INNOVATIVE SOLUTIONS

INFOSHIELD:
AN ANTIDOTE FOR
CYBER THREATS

SECURITY AWARENESS

INFOSHIELD
Be Aware, Be Secure

INFOSHIELD
Be Aware, Be Secure

Table of **Contents**

Executive **Summary**

Security awareness is important to every organization nowadays as they are faced with unpreceded challenges when it comes to protection against sophisticated cybersecurity threats. These challenges include external threats such as targeted attacks, ransomware and phishing and internal threats such as accidental errors and unintended deletion that can cause catastrophic damages to organizations and are more often than not very difficult to recover from. Until very recently, organizations have been focusing only on building defenses to tackle external threats while ignoring internally generated threats. Notably, protecting critical assets from internal threats has lately become as significant as preventing external ones in many organizations. Consequently, organizations have been developing and implementing comprehensive security awareness programs that tackle most of human-related security threats through properly educating and investing in the human factor. In turn, organizations worldwide have been able to mitigate the risk of internal threats.

In general, a security awareness program must cover current and emerging security issues and risks and should enable decision-makers to track user education process accurately, measure key performance indicators and produce comprehensive reports about overall organizations compliance and maturity. First and foremost, the aim of a comprehensive security awareness program is to effectively change staff behavior and measurably reduce security-related risks which in turn will assist in spreading a strong security awareness culture for a safer environment. Furthermore, organizations with adequate security awareness culture would realize better return on security investments (ROI) and would be able to mitigate the cost of security breaches.

Security awareness is all about communication and behavioral change; therefore, organizations need to adopt solutions that spread security awareness in a dedicated and concise way to ensure the maximum benefits where users can learn and apply the best security practices at the workplace.

Top Human Security **Risks**

One of the top risks that organizations face nowadays relates to employees simply not realizing they are a target. Here are the most shared security risks among organizations:
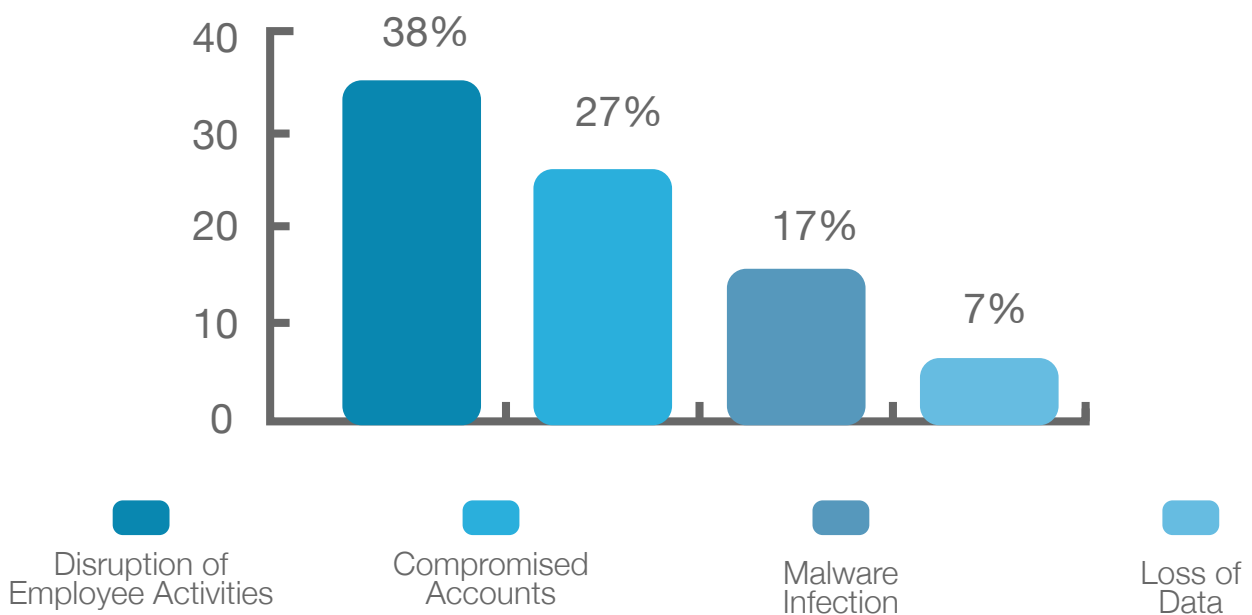
Phishing:
Phishing attacks have become a serious threat and are recognized by the security awareness community as the main human risk due to the ever-changing techniques and forms used to target and reveal sensitive information. The impact of phishing attacks is harmful and continue to be a risk to employees and organizations alike.

Impact of Phishing

Phishing attacks can be devastating to organizations, so we wanted to learn more about the specific impacts.
What has the impact of phishing been on your organization?
(choose all that apply)

40	38%
30	27%
20	17%
10	7%
0	

Disruption of Employee Activities — Compromised Accounts — Malware Infection — Loss of Data

Weak Passwords:

Passwords are considered one of the basic but most effective security controls within any environment. However, employees still use weak passwords, and moreover, reuse them for different accounts which introduces security risks to an organization. As an example, lack of password management and enforcement would lead to compromised systems and might place organizational reputation at stake.

Accidental Errors:

One of the main reasons for data loss are human errors. This includes unintentional file deletion, loss of mobile devices containing sensitive data and sending out confidential emails accidently. These accidental errors may cost organizations more than malicious incidents.

Malware:

Currently, ransomware is a malware that is considered one of the most serious threats seen. Many organizations are witnessing consecutive strikes resulting in holding critical business data as a hostage. Users should be aware of such kind of attacks and are trained and expected to safely deal with suspicious emails, embedded links and malicious websites.

Social Media:

Social media is a fertile ground for adversaries to gather information about employees, such as private or work-related information, in order to launch more targeted and sophisticated attacks.

Lack Of Security **Awareness**

Most of organizations that have been suffering serious security attacks have been found to lack effective security awareness and training programs. The main reasons organizations are being targeted easily are:

•Not addressing the human factor in the information security lifecycle which poses a serious threat to organizations and jeopardizes businesses reputation as one phishing attack can compromise the entire environment.

•Investing heavily in technology to protect critical assets even though the number of attacks targeting employees continuing to rise.

Business Benefits Of Security **Awareness**

Data breaches cost organizations millions of dollars depending on the size of the breach. Moreover, cybersecurity attacks can lead to more downtime and decreased production in organizations. Also, they add overhead on security professionals responding to malware infections and investigating data breaches. As cybersecurity attacks become more focused and mainly target humans as it is easy to hack a human than a computer, organizations are urged to invest more in cybersecurity awareness and training to strengthen the human link. Educating employees on concise security awareness topics and focusing on essential security skills will prepare them to thwart security threats effectively.

One Phishing attack can compromise critical systems and cause serious damage and may render sensitive data unusable to enforce victims to pay attackers a ransom. Organizations can mitigate these risks by investing in the human factor which will being about the following benefits:

Mature Security Culture

Preserving a mature security culture should be the ultimate goal of organizations seeking to prevent cybersecurity threats. This requires implementing a comprehensive security awareness program as well as investing in human training through dedicated security awareness solutions that aim to change users' behaviors and continuously seek to improve the organizational maturity level. Preparing employees to be aware of security threats is corner stone to protecting business.

Preserving Reputation

Data breaches have a serious impact on organizations' reputation as data breaches could expose organizational sensitive information such as financial reports and intellectual properties. Tightening organization security perimeter is the key stone to prevent reputational damage.

Security Awareness is the key aspect of security for strengthening the first line of defense – the employees – that is, they are the main target for adversaries to elicit sensitive information that could lead to a serious damage to organizational assets as well as reputation.

Summary

As data breaches continue, organizations facing challenges due to a lack of visibility into or control over security awareness. Elevating employees' security awareness to reach an adequate maturity level is a must for all organizations concerned with protecting critical assets and thwarting security threats effectively.

Organizations worldwide have learned that effective security awareness is achieved through a comprehensive, solution-based approach that does not leave employees vulnerable and exposed. This would include a combination of platforms, products, resources, support and updated content to help organizations with compliance as well as continuous improvement.

An end-to-end security awareness solution can help transform employees from the weakest link to the first line of defense against cyber threats. The frequent provisioning of security awareness and training activities will ensure that employees are continually made aware of cybersecurity related risks. Organization ultimate goal should be to make risk-aware behavior as "business as usual" for all employees. Selecting a security awareness solution is only a piece of the requirement as solutions are only as good as the effort involved in managing a security awareness program throughout the organization.

Infoshield: A Complete Security Awreness Solution

InfoShield is a comprehensive solution designed and developed to fulfill all requirements for cybersecurity awareness and training. It consists of a Learning Management System (LMS) developed by Innovative Solutions in response to the ever-increasing number and severity of attacks targeting and breaches caused by employees. The solution aims at structurally spreading essential knowledge about cybersecurity and associated risks in addition to providing extensive information and proper course of actions when targeted by cyber threats.

Infoshield is an integrated, end-to-end security awareness solution that delivers best-in-class awareness and training modules using expert content. The solutions aims at:

•Promoting security awareness and knowledge within an organization efficiently.

•Educating employees about expected behavior and responsibilities for safeguarding information.

•Increasing effectiveness of security awareness by providing interactive content.

•Targeting different levels within an organization with a variety of security topics.

•Minimizing human errors by disseminating best security practices.

•Strengthening the human link in the information security chain at any organization.

•Providing up-to-date security awareness modules that tackles most security risks.

Infoshield also has many distinguished features that places it amongst the top security awareness solutions in the region as it provides:

Bilingual Support
A full support of Arabic and English languages

Branding
Co-branding or sole branding can be provided

Scheduling
Ability to schedule modules based on organization's orientation timelines

User Integration
Easy to synchronize users through integrating with Active Directory

Tracking and Reports
Supplies inclusive reports, Key Performance Indicators and dashboards

Testing
Quizzes are associated with modules to test the employee's knowledge

Deployment
Easily deployed as a service or on premise

Customization
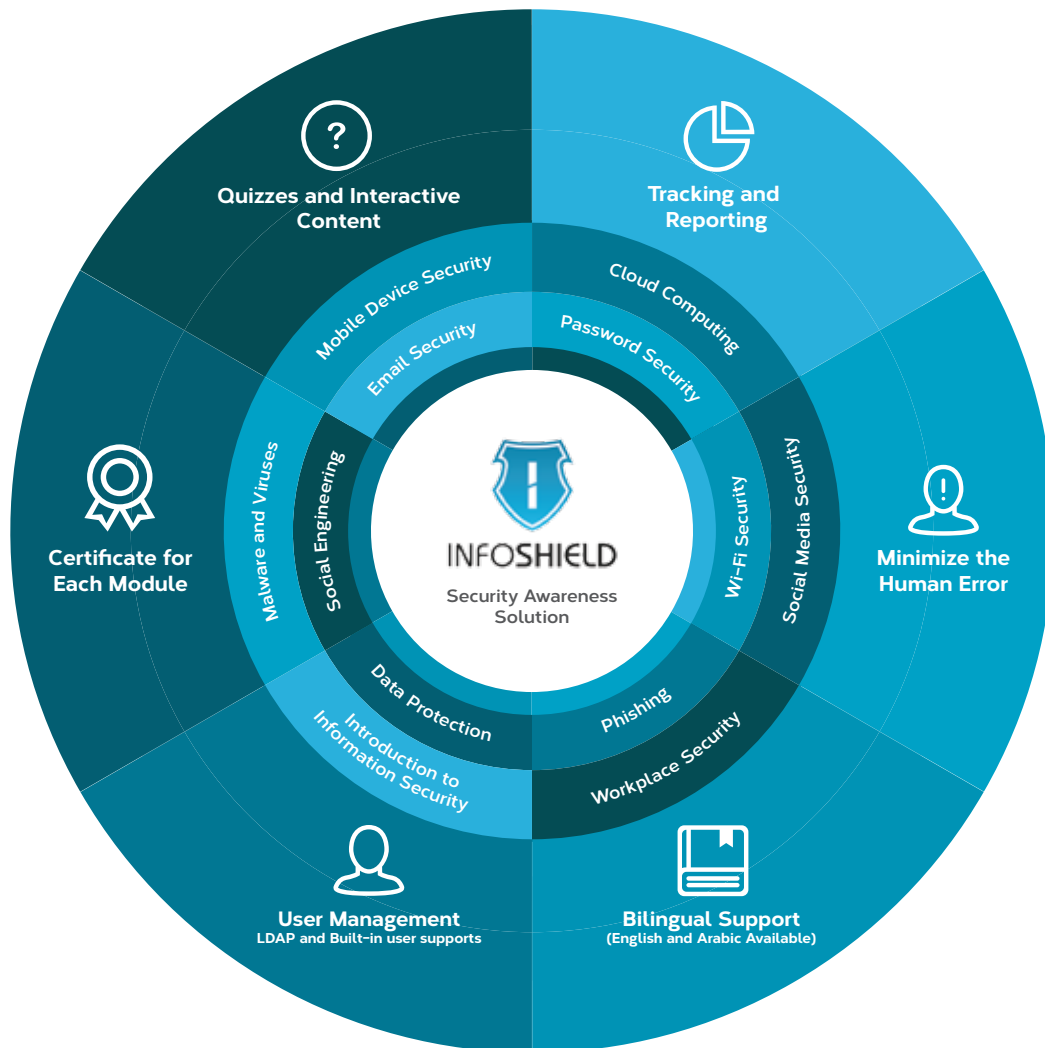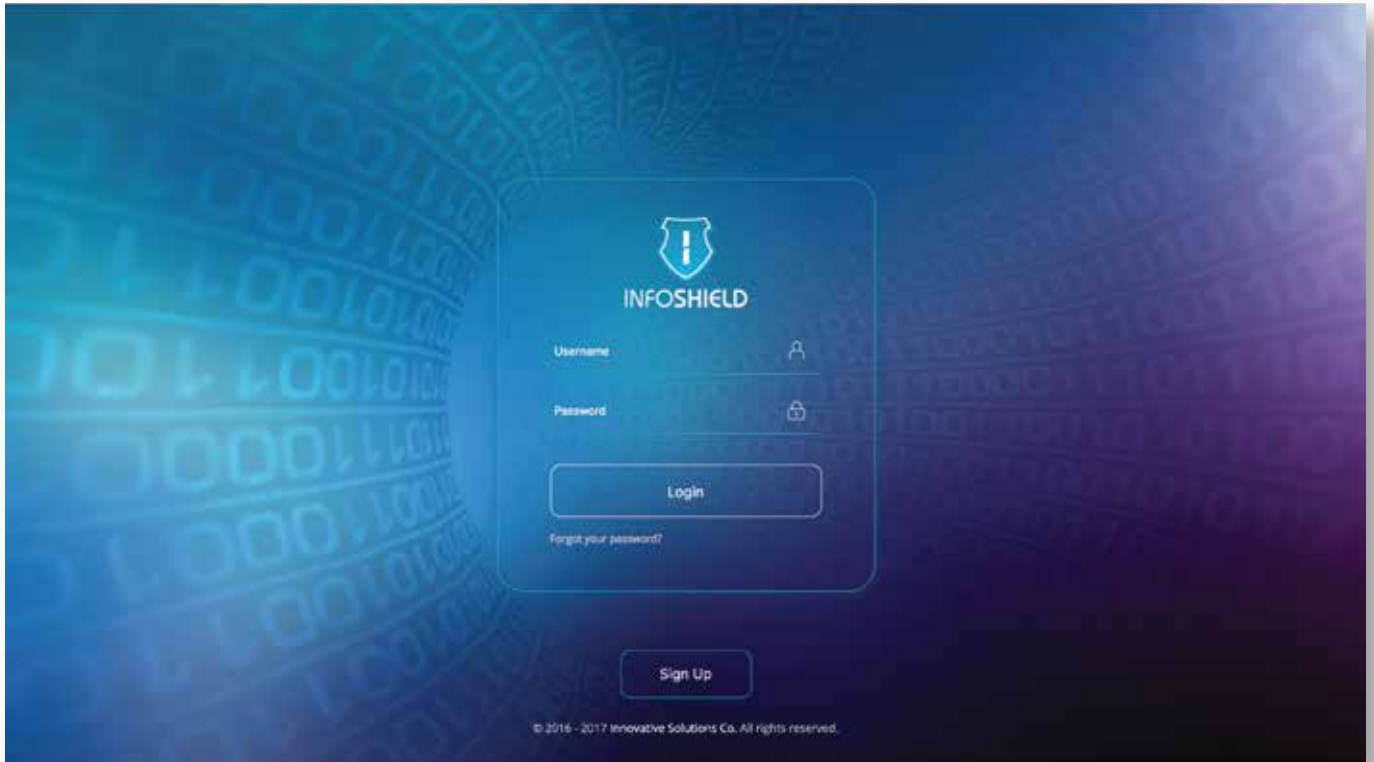Fully customizable according to organization's requirements

On Demand - Modules
Content can be customized or developed based on organization's needs

Infoshield Security Awareness Solution

Quizzes and Interactive Content

Tracking and Reporting

Mobile Device Security

Cloud Computing

Email Security

Password Security

Malware and Viruses

Social Engineering

Wi-Fi Security

Social Media Security

Certificate for Each Module

Minimize the Human Error

Data Protection

Phishing

Introduction to Information Security

Workplace Security

INFOSHIELD
Security Awareness Solution

User Management
LDAP and Built-in user supports

Bilingual Support
(English and Arabic Available)

Infoshield Application Interface

INNOVATIVE SOLUTIONS

Head Office – Riyadh

P. O. Box 69328, Riyadh 11547,
Saudi Arabia

+ 966 11 2931501

info@is.com.sa

www.is.com.sa

Branches

Dubai | Jeddah | Al Khobar

@Innovative-Solutions

@is_arabia

Innovative Solutions SA