**Group Project Idea:**

**PROJECT RUFUS**

For our group work project, we have voted to pursue Project RUFUS. This project was originally conceived during my current role at Apple in the Technical Support space, but has evolved to become a group work project. The idea behind the project is to assist people who are unsure if they have been the target of social engineering and scams.

Unfortunately in many instances, by the time a vulnerable technology user realises they may have been the target of an online attack, they have already provided sensitive information or financial details to scammers. Our group are setting out to create a community-based online notification and rating system that will provide advice to users on wether an email is fake or legitimate. Project RUFUS will be delivered as a software application, designed as a plug in to run along side users existing email systems.

The motivation behind the project is to help others with technology and protecting their online security and personal data. Unfortunately many vulnerable technology users have fallen victim to phishing scams, resulting in their sensitive information being abused. For example, financial information being used for financial gain or personal information being misappropriated by cyber criminals for nefarious purposes.

Further, a recent study conducted by the cyber security firm Proofpoint highlighted that 83% of respondents in a recent security survey indicated they had experienced a phishing attack in 2018. Of note, this was up 76% from the previous year. Also interesting to note was that the study stated security awareness training had a significant impact on preventing these kinds of attacks (Spadafora, 2018). By developing Project RUFUS, our group hope to spread awareness of phishing attacks and educate vulnerable online users, such as the elderly, parents, middle aged adults, and people with busy lifestyles who may not be aware of current scams or attacks.

The key features of Project RUFUS are as follows:

**Real-time awareness:** Project RUFUS will be a real-time awareness tool that will work to benefit the community. This is not a tool to replace junk mail filters, rather a tool that should be viewed as an enhancement to existing systems.

**Education tool:** Our aim with this project is to have an education tool to help spread awareness of phishing attacks and other online scams.

**Community based:** The project will rely on active participation from the community. The service will be based on members of the community reporting information to the project that will inform the advice and rating system delivered through the software.

**User-friendly:** Project RUFUS will aim to be a user-friendly experience. The target audience of this project are those less likely to be confident with technology, such as the elderly. Therefore it is crucial information is delivered in an easy to understand format.

**Colour coded risk advice:** The project will use a basic traffic light colour coding system to advise of risk. Green = safe, the email is safe to open. Yellow = caution, the email is deemed suspicious, exercise caution. Red = stop, the email is known as malicious, delete and do not action.

**Accessibility:** The project aims to be accessible to multiple users. There will be accessibility options built into this project, such as a voice over option for the visual impaired. The simple colour coding system also aims to overcome language barriers by applying a universal, easy to understand rating system for advice.

**Not-for-profit service:** There will be no cost to install or use RUFUS. The goal of this project is to help people, not to profit from their vulnerability. The project will seek support from tech companies to supply assistance in the form of volunteering people and knowledge to actualise the project. The project will also approach financial institutions (banks etc) for sponsorship of the project. It is likely sponsorship could be gained from financial institutions as the reduction in phishing attacks could see a reduction in financial claims or losses for their clients.

The tools and technologies that our group will require to develop Project RUFUS are:

* Internet access will be required to research and develop the software application, as well as to keep the application running with the most up-to-date information.
* A server will be needed to store the data required for the plug in to function.
* The software will need to be compatible with all major email servers and protocols in order to reach the most amount of people.
* There will be a need to experiment with different portable and desktop devices to ensure the software is functioning properly.
* Voice over technology will be required for the accessibility options envisaged for the project.

**Skills required:**

Hardware: Our group will need to learn how to build a cloud-based server that can synchronise with the app/plugin over different platforms. Our group will need to learn how to collate emails the plug in sends to the server with the different rankings for each user. It will also need to be able to send “live” updates to the plug in as well.

Software: An in-mail app plug in would be the best way for my project to reach the intended audience. It needs to be written so it can plug in and work within the inbox and be easy to see, read and understand. It would need to suitable for all apps and email accounts if possible.

As our group are all relatively new to the world of programming, we are yet to learn the skills required to realise our vision in creating Project RUFUS. As we continue our tertiary education, we expect to gain a better understanding of the tools that will be available to us to be able to create this project. We will also gain a better understanding of the resources and costs that will be involved to develop this project. We anticipate there will be many unforeseen obstacles throughout this project, however we will require the skills to be highly adaptable in order to modify elements of our project and ensure its success.

Our desired time-frame for the implementation of Project RUFUS would be 12 months. However, as we are only just embarking on our university studies, we think a more reasonable time frame will be 2-3 years. This will allow us to continue to develop the skills and knowledge needed, through university study, to be able to actualise this project. We hope the outcome of this project will be a dramatic reduction in the amount of people impacted by phishing attacks and scams. While we are realistic that we will not be able to stop the cause of the problem, we are confident that we can initiate massive harm reduction by influencing the targets of these attacks. Through timely education and advice, we aim to significantly minimise the risk to vulnerable internet users.

**Rav Comments:**

Addition to section - Accessibility:   
The project aims to be accessible to multiple users. There will be accessibility options built into this project, such as a voice over option for the visual impaired. The simple colour coding system also aims to overcome language barriers by applying a universal, easy to understand rating system for advice. <my addition>The colour coding system can also be calibrated for the different varieties of colour blindness, allowing users to adjust the levels of severity with a colour that is easily identifiable for them.</my addition>

<my addition>New section below Accessibility - Encryption: Any data we do collected will be anonymous and only to improve our algorithm in detecting dangerous emails. All information that is sent to our servers through our email plugin will be 256-bit end-to-end encrypted. This means that no one but the computers see's the data coming through to it.</my addition>

**Dane Comments:**

Will it include measures to make sure that the app itself can't be hacked, or how will it prevent scammers from recreating a "green light".

E.g scammers create a hack to let the email slip through and green light the email. People then mistakenly trust that it’s ok.

What technology will be in place to prevent this?

What skills will we need to ensure we get that right?

In regards to testing the project, how would we do that? Would we use our own developed skills to try and see if we can beat it?

Would we contract an external specialist such as Acumenis (BNE based penetration testing company) to test it for us?

What is the reason to make it not for profit? I think it has the potential to generate significant revenue if sold as a package to big business.

I realise the intent is to help people too, but no reason we can't make money if we put a heap of work into it.

Will it be usable on any device? What plans do you have to achieve this?

Will different devices require different skillsets to implement? What are these?