Hotel Guests Beware - New Scam Makes You an Easy ID Theft Target

September 3, 2013 - Whether you travel for business or pleasure, you probably don't think that the simple act of staying in a hotel as something that would make you a prime target for identity theft. But there is a new scam that is spreading and it is remarkably simple for thieves to pull off. Moreover, if you are one of the millions of people who post information about your travel schedule to social media sites, you could easily be setting yourself up for victimization.

Tweet

(function() {
var s = document.createElement('SCRIPT'), s1 = document.getElementsByTagName('SCRIPT')[0];
s.type = 'text/javascript';
s.src = 'http://widgets.digg.com/buttons.js';
s1.parentNode.insertBefore(s, s1);
})();

(function() {
var po = document.createElement('script'); po.type = 'text/javascript'; po.async = true;
po.src = 'https://apis.google.com/js/plusone.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(po, s);
})();

The scam is very simple. An identity thief calls the front desk of a hotel and asks to be put through to a specific room number. If the hotel guest answers the phone, the caller poses as someone working at the hotel front desk and tells the guest that there is an issue with their credit card. The guest is then asked to provide the card number, their name as it appears on the card and its security code over the phone. And just for good measure, can you please confirm your billing address? In a matter of 20 or 30 seconds, the guest has given the caller everything they need to start charging up a storm.

While many hotels require callers to give the guest's name before putting a call through, others may not. And even if that is a requirement of the hotels that you stay in, getting that information could be as simple as searching Facebook, LinkedIn or any other social media site that you post to.

Millions of people use social media sites every day. And it is quite common for people to post information about what city they are visiting and which hotel they are staying in. ID thieves know this and they are looking for ways to use that information.

If you use your real name on social media sites, and you post the type of information referenced above, then you are really issuing an open invitation for crooks to target you.

But even if you don't post all of the details of your life online, you could still find yourself receiving one of these calls while staying in a hotel. It could be that your hotel doesn't require callers to provide the name of the guest they are calling. Or it could be that the person at the front desk is new, inexperienced, exhausted, etcâ€¦ and they forget to ask the caller for the name of the guest. If the call gets through to your room, the reason it gets through is much less important than your reaction to it. Luckily, as simple as this scam is to execute for the crooks, it is just as simply defeated.

Anyone who receives this type of call should simply refuse to provide their information over the phone. You don't even

need to be rude about it. Simply say that you will come right down to the front desk and provide the information in person. Then get off the phone.

By taking this approach, if the call was legitimate it will only take a couple of minutes to find out. And if the call was a scam, you will save yourself from countless hours of trying to straighten out your credit record after you've become a victim.

byJim Malmberg

Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.

Follow me on Twitter:

Follow ACCESS