PHISHING

Minimize the risk of phishing attacks by assessing and educating end users.

What is phishing?

Phishing emails appear to come from someone you trust, such as an online provider, bank, credit card company or popular website. These emails typically try to trick you into giving away sensitive information, such as your username, password or credit card details.

They may also try to install malware onto your computer by getting you to click on a malicious link or open an infected attachment.

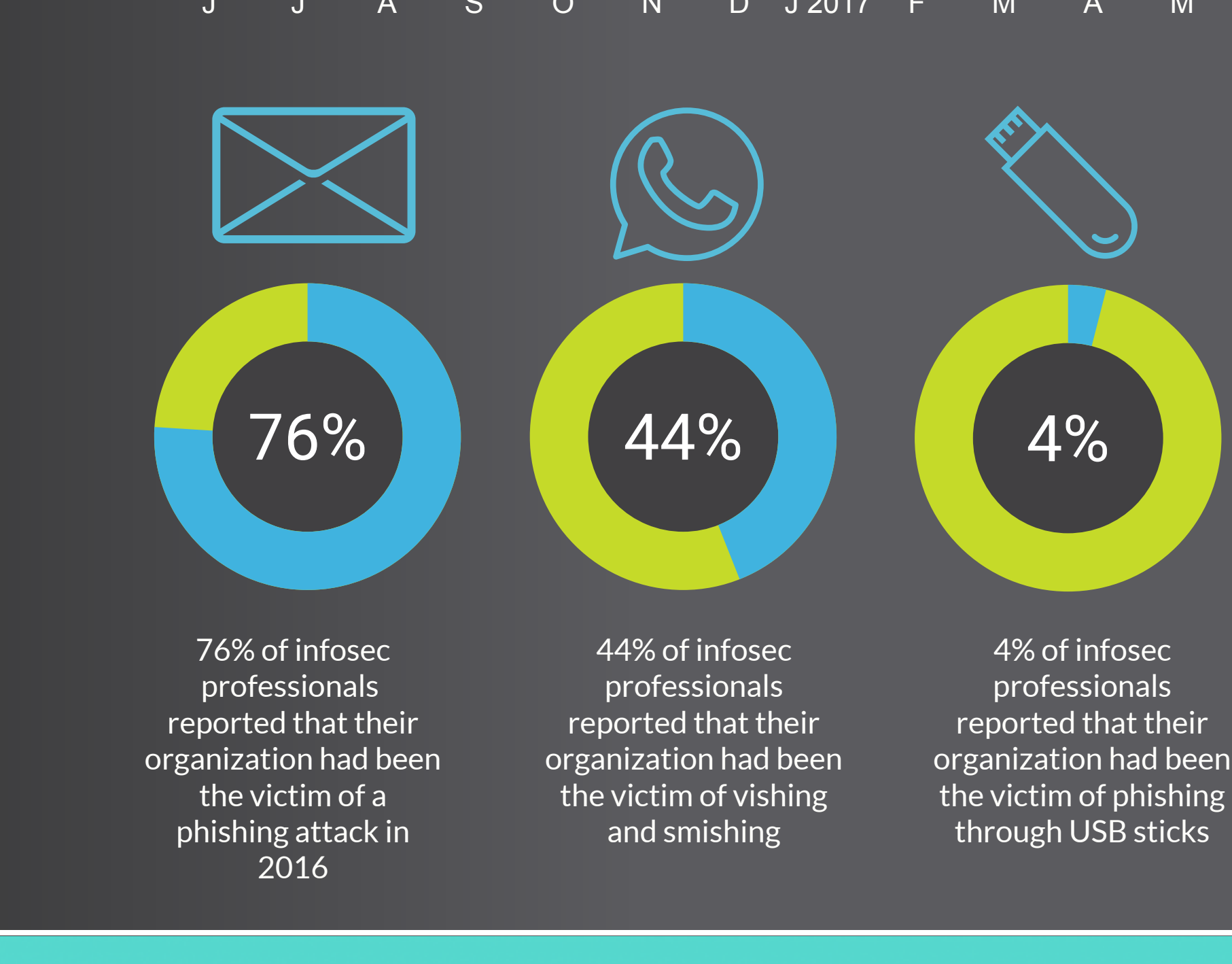
Spear phishing	Whaling	Vishing	Smishing
Email-spoofing fraud specifically targeting a company.	Spear-phishing attack targeting C-level execs or spoofing their email addresses to reach lower-level staff.	Fraudulent phone calls urging the recipient to reveal sensitive information.	Text messages urging the recipent to click a link that downloads malware onto their device.

According to data from IBM X-Force data, 70% of credentials are stolen in the first hour of a phishing attack. Four hours into that phishing site being online, that number rises to 80%. [1]

The current state of phishing

[2]

In May 2017, every 1 in 2,998 emails was a phishing email.

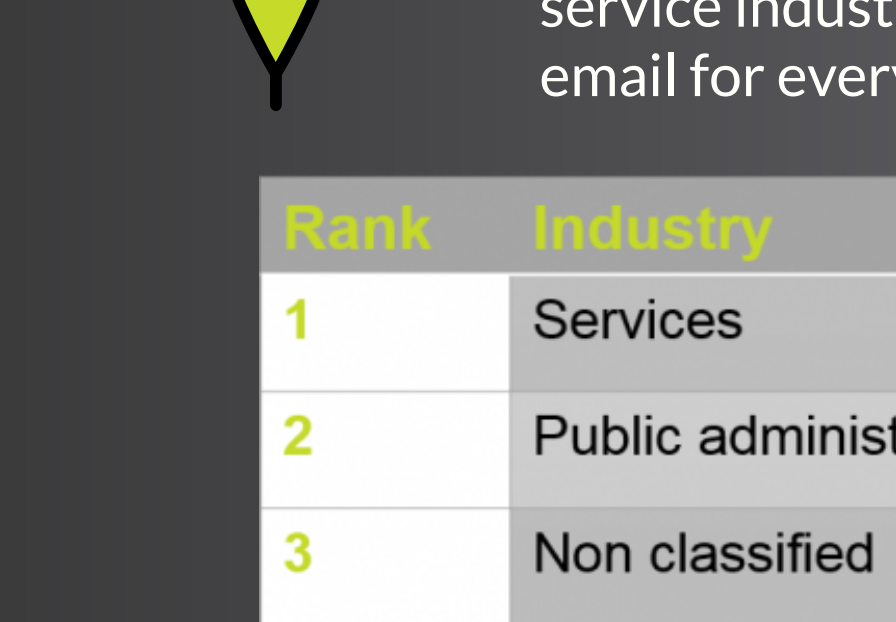


76% of infosec professionals reported that their organization had been the victim of a phishing attack in 2016

44% of infosec professionals reported that their organization had been the victim of vishing and smishing

4% of infosec professionals reported that their organization had been the victim of phishing through USB sticks [3]

Phishing and ransomware work together [4]



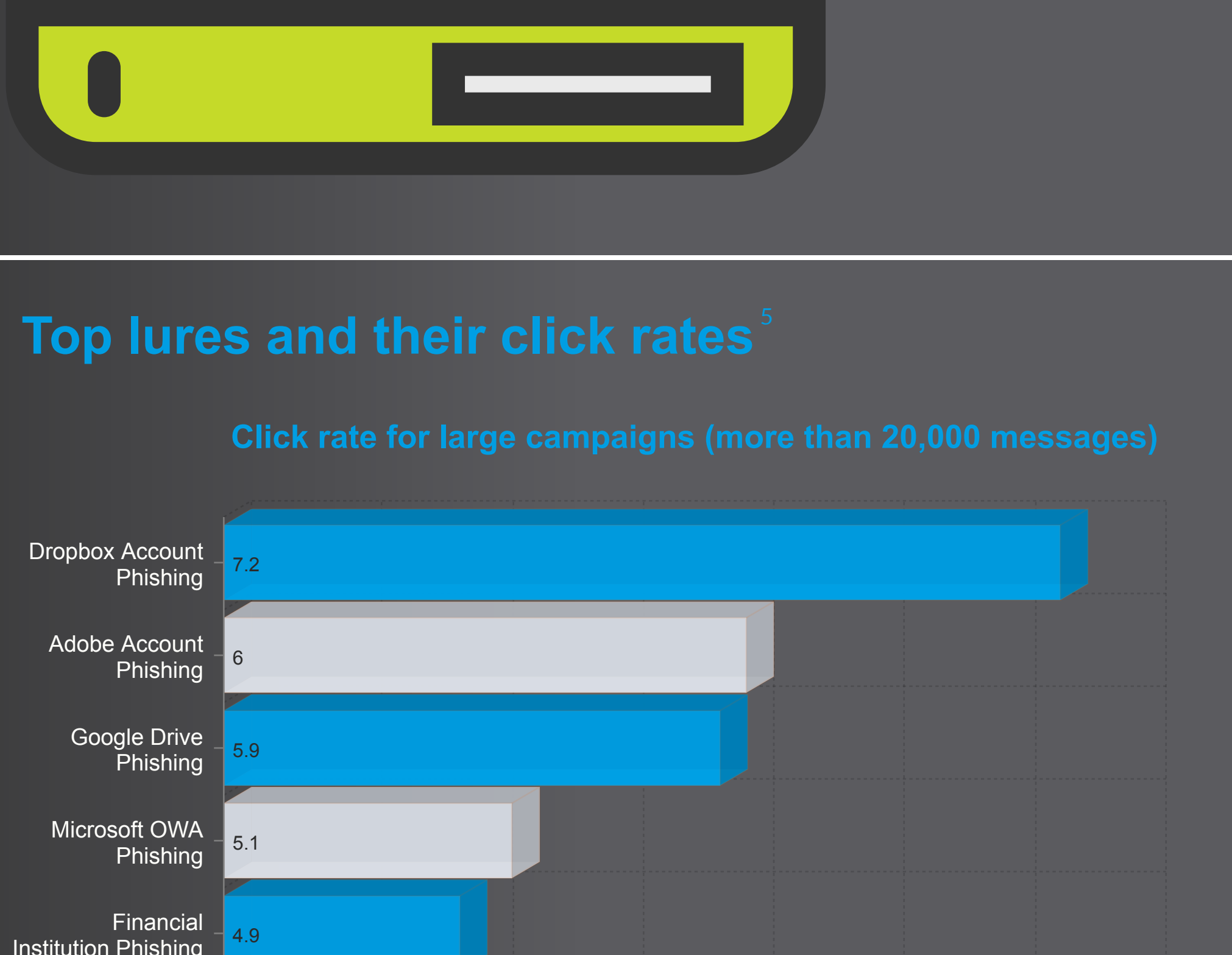
The number of phishing emails containing a form of ransomware grew to 97.25% during Q3 2016, up from 92% in Q1 2016.

Phishing by industry sector [2]

Phishing affects almost every industry. However, the service industry is the worst affected, with 1 phishing email for every 1,903 emails received in May 2017.

Rank	Industry	May 2017 (1 in)
1	Services	1,903
2	Public administration	1,981
3	Non classified	2,022
4	Agriculture, forestry and fishing	2,127
5	Mining	3,122
6	Manufacturing	3,955
7	Retail trade	4,298
8	Finance, insurance & real estate	4,797
9	Wholesale trade	4,863
10	Construction	5,237

How to spot a phishing attack



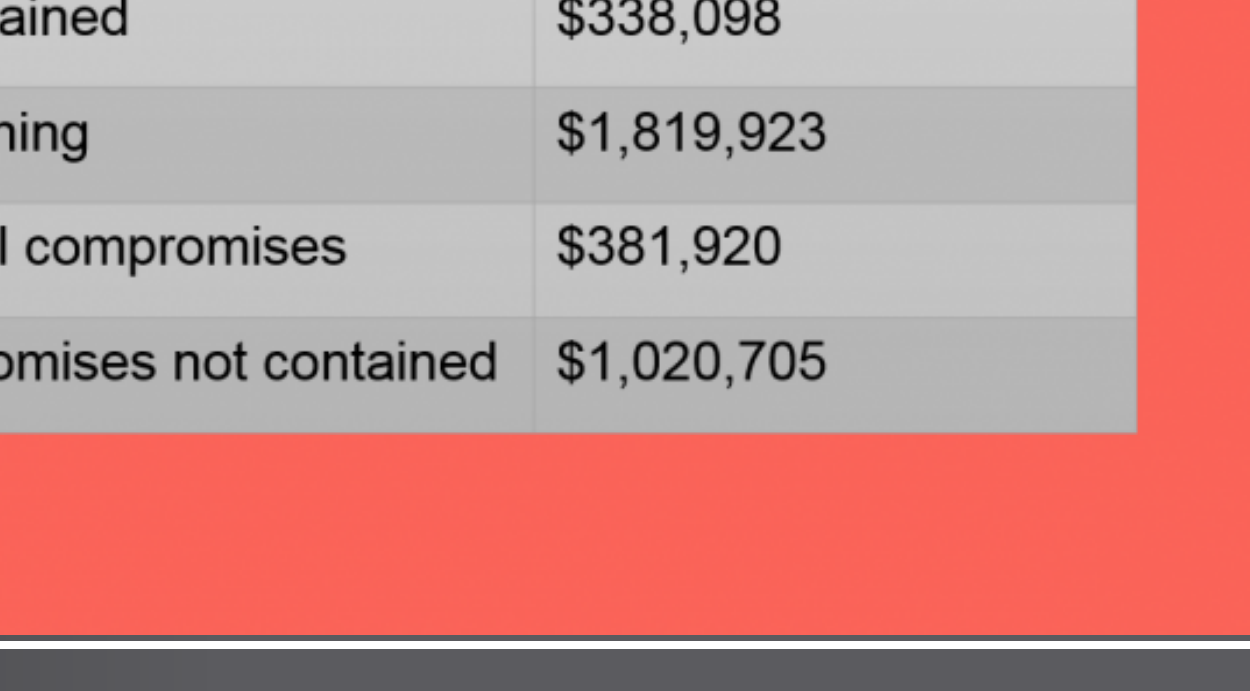
Top lures and their click rates [5]

Industry suseptibility to phishing attacks [5]

The majority of industries are not significantly different with regard to the percentage of users that click on phishing links or attachments.

The cost of phishing [6]

In 2015, the Ponemon Institute concluded that lost employee productivity is the largest cost associated with phishing (roughly $1.8M for a 10,000-person company).



The impact of phishing on organizations

Type of cost	Estimated cost
The cost to contain malware	$208,174
The cost of malware not contained	$338,098
Productivity losses from phishing	$1,819,923
The cost to contain credential compromises	$381,920
The cost of credential compromises not contained	$1,020,705

Examples of breaches

CEO Sacked After $56 Million Whaling Attack

FACC Operations GMBH's financial accounting department was targeted by a whaling attack — approx. €50 million was transferred to a fraudulent account. [7]

Cyberheist Dumps Seagate Technology

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

An Apology to Our Employees

Snapchat's payroll department was targeted by a whaling email scam — payroll information about some current and former employees was disclosed. [9]

How to defend your organization from phishing attacks

The combination of IT Governance's Simulated Phishing Attack and Staff Awareness Course will help you reduce your phishing exposure by testing and assessing your staff's vulnerability to phishing attacks.

Simulated Phishing Attack	Phishing Staff Awareness Course
A Simulated Phishing Attack will establish whether your employees are vulnerable to phishing emails, enabling you to take remedial action to improve your cybersecurity posture.	This e-learning course will help your staff understand how phishing attacks work, the tactics that cyber criminals employ to lure inattentive users, and how to spot and avoid a phishing campaign.
Buy online	Buy online

Find out more about how IT Governance can help identify risks in your existing systems and processes, or how to proactively detect and prevent internal and external threats by clicking here or calling +1 877 317 3454.

References

1. "Hey Phishing, You Old Foe — Catch This Cognitive Drift?", IBM Security Intelligence (March 2017)
2. Monthly Threat Report, Symantec Security Response (May 2017)
3. The State of the Phish 2017, Wombat Security Technologies (January 2017)
4. 2016 Q3 Malware Review, PhishMe (November 2016)
5. The Human Factor Report, Proofpoint (June 2017)
6. The Cost of Phishing & Value of Employee Training, Ponemon Institute (August 2015)
7. "CEO Sacked After $56 Million Whaling Attack", Infosecurity Magazine (May 2016)
8. "An apology to our employees", Snap Inc. (February 2016)
9. Cyberheist Dumps Seagate Technology, Snapchat Deep In Phishing Hole, www.investors.com