DigiEduHack Solution
Edinburgh - Edinhack: DigiEduHack at the University of Edinburgh
Challenge: Edinburgh - Edinhack: DigiEduHack at the University of Edinburgh Challenge 2020

College Phish

College Phish: Crowdsourced Phish Detector

College Phish leverages historical and user submitted data to advise students and staff on the credibility of their emails, protecting people against scammers and fraud.

Team: Natural Mineral Water Sparkling 50% Recycled Plastic Open with Care as This is a Pressurised Container

Team members

Elena Lape

Members roles and background

Computer Science and Artificial Intelligence undergraduate && software developer. Finds joy in building creative projects and keeping things simple.

Contact details

https://twitter.com/elena_lape

Solution Details

Solution description

For years now, Edinburgh University and most other institution email servers have been plagued with phishing emails. Now that most teaching and studying happens on the interwebs, bad actors focus all of their attention on online activities. Phishing is one of the most common forms of online scams.

City of London Police revealed that Brits handed over **£19M in online frauds** in 2019, with malicious emails containing harmful links one of the most successful methods used by cyber-criminals. This is in the UK alone!

College Phish addresses this problem via crowdsourcing data from IT administrators and email recipients to advise people on the likelihood of their suspicious email being a scam.

Live app is here: https://collegephish.lape.io. (*Note: there isn't a lot of email data at the time of this submission*)

The app behaves as follows:

- Users copy and paste the content and the sender of a suspicious email they have received on College Phish.
- The user submission is checked against an existing database of known phishes (I got a dataset from our university's Information Services department), curated by the educational insitution's IT admins. Then:
    - If user submission matches a known phish, a similarity score is returned, and the user is advised on the likelihood that the email they have received is a phish (very high/high/low).
    - If there aren't any similar known phishes, the user can then check whether any other people have received a similar email. A similarity score is also returned.
- The app also checks whether that sender has previously been flagged by IT admins or other users as a potential scammer/spammer.

All new user submissions are sent to the user submissions' database. The IT admins can further investigate those emails, and, if needed, add them to the database of confirmed phishes.

College Phish is open source and MIT licenced, so other institutions are welcome to reuse and/or tweak the app.

Solution context

Now and in the foreseeable future, teaching and learning is nearly fully distributed. This means that bad actors focus all of their attention on online activities.

Unfortunately, educational email addresses are easy for scammers to target. Take a look at the following examples:

- thiscanliterallybeanything@gmail.com
- s16xxxxx@sms.ed.ac.uk, where 16 represents the year of enrollment, and the x's represent a 5 digit student ID

An educational email address typically follows a very predictable pattern. There is a finite number of variations it can have — the **entropy** is low. Therefore, an attacker doesn't need to go through the

hurdles of checking whether most of the email addresses they decided to target have a real person behind them. In addition to that benefit, they can also knowingly target a group with limited financial resources (students), or in a particular area (based on the email domain), allowing them to come up with *excellent* extortion scenarios designed specifically for that group.

Phishing *is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. (from phishing.org)*

Phishing is one of the most common online scams. Some phishes are obvious, but given the context about .edu email addresses, attackers can get pretty darn creative when it comes to drafting effective emails.

Everyone can fall victim to such crime, but new people on campus, international arrivals, non-native speakers, and generally non-technical people are particularly at risk.

IT support teams are working hard to reduce harm. They receive reports about phishing emails, but sometimes it's too late. Some administrators choose to put banners and warnings on emails that don't come from within the university network, but this isn't always effective — an average person receives tons of legitimate emails from 3rd party services, and seeing a big red banner on false positives might *desensitise* them to *all* warnings.

Solution target group

University and school students, teaching staff, support staff — everyone in the world with an email inbox.

Solution impact

People in the UK lost **over £19M in online frauds in 2019 alone**, a lot of it coming from phishing attacks. Even if a small percentage of those people could have easily checked the likelihood of their email being a scam, that's still **thousands** saved.

A few benefits of College Phish:

- A website like this can easily be shared in group conversations — this is important, because lots of conversations between students happen in informal channels.
- Universities' IT teams can have an insight of potential phishes, and review user submissions to be added to the main phish database.
    - This data can be used for staff training purposes.
    - Or shared with other universities for further training and integration.
- The app is very lightweight — it is cheap to deploy and use anywhere in the world.
    - User data can be crowdsourced from all over the globe.
    - ...or be unique to campuses.
- Endless opportunities for additional features: admin accounts, edu sign-ins, users forwarding emails to the app instead of going on a website, Outlook add-ons, gamification through leaderboards.
- Safer distributed learning experience
    - Greater protection of vulnerable groups: newcomers, international students, non-native English speakers, non-technical people.

Solution tweet text

College Phish is a crowdsourced phish detection tool, helping people around the world to protect themselves against scammers.

Solution innovativeness

College Phish moves away from big red "exercise caution" warning banners, which we are somewhat desensitised to. It leverages both the IT administrator expertise in confirming suspicions about emails, and crowdsourcing data.

To detect email content similarity, Dice's Coefficient is used, which is the algorithm that the string-similarity npm package implements.

The application is built in React and Node.js, using Firebase Firestore and Firebase Cloud Functions as a backend. It is a modern, quick, responsive, lightweight web app that doesn't require a lot of bandwith, making it cheap or free.

Solution transferability

College Phish can absolutely be made into WorkPhish or NeighbourhoodPhish — the *sea* of opportinity is endless. It is also possible to create a global College Phish version, where user submitted phishes could be sourced from all over the world, or regionally. For example, in the UK, one of the most common phishing scenarios is the "tax agency" — "HMRC" — contacting students about their pending tax returns. Therefore, it would make sense to have a College Phish just for UK-based students.

It shouldn't be too difficult to integrate the application's back-end with email service provider add-ons, such as Outlook Add-ons. Another alternative would be to set up a "listener inbox", like phishing@university.edu, that people could forward their suspicious emails to, and get a response with similarity results.

Solution sustainability

College Phish is Open source and MIT licensed. Any school in the world can use the source code of the app for free and add any aditional tweaks to it. It is relatively simple for an IT admin to deploy it on their servers or in the Cloud.

The costs of administering and hosting CollegePhish should be nearly free — provided there are less than ~20K API calls a *day* per each school (that's similarity score calculated for 20K emails checked a day). Even after that, Firebase costs are low, so the tool doesn't discriminate against region.

One piece of feedback I got from our Information Services team was how do we keep the information up to date and reduce the need for constant administrator intervention. To address this issue, each submission to the database has a timestamp. Instead of simply telling the user "X users found a similar thing in their inbox", the app's front end can be tweaked to say "X users found a similar thing in their inbox within the last Y weeks" etc., and then the user can make a more educated decision on the credibility of the email.

Solution team work

Having participated in many hackathons in the past, always with the presence of a very strong team, I wanted to challenge myself to do this hackathon solo. The hardest part was to find a problem that mattered. I wanted to build a working solution that could have a real, potentially global impact.

Writing the code in ~24 hours wasn't particularly easy, but as I've discovered, milky sugary tea is a hacker's best friend.

Big shout out to Edinburgh University's Information Services for providing me with the context of the problem and some training data!