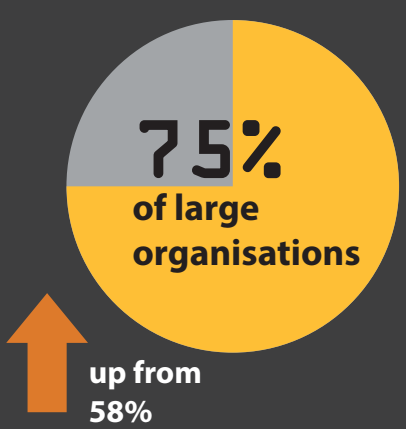
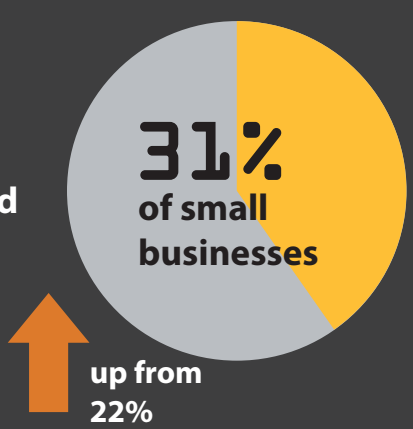
Are your employees resistant to phishing attacks?



of large organisations

up from 58%

and



of small businesses

up from 22%

had a staff-related security incident in 2015[1]

9 in 10 cyber attacks begin with emails[2]

557,964

unique phishing attacks since January 2016[3]

36%

of UK adults don't know what phishing is[4]

Phishing is a form of scam in which the attacker tries to obtain sensitive information by impersonating a known entity or person in email or other media

76%

of UK adults don't know what ransomware is[4]

Ransomware is a type of malware used for data kidnapping: the attack encrypts the victim's data and asks for money in exchange for the decryption key

55% **of organisations witnessed an increase in the volume of whaling attacks[5]**

Whaling is a type of phishing scam that targets high-profile end users such as C-level executives

FACC Operations GMBH's financial accounting department was targeted by a whaling attack - approx. €50 million was transferred to a fraudulent account.[6]

Seagate Technology's data storage employee was targeted by a whaling attack - up to 10,000 W-2 tax documents of current and past employees were revealed.[8]

Jan 2016

Feb 2016

Snapchat's payroll department was targeted by a whaling email scam - payroll information about some current and former employees was disclosed.[7]

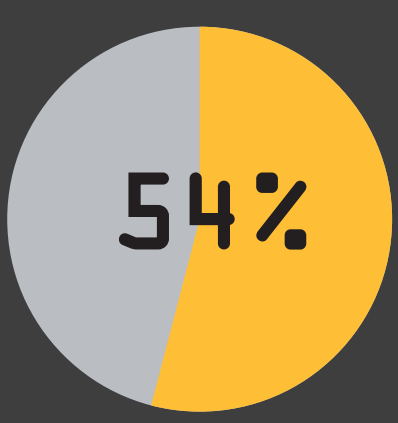
Mar 2016

Test your employees' resistance to phishing attacks

The IT Governance's Simulated Phishing Attack simulates a spear-phishing campaign against your employees. It establishes your employees' vulnerability to spear-phishing and whaling campaigns.

Spear-phishing is a type of phishing scam targeting a specific group of people.

Spear-phishing emails appear to be sent from an individual or entity that the victims know, and look legitimate. They encourage the victim to click on a malicious link set up for fraudulent purposes.



of employees tested since January 2016 failed the test

- they clicked through the masked malicious link within a few seconds of receiving the email.

Top 6 teams that swallowed the bait:

1. **Compliance**
2. **Sales & development**
3. **IT**
4. **Finance**
5. **Account management**
6. **Management**

How vulnerable are your staff?

Adopt a 3-step approach to preparing your staff to combat scams:

1. Test your employees' vulnerability to phishing attacks with the **Simulated Phishing Attack**.
2. Based on the result, train them with the **Phishing staff awareness e-learning course**.
3. **Repeat the test** to assess improvement.

Further reduce the risk of cyber threats.

Book a Simulated Phishing Attack today >>

Sources:
1. 2015 Information Security Breaches Survey, PwC
2. Industry-First Impersonation Protect from Mimecast Combats New Spike in Multi-Billion Dollar Whaling Threat, Mimecast, 5 April 2016
3. Phishing Activity Trends Report – 1st Quarter 2016, APWG
4. More Than Half of UK Office Workers Say Employers Give No Security Training, ISACA, 7 June 2016
5. A Whale of a Tale: How to Stop the Rising Tide of Impersonation Attacks Impersonation Protect, Mimecast
6. CEO Sacked After $56 Million Whaling Attack, www.infosecurity-magazine.com
7. An Apology to Our Employees, Snapchat Blog, 28 February 2016
8. Cyberheist Dumps Seagate Technology, Snapchat Deep In Phishing Hole, www.investors.com

@ITGovernance

/it-governance

/ITGovernanceLtd

IT Governance™

IT Governance Ltd
Unit 3, Clive Court, Bartholomew's Walk
Cambridgeshire Business Park
Ely, Cambs CB7 4EA
United Kingdom

t: +44 (0) 845 070 1750
e: servicecenter@itgovernance.co.uk
w: www.itgovernance.co.uk