CybeReady – Prevention of Phishing Attacks

Datasheet

About CybeReady:

CybeReady is a systematic and comprehensive awareness and behavior change initiative focused on the most significant cyber threat to organizations – Phishing attacks. This intervention is a globally proven and well-established programme which systematically enables, measures and monitors behavior change of members (and risk profiles associated with phishing risks) of staff over a prolonged period (one year).

The initiative also provides management with customizable, on-line measurements and information on risk profiles, at all levels (individual, group, organizational) – thereby providing management with a quantifiable means of measuring the extent of behavior change of staff and organizational risk profile with respect to phishing attacks.

Key Benefits:

- ✓ Sustained and comprehensive awareness and staff behavior change intervention;
- ✓ Measurable – on-line dashboard for company Executives;
- ✓ Delivers content to the right people instead of wasting employees' time;
- ✓ Instantly deployable – no installation and configuration required.

Approach:

Cyber Ready is a customized approach to readiness training, and is designed and implemented in close partnership with the designated company representative. Following a setting-up phase, the campaign is managed through a well-planned simulated phishing campaign for staff over a full year.

The campaign involves the sending of carefully crafted and disguised phishing e-mails to employees using different attack scenario simulations (including both spray and spear phishing) on a pre-determined and ongoing basis. Employee's reactions and behaviors are tested using various methods and levels of deception, and monitored. Should an employee react to any of the simulated phishing emails, the employee will be immediately treated to a short (90 second) educational video which provides background and insights into the nature of phishing emails and associated desirable and undesirable responses.

Learning Objectives - Deliverables:

Delegates will be converted from passive observers to cyber defense warriors through practical and memorable training on phishing attacks and how these should managed to reduce the risk of exposure.

Additional Course information:

- ✓ Engagement is conducted over a twelve month period;
- ✓ Engagement includes a set-up phase, and an active operational phase;
- ✓ Includes a near real time dashboard and metrics report;
- ✓ Is designed to include four customized campaigns; and
- ✓ The campaign is provided remotely.

Contact information:

For further information about this course please contact Dr Graham Wright at-

Mobile: +27 83 252 5727

Email: Grahamw@gnlcyber.com