Social Engineering

DATASHEET

+1-408-540-6771   onemindservices.com   sales@onemindservices.com

Testing the Human Factor

The largest cybersecurity vulnerability at any company is its employees. Cyber breaches happen every day because someone clicked on a malicious link in an email or gave out sensitive information to unauthorized individuals. Attackers have numerous methods to exploit your employees, including malicious phone calls, emails, or even physically entering your premises.

While having policies to combat these threats is critical, it's vital to test their effectiveness regularly. OneMind's Social Engineering engagements simulate real-world scenarios to assess how well your employees recognize and respond to these types of threats. Security awareness training alone isn't enough; you need practical testing to ensure your policies work as intended and identify areas needing improvement.

Types of Social Engineering

We offer two main types of social engineering testing: Remote and Onsite.

Remote Social Engineering:
• **OneMind Phishing** allows you to send simulated phishing emails to test employee susceptibility to malicious links or attachments.
• **OneMindVishing (Voice Phishing)** involves simulated phone calls designed to test employee responses and assess vulnerabilities to phone-based social engineering attacks.

Onsite Social Engineering:
This physical testing evaluates adherence to visitor policies and assesses whether unauthorized individuals could access sensitive organizational areas by posing as trusted agents or vendors. Our expert Information Security Analysts employ various disguises and cover stories designed to test and reinforce employee vigilance.

What's Next?

Post-testing, you'll clearly understand your employees' adherence to your security awareness policies and procedures. It's crucial to educate staff on recognizing threats proactively, especially for those who fall for simulated attempts. This is also the ideal time to implement or update essential policies such as visitor escorts and improve security awareness training programs to address identified knowledge gaps.

Key Takeaways:

- ✓ Manual exploitation of vulnerabilities using real-world hacking techniques
- ✓ Understand network security gaps and how to fix them
- ✓ Simulate attacker access through unsecured networks
- ✓ Verify effectiveness of network security controls

Frequently Asked Questions

Can you use more than one cover story between locations?
We prefer minimizing costume/disguise changes but can accommodate multiple scenarios upon request.

Do you perform USB drops?
Typically, this is not included but can be performed upon request as a separate service.

What script do you use for vishing calls?
We offer various effective scripts, and we're open to incorporating your suggestions as well.

How often is the phishing platform updated? Can we expect new phishing templates regularly?
We continually seek innovative methods and periodically release new templates. Additionally, our platform allows you to create your own customized phishing content.

Does OneMind phish employees continuously or at set intervals?
This depends on your engagement scope, typically quarterly intervals with staggered email dispatches.

What happens if an employee fails a phishing attempt?
Employees who fail phishing tests are logged in our system, and you receive detailed reports specifying the exact actions taken (email opened, link clicked) along with timestamps. You can also configure educational messages to notify employees of their errors and provide security improvement tips.

How much does support cost? What if there's a software issue?
Support is included at no additional cost.