

# USBGuru Memory Device Attack Simulation Service

## Assess vulnerability and train employees about the appropriate use of memory devices

### Simultaneously Assess and Reduce Vulnerability to Attack

Targeted attacks and advanced persistent threats continue to target the human element within organizations. It is widely recognized that employees are the weakest link in cyber security. While many companies perform penetration testing annually to determine organizational vulnerabilities to attack, determining vulnerability and working to reduce it have been two separate actions.

Better than a Pen Test, Wombat's USBGuru™ not only assesses user vulnerability but also trains users who fall for the attack. USBGuru is one of Wombat's Social Engineering Assessment services that applies our proven simulated attack methodology to removable memory devices. Security officers can simulate an attack by placing USB drives, loaded with custom executable files, around the office to assess employee vulnerability. The moment someone accesses the file on the USB drive, their identity is captured and they are presented with immediate brief training about USB attacks and how to avoid them.



### Don't just Pen Test, Create a Teachable Moment

Wombat's USBGuru is a software-as-a-service product that enables security officers to assess employees and train them not to use removable memory devices of unknown origin. Security officers use Wombat's cloud-based interface to easily create a custom executable file with a brief training message embedded in the file. The executable file is saved onto removable memory devices which can be distributed to any location around the organization.

When an employee plugs the USB drive into their computer they will be presented with just-in-time training. The training message will explain the risks associated with removable memory devices and provide practical advice to the employee. The USBGuru administrator interface provides detailed reports for security officers to know who is most susceptible to memory device attack, track individual devices, report training completion, and be able to group the susceptible individuals for follow up.



**wombat**  
security technologies

**USB Training**  
Exploring the dangers of USB Drivers

**How Dangerous Can USB Drives Be?**  
If you aren't careful you may....

Accidentally disclose sensitive corporate or personal information  
Install a virus onto your computer

+

### What can USBGuru do for you?

- Determine the organizational risk of rogue memory devices
- Show which employees are most susceptible to these attacks and who should receive additional training
- Provide a teachable moment that ensures employees will follow company policy and only use USB devices from IT
- Increase acceptance of follow-on security awareness training
- Protect corporate networks from Malware, Spyware and other malicious software

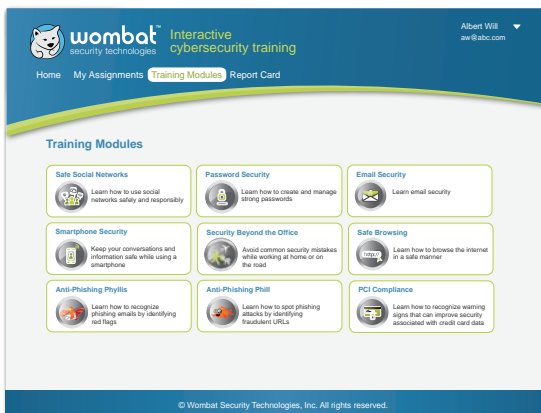
# USBGuru Memory Device Attack Simulation Service

## Assess vulnerability and train employees about the appropriate use of memory devices

### Our Security Training Platform

The USBGuru™ service is just one of the security assessment and training tools available in the Wombat Security Training Platform that enables security professionals and administrators to assess employees, deliver training, track results, and improve their cyber security posture.

The Platform provides a complete library of 10-minute long, interactive and highly effective training modules on topics such as phishing, data protection, smartphones, creating strong passwords, working outside the office, Internet browsing, and social networking. Reporting capabilities in the Platform provide both aggregate and individual user data to guide follow-up training programs and show improved results over time.



Our training modules are software-based, very interactive, and capture data as users practice critical concepts.

The Platform provides a complete library of 10-minute long, interactive and highly effective training modules

### Why choose Wombat?

- **Assessment and training methodology is based upon scientific research in cyber security and learning science**
- **Learning science principles ensure users learn key concepts and retain content much longer**
- **Mock attacks and interactive software-based training modules can be delivered throughout the year to ensure a continuous learning environment and behavior change**
- **Detailed data is captured from every learning tool to provide security posture intelligence**
- **Software-as-a-service assessments and training are easy to deploy and provide seamless content and functionality updates**

To learn more about our Social Engineering Assessments and our Security Training Platform contact Wombat today!



[www.wombatsecurity.com](http://www.wombatsecurity.com)

Phone: +1-412-621-1484

Fax: +1-412-621-1489

4620 Henry Street, Third Floor  
Pittsburgh, PA 15213