EC-Council aware
When Everyone Protects

CONSTELLATION CYBER CONSULTANCY
Cyber Vulnerability Solutions

EC-Council

Secure your First Line of Defense

The Problem:

Studies show that 90% of cybersecurity breaches are caused by human error.*
Taking precautions to ensure that the entrance of your organization's network is secure from attackers is a must. However, social engineering attacks like phishing emails can still trigger a breach due to human error. Every phishing email that reaches the inbox of a user on a company's network could be a threat. How will you ensure that your employees remain aware of such attacks and recognize them before falling prey?

The Solution:

Aware phishing, vishing, SMiShing, and USB baiting simulations mimic real-life attack scenarios that teach your employees to spot phishing scams and avoid the hefty cost of a data breach. We leverage our experience of delivering world-famous education and training in cybersecurity to enable your staff with the required degree of security awareness. Our LMS & gamification module is a platform which provides security awareness training content that helps you assign customized training to specific individuals.

Why Aware?

According to online reports, susceptibility to phishing emails drops almost 20% after a company runs just one simulation. So people do learn, awareness does rise, and risks do reduce with an intelligent solution like Aware.

Why Aware Over Other Security Solutions?

How "Aware" is Different?

Training Videos
The Aware Application let's your team learn on the go. For security awareness, training plays a crucial role.

Challenge
Aware enables users to participate in live quiz sessions with their friends and colleagues.

Game Time
With the Aware Application, quizzes can turn into company wide competitions.

Leader Board
The Leader Board shows which teams or individuals are leading the competition.

Phishing Simulations
Aware comes with a wide variety of Phishing Simulations as well to test employee's susceptibility to social engineering attacks.

CheckAPhish
CheckAPhish helps you gain visibility into your organization's risk behavior and measure the overall risk levels across your user groups.

What Is Email Phishing?

Humans are the weakest link in the information security chain, and cybercriminals know this better than anyone else, using malicious tactics to lure victims into revealing personal data.

Identifying an email scam is not always a straightforward process because of their targeted nature.

What is **SMiShing?**

SMiShing or SMS phishing is another variant of phishing scams. It uses text messages to trick users into divulging confidential information. As texting is a common communication method among many users, it makes for an easy target.

SMiShing has become one of the main tools in a scammer's arsenal, partly because it is so easy to wield and requires little technical knowledge..

What is **Vishing?**

Voice phishing, commonly known as vishing, is the telephone equivalent of phishing. Like its email counterpart, vishing tricks users into revealing personal data over phone by posing as a trusted entity. Vishing scams can be very convincing because these callers are usually experts in their respective fields. The main reason why vishing scams are on the rise is because of how easily cybercriminals can execute these attacks with minimal risk of detection.

What is **Baiting?**

Baiting is another type of social engineering attack where the attacker uses physical mediums like a USB flash drive or CD-ROMs. The attackers leave malware-infected devices in public locations where they can easily be found. The victim, out of curiosity, inserts the device into a computer, thus infecting their workstation and the entire network of the organization.

This Is Where Aware Comes In!

Aware is a security solution to assess your employees' susceptibility to social engineering attacks. It provides comprehensive security awareness training, fully automated end-to-end phishing, vishing, and SMiShing simulation services. Aware's phishing simulations mimic real-life attack scenarios that teach your employees to spot phishing scams and avoid the hefty cost of a data breach. It empowers them through detailed security awareness training. The platform gives clients a platform to launch campaigns for their employees, capturing responses and providing detailed reports and trends (on a real-time basis) through a dashboard. The results can be tracked by the user's department, designation, office, etc.