PHISHING AS A SERVICE

KEY BENEFITS

- **Assess the danger:** Build a business case for investing in security or user education with a realistic view of your Phishing risk
- **Reduce risk:** By training employees to spot and avoid phishing attacks, lowers the risk of future downtime and security breaches
- **Enhance security:** Benefit from expert advice from ethical hackers using realistic simulated Phishing tactics
- **Remediate issues:** Detailed insights into specific user and device vulnerabilities allow you to take swift and effective action

KEY SERVICE FEATURES

- **Simulate 'real' attacks:** Phishing campaigns are designed by highly skilled ethical hackers
- **Tailored campaigns:** Target any combination of employees with custom crafted campaigns
- **Executive reporting:** A detailed breakdown of each campaign, identifying who opened, clicked or entered corporate credentials and passwords
- **Guidance on mitigation:** Expert advice on how an attack is likely to succeed and recommendations for mitigating the risk of an successful attack
- **Education and training:** Expert advice on how users can protect themselves in specific situations or on certain devices

SERVICE DESCRIPTION

Almost all the major, recent compromises exploited the weakest link in a business's defences: its people. Phishing can inflict enormous damage –yet most businesses have no idea how vulnerable they are. As Phishing attacks become more frequent, targeted and sophisticated, it's crucial to understand and reduce the risks.

Phishing uses social engineering to trick employees into downloading malware or disclosing sensitive information. Fraudulent emails are most common, but cybercriminals also use instant messaging, mobile apps, social networks and SMS text messaging. These attacks frequently succeed because they target users, not technology. Your business is only ever as secure as its least security conscious employee.

To reduce the threat, you need to understand how susceptible users are to Phishing. By deploying highly skilled ethical hackers to simulate a real attack and monitor responses, Phishing as a Service can accurately gauge your level of risk. These practical, 'live' exercises are tailored and executed by social engineering specialists regularly using Phishing in our Red Team assessment services.

By simulating attacks, our experts can educate users on real Phishing tactics and security best practices - dramatically strengthening your security posture. Meanwhile, detailed reporting provides clear insights into your changing level of risk, including users that are particularly vulnerable, allowing you to take appropriate action.

KEY TECHNICAL COMPONENTS

- **Fast, easy-to-adopt service** that requires no hardware or software installation
- **Regular tailored campaigns** that adapt depending on user behavior
- **Custom lures** to get more users to respond to simulated Phishing e-mails.
- **Custom landing pages** to entice more users to provide credentials
- **Detailed reporting** containing all the information you need to reduce risk
- **User-defined time limits** mean total control over the length and duration of the simulated Phishing campaign

FOR MORE INFORMATION PLEASE CONTACT US
T: +44 (0)1622 723400 | E: info@secdata.com

WHY SECUREDATA

Outstanding expertise:
Social engineering specialists at SensePost, the elite consulting arm of SecureData, design Phishing campaigns using the same sophisticated techniques as fraudsters themselves. These expert consultants think like the bad guys, ensuring your users have accurate preparation for the latest Phishing tactics used in the wild.

Practical approach:
Our 'real-world' Phishing campaigns have far more impact on user behaviour than traditional, passive security training, or campaigns run by internal teams. We also work with you closely on remedial education and training.

Flexible delivery:
Deploying Phishing as a Service is fast and simple. Hosted in our secure cloud and with minimal setup requirements, we can make a dramatic impact on your security with no disruption to business-as-usual.

Complementary services:
We offer a broad range of services that complement Phishing as a Service and strengthen your security posture, including Managed Vulnerability Scanning, Managed Threat Detection and Managed Compliance Monitoring.

ABOUT SECUREDATA

SecureData is a leading provider of cybersecurity services and solutions.

SecureData looks beyond point technologies to address cybersecurity as a whole. The company offers a comprehensive set of professional and managed security services across the entire attack continuum.

For over 25 years SecureData has been helping organisations assess risks, detect threats, protect assets and respond to breaches quickly and effectively ensuring essential IT infrastructure always remains secure and available.

SensePost, the consulting arm of SecureData includes some of the world's most preeminent cybersecurity experts. Trusted by both corporate and military organisations across multiple countries, SensePost helps organisations to protect IT infrastructure and stay ahead of evolving cybersecurity threats.

Operating across the UK, South Africa and the USA, SecureData has an enviable track record having delivered cybersecurity services for many business sectors including finance, insurance, retail, property, professional services, technology and government.

@SECUREDATAEUROPE @SECDATAEU WWW.SECDATA.COM

@SENSEPOST @SENSEPOST WWW.SENSEPOST.COM

FOR MORE INFORMATION PLEASE CONTACT US
T: +44 (0)1622 723400 | E: info@secdata.com