



# BSD Information Security



## Cyber Safe Traveling

### In this issue of the BSD ISO Cybersecurity Newsletter...

- **Cyber Safe Traveling** – Cyber criminals don't take the holidays off and are ready to take advantage of travelers during the holiday season when they have their guard down. Whether you're taking a personal holiday or a business trip, traveling by car or by plane, planning a quick jaunt or preparing for an extended stay, make sure your cyber security best practices are coming along for the ride. Read the following story about how Lydia stayed cyber safe while traveling. (*Page 1*)
- **What's NEW ...**
  - **Phishing Awareness Assessment** - As you know, we take information security seriously. As part of our ongoing security awareness program at times we will assess the Biological Sciences Division's understanding of cyber security. In the upcoming months, the BSD Information Security Office will kick off a Phishing Awareness Assessment. Please read the Phishing Awareness section for more information about this assessment. (*Page 2*)

### Cyber Safe Traveling

"Why did I wait until the last minute to pack?" Lydia muttered angrily to herself as she hurriedly threw clothes on the bed. It was going to be a crazy trip: to her parents in Minnesota for the holidays, then a medical conference in Orlando, followed by a week's vacation in the Caribbean. How do you pick outfits for that range of climates?

#### Additional Resources

For more tips on traveling safe, see the following resources:

- Department of Homeland Security - [Cybersecurity While Traveling Tip Card](#)
- US-CERT (Computer Emergency Readiness Team) - [Holiday Traveling with Personal Internet-Enabled Devices](#)
- BSD Information Security Policies Web Page - <http://security.bsd.uchicago.edu/Security-Policies>

Frantically, Lydia pulled her largest suitcase off the top shelf of her closet. As she awkwardly lugged it down to the floor, a piece of crumpled brown paper fell out, bouncing off her cheek. "What's this," she wondered, scooping it off the floor and smoothing it out, "some kind of list?"

"TRAVELERS BEWARE..." it read in suspiciously red-brown, jagged handwriting, across the top of the page. Lydia had never seen it before, and was frankly kind of grossed out, but some mysterious force drew her eyes to read the items below.

...OF SOCIAL MEDIA

"Social media?" Lydia asked out loud, but suddenly, a vision of a stranger sneaking into her office and turning on her computer flew through her mind, followed by a Facebook post of her on a beach with the caption "Having a great week!"

## ...OF PUBLIC COMPUTERS

Another vision, this time of Lydia checking her e-mail at a workstation in a hotel lobby, only to be replaced by a woman who logs in and accesses her passwords through a keylogger program.

## ...OF PUBLIC NETWORKS

Lydia sees herself in an airport terminal, desperate to download a new book on her tablet before her flight, and trying every available wifi network in range. Finding one that works at last, she quickly downloads the latest bestseller, while a scruffy teenager nearby smiles at his laptop as her credit card information pops up on his screen.

## ...OF UNATTENDED DEVICES

Fading in to a hotel pool, where Lydia watches herself put her smartphone in the pocket of a beach bag, then jump into the deep end for some morning laps. As she turns her back, an employee slips by and smoothly plucks her phone from the bag, gaining access to her e-mails, texts, and documents -- and the work and personal information they contain.

Suddenly, the wrinkled parchment glowed bright orange, then disappeared in a poof of smoke. Chilled, Lydia put aside her hurried packing, and decided to take precautions. She installed locator apps on her phone and tablet, so that she could track them if stolen, and even wipe their hard drives remotely. She turned off the wifi and Bluetooth auto-connect on her devices and laptop, so that she didn't unknowingly log onto to any insecure networks. And she called her credit card company to let them know she would be traveling, so they could monitor for fraudulent activity.

Where the mysterious list came from, she'd never know. But at least one travel preparation -- her data security -- wasn't going to wait until the last minute.

## **Phishing Awareness**

---

As you know, we take information security seriously. As part of our ongoing security awareness program, at times, we will assess the BSD's understanding of cyber security. In the upcoming months, the BSD Information Security Office will kick off a Phishing Awareness Assessment. A phishing awareness assessment is nothing more than when we send out an email pretending to be a hacker; these are the very same email attacks that the bad guys are sending. The only difference is these emails will not harm you in any way, they are only designed to measure behaviors and help you learn how to identify these scams and protect yourself.

A couple of key points:

- We will send out these emails to every BSD employee.
- If you fall victim to one of these phishing emails you will be notified immediately and you will be enrolled in phishing awareness training.

If you have any questions about this program or suggestions on how to improve it, please contact the BSD Information Security Office at [security@bsd.uchicago.edu](mailto:security@bsd.uchicago.edu).

## **What to do if you become aware of an information security incident?**

---

Contact the BSD ISO Team via email at [security@bsd.uchicago.edu](mailto:security@bsd.uchicago.edu).

### **Information Security Office Team**

Plamen Martinov, Chief Information Security Officer

O: 773-834-1714

[pmartinov@bsd.uchicago.edu](mailto:pmartinov@bsd.uchicago.edu)

Kim Cooke, IT Security and Compliance Analyst

O: 773-834-7897

[kcooke3@bsd.uchicago.edu](mailto:kcooke3@bsd.uchicago.edu)