Student ID: 2136685

HBCS CW2

Security and usability trade-offs

Santander Online Banking System

Table of Contents

Table of Figures

Overview

The Santander Online Banking System is an example of a system that is comprised of many implementations that prioritise usability over security, or vice versa. As Kainda references in their paper, Santander is an example of a system that has yet to implement usability features with security in mind, but instead chooses to focus on one over the other. (Kainda, Flechais and Roscoe, 2010)

Usage scenarios

Logging into online banking

When a user attempts to log onto the Online Banking system, a customer is greeted with a request for their "personal ID" and "security number", as seen in Figure 1. The trade-off between security and usability is shown in Figure 2, by requiring additional steps to log on to the system. After authorising the log on, the mobile app announced that I must authorise it again, afterwards it used biometrics to verify my identity, making the log on process a four-step endeavour, for the sake of security. If there is no mobile banking app to verify the log on, Santander would send a One-Time Password (OTP) via SMS to verify it, which is a much simpler, but more unsafe approach.

Changing the personal ID

A user might want to change their personal ID to something more memorable. This is easily done, by simply knowing the current personal ID and typing in the new one, as seen in Figure 3. No other checks are required, such as an OTP. This is very simple and easy to use, however the change is not notified to the customer anywhere, therefore it sacrifices security for usability.

Changing the security number

When changing credentials, for example the security number used to log in, all one needs is the old security number, the new one and the password set to the account, as seen in Figure 4. Therefore, Santander use 3 types of credentials needed for a customer to access their account and moreover, a customer must remember them. After the new security number is settled, an OTP is sent to the mobile number associated with the account, to verify the change. For a banking system, a customer would feel satisfied and safe with the amount of security in place, and they would think that having to remember the credentials is a good compromise of usability for security, as they would want their money secure.

Threat scenarios

One-Time Passwords

The mobile banking app is used to authorise all actions a customer will do with their account, be it logging in or approving a transaction. If a customer doesn't have the mobile banking application, a One-Time Password (OTP) will be sent to the mobile number associated with the customer's account. However, a threat actor could impersonate the customer and call their mobile carrier to request a new SIM card, therefore giving them full access to the customer's account.

Logging in on public Wi-Fi

Some customers may want to check their online banking while they are on the move. Logging into the online banking system may be dangerous when on public Wi-Fi as a threat actor can take the credentials with a "Man-In-The-Middle" (MITM) attack. However, this type of attack is unlikely to work nowadays as the connection to Santander's online banking system is uses HTTPS, which is an encrypted connection so a threat actor cannot see what is sent or received. A customer can verify if they are using HTTPS by checking the lock icon next to the URL, as seen in Figure 5.

Phishing

A customer may receive an email by a threat actor impersonating Santander, asking them to urgently sign into their account using the link they have sent as all their money has been taken away. The customer, genuinely worried, would quickly sign into the false online banking website therefore giving access to their online banking account to the threat actor. Santander doesn't currently send any mock phishing emails; therefore, a customer would have a difficult time recognising a phishing email from a real email, especially in a panic. Phishing attacks are very common nowadays and users of all ages fall for these. Usability will be affected by phishing as the customer's bank account can become locked or it can suddenly have no funds, which will frustrate the user greatly as they thought they were doing the right thing.

Recommendations

For one-time passwords, my recommendation would be to not use them via SMS. Instead, use a mobile authenticator such as the Google Authenticator for time-based one-time passwords (TOTP). Security would be increased as TOTPs are at the user's discretion and they can be used without needing an SMS, therefore eliminating the risk of someone stealing a customer's SIM card. TOTPs via a mobile authenticator work well as threat actors cannot access these codes as they would be able to via SMS. Moreover, if a threat actor does gain access to a TOTP code, they only have a small time frame in which they are valid. The usability remains the same, as the customer would still need to get the code by going through their smartphone. (Umawing, 2019)

For logging in on public Wi-Fi, most websites use HTTPS as their protocol nowadays, including Santander. Man-in-the-middle (MITM) attacks still can happen, and their encrypted data could get decoded by a savvy threat actor. Therefore, as a recommendation, users should not use public Wi-Fi and rather they should try to wait until they are on a network they trust. Mobile networks are not secure either, as there are cellular phone surveillance devices that can mimic a wireless carrier cell tower and carry out MITM attacks. Those devices are called "Stingray phone trackers". (Aviram, 2016; Moody, 2016)

For phishing, Santander should make clear to their customers that they would never ask for their login credentials. A simple SMS message or an email could be very effective, and it can increase security at no cost for usability. On the other hand, Santander should send mock phishing emails so that their customers can get accustomed to the hints of a phishing email, such as bad grammar.

References

Aviram, A. (2016). *Revealed: Bristol's police and mass mobile phone surveillance*. [online] The Bristol Cable. Available at: https://thebristolcable.org/2016/10/imsi/ [Accessed 3 Feb. 2023].

Kainda, R., Flechais, I. and Roscoe, A.W. (2010). Security and Usability: Analysis and Evaluation. *2010 International Conference on Availability, Reliability and Security*. doi:10.1109/ares.2010.77.

Moody, G. (2016). *Stingrays bought, quietly used by police forces across England*. [online] Ars Technica. Available at: https://arstechnica.com/tech-policy/2016/10/stingrays-in-use-across-england-by-police/ [Accessed 3 Feb. 2023].

Umawing, J. (2019). *Has two-factor authentication been defeated? A spotlight on 2FA's latest challenge | Malwarebytes Labs*. [online] Malwarebytes. Available at: https://www.malwarebytes.com/blog/news/2019/01/two-factor-authentication-defeated-spotlight-2fas-latest-challenge [Accessed 3 Feb. 2023].

Appendix

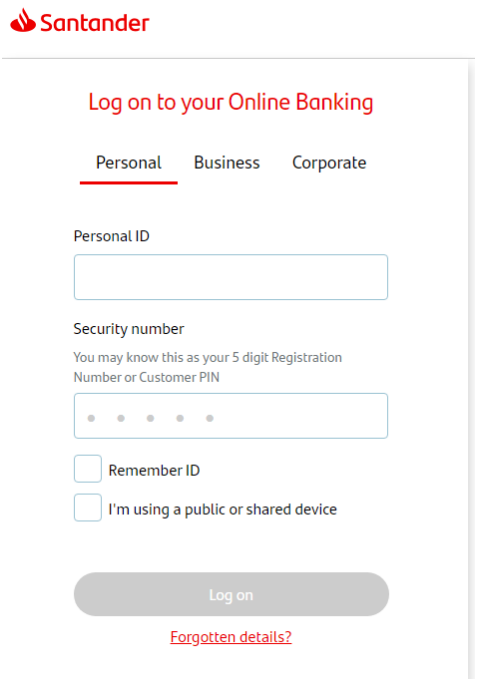

Figure 1 - Logging on to Online Banking

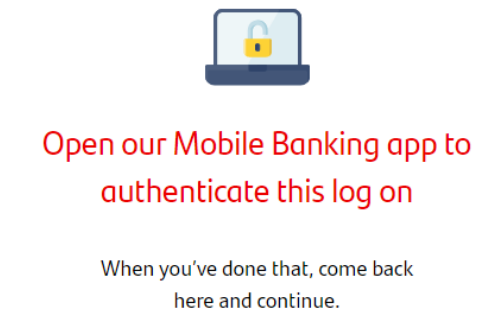

Figure 2 - Additional action needed when logging in

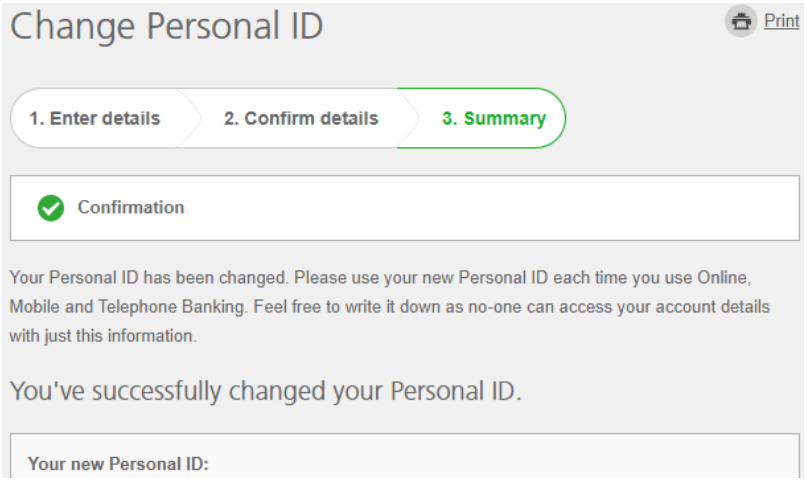

Figure 3 - Changing the personal ID

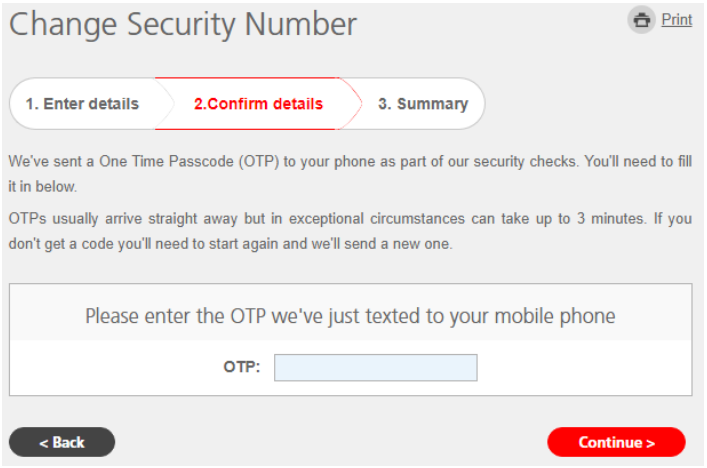

Figure 4 – Changing the security number

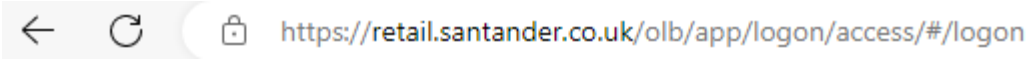

Figure 5 - HTTPS lock