Week 1: Welcome to Human-Computer Interaction

Nicole Meng-Schneider and Dr Tara Capel

Part of slidedeck inspired by Dr Kami Vaniea

Who are we?

Dr Tara Capel

Nicole Meng-Schneider

Photo by Niels And Marco on Unsplash

Photo by Victor Freitas on Unsplash

Related to HCI

Photo by Jessie McCall on Unsplash

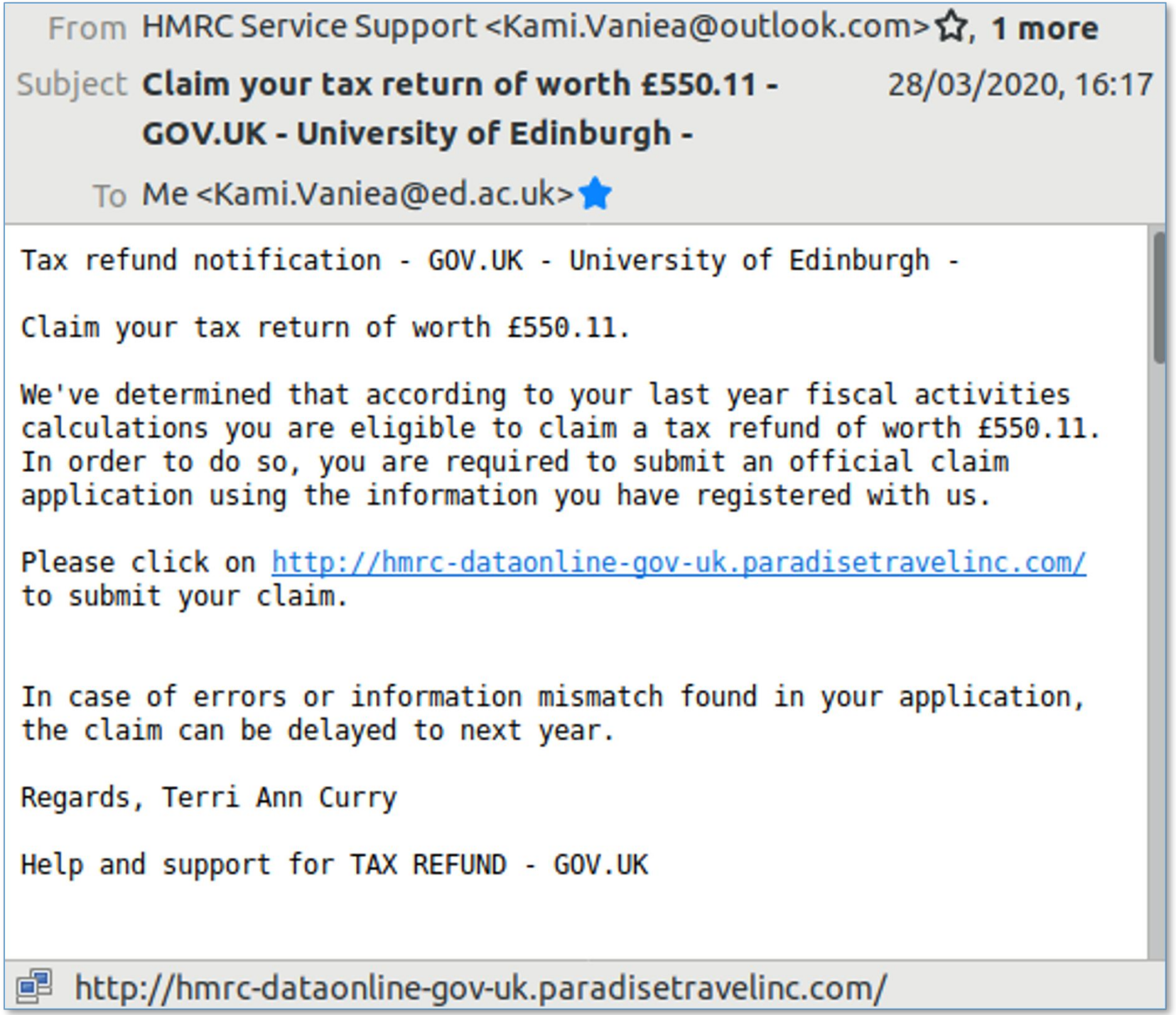
Think – Pair – Share

What other examples can you think of?

Think for 1 min
Discuss with your neighbour for 2 min
Share with the class for 3 min

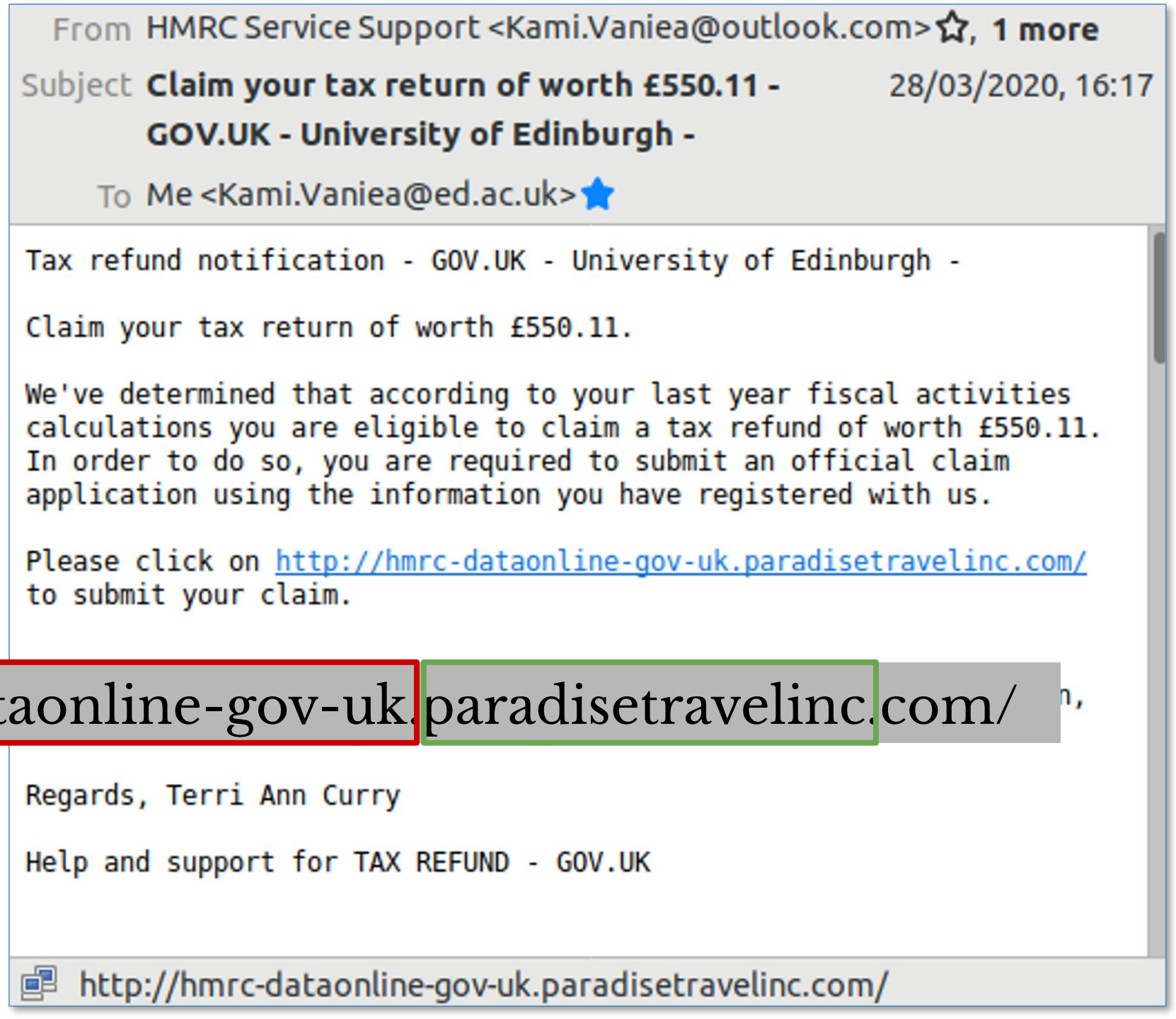
HCI is everywhere.

URLs are used in Phishing



URLs are used in Phishing

http://hmrc-dataonline-gov-uk.paradisetravelinc.com/



People can't read URLs*

None of these go to Paypal

- paypal.com.login-myaccount.policy.country
- paypal.com.updates-information-accounts.ga
- paypal.com.account.update.amquipac.org
- paypal.com.login.summary-limited-account.gq
- paypal.com-websecure.limited
- paypal.com.resolution-ticket.tk
- www.update-paypal-informations-account.ga

* Sara Albakry, Kami Vaniea, and Maria K. Wolters. 2020. What is this URL's Destination? Empirical Evaluation of Users' URL Reading. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20). Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376168

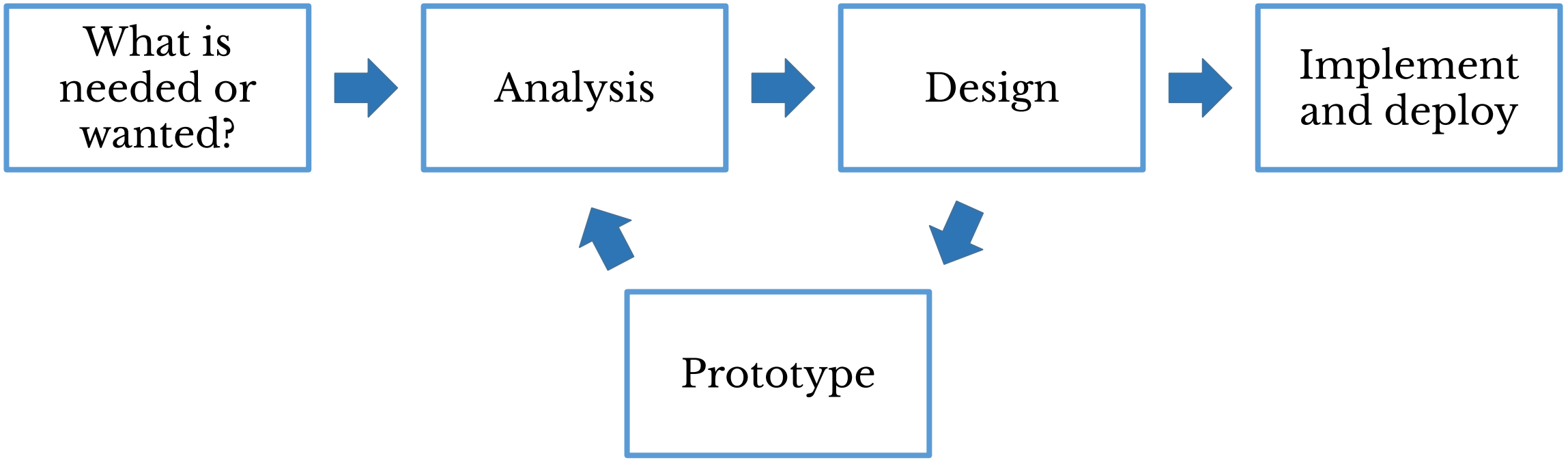
People can't read URLs*

None of these go to Paypal

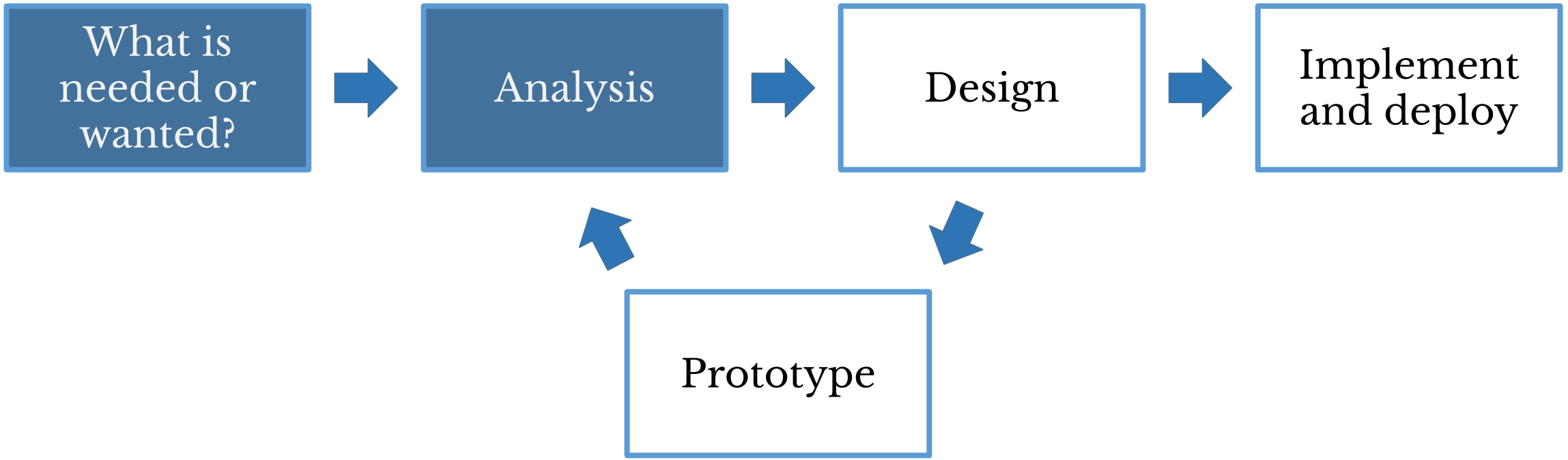
- paypal.com.login-myaccount.policy.country
- paypal.com.updates-information-accounts.ga
- paypal.com.account.update.amquipac.org
- paypal.com.login.summary-limited-account.gq
- paypal.com-websecure.limited
- paypal.com.resolution-ticket.tk
- www.update-paypal-informations-account.ga

* Sara Albakry, Kami Vaniea, and Maria K. Wolters. 2020. What is this URL's Destination? Empirical Evaluation of Users' URL Reading. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20). Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376168

Design Process



Design Process



Run survey to verify theory

RQ: Can people differentiate between parts of a URL?

- facebook.profile.com
- mobile.twitter.com
- profile.travbuddy.com
- weheartit.mobile.com
- bbc.profile.com
- mobile.cnn.com
- profile.dunfermlinepress.com
- haysfreepress.mobile.com
- paypal.profile.com
- mobile.westernunion.com
- profile.purepoint.com
- revolut.mobile.com

* Sara Albakry, Kami Vaniea, and Maria K. Wolters. 2020. What is this URL's Destination? Empirical Evaluation of Users' URL Reading. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20). Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376168

Run survey to verify theory

RQ: Can people differentiate between parts of a URL?

Results:

8% of participants consistently answered with the domain (correct answer)

92% of participants cannot read a URL.

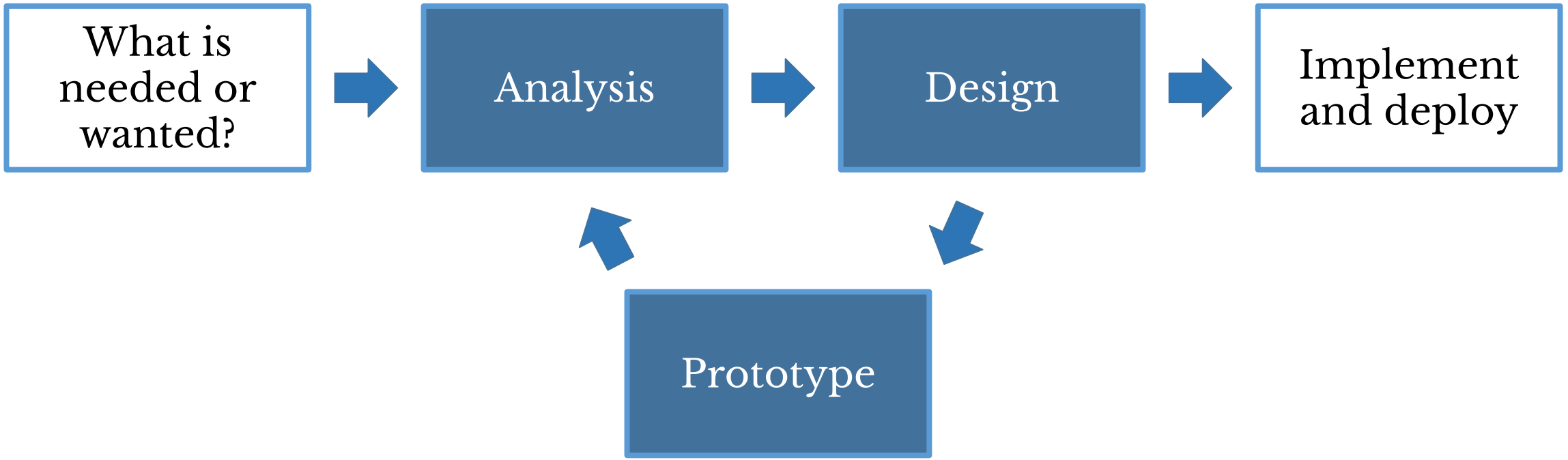
* Sara Albakry, Kami Vaniea, and Maria K. Wolters. 2020. What is this URL's Destination? Empirical Evaluation of Users' URL Reading. In Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (CHI '20). Association for Computing Machinery, New York, NY, USA, 1–12. https://doi.org/10.1145/3313831.3376168

92% of participants cannot reliably answer this question:

Does this URL go to Facebook?

`https://facebook.mobile.com`

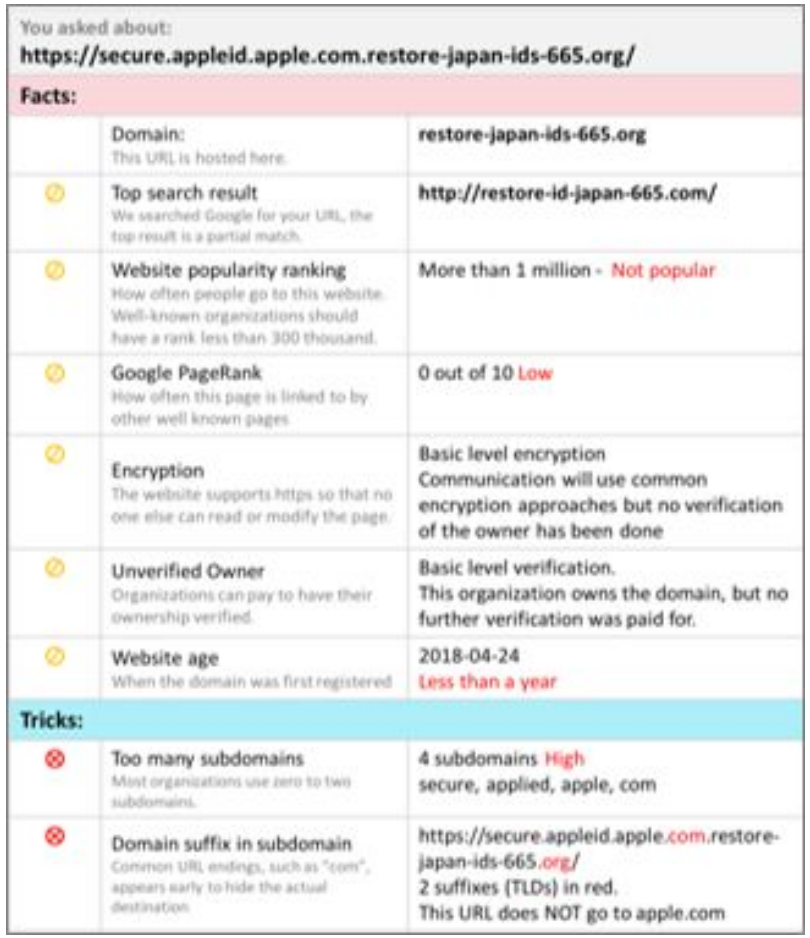
Design Process



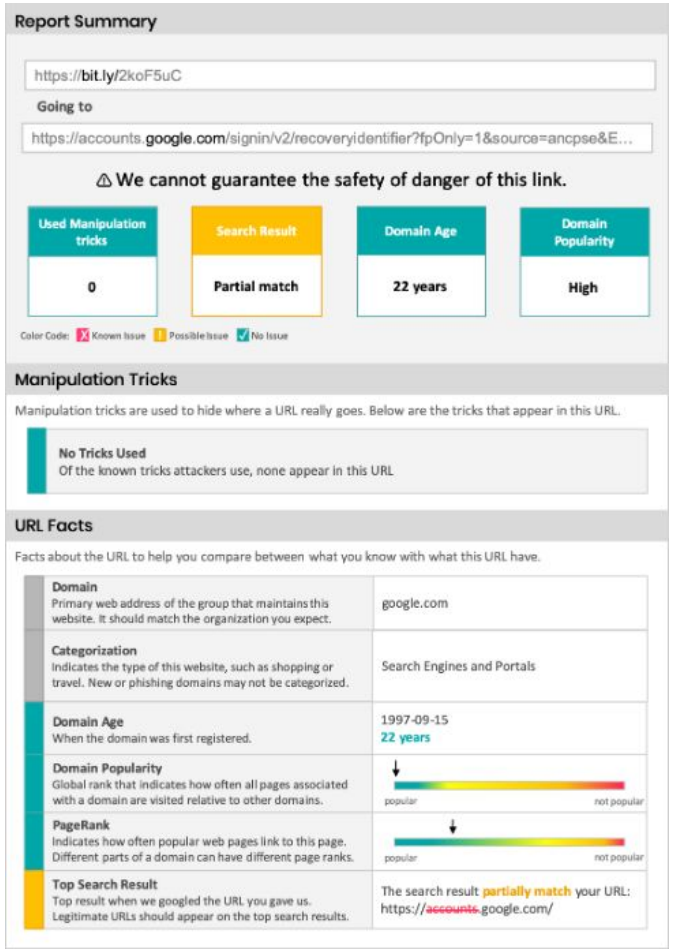
Designing Methodology

Initial Design

Inspired by (Kelly et al, 2009)

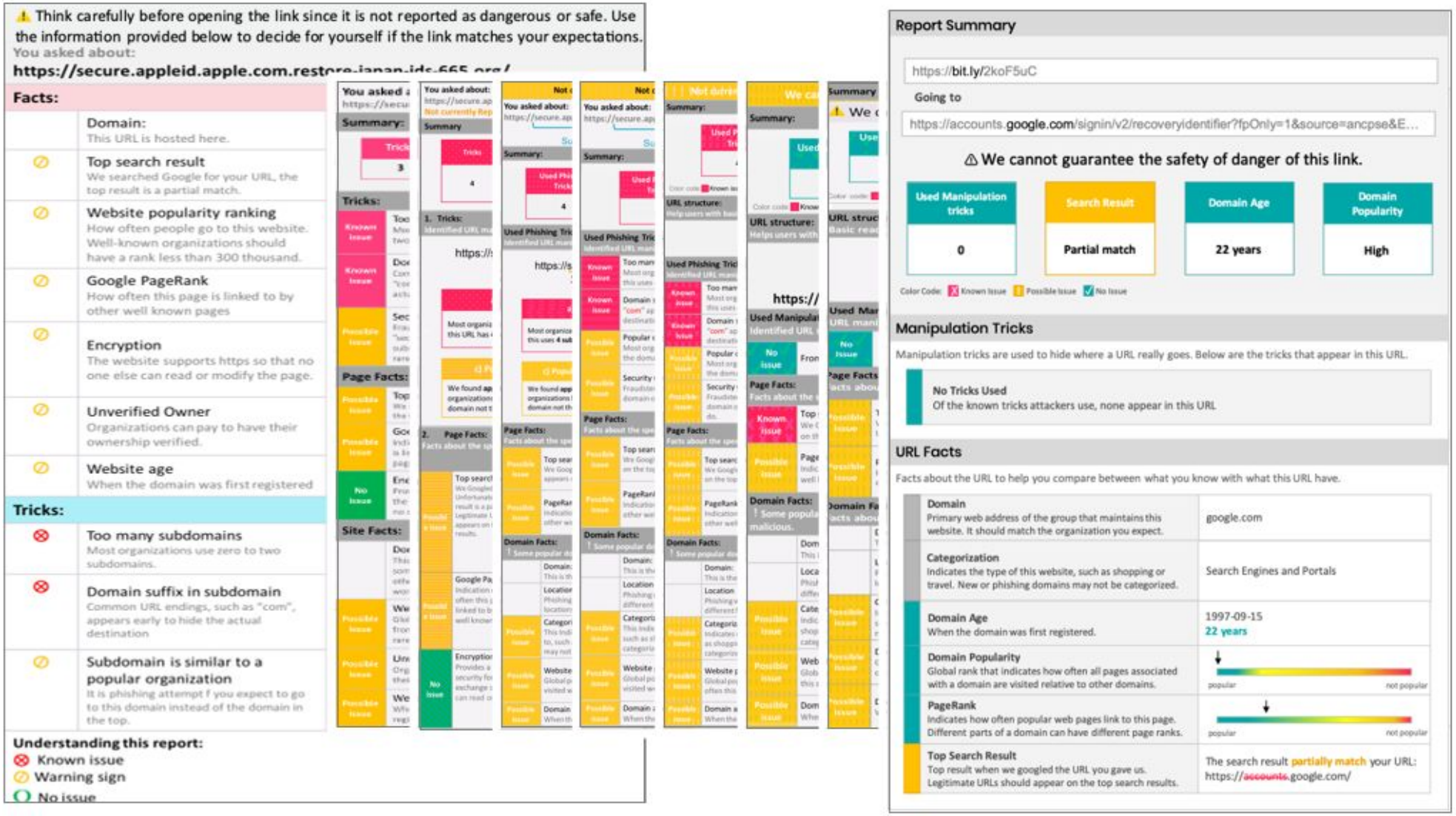


After 8 Focus Groups



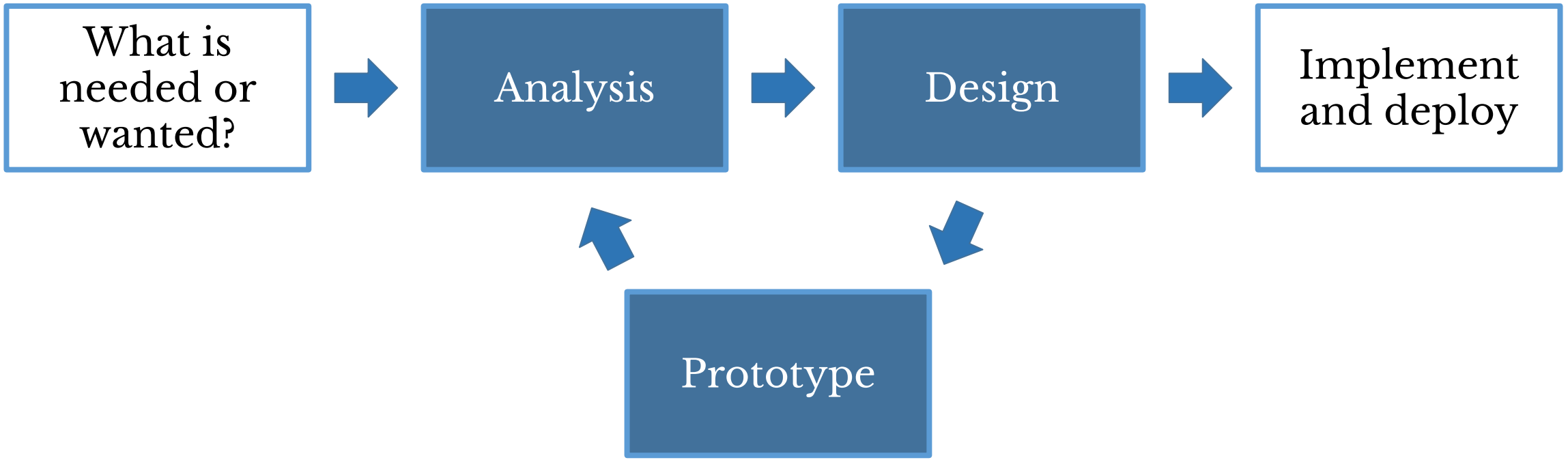
Kholoud Althobaiti, Nicole Meng, and Kami Vaniea. 2021. I Don't Need an Expert! Making URL Phishing Features Human Comprehensible. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21). Association for Computing Machinery, New York, NY, USA, Article 695, 1–17. https://doi.org/10.1145/3411764.3445574

Design Iterations



Kholoud Althobaiti, Nicole Meng, and Kami Vaniea. 2021. I Don't Need an Expert! Making URL Phishing Features Human Comprehensible. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21). Association for Computing Machinery, New York, NY, USA, Article 695, 1–17. https://doi.org/10.1145/3411764.3445574

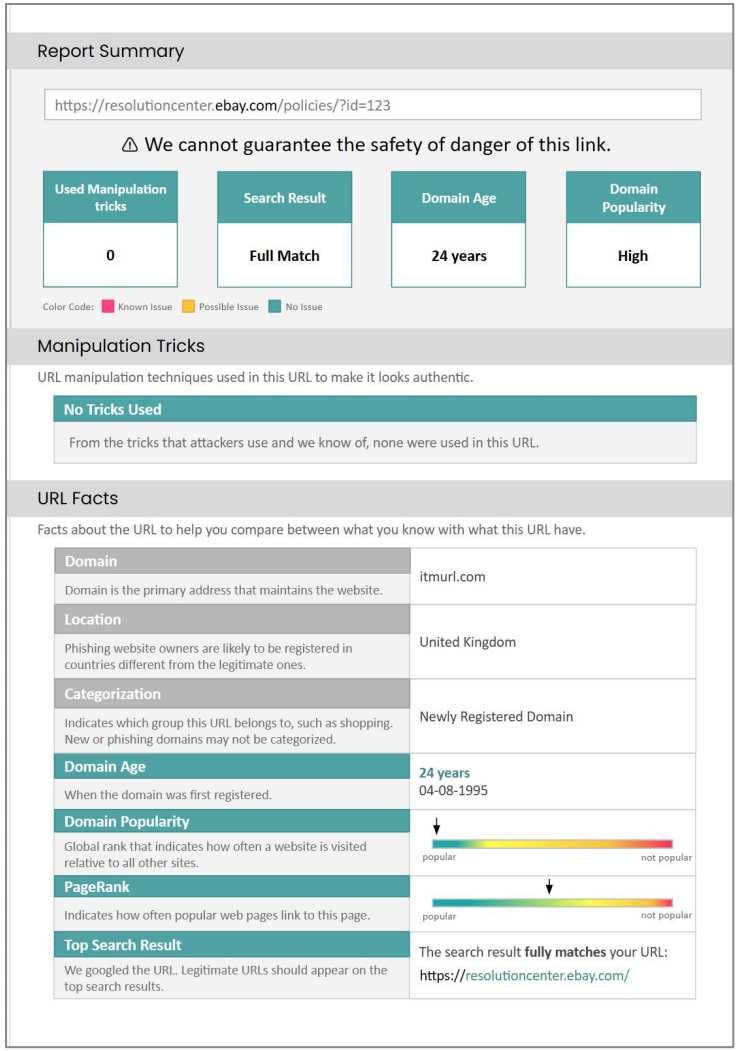
Design Process

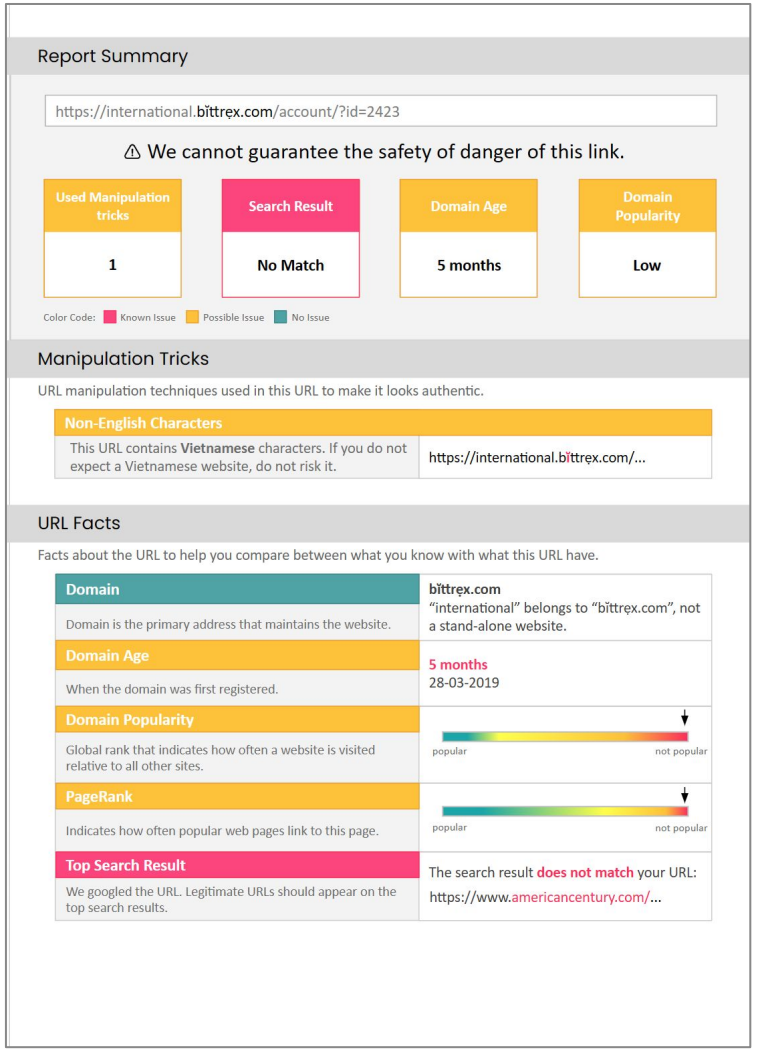


Design Validation

Report Appearance

- Tested on 2023 safe and 2617 phishing URLs
- Test appearance of visual cues and colours
- only 3.4% of safe URLs showed a “trick”
- Safe URLs were normally green and phishing ones had red rows





Kholoud Althobaiti, Nicole Meng, and Kami Vaniea. 2021. I Don’t Need an Expert! Making URL Phishing Features Human Comprehensible. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21). Association for Computing Machinery, New York, NY, USA, Article 695, 1–17. https://doi.org/10.1145/3411764.3445574

Design Validation

Online User Study

- 158 Prolific participants were asked to judge URL safety
- 3 groups with domain highlighting as control setting

https://resolutioncenter.ebay.com/policies/?id=123

- Participants were able to answer comprehension questions for 7.73/10 row descriptions on average

Condition	Accuracy	Per user correctness
Domain highlighting	65%	3.88/6
Report Summary	83%	4.96/6
Full report	92%	5.5/6

Kholoud Althobaiti, Nicole Meng, and Kami Vaniea. 2021. I Don't Need an Expert! Making URL Phishing Features Human Comprehensible. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21). Association for Computing Machinery, New York, NY, USA, Article 695, 1–17. https://doi.org/10.1145/3411764.3445574

What is this URL's Destination? Empirical Evaluation of Users' URL Reading

Sara Albakry
University of Edinburgh
Umm Al-Qura University
sara.albakry@ed.ac.uk

Kami Vaniea
University of Edinburgh
Edinburgh, UK
kvaniea@inf.ed.ac.uk

Maria K. Wolters
University of Edinburgh
Edinburgh, UK
maria.wolters@ed.ac.uk

ABSTRACT

Common anti-phishing advice tells users to mouse over links, look at the URL, and compare to the expected destination, implicitly assuming that they are able to read the URL. To test this assumption, we conducted a survey with 1929 participants recruited from the Amazon Mechanical Turk and Prolific Academic platforms. Participants were shown 23 URLs with various URL structures. For each URL, participants were asked via a multiple choice question where the URL would lead and how safe they feel clicking on it would be. Using latent class analysis, participants were stratified by self-reported technology use. Participants were strongly biased towards answering that the URL would lead to the website of the organization whose name appeared in the URL, regardless of its position in the URL structure. The group with the highest technology use was only minorly better at URL reading.

Author Keywords

Uniform Resource Locators; web literacy; URL readability; link destination; online security; technology usage; phishing

CCS Concepts

•Security and privacy → Usability in security and privacy; •Human-centered computing → Usability testing; Hypertext / hypermedia; Empirical studies in HCI; •Social and professional topics → Computing literacy;

INTRODUCTION

Malicious web links embedded in emails and other communications continue to plague companies resulting in compromises and lost revenue. FBI's Internet Crime Report estimates that phishing loses exceeded $29 million in 2017 for US organizations [40]. The Ponemon Institute estimates phishing costs UK organizations an average of $2.01 million per incident [35].

Automatic phishing detection, which is used by most organizations, is the most straight forward solution allowing organizations to detect and remove obviously malicious communication before it reaches users. Browsers also automatically block and provide warnings when they are confident that a URL is phishing [13]. Unfortunately, automatic detection is not perfect, sometimes allowing through malicious links or blocking benign ones [41]. Automatic detection systems also have difficulty identifying targeted communications which are carefully crafted and sent to a single target, known as spear phishing. In 2017, Google and Facebook were both tricked into paying $100 million to a scammer who was impersonating a manufacturer with whom the two companies interact [18].

To handle the fact that some malicious communications get through filters, security experts turn to users as the last line of defense, providing them with training and expecting them to identify phishing attacks, which they are not necessarily good at [14, 15]. Properly training people to detect phishing is also possibly more expensive than it is worth [21]. Knowing what advice to even train users with is also tricky. When security experts were asked to provide advice to internet users, "Don't click on dangerous links" and "Check the URL for an expected site" were common pieces of advice [37]. Both pieces of advice are based on the assumption that if the user pays close attention to the link text, they will be able to determine that it goes to a different website than what the accompanying message claims. The complexity of both the URL and human language processing systems along with the fact that phishers use URLs that contain brand names in different parts of the URL string [34], suggests that users may have trouble with this type of prediction. Hence, a systematic empirical evaluation is critical to form a clear understanding of users' URL reading abilities and to adapt our user-facing approaches accordingly.

In this work, we hypothesize that the majority of web users cannot differentiate between the following two Uniform Resource Locators (URLs): `https://facebook.profile.com` and `https://profile.facebook.com`. We take a slight twist on traditional anti-phishing research. Instead of measuring peoples' ability to identify phishing links, we focus on their ability to predict where a URL is likely to lead. To do so, we designed an online survey where participants were shown 23 URLs with a range of structures. For each URL, the participant was asked via a multiple choice question where the URL will lead and how safe they felt it was to click on, if it was sent from someone they know.

Research Questions

We focus on two high level research questions: ability to read a URL and assessment of the safety of a URL.

CHI '20, April 25–30, 2020, Honolulu, HI, USA.

ISBN 978-1-4503-6708-0/20/04…15.00

DOI: http://dx.doi.org/10.1145/3313831.3376168

I Don't Need an Expert! Making URL Phishing Features Human Comprehensible

Kholoud Althobaiti
University of Edinburgh
Taif University
Edinburgh, UK -Taif, KSA
khlod.k@tu.edu.sa

Nicole Meng
University of Edinburgh
Edinburgh, UK
nicole.meng@ed.ac.uk

Kami Vaniea
University of Edinburgh
Edinburgh, UK
kvaniea@inf.ed.ac.uk

ABSTRACT

Judging the safety of a URL is something that even security experts struggle to do accurately without additional information. In this work, we aim to make experts' tools accessible to non-experts and assist general users in judging the safety of URLs by providing them with a usable report based on the information professionals use. We designed the report by iterating with 8 focus groups made up of end users, HCI experts, and security experts to ensure that the report was usable as well as accurately interpreted the information. We also conducted an online evaluation with 153 participants to compare different report-length options. We find that the longer comprehensive report allows users to accurately judge URL safety (93% accurate) and that summaries still provide benefit (83% accurate) compared to domain highlighting (65% accurate).

CCS CONCEPTS

• **Security and privacy → Phishing.**

KEYWORDS

Phishing; URL reading; phishing awareness; usable privacy and security; real-time learning; security education, decision support

ACM Reference Format:
Kholoud Althobaiti, Nicole Meng, and Kami Vaniea. 2021. I Don't Need an Expert! Making URL Phishing Features Human Comprehensible. In *CHI Conference on Human Factors in Computing Systems (CHI '21), May 8–13, 2021, Yokohama, Japan.* ACM, New York, NY, USA, 17 pages. https://doi.org/10.1145/3411764.3445574

1 INTRODUCTION

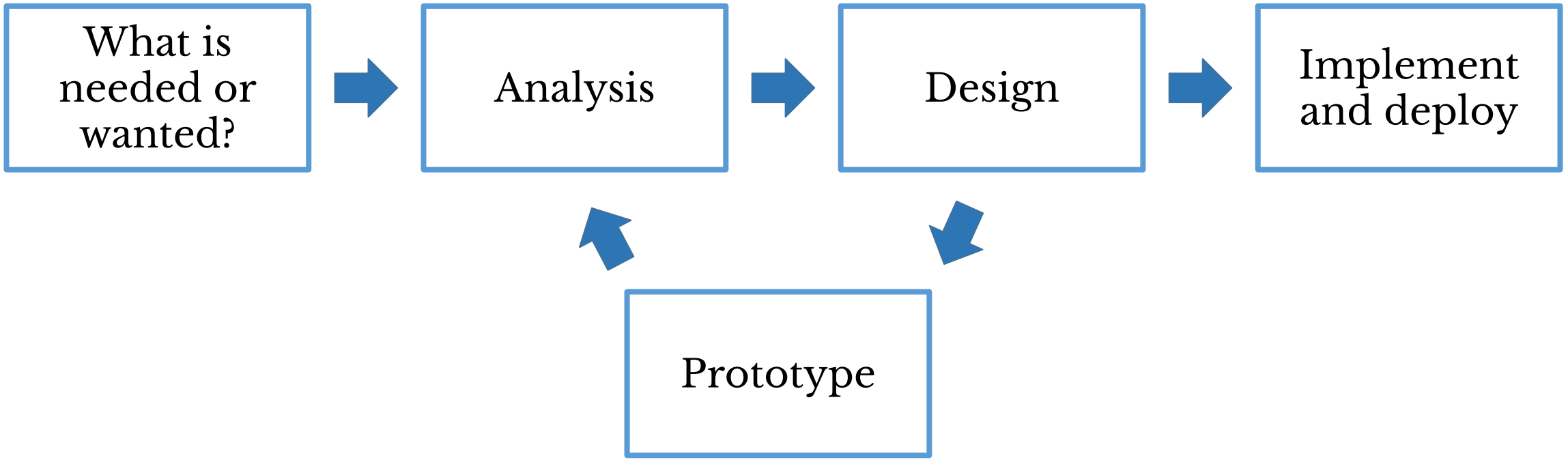
Determining if a link (URL) in a communication is malicious phishing designed to trick users or not is something that even security experts struggle to do without the aid of tools and additional information. While looking at the URL text is a good first step, fully reading a URL and determining its actual destination is surprisingly complex and often requires the help of third-party services that provide information like how long ago the domain was registered or if the URL redirects anywhere. Yet, despite these complexities, URLs remain one of the stronger indicators of malicious communication [52, 62], particularly if a communication claims to come from an organization but the URLs lead to other destinations. For example, an email claiming to be from PayPal but containing links to `PayPal-com-security-website.org` is quite likely a malicious email. While the example is simple, it brings up several key issues with detecting malicious links. First off, it requires that the person making the judgment knows PayPal's correct URL and is also able to compare it to the one in the email. The "correct" URL for a website is not necessarily obvious; for example, which of the following is the correct website for the New York Times newspaper: `nyt.com` or `newyorktimes.com`? The answer is that both URLs redirect to the real URL `www.newyorktimes.com`. Comparing URLs is also not necessarily easy. End users often confuse elements of a URL, such as the domain and subdomain [2] making comparing URLs error-prone. Experts handle these complexities using a range of tools and information sources that help them make decisions, but end users are often only provided with training on lexical reading [43, 74, 82] and possibly a tool checks if the URL has been confirmed as malicious. In this work, we aim to change this situation by making the types of approaches used by experts more accessible to end users.

Obviously users are not the best first option to detect phishing. Automated phishing filters are far less expensive and also relatively accurate [40]. They can quickly compare a URL to lists of known phishing or break the URL into features used to classify it as phishing or not. Most organizations already use automated approaches to protect users on their networks with great success. However, this usage means that any phishing communications a user sees has likely already been through an automated filter and therefore has already been scanned against common computer-friendly features. Assisting users in making these judgments on their own is necessary because automated approaches are not yet 100% accurate [61] and experts are also typically not available to consult on every potential phishing communication in a timely manner. Phishing communication also often uses tactics to pressure the user into responding quickly such as threatening to shut down their account, charge them money, upset their boss, or lose out on a limited time offer [55, 86]. These time pressures make it emotionally hard for users to report the email and then wait for an official response, leading them to use their own or their peers' judgment [56]. The effects are readily apparent in public phishing reports. Phishing is regularly listed as one of the top causes of data breaches (93%) [80] and the most frequent Internet crimes complaint to the FBI [21]. Financial losses from phishing can also be expensive, exceeding $29 million in 2017 [32] and $1.7 billion in 2019 [21]. Tools supporting users in accurately making such decisions on their own are

CHI '21, May 8–13, 2021, Yokohama, Japan

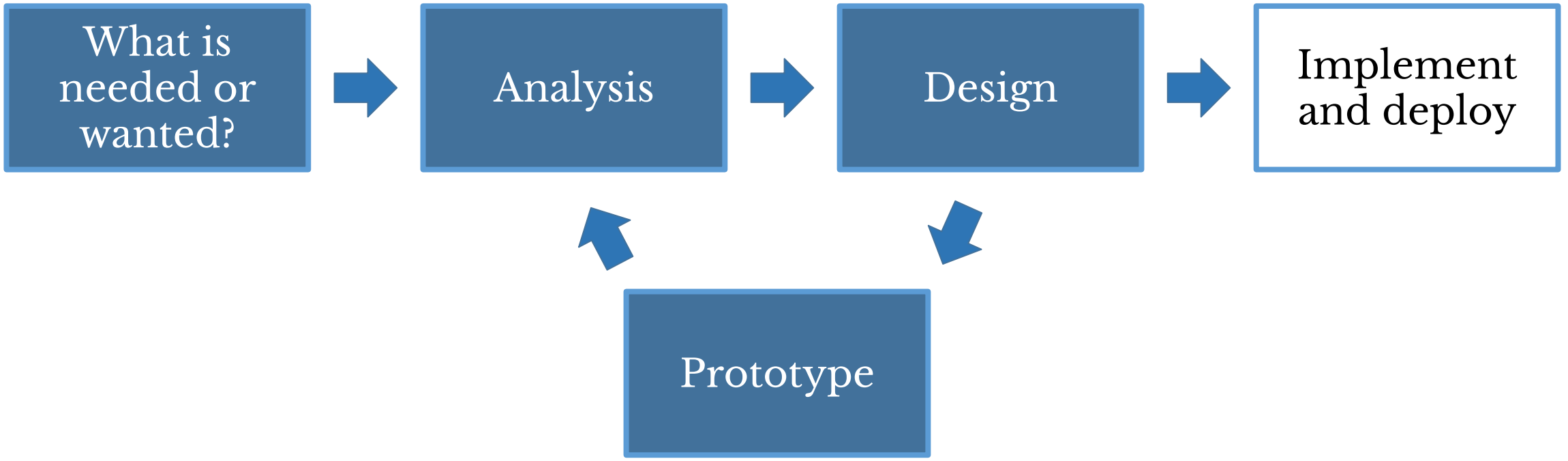
ACM ISBN 978-1-4503-8096-6/21/05…$15.00
https://doi.org/10.1145/3411764.3445574

Design Process



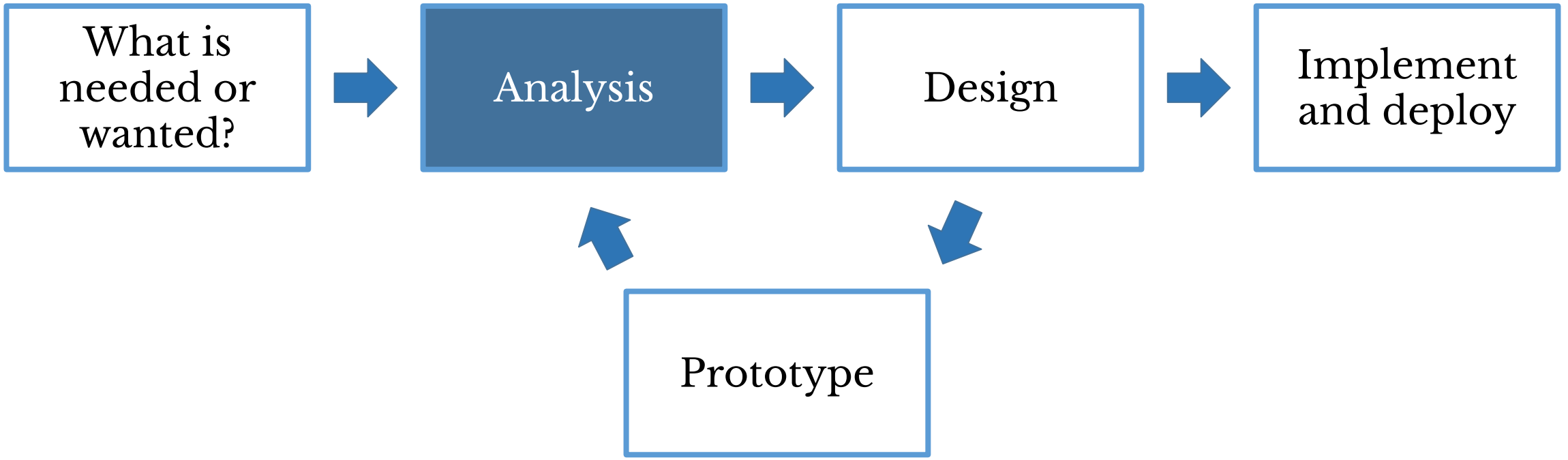
Design Process

Coursework 1: Initial Mockup of Learn (OpenCourse)



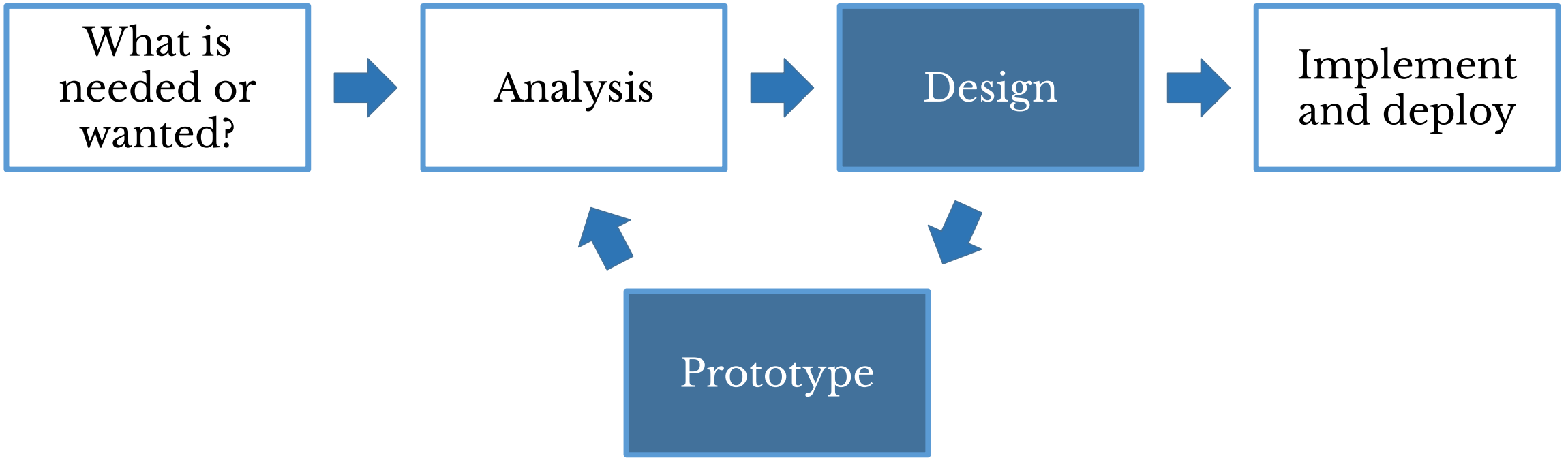
Design Process

Coursework 2: Evaluate other designs and give design recommendations



Design Process

Coursework 3: Refine and justify design



Group Sign Up

- You will pretend to be the design team working with a client who wants to redesign learn and opencourse.
- You will be working in groups of 3 or 4 and produce three short reports and develop mock-ups on figma.
- We do not expect fully functioning prototypes, but focused redesigns of problematic screens.

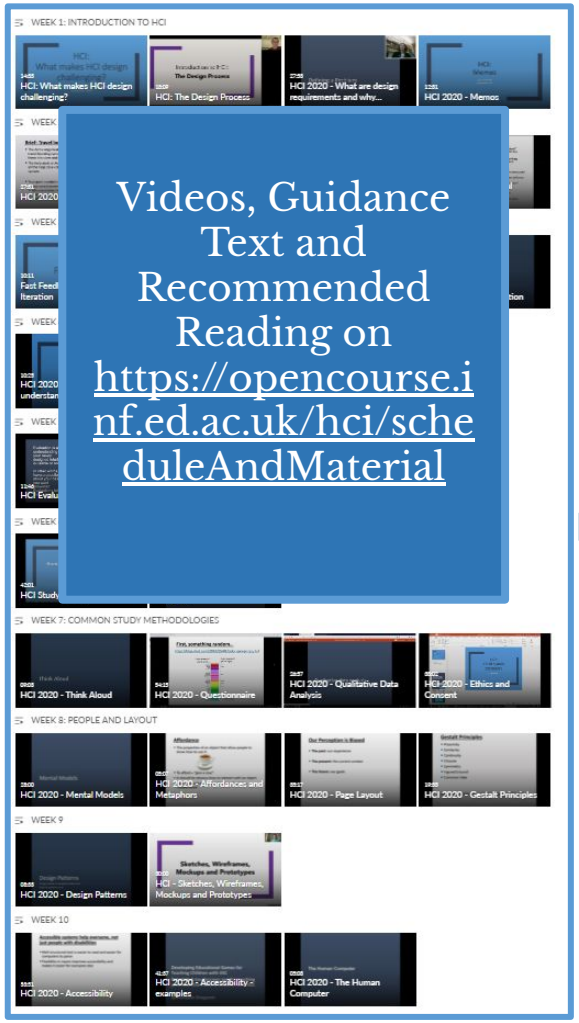
Group Sign Up instructions under assessment on opencourse:

SIGN UP BEFORE WEDNESDAY NEXT WEEK.

What else are we going to cover in this class?

- Accessibility
- Defining a problem and requirements
- Develop a prototype and how to iterate on it
- Design Evaluation
- User studies and how to design and conduct them
- Qualitative data analysis
- Ethics
- Interface design
- Design research

Flipped Classrooms

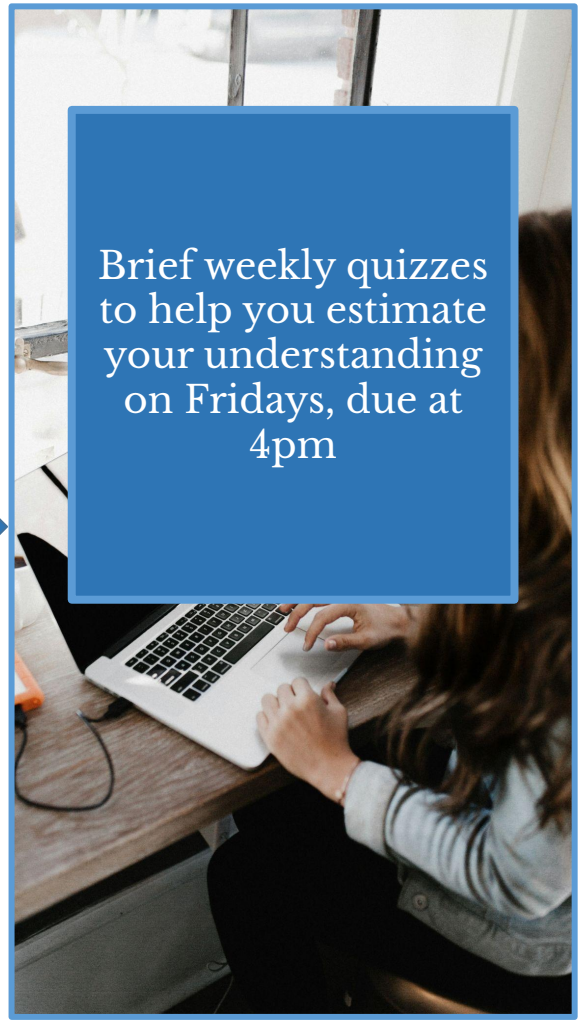


Videos, Guidance Text and Recommended Reading on https://opencourse.inf.ed.ac.uk/hci/scheduleAndMaterial

Screenshot of last year's HCI playlists on media.ed.ac.uk

Live Sessions with Recap, Q&A and Hands-On Activities on Tuesdays and Fridays

Photo by Dylan Gillis on Unsplash



Brief weekly quizzes to help you estimate your understanding on Fridays, due at 4pm

Photo by Andrew Neel on Unsplash

x 10

for 10 weeks in the semester

Any questions for now?

HCI is Important

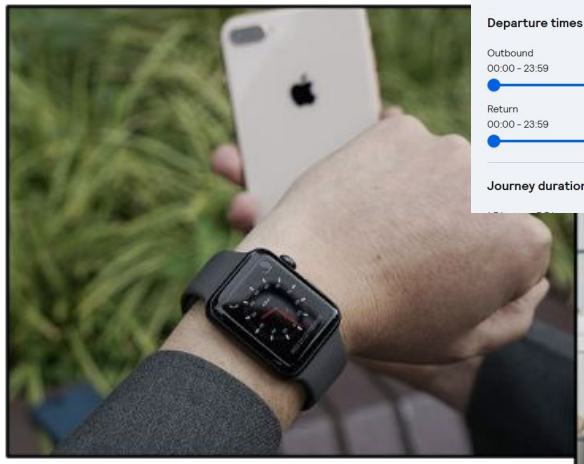
Raise your hand if you've ever had a similar experience with technology

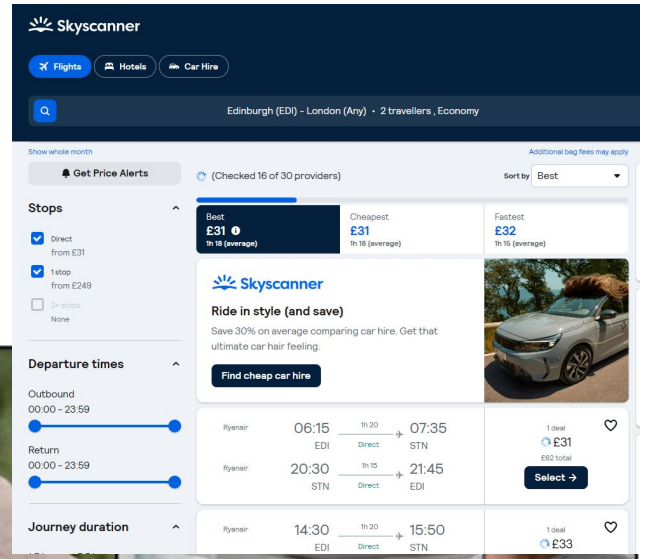
https://www.youtube.com/watch?v=HtTUsOKjWyQ

Experience with Technology

Work in pairs - 2 minutes each

Consider any interactive technology you use





Is it easy to use?

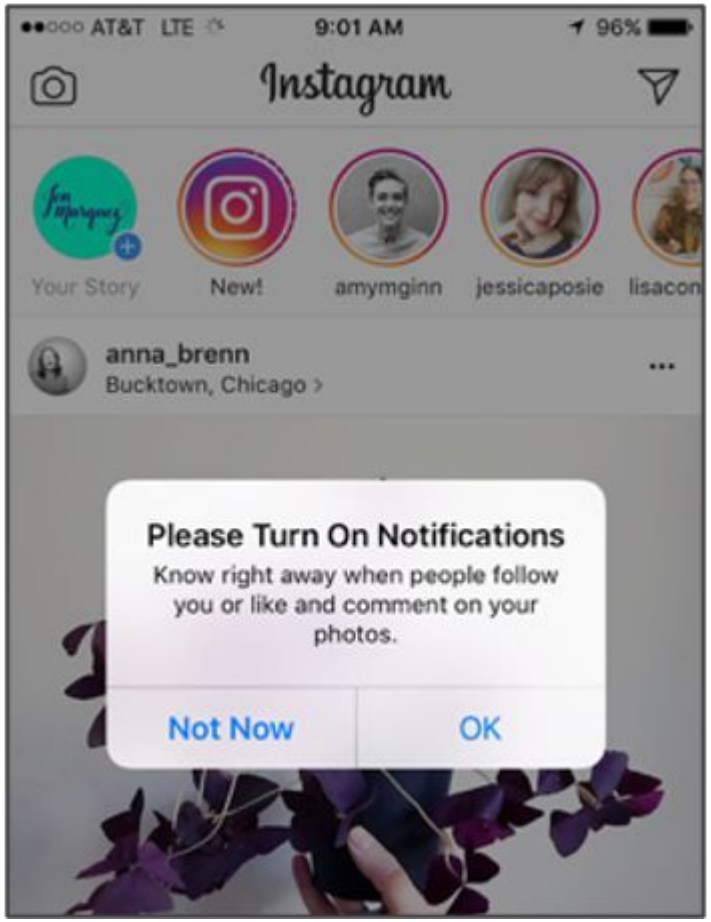
Is it useful?

Is is enjoyable, satisfying or frustrating to use?

Why?

Why is HCI Important?

- Understand users and their needs
- Create a smooth user experience, reduce frustration, and increase usefulness
- Being aware of the dark side of user experience design



https://darkpatterns.uxp2.com/pattern/instagram-no-option-for-no/
https://www.deceptive.design/

Who is HCI important for?

- Anyone who interacts with technology
- People with accessibility needs

Homework

- Until Friday, note down any technology or interfaces you experience difficulties with. Take a screenshot or jot down some notes to discuss during out in-class activity on Friday.

Week 1: Welcome to Human-Computer Interaction

Nicole Meng-Schneider and Dr Tara Capel

Part of slidedeck inspired by Dr Kami Vaniea