IBM Newsroom

IBM Security: Cybersecurity Threats Growing In Travel and Transportation Industries

Transportation grows to second-most targeted industry for cybercriminals in 2018; New survey finds that more than 70% of travelers have exposed themselves to cyber risks through high-risk behaviors

CAMBRIDGE, Mass., May 21, 2019 /PRNewswire/ -- IBM (NYSE: IBM) Security today issued new research highlighting that the travel industry and its customers are increasingly the targets of cyberattacks as criminals seek to monetize highly valuable travel data. Compounding the problem, a new survey conducted by Morning Consult on behalf of IBM Security[1] reveals that travelers are still blind to the risks they face on the road. The survey found that only 40% of respondents believed it was likely they would be targeted for cybercrime while traveling, yet 70% are engaging in high-risk behaviors while on the road.

Attacks in the travel and transportation industry are becoming more frequent, opening already unwary travelers to cybersecurity threats during their journeys. According to the 2019 IBM X-Force Threat Intelligence Index, the transportation industry has become a priority target for cybercriminals as the second-most attacked industry—up from tenth in 2017— attracting 13% of observed attacks. Since January 2018, 566 million records from the travel and transportation industry have been leaked or compromised in publicly reported breaches.

"Traveling has always been when people are more vulnerable. A few hundred years ago, the perpetrators were pirates or highwaymen. Now those criminals are still out there, but they've changed their methods to focus on digital attacks instead," said Caleb Barlow, Vice President of X-Force Threat Intelligence at IBM Security. "People carry a goldmine of data when traveling including passports, payment information and detailed travel itineraries. When placed in the hands of a cybercriminal, all of this information can be patched together into a complete picture of the traveler's life to inform identity theft, initiate spear phishing attacks, or be sold on the dark web."

Traveling a Dangerous Road

Traveling can make people more vulnerable to security threats than they are at home. On the road, people tend to be distracted and overwhelmed, often opting for convenience over security. At home, they may have safeguards like controlling physical access to devices and setting up firewalls to prevent digital intrusions, but on the road, they might be more exposed.

Morning Consult conducted an online survey on behalf of IBM Security to understand exactly how much risk travelers expose themselves to while away from home, and found most Americans engage in high-risk behaviors while traveling. More than 70% of Americans surveyed have connected to public Wi-Fi, charged a device using a public USB station, or enabled auto-connect on their devices which puts their information at risk.

Business travelers are even more likely to engage in risky behaviors. Nearly half (45%) of business travelers carry a device with valuable or sensitive information on it, yet business travelers admitted much more frequently to risky behaviors such as:

- Connecting to public Wi-Fi—42% of business travelers do this every time or very often vs. 34% for personal travelers do this every time or very often
- Charging a device using a public USB station—40% of business travelers do this every time or very often vs. 28% of personal travelers do this every time or very often
- Enabling auto-connect on their devices—39% of business travelers do this every time or very often vs. 30% of personal travelers do this every time or very often

Travelers are acutely aware of the risks to their financial information with more than half of those surveyed saying that they are extremely or very concerned that their credit card (53%) or other sensitive digital information (52%) will get stolen when traveling. That number drops significantly when they are not traveling, with only 40% similarly concerned that financial information will be stolen at home and 41% that their digital information will be stolen at home.

Digital Guardrails for a Safer Trip

As the 2019 summer travel seasons begins, it is important for travelers and travel and transportation companies to understand the threats facing them and take precautions to help protect their sensitive data. Cybercriminals are drawn to the travel industry because of the wealth of data it holds and the economic value it drives.

Travel is a profitable industry, with travelers spending $1.1 trillion in 2018 and supporting 15.7 million jobs in the U.S., according to the US Travel Association. This year, 43 million Americans will travel during the Memorial Day weekend to kick off the summer season, giving financially motivated hackers plenty of individual targets for their attacks.

Some digital safety tips for travelers include:

- **Monitor Loyalty Rewards:** Your loyalty information and rewards are as good as cash to cybercriminals. Monitor accounts for unusual activity, use strong passwords, set up multifactor authentication where possible.
- **Choose Your Wi-Fi With Care**: It's easy for cybercriminals to host Wi-Fi networks in public places to collect data such as credit card information and more. Even legitimate networks hosted by establishments can be open to digital eavesdropping. Avoid public networks if you can; and consider using a VPN for additional security.
- **Bring A Backup Battery:** Free USB power charging stations may come with a cost you can't see. Cybercriminals can modify USB connections to download data from your phone or install malware without your knowledge. Instead, bring your own battery bank to recharge your phone when you're low or use traditional wall plugs instead of USB ports.
- **Turn Off Unneeded Connectivity:** If you don't need it, turn it off. This includes Wi-Fi, Bluetooth, and auto-connecting to networks.
- **Shred Your Tickets:** The little scraps of paper from your tickets, boarding pass, luggage tag, or hotel folio may seem useless and harmless after you complete your trip, but savvy criminals can gather a lot of information about your loyalty rewards program from them. Be sure to save them until you can destroy them appropriately by shredding.
- **Be Smart When Paying:** Don't use your debit card at stores or restaurants that may not have the security to protect their point-of-sale systems. If you use an ATM, select one inside a bank branch or inside an airport, where the chance of tampering or skimmers on the ATM is reduced.

To learn more about travel and transportation security go to: https://www.ibm.com/security/industry/travel-transportation

The full Morning Consult survey results are available here: https://www.ibm.com/downloads/cas/ZP95XZ6O

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 70 billion security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide. For more information, please check www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM

Security Intelligence blog.

[1] Morning Consult conducted this online survey on behalf of IBM Security between April 23-24, 2019, among a national sample of 2201 U.S. adults.

Media Contact:
Kelly Kane
IBM Security Media Relations
kkane@us.ibm.com
413-297-2668

SOURCE IBM
