The Massive Marriott Data Breach: Some Practical Advice For Business Travelers

If you have stayed in one or the following hotels in the last 4 years, it's very likely that your personal data—and even potentially your passport number—has been stolen and is available to the bad guys so they can use it for a raft of nefarious purposes. Apart from the Marriott brand, the Starwood hotels own the following brands:

- Westin
- Sheraton
- The Luxury Collection
- Four Points by Sheraton
- W Hotels
- St. Regis
- Le Méridien
- Aloft
- Element
- Tribute Portfolio
- Design Hotels

I would estimate that's a very high percentage of all U.S. and Europe business travel. It's prudent to prepare for the worst. Assume your data is compromised and be on the lookout for a variety of social engineering attacks.

Here are four things to watch out for, and one thing you can do right now to protect yourself while traveling

1) Spear Phishing Alert

Starwood Preferred Guests accounts have been compromised, which means that both your business and possibly your personal email addresses can be misused. It is heaven for the bad guys because now they can create very convincing travel-related phishing emails with this type of detailed information. Watch for those in your inbox and immediately delete, or report them to your Incident Response team.

2) Copycat Phishing, Vishing or SMShing

Various flavors of cyber criminals are going to jump on this bandwagon whether they actually have access to your compromised account or not.

Marriott said it will email Starwood Preferred Guests and those who may be impacted, so bad guys are going to make exact copies of that email, but with one or more malicious links in it. Do not click on links in emails or other (social media) communications that seem to have come from Marriott or any Starwood hotels. Do not open any documents that might be attached.

Also, remember to not respond to voice mail messages, robo calls or text messages that claim they are from any of the above hotels, because bad guys may use this massive data breach to attack you using your phone too. Look up the correct phone number and call the hotel—yes, old-style talking to someone— to confirm your business.

3) Have A Chat With Accounting

If you have a business credit card—and many of us do—the bad guys may have access your encrypted credit card information. At this point it's not sure yet if the criminals are able to use these numbers. In any case, ask Accounting to monitor your credit card for any suspicious activity. As a safety precaution, they should change the password they use to online manage business credit card accounts.

If you use your own credit card and get reimbursed for business travel, also monitor your account closely for unauthorized charges, change the password or call your credit card company and ask for a new card. Never use the same password for any financial website, and if you did, immediately change the password on those websites. As a best security practice, always choose a different, strong password for each sensitive account, better yet, use a password manager.

4) Do Not Search Google For “WebWatcher”

Marriott is offering victims in the USA, UK and Canada a free, one year subscription to a Kroll Identity Service called "Web Watcher". They call this a service that monitors "internet sites where personal information is shared", meaning they monitor hacking sites on the dark web for compromised data records.

However, don't Google "Web Watcher", because you will find lots of links to parental monitoring—really spyware—of the same name. If you decide to sign up for Marriott's free monitoring, follow the links at at info.starwoodhotels.com to country-specific versions of that service.