samphire

Virtual Kidnap

What is virtual kidnap?

‘Virtual kidnapping’ is described by the US Federal Bureau of Investigation as:

‘An extortion scheme - one that tricks victims into paying a ransom to free a loved one they believe is being threatened with violence or death. Unlike traditional abductions, virtual kidnappers have not actually kidnapped anyone. Instead, through deceptions and threats, they coerce victims to pay a quick ransom before the scheme falls apart.’

How does this threat manifest?

Typically, but not exclusively, a virtual kidnap manifests as follows:

- Perpetrators either target a specific person or organization or attempt to contact multiple random people one by one until contact is made.
- Contact could be by voice, direct message, email or social media.
- Contact could be via landline telephone, cell phone, personal electronic device or a computer.
- Once the perpetrator has made contact, details of the alleged kidnapped victim are provided, threats are made and a ransom demanded.
- Most usually, a relatively low financial demand for payment is made quickly to prevent checks being made on the victim’s location and welfare by the recipient of the call; primarily because there is no victim.
- Ransom payments are usually transferred electronically from a bank or by means of cryptocurrency transfer.
- Once payment has been received the person paying the ransom may or may not be informed that the victim has been freed.

Recent virtual kidnappings in Asia, Oceania and the Americas have been enhanced by:

- Using sound effects to increase the impact of a ransom call;
- Identifying victims before a ransom call is made and coercing them into providing virtual evidence of their kidnapping (most usually by using a social media live feed to show themselves tied up or under duress); or
- Identifying victims before a ransom call is made and coercing them into ceasing contact with their family before renting a hotel room and faking a hostage situation which is then live streamed to obtain funds from relatives overseas.

How can you mitigate the risk?

Despite the real and evolving threat of kidnap and virtual kidnap, there are some simple steps that can be taken to reduce the risk to both individuals and organizations:

- Train staff so they understand how a virtual kidnap threat manifests (as above) and can therefore recognize if a virtual kidnap may have occurred.
- Consider rehearsing processes and procedures in staff training in those locations where virtual kidnap is an issue (in a similar way to training that helps staff recognize the signs of a phishing scam).
- Support employees in sharing this training with family, friends, and their communities. As well as ensuring close personal contacts know how to recognize the threat, this can also send an indirect, but clear message to the wider community that your organization is vigilant.
- Advocate discretion and advise all staff to avoid discussing in public:
    - Travel itineraries and diary information
    - Personal and family information (including cell phone numbers)
    - Anything related to finances
- Encourage staff to consider:
    - Their online social media or website profiles
    - Their use of location-based services
    - Avoiding the use of ‘live’ location information and who they accept as ‘friends’
    - Monitoring tagged photos
    - The cyber threat associated with public WiFi, Internet cafes and Bluetooth
- Advocate the use of a ‘safe word’ that individuals would use if they are genuinely in danger.
- Educate staff so they know exactly what to do and how to behave if a ransom call is received eg. Demand immediate proof of life.

How should a ransom call be responded to?

- By taking simple measures to mitigate the risk, your staff should be better prepared to recognise the signs of a virtual kidnap particularly if no proof of holding the victim can be provided.
- Simply hanging up the call, or ceasing the means of communication used, will often be enough to bring the incident to a close.
- If staff are in doubt, there should be clear and simple guidance in place, so they know how, where and when to escalate an issue or concern internally.
- Following this, the intended target of the ransom demand should have clear guidance on how to feedback to the appropriate internal stakeholders the nature of the incident. This is an important step as it should allow for further learning around mitigating future threats of this nature.

About Samphire Risk

Samphire Risk was formed in 2021 and is a world-leading independent Managing General Agent (MGA) focused on insuring people and companies against hostile and malicious risks. Through an expert team and exceptional technology, Samphire aims to create world-class products that insure against extortive crime, hostage-taking and kidnap; terrorism in all its guises; travel into, and within, insecure countries and locations.

Contact us at info@samphirerisk.com if you have any questions regarding virtual kidnap. To find out more about Samphire please visit our website www.samphirerisk.com or follow us on LinkedIn.

Samphire and Samphire Risk are trading names of Samphire Services Limited which is an appointed representative of Davies MGA Services Limited, a company authorised and regulated by the Financial Conduct Authority under firm reference number 597301 to carry on insurance distribution activities. Samphire Services Limited is registered in England and Wales number 13421262. Registered Office: 1-3 Leadenhall Market, London, EC3V 1LR.