"*They brought in the horrible key ring thing!*" Analysing the Usability of Two-Factor Authentication in UK Online Banking

Kat Krol, Eleni Philippou, Emiliano De Cristofaro, M. Angela Sasse

University College London, UK

Background

- 2FA increasingly popular, news of password breaches drive companies to adopt 2FA
- 42% of EU and 51% of US customers use online banking (2013)
- Little research has focused on the adoption and actual use of 2FA

2F landscape in the UK

- Hardware tokens:
  - Card Reader
  - SecureKey
- SMS
- Mobile phone app
- Phone call

Study objectives

- Explore the perceptions and opinions of existing users
- Attempt to compare the different 2F technologies
- See what can be improved

Participants

- 66 people filled in a pre-screen, 21 were chosen
- 11f / 10m, age range: 19-69 (mean: 32.4, SD=10.87)

- 2F technologies used:
  - Card Reader: 16
  - SecureKey: 9
  - OTP via SMS: 5
  - OTP over the phone: 4
  - OTP via smartphone app: 3

Study stages

1. Preliminary interviews (~30mins/£5)

2. Diary (10-12 days)

3. Final interviews (~30mins/£15)

Interview results: Hardware tokens

Advantages

- Easy to use (4)
- Portable (4)
- Easy to incorporate into everyday life (4)

Disadvantages

- Needs to remember to bring it (7)
- Inconvenient (5)
- Frustrating to use (4)
- Irritating (3)

"It's OK when I am at home, but when you are at work and you are pretending you are actually doing work when you are actually checking on your account, then you have to bring out this calculator thing and it's kind of obvious you are not doing work. I'd rather have something where I am just on the screen and it's lot quicker." (P11)

Authentication terminology

"*Is it a passphrase or passcode or key phrase what they need? [chuckling] I think it is slightly confusing. Although I'm experienced [...], it's frustrating*." (P08)

Interruption to the primary task

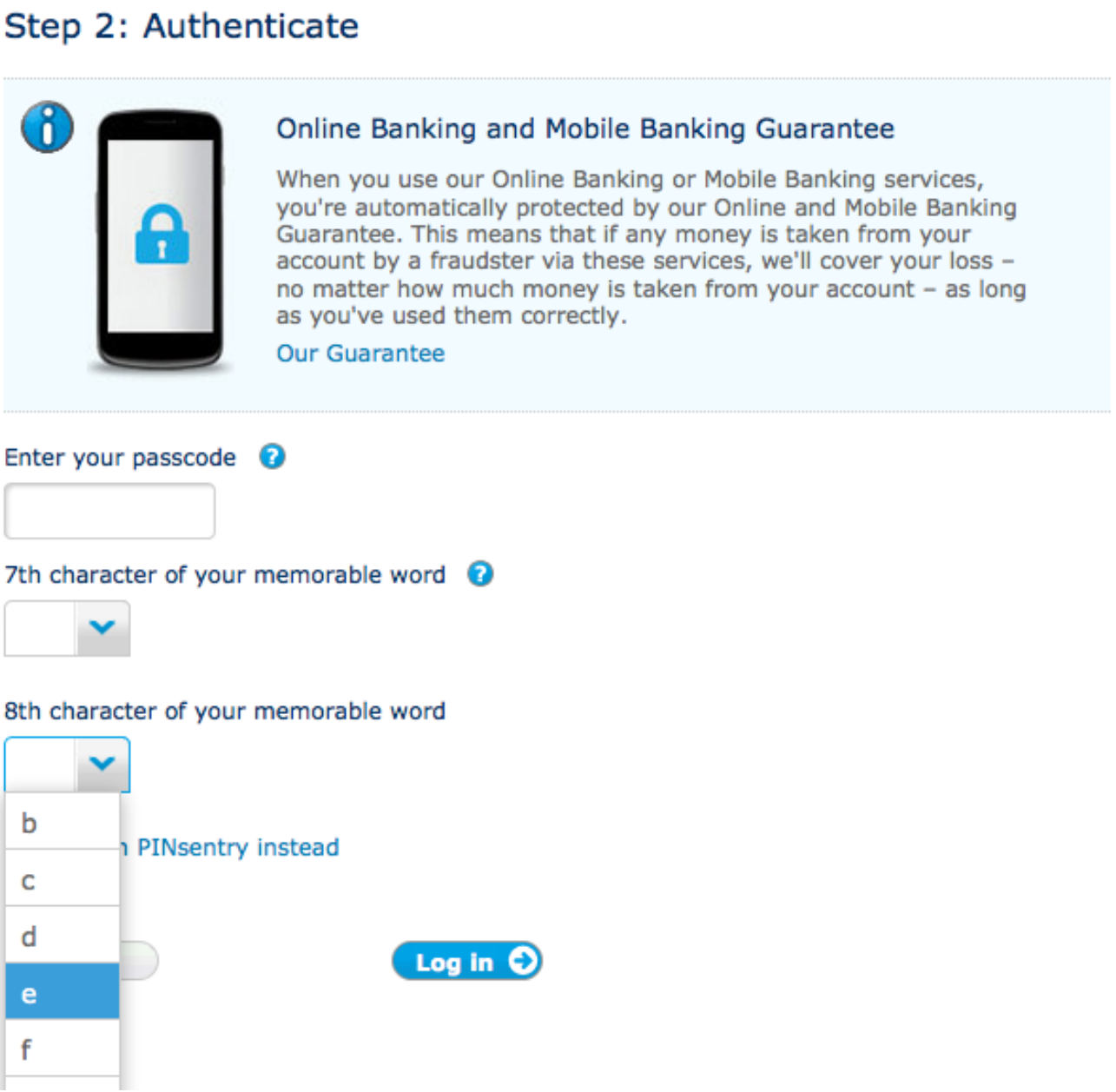
"*If I am in a rush, I maybe misspell my surname or I do not enter the card number correctly […] I'll have to get myself together mentally and let's say "Focus! Whatever is in your mind, forget it.*" (P14)

Other problems

- Assigned usernames prevented participants from logging in

- Cumbersome resets led to simpler credentials

Use of drop-down menus



Mental models

- Credentials are checked manually by bank employees
- Where do OTPs come from?
- Card reader needs protection, information can be stolen off it

Security rituals reassure users (e.g., anti-virus, hiding the token, using password as memorable answer)

Ideal authentication

- Biometrics!

“I think, in a few 100 years from now you’ll just put your finger on a machine and it reads your fingerprint. Today, it’s slow – you know fast is good! The faster the better.”

Implicit authentication

- Reliability concerns (5)
- Privacy concerns (6)

"*I could see implicit working but you'll probably run to privacy issues about that: Who's doing the software? How's the monitoring done? Who gets the information from the monitoring? blah blah blah. That would be the real issue.*" (P10)

Diary results

- 17 participants kept an authentication diary for approx. 11 days
- 90 entries, 5.29 per person (1-15, SD=3.99)
- There were problems on 12 occasions (13.3%)
  - Mistyped credentials (5)
  - Misplaced tokens (2)
  - Wrong memorable answer, wrong sequence of steps, forgotten username etc.

Participant satisfaction

- Lower when they generated an OTP to authenticate
- Lower the more pieces of information they had to enter
- Lower with banks that required a token to generate an OTP

Recommendations

- Give customers choice of authentication options
- Unify wording for credential names
- Check your security features actually work
  - Use of drop-down menus
  - Providing selected characters out of order

Summary

- An in-depth qualitative and quantitative study with 21 users of 2FA in UK online banking
  - Mandatory 2FA
  - Post-adoption: Views from existing users
- Users disliked tokens, they found them limiting
- Recommendations

Thank you!

k.krol@cs.ucl.ac.uk