DATA ALERT

SECURITY AWARENESS PROGRAM

Security Awareness Training and Simulated Phishing Platform. Helps you manage the problem of social engineering

FEATURES	SILVER	MOST POPULAR GOLD	PLATINUM
Admin Management Console	✓	✓	✓
Unlimited Phishing Security Tests	✓	✓	✓
Security ‘Hints & Tips’	✓	✓	✓
Onsite Security Awareness Training	✓	✓	✓
Automated Training Campaigns	✓	✓	✓
Crypto-Ransom Guarantee	✓	✓	✓
Outlook Phish Alert Add-in	✓	✓	✓
Access to All Training Modules		✓	✓
Monthly Email Exposure Check		✓	✓
Vishing Module (IVR phishing)		✓	✓
EZXploit™ - “Automated Human Pentesting”			✓
USB Drive Test™			✓
Priority Level Support			✓

SILVER LEVEL: Includes the onsite security awareness training, 45-minute online training, the shortened 25-minute module, the executive 15-minute version, in addition to unlimited Simulated Phishing Testsand enterprise-strenght reporting for the lenght of your subsciption.

GOLD LEVEL: Includes all Silver Level features plus access to our complete library of training modules. Gold also includes monthly Email Exposure Check (EEC) Reports and Vishing (Voice Phising module). The EEC report is a proprietary tool, which conducts a monthly scan of the internet finding all publicly available emailaddresses belonging to your domain and where they were found, including email addresses embedded in .xls, csv, .doc and PDF’s. The emails listed on the report constitute your highest risk users and your phishing attack surface.
The Vishing module allows you to upload the phone numbers of your employees and select one of the “Vishing” templates or scenarios. This enables our system to make robo-calls attacks to your employees. This type of attack prompts your employees to leave confidential information via their phone that can be used to social engineer them later on.

PLATINUM LEVEL: Includes all features of Silver and Gold. Platinum also includes our new EZXploit, enabling you to do human pen testing as well as our USB Drive Tests.

EZXploit- This patent pending functionality allows an internal, fully automated “human pentest” where the system admin can launch a simulated phishing attack - which if clicked on - comes up with a secondary ruse like Java popup that the user is social engineered to click on. If the user clicks on the secondary action, their workstation can be scanned for several things like user name, IP address and other data realated to that user’s workstation and Active Directory as specified by the admin.

USB Drive Test- This feature allows the admin to copy a special, “beaconized” Microsoft Office file from the admin console onto a USB drive which the admin can drop at an on-site high traffic area. If an employee picks up the USB drive, plugs it into their workstation, and opens the file, it will “call home” and report the fail.