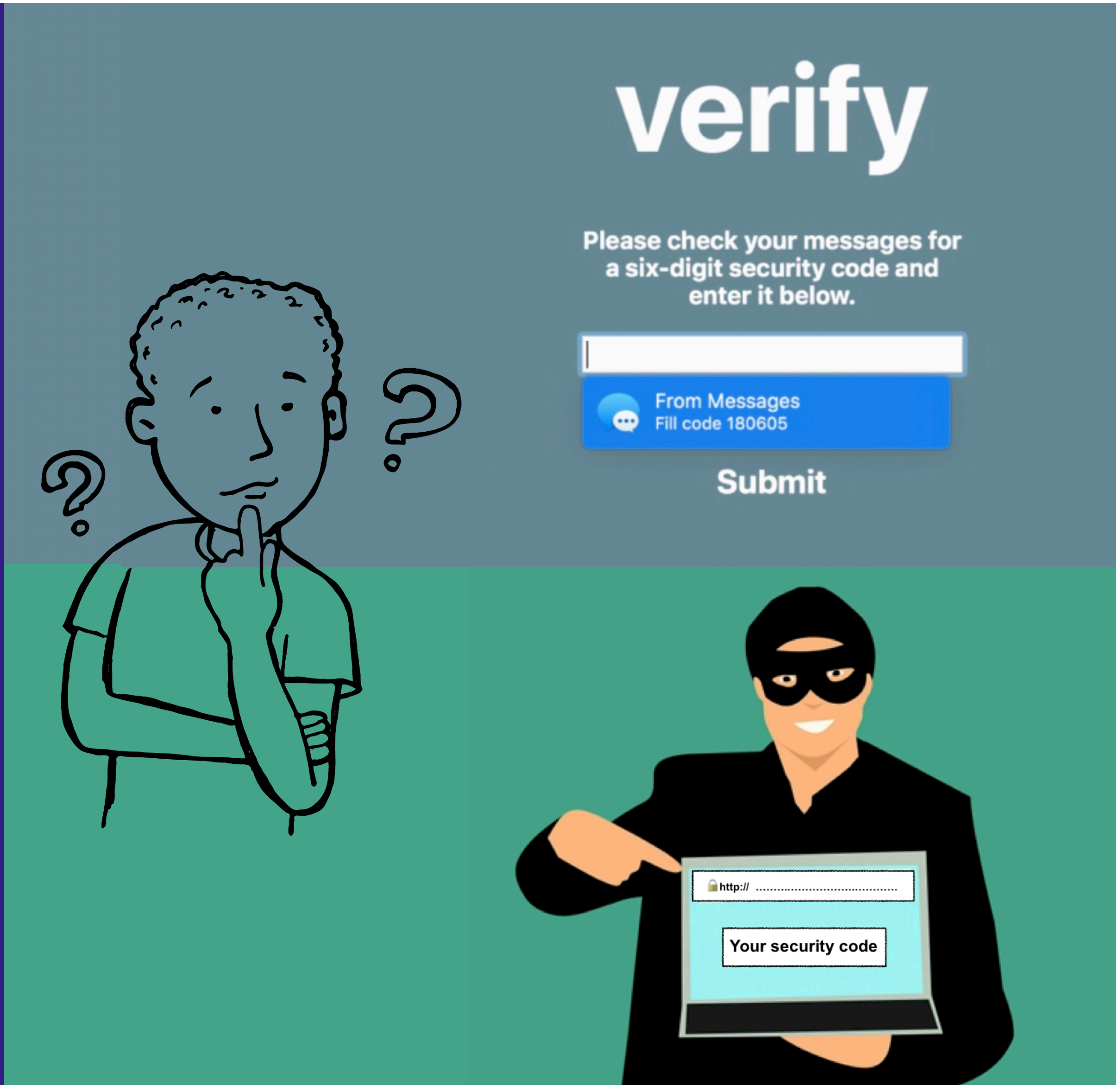
OneSpan
Cambridge Innovation Centre

UCL

Privacy & Us

Taken Out of Context:

Security Risks with Security Code AutoFill in iOS & macOS



verify

Please check your messages for a six-digit security code and enter it below.

From Messages
Fill code 180605

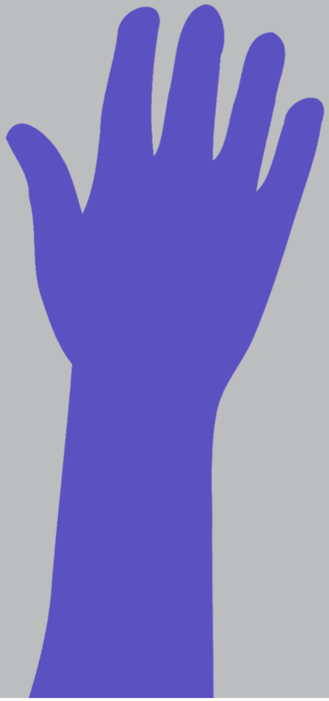
Andreas Gutmann, Steven J. Mudoch, WAY19 | @kryptoandi

PLEASE RAISE YOUR HAND

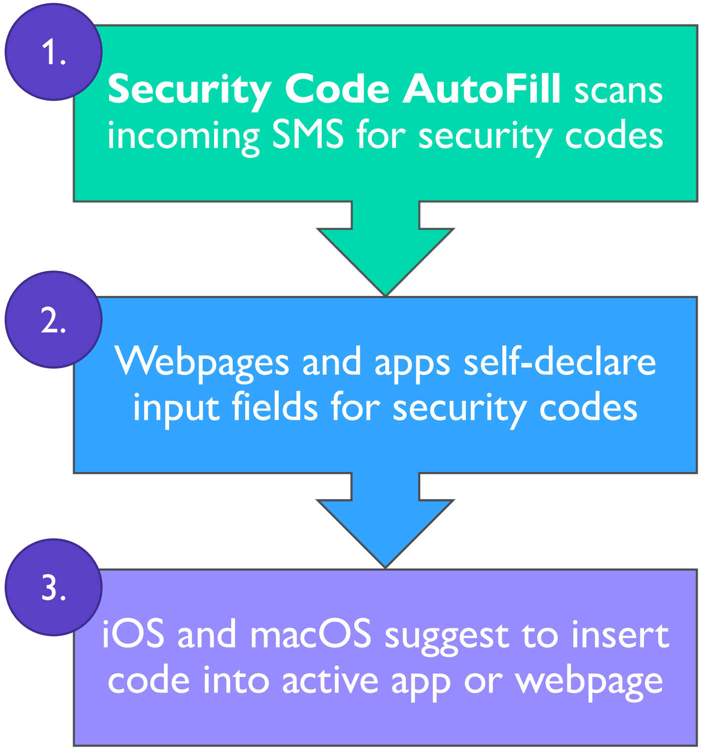
Have you ever…

- received a **security code via SMS**?
- needed to
  1. **memorise** or **manually copy** the code,
  2. **switch** apps, and
  3. **quote it** on the other app?
- found it **cumbersome** to do all this?

Last year, Apple introduced a new convenience feature:
Security Code AutoFill



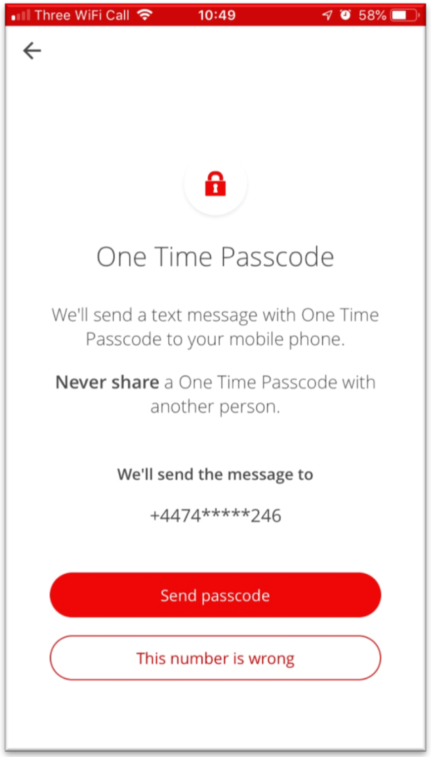
SECURITY CODE AUTOFILL



1. **Security Code AutoFill** scans incoming SMS for security codes

2. Webpages and apps self-declare input fields for security codes

3. iOS and macOS suggest to insert code into active app or webpage



Three WiFi Call 10:49 58%

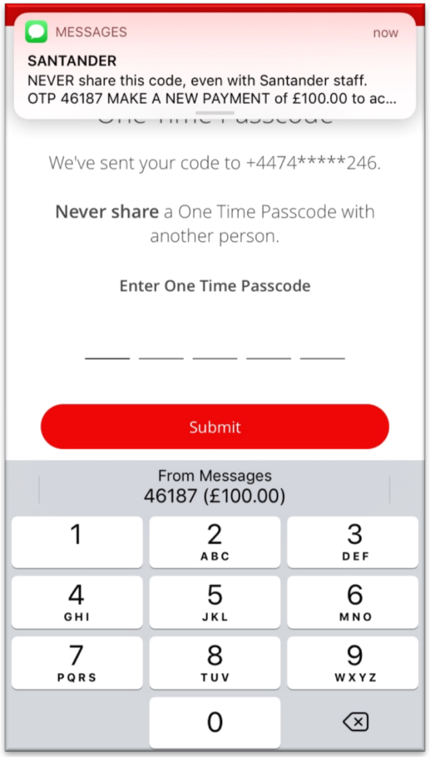
One Time Passcode

We'll send a text message with One Time Passcode to your mobile phone.

Never share a One Time Passcode with another person.

We'll send the message to

+4474*****246



MESSAGES now

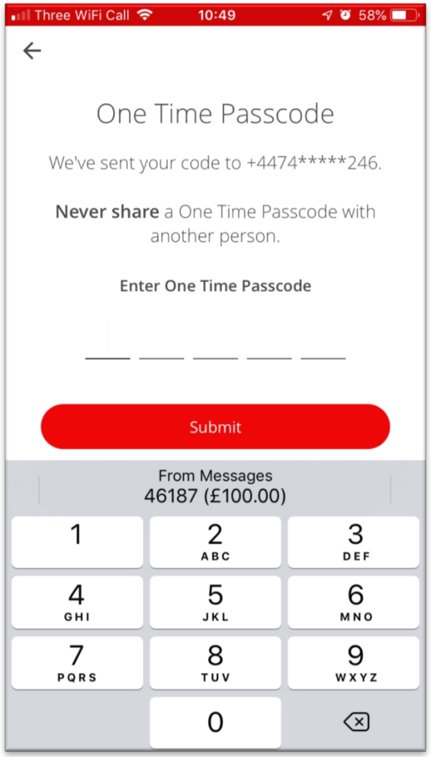
SANTANDER

NEVER share this code, even with Santander staff.
OTP 46187 MAKE A NEW PAYMENT of £100.00 to ac...

We've sent your code to +4474*****246.

Never share a One Time Passcode with another person.

Enter One Time Passcode



Three WiFi Call 10:49 58%

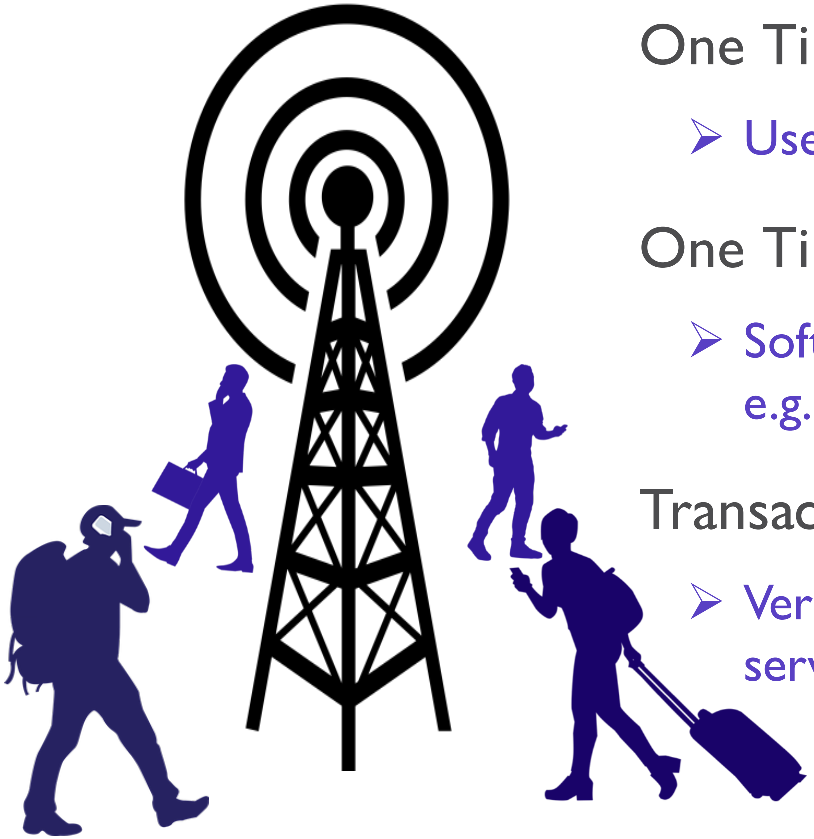
One Time Passcode

We've sent your code to +4474*****246.

Never share a One Time Passcode with another person.

Enter One Time Passcode

WORKS WITH ALL TYPES OF SECURITY CODES



One Time Password (OTP)

- ➢ User authentication, e.g. remote login

One Time Authorisation (OTA)

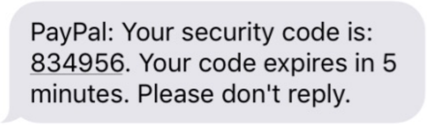
- ➢ Software activation or registration to a phone number, e.g. instant messenger

Transaction Authorisation Number (TAN)

- ➢ Verification of integrity of instructions received by the server, e.g. online payments

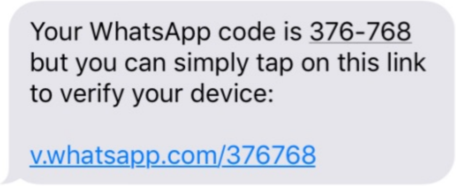
AUTOFILL USER INTERFACE

OTP



PayPal: Your security code is: 834956. Your code expires in 5 minutes. Please don't reply.

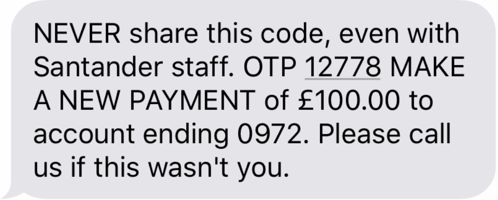
OTA



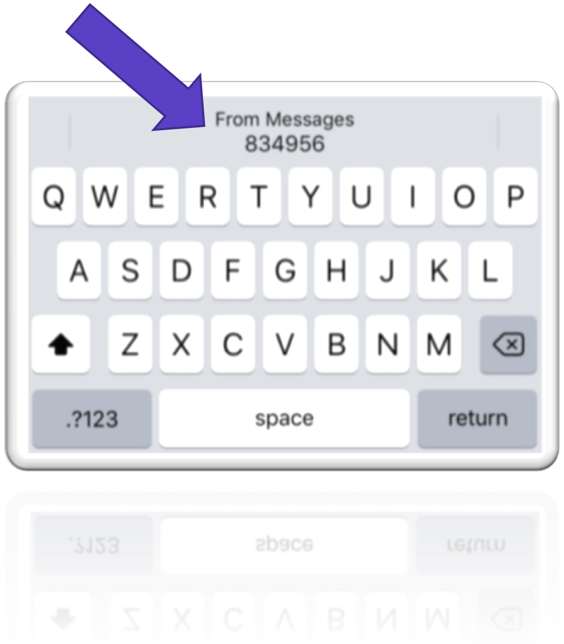
Your WhatsApp code is 376-768 but you can simply tap on this link to verify your device:

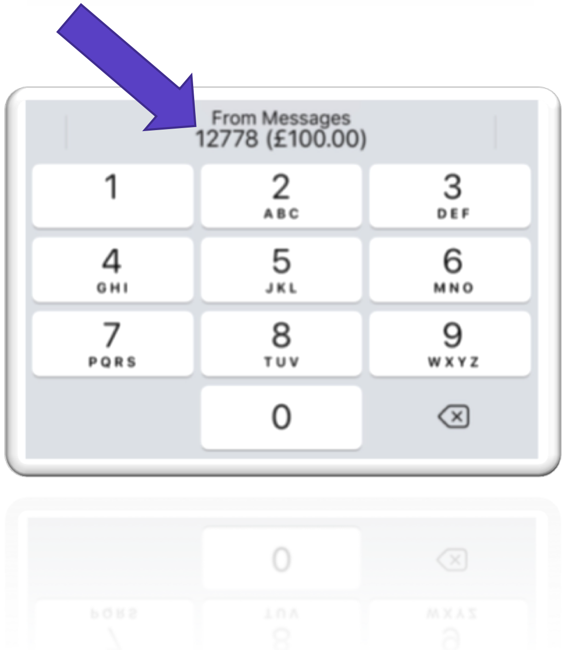
v.whatsapp.com/376768

TAN



NEVER share this code, even with Santander staff. OTP 12778 MAKE A NEW PAYMENT of £100.00 to account ending 0972. Please call us if this wasn't you.

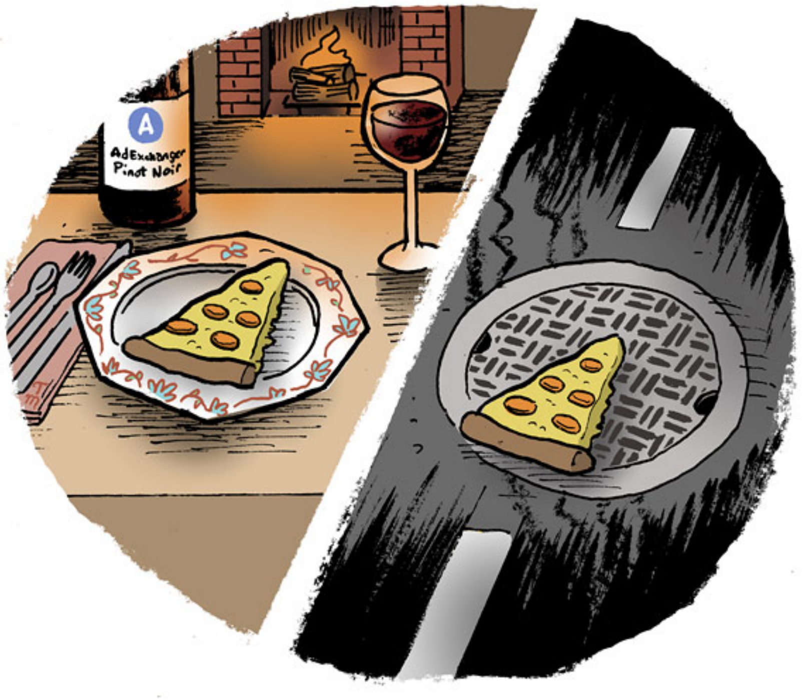




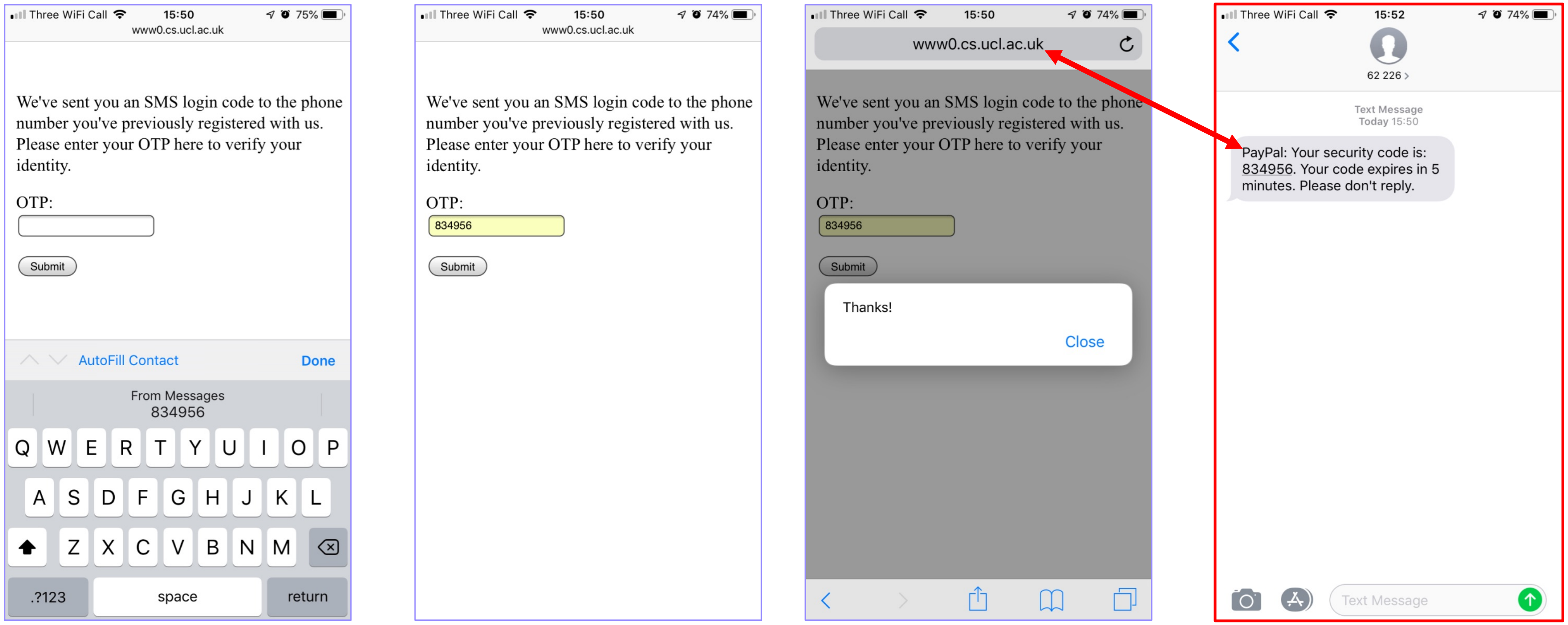
HOW THINGS GO WRONG...

THE SOURCE OF RISKS

Security Code AutoFill **de-contextualises security codes**, but relies on users to make **security-cautious decisions**.



EXAMPLE: REMOTE LOGIN



We've sent you an SMS login code to the phone number you've previously registered with us. Please enter your OTP here to verify your identity.

OTP:

Submit

We've sent you an SMS login code to the phone number you've previously registered with us. Please enter your OTP here to verify your identity.

OTP: 834956

Submit

We've sent you an SMS login code to the phone number you've previously registered with us. Please enter your OTP here to verify your identity.

OTP: 834956

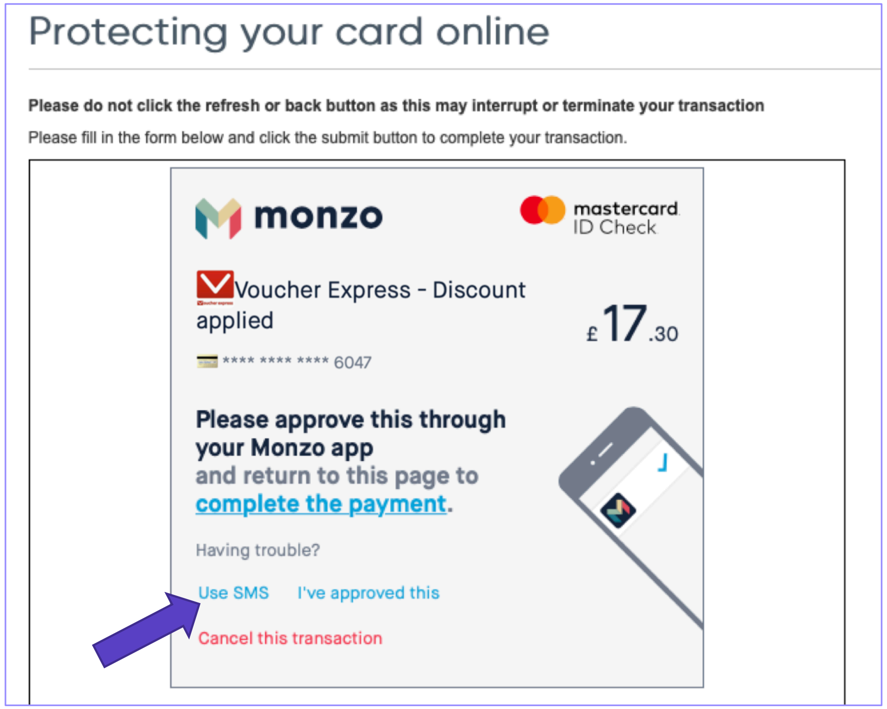
Submit

Thanks!

Close

PayPal: Your security code is: 834956. Your code expires in 5 minutes. Please don't reply.

EXAMPLE: ONLINE SHOPPING



Protecting your card online

Please do not click the refresh or back button as this may interrupt or terminate your transaction

Please fill in the form below and click the submit button to complete your transaction.

Voucher Express - Discount applied

£17.30

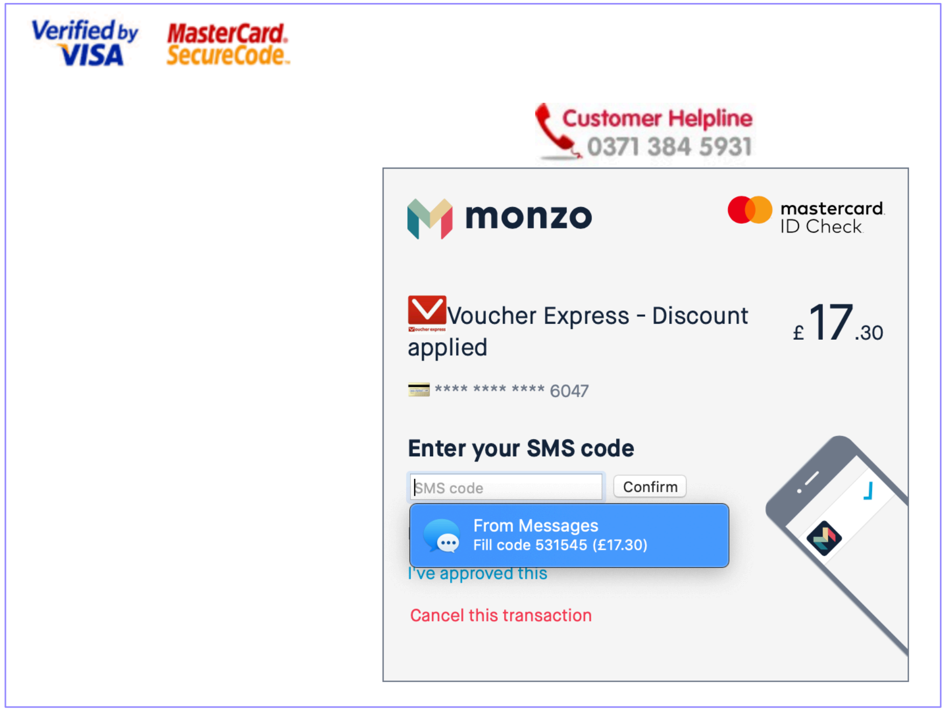
**** **** **** 6047

Please approve this through your Monzo app and return to this page to complete the payment.

Having trouble?

Use SMS I've approved this

Cancel this transaction



Voucher Express - Discount applied

£17.30

**** **** **** 6047

Enter your SMS code

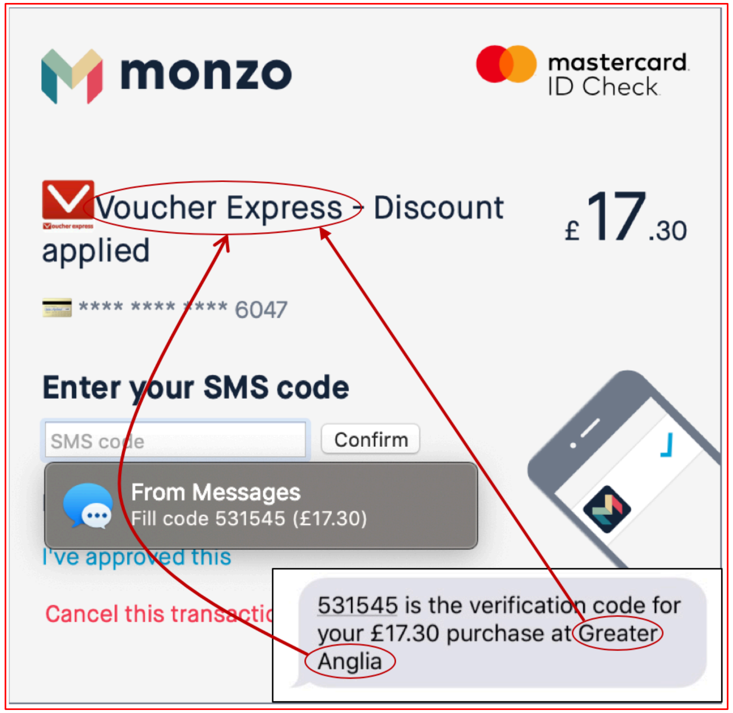
SMS code Confirm

From Messages
Fill code 531545 (£17.30)

I've approved this

Cancel this transaction

EXAMPLE: ONLINE SHOPPING



monzo

mastercard ID Check

Voucher Express - Discount applied

£17.30

**** **** **** 6047

Enter your SMS code

SMS code

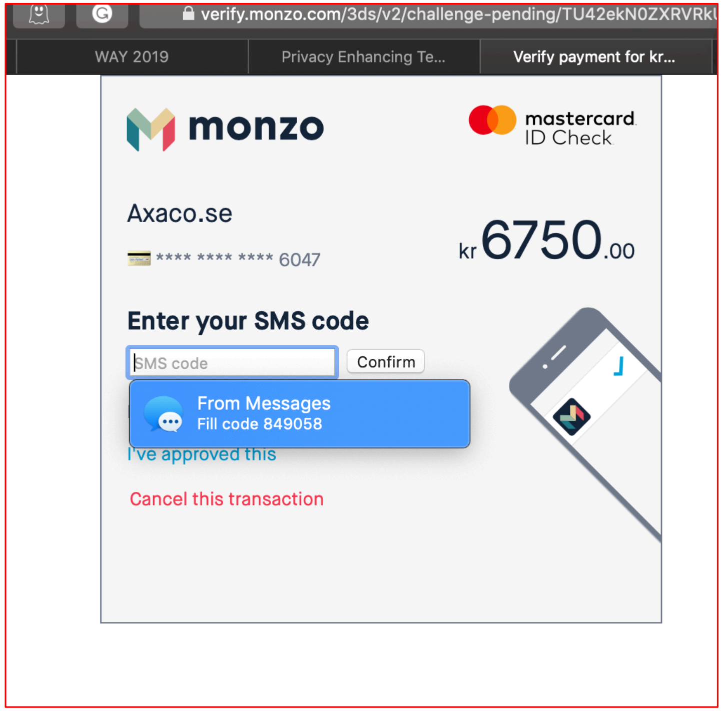
Confirm

From Messages
Fill code 531545 (£17.30)

I've approved this

Cancel this transaction

531545 is the verification code for your £17.30 purchase at Greater Anglia



verify.monzo.com/3ds/v2/challenge-pending/TU42ekN0ZXRVRkU

WAY 2019 | Privacy Enhancing Te... | Verify payment for kr...

monzo

mastercard ID Check

Axaco.se

kr6750.00

**** **** **** 6047

Enter your SMS code

SMS code

Confirm

From Messages
Fill code 849058

I've approved this

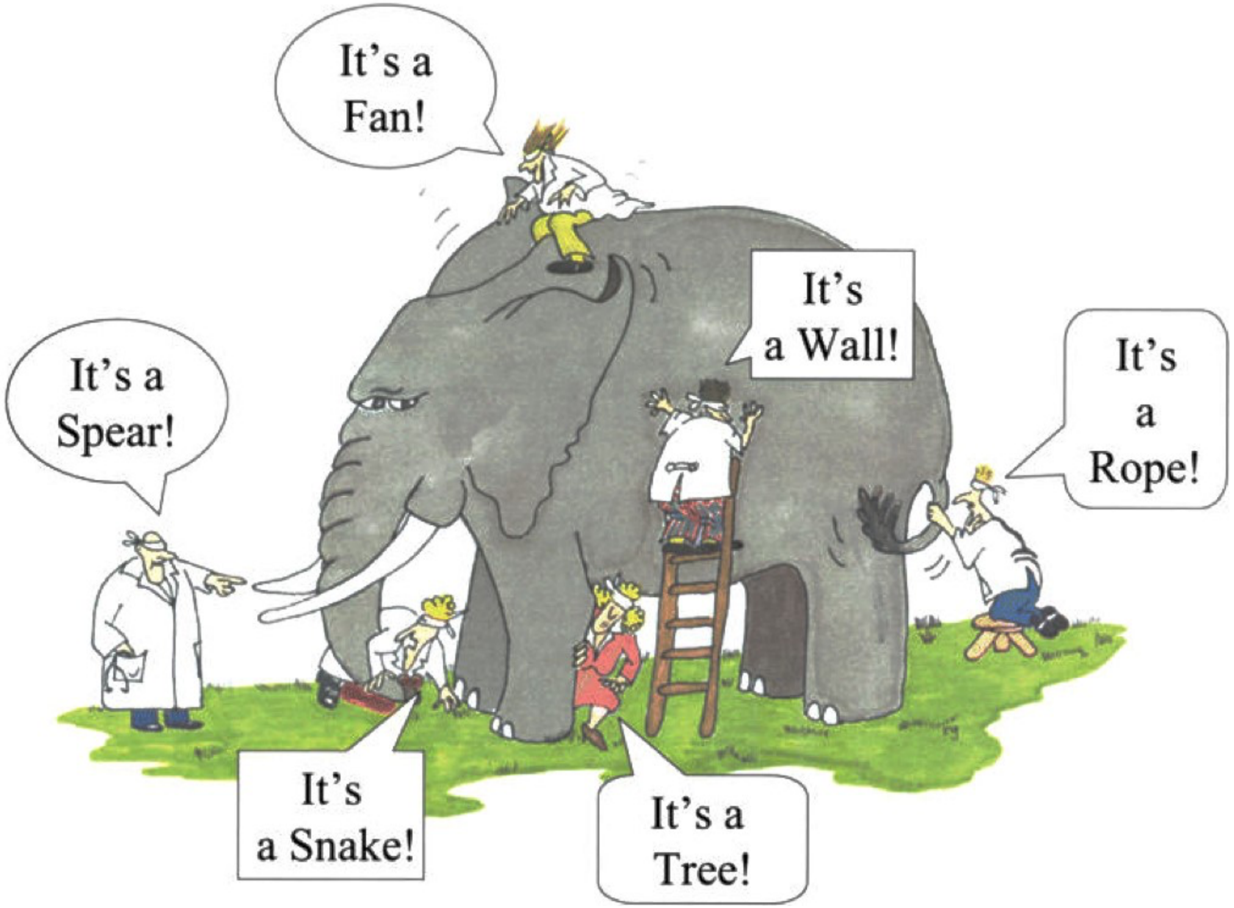
Cancel this transaction

ATTACKS WE DEMONSTRATED

- Login to remote account despite 2FA protection.
- Hijack the user's instant messenger installation.

- User pays for wrong online credit card payment despite 3D-Secure protection.
- Redirect an online banking transaction despite transaction authorization protection.

IN SUMMARY: CONTEXT MATTERS



THANK YOU FOR YOUR ATTENTION

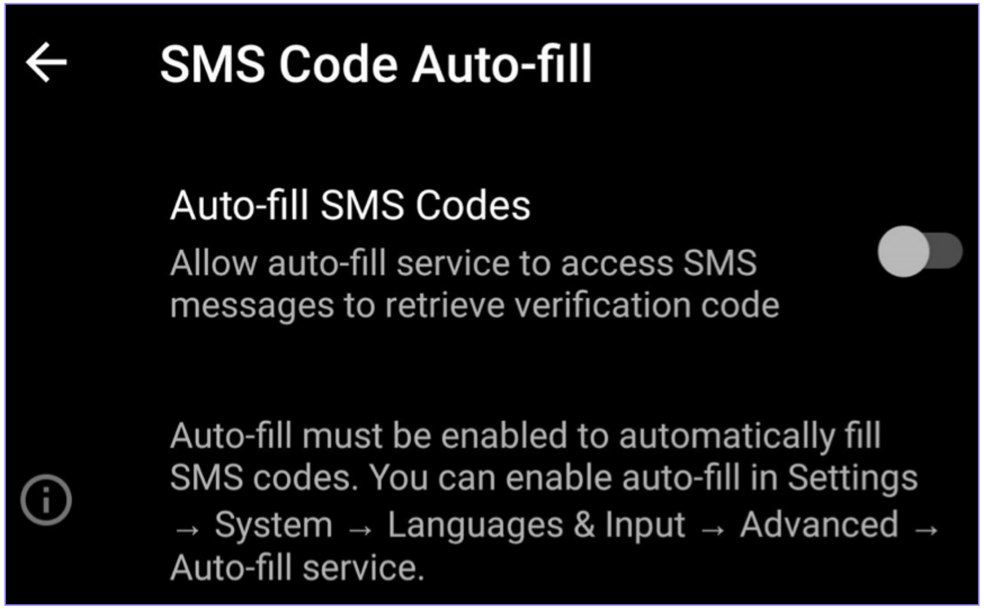
Taken Out of Context: Security Risks with Security Code AutoFill in iOS & macOS

Andreas Gutmann
OneSpan Cambridge Innovation Centre &
University College London
andreas.gutmann@onespan.com

Steven J. Murdoch
OneSpan Cambridge Innovation Centre &
University College London
s.murdoch@ucl.ac.uk

This work has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement **No 675730**, within the Marie Skłodowska-Curie Innovative Training Networks (ITN-ETN) framework.

THE FORESHADOWING

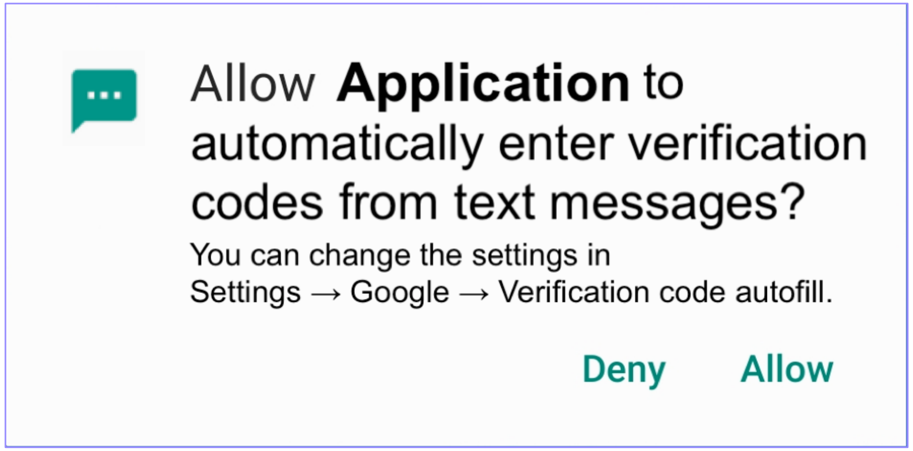


SMS Code Auto-fill

Auto-fill SMS Codes

Allow auto-fill service to access SMS messages to retrieve verification code

Auto-fill must be enabled to automatically fill SMS codes. You can enable auto-fill in Settings → System → Languages & Input → Advanced → Auto-fill service.



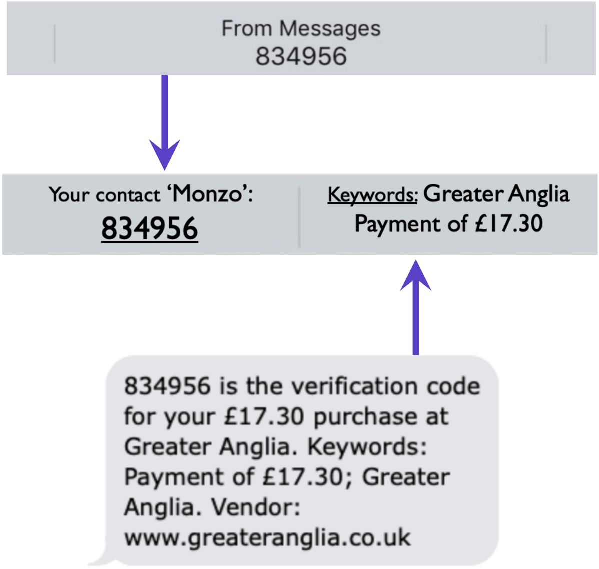
Allow **Application** to automatically enter verification codes from text messages?

You can change the settings in Settings → Google → Verification code autofill.

IDEAS FOR ALTERNATIVE DESIGNS

Two main design challenges:

- Salient context data shall be extracted from the SMS, yet SMS shall remain legible for users without the feature.
- Character and space constraints on the length of SMS and from the device's screen, respectively.



From Messages
834956

Your contact 'Monzo':
834956

Keywords: Greater Anglia
Payment of £17.30

834956 is the verification code for your £17.30 purchase at Greater Anglia. Keywords: Payment of £17.30; Greater Anglia. Vendor: www.greateranglia.co.uk

Opportunities we identified:

1. Replace '*From Messages*' text with information about the sender.
2. Introduction of '*Keywords*' in SMS for context information.
3. Method to specify intended website/app in the SMS.

Alternative: Display the entire SMS on the screen

REMOTE LOGIN

Scenario:

- User has an account with PayPal and activated the Two-Factor Authentication feature.
- Adversary knows user's PayPal credentials, i.e. email address and password.

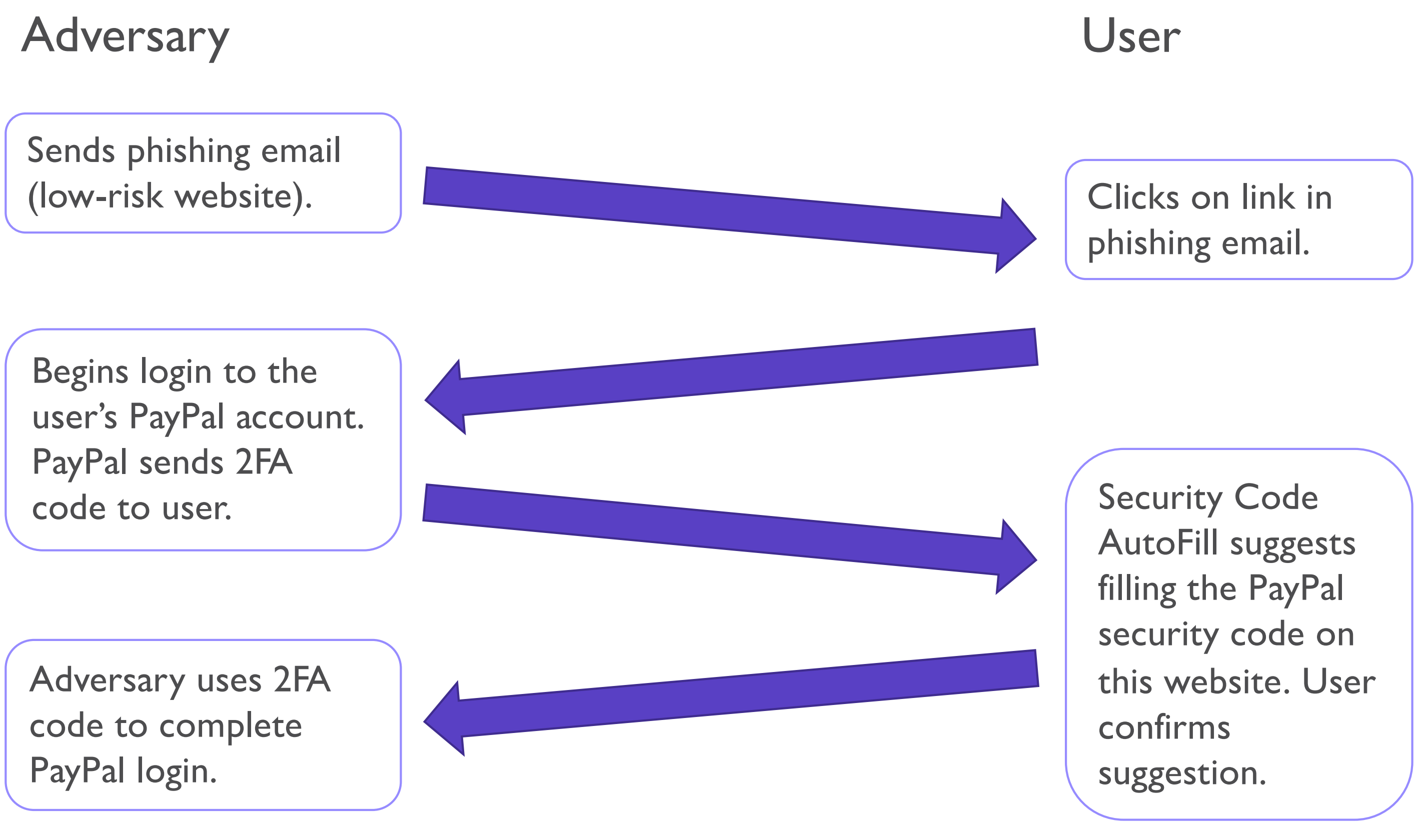
Attack vector:

- Adversary sends a phishing email for an unrelated, 'low-risk' website to the user.

  People are less likely to detect phishing emails of 'low-risk' websites due to changes in the expected cost-benefit ratio.[1]

[1] Herley, C. (2009). So long, and no thanks for the externalities: the rational rejection of security advice by users. NSPW.

REMOTE LOGIN



Adversary

User

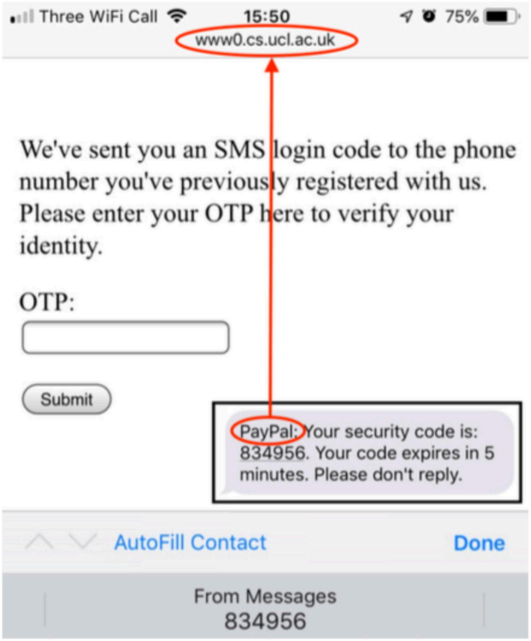
Sends phishing email (low-risk website).

Clicks on link in phishing email.

Begins login to the user's PayPal account. PayPal sends 2FA code to user.

Security Code AutoFill suggests filling the PayPal security code on this website. User confirms suggestion.

Adversary uses 2FA code to complete PayPal login.



We've sent you an SMS login code to the phone number you've previously registered with us. Please enter your OTP here to verify your identity.

OTP:

PayPal: Your security code is: 834956. Your code expires in 5 minutes. Please don't reply.

APP REGISTERED TO PHONE NUMBER

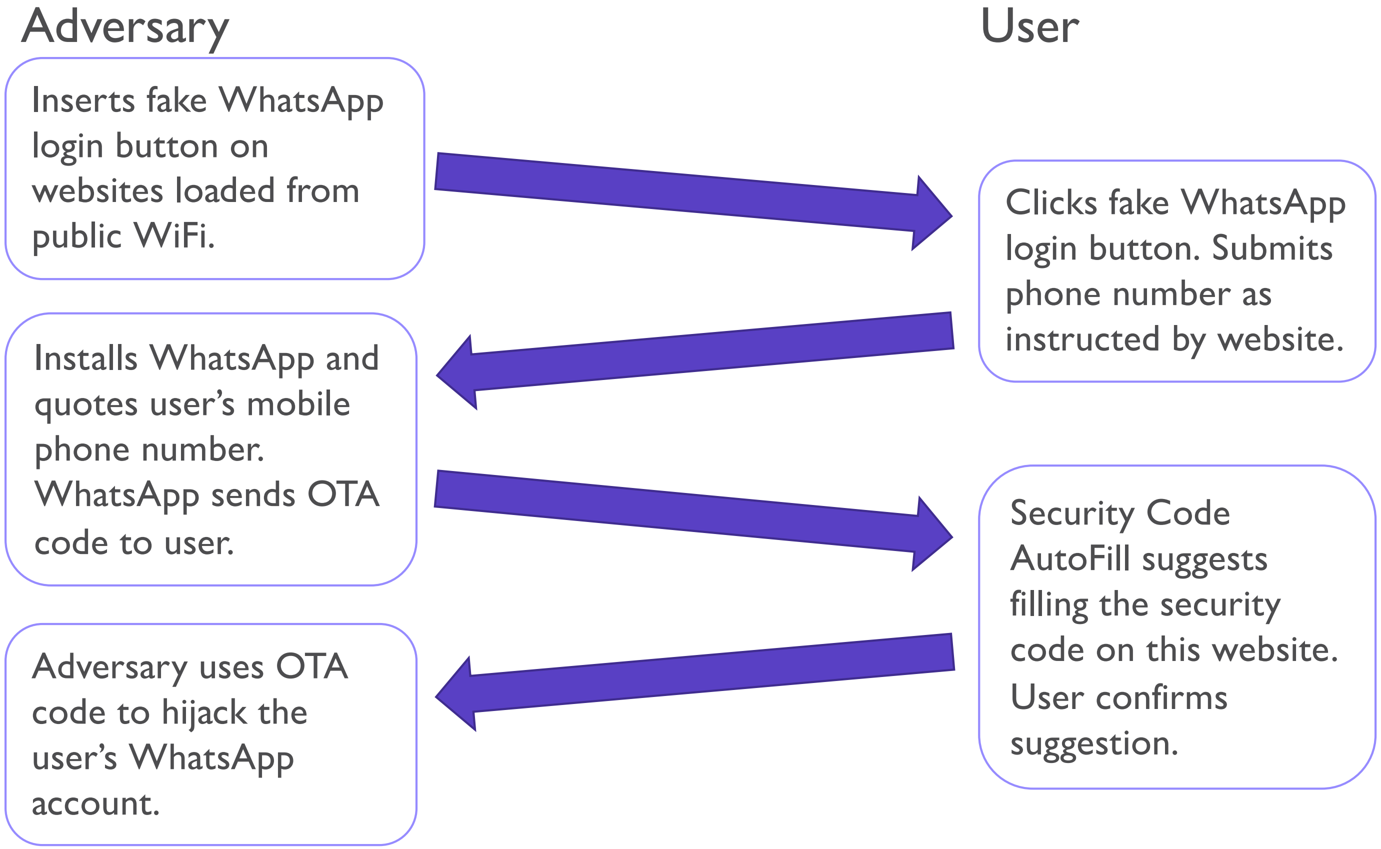
Scenario:

- Adversary wants to hijack other people's WhatsApp messenger to subsequently social engineer and defraud their contacts.
- User browses Internet via unsecured public WiFi.

Attack vector:

- Adversary conducts a trawling Man-in-the-Middle attack on an unencrypted Wi-Fi, scans websites for social login buttons (e.g. g Login with Google), and injects a fake WhatsApp login button.

APP REGISTERED TO PHONE NUMBER



Adversary

User

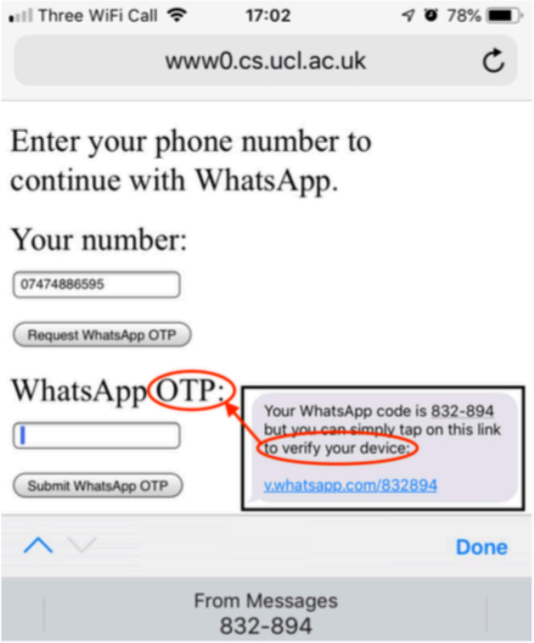
Inserts fake WhatsApp login button on websites loaded from public WiFi.

Clicks fake WhatsApp login button. Submits phone number as instructed by website.

Installs WhatsApp and quotes user's mobile phone number. WhatsApp sends OTA code to user.

Security Code AutoFill suggests filling the security code on this website. User confirms suggestion.

Adversary uses OTA code to hijack the user's WhatsApp account.



Enter your phone number to continue with WhatsApp.

Your number:

07474886595

Request WhatsApp OTP

WhatsApp OTP:

Submit WhatsApp OTP

Your WhatsApp code is 832-894 but you can simply tap on this link to verify your device:

v.whatsapp.com/832894

ONLINE PAYMENT

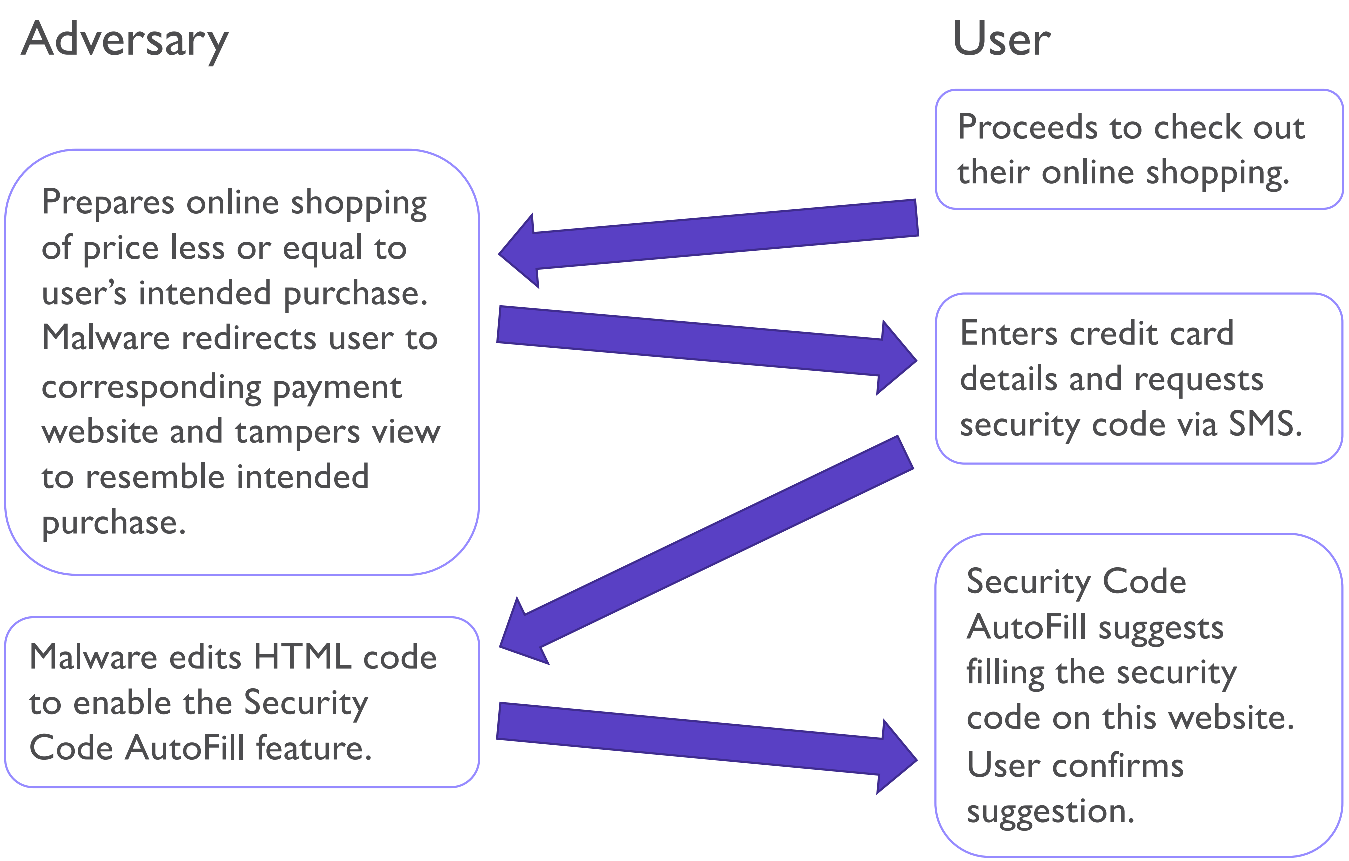
Scenario:

- User wants to make a credit card payment at an online shop.
- Adversary wants user to make payment for their purchase instead.

Attack vector:

- The adversary has infected the user’s MacBook with malware, e.g. a Man-in-the-Browser attack.

ONLINE PAYMENT



Adversary

User

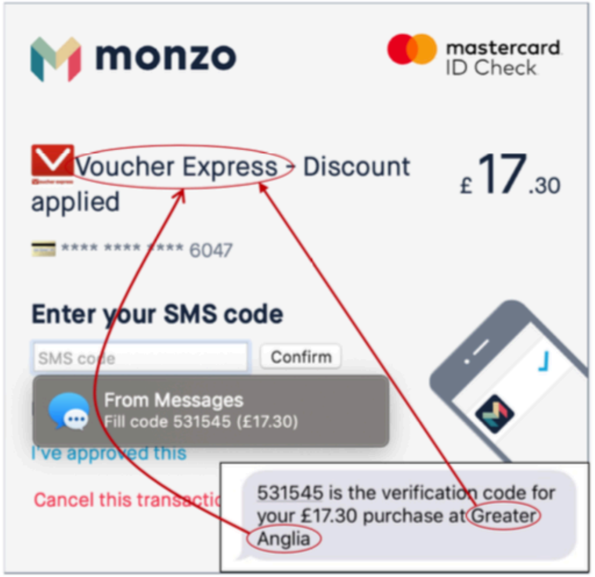
Proceeds to check out their online shopping.

Prepares online shopping of price less or equal to user’s intended purchase. Malware redirects user to corresponding payment website and tampers view to resemble intended purchase.

Enters credit card details and requests security code via SMS.

Malware edits HTML code to enable the Security Code AutoFill feature.

Security Code AutoFill suggests filling the security code on this website. User confirms suggestion.



Voucher Express - Discount applied £17.30

**** **** **** 6047

Enter your SMS code

From Messages
Fill code 531545 (£17.30)

I've approved this

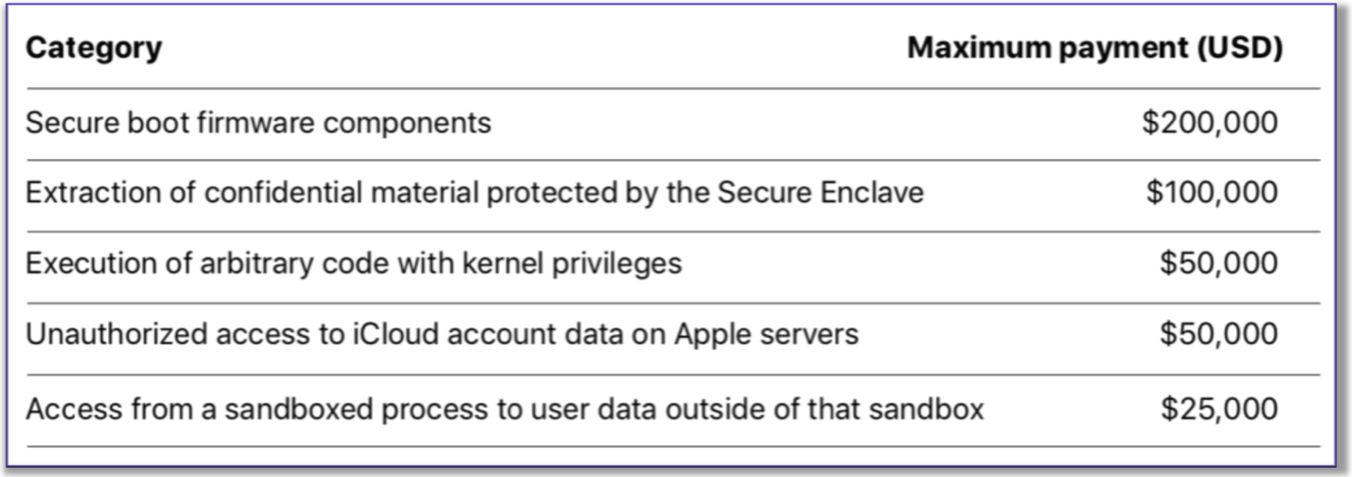
Cancel this transactio

531545 is the verification code for your £17.30 purchase at Greater Anglia

APPLE'S SECURITY BOUNTY POLICY

Apple does not reward the security risks we identified through their Bug Bounty program.

They recognise the following:



Category	Maximum payment (USD)
Secure boot firmware components	$200,000
Extraction of confidential material protected by the Secure Enclave	$100,000
Execution of arbitrary code with kernel privileges	$50,000
Unauthorized access to iCloud account data on Apple servers	$50,000
Access from a sandboxed process to user data outside of that sandbox	$25,000

https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf

METHODOLOGY: COGNITIVE WALKTHROUGH IN MALICIOUS SETTINGS

Cognitive Walkthrough (CW)

One or more evaluators work through a series of tasks from the user's perspective and evaluate the systems ability to guide its users towards achieving their goals.

Define:

- User interface and context
- User and their goals
- User's necessary sequence of actions

Questions asked at each step of a CW:

1. Will the user know what to do at this step?
2. If the user does the right thing, will they know they did the right thing and make progress towards their goal?

CW in Malicious Settings

We extend the CW methodology to enable the simulation of an adversary.

Define:

- Adversary goals
- Threat model and attack vectors

Additional questions asked at each step of a CW in Malicious Settings:

3. What actions could an adversary take to get closer to their goal?
4. How could the user foil such an attack at this step?

Benefits of CW in Malicious Settings

- Focused evaluations of selected features:

  Easier to evaluate events that might rarely occur during an empirical user study

  Avoids bias when asking participants to focus on certain tasks/events

  Easier to transfer results between different versions or variations of the evaluated system

- Avoiding partial disclosure / deception:

  Sensitive tasks can require researchers to withhold information about the nature and objectives of the research.

Use of CW in Malicious Settings

- Prototyping / development
- Pre-studies
- Identifying security and privacy risks

BACKGROUND: DESIGN OF SECURITY MESSAGES

- Principle of *'Explicit Communication'* *(Abadi and Needham, 1996)*

  "Every message should say what it means: the interpretation of the message should depend only on its content."

- *'Design principles for warning messages'* (Laughery and Wogalter, 1997)
  - ➢Be concise but clearly convey the message
  - ➢Use concrete rather than abstract wording
  - ➢Avoid unfamiliar abbreviations or ambiguous statements
  - ➢Use short sentences with short, familiar words
  - ➢Messages should be explicit in what the reader should do or not do