸ਼ਾ ਵਿੱਚ ਤੁਰੋ**।
- **ਆਪਣੇ ਹੱਥਾਂ ਨੂੰ ਖਾਲੀ ਰੱਖੋ** ਅਤੇ ਆਪਣੇ ਆਲੇ-ਦੁਆਲੇ ਤੋਂ ਸੁਚੇਤ ਰਹੋ।
- **ਫ਼ੋਨ 'ਤੇ ਗੱਲ ਕਰਨ**, ਹੈੱਡਫ਼ੋਨ ਪਹਿਨਣ ਜਾਂ ਲੰਬੇ ਟੈਕਸਟ ਮੈਸੇਜ ਭੇਜਣ ਤੋਂ ਬਚੋ।
- **ਪੈਦਲ ਤੁਰਨ ਵੇਲੇ** ਸੁਚੇਤ ਰਹੋ ਅਤੇ ਕਿਸੇ ਸਥਾਨ 'ਤੇ ਜ਼ਿਆਦਾ ਟਹਿਲਣ ਤੋਂ ਬਚੋ।
- **ਬੈਂਕਿੰਗ ATM ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਸਮੇਂ**, ਜਨਤਕ ਸਥਾਨ 'ਤੇ ਨੋਟ ਦਿਖਾਉਣ ਤੋਂ ਬਚੋ।

ਰਾਈਡਸ਼ੇਅਰ ਸੇਵਾਵਾਂ

ਰਾਈਡਸ਼ੇਅਰ ਐਪਲੀਕੇਸ਼ਨ ਦੀ ਵਰਤੋਂ ਕਰਦੇ ਸਮੇਂ, ਆਪਣੇ ਸਥਾਨ ਅਤੇ ਮੰਜ਼ਿਲ ਦੇ ਵੇਰਵਿਆਂ ਬਾਰੇ ਕਿਸੇ ਦੋਸਤ ਜਾਂ ਸਹਿਕਰਮੀ ਨੂੰ ਸੂਚਿਤ ਕਰਨ ਬਾਰੇ ਵਿਚਾਰ ਕਰੋ। ਰਾਈਡ ਨੂੰ ਸਵੀਕਾਰ ਕਰਨ ਅਤੇ ਵਾਹਨ ਵਿੱਚ ਦਾਖਲ ਹੋਣ ਤੋਂ ਪਹਿਲਾਂ ਡ੍ਰਾਈਵਰ ਅਤੇ ਵਾਹਨ ਦੇ ਵੇਰਵਿਆਂ ਦੀ ਜਾਂਚ ਕਰੋ।

ਸ਼ੱਕੀ ਗਤੀਵਿਧੀ ਨੂੰ ਪਛਾਣੋ ਅਤੇ ਇਸਦੀ ਰਿਪੋਰਟ ਕਰੋ

ਸ਼ੱਕੀ ਗਤੀਵਿਧੀ ਨੂੰ ਪਛਾਣੋ ਅਤੇ ਇਸਦੀ ਰਿਪੋਰਟ ਕਰੋ - ਜਿਵੇਂ ਕਿ ਤੁਹਾਡੇ ਘਰ, ਕਾਰਜ-ਸਥਾਨ ਜਾਂ ਵਾਹਨ ਦੇ ਆਲੇ-ਦੁਆਲੇ ਕਿਸੇ ਖਾਸ ਕਾਰਨ ਤੋਂ ਬਿਨਾਂ ਘੁੰਮ ਰਹੇ ਲੋਕ, ਜਾਂ ਲੁਕਵੇਂ ਢੰਗ ਨਾਲ ਤੁਹਾਡੀਆਂ ਤਸਵੀਰਾਂ ਖਿੱਚਣ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰ ਰਹੇ ਲੋਕ। ਜੇ ਤੁਸੀਂ ਦੇਖਦੇ ਹੋ ਕਿ ਕੋਈ ਵਿਅਕਤੀ ਤੁਹਾਡੇ ਘਰ, ਕਾਰਜ-ਸਥਾਨ ਜਾਂ ਵਾਹਨ ਦੇ ਨੇੜੇ ਕੋਈ ਵਸਤੂ ਜਾਂ ਪੈਕੇਜ ਛੱਡਦਾ ਹੈ, ਤਾਂ ਇਸਦੀ ਫੌਰਨ ਪੁਲਿਸ ਨੂੰ ਰਿਪੋਰਟ ਕਰੋ। "ਜੇ ਤੁਸੀਂ ਕੁਝ ਦੇਖਦੇ ਹੋ, ਤਾਂ ਕੁਝ ਕਹੋ®" ਮੁਹਿੰਮ 'ਤੇ ਜਾ ਕੇ ਸ਼ੱਕੀ ਗਤੀਵਿਧੀ ਦੀ ਰਿਪੋਰਟ ਕਰਨ ਬਾਰੇ ਹੋਰ ਜ਼ਿਆਦਾ ਜਾਣੋ।

ਨਿੱਜੀ ਸੁਰੱਖਿਆ ਡਿਵਾਈਸ

ਹਮਲਾਵਰ ਨੂੰ ਭਟਕਾਉਣ, ਕੋਲ ਖੜ੍ਹੇ ਲੋਕਾਂ ਨੂੰ ਸੂਚਿਤ ਕਰਨ ਅਤੇ ਖੁਦ ਨੂੰ ਬਚ ਕੇ ਨਿਕਲਣ ਦਾ ਮੌਕਾ ਦੇਣ ਲਈ ਪੈਪਰ ਸਪ੍ਰੇਅ (ਮਿਰਚ ਸਪ੍ਰੇਅ), ਸੁਣਾਈ ਦੇਣ ਵਾਲਾ ਅਲਾਰਮ, ਜਾਂ ਵਧੀਕ ਨਿੱਜੀ ਸੁਰੱਖਿਆ ਡਿਵਾਈਸ ਆਪਣੇ ਨਾਲ ਰੱਖਣ ਬਾਰੇ ਵਿਚਾਰ ਕਰੋ। ਜਿੱਥੇ ਹੋ ਸਕੇ, ਅਤੇ ਸੰਘੀ ਅਤੇ ਸਥਾਨਕ ਕਾਨੂੰਨਾਂ ਅਤੇ ਨਿਯਮਾਂ ਦੇ ਅਨੁਸਾਰ, ਨਿੱਜੀ ਸੁਰੱਖਿਆ ਡਿਵਾਈਸਾਂ ਨੂੰ ਆਪਣੇ ਨਾਲ ਰੱਖੋ ਅਤੇ ਇਨ੍ਹਾਂ ਦੀ ਵਰਤੋਂ ਕਰੋ।

ਹੇਠਾਂ ਦਿੱਤੇ ਚੇਤਾਵਨੀ ਦੇ ਸੰਕੇਤਾਂ ਵੱਲ ਸਾਵਧਾਨੀ ਨਾਲ ਧਿਆਨ ਦੇਣ ਅਤੇ ਇਨ੍ਹਾਂ ਦੀ ਫੌਰਨ ਰਿਪੋਰਟ ਕਰਨ ਨਾਲ ਕਿਸੇ ਸੰਭਾਵੀ ਘਟਨਾ ਨੂੰ ਘਟਾਉਣ ਵਿੱਚ ਮਦਦ ਮਿਲ ਸਕਦੀ ਹੈ:

- **ਤੁਹਾਡੇ, ਤੁਹਾਡੇ ਘਰ**, ਸੰਪੱਤੀ ਜਾਂ ਰੁਜ਼ਗਾਰ ਦੇ ਸਥਾਨ ਵਿਰੁੱਧ ਜ਼ੁਬਾਨੀ ਜਾਂ ਲਿਖਤੀ ਧਮਕੀ।
- **ਨੁਕਸਾਨ ਪਹੁੰਚਾਏ ਗਏ** ਜਾਂ ਛੇੜਛਾੜ ਕੀਤੇ ਸਿਸਟਮ ਅਤੇ ਉਪਕਰਨ।
- **ਸ਼ੱਕੀ ਜਾਂ ਲਾਵਾਰਸ ਪਈਆਂ ਵਸਤੂਆਂ**—ਜਿਨ੍ਹਾਂ ਵਿੱਚ ਬੈਗ, ਬਕਸੇ, ਲੁਕੋਏ ਹੋਏ ਡੱਬੇ ਸ਼ਾਮਲ ਹਨ—ਜਿਨ੍ਹਾਂ ਵਿੱਚ ਖ਼ਤਰਨਾਕ ਪਦਾਰਥ ਹੋ ਸਕਦੇ ਹਨ।
- **ਇਮਾਰਤਾਂ ਦੇ ਫਲੋਰ ਪਲਾਨ**, ਪ੍ਰਵੇਸ਼ ਦੁਆਰ/ਨਿਕਾਸ ਦੇ ਸਥਾਨਾਂ, ਐਲੀਵੇਟਰਾਂ, ਅੱਗ ਬੁਝਾਉਣ ਵਾਲੇ ਯੰਤਰਾਂ, ਪਾਣੀ ਦੀ ਸਪਲਾਈ ਦੇ ਨਾਲ-ਨਾਲ ਹੀਟਿੰਗ, ਹਵਾਦਾਰੀ ਅਤੇ ਏਅਰ ਕੰਡੀਸ਼ਨਿੰਗ (HVAC) ਪ੍ਰਣਾਲੀਆਂ ਬਾਰੇ ਸ਼ੱਕੀ ਪੁੱਛ-ਗਿਛ।
- **ਜਲਦੀ ਅੱਗ ਫੜਨ ਵਾਲੀ ਜਾਂ** ਜਲਣਸ਼ੀਲ ਸਮੱਗਰੀ ਦੀਆਂ ਅਸਧਾਰਨ ਮਾਤਰਾਵਾਂ ਜਾਂ ਸਥਾਨ, ਜਿਨ੍ਹਾਂ ਵਿੱਚ ਅੱਗ ਵਧਾਉਣ ਵਾਲੇ ਪਦਾਰਥ, ਪੇਂਟ, ਡੀਗ੍ਰੀਸਰ, ਅਲਕੋਹਲ-ਆਧਾਰਿਤ ਕਲੀਨਰ, ਐਰੋਸੋਲ ਅਤੇ ਪ੍ਰੋਪੇਨ ਗੈਸ ਦੇ ਟੈਂਕ ਸ਼ਾਮਲ ਹਨ।
- **ਸੋਸ਼ਲ ਮੀਡੀਆ ਮੈਸੇਜ ਜੋ ਹਮਲੇ** ਕਰਨ ਲਈ ਕਿਸੇ ਵੀ ਚਿੱਤਰ ਜਾਂ ਵਿਚਾਰਾਂ ਦਾ ਪ੍ਰਚਾਰ ਕਰਦੇ ਹਨ।

ਹੋਰ ਜਾਣਕਾਰੀ ਲਈ, ਸ਼ੱਕੀ ਗਤੀਵਿਧੀ ਦੀ ਰਿਪੋਰਟ ਕਰਨ ਦੇ ਸੂਚਕ ਅਤੇ ਉਦਾਹਰਨਾਂ ਦੇਖੋ।

ਟਕਰਾਅ

ਆਪਣੇ ਆਪ ਨੂੰ ਟਕਰਾਅ ਵਾਲੀ ਸਥਿਤੀ ਵਿੱਚ ਪਾਉਣਾ ਤਣਾਅਪੂਰਨ ਹੋ ਸਕਦਾ ਹੈ। ਧਿਆਨ ਅਜਿਹੇ ਵਿਵਹਾਰਾਂ 'ਤੇ ਕੇਂਦਰਿਤ ਹੋਣਾ ਚਾਹੀਦਾ ਹੈ ਜੋ ਸੰਭਾਵੀ ਹਿੰਸਾ ਦੇ ਸੰਕੇਤ ਹੋ ਸਕਦੇ ਹਨ। ਇਨ੍ਹਾਂ ਸਥਿਤੀਆਂ ਵਿੱਚ, ਸ਼ਾਂਤ ਰਹਿਣਾ ਅਤੇ ਸਥਿਤੀ ਦਾ ਮੁਲਾਂਕਣ ਕਰਕੇ ਇਹ ਨਿਰਧਾਰਤ ਕਰਨਾ ਮਹੱਤਵਪੂਰਨ ਹੈ ਕਿ ਕੀ ਇਸ ਵਿੱਚ ਸ਼ਾਮਲ ਹੋਣਾ ਸੁਰੱਖਿਅਤ ਹੈ। ਆਪਣੀਆਂ ਖੁਦ ਦੀਆਂ ਸਮਰੱਥਤਾਵਾਂ ਦੀਆਂ ਸੀਮਾਵਾਂ 'ਤੇ ਵਿਚਾਰ ਕਰੋ ਅਤੇ ਜਿਵੇਂ ਹੀ ਅਜਿਹਾ ਕਰਨਾ ਸੁਰੱਖਿਅਤ ਹੋਵੇ, ਸੁਰੱਖਿਆ ਸਟਾਫ਼ ਜਾਂ ਕਾਨੂੰਨ ਲਾਗੂ ਕਰਨ ਵਾਲਿਆਂ ਤੋਂ ਸਹਾਇਤਾ ਲਵੋ।

ਜੇ ਤੁਹਾਨੂੰ ਸਿਖਲਾਈ ਮਿਲੀ ਹੋਈ ਹੈ ਅਤੇ ਤੁਸੀਂ ਨਿਪੁੰਨ ਹੋ, ਤਾਂ ਪ੍ਰਭਾਵਸ਼ਾਲੀ ਢੰਗ ਨਾਲ ਗੱਲ ਸੁਣਨਾ ਅਤੇ ਗੱਲਬਾਤ ਕਰਨ ਸਮੇਤ, ਉਦੇਸ਼ਪੂਰਨ ਕਾਰਵਾਈਆਂ ਦੁਆਰਾ ਗਰਮ ਸਥਿਤੀਆਂ ਨੂੰ ਸੁਰੱਖਿਅਤ ਢੰਗ ਨਾਲ ਠੰਡਾ ਕਰਨ ਬਾਰੇ ਵਿਚਾਰ ਕਰੋ। ਯਾਦ ਰੱਖੋ "ਤਣਾਓ ਨੂੰ ਘੱਟ ਕਰਨਾ" ਕੁਝ ਅਜਿਹਾ ਨਹੀਂ ਹੈ ਜੋ ਤੁਸੀਂ ਕਰਦੇ ਹੋ; ਇਹ ਟੀਚਾ ਹੈ।

ਚੌਕਸ ਰਹਿਣ ਅਤੇ ਸੰਭਾਵੀ ਵਿਰੋਧ ਵਾਲੀਆਂ ਸਥਿਤੀਆਂ ਨੂੰ ਸੰਭਾਲਣ ਬਾਰੇ ਸੁਝਾਅ ਸਿੱਖਣ ਲਈ CISA ਦੀ ਤਣਾਓ ਘਟਾਉਣ ਬਾਰੇ ਲੜੀ 'ਤੇ ਜਾਓ।

ਮੋਟਰ ਵਾਹਨ ਅਤੇ ਯਾਤਰਾ

ਆਪਣੇ ਘਰ ਜਾਂ ਕਾਰਜ-ਸਥਾਨ ਨੂੰ ਛੱਡਣ ਤੋਂ ਪਹਿਲਾਂ, ਆਲੇ-ਦੁਆਲੇ ਦੇਖੋ ਅਤੇ ਕਿਸੇ ਵੀ ਸ਼ੱਕੀ ਵਾਹਨ ਵੱਲ ਧਿਆਨ ਦਿਓ ਜੋ ਸ਼ਾਇਦ ਲੁਕੇ ਹੋਏ ਜਾਂ ਘੁੰਮ ਰਹੇ ਹੋ ਸਕਦੇ ਹਨ। ਵਾਹਨ ਦੇ ਆਲੇ-ਦੁਆਲੇ ਦੇ ਖੇਤਰ ਦੀ ਅਜਿਹੀ ਕਿਸੇ ਵੀ ਚੀਜ਼ ਲਈ ਜਾਂਚ ਕਰੋ ਜੋ ਤੁਹਾਡੇ ਵਾਹਨ 'ਤੇ ਜਾਂ ਇਸਦੇ ਨੇੜੇ ਨਹੀਂ ਹੋਣੀ ਚਾਹੀਦੀ। ਜੇ ਕੋਈ ਸਥਿਤੀ ਪੈਦਾ ਹੋ ਹੀ ਜਾਂਦੀ ਹੈ, ਤਾਂ ਇਹ ਜਾਣਕਾਰੀ ਪੁਲਿਸ ਲਈ ਮਦਦਗਾਰ ਹੋ ਸਕਦੀ ਹੈ।

ਜੇ ਸੰਭਵ ਹੋਵੇ, ਤਾਂ ਆਪਣੇ ਯਾਤਰਾ ਪ੍ਰਬੰਧਾਂ ਵਿੱਚ ਦੁਹਰਾਉਣ ਵਾਲੇ ਪੈਟਰਨਾਂ ਤੋਂ ਬਚੋ ਤਾਂ ਜੋ ਸੰਭਾਵੀ ਮੰਦਭਾਵਨਾ ਵਾਲੇ ਵਿਅਕਤੀ ਤੁਹਾਡੇ ਟਿਕਾਣੇ ਦਾ ਅੰਦਾਜ਼ਾ ਨਾ ਲਗਾ ਸਕਣ। ਜਿੰਨਾ ਸੰਭਵ ਹੋ ਸਕੇ ਆਪਣੇ ਰਸਤੇ ਬਦਲੋ ਅਤੇ ਰਵਾਨਗੀ ਦੇ ਸਮੇਂ ਨੂੰ ਬਦਲਦੇ ਰਹੋ। ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਤੁਹਾਡੀ ਯਾਤਰਾ ਦੌਰਾਨ ਵਾਹਨ ਦੇ ਸਾਰੇ ਦਰਵਾਜ਼ੇ ਅਤੇ ਟਰੰਕ (ਡਿੱਕੀ) ਬੰਦ ਰਹਿਣ। ਖਿੜਕੀਆਂ ਨੂੰ ਸਿਰਫ਼ ਹਵਾਦਾਰੀ ਲਈ ਹੀ ਖੋਲ੍ਹੋ। ਸੁਰੱਖਿਅਤ ਢੰਗ ਨਾਲ ਡ੍ਰਾਈਵ ਕਰੋ ਅਤੇ ਆਪਣੇ ਸਾਹਮਣੇ ਵਾਹਨ ਤੋਂ ਸੁਰੱਖਿਅਤ ਦੂਰੀ ਬਣਾ ਕੇ ਰੱਖੋ। ਨਾਲ ਹੀ—ਹਮੇਸ਼ਾ ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਤੁਹਾਡੇ ਵਾਹਨ ਵਿੱਚ ਤੁਹਾਡੀ ਯਾਤਰਾ ਲਈ ਲੋੜੀਂਦਾ ਫਿਊਲ ਹੈ (ਜਾਂ, ਜੇ ਇਲੈਕਟ੍ਰਿਕ ਵਾਹਨ ਹੈ, ਤਾਂ ਇਸ ਨੂੰ ਲੋੜੀਂਦਾ ਚਾਰਜ ਕੀਤਾ ਗਿਆ ਹੈ)।

ਜੇ ਤੁਹਾਨੂੰ ਲੱਗਦਾ ਹੈ ਕਿ ਤੁਹਾਡਾ ਪਿੱਛਾ ਕੀਤਾ ਜਾ ਰਿਹਾ ਹੈ, ਤਾਂ ਸ਼ਾਂਤ ਰਹਿਣ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰੋ ਅਤੇ ਆਪਣੇ ਵਾਹਨ ਨੂੰ ਚਲਦਾ ਰੱਖੋ। ਸਾਰੀਆਂ ਖਿੜਕੀਆਂ ਬੰਦ ਕਰੋ ਅਤੇ ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਤੁਹਾਡੇ ਦਰਵਾਜ਼ੇ ਬੰਦ ਹਨ। ਤੁਰੰਤ ਕਾਨੂੰਨ ਲਾਗੂ ਕਰਨ ਵਾਲਿਆਂ ਨਾਲ ਸੰਪਰਕ ਕਰੋ। ਜੇ ਤੁਸੀਂ ਕਰ ਸਕਦੇ ਹੋ, ਤਾਂ ਨਜ਼ਦੀਕੀ ਪੁਲਿਸ ਸਟੇਸ਼ਨ ਵੱਲ ਜਾਓ—ਡ੍ਰਾਈਵ ਕਰਕੇ ਘਰ ਨਾ ਜਾਓ। ਕਿਸੇ ਵੀ ਸ਼ੱਕੀ ਵਾਹਨ ਦੀ ਲਾਇਸੈਂਸ ਪਲੇਟ ਨੰਬਰ, ਨਿਰਮਾਤਾ ਅਤੇ ਮਾਡਲ ਨੋਟ ਕਰਨ ਦੀ ਕੋਸ਼ਿਸ਼ ਕਰੋ।

ਜੇ ਤੁਸੀਂ ਕਿਸੇ ਵਾਹਨ ਦੀ ਟੱਕਰ ਵਿੱਚ ਸ਼ਾਮਲ ਹੋ ਜਾਂ ਕਿਸੇ ਮਕੈਨੀਕਲ ਖ਼ਰਾਬੀ ਦਾ ਸਾਹਮਣਾ ਕਰਦੇ ਹੋ, ਤਾਂ ਆਪਣੇ ਆਲੇ-ਦੁਆਲੇ ਬਾਰੇ ਵਿਚਾਰ ਕਰੋ ਅਤੇ ਤੁਰੰਤ ਐਮਰਜੈਂਸੀ ਕਰਮਚਾਰੀਆਂ ਅਤੇ ਵਾਹਨ ਟੋਅ ਕਰਨ ਵਾਲੀ ਸੇਵਾ ਨਾਲ ਸੰਪਰਕ ਕਰੋ। ਕਾਨੂੰਨ ਲਾਗੂ ਕਰਨ ਵਾਲਿਆਂ ਦੀਆਂ ਹਿਦਾਇਤਾਂ ਦੀ ਪਾਲਣਾ ਕਰੋ।

ਗੁੰਮਨਾਮ ਫ਼ੋਨ ਕਾਲਾਂ ਅਤੇ ਧਮਕੀਆਂ[6]

ਗੁੰਮਨਾਮ ਫ਼ੋਨ ਕਾਲਾਂ ਅਤੇ ਧਮਕੀਆਂ ਦਾ ਉਦੇਸ਼ ਆਮ ਤੌਰ 'ਤੇ ਡਰ, ਚਿੰਤਾ ਅਤੇ ਪਰੇਸ਼ਾਨੀ ਪੈਦਾ ਕਰਨਾ ਹੁੰਦਾ ਹੈ। ਹਮੇਸ਼ਾਂ ਹੇਠਾਂ ਦਿੱਤੇ ਕੰਮ ਕਰਨਾ ਯਾਦ ਰੱਖੋ:

- **ਸ਼ਾਂਤ ਰਹੋ** ਅਤੇ ਫ਼ੋਨ ਨਾ ਕੱਟੋ।
- ਜਿੰਨੀ ਲੰਬੀ ਦੇਰ ਲਈ ਹੋ ਸਕੇ **ਕਾਲਰ ਨੂੰ ਲਾਈਨ 'ਤੇ ਰੱਖੋ**। ਨਿਮਰ ਬਣੋ ਅਤੇ ਦਿਲਚਸਪੀ ਦਿਖਾਓ ਤਾਂ ਜੋ ਉਹ ਗੱਲ ਜਾਰੀ ਰੱਖਣ। ਉਹ ਅਜਿਹੀ ਮਹੱਤਵਪੂਰਨ ਜਾਣਕਾਰੀ ਦਾ ਖੁਲਾਸਾ ਕਰ ਸਕਦਾ ਹੈ ਜੋ ਪੁਲਿਸ ਜਾਂਚ ਦੀ ਸਥਿਤੀ ਵਿੱਚ ਮਦਦ ਕਰ ਸਕਦੀ ਹੈ।
- ਜੇ ਸੰਭਵ ਹੋਵੇ, ਤਾਂ ਆਪਣੇ ਆਲੇ-ਦੁਆਲੇ ਦੇ ਹੋਰ ਵਿਅਕਤੀ(ਆਂ) ਨੂੰ **ਸੰਕੇਤ ਦਿਓ ਜਾਂ ਨੋਟ ਫੜ੍ਹਾਓ** ਤਾਂ ਜੋ ਉਹ ਤੁਹਾਡੀ ਗੱਲ ਸੁਣ ਸਕਣ ਅਤੇ ਅਧਿਕਾਰੀਆਂ ਨੂੰ ਸੂਚਿਤ ਕਰਨ ਵਿੱਚ ਮਦਦ ਕਰ ਸਕਣ।
- ਜਿੰਨਾ ਸੰਭਵ ਹੋ ਸਕੇ ਵੱਧ ਤੋਂ ਵੱਧ ਜਾਣਕਾਰੀ **ਲਿਖੋ**—ਕਾਲਰ ID ਨੰਬਰ, ਧਮਕੀ ਦੇ ਸਟੀਕ ਸ਼ਬਦ, ਆਵਾਜ਼ ਜਾਂ ਵਿਵਹਾਰ ਦੀ ਕਿਸਮ, ਆਦਿ— ਜੋ ਜਾਂਚਕਰਤਾਵਾਂ ਦੀ ਮਦਦ ਕਰੇਗੀ।
- **ਕਾਲ ਰਿਕਾਰਡ ਕਰੋ**, ਜੇ ਸੰਭਵ ਹੋਵੇ ਅਤੇ ਕਾਨੂੰਨੀ ਤੌਰ 'ਤੇ ਇਸਦੀ ਇਜਾਜ਼ਤ ਹੋਵੇ।

ਧਮਕੀ ਭਰੀਆਂ ਜਾਂ ਅਪਮਾਨਜਨਕ ਫ਼ੋਨ ਕਾੱਲਾਂ ਕਰਨਾ ਸੰਘੀ ਕਾਨੂੰਨ ਦੇ ਵਿਰੁੱਧ ਹੈ। ਜੇ ਤੁਹਾਨੂੰ ਇਸ ਤਰ੍ਹਾਂ ਦੀਆਂ ਕੋਈ ਕਾੱਲਾਂ ਮਿਲਦੀਆਂ ਹਨ, ਤਾਂ ਆਪਣੇ ਸਥਾਨਕ ਕਾਨੂੰਨ ਲਾਗੂ ਕਰਨ ਵਾਲਿਆਂ ਨਾਲ ਸੰਪਰਕ ਕਰੋ। ਇਸ ਤੋਂ ਇਲਾਵਾ, ਤੁਸੀਂ FBI ਨੂੰ ਖ਼ਤਰੇ ਦੀ ਰਿਪੋਰਟ ਕਰ ਸਕਦੇ ਹੋ। ਸੁਝਾਵਾਂ ਲਈ FBI ਦੀ ਧਮਕੀ ਨਾਲ ਡਰਾਉਣ ਬਾਰੇ ਗਾਈਡ ਦੇਖੋ।

ਜਿਵੇਂ ਕਿ ਜ਼ਿਆਦਾਤਰ ਬੰਬ ਧਮਕੀਆਂ ਟੈਲੀਫੋਨ ਰਾਹੀਂ ਦਿੱਤੀਆਂ ਜਾਂਦੀਆਂ ਹਨ, DHS ਦੀ ਬੰਬ ਦੀ ਧਮਕੀ ਸੰਬੰਧੀ ਜਾਂਚ ਸੂਚੀ ਅਤੇ CISA ਦੀ ਬੰਬ ਦੀ ਧਮਕੀ ਬਾਰੇ ਗਾਈਡ ਦੇਖੋ, ਜਿਸ ਵਿੱਚ ਇਸ ਬਾਰੇ ਹਿਦਾਇਤਾਂ ਦਿੱਤੀਆਂ ਗਈਆਂ ਹਨ ਕਿ ਬੰਬ ਦੀ ਧਮਕੀ 'ਤੇ ਕਿਵੇਂ ਪ੍ਰਤਿਕਿਰਿਆ ਕਰਨੀ ਹੈ, ਅਤੇ ਨਾਲ ਹੀ ਜਾਣਕਾਰੀ ਦੀ ਇੱਕ ਵਿਆਪਕ ਸੂਚੀ ਹੈ ਜੋ ਬੰਬ ਦੀ ਧਮਕੀ ਦੀ ਜਾਂਚ ਵਿੱਚ ਕਾਨੂੰਨ ਲਾਗੂ ਕਰਨ ਵਾਲਿਆਂ ਦੀ ਸਹਾਇਤਾ ਕਰੇਗੀ।

ਔਨਲਾਈਨ ਸੁਰੱਖਿਆ

ਸੰਭਾਵੀ ਤੌਰ 'ਤੇ ਨੁਕਸਾਨਦੇਹ ਡਾਉਨਲੋਡਾਂ ਤੋਂ ਬਚਣ ਲਈ ਸਿਰਫ਼ ਨਾਮੀ "ਐਪ ਸਟੋਰਾਂ" ਤੋਂ ਹੀ ਐਪਲੀਕੇਸ਼ਨਾਂ ਇਨਸਟਾਲ ਕਰੋ। ਅਗਿਆਤ ਜਾਂ ਅਣਪਛਾਤੇ ਸਰੋਤਾਂ ਤੋਂ ਐਪਲੀਕੇਸ਼ਨਾਂ ਡਾਉਨਲੋਡ ਨਾ ਕਰੋ। ਇਸ ਗੱਲ ਦਾ ਧਿਆਨ ਰੱਖੋ ਕਿ ਐਪਲੀਕੇਸ਼ਨਾਂ ਕੋਲ ਤੁਹਾਡੇ ਫ਼ੋਨ 'ਤੇ ਹੋਰ ਜਾਣਕਾਰੀ ਤੱਕ ਪਹੁੰਚ ਕਰਨ ਲਈ ਕਿਹੜੀਆਂ ਇਜਾਜ਼ਤਾਂ ਹਨ।

> ***ਸਾਫ਼ਟਵੇਅਰ ਅੱਪਡੇਟਾਂ***
>
> **ਸਾਫ਼ਟਵੇਅਰ ਨੂੰ ਨਵੀਨਤਮ ਰੱਖੋ ਤਾਂ ਜੋ ਹਮਲਾਵਰ ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ ਜਾਂ ਕਮਜ਼ੋਰੀਆਂ ਦਾ ਫਾਇਦਾ ਨਾ ਚੁੱਕ ਸਕਣ।** ਬਹੁਤ ਸਾਰੇ ਆਪਰੇਟਿੰਗ ਸਿਸਟਮ ਆਟੋਮੈਟਿਕ ਅੱਪਡੇਟਾਂ ਪ੍ਰਦਾਨ ਕਰਦੇ ਹਨ। ਜੇ ਇਹ ਇੱਕ ਵਿਕਲਪ ਉਪਲਬਧ ਹੈ, ਤਾਂ ਡਿਵਾਈਸ ਦੀਆਂ ਐਪਲੀਕੇਸ਼ਨ ਸੁਰੱਖਿਆ ਸੈਟਿੰਗਾਂ ਵਿੱਚ ਆਟੋਮੈਟਿਕ ਅਪਡੇਟਾਂ ਨੂੰ ਚਾਲੂ ਕਰੋ।

ਇੱਕ ਮਜ਼ਬੂਤ ਪਾਸਵਰਡ ਬਣਾਓ ਅਤੇ ਬਣਾਈ ਰੱਖੋ ਜੋ ਤੁਹਾਡੇ ਹਰੇਕ ਡਿਵਾਈਸ ਜਾਂ ਖਾਤਿਆਂ ਲਈ ਵਿਲੱਖਣ ਹੋਵੇ ਅਤੇ ਉਨ੍ਹਾਂ ਨੂੰ ਵਿਵਸਥਿਤ ਕਰਨ ਲਈ ਇੱਕ ਪਾਸਵਰਡ ਮੈਨੇਜਰ ਦੀ ਵਰਤੋਂ ਕਰੋ। ਹਰੇਕ ਖਾਤੇ ਜਾਂ ਅਜਿਹੀ ਐਪ ਲਈ ਮਲਟੀਫੈਕਟਰ ਪ੍ਰਮਾਣੀਕਰਨ (MFA) ਚਾਲੂ ਕਰੋ ਜਿਸ ਵਿੱਚ ਇਹ ਸਹੂਲਤ ਹੈ। MFA ਨੂੰ ਸਮਰੱਥ ਕਰਨ ਨਾਲ ਤੁਹਾਡੀ ਈਮੇਲ, ਸੋਸ਼ਲ ਮੀਡੀਆ, ਆਰਥਿਕ ਵਰਗੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਅਤੇ ਹੋਰ ਮਹੱਤਵਪੂਰਨ ਜਾਣਕਾਰੀ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰਨ ਵਿੱਚ ਮਦਦ ਮਿਲਦੀ ਹੈ।

ਆਪਣੇ ਵੈੱਬ ਬ੍ਰਾਊਜ਼ਰ ਵਿੱਚ "http" ਦੀ ਬਜਾਏ "https"—ਇਹ ਸੰਕੇਤ ਕਿ ਸਾਈਟਾਂ ਏਨਕ੍ਰਿਪਸ਼ਨ ਦੀ ਵਰਤੋਂ ਕਰਦੀਆਂ ਹਨ—ਨਾਲ ਸ਼ੁਰੂ ਹੋਣ ਵਾਲੇ ਯੂਨੀਫਾਰਮ ਰਿਸੋਰਸ ਲੋਕੇਟਰ (URL) ਦੀ ਭਾਲ ਕਰੋ। ਹਾਈਪਰ ਟੈਕਸਟ ਟ੍ਰਾਂਸਫਰ ਪ੍ਰੋਟੋਕੋਲ ਸਿਕਿਓਰ (HTTPS) ਇੰਟਰਨੈਟ ਸੰਚਾਰ ਪ੍ਰੋਟੋਕੋਲ ਹੈ ਜਿਸ ਨੂੰ ਵਰਤੋਂਕਾਰ ਦੇ ਵੈੱਬ ਬ੍ਰਾਊਜ਼ਰ ਅਤੇ ਉਨ੍ਹਾਂ ਦੁਆਰਾ ਕਨੈਕਟ ਕੀਤੀ ਗਈ ਵੈੱਬਸਾਈਟ ਦੇ ਵਿਚਕਾਰ ਜਾਣਕਾਰੀ ਨੂੰ ਏਨਕ੍ਰਿਪਟ ਅਤੇ ਸੁਰੱਖਿਅਤ ਰੂਪ ਨਾਲ ਸੰਚਾਰਿਤ ਕਰਨ ਲਈ ਵਰਤਿਆ ਜਾਂਦਾ ਹੈ। ਇਹ ਵੈੱਬਸਾਈਟਾਂ 'ਤੇ ਜਾਣ 'ਤੇ ਵਰਤੋਂਕਾਰ ਦੀ ਜਾਣਕਾਰੀ ਦੀ ਅਖੰਡਤਾ ਅਤੇ ਗੁਪਤਤਾ ਨੂੰ ਬਿਹਤਰ ਢੰਗ ਨਾਲ ਸੁਰੱਖਿਅਤ ਕਰਨ ਲਈ ਤਿਆਰ ਕੀਤਾ ਗਿਆ ਹੈ।[7]

ਔਨਲਾਈਨ ਸੁਰੱਖਿਅਤ ਰਹਿਣ ਬਾਰੇ ਹੋਰ ਜਾਣਕਾਰੀ ਲੈਣ ਲਈ CISA ਦੀ Secure Our World (ਸਾਡੀ ਦੁਨੀਆ ਨੂੰ ਸੁਰੱਖਿਅਤ ਬਣਾਓ) ਦੇਖੋ।

6 Federal Bureau of Investigation. n.d. Threat Intimidation Guide. 8 ਅਗਸਤ, 2023 ਨੂੰ ਪਹੁੰਚ ਕੀਤੀ ਗਈ। fbi.gov/file-repository/threat-intimidation-guide-english-022322.pdf/view.

7 U.S. Department of Homeland Security. 2018. Hyper Text Transfer Protocol Secure (HTTPS). ਫਰਵਰੀ 12, 2024 ਨੂੰ ਪਹੁੰਚ ਕੀਤੀ ਗਈ। cisa.gov/resources-tools/resources/hyper-text-transfer-protocol-secure-https.

ਇਲੈਕਟ੍ਰਾਨਿਕ ਡਿਵਾਈਸਾਂ ਦੀ ਵਰਤੋਂ

ਮੋਬਾਈਲ ਡਿਵਾਈਸਾਂ ਅਤੇ ਨੈੱਟਵਰਕਾਂ ਵਿੱਚ ਕਈ ਤਰ੍ਹਾਂ ਦੇ ਨਿੱਜੀ ਵੇਰਵੇ ਰੱਖੇ ਹੋ ਸਕਦੇ ਹਨ, ਜਿਵੇਂ ਕਿ ਔਨਲਾਈਨ ਬੈਂਕਿੰਗ ਜਾਣਕਾਰੀ, ਈਮੇਲ, ਟੈਕਸਟ ਮੈਸੇਜ, ਸੰਪਰਕ, ਸੋਸ਼ਲ ਮੀਡੀਆ ਅਤੇ ਤਸਵੀਰਾਂ। ਆਪਣੇ ਡਿਵਾਈਸ ਨੂੰ ਸੁਰੱਖਿਅਤ ਰੱਖਣ ਲਈ, ਸਾਰੀਆਂ ਸੁਰੱਖਿਆ ਵਿਸ਼ੇਸ਼ਤਾਵਾਂ ਦੀ ਵਰਤੋਂ ਕਰੋ ਅਤੇ ਯਕੀਨੀ ਬਣਾਓ ਕਿ ਤੁਸੀਂ ਡਿਵਾਈਸ ਸਾਫ਼ਟਵੇਅਰ ਨੂੰ ਲਗਾਤਾਰ ਅੱਪਡੇਟ ਕਰ ਰਹੇ ਹੋ। ਆਪਣੇ ਫ਼ੋਨ ਅਤੇ ਸਿਮ ਕਾਰਡਾਂ ਲਈ ਮਜ਼ਬੂਤ ਪਾਸਕੋਡ ਬਣਾਓ ਅਤੇ ਬੇਲੋੜੀਆਂ ਟਿਕਾਣਾ ਸੇਵਾਵਾਂ ਨੂੰ ਬੰਦ ਕਰੋ।[8]

ਹਮੇਸ਼ਾਂ ਵੈਇਸਮੇਲ ਤੱਕ ਪਹੁੰਚ ਕਰਨ ਲਈ ਆਪਣੇ ਡਿਫ਼ਾਲਟ ਪਿੰਨ ਨੂੰ ਬਦਲੋ। ਆਪਣੇ ਫ਼ੋਨ 'ਤੇ ਟਿਕਾਣਾ ਸੇਵਾਵਾਂ ਨੂੰ ਸੀਮਿਤ ਕਰਨ 'ਤੇ ਵਿਚਾਰ ਕਰੋ ਅਤੇ ਦੂਜਿਆਂ ਨੂੰ ਤੀਜੀ ਧਿਰ ਦੀਆਂ ਐਪਲੀਕੇਸ਼ਨਾਂ ਰਾਹੀਂ ਤੁਹਾਡੀਆਂ ਹਰਕਤਾਂ 'ਤੇ ਨਜ਼ਰ ਰੱਖਣ ਅਤੇ ਤੁਹਾਡੇ ਘਰ ਦੇ ਪਤੇ ਜਾਂ ਕੰਮ ਦੀ ਥਾਂ ਦੀ ਪਛਾਣ ਕਰਨ ਤੋਂ ਰੋਕਣ ਲਈ ਨਿੰਜਤਾ ਸੈਟਿੰਗਾਂ ਦੀ ਸਮੀਖਿਆ ਕਰੋ। ਆਪਣੇ ਡਿਵਾਈਸ(ਡਿਵਾਈਸਾਂ) ਦੀ ਸੁਰੱਖਿਆ ਨੂੰ ਵਧਾਉਣ ਲਈ Apple ਅਤੇ Android ਦੀਆਂ ਨਿੰਜਤਾ ਅਤੇ ਸੁਰੱਖਿਆ ਸੰਬੰਧੀ ਉਪਾਵਾਂ ਦੀ ਸਮੀਖਿਆ ਕਰੋ।

ਸੋਸ਼ਲ ਮੀਡੀਆ

ਇੰਟਰਨੈੱਟ ਜਾਣਕਾਰੀ, ਸਿੱਖਿਆ ਅਤੇ ਮਨੋਰੰਜਨ ਦਾ ਇੱਕ ਕੀਮਤੀ ਸਰੋਤ ਹੋ ਸਕਦਾ ਹੈ। ਹਾਲਾਂਕਿ, ਚੌਕਸ ਰਹਿਣ ਅਤੇ ਤੁਸੀਂ ਔਨਲਾਈਨ ਜੋ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਪ੍ਰਕਾਸ਼ਿਤ ਕਰਦੇ ਹੋ—ਖਾਸ ਕਰਕੇ ਸੋਸ਼ਲ ਮੀਡੀਆ 'ਤੇ—ਉਸ ਦੀ ਮਾਤਰਾ ਨੂੰ ਸੀਮਿਤ ਕਰਨ ਲਈ ਸਾਵਧਾਨੀਆਂ ਵਰਤਣਾ ਜ਼ਰੂਰੀ ਹੈ।

ਪ੍ਰਸਿੱਧ ਸੋਸ਼ਲ ਮੀਡੀਆ ਸਾਈਟਾਂ ਵਿਅਕਤੀਆਂ ਨੂੰ ਇੱਕ ਨਿੱਜੀ ਪ੍ਰੋਫਾਈਲ ਬਣਾਉਣ ਅਤੇ ਦੂਜਿਆਂ ਨਾਲ ਔਨਲਾਈਨ ਗੱਲਬਾਤ ਕਰਨ ਦੀ ਸਹੂਲਤ ਦਿੰਦੀਆਂ ਹਨ। ਕਾਰੋਬਾਰੀ ਨੈੱਟਵਰਕਿੰਗ ਸਾਈਟਾਂ 'ਤੇ, ਲੋਕ ਆਪਣੇ ਪ੍ਰੋਫਾਈਲਾਂ ਵਿੱਚ ਵਧੇਰੇ ਵੇਰਵੇ ਸ਼ਾਮਲ ਕਰ ਸਕਦੇ ਹਨ ਅਤੇ ਕੰਮ ਦਾ ਇਤਿਹਾਸ ਅਤੇ ਪਿਛੋਕੜ ਸੰਬੰਧੀ ਹੋਰ ਜਾਣਕਾਰੀ ਸ਼ਾਮਲ ਕਰ ਸਕਦੇ ਹਨ। ਹਾਲਾਂਕਿ ਇਹ ਸਾਧਨ ਦੂਜਿਆਂ ਨਾਲ ਸੰਚਾਰ ਕਰਨ ਅਤੇ ਤੁਹਾਡੇ ਪੇਸ਼ੇਵਰ ਪਿਛੋਕੜ ਦੀ ਮਸ਼ਹੂਰੀ ਕਰਨ ਵਿੱਚ ਤੁਹਾਡੀ ਮਦਦ ਕਰਦੇ ਹਨ, ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਨੂੰ ਔਨਲਾਈਨ ਪ੍ਰਕਾਸ਼ਿਤ ਕਰਨਾ ਸੰਭਾਵੀ ਜੋਖਮ ਪੇਸ਼ ਕਰਦਾ ਹੈ।

ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਪੋਸਟ ਕਰਦੇ ਸਮੇਂ ਸਾਵਧਾਨ ਰਹੋ। ਮੰਦਭਾਵਨਾ ਨਾਲ ਕੰਮ ਕਰਨ ਵਾਲੇ ਵਿਅਕਤੀ ਹੈਕ ਕਰਨ ਜਾਂ ਪਛਾਣ ਦੀ ਚੋਰੀ ਕਰਨ ਵੇਲੇ ਫੋਟੋਆਂ ਤੋਂ ਟਿਕਾਣਾ ਡੇਟਾ, ਜਨਮਦਿਨਾਂ, ਪੂਰੇ ਨਾਮ, ਘਰ ਦੇ ਪਤੇ ਅਤੇ ਈਮੇਲ ਵੇਰਵਿਆਂ ਦੀ ਵਰਤੋਂ ਕਰ ਸਕਦੇ ਹਨ। ਇਸ ਤੋਂ ਇਲਾਵਾ, ਰੁਜ਼ਗਾਰ, ਪਰਿਵਾਰਕ ਮੈਂਬਰਾਂ, ਸ਼ੌਕਾਂ ਜਾਂ ਵਾਹਨ ਦੇ ਵੇਰਵਿਆਂ ਬਾਰੇ ਜਾਣਕਾਰੀ ਅਪਰਾਧੀਆਂ ਅਤੇ ਵੈਰਪੂਰਨ ਧਿਰਾਂ ਲਈ ਕੀਮਤੀ ਹੁੰਦੀ ਹੈ। ਤੁਹਾਡਾ ਪਰਿਵਾਰ ਅਤੇ ਦੋਸਤ ਵੀ, ਜੇ ਉਹ ਆਪਣੀ ਪ੍ਰੋਫਾਈਲ ਜਾਣਕਾਰੀ ਦੀ ਰੱਖਿਆ ਕਰਨ ਲਈ ਉਚਿਤ ਉਪਾਅ ਨਹੀਂ ਕਰਦੇ ਹਨ, ਤਾਂ ਅਣਜਾਣੇ ਵਿੱਚ ਤੁਹਾਡੇ ਬਾਰੇ ਜਾਣਕਾਰੀ ਸਾਂਝੀ ਕਰ ਸਕਦੇ ਹਨ। ਯਾਦ ਰੱਖੋ, ਇੰਟਰਨੈੱਟ 'ਤੇ ਕੋਈ "ਡਿਲੀਟ" ਬਟਨ ਨਹੀਂ ਹੁੰਦਾ ਹੈ। ਸਾਵਧਾਨੀ ਨਾਲ ਸਾਂਝਾ ਕਰੋ, ਕਿਉਂਕਿ ਭਾਵੇਂ ਤੁਸੀਂ ਆਪਣੇ ਪ੍ਰੋਫਾਈਲ ਤੋਂ ਕੋਈ ਪੋਸਟ ਜਾਂ ਤਸਵੀਰ ਡਿਲੀਟ ਕਰ ਦਿੰਦੇ ਹੋ, ਸੰਭਾਵਨਾ ਹੈ ਕਿ ਹਾਲੇ ਵੀ ਕਿਸੇ ਨੇ ਇਸਨੂੰ ਦੇਖ ਲਿਆ ਹੋਵੇਗਾ।

ਕੁਝ ਸੋਸ਼ਲ ਨੈੱਟਵਰਕਿੰਗ ਸਾਈਟਾਂ ਕੋਲ ਤੁਹਾਡੇ ਦੁਆਰਾ ਪੋਸਟ ਕੀਤੇ ਗਏ ਕਿਸੇ ਵੀ ਡੇਟਾ ਦੀ ਮਲਕੀਅਤ ਹੁੰਦੀ ਹੈ ਅਤੇ ਉਹ ਤੁਹਾਡੇ ਵੇਰਵੇ ਤੀਜੀ ਧਿਰਾਂ ਨੂੰ ਵੇਚ ਦਿੰਦੀਆਂ ਹਨ। ਇਨ੍ਹਾਂ ਸਾਈਟਾਂ 'ਤੇ ਆਪਣੀ ਨਿੰਜਤਾ ਅਤੇ ਟਿਕਾਣਾ ਟੈਗਿੰਗ ਸੈਟਿੰਗਾਂ ਦੀ ਨਿਯਮਿਤ ਤੌਰ 'ਤੇ ਸਮੀਖਿਆ ਕਰੋ, ਨਹੀਂ ਤਾਂ ਤੁਹਾਨੂੰ ਤੁਹਾਡੇ ਨਿੱਜੀ ਪ੍ਰੋਫਾਈਲ ਦੇ ਕੁਝ, ਜਾਂ ਸਾਰੇ, ਹਿੱਸੇ ਨੂੰ ਅਜਿਹੇ ਬਹੁਤ ਜ਼ਿਆਦਾ ਲੋਕਾਂ ਦੁਆਰਾ ਦੇਖੇ ਜਾਣ ਦਾ ਜੋਖਮ ਹੈ, ਜਿਨ੍ਹਾਂ ਨੂੰ ਤੁਸੀਂ ਨਹੀਂ ਜਾਣਦੇ ਹੋ।[9, 10]

8 Federal Communications Commission. 2019. Protect Your Smart Device. 20 ਸਤੰਬਰ 2023 ਨੂੰ ਪਹੁੰਚ ਕੀਤੀ ਗਈ। fcc.gov/consumers/guides/protect-your-mobile-device.

9 Government of the United Kingdom. National Cyber Security Centre. 2019. Social Media: how to use it safely. ਸਤੰਬਰ 20, 2023 ਨੂੰ ਪਹੁੰਚ ਕੀਤੀ ਗਈ। ncsc.gov.uk/guidance/social-media-how-to-use-it-safely.

10 Cybersecurity and Infrastructure Security Agency, National Cyber Alliance. 2019. Social Media Cybersecurity. ਸਤੰਬਰ 20, 2023 ਨੂੰ ਪਹੁੰਚ ਕੀਤੀ ਗਈ। cisa.gov/sites/default/files/publications/NCSAM_SocialMediaCybersecurity_2020.pdf.

ਸੋਸ਼ਲ ਮੀਡੀਆ ਨਿੰਜਤਾ ਅਤੇ ਟਿਕਾਣਾ ਸੈਟਿੰਗਾਂ ਦੀ ਸਮੀਖਿਆ ਕਰੋ

X, ਜਿਸ ਨੂੰ ਪਹਿਲਾਂ Twitter ਵਜੋਂ ਜਾਣਿਆ ਜਾਂਦਾ ਸੀ

- twitter.com/settings/privacy_and_safety
- twitter.com/settings/location_information

Instagram

- help.instagram.com/811572406418223
- **IOS:** help.instagram.com/171821142968851
- **Android:** ਆਪਣੇ Android ਡਿਵਾਈਸ 'ਤੇ, Settings > Apps > Instagram > Permissions > Location 'ਤੇ ਜਾਓ

Facebook

- facebook.com/help/325807937506242/
- facebook.com/help/337244676357509

Snapchat

- help.snapchat.com/hc/en-gb/sections/5690164367636-Privacy-Settings
- help.snapchat.com/hc/en-us/articles/7012322854932-How-do-I-turn-on-Ghost-Mode

TikTok

- tiktok.com/safety/en/privacy-and-security-on-tiktok/
- support.tiktok.com/en/account-and-privacy/account-privacy-settings/location-services-on-tiktok

ਡੌਕਸਿੰਗ

ਡੌਕਸਿੰਗ ਦਾ ਮਤਲਬ ਹੈ ਕਿਸੇ ਵਿਅਕਤੀ ਦੀ ਨਿੱਜੀ ਤੌਰ 'ਤੇ ਪਛਾਣਯੋਗ ਜਾਣਕਾਰੀ (PII)—ਜਾਂ ਕਿਸੇ ਸੰਗਠਨ ਦੀ ਸੰਵੇਦਨਸ਼ੀਲ ਜਾਣਕਾਰੀ—ਨੂੰ ਖੁੱਲ੍ਹੇ ਸਰੋਤਾਂ ਜਾਂ ਸਮਝੌਤਾ ਕੀਤੀ ਸਮੱਗਰੀ ਤੋਂ ਇਕੱਠਾ ਕਰਨਾ ਅਤੇ ਇਸ ਨੂੰ ਜਨਤਕ ਤੌਰ 'ਤੇ ਜਾਰੀ ਕਰਨਾ ਜਾਂ ਮੰਦਭਾਵਨਾ ਵਾਲੇ ਉਦੇਸ਼ਾਂ ਲਈ ਵਰਤਣਾ।[11, 12] ਅਪਰਾਧੀ ਇਸ ਜਾਣਕਾਰੀ ਦੀ ਵਰਤੋਂ ਸੰਭਾਵੀ ਟੀਚਿਆਂ ਨੂੰ ਬਲੈਕਮੇਲ ਜਾਂ ਉਨ੍ਹਾਂ ਵਿੱਚ ਡਰ ਪੈਦਾ ਕਰਨ ਲਈ ਕਰਦੇ ਹਨ।

ਜਦੋਂ ਤੁਸੀਂ ਔਨਲਾਈਨ ਪੋਸਟ ਕਰਦੇ ਹੋ, ਤਾਂ ਇਹ ਜਾਣਨਾ ਮਹੱਤਵਪੂਰਨ ਹੁੰਦਾ ਹੈ ਕਿ ਤੁਸੀਂ ਕੀ ਅਤੇ ਕਿਵੇਂ ਪੋਸਟ ਕਰ ਰਹੇ ਹੋ। ਜੇ ਤੁਸੀਂ ਢੁਕਵੀਆਂ ਨਿੱਜਤਾ ਸੈਟਿੰਗਾਂ ਨੂੰ ਲਾਗੂ ਕੀਤੇ ਬਿਨਾਂ ਬਹੁਤ ਜ਼ਿਆਦਾ ਜਾਣਕਾਰੀ ਪੋਸਟ ਕਰਦੇ ਹੋ, ਤਾਂ ਤੁਸੀਂ ਆਪਣੀ ਨਿੱਜੀ ਸੁਰੱਖਿਆ ਨੂੰ ਜੋਖਮ ਵਿੱਚ ਪਾ ਰਹੇ ਹੋ ਸਕਦੇ ਹੋ। ਲੋਕ ਇਸ ਜਾਣਕਾਰੀ ਦੀ ਵਰਤੋਂ ਤੁਹਾਡੇ ਸੰਬੰਧਾਂ, ਵਿਚਾਰਾਂ, ਦਿਲਚਸਪੀ ਵਾਲੀਆਂ ਥਾਵਾਂ ਅਤੇ ਹੋਰ ਵਿਸ਼ਿਆਂ ਦੀ ਤਸਵੀਰ ਬਣਾਉਣ ਲਈ ਕਰ ਸਕਦੇ ਹਨ ਜਿਸਦਾ ਉਹ ਭਵਿੱਖ ਵਿੱਚ ਫਾਇਦਾ ਉਠਾ ਸਕਦੇ ਹਨ।

ਡੇਟਾ ਬ੍ਰੋਕਰ ਵੀ ਇਸ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਨੂੰ ਇਕੱਠਾ ਕਰ ਸਕਦੇ ਹਨ ਅਤੇ ਦੂਜੀਆਂ ਕੰਪਨੀਆਂ ਨੂੰ ਵੇਚ ਸਕਦੇ ਹਨ। ਆਪਣੇ ਡੇਟਾ ਨੂੰ ਦਲਾਲਾਂ ਦੇ ਹੱਥ ਲੱਗਣ ਨੂੰ ਘੱਟ ਤੋਂ ਘੱਟ ਕਰਨ ਲਈ:

- PII ਨੂੰ ਸਾਂਝਾ ਕਰਨ ਤੋਂ **ਬਚੋ**।
- ਸੋਸ਼ਲ ਮੀਡੀਆ 'ਤੇ ਉਨ੍ਹਾਂ ਲੋਕਾਂ ਨੂੰ ਸਵੀਕਾਰ **ਨਾ ਕਰੋ** ਜਿਨ੍ਹਾਂ ਨੂੰ ਤੁਸੀਂ ਅਸਲ ਜ਼ਿੰਦਗੀ ਵਿੱਚ ਨਹੀਂ ਜਾਣਦੇ ਹੋ।
- **ਯਕੀਨੀ ਬਣਾਓ** ਕਿ ਤੁਹਾਡੇ ਦੁਆਰਾ ਵਰਤੀਆਂ ਜਾਣ ਵਾਲੀਆਂ ਐਪਾਂ ਵਿੱਚ ਐਂਡ-ਟੂ-ਐਂਡ ਏਨਕ੍ਰਿਪਸ਼ਨ ਹੈ।
- ਐਪ ਇਜਾਜ਼ਤਾਂ ਨੂੰ **ਸੀਮਿਤ ਕਰੋ**।
- ਆਪਣੇ ਨਾਮ ਲਈ Google Alerts **ਸੈੱਟ-ਅਪ ਕਰੋ**।
- ਮੁੱਖ ਡੇਟਾ ਬ੍ਰੋਕਰ ਅਤੇ ਲੋਕਾਂ ਦੀ ਖੋਜ ਕਰਨ ਵਾਲੀਆਂ ਸਾਈਟਾਂ ਤੋਂ ਬਾਹਰ ਹੋਣ ਲਈ **ਸਮਾਂ ਕੱਢਣ ਬਾਰੇ ਵਿਚਾਰ ਕਰੋ** ਜਾਂ ਤੁਹਾਡੇ ਲਈ ਇਹ ਕਰਨ ਲਈ ਕਿਸੇ ਸੇਵਾ ਦਾ ਸਬਸਕ੍ਰਿਪਸ਼ਨ ਲਵੋ।

ਸਥਾਨ-ਅਧਾਰਿਤ ਜਾਣਕਾਰੀ ਸੋਸ਼ਲ ਨੈੱਟਵਰਕਾਂ 'ਤੇ ਪੋਸਟ ਕੀਤੀ ਜਾ ਸਕਦੀ ਹੈ, ਖਾਸ ਤੌਰ 'ਤੇ GPS-ਸਮਰੱਥ ਸੈੱਲ ਫੋਨਾਂ ਅਤੇ ਮੋਬਾਈਲ ਡਿਵਾਈਸਾਂ ਤੋਂ। ਇਹ ਜਾਣਕਾਰੀ ਸੁਰੱਖਿਅਤ ਨਹੀਂ ਹੈ ਅਤੇ ਕਿਸੇ ਵੀ ਵਿਅਕਤੀ ਦੁਆਰਾ ਦੇਖੀ ਜਾ ਸਕਦੀ ਹੈ, ਉਨ੍ਹਾਂ ਲੋਕਾਂ ਸਮੇਤ ਜੋ ਸ਼ਾਇਦ ਤੁਹਾਨੂੰ ਨੁਕਸਾਨ ਪਹੁੰਚਾਉਣਾ ਚਾਹੁੰਦੇ ਹਨ। ਤੁਸੀਂ ਜੋ ਵੀ ਪੋਸਟ ਕਰਦੇ ਹੋ ਉਸ 'ਤੇ ਨਜ਼ਰ ਰੱਖੋ ਅਤੇ ਜ਼ਿੰਮੇਵਾਰੀ ਨਾਲ ਪੋਸਟ ਕਰੋ ਤਾਂ ਜੋ ਇਹ ਯਕੀਨੀ ਬਣਾਇਆ ਜਾ ਸਕੇ ਕਿ ਤੁਹਾਡੇ ਦੁਆਰਾ ਜਨਤਕ ਕੀਤੀ ਜਾਣ ਵਾਲੀ ਜਾਣਕਾਰੀ ਨਾਲ ਕੋਈ ਵੀ ਜੋਖਮ ਵਿੱਚ ਨਹੀਂ ਆ ਜਾਂਦਾ ਹੈ।

ਜੇ ਤੁਹਾਨੂੰ ਲੱਗਦਾ ਹੈ ਕਿ ਤੁਹਾਨੂੰ ਡੌਕਸ ਕੀਤਾ ਜਾ ਰਿਹਾ ਹੈ:

- ਸਥਾਨਕ ਕਾਨੂੰਨ ਲਾਗੂ ਕਰਨ ਵਾਲਿਆਂ ਅਤੇ ਕਿਸੇ ਵੀ ਔਨਲਾਈਨ ਪਲੇਟਫਾਰਮ ਨੂੰ **ਘਟਨਾ ਦੀ ਰਿਪੋਰਟ ਕਰੋ** ਜਿੱਥੋਂ ਤੁਹਾਡੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਜਾਰੀ ਕੀਤੀ ਗਈ ਹੋ ਸਕਦੀ ਹੈ।
- ਜੋ ਕੁਝ ਹੋਇਆ, ਉਸਨੂੰ **ਦਸਤਾਵੇਜ਼ੀ ਰੂਪ ਦਿਓ** ਅਤੇ ਜਾਂਚਕਰਤਾਵਾਂ ਨਾਲ ਸਾਂਝਾ ਕਰਨ ਲਈ ਸਕ੍ਰੀਨ ਸ਼ਾਟ ਲਓ।
- **ਨਿਰਧਾਰਤ ਕਰੋ** ਕਿ ਕਿਹੜੀ ਜਾਣਕਾਰੀ ਦੀ ਦੁਰਵਰਤੋਂ ਕੀਤੀ ਗਈ ਸੀ, ਖਤਰੇ ਦੀ ਗੰਭੀਰਤਾ ਕੀ ਹੈ ਅਤੇ ਉਲੰਘਣਾ ਜਾਂ ਛੇੜਛਾੜ ਕਿੱਥੇ ਹੋਈ ਸੀ।
- ਵੈੱਬਸਾਈਟਾਂ ਜਾਂ ਐਪਲੀਕੇਸ਼ਨਾਂ ਤੋਂ ਜਾਣਕਾਰੀ ਹਟਾਉਣ ਲਈ **ਵੈੱਬਸਾਈਟ ਪ੍ਰਸ਼ਾਸਕਾਂ ਨਾਲ ਕੰਮ ਕਰੋ**।
- **ਨਿੱਜਤਾ ਸੈਟਿੰਗਾਂ ਨੂੰ** ਸਭ ਤੋਂ ਨਿੱਜੀ ਵਿਕਲਪਾਂ 'ਤੇ ਕੌਂਫਿਗਰ ਕਰੋ।
- ਪਛਾਣ ਦੀ ਚੋਰੀ ਦੇ **ਸੰਕੇਤਾਂ ਤੇ ਨਜ਼ਰ ਰੱਖੋ**, ਵਿੱਤੀ ਖਾਤਿਆਂ ਦੀ ਨਿਗਰਾਨੀ ਕਰੋ, ਧੋਖਾਧੜੀ ਦੀਆਂ ਚੇਤਾਵਨੀਆਂ ਸੈੱਟ ਕਰੋ ਅਤੇ ਸਾਰੇ ਔਨਲਾਈਨ ਖਾਤਿਆਂ ਲਈ ਲੌਗ-ਇਨ ਅਤੇ ਪਾਸਵਰਡ ਜਾਣਕਾਰੀ ਬਦਲ ਦਿਓ।

ਡੌਕਸਿੰਗ ਦੇ ਵਿਰੁੱਧ ਕਾਨੂੰਨ ਅਧਿਕਾਰ ਖੇਤਰ ਦੇ ਅਨੁਸਾਰ ਵੱਖ-ਵੱਖ ਹਨ, ਇਸ ਲਈ ਜਦੋਂ ਤੁਸੀਂ ਜੋਖਮ ਨੂੰ ਘਟਾਉਣ ਅਤੇ ਰੋਕਥਾਮ ਦੇ ਵਿਕਲਪਾਂ 'ਤੇ ਵਿਚਾਰ ਕਰਦੇ ਹੋ, ਇਹ ਮਹੱਤਵਪੂਰਨ ਹੈ ਕਿ ਤੁਸੀਂ ਆਪਣੇ ਖੇਤਰ ਵਿੱਚ ਉਨ੍ਹਾਂ ਬਾਰੇ ਪਤਾ ਕਰੋ। ਜੇ ਤੁਸੀਂ ਸਰੀਰਕ ਸੁਰੱਖਿਆ ਬਾਰੇ ਚਿੰਤਤ ਹੋ, ਤਾਂ ਅਗਲੇ ਕਦਮਾਂ ਲਈ ਸਥਾਨਕ ਕਾਨੂੰਨ ਲਾਗੂ ਕਰਨ ਵਾਲਿਆਂ ਨਾਲ ਸੰਪਰਕ ਕਰੋ।

ਫਿਸ਼ਿੰਗ ਨੂੰ ਪਛਾਣੋ ਅਤੇ ਇਸਦੀ ਰਿਪੋਰਟ ਕਰੋ

ਅਪਰਾਧੀ ਅਕਸਰ ਫਿਸ਼ਿੰਗ ਰਣਨੀਤੀਆਂ ਦੀ ਵਰਤੋਂ ਕਰਕੇ ਤੁਹਾਨੂੰ ਨੁਕਸਾਨਦੇਹ ਲਿੰਕਾਂ, ਈਮੇਲਾਂ ਜਾਂ ਅਟੈਚਮੈਂਟਾਂ ਨੂੰ ਖੋਲ੍ਹਣ ਲਈ ਪ੍ਰੇਰਿਤ ਕਰਦੇ ਹਨ ਜੋ ਤੁਹਾਡੀ ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਲਈ ਬੇਨਤੀ ਕਰ ਸਕਦੇ ਹਨ ਜਾਂ ਤੁਹਾਡੇ ਡਿਵਾਈਸਾਂ ਨੂੰ ਪ੍ਰਭਾਵਿਤ ਕਰ ਸਕਦੇ ਹਨ। ਇਹ ਮੈਸੇਜ ਅਕਸਰ ਇਸ ਤਰ੍ਹਾਂ ਤਿਆਰ ਕੀਤੇ ਜਾਂਦੇ ਹਨ ਜਿਵੇਂ ਕਿ ਉਹ ਕਿਸੇ ਭਰੋਸੇਯੋਗ ਵਿਅਕਤੀ ਜਾਂ ਸੰਗਠਨ ਤੋਂ ਆਏ ਹੋਣ।

ਫਿਸ਼ਿੰਗ ਮੈਸੇਜ ਈਮੇਲ, ਟੈਕਸਟ ਮੈਸੇਜ, ਸੋਸ਼ਲ ਮੀਡੀਆ 'ਤੇ ਸਿੱਧੇ ਮੈਸੇਜ ਜਾਂ ਇੱਕ ਫ਼ੋਨ ਕੌਲ ਦੇ ਰੂਪ ਵਿੱਚ ਆ ਸਕਦੇ ਹਨ। ਜ਼ਰੂਰੀ ਜਾਂ ਭਾਵਨਾਤਮਕ ਭਾਸ਼ਾ, ਨਿੱਜੀ ਜਾਣਕਾਰੀ ਭੇਜਣ ਦੀਆਂ ਬੇਨਤੀਆਂ, ਅਵਿਸ਼ਵਾਸਯੋਗ ਛੋਟੇ URL ਅਤੇ ਗਲਤ ਈਮੇਲ ਪਤਿਆਂ ਅਤੇ ਲਿੰਕਾਂ ਬਾਰੇ ਸਾਵਧਾਨ ਰਹੋ।

ਜੇ ਤੁਹਾਨੂੰ ਸ਼ੱਕ ਹੈ ਕਿ ਤੁਸੀਂ ਫਿਸ਼ਿੰਗ ਦੀ ਕੋਸ਼ਿਸ਼ ਦਾ ਨਿਸ਼ਾਨਾ ਬਣੇ ਹੋ ਤਾਂ ਕਿਸੇ ਵੀ ਲਿੰਕ ਜਾਂ ਅਟੈਚਮੈਂਟ 'ਤੇ ਕਲਿੱਕ ਨਾ ਕਰੋ। ਇਸਦੀ ਬਜਾਏ, ਉਸਦੀ ਰਿਪੋਰਟ ਕਰੋ, ਫਿਰ ਮੈਸੇਜ ਨੂੰ ਮਿਟਾ ਦਿਓ।

11 Department of Homeland Security. 2024. Office of Partnership and Engagement. Resources for Individuals on the Threat of Doxing. ਫਰਵਰੀ 09, 2024 ਨੂੰ ਪਹੁੰਚ ਕੀਤੀ ਗਈ। dhs.gov/publication/resources-individuals-threat-doxing.

12 European Council for Nuclear Research. 2017. Computer Security: Enter the next level: Doxware. ਦਸੰਬਰ 12, 2023 ਨੂੰ ਪਹੁੰਚ ਕੀਤੀ ਗਈ। home.cern/news/news/computing/computer-security-enter-next-level-doxware.

ਵਸੀਲੇ

ਭੌਤਿਕ ਸੁਰੱਖਿਆ

- CISA Security and Resiliency Guide (CISA ਦੀ ਸੁਰੱਖਿਆ ਅਤੇ ਲਚਕਤਾ ਗਾਈਡ)
- CISA Active Shooter Preparedness (CISA ਦੀ ਕਿਰਿਆਸ਼ੀਲ ਸ਼ੂਟਰ ਸੰਬੰਧੀ ਤਿਆਰੀ)
- FBI Threat Intimidation Guide (FBI ਦੀ ਧਮਕੀ ਨਾਲ ਡਰਾਉਣ ਬਾਰੇ ਗਾਈਡ)
- CISA Bomb Threats (CISA ਬੰਬ ਦੀਆਂ ਧਮਕੀਆਂ)
- CISA De-escalation Series (CISA ਦੀ ਤਣਾਉ ਘਟਾਉਣ ਬਾਰੇ ਲੜੀ)

ਸਥਿਤੀ ਸੰਬੰਧੀ ਜਾਗਰੂਕਤਾ

- Stalking Prevention, Awareness, & Resource Center (SPARC)
  (ਪਿੱਛਾ ਕਰਨ ਨੂੰ ਰੋਕਣਾ, ਜਾਗਰੂਕਤਾ, ਅਤੇ ਸਰੋਤ ਕੇਂਦਰ)

ਔਨਲਾਈਨ ਸੁਰੱਖਿਆ

- CISA Secure Our World (CISA ਸਾਡੀ ਦੁਨੀਆ ਨੂੰ ਸੁਰੱਖਿਅਤ ਕਰੋ)
- CISA Privacy and Mobile Device Apps (CISA ਨਿੱਜਤਾ ਅਤੇ ਮੋਬਾਈਲ ਡਿਵਾਈਸ ਐਪਾਂ)
- CISA Insights: Mitigating the Impacts of Doxing on Critical Infrastructure (CISA ਸੂਝ: ਮਹੱਤਵਪੂਰਨ ਬੁਨਿਆਦੀ ਢਾਂਚੇ 'ਤੇ ਡੌਕਸਿੰਗ ਦੇ ਪ੍ਰਭਾਵਾਂ ਨੂੰ ਘਟਾਉਣਾ)
- CISA Social Media Cybersecurity (CISA ਸੋਸ਼ਲ ਮੀਡੀਆ ਸਾਈਬਰ ਸੁਰੱਖਿਆ)