travel scams: they're not just for tourists anymore

equip your employees to survive travel scams while on assignment

If there is one thing you care about, it's your employees' experiences while relocating or on assignment. And, while you can't guarantee your employees won't fall victim to any number of common travel scams, you can certainly equip them to spot some big ones that could do a lot of damage – both to them and your company.

Enter "travel scams" into your web search engine, and you'll see pages and pages of search results, endless articles on common travel scams and how to avoid them, with even more helpful tips and comments provided by readers who have fallen victim to scams.

No matter how comprehensive your plan for assisting your employees in an emergency, you can't possibly prepare your employees for every scam. You can, however, prepare your employees to identify these three heavy-hitting scams, educate them around what they can do to protect themselves, and mitigate risk to your company in the process. If they know how to navigate these, they will likely better identify other common scams, as well.

1 identity scams

Place trust wisely: It is not uncommon for legitimate immigration authorities to check passports in public spaces. As a result, scammers have begun posing as immigration officials or police officers, and are known to stop people in public spaces, demanding to see their passports with the hope of stealing personal ID information (along with money). The uncertainty and threat of the situation can be scary and difficult to navigate. Many times, not even locals can tell if the person is an actual immigration authority.

There are a couple of strategies that can help your employees determine who is trustworthy. One – have them ask the immigration official to accompany them to the nearest police department (or even your company's office where there are known witnesses), where they will be happy to confirm their immigration status. If they refuse such an offer or insinuate that the passport isn't proper, this can be an indication of a scam.

Two – if the employee has already pulled out their passport, the immigration official should not be checking through or asking for other documentation, such as currency or credit cards. This should be a sure red flag.

How to recover: If your employee's passport is lost or stolen while moving or on assignment, they will need to file a police report right away, and keep a copy of the police report so that they can prove their identity if they are stopped again. Advise your employees to keep a copy of their passport with them in order to overcome any language barriers that would frustrate the process.

Make sure your employees know where their closest embassy is located. They will need to schedule an appointment to apply for a new passport.

Equip your employees with the right documentation to apply for a replacement. They will also need proof of citizenship and a primary form of identification.

2 money scams

Place trust wisely: A common scam used to target people who don't appear to be local is the ATM "helper." And, if your employee is using a corporate-issued credit card, your company is at risk as well. Inform your employees that anyone who offers to help them avoid local bank fees at an ATM is likely a scammer. ATM "helpers" are known to use card skimmers to fraudulently take card information, and then watch people enter their PIN. Make sure your employees know to cover the keypad of the ATM with one hand to protect their PIN. If your employee actually needs help, they will be better served at a bank, not at an ATM.

How to recover: Similar to a passport, if your employee's credit card information is lost or stolen while moving or on assignment, they will need to file a police report, and retain copies for their bank, credit card and insurance companies.

Your employee can then utilize their nearest embassy to receive wired funds to replace what was stolen.

3 data scams

Place trust wisely: Connecting to the internet can be a little different, and sometimes tricky, depending on the country. Hackers will set up unsecured Wi-Fi hotspots in public spaces, making it easy and tempting to connect to their network in the predictable desire to stay connected. Once your employee connects, hackers have access to all kinds of personal information on their computer, tablet or smartphone and, potentially, passwords and access to company information. Not to mention, your employee is open to large degrees of cyber-theft.

Make sure your employees are informed on data security practices such as only connecting to Wi-Fi connections they know to be official. You can also equip your employees with a Virtual Private Network (VPN), so they can stay connected with layers of added security and encryption. VPN companies offer a range of data security services, including VPN apps for smartphones, with the expertise to go along with it.

How to recover: If your employees suspect they may have fallen victim to this scam, make sure they have a clear set of steps to follow from your IT and data specialists, such as disconnecting from the Wi-Fi hotspot immediately, changing all passwords from a secure location, notifying their credit card companies and bank, and notifying your company's IT specialists.

Your employees are the most important asset to your company, and you can help them travel securely and confidently, keeping them on task and in high spirits.

For further insight into ensuring employee security on assignment, watch the video from Plus's thought leadership event on global terrorism and medical epidemics.