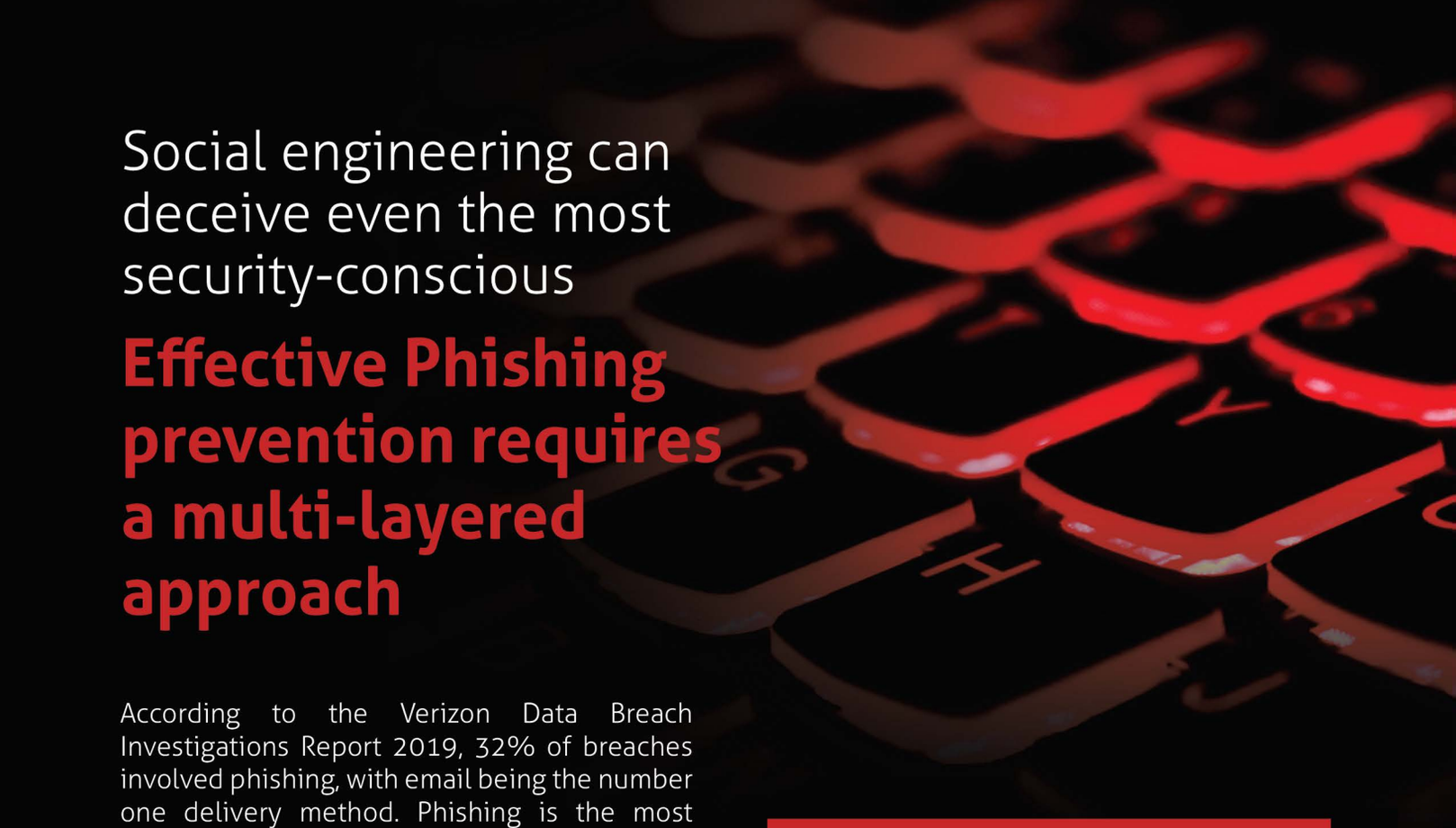

Social engineering can deceive even the most security-conscious

Effective Phishing prevention requires a multi-layered approach

According to the Verizon Data Breach Investigations Report 2019, 32% of breaches involved phishing, with email being the number one delivery method. Phishing is the most effective technique that manipulates humans into unknowingly giving up sensitive information and opening the door to a wider cyber-attack on an organisation.

Phishing Challenges:

- Increased volume and sophistication of phishing attacks that are difficult to identify and avoid
- Most common targeted method of cyber attacks
- Human error - the weakest link in the cyber security defence chain
- Failing traditional email security safeguards
- Lack of education and security awareness
- Compliance Pressures
- Repeat attacks to vulnerable users
- High percentage of workforce using mobile devices
- Cloud-based phishing increasing due to high adoption of cloud

CITADEL
DIGITAL SECURITY

Phishing-as-a-Service
Measure and Improve Human Based Risk

Key Features

- Fully managed phishing campaigns with tailored emails to designated employees simulating a phishing attack
- Monthly, quarterly or annual phishing service
- Flexible recipient / elastic on per user basis
- Tailored report detailing campaign results and recommendations
- Helps to steer cyber training decision making
- Supports business and security compliance
- Security Awareness Training provided as an additional service

CITADEL
DIGITAL SECURITY

Control & Simulate

Simulated Phishing-as-a-Service

Citadel Simulated Phishing-as-a-Service (SimPHaaS) provides a programme of simulated 'real-world' phishing email campaigns to highlight vulnerabilities in the workforce in a safe and controlled environment.

Gaining visibility of your most vulnerable users and providing the relevant security awareness training to **educate**, **protect** and **enable** employees, will help to reduce the likelihood of cyber-attacks caused by phishing and other social engineering tactics.

Simulated Phishing-as-a-Service should be delivered as part of a multi-layered approach to phishing through a combination of technical controls and user education:

1. Make it difficult for attackers to reach your users
2. Help users identify and report suspected phishing emails
3. Protect your organisation from the effects of undetected phishing emails
4. Respond quickly to incidents

CELERITY

Celerity, working in partnership with NCSC, regional cyber protection units & certified industry specialists to fight the war on cyber-crime.

ISO 27001 CERTIFIED
British Assessment Bureau

CYBER ESSENTIALS PLUS

Take control of your Digital Security & Cyber Defence.

Speak to a Celerity Security expert today.

T: **+44 (0) 8455 652 097**
E: **info@celerity-uk.com**
www.celerity-uk.com

Head Office: 11 St. George's Court, Kirkham, Preston, PR4 2EF
View Privacy Policy at https://www.celerity-uk.com/privacy-policy