KnowBe4
Human error. Conquered.

Security Awareness Training Blog

30
Nov

[Heads-up] Bad Guys Love Marriott: 500 Million Data Breach Is Phishing Heaven

Stu Sjouwerman

So I guess we have just reached the tipping point, it's "privacy game over" for business travelers.

For about 327 million of the 500, the breached data includes names, mailing addresses, phone numbers, email addresses, passport numbers (!), Starwood Preferred Guest ("SPG") account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences.

The company said in a statement that it discovered "unauthorized access" to the database, which extended back until 2014.The hacker had copied and encrypted information and "took steps toward removing it," Marriott said.

In some cases, payment card numbers and expiration dates were also taken, but Marriott said it's unclear whether the hackers have information to decrypt the payment card numbers.

Marriott said it has set up a website for consumers impacted by the hack, at info.starwoodhotels.com, and a call center. "Call volume may be high, and we appreciate your patience," the company said. NPR mentioned that Starwood would send an email to all addresses affected.

Here is where the bad guys come in.

You can expect a raft of phishing attacks that try to exploit this data breach, either by using just scare tactics, or by using actual data from the breach itself to make it look as real as possible.

If you are a KnowBe4 customer, we strongly recommend you inoculate your users and send a simulated phishing attack to your users that uses this Marriott data breach as the theme.

Two new phishing templates have been added to our Current Events phishing templates category in light of the recent Marriott data breach which affected up to 500 million customers. Use them to prepare your users before the bad guys use social engineering tactics and trick them. Each template leads to a fake Marriott login page to mimic a credentials phishing attack.

Template names:

- Marriott: Data Breach Notification (Link) (Credentials Landing Page)
- Marriott: We're sorry. Here is a free 2-night stay at any Marriott location. (Link) (Credentials Landing Page)

A Marriott landing page has also been added to the Data Breach category and is associated with each of these templates.

- Marriott Login Page

Grab these template and landing pages and send it to either all users, or if you have a Smart Group containing your Frequent Travelers, that would be the first priority.

if you are not a KnowBe4 customer yet, we suggest you step your users through this free module that is available until the end of December 2018!

“Safe Travels For Road Warriors" is a 12-minute animated course with lots of interactivity for those that travel for business—and some very helpful tips for personal travel too. We believe this is a very good new module, we have been working on internally for a long time, with input from experts like Kevin Mitnick. You will step through what to do:

- Before Leaving the Office
- While Packing
- In the Taxi
- At the Airport
- In Flight
- At meetings and Conferences
- At the Hotel

This module is 12 minutes in length. Free Access during November and December 2018.
Click here to launch the module

The purpose of this course is to make learners aware of the latest threats to security for the modern traveling business person. This course will also provide strategies and practice advice for traveling safely.

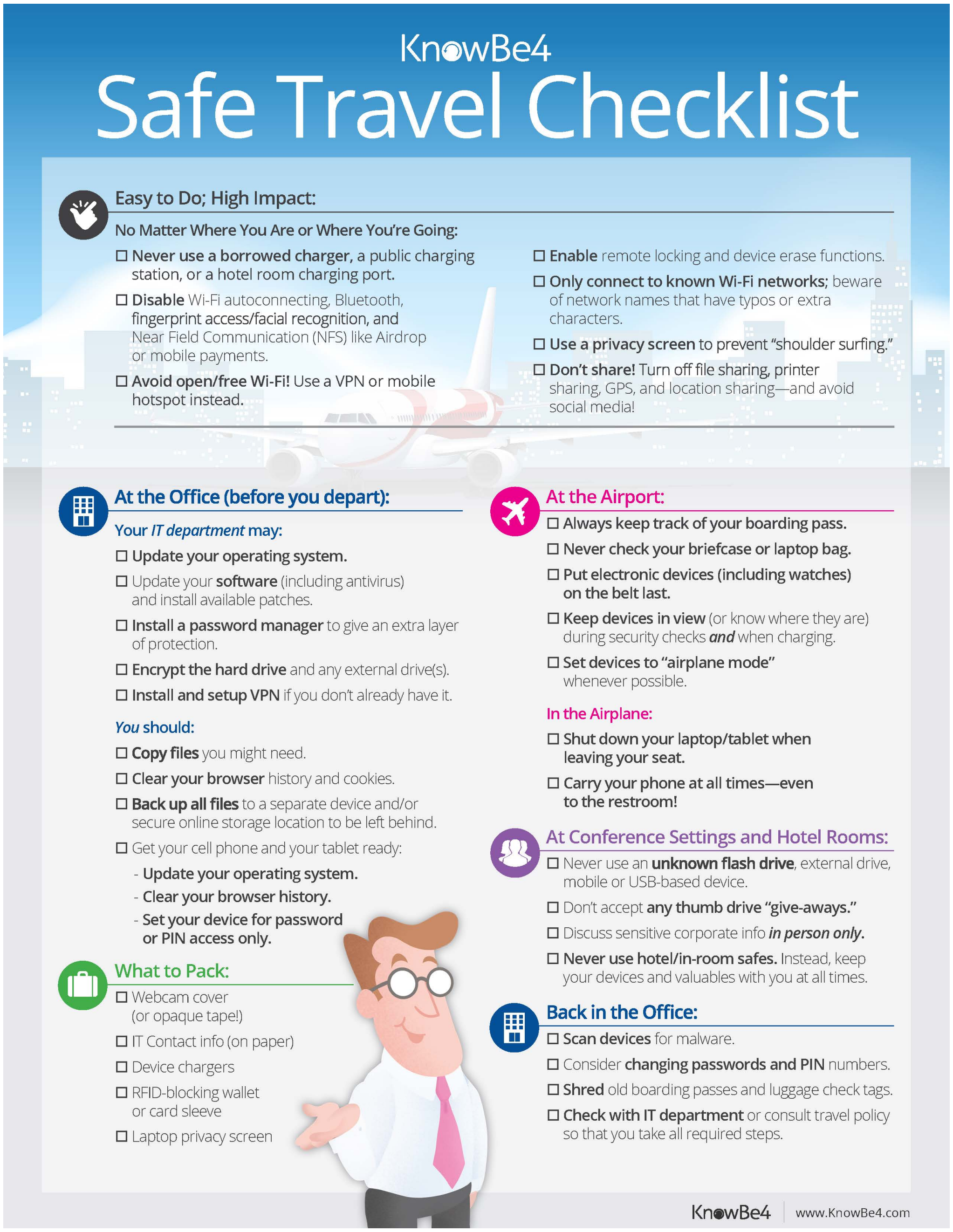
The module objectives are:

- Be aware of the latest potential security pitfalls when traveling for business (and some tips you should consider personally)

- Know how to properly prepare for a business trip and avoid exposure of business, client, or even personal information.
- Strategies and practical steps that can be taken to mitigate security concerns that can arise while traveling.

Printable resources—and we suggest you grab the PDF from the module, print and laminate it and give it to all your frequent travelers. It's the whole module summarized on just one page, incredibly handy. Here is the PDF as a free job aid you can give to your employees.

We strongly recommend to step Board members, C-levels, and any business traveler through these 12 minutes. I guarantee that even the most savvy road warriors will learn a few new tricks!



KnowBe4

Safe Travel Checklist

Easy to Do; High Impact:

No Matter Where You Are or Where You're Going:

☐ **Never use a borrowed charger,** a public charging station, or a hotel room charging port.

☐ **Disable** Wi-Fi autoconnecting, Bluetooth, **fingerprint access/facial recognition, and** Near Field Communication (NFS) like Airdrop or mobile payments.

☐ **Avoid open/free Wi-Fi!** Use a VPN or mobile hotspot instead.

☐ **Enable** remote locking and device erase functions.

☐ **Only connect to known Wi-Fi networks;** beware of network names that have typos or extra characters.

☐ **Use a privacy screen** to prevent "shoulder surfing."

☐ **Don't share!** Turn off file sharing, printer sharing, GPS, and location sharing—and avoid social media!

At the Office (before you depart):

Your *IT department* may:

☐ **Update your operating system.**

☐ Update your **software** (including antivirus) and install available patches.

☐ **Install a password manager** to give an extra layer of protection.

☐ **Encrypt the hard drive** and any external drive(s).

☐ **Install and setup VPN** if you don't already have it.

You should:

☐ **Copy files** you might need.

☐ **Clear your browser** history and cookies.

☐ **Back up all files** to a separate device and/or secure online storage location to be left behind.

☐ Get your cell phone and your tablet ready:

- **Update your operating system.**
- **Clear your browser history.**
- **Set your device for password or PIN access only.**

What to Pack:

☐ Webcam cover (or opaque tape!)

☐ IT Contact info (on paper)

☐ Device chargers

☐ RFID-blocking wallet or card sleeve

☐ Laptop privacy screen

At the Airport:

☐ **Always keep track of your boarding pass.**

☐ **Never check your briefcase or laptop bag.**

☐ **Put electronic devices (including watches) on the belt last.**

☐ **Keep devices in view** (or know where they are) during security checks ***and*** when charging.

☐ **Set devices to "airplane mode"** whenever possible.

In the Airplane:

☐ **Shut down your laptop/tablet when leaving your seat.**

☐ **Carry your phone at all times—even to the restroom!**

At Conference Settings and Hotel Rooms:

☐ Never use an **unknown flash drive**, external drive, mobile or USB-based device.

☐ Don't accept **any thumb drive "give-aways."**

☐ Discuss sensitive corporate info ***in person only***.

☐ **Never use hotel/in-room safes.** Instead, keep your devices and valuables with you at all times.

Back in the Office:

☐ **Scan devices** for malware.

☐ Consider **changing passwords and PIN** numbers.

☐ **Shred** old boarding passes and luggage check tags.

☐ **Check with IT department** or consult travel policy so that you take all required steps.

KnowBe4 | www.KnowBe4.com