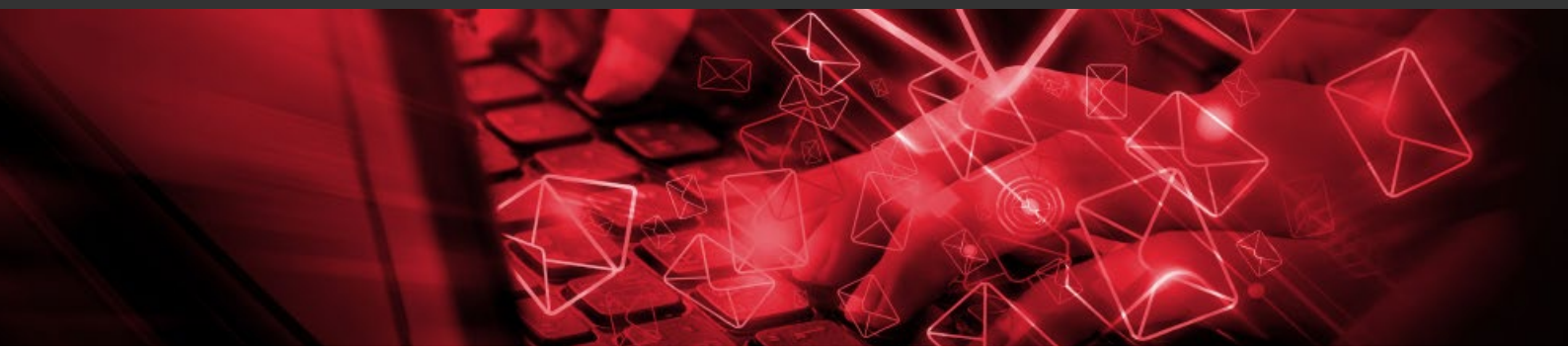
krome

DATA SHEET



PHISHING ASSESSMENT & TRAINING SERVICE

Cybercriminals continue to create and send thousands of phishing attacks daily. With such a sharp rise in numbers and an increase in their sophistication, phishing is now a major security concern.

Companies that do not have adequate measures in place to prepare and protect against these threats will potentially find themselves susceptible to data loss, loss of productivity, loss of revenue and loss of reputation.

Our Phishing Assessment Service enables companies to analyse the human vulnerabilities within the business; organisations will have firewalls, threat prevention, anti-virus, zero-day tools etc, which are all a normal part of any IT security infrastructure, but what is often the forgotten vulnerability, is the human element. By regularly evaluating and educating your end users you can create an additional security layer - the human firewall.

In 2020, phishing attacks increased by 42% in comparison to 2019.

Daily phishing threats are estimated at over 25,000.

Research shows that training staff reduces your risk by up to 80%.

Phishing assessments enable you to establish a baseline, set goals and mitigate the risk.

EVALUATE THE HUMAN RISK

Cybercriminals play on users' fear, curiosity, and insecurities, encouraging them to think they are clicking on trusted links; as the sophistication of the phishing attacks rise, they are now legitimate looking requests, from recognised organisations and unfortunately, they are regularly catching people out.

Regular and controlled phishing assessments enable an organisation to measure their internal risk, delivering valuable insights into where any human security weakness resides, with immediate remedial training delivered if a nefarious link is clicked or a phishing email is opened.

Our phishing assessment testing offers critical management reporting on the overall level of vulnerabilities found across the users of your business. For example we can create a fake phishing attempt and target it to a specific group or department, by remote or in-house staff, designing specific attacks relevant to their role or location etc, this then enables the business to deliver bespoke training sessions to the users or teams that need it the most.

How does the testing work?

- A series of phishing emails are created specific to your company
- Fake phishing emails are sent out to specific users/groups
- Analysis and reporting on success/failure of emails and users
- Identify weaknesses, deliver user awareness training
- Re-test following training, sending out revised emails
- Re-direct users for further training upon failure
- Benchmark and report on trends and revision to testing

We can deliver the service as a single point-in-time assessment to help you quickly understand where you have vulnerabilities and to provide training for your staff, however we strongly recommend that you regularly test and educate, as part of your security strategy, to strengthen your security measures from within.

krome

PHISHING SIMULATION

Our phishing simulation platform links securely with your Active Directory, and scales for organisations of any size.

A series of phishing emails are developed by our highly experienced team, based specifically on your business, users, location or any other personalisation requirements.

Sophisticated looking phishing emails will be sent that contain links, attachments and will direct users to fake login pages.

Phishing emails can be created with spoofed email addresses from outside of the organisation, but can also be created to look like internal communications from within the organisation.

Emails can be highly targeted, but can be sent out in bursts. Emails are delivered at the same time, but use varying phishing templates across your users or groups. This avoids colleagues warning each other, or relaying to each other the details of the phishing email they have received. Email sends can also be sent in a phased approach.

COMPLIANCE REPORTING

Every user interaction, including email opens, image downloads, attachment opens and link clicks are fully recorded for reporting. Enabling you to easily identify repeat offenders, or any potential high-risk departments.

Review users by geo-location, operating system, browser edition, allowing you to identify any system vulnerabilities.

Assess employees level of understanding and overall risk within the organisation. Use the data to implement targeted user training.

With regular assessments the business will have an in depth analysis to benchmark user awareness and identify trends.

Helps organisations to meet legal and regulatory compliance requirements inc security accreditations (ISO27001, NIST, COBIT, Cyber Essentials and ASD4).

In order to comply with GDPR regulations, organisations are required to raise the level of security awareness of their staff.

AWARENESS TRAINING

Focused security awareness training is delivered based on the identified knowledge gaps and it can be delivered in several ways: company-wide, scheduled or real-time.

We recommend that during the first phase of the phishing assessment, users are not notified that they have opened or clicked on a suspicious link. At this stage we recommend that you use this exercise to gather data insights in order to analyse any weaknesses, we will then use the data to deliver company wide awareness training.

Following the initial assessment and user training session, subsequent training can then be provided in response to user actions.

If required, we can set the system to automatically send out specific training guides, company policy or data compliance reminders once a user engages in potentially damaging activity, or when repeat offenders are identified.

With regular user testing and training, you strengthen your users security awareness and mitigate the risk to business.

MANAGED SERVICE

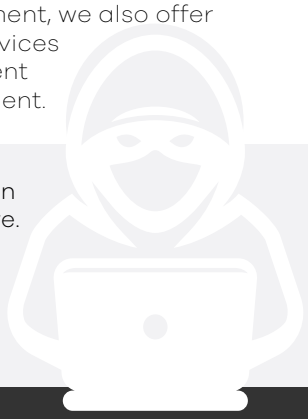
Phishing is yet another rising attack vector, one that requires your IT teams attention and time, our managed phishing assessment and training service eliminates the internal burden on your own IT resources.

Our experienced team will set up the phishing simulation platform, configure and execute the first series of emails. The results will be analysed, user training will be provided and a full report of the findings will be submitted.

Following this initial assessment, the data would be reviewed, working collaboratively with you we will then agree on the required recurring schedule. Some clients choose to run testing quarterly, some select monthly but with a quarterly review and analysis report.

The service is flexible and can be tailored to your specific requirements based on the assessment findings.

In addition to our phishing assessment, we also offer additional security assessment services such as our Vulnerability Assessment and Cyber Essentials Plus Assessment.



Using cyber security products within our portfolio we can also deploy various inspection tools that can analyse your entire cyber security provisions and identify any vulnerabilities within your infrastructure.

If you would be interested to learn more about how our security assessment services can help you to understand where your systems, or people, are most vulnerable, and the steps required to protect your business, please contact us on **01932 232345**.

Krome Technologies
Head Office | Krome House | Pound Road | Chertsey | Surrey | KT16 8ER
01932 232345 | sales@krome.co.uk | www.krome.co.uk