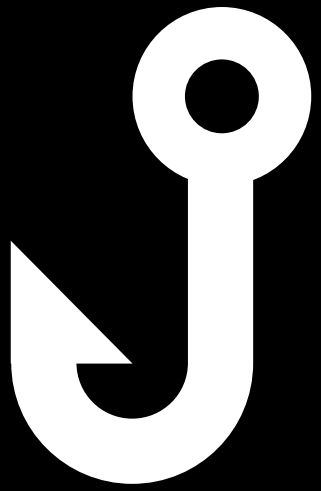
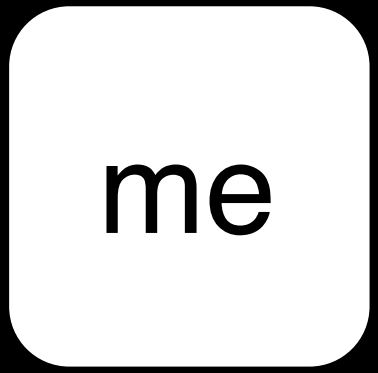


Building an Enterprise Wide Phishing Program



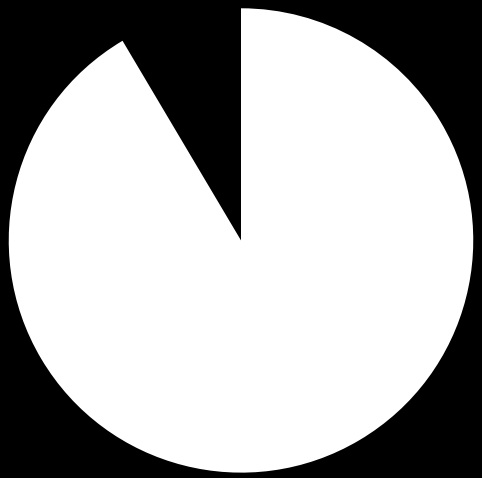
Gavin Duffy BSc

Global Head of Cyber Training & Awareness

DIAGEO

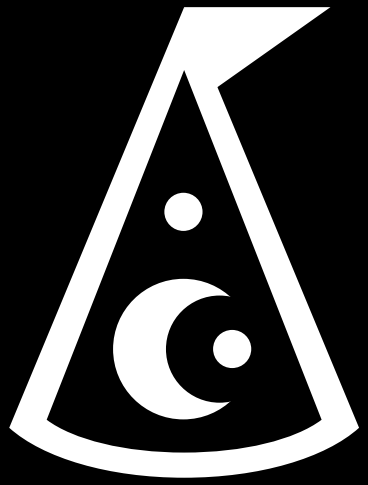
The world's leading premium drinks company

30,000+ employees across 24 global markets.



91%

91% of cyberattacks start with a phishing email.



Deception

The more customised and urgent the message appears, the more likely people are to fall for it.

Plan, what plan?

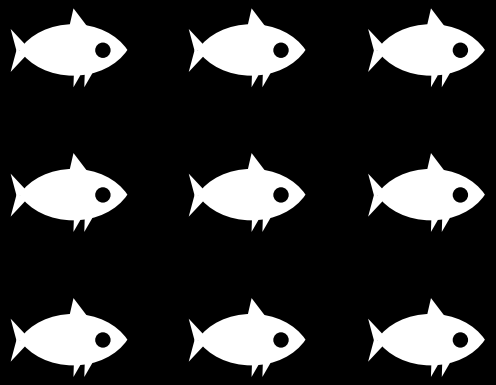
Not implementing a proper plan limits the effectiveness of the exercise.

National Cyber Security Centre

a part of GCHQ

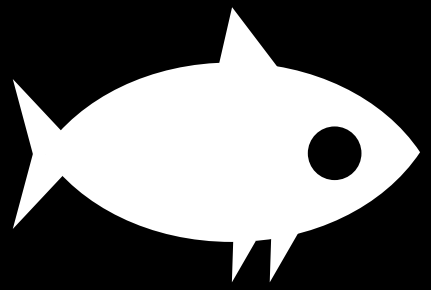
Definitions

For the purpose of this session we will use the NCSC definitions for various phishing techniques.



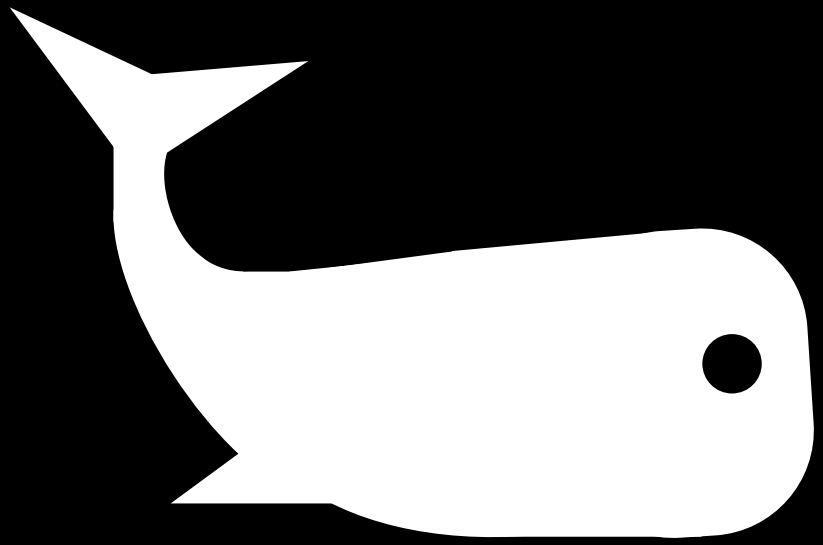
Phishing

Untargeted, mass emails sent to many people asking for sensitive information or encouraging them to visit a fake website.



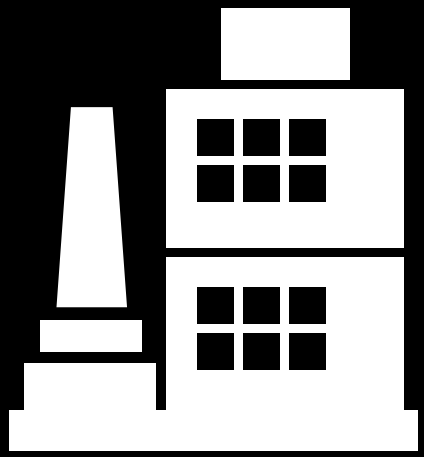
Spear-phishing

A more targeted form of phishing, where the email is designed to look like it's from a person the recipient knows and/or trusts.



Whaling

Highly targeted phishing attacks (masquerading as legitimate emails) that are aimed at senior executives.



Phishing the Enterprise

Developing an embedded simulated phishing campaign and program of continuous improvement across the enterprise.

Approval

First things first, get approval.

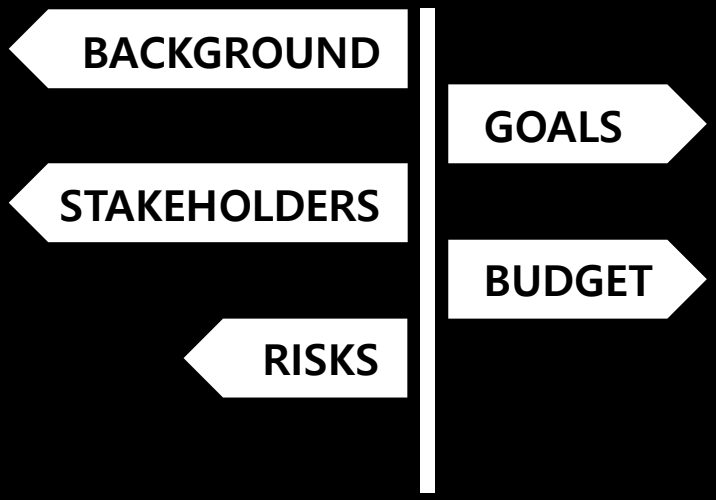
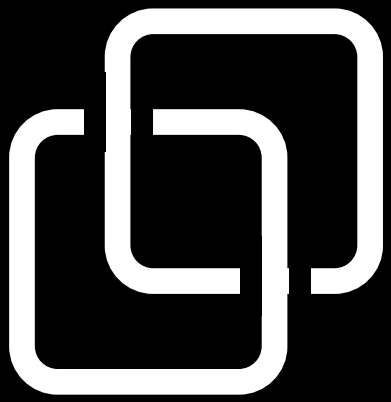


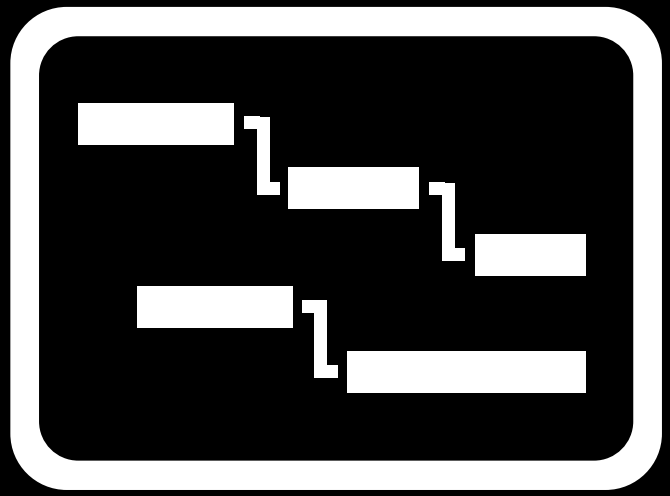
Chart your course

A project charter should not only establish basic information, but also reflects key stakeholders' common vision.



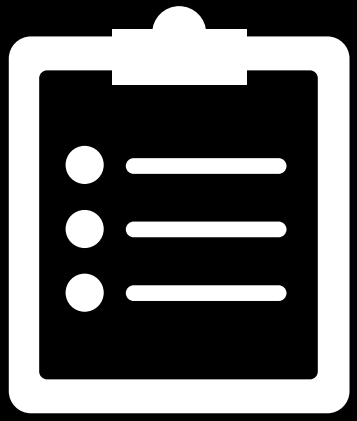
Select the vendor

Analyse business requirements, search for prospective vendors, request for proposal, vendor selection and contract negotiation.



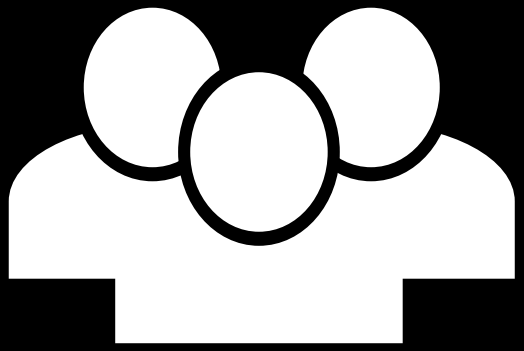
Get planning

Not having a plan is akin to going on a trip without a map and then complaining that you didn't get where you wanted to go.



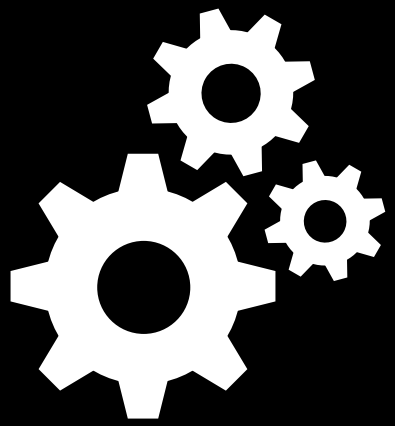
Have SMART objectives

Define the specific and measureable outcomes desired from the program.



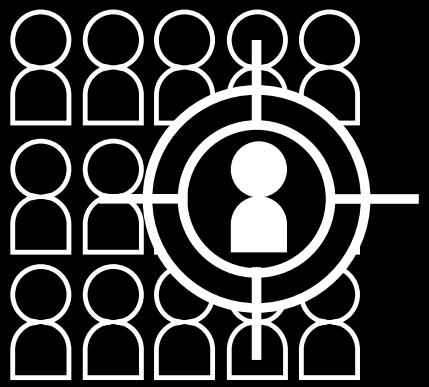
(Avoid) problems with stakeholders

Stakeholders can affect, or be affected by
the program actions, objectives and policies.



Get whitelisting!

Whitelisting vendor mail servers, IPs and domains is essential to ensure timely inbound delivery of emails and access to education.

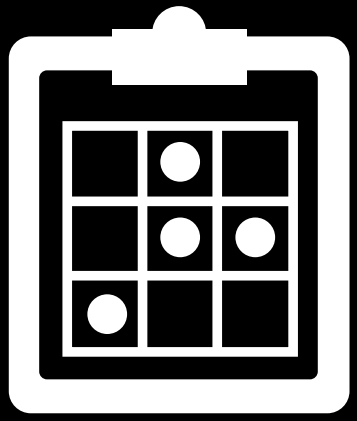


Who’s in the crosshairs?

Determine which target groups are appropriate to test and how are they exposed.

Think globally, functionally and locally

Consider targeting high-risk employees and specific functions as well as the total population.

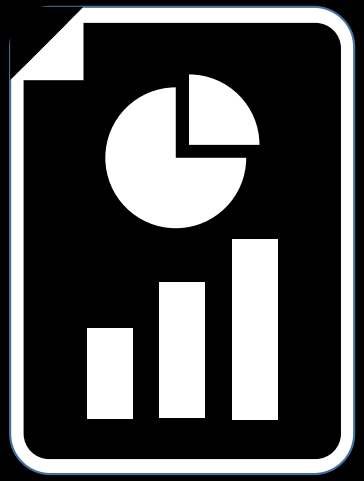


Create a simple, iterative program

Think about program goals, the specific needs of your enterprise and adapt your plan frequency to fit.

Inform the workforce

This what we are doing, and this is why we are doing it.

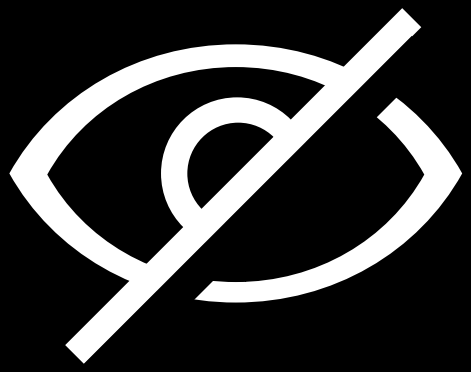


The KPIs, CSFs & ROIs

Measuring change in behaviour is key to demonstrating the value of your program.

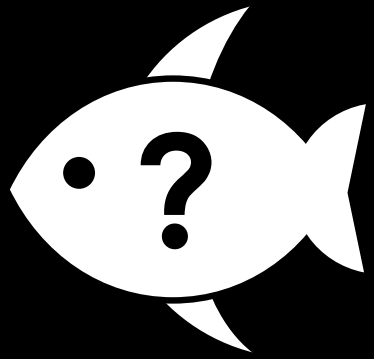
Success

So, what worked well?



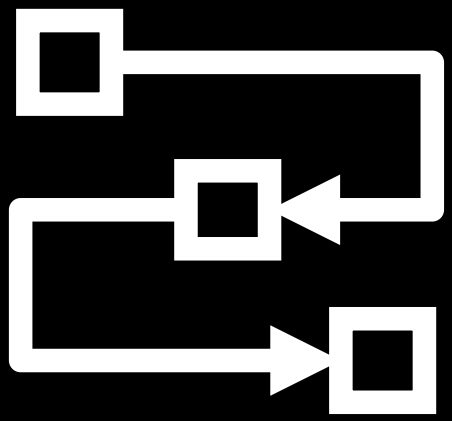
Works Council approval

Works Councils have a well-earned reputation as rigorous guardians of employee privacy rights – their consensus is essential.



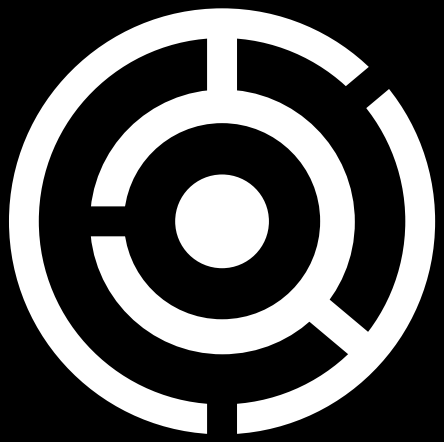
Reporting phishing

Reporting empowers employees to proactively participate in the enterprise's security program.



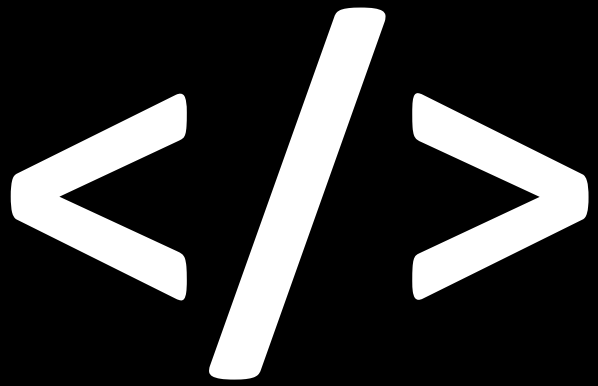
Focus on repeat offenders

Spending extra time on repeat offenders will result in improved alertness and behaviour.



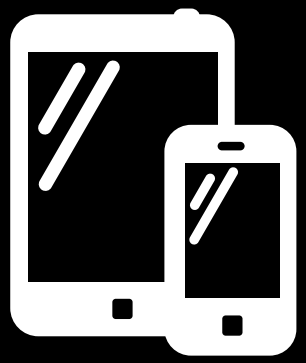
Challenges

Be aware of the known unknowns.



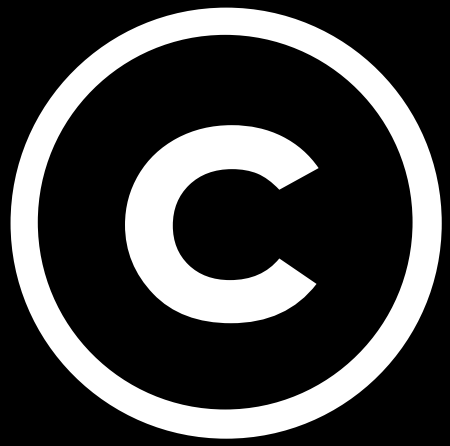
Why whitelisting isn’t enough

Email gateway filtering, spam confidence levels and group policy changes may need to be considered.



Mobile devices

Easy-to-install reporting buttons work well on PCs, but the growing mobile device environment presents significant challenges.



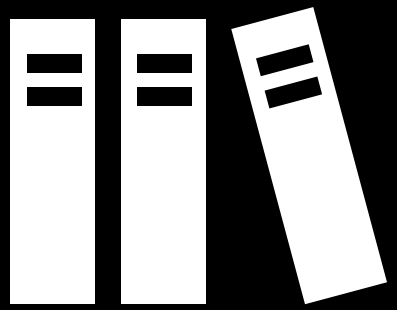
The Use of Company Logos

Cybercriminals have no problem violating the intellectual property of the company in their phishing messages.

SPAM

Reporting spam as phishing

Simplifying the process for reporting can lead to an increase in generic spam being sent to the security team for analysis.

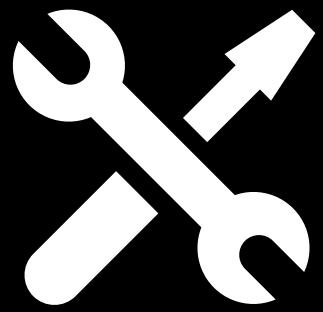


Lessons learned

Key takeaways that will help success.

Thank you.

Questions and comments are welcomed.



Building an Enterprise Wide Phishing Program

Workshop.