SIZZLING SUMMER SCAMS

May 2024| Issue 2024:5

SCAMMERS NEVER TAKE A HOLIDAY

The TSA PreCheck program is a trusted and reliable service offered by the Transportation Security Administration (TSA) to help expedite security screenings for eligible travelers at U.S. airports. The program allows pre-screened passengers to move quickly through security lines and avoid having to remove their shoes, belts, and light jackets or take laptops and liquids out of their carry-on bags.

Unfortunately, even the federal government is not exempt from cyber criminals. Fraudulent fake TSA PreCheck services, are now a real threat, either through online scams or in-person at airports. These scams are designed to trick travelers into paying for a false TSA PreCheck experience and may also result in the unauthorized sharing of personal information and payment details. It is one of the most prevalent travel scams these days.

In addition to encouraging people to sign up for the fake TSA PreCheck program, criminals also target those who want to renew their status.

To avoid falling for a TSA PreCheck scam and its variation, travelers should always go through the official TSA PreCheck enrollment or renewal process. This includes completing an application, undergoing a background check, and receiving a Known Traveler Number (KTN). The KTN is used when making flight reservations and helps the TSA determine if a passenger is eligible for TSA PreCheck.

Only renew your TSA PreCheck through the official channels to ensure security and avoid scams. If you believe you've fallen victim to a scam, report it to your local police and file a report with the Federal Trade Commission (FTC). Contact your bank or credit card company immediately to address any fraudulent charges. The TSA will not reimburse applicants who enroll through fraudulent websites.

Solomon Adote
Chief Security Officer

ON THE GO? SO ARE CYBER CRIMINALS

Ready, Set. Go! Summer vacation time is almost in full swing. As you are making plans, be on the lookout for these summer spoiler scams.

Fake Rental Properties - Vacation rentals are great options for traveling and still having the comforts of home. Watch out for listings for properties that either aren't for rent, don't exist, or are significantly different than pictured. Con artists lure in vacationers with the promise of low fees and great amenities. The "owner" creates a false sense of urgency – such as telling potential clients that another vacationer is interested in the rental – to get a quick "deposit" before the client has time to sufficiently research the validity of the offer.

Talk with the owner by phone. If you are not using a service that verifies properties and owners, do not negotiate a rental solely by email. Speaking with the owner on the phone, asking detailed questions about the property, and local attractions will clarify if the listing is true. An owner with vague answers is a red flag. Investigate online by looking up the address and use Google Street View to confirm the property matches the one advertised. Also, verify distances to beaches, attractions and airports while on the site.

HOTEL SCAMS - According to estimates by the American Hotel & Lodging Association, approximately 15 million online hotel reservations are made on bogus third-party sites every year. These rogue websites trick people into thinking they're reserving directly with their hotel of choice. Instead, the victims are making reservations on phony sites set up to steal their credit card information. With cybercriminals pocketing more than $1.3 billion in fake hotel reservations, consumers need to beware when booking hotel rooms and other travel reservations online — such as for airline flights and rental cars, too.

When staying in a hotel watch out for these tricks:

Fake Front Desk Calls: Scammers call late at night impersonating the front desk person. The caller claims there's a problem with the card on file and asks the traveler to "re-verify" the credit card information.

"Free" Wi-Fi Connections: Wi-fi "skimming" is a growing scam that targets travelers with the promise of free Internet access. Scammers set up a fake connection that appears to be free, but it's not safe. They will control the connection through their computer, collect all the data the traveler transmits.

Fake Food Delivery: Scammers will distribute fake menus to hotel rooms. When a traveler calls to order delivery, the callers' credit card information is collected, and the food is never delivered.

READ MORE CYBERSECURITY NEWS at DIGIKNOW!

Delaware Department of Technology & Information publishes and sends this newsletter to all network users because we need YOUR help to keep our network secure. If you are having problems viewing this message, accessing the links or want to print a PDF copy, go to:https://digiknow.dti.delaware.gov/news/index.shtml?dc=newsletters

Department of Technology and Information
Contact us at **esecurity@delaware.gov**