COMS30038 — SECURITY BEHAVIOURS

LAB 1: CRAFTING SOCIAL ENGINEERING ATTACKS

This week you will be getting some hands-on experience creating some of the most typical and effective forms of social engineering attacks: scam emails and phishing websites. The aim is that by getting you to create these attacks, you'll have a better intuition for how they work and how they might be countered. *Using these methods against people without their prior agreement is a crime. Your intended learning outcomes do not include "getting convicted". Please do not commit crimes as a result of this unit.*

There is also a short OSINT challenge at the end, for those of you who want to hone your investigative skills. It requires no deceptive interaction with any person or service provider. Everything you need is openly accessible public information.

1 SCAM EMAILS

Look at the email samples in `emails.zip`. Each file is a real example of a scam email of some form or another.

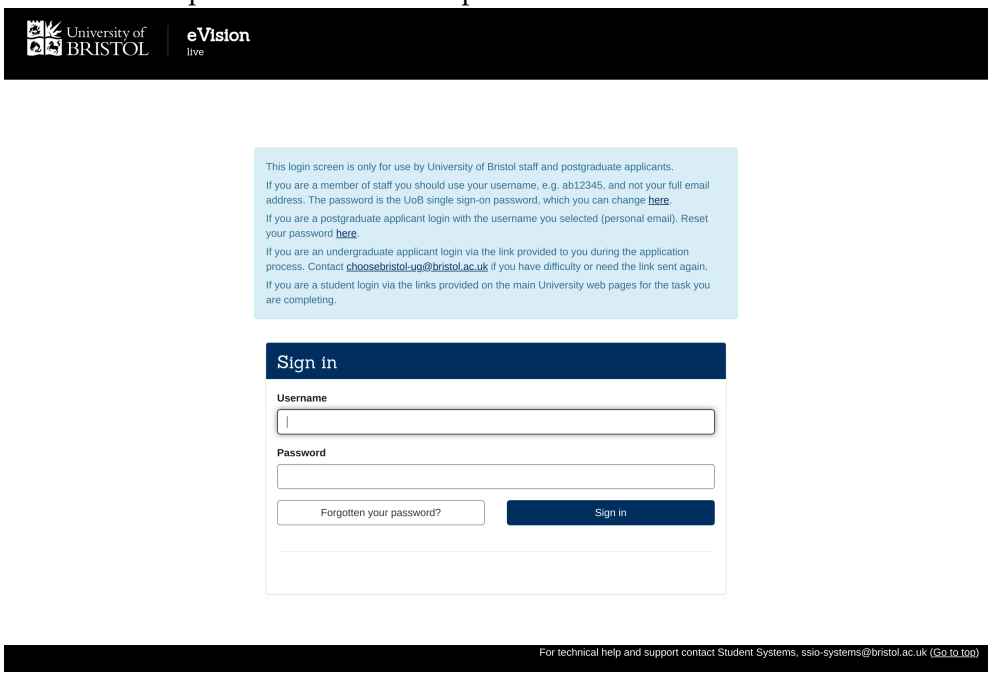
1. Together with your group, discuss the different scam email formats. For each, try to cover:
   (a) Whether anyone you know has fallen for a scam like this;
   (b) What marks it out as a scam;
   (c) Which persuasion strategies can you see at work in the scam?
2. Collaboratively or individually, write a new scam email in one of the genres you've seen. Try to make use of the same persuasion principles, but without reusing the same material. Post your efforts on the Padlet at `https://padlet.com/matthew_john_edwards/scam-letter-attempts-s4df7uof9phgq9w8`.

2 PHISHING SITE

We are going to create phishing site that can harvest credentials from university students. Please note that this is a learning exercise only, with the aim of showing you how easy phishing can be, and the sorts of errors phishers might make. Anyone actually *deploying* these methods against fellow students will be met with severe repercussions. *Also, please do not release your phishing page publicly (e.g., on Github) – there's no need to make things easier for real criminals.*

FIRST You will need access to a machine with **Python 3** installed on it.

A good target for a phishing page is a sign-in page that people encounter regularly, ideally while they are following links to other resources or meeting administrative requirements. For example:



You are going to create a phishing page that:

- Fully duplicates the look of Bristol's eVision login page[1];
- Records submitted credentials to a file;
- Seamlessly redirects users to the real eVision page, so that they can believe they simply mistyped something.

Stage 1 is to obtain a copy of the web page files. You can do this via your browser by clicking 'Save as' and selecting 'Web page, complete'. This will save both the HTML and most of the associated assets on the page to a local directory, and rewrite a lot of the internal references appropriately.

[1] `https://evision.apps.bristol.ac.uk/urd/sits.urd/run/siw_lgn`

To test this out properly, you'll want to launch a web server in the directory where you saved the web page. You can do this straightforwardly using a default Python module by running the command:

```
python -m http.server --cgi
```

The `--cgi` flag enables server-side scripts, which you'll need shortly. First, test out the site by navigating to `localhost:8000` in your browser. The page save function is not always perfect – spot and fix the differences by downloading any missing resources from the original page, and fixing references in your local files.

Stage 2 is to alter the form in the webpage so that instead of posting to the original eVision login page, it posts form data to a local script. Next, write that script! First of all, you simply want the script to extract the username and password fields from the POST data, and save them to a file locally. You'll want to look at the documentation for the Python `cgi` module in order to figure this out.

Stage 3 is to cover your tracks. Currently it is obvious that something has gone wrong with the password submission – the user doesn't get logged-in or redirected to the service they were expecting. If you were really harvesting credentials this would be a problem, because they are likely to investigate the issue and change their password. The simplest behaviour here is to convince the user that they mistyped their password, by having your script redirect them to the *real* login page.

Finally:

1. Compare solutions with others in your group. Can you point out flaws that others missed?

2. What are the signs still visible that indicate your page isn't the genuine sign-on page? Could anything be done to make these signs less obvious?

3. How could you deliver the page so that it gets used by a target? What hurdles would you have to overcome?

4. Given what you now know about implementing a phishing site, can you think of any methods (technical support or straightforward advice) to support people and prevent them falling for them?

3 OSINT CHALLENGE: THREE PICTURES

Try to answer the below questions about images. All the required information is openly accessible on the web.

1. There's a picture at `http://www.research.lancs.ac.uk/portal/files/22739740/Matthew_Edwards.jpg`. Hopefully you have some idea who the subject is, but:
   (a) When was the picture taken?
   (b) Who took the picture?
   (c) What is the photographer's opinion on velociraptors?
2. Now consider this picture:

   (a) Who is this person?
   (b) What subject did they pursue a degree in?
3. And finally, this stock photo from a Bristol website:

   (a) What did the photographer get for Christmas in 2019?
   (b) How old was the photographer when the photograph was taken?

4 WRITING PRACTICE

This section isn't part of the lab itself, but an opportunity for you to practice writing essay-style answers to (week-topical) questions. You can show your answer to your TA next week, or share in your group's Teams channel to get feedback on how you're answering questions.

1. Give an example of a time you've observed a peripheral persuasion strategy in practice – online or offline. This could be an advert, scam, or other form of social manipulation. Discuss how and why the examplified technique works or is intended to work, and what signatures give away the strategy as manipulative. [≈250 words]