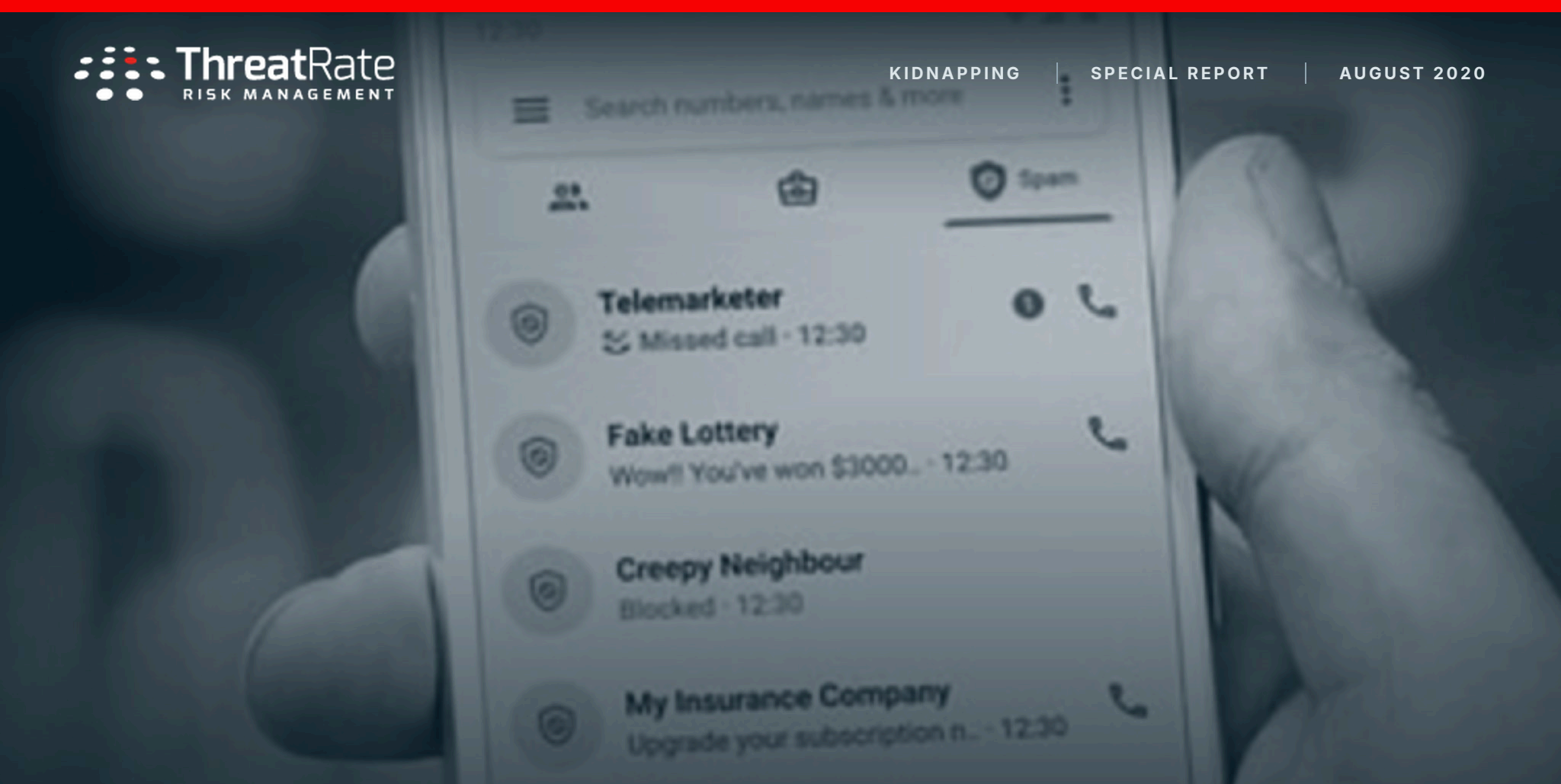


THE CURRENT STATE OF VIRTUAL KIDNAPPING

PUBLISHED
9 August 2020

CATEGORY
Kidnapping

KIDNAPPING · AUGUST 2020

The Current State of Virtual Kidnapping

The growth of interconnectivity and its risks

The expansion of global interconnectivity – particularly through low- or no-cost communication tools – has enabled more efficient business operations. For instance, individuals can collaborate on projects with team members worldwide, and families with loved ones serving in the military can stay connected through video chat applications.

However, this growth is not entirely positive. As seen with the evolution of email, scammers and other criminal actors exploit new technologies to expand their operations, deceiving unsuspecting individuals into sending them money. One particularly dark trend, virtual kidnapping, emerged in Latin America nearly two decades ago and has since spread to Asia and North America. Authorities are now warning the public about its dangers, as victims have been left financially devastated and emotionally distraught by the experience.

The role of artificial intelligence (AI)

Virtual kidnapping is a form of extortion that relies on deception and psychological manipulation rather than actual physical abduction. Criminals exploit digital communication platforms, falsely claiming they have kidnapped a loved one, and use fear and urgency to pressure victims into paying a ransom.

Increasingly, artificial intelligence (AI) is being used to make virtual kidnappings more convincing. AI-driven deepfake audio and video tools allow criminals to imitate the voices and appearances of supposed kidnapping victims, making their scams more effective.

Voice Cloning: AI-generated voice replication enables criminals to convincingly mimic a person's voice with minimal audio samples, intensifying the psychological distress for victims.

Deepfake Videos: Advanced video manipulation creates realistic hostage scenarios, increasing the likelihood that victims will comply with ransom demands.

Estimated cases and most affected countries

Determining global statistics is challenging due to underreporting and jurisdictional differences, but law enforcement agencies have noted a rise in virtual kidnappings in recent years. The FBI and international law enforcement estimate that tens of thousands of cases occur worldwide each year.

Mexico, with its high levels of organized crime and limited enforcement capacity, experiences a significant number of virtual kidnapping incidents annually. Initially, this crime primarily targeted Spanish-speaking populations in the United States, often perpetrated by inmates in Mexican prisons attempting to extort money to improve their conditions or secure their release.

more notably, to Mandarin-speaking communities abroad. Authorities in Calgary, Alberta, and other Canadian cities, as well as in Australia, have reported cases involving international students – primarily Chinese nationals. Scammers often impersonate law enforcement

© 2025 ThreatRate Risk Management. All Rights Reserved

officers, claiming the students are in legal trouble and coercing them into hiding while demanding ransoms from their families.

Beyond Canada and Australia, the Chinese Embassy in the United Kingdom has issued similar warnings. Embassy officials report that scammers pose as Chinese police officers or embassy staff, threatening international students and coercing them into participating in fake hostage videos. These realistic videos are then sent to victims' families in China, increasing the likelihood of ransom payment. Reports of similar scams have surfaced in New Zealand and the United States.

In Spain, the National Police recorded nearly 1,500 cases between 2014 and 2019, with many more likely unreported. According to Spain's National Police Kidnappings and Extortion Department, scammers – often prisoners in Latin America – typically demand €10,000 initially, though they frequently lower the amount, sometimes to as little as €500.

Mitigation efforts

To reduce the risk of falling victim to a virtual kidnapping scam, the FBI recommends the following precautions:

- Stay calm.
- Slow the situation down.
- Avoid sharing personal information about yourself or your family during the call.
- Listen carefully to the voice of the supposed victim.
- Attempt to contact the "kidnapped" person to verify their whereabouts.
- Request to speak with the victim and ask for "proof of life."
- Ask specific questions that only the victim would know the answer to.
- Request that the alleged victim call back using their personal cell phone.
- Try alternate methods of contacting your loved one.
- Do not mention the person's name on the call. Scammers may not know it, and providing the name only strengthens their deception.
- Do not pay the ransom.
- Most importantly, report suspected kidnappings to your local law enforcement agency or the FBI immediately.

Conclusion

Addressing virtual kidnappings requires international cooperation, public awareness campaigns, and enhanced cybercrime enforcement. Educating the public and establishing rapid reporting mechanisms can significantly reduce the success rate of these scams and improve financial recovery.

As virtual kidnappings continue to evolve, combating them will require global law enforcement collaboration, advancements in AI detection technology, and widespread public awareness to mitigate their impact effectively.

© 2025 ThreatRate Risk Management. All Rights Reserved



Risk intelligence that keeps you safe

ABOUT THREATRATE

ThreatRate helps you benchmark your risk management strategy against rapidly evolving global and local trends, with real-time, actionable analytics and insights.

For more information contact us at

info@threatrate.com

MEMBERS HAVE ACCESS TO

100+
risk-focused reports published annually

API
customised access option

Dashboards
customised dashboards and infographics

Experts
ThreatRate analysts with cross-industry depth

© 2025 ThreatRate Risk Management. All Rights Reserved

ThreatRate RISK MANAGEMENT