Resources for Chapter 9 – Awareness raising

RESOURCES

- **Raising user awareness of information security – Cardiff University, case study**
- **Development and use of a phishing exercise to raise awareness of phishing as an issue – Cardiff University, case study**

Raising user awareness of information security - Cardiff University, case study

This case study describes the approach taken by Cardiff University in its attempt to increase and improve user awareness of information security and thus mitigate, to an extent, information security risk.

The Case

Cardiff University is a member of the Russell Group, a group of 24 leading UK research intensive universities. It is the 12th largest university in the UK in terms of student numbers and features amongst its academic staff two Nobel Prize winners Professor Sir Martin Evans and Professor Robert Huber.

In July 2012 the Information Security Framework (ISF) programme was initiated. The aim of the three year programme was to create a framework by which the University can manage the significant financial and reputational risks involved in collecting, storing and using personal and other data and to assure external stakeholders that the University can be regarded as secure in relation to the way it manages its information/data. The programme considers all aspects of information security, both technological and organisational.

The programme was split into three stages: Foundations, Assessment and Evaluation and Implementation.

Challenge

The University employs a wide range of individuals carrying out a diverse set of roles. From staff tasked with managing the University estate to academic staff engaged in novel research, delivering education and so on. Engaging with such a diverse audience is not straightforward.

A further challenge when trying to engage individuals with the subject of information security, is the preconception that information security is a concern for the IT department alone, that information security is all about the confidentiality of information and that information security is about stopping people from doing things, creating barriers to using new technology (Cloud Storage for example).

Finding a mechanism for engaging and educating a broad range of individuals then, is the challenge.

The Study

The below activities cover the primary awareness raising activities delivered by the Information Security Framework Programme between January 2013 and June 2014.

In addition to the below, briefings and updates about the programmes objectives and progress were delivered through a range of regular communication channels: staff meetings in Schools, various departmental briefings, updates in a range of internal publications/ newsletters, emails etc.

Connections

At the outset of the programme an online Information Security Community was created using the Universities online collaborative workspace called 'Connections'. The purpose of this community was to have an area, accessible only to members of staff, where updates about the programme could be posted, key documents shared for comment and review, and to blog about important information security news stories which related to the work of the programme.

Information Security Risk Assessment Workshops

These workshops were carried out as part of the Assessment and Evaluation phase of the programme in order to identify the most significant risks affecting the University's information assets. Workshops involved academic and professional services staff and on average involved 10 participants. The workshops ran from February 2013 to July 2013 were carried out to assess the risks to each of the Universities information assets. The risks scored as part of the workshops were compiled into formal reports and circulated to participants after the workshop. Participants were subsequently invited to the Connections Community in order that they could continue to engage with the programme. The products of all the workshops, sixteen in total, were consolidated into an Overall Risk Report and used as the basis for identifying suitable control measures which could be delivered through the programme.

Whilst the workshops were not a communications exercise they did serve to create a core of individuals who were aware of the programme and had experienced the chosen risk assessment methodology.

Survey

In March 2013, the first of an annual, all-staff, information security survey was released. The survey asked staff for their views on a range of information security questions, from how secure they feel the University keeps their data, to what measures they take at home to protect personal computers from which they connect to the University.

The survey was announced in an email to all staff sent in the Vice Chancellors name, it was also advertised via an internal news feed, through the Connections Community, the programmes Operational Group (a cross discipline team with representatives from the Universities Colleges and Professional Services departments) and through various meetings.

The survey attracted an 11% response rate (655 of 6000 staff)

The 2014 survey will ask staff the same questions with the addition of two questions around increasing awareness of information security and importance of information security.

Teaser campaign

During the initial stages of the implementation phase of the project, one of the key deliverables was an information security website http://cardiff.ac.uk/isf.

In order to generate interest in the run up to the launch of the website the concept of a teaser campaign was used. This took the form of a life sized robot (Appendix 1) carrying a sack of data. This decal was installed in buildings across the University campus in areas of high foot fall in order to get staff and students curious about what it was for, so that when subsequent communications and activities took place there was a pre-established interest.

Once the robot had been on display for two working weeks a set of 6 posters (Appendix 2) were deployed across the campus (in both English and Welsh language). Each poster provides advice on a specific information security topic. The topics for the posters being chosen to resonate with issues which affect users both in their personal lives as well as in a University context. To accompany the posters a set of stickers were also distributed across campus (Appendix 3). The stickers consisted of a robot from the posters as well as the URL or the information security website and were located in unexpected areas to catch the eye of passers-by and generate traffic to the website.

Website

The culmination of the teaser campaign was the launch of the Cardiff University Information Security Website http://cardiff.ac.uk/isf.

The website provides information about the ISF programmer, advice on a variety of information security topics, a home for the new information security policies generate by the programme, information to assist researchers when completing information security questionnaires as part of research bids, hosts the University Information Classification Scheme and associated handling rules, and a blog for the programme to share information security news.

In the first 3 months the site has received over 1500 unique visitors and 6872 page views with visitors viewing an average of 5 pages per visit.

Phishing Exercise

During early June 2014 the programme initiated a phishing exercise. An email purporting to be from the University IT department, but sent from a .co.uk domain and containing various other 'give-aways' was distributed to all University staff (some 10,000 email addresses) over a period of 3 weeks. The aim of the exercise being to test susceptibility to phishing and provide a metric for the programme to measure over time. Upon receipt of the phish, the user was prompted to click on a link advertised as taking the user to a site to login using their University credentials and apply for extra network drive capacity. The page which the user is actually taken to http://sites.cardiff.ac.uk/isf/cardiff-university-phishing-exercise/ provided the user with advice on how they could have identified the email as a phish and how to avoid such scams in the future.

Statistics were generated about both the numbers of staff reporting the email as suspicious through the IT Service Desk as well as numbers of unique visitors to the web page.

Password Change

Whilst not an awareness raising exercise in itself, the ISF programme has initiated a project to change the University Password Policy. As part of this project the robot from the 'Passwords can be very predictable' poster has been deployed to all University managed workstations as an icon. The icon launches a web browser to the ISF website page describing the changes to the policy.

Next Steps

Evaluation

To evaluate the responses to the 2014 information security survey and assess the effectiveness of the programme in changing the levels of awareness of information security and to identify areas for further effort.

Training

One of the next steps for the programme is the development and roll out of mandatory information security awareness training for all staff and Post Graduate Researchers. This will further communicate to staff the importance of information security awareness but in a more formal setting where there will be enforcement around compliance.

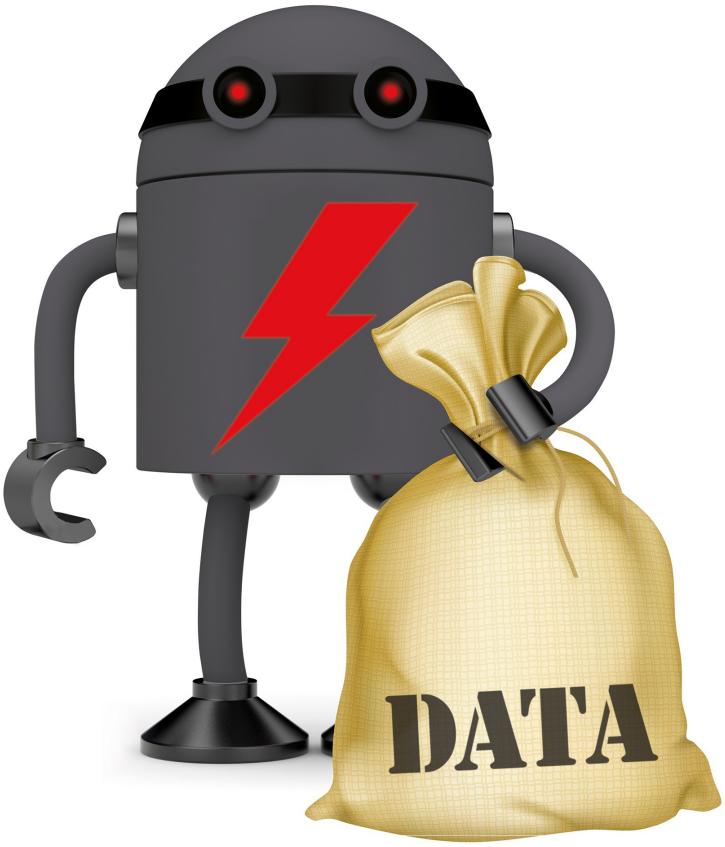
Appendices

Appendix 1 – Dark Robot Decal

Appendix 2 – ISF Posters

Appendix 3 – ISF Example Sticker

Appendix 1 Dark Robot Decal



Appendix 2 - ISF Posters

Protecting your identity online **is easy**

Simply...
- Use firewall protection
- Use anti-virus protection
- Use anti-spyware protection
- Seek help if you see warning signs
- Update your anti-virus software regularly

Think. Secure. Protect.

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

For more information visit: www.cardiff.ac.uk/isf

Protecting yourself online **is easy**

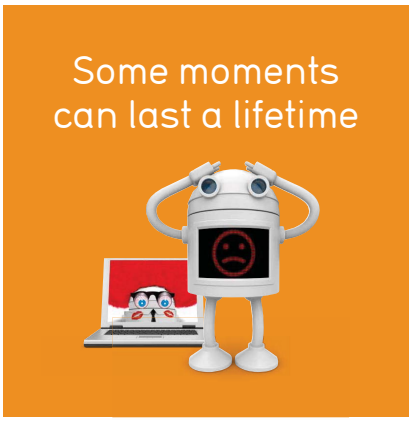
In a Phishing scam, a criminal sends you an email message that appears legitimate (e.g. your bank) The message will usually contain a link asking you to 'verify' or 'confirm' your information. This link will take you to a counterfeit website.

Simply...
- Delete suspicious messages immediately
- Never respond to email requests for personal info

Think. Secure. Protect.

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

For more information visit: www.cardiff.ac.uk/isf



Protecting yourself online **is easy**

Simply...
- Always check your privacy settings
- Consider carefully how much personal information you make public online
- Think before uploading embarrassing pictures

Think. Secure. Protect.

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

For more information visit: www.cardiff.ac.uk/isf

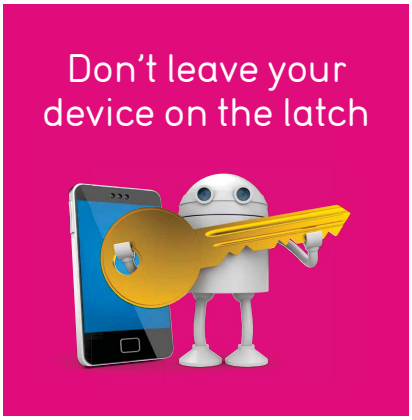
Protecting yourself online **is easy**

Simply...
- Use a strong password
- Use a mix of letters, numbers and symbols
- Use different passwords for each account
- Protect your personal data at home and work

Think. Secure. Protect.

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

For more information visit: www.cardiff.ac.uk/isf



Protecting your identity online **is easy**

Simply...
- Always lock your device
- For added security set your device to automatically lock when it goes to sleep
- An unlocked device leaves access to your data

Think. Secure. Protect.

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

For more information visit: www.cardiff.ac.uk/isf

Protecting your identity online **is easy**

Simply...
- Keep your security software up to date
- Allow automatic updates for security patches
- Install firewall and anti-virus software
- Scan external devices (e.g. USB sticks) for viruses

Think. Secure. Protect.

CARDIFF UNIVERSITY
PRIFYSGOL CAERDYDD

For more information visit: www.cardiff.ac.uk/isf

Appendix 3 - ISF Example Sticker

Development and use of a phishing exercise to raise awareness of phishing as an issue - Cardiff University, case study

What is a phish?

Phishing is the name given to the practice of sending emails at random, purporting to come from a genuine organisation. This sort of email attempts to trick the recipient into entering confidential information, such as credit card or bank details, usernames and passwords. The links contained within the message are false, and often re-direct the user to a fake web site.

Commissioning the exercise

As part of the University wide Information Security Framework programme, and as a method for addressing a specific risk around user awareness of phishing, it was identified that an exercise to raise awareness of phishing would be beneficial.

Authorisation for carrying out the exercise was secured through the Information Security Framework programme Steering Group and communicated to the University Business Change Portfolio Oversight Group. Both bodies include representation from senior Professional Services and Academic members of staff.

Carrying out the exercise

The exercise consisted of sending all University staff an email which was representative, in terms of the level of sophistication, of the sorts of phishing emails routinely received by University staff.

The email warned recipients that they were running low on storage quota and to follow a link to enter their credentials and apply for extra storage.

The email contained a number of tell-tale signs of being a phish including, spelling mistakes, a non '.ac.uk' originating email address, URGENT markings and an embedded hyperlink taking users to an address different to that which it advertised.

Those recipients who subsequently clicked on the hyperlink were taken to a University hosted 'landing page' (via a redirected web address with a domain matching the one from which the email was sent) which informed them that the email had been a phishing exercise run by the University, provided a reassuring message about the purpose of the exercise, highlighted the tell-tale signs that the email was a phish and provided advice and links to further information on phishing. By using this mechanism targeted education on how to avoid falling for phishing emails was provided to those most likely to fall victim to such attacks.

The email and landing page can be viewed here http://sites.cardiff.ac.uk/isf/advice/phishing/cardiff-university-phishing-exercise/

By keeping awareness of the details of the exercise to a limited group (IT Service Desk and Programme Team) it was possible to ensure that the reactions of staff, including the responses of devolved IT staff within Departments and Schools were as they would be had the email been a real phishing attack.

Where individuals contacted the IT Service Desk, or read the content of the landing page they were encouraged to keep their awareness of the exercise to themselves and not warn colleagues.

Unique hits to the landing page were measured using Google Analytics (access to the landing page was only possible through receiving and clicking on the link in the phish).

Facts and Figures

- Emails were sent over a period of approximately one month to 9001 email addresses at a rate of 500 emails per day.
- A total of 1905 users followed the link in the phishing email which represents 21% of the email recipients.
- A total of 291 calls were placed to the IT Service Desk to report the phish (3.2%)

Learning Points

- Some staff, particularly those who work in IT, recognised the email was a phish, but chose to click on the link to see what would happen/where it would take them. It was not possible to quantify the number of these 'curiosity clicks' and so they cannot be disaggregated from the results.
- There may be staff who avoided the phish by virtue of not reading the email, in future exercises it may be desirable to be able to send a follow-up or chase email.
- Levels of reporting to the IT Service Desk were relatively low (3.2%) and work is needed to encourage staff to report such threats.
- There was evidence of local reporting mechanisms at School and Department level which are not formally recorded and which may have significantly increased the percentage figure for staff reporting the phish.
- The exercise tests whether users will click on potentially dangerous links, but as an inherent assumption that they would then enter their credentials. As above some staff, in order to investigate how 'good' a phish it was were clicking on the link out of curiosity but would not have entered credentials.

When repeating the exercise in the future, users should be delivered to a screen on which to enter ones credentials, doing so and selecting enter should then deliver the user to the landing page.

Next Steps

- The outcomes of the exercise will be communicated to the University Information Security Review Group.
- The outcomes of the exercise will be publicised across the University to further raise awareness and to flag the advice to those who have not already accessed it through the phishing email.
- A further exercise is to be planned taking on board the learning points.