Technical safeguards like firewalls, antivirus software, and email filters are critical for defending your infrastructure, but they cannot prevent one pervasive threat: user error. The simple truth is that successful social engineering attacks — like those perpetrated through phishing emails, malicious SMS/text messages, and infected USB drives — hit their targets because users make poor decisions.

Organizations that are strictly reactive only learn about their vulnerabilities during the aftermath of successful attacks. When you engage with Wombat, you gain the ability to be proactive. Our ThreatSim®, SmishGuru®, and USBGuru® simulated attacks allow you to assess your levels and areas of susceptibility — and begin to mitigate threats — in a safe, controlled manner.

Though our assessments can be used as standalone tools, we advise our customers to take a wider view of security awareness and training and follow simulated attacks with our interactive training modules. Our unique Continuous Training Methodology combines assessments with education, reinforcement, and data measurement to change employee behaviors and reduce risk. Customers who have used this approach have experienced up to a 90% reduction in successful phishing and malware attacks.
Key Benefits of Wombat Simulated Attacks

- Safely evaluate how your employees respond to phishing and spear phishing emails, malicious SMS/text messages, and infected/unauthorized portable storage devices.
- Establish a baseline vulnerability measurement that you can use to gauge progress.
- Analyze data gathered during assessments and education, and use that information to plan your future security awareness and training efforts.
- Prime your employees for follow-up education. Add our interactive training modules to your license and use them to teach your staff to recognize cyber security threats and react appropriately to keep data and systems safe.

ThreatSim: Simulated Phishing Attacks Expose Real-World Vulnerabilities

Every day, new phishing emails reach employee inboxes, in spite of spam filters and other technical safeguards. With fraudsters becoming more sophisticated, it’s more important than ever to teach employees how to identify, avoid, and report malicious emails.

A software-as-a-service product, ThreatSim gives your employees a firsthand understanding of email scams — and the consequences of clicking. Users can then put that knowledge to work to protect data and systems.

As an added benefit, our PhishAlarm® email reporting button allows employees to participate in prevention. This email client add-on is simple and intuitive, allowing users to report suspicious emails with a single mouse click. Anyone who reports a suspicious email is immediately rewarded with a “thank you” pop-up message or an email that encourages this behavior in the future.

PhishAlarm allows users to quickly and effectively alert security and incident response teams to suspected phishing emails, which can help stop an attack in its tracks.

The ThreatSim Assessment and Education Cycle
What ThreatSim Can Do For You

**Reveals knowledge gaps** – Our mock attacks will give you a clear sense of how well your employees identify — and avoid — phishing and spear phishing emails.

**Simulates key attack scenarios** – Customizable email templates test three common attack methods: attachments, embedded links, and data entry requests.

**Allows testing of multiple messages** – Themes in our template library include banking, social networking, seasonal messages, IT prompts, and simulations of attacks from the wild. You can also write your own emails, which is ideal for assessing known issues.

**Provides just-in-time teaching** – Employees who fall for a mock attack receive an explanation and brief, practical tips via our customizable Teachable Moments (see graphic).

**Randomizes email distribution** – Our Staggered Delivery feature spreads out and randomizes mock attack deliveries. This minimizes the impact on your email servers and IT helpdesk, and reduces the likelihood that employees will figure out — and discuss — the mock attacks.

**Supports multiple languages** – Our top 12 templates and a selection of training modules are available in more than 20 languages (and counting). This allows you to assess and educate employees around the globe in their native languages.

**Tracks results and progress** – Exportable reports provide extensive analytics and data about employee interactions with your campaigns. You’ll have access to open and click rates, reporting data, browsers and device identifiers, and worldwide IP mapping.

**Provides endpoint security insights** – Our Weak Network Egress feature can help detect data egress from users’ PCs, which helps security personnel identify and reduce security weak spots. In addition, administrators can check for browser vulnerabilities, including out-of-date third-party plug-ins.

**Seamlessly supports training assignments** – Users who fall for mock attacks are far more motivated to complete follow-up training. If you’d like to add an education component, our Auto-Enrollment feature allows you to automatically assign training to any employee who falls for a mock attack.

---

**REPORTS SHOW RESULTS AND HELP YOU TAILOR ADDITIONAL EFFORTS**

**IN-DEPTH TRAINING MODULES**

---

**REPORTING**

---

**Email Security Tutorial: Learn How to Play**

Contacts
- Bank of North America
- Dreamary Travel
- GigaMart
- MVerse Wireless
- Purchase
- Speek

To: Phyllis
From: phyllise405@ise.com
Subject: Attachments

We would like your opinion on your recent purchase at Purchase. The survey link is valid for two days, so please hurry.

Thank you,
Pierce Survey Department

The survey link is only valid for two days, so please hurry.

Click safe if it is an indicator of a phishing email. Click unsafe if it is a risk.

safe
unsafe

Campaign from 11/01/2015 to 12/01/2016

All Campaign History

---

**REPEAT**
SmishGuru: Gauge Vulnerability on Mobile Phones

Mobile devices allow on-the-go access to networks and communications — and social engineering scams. Mobile threats are continuing to become more prevalent, and with business data and systems on the move, it’s increasingly important to be able to rely on your employees to handle their devices appropriately.

Our industry-leading SmishGuru simulated attack program allows you to send SMS phishing (i.e., smishing) messages to assess your organization’s susceptibility to actual malicious messages. It is a natural add-on to ThreatSim assessments and an ideal precursor to our interactive training modules that focus on mobile device and mobile app safety.

What SmishGuru Can Do For You

- Mitigates the risks your organization faces from careless interactions with messages.
- Provides multiple customizable text messages that are sent directly to your employees’ mobile phones.
- Delivers customizable Teachable Moments (see opposite page) that alert employees to what happened when they fall for a mock attack. They get your staff thinking about best practices and how to respond to future threats.

USBGuru: Evaluate Use of ‘Infected’ Devices

Our USBGuru simulated attack tool allows you to test employees on a pervasive and dangerous threat vector: infected removable memory devices. Hackers have been known to plant infected devices and drives in common areas, and even new USB drives have been manufactured to carry malware. Simply plugging in these devices can pose a threat, and seemingly innocent files can carry a payload that can cripple an entire network.

USBGuru puts you in the scammers’ shoes without putting your organization at risk. Using our cloud-based interface, you can easily create a custom executable file that is embedded with a brief Teachable Moment. The file is then loaded onto USB devices that can be randomly placed throughout your organization — just waiting to be plugged in.

What USBGuru Can Do For You

- Allows you to track the unique USB devices that are accessed during an assessment period.
- Gives you insights into which users accessed a planted device and how many times the device was used.
- Delivers practical tips via customizable Teachable Moments (see opposite page) when your employees interact with a planted USB device.

Do Not Use Unknown Storage Devices
Infected USB Drives Put You and Your Company at Risk

- Scammers tamper with USB drives and distribute them through many channels.
- An infected drive doesn’t give a warning sign; you might never know it’s dangerous.
- Even new USB drives can be infected with malicious software.

File Sharing Safety Tips

- Never use a USB drive you find lying around, not even in your office environment.
- Ask your IT department before plugging in a USB drive.
- Choose trusted sources for downloads, and use secure servers to share sensitive data.

© 2008-2014 Investment Security Technologies, Inc. All rights reserved. Confidential. Do Not Reproduce.
Assessments and Teachable Moments: An Effective Pairing

At Wombat, we understand that simulated attacks can have a positive or negative impact on end users, depending on how the messages are delivered and how employees feel in the critical moments following the attacks.

Our Teachable Moments appear on-screen at the time a user falls for a simulated attack. These just-in-time teaching messages deliver concise, constructive advice; they explain what happened, alert employees to what they did wrong, and offer helpful, actionable tips about how to avoid future threats. This approach has been proven to engage employees and help them understand the consequences of falling for a phishing attack.

As an added bonus, Teachable Moments set the stage for additional education, which can be delivered via our interactive training modules. Our data has shown that users who fall for a simulated attack are up to 90% more likely to complete follow-up training.

You can choose from multiple design styles, and you can customize your messages to identify alternate tips or communicate company policies and procedures. We currently offer the five options described below:

1. Multi-panel illustration – This style uses four illustrated panels, and users will see the mock attack message they clicked on prior to receiving the Teachable Moment. This design is available with SmishGuru. Support for ThreatSim and USBGuru are planned for a future release.

2. Interactive challenge – This option, which is available only for ThreatSim, challenges users to review a sample phishing message and identify whether or not it is safe. Immediate feedback explains why the user’s choice is or isn’t correct.

3. Landing page – This design mimics the look of a web-based landing page, and we offer multiple variations, including animated options and multinational translations. This Teachable Moment style is available with all of our simulated attacks.

4. Video – Our brief ThreatSim video messages utilize computer animations and illustrations to inform users about the dangers associated with different phishing attack methods.

5. Redirect to your message – If you prefer not to use one of our designs, you can route your employees to your own internal messaging. This option is supported on all our simulated attacks.
Why Wombat?

- Our award-winning Security Education Platform provides everything you need to deliver a complete, effective security awareness and training program.
- Research conducted by the Ponemon Institute showed that organizations with ~10,000 corporate email users can expect to see up to a 50x ROI on the cost of our anti-phishing training program.
- Our approach to security awareness and training is based on our Learning Science Principles, which facilitate longer knowledge retention and help create lasting behavior change.
- Our simulated attack products deliver measurable results on their own, and they only become more effective when paired with our growing library of interactive training modules.
- You can deliver assessments and training in more than 20 languages. For a full list of translations, visit www.wombatsecurity.com/multinational.
- Comprehensive support services — before, during, and after your program launch — are included at no extra cost.

About Wombat and Our Continuous Training Methodology

Wombat Security Technologies was born from research at the world-renowned Carnegie Mellon University, where our co-founders are faculty members at the CMU School of Computer Science. In 2008, they led the largest national research project on combating phishing attacks, with a goal to address the human element of cyber security and develop novel, more effective anti-phishing solutions.

These technologies and research provided the foundation for our product solutions as well as our Continuous Training Methodology. The methodology, comprised of a continuous cycle of assessment, education, reinforcement, and measurement, has been shown to deliver up to a 90% reduction in successful phishing attacks and malware infections.

Anti-Phishing Training Suite: Our Methodology in Action

Reduce susceptibility and change behavior with our Anti-Phishing Training Suite, which combines and integrates ThreatSim assessments with three interactive training modules that are 10 to 15 minutes long: Email Security or Anti-Phishing Phyllis™; URL Training or Anti-Phishing Phil™; and Social Engineering. This suite of products is available in more than 20 languages, which gives you more flexibility for global training.

With our exclusive Auto-Enrollment feature, which directly links assessments and education, you can significantly increase the effectiveness of your security awareness and training program. Our interactive modules will help your users recognize the different facets of phishing attacks, identify malicious URLs, and spot (and avoid) common social engineering scams.

For more information, click here.

CONTACT US AT: RSAUniversity@rsa.com