Courtesy of
SCS Agency Inc

CYBERRISKS&LIABILITIES_

Juice Jacking Explained

Charging a battery through a free public USB charging station may seem innocuous, but doing so could result in costly cybersecurity issues. Through a tactic known as juice jacking, a malicious actor can gain access to an individual's device when they connect to these ports.

Since these charging stations are common in public places like airports and hotel lobbies, businesses should be cognizant of this threat. This is especially true of businesses with employees who travel with company devices and confidential data.

This article provides more information on juice jacking and offers tips on mitigating its associated risks.

Understanding Juice Jacking

Juice jacking refers to a type of cyberattack in which a malicious actor gains access to a device connected to a public USB charging station. Once the perpetrator has breached the device, they pose numerous threats, including the ability to steal data, load malicious software onto the device or disable it completely.

Although the Federal Communications Commission (FCC) reports that it is not aware of any confirmed cases of juice jacking, it notes that it has been demonstrated to be technically possible. This is because a USB port can be used to both charge a device and transfer data. In addition to the FCC's notice, the FBI's Denver office also issued a warning about the risks of using public USB ports due to the threat of juice jacking.

Tactics juice jacking perpetrators may use include embedding chips with malicious software into USB charging ports, tricking individuals into using infected cables designed to look legitimate or utilizing hardware that turns the connected device into a Wi-Fi access point that allows them to exfiltrate data.

The Risks of Juice Jacking to Businesses

With employees often conducting business on portable devices, juice jacking poses a threat to businesses. If a malicious actor gains access to employee devices through juice jacking techniques, confidential information may be compromised and costly equipment can be ruined. Installed malware may also allow a perpetrator to steal credentials and gain access to servers or clouds with additional business information, and it may result in the continuous siphoning of data.

These data breaches can have significant financial and reputational impacts on businesses. They may result in the need to pay legal and regulatory fees, fines and penalties and erode the trust and confidence of partners, vendors and clients.

Mitigating the Risks of Juice Jacking

There are several measures businesses and employees can take to reduce the risk of being the victim of a juice-jacking attack. These include:

- **Provide employee education.** Educating employees about cybersecurity threats, such as juice jacking, can help them be aware of these risks and learn how to mitigate them.
- **Avoid public charging stations.** Avoiding the use of public USB charging stations is a surefire way to eliminate the risks juice jacking presents. Ensuring devices are adequately charged before trips and employing battery-saving methods such as darkening the screen display can help accomplish this goal.
- **Use AC power outlets and a personal charger.** Bringing a personal charger and finding an AC power outlet to connect it to can allow employees to charge their batteries without having to rely on public USB ports.

SCS AGENCY
INSURANCE

This Cyber Risks & Liabilities document is not intended to be exhaustive nor should any discussion or opinions be construed as legal advice. Readers should contact legal counsel or an insurance professional for appropriate advice.

- **Carry an external battery pack or power bank.** External battery packs or power banks can hold enough energy to power devices, allowing employees to avoid public USB charging stations. Users should ensure they are storing and using these power sources in accordance with the manufacturer's instructions.
- **Carry a charging-only cable or USB data blocker.** A charging-only cable does not allow data to transfer, so users can add a layer of protection between the charging station and their device. Similarly, a USB data blocker is a small device that is plugged in between a user's device and a charging port to prevent data transfer while allowing charging.
- **Check security settings.** Individuals should review their device's security settings to ensure they are not set to allow automatic data transfer upon connection to an outside device.
- **Select "charge only."** If a message prompt appears when using a public USB charging station, users should only select the "charge only" option. They should avoid selecting options to "trust the charging device" or "share data" and make certain the device is locked while it is charging.
- **Keep software updated and patched and install antivirus protection.** Ensuring employees take standard cybersecurity precautions, such as ensuring devices are updated and patched and antivirus protection is installed, is essential in reducing the threats from cybercriminals.
- **Secure cyber insurance.** Obtaining cyber insurance can help mitigate the losses associated with juice jacking and other cyberattacks. A licensed professional can work with businesses and help them secure the coverage that best fits their needs.

Conclusion

As cyberthreats such as juice jacking continue to emerge, businesses must remain informed and vigilant. By taking measures to address cybersecurity risks, businesses can safeguard their data, mitigate potential financial losses and protect their reputations.

Contact us today for more information and cyber risk management guidance.