



SECURE IT

USER DEFENCE



Increase User Defence to Protect Your Organization Against Cyber Attacks

PRODUCT OVERVIEW

Secure IT - User Defence is a suite of security services that are specifically tailored to empower your employees to become the first line of defence against cyber attacks. This suite of integrated and ongoing services provides a turnkey solution that allows for rapid integration into your IT environment. The services in our solution include

ready to implement comprehensive cybersecurity awareness training, simulated phishing attacks to test employee knowledge/best practices and real time dark web intelligence tools that hunt for leaked user credentials. Track and measure performance using regular user defence reports that demonstrate the overall cybersecurity posture of your employees.



TRAIN EMPLOYEES

Receive access to online self-paced user cybersecurity training and reference material on the latest cyber threats.



TEST EMPLOYEES WITH TARGETED SIMULATED PHISHING

Simulate common phishing threats to test employees. Use the results to bolster training and improve knowledge.



DETECT COMPROMISED CREDENTIALS

Leading edge detection tools hunt the dark web for stolen or leaked credentials and report back when detected.



TURNKEY AND FIXED COST

Receive all the software, licensing, installation and operations required to deliver the services for a fixed monthly cost.



TURNKEY USER DEFENCE PROGRAM



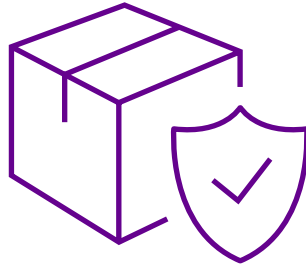
TRAIN

Our training videos are easy to understand and end with an online quiz to verify an employee's retention of the training content.



DETECT

Detect stolen credentials on the dark web before they are maliciously used by threat actors.



PHISHING

Test and improve employee cybern habits with scheduled, customizable phishing tests.



HARDEN

Equip your employees with the knowledge and skills they need to protect themselves and your business.

INTEGRATION

Secure IT – User Defence easily integrates with an organization's Azure Active Directory or LDAP to determine the required user information. Each aspect of the solution is then setup during the onboarding process. Our deployment team works hand in hand with your staff to assess, design and deploy the solution to deliver the solution with minimal impact to users.



ASSESSMENT OF CLIENT USER ENVIRONMENT



SET UP CREDENTIAL MONITORING



SET UP SIMULATED PHISHING CAMPAIGNS



SCHEDULE CYBER TRAINING MODULES



FULL END-USER SECURITY REVIEW AND ANALYSIS

PROGRAM BASICS



INTEGRATION WITH LDAP/AD



ABILITY TO MANUALLY IMPORT



TRAINING BASED ON ORGANIZATIONAL GROUPS:

- Executive
- Managers
- HR
- Admin and Finance
- Sales
- Operations
- Customer Service



C-SUITE / EXECUTIVE PERSONAL EMAIL SCANNING



24/7/365 CREDENTIAL MONITORING



SIMULATED PHISHING CAMPAIGNS

- 12 campaigns per year
- Predefined templates
- Campaign runs for 30 – 45 days
- Ability to assign groups to each campaign
- Automated staggered delivery dates
- Monthly reporting available



CYBERSECURITY TRAINING PROGRAM

- One training module for each calendar month
- Assign groups to each campaign
- Monthly reporting available

To learn more about Secure IT - User Defence, contact us at: Sales@AcronymSolutions.com

1.866.345.6820

Join our mailing list

[SIGN UP ▶](#)