SAFE TRAVELER™ COURSE
Self-Paced Training

BLACK HORSE

a **PARSONS** Company

Course Overview

The Safe Traveler™ Course is an online lecture series focused on delivering best practices for travelers, Military members, and executives on business who are at risk of becoming soft targets for cybercriminals. Safe Traveler™ training modules teach students to take proactive steps against adversarial threats by learning how to secure personal devices across physical, digital, and network data environments.

Safe Traveler courses utilize hands-on practical scenarios and instruction covering tactics, techniques, and tradecraft where learning new skills is the focus, as opposed to learning technology or tools. Safe Traveler is designed for students to improve their personal security with computer and mobile devices both at home and abroad, via a uniquely designed curriculum which provides students with cutting edge best practices. Current and former Safe Traveler clients include Fortune 100 companies, elite Special Operations Units within the Department of Defense (DoD), Law Enforcement Agencies, and Intelligence Community (IC) partners.

Framework and Skills Taught

Safe Traveler teaches students a comprehensive signals reduction methodology that can be applied with the use of various tools and applications to protect both personal, professional, and operational information via a self-paced, online curriculum.

Safe Traveler: Quick Facts

- Self-paced, module-based online curriculum to enable training from anywhere.

- 30-access license for students to conduct learning at their own pace.

- Use of video and hands-on practical scenarios for students to test techniques at home.

- Digital security tradecraft is applicable to personal and work travel.

The Safe Traveler Difference

Thinking Person's Course – Students learn how to think about security through threat modeling; not every scenario calls for every tool.

Tool Agnostic – No dependence on a given application, hardware, or software. Students will be taught how to evaluate tools for themselves.

No Fluff – You won't find history lessons or offensive techniques here; We will teach you actionable tools, techniques, and procedures.

"Just how much am I at risk when I travel overseas, and what can I do to protect myself?"

- -Private Equity Manager

According to recent cyber security surveys:

- People travelling abroad are more likely to be robbed of their data (one in five generally, and three in 10 senior business managers)
- Old habits die hard and 44 percent of people go online by the time they leave the airport, regardless of security risks
- 82 percent of travelers connect to unsecured public Wi-Fi networks (e.g. travel terminals, hotels, cafes, and restaurants)
- 69 percent connect after they land in order to let family and loved ones know they have arrived safely
- Three in five travelers (61 percent) spend the same amount of time – or more – searching for information on the Web when they are abroad
- Almost three in 10 travelers (28 percent) admit they have left devices unsupervised in public spaces
- 41 percent of official travelers expect their employers to have set strong security measures. "Indeed, the view from the top is that, if employers are to send staff overseas, they must accept any security risks that go with it."
- Half of all travelers (50 percent) indicate they made no distinction between their online activities when travelling for work or leisure

ref: https://resources.infosecinstitute.com

Safe Traveler™ Course Deliverables and Schedule $500 per license

Training Modules

Basic Computer Security
- UAC/PLP
- OS and Application Updates
- Anti-Virus/Anti-Malware
- Windows Telemetry Mitigation

Account Authentication
- Creating better passwords
- Password managers
- Multifactor Authentication

Protecting Data at Rest
- AES encryption
- Full disk encryption
- File encryption

Browser Hardening
- Creating a more secure web browsing experience

Protecting Data in Motion
- Threats to data-in-motion
- Transport layer security
- Virtual private networks

Mobile Device Threats
- What is a smartphone?
- Metadata
- Location Tracking (historical/Near Real Time)
- Traffic Interception
- Camera/Mic Hijacking
- Malware
- Hardware Exploitation

Mobile Device Personnel Security
- Mobile Hardware Hardening
- Malware Defense
- Protecting Traffic
- Hardware Defense

Basic Identity Management
- Social Media Hardening
- Mobile OS Security
- Facebook
- Twitter
- Instagram

End of Course Exercise: Two individual exercises designed to test your new abilities in responding to real world challenges.

Certificate of Training Completion

Students who successfully graduate from CSR courses will be eligible to become certified. Once all certification requirements are met and evaluated by BlackHorse, students will receive a certificate recognizing their proficiency in the skills and methods acquired during the program.

Al Merino / Vice President Technical Operations
6415 Brookstone Ln #104 & #201, Fayetteville, NC 28314
Al.Merino@blackhorsesolutions.com / (910)-286-1743

More Info and Enrollment!

We offer the option to create a contracted, dedicated course to meet your organization's operational requirements.

For contracted training, open enrollment course information, and price quotes please send all inquiries to

TOGTraining@blackhorsesolutions.com