PHYSICAL SECURITY

A focused look into physical access and insider threats

THIS MONTH'S TOPICS:

With the growing digital landscape, it's easy to forget about one crucial element of data safety - physical security. It may not seem like a big deal to work from a coffee shop or let someone into your office, but these decisions could pose serious risks.

Unauthorized access often stems from a lack of physical security. Whether it's sneaking into a building or using a lost device to get into a system, there are many ways poor physical security could lead to a breach.

In this month's newsletter, learn more about physical security and the risks that come with unauthorized access.

Physical Security Defined

1 WHAT IS PHYSICAL SECURITY?

Physical security refers to keeping people, property, and information, safe from threats. In relation to cybersecurity, it prevents physical access to personally identifiable information (PII), which could be used against a company or person.

2 WHAT DOES IT INCLUDE?

Physical security measures include everything from locking an office door, to shredding documents that hold confidential information. Overall, it encompasses the measures that stop an unauthorized person from accessing information.

3 HOW DOES WORKING REMOTELY IMPACT PHYSICAL SECURITY?

Whether you are at home, or working on the go, it is important not to leave documents or devices open and unattended. Consider using a privacy screen and headphones when working in a public setting.

4 WHAT ABOUT THE OFFICE?

In the office, locking up files, computers, and removable devices, are important steps towards keeping information secure. If your office requires badges or keys to access the building, be aware of people trying to slip in behind you without credentials. Tailgaters aren't always malicious, but it is best to play it safe.

5 HOW HAS PHYSICAL SECURITY EVOLVED?

While the basics of physical security have been around for decades, there are new tactics cybercriminals are using to combine physical access with even more complex cyber schemes.

UNAUTHORIZED ACCESS

Unauthorized access and unintentional insider threats are growing issues. Let's dive into some of the evolving ways that physical and cyber security are colliding.

Wi-Fi Attacks

Some cybercriminals are getting physically close enough to a company's Wi-Fi network to gain access to the system. In one particular incident, the cybercriminal had access to an employee's exposed credentials and was able to log in by using a drone to connect to the company Wi-Fi.

Artificial Intelligence

Most employees know not to share private information online, however, the rise of AI chatbots has brought a new threat. Many employees are becoming unintentional insider threats by sharing company information with chatbots, which could then potentially store and share that data.

Connected Devices

There is an increasing variety of devices connected to the internet. If the devices used by critical infrastructure plants or medical practices are compromised, there could be serious impacts on the public. One case of unauthorized physical access or compromised credentials is often all it takes for many important devices to be compromised.

QUICK TIPS

- Do not share information with an AI chatbot that you would not post openly to everyone on the internet.
- Lock office doors, shred confidential documents before disposing of them, and get familiar with your company's breach response protocol.
- Keep keys and badges in a safe place. Do not share Wi-Fi passwords or leave log-in information out in the open.

SCAM OF THE MONTH

Each month we highlight a scam that demonstrates tactics criminals are using RIGHT NOW, to better prepare you when the next scam hits.

Felipe and Charlotte work together at a bustling financial firm. One Friday morning, Charlotte was running late. She was fumbling through her bag, looking for her key card but couldn't find it. Just as Charlotte was about to give up, she saw Felipe scanning his card at the entrance.

Charlotte called out to Felipe, and he held the door open for her. She thanked him and explained that she must have left her key card at home or in the car. Charlotte made it into the office just in time for her big meeting. The rest of the day went by like normal. She never found her key card but decided to figure it out the following week.

Unfortunately, the key card had been taken from Charlotte's unlocked car by a criminal. Later that night, the criminal was able to get into the office. Once they were in, the attacker used log-in credentials left on a sticky note at another employee's desk and gained access to all the company files and employee information.

Did you spot the red flags?

- Felipe let Charlotte "tailgate" by following him into the building without her own key card. This allowed Charlotte to forget about her missing key card instead of resolving the issue immediately.
- Charlotte left her car unlocked and another employee left account credentials out for everyone to see. This allowed for company information to fall into the wrong hands.

If you lose a key or any physical credential, notify your company immediately and follow the necessary steps to ensure physical security.

Keep work spaces clean to avoid misplacing important items or documents. Do not keep passwords on sticky notes or in visible places.

In addition to coworkers, tailgaters could be visitors or criminals. Criminals use our tendency to be polite and give people the benefit of the doubt to carry out their attacks. If you do not recognize someone who is trying to tailgate, direct them to the proper sign-in location, or depending on the circumstance, consider asking who or what they are looking for.

THE MONTHLY MASHUP

KEY TAKEAWAYS

While security threats online are as prevalent as ever, so are physical security risks. Keep devices in a safe place, lock files away, and monitor office access to keep data physically secure.

JOKE OF THE MONTH

What is a criminal's favorite part of a sporting event?

Tailgating!

AUGUST 31ST: TRAIL MIX DAY

Enjoy some trail mix today and remember that just like trail mix, security involves many parts to make a better whole. Physical security is a crucial part of your security mix.

PHYSICAL SECURITY CHALLENGE

Who has a riskier work environment?

1. SARAH

2. JEREMY

Answer: Jeremy

While Sarah's workspace has some distractions and potential for risk, Jeremy left devices and files open and unattended. His space is messy and could lead to lost files or unauthorized access.