Provided by Risk Strategy Solutions

RISK ADVISOR

February 2024

COMMERCIAL

Tailgating and Piggybacking

Tailgating and piggybacking are low-tech tactics used by malicious actors to enter secure areas. They occur when an unauthorized person gains physical access to a location with sensitive information or vulnerable IT equipment. These intrusions can have significant financial and reputational impacts on businesses, so it is essential for companies to take measures to prevent these events.

Tailgating and Piggybacking Explained

Tailgating can occur when an intruder sneaks into a secure area by following an authorized employee. On the other hand, piggybacking is a type of social engineering technique that occurs when an intruder tricks an authorized individual into letting them into a secure area.

Once inside, the perpetrator can steal or view sensitive data, upload malware, take property or damage devices. Tailgating and piggybacking can lead to significant data breaches that create compliance violations and reputational damage, erode the trust of vendors and clients, and lead to costly fines and penalties. The following are examples of how these intrusions can occur:

- A perpetrator disguises themselves as a delivery person or contractor so an authorized employee allows them to enter restricted premises.
- An authorized individual holds the door open for the unauthorized person behind them.
- A malicious actor pretends to be an employee who has forgotten or lost their credentials.
- An intruder carries a bulky item in their hands, making them appear too full to open the door, or they pretend to be distracted while talking on the phone and follow someone inside.
- A trespasser acts as if they are a guest and even uses specific names of people in the office to appear legitimate.
- An unauthorized individual follows an authorized individual through a slowly closing door before the door shuts and locks.

Tips on Preventing Tailgating and Piggybacking

As part of a comprehensive approach to cybersecurity, businesses should implement measures to prevent tailgating and piggybacking. Consider the following strategies:

- Implement access control systems (e.g., badge readers and biometric scanners) and install physical barriers (e.g., turnstiles and security gates).
- Utilize surveillance cameras and video analytics.
- Maintain clear security policies and procedures and train employees on physical security awareness.
- Use visitor management systems for tracking and authorizing visitors.
- Conduct regular security audits to identify vulnerabilities.

Taking steps to understand and prevent these tactics can help reduce the risk of them occurring and offer financial and reputational protection. For more information, contact us today.

This document is not intended to be an exhaustive source of information nor should any discussion or opinions be construed as legal advice. Readers should consult legal counsel or a licensed insurance professional for appropriate advice.

Risk Strategy Solutions

AI’s Role in Virtual Kidnapping Scams

As artificial intelligence (AI) advances, criminals have developed ways to exploit the technology, such as leveraging AI in virtual kidnapping schemes. In these scams, criminals use AI to recreate an individual’s voice and make it sound like they have been kidnapped. A ransom demand for their release typically accompanies this. Businesses must be aware of virtual kidnapping and its impact on their companies and employees. These schemes can have significant financial consequences from the associated extortion and fraud and harm a company’s reputation if the company doesn’t know how to handle these situations. Moreover, virtual kidnappings can lead to severe emotional and psychological distress for involved parties. Therefore, it’s critical for businesses to be able to recognize, prevent and respond to these scams.

Virtual Kidnapping and AI Overview

Criminals can use AI to identify potential targets and create high-tech virtual kidnapping schemes. For example, a malicious actor may use recordings of a victim’s voice they found online and manipulate it by using an AI voice-cloning tool. This can make it sound like the victim is in distress, crying or asking for help. The criminal can then use the audio file when they contact the victim’s friends or family and demand payment for their release. They can also use additional editing tools to manipulate photos or videos to make the scam seem more realistic. The resulting content is sometimes referred to as a deepfake. Additionally, AI chatbots can utilize data about the victim to generate realistic conversations. These scams are a growing concern as the technology becomes more available and advanced, and identifying the content as forgery is becoming increasingly difficult.

AI and Virtual Kidnapping Scheme Recognition, Prevention and Response

Indications that a virtual kidnapping scheme may be taking place include a call coming from an unknown number, the caller creating a sense of urgency, and the caller demanding a ransom to be wired or sent digitally immediately. While businesses should not entirely dismiss the possibility that a kidnapping has taken place, they should take measures to prevent and respond to virtual kidnapping scenarios. Consider the following tips:

- **Provide education** to help employees recognize and address virtual kidnappings.
- **Be aware of what is put online to** reduce the amount of data perpetrators can leverage in a virtual kidnapping scam.
- **Verify information** by asking questions only the alleged kidnap victim would know.
- **Avoid sharing information** with the caller and consider hanging up if a virtual kidnapping scheme is suspected.
- **Try to contact the alleged victim** via text or another method to establish if they are safe.
- **Develop a safety plan and implement robust security strategies** to help create order in a potentially chaotic situation and minimize the potential of being targeted.
- **Do not agree to pay a ransom,** as doing so can encourage the perpetrators to repeat the scam and fund their criminal activities.
- **Secure kidnap and ransom insurance** to help offset the financial losses of a virtual kidnapping and obtain additional services.
- **Work with the authorities** on how to handle these situations.

For more risk management guidance, contact us today.

According to the FBI, the success of virtual kidnapping schemes depends on **speed and fear**. Criminals are aware that they **only have a short amount of time** to exact a ransom before the scam is detected or authorities become involved.