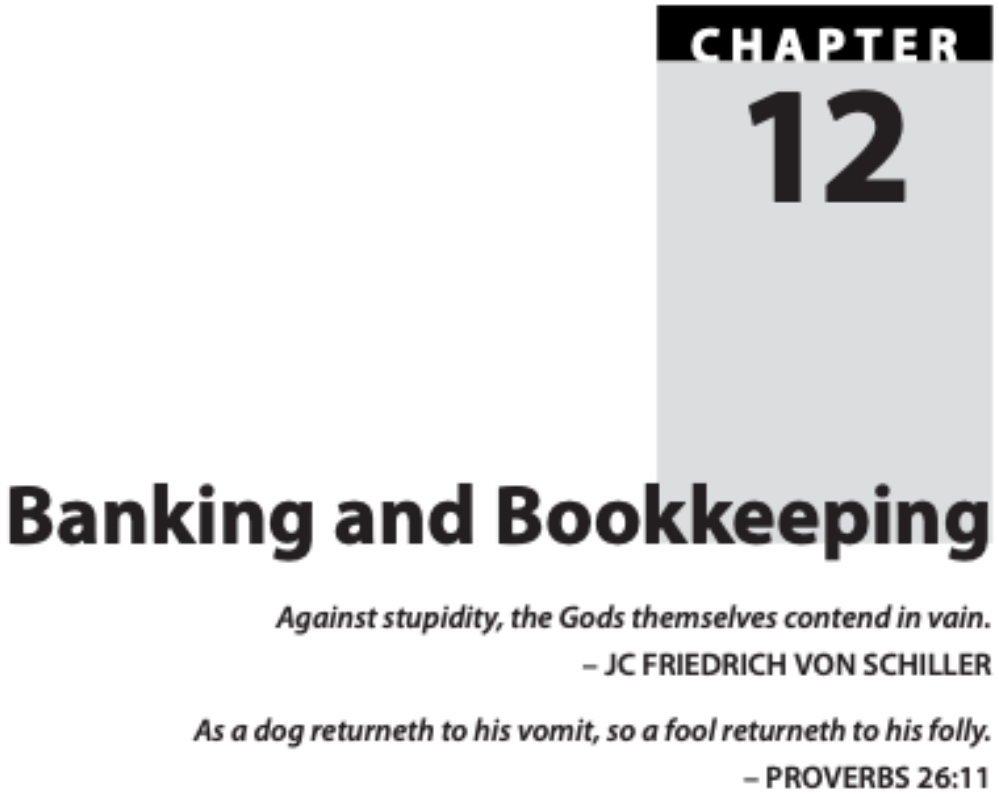
Security Engineering

INFR11208 (UG4) // NFR11228 (MSc)

Daniel W. Woods* **and Jingjie Li**
Email: daniel.woods@ed.ac.uk **and** jingjie.li@ed.ac.uk

Chapter 12, Security Engineering


CHAPTER

12

Banking and Bookkeeping

Against stupidity, the Gods themselves contend in vain.

– JC FRIEDRICH VON SCHILLER

As a dog returneth to his vomit, so a fool returneth to his folly.

– PROVERBS 26:11

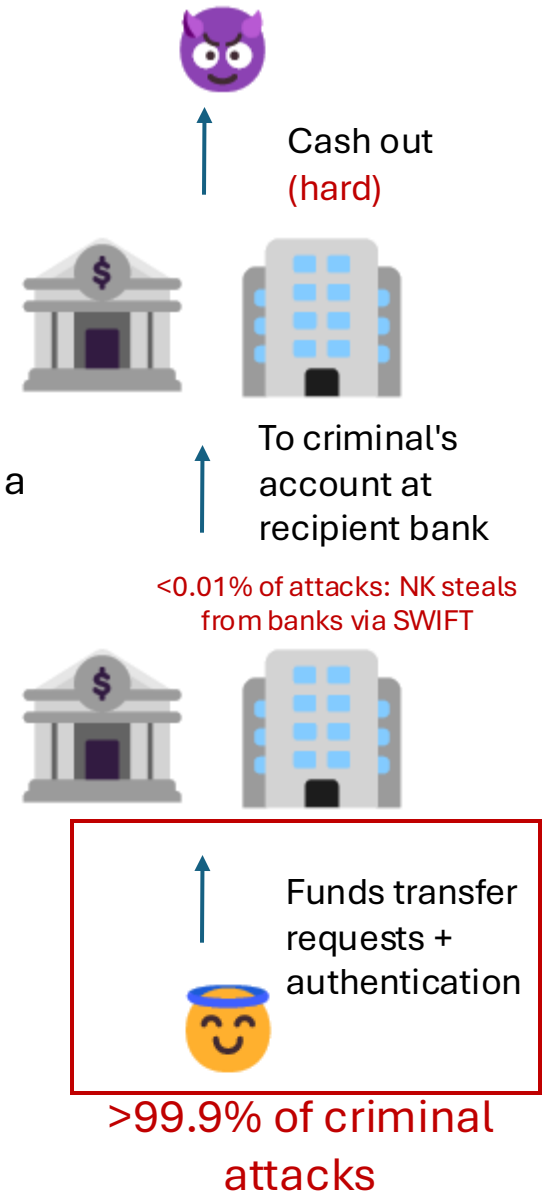
https://www.cl.cam.ac.uk/archive/rja14/Papers/SEv3-ch12.pdf

How can a "hacker" steal from a bank?

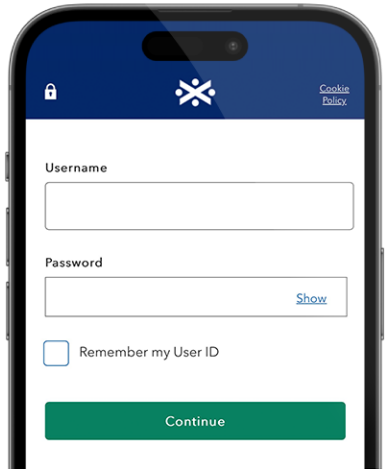
1. **Money Creation**
   Violate Clark-Wilson integrity model and credit criminal's account without debiting another account
   - Hard thanks to MAC
   - No known examples, which would exploit implementation details
     - Lucky given this violates trust in the entire banking system
2. **Break authentication and impersonate the victim**
   Work within Clark-Wilson model and credit criminal's account by debiting victim's account via the criminal authenticating as the victim (or some delegated authority)
   - All kinds of attacks have been demonstrated here
     - Forging signature of a physical cheque
     - Getting access to victim's banking website account/app
     - Impersonating card, stealing/bypassing PIN, manipulating terminal
     - Compromise SWIFT to manipulate interbank transfers
   - Occasionally used by cyber criminals at scale

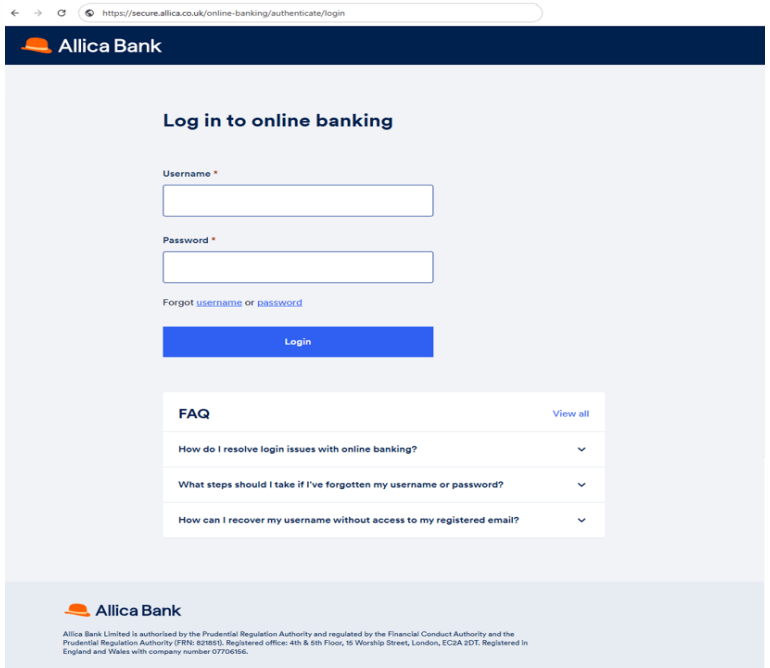
Today's lecture

3. **Socially engineer the victim**
   Work within Clark-Wilson model and socially engineer victim to credit criminal's account by debiting their own account, authenticating as themselves
   - Vast majority of cybercrime losses across investment fraud, business email compromise etc



Potential weak points to attack





How banks move money around

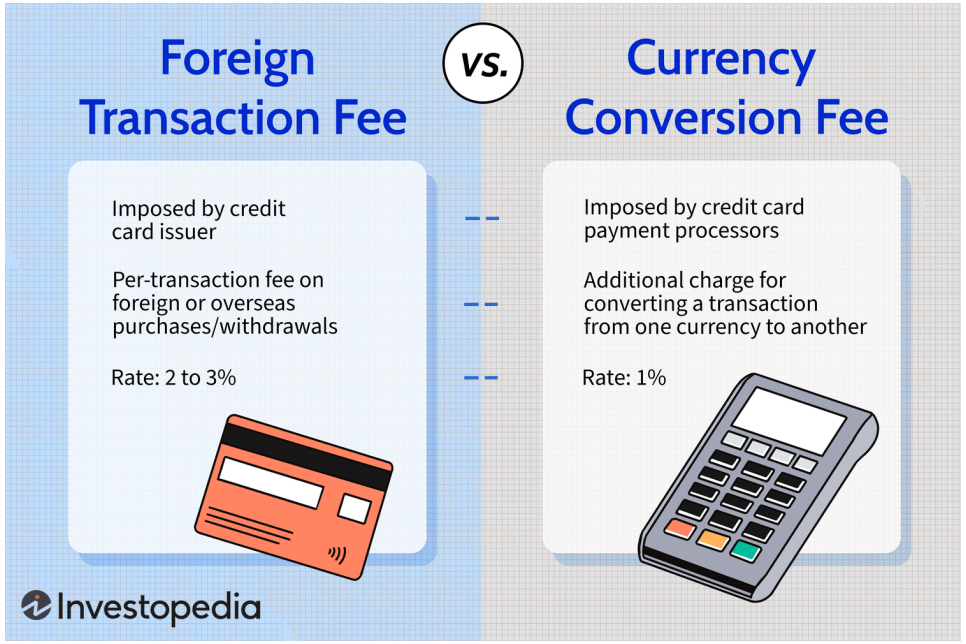
When bank receives transfer request and actions the request

Bank transfers

- In branch requests for bank transfers
  - “Please pay Alice £100 from my account with you no. 1234, signed Bob”
- Can authenticate via combination of personal relationship, signature and ID
  - Then forward funds to Alice's bank
- Interbank transfers sent to a Clearing House and net out at end of day
  - BACS in UK, ACH in US
  - **Why is this hard for threat actors to attack?**

How do banks ‘send’ money abroad?

- Banks have accounts at correspondent banks in other countries
  - Often reciprocated
  - Some banks set up foreign subsidiaries
- If you want to send Aus$1000 to Aunt Agatha in Sydney, your bank sends:
  - ‘To National Australia Bank. Please pay Aus$1000 to AD Jones, account XYZ, from our account with you number ABC’
- Now how do you send the request?



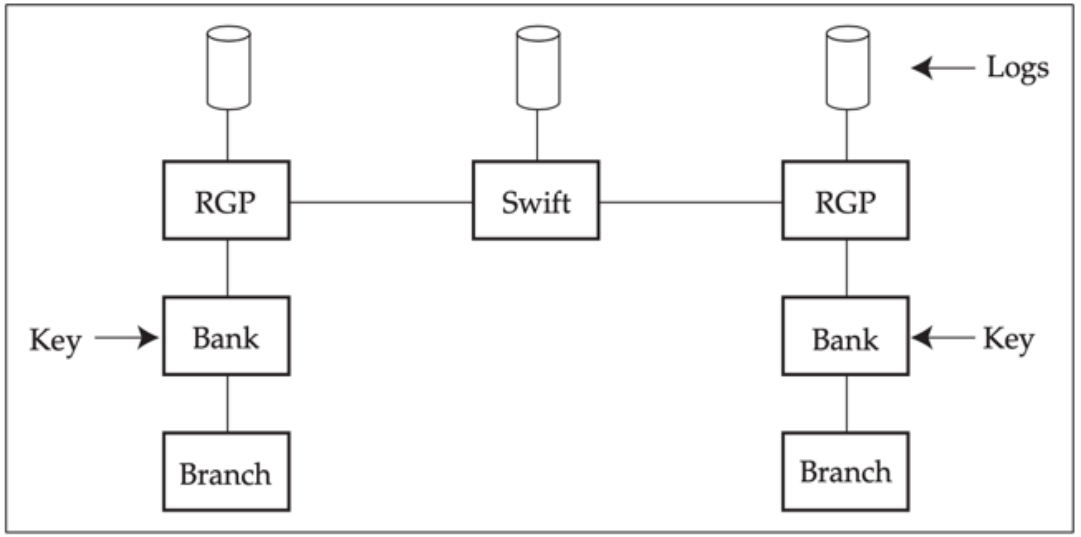
19th century: 'Victorian Internet'

- From the 1840s, the telegraph allowed banks to transfer money quickly
  - But how do you stop fraud?
- Answer: a 'test key' or manual crypto hash to check integrity
- Want to send £376,000, then include auth: 207
  - 53 is 0x1,000,000. 53 is 3x100,000. 29 is 7x10,000. 71 is 6x1,000. --> 53 + 54 + 29 + 71 = 207
  - If attacker adds a million to telegraph message, then bank calculates 207 + (77 – 53) = 231

	0	1	2	3	4	5	6	7	8	9
x 1000	14	22	40	87	69	93	71	35	06	58
x 10,000	73	38	15	46	91	82	00	29	64	57
x 100,000	95	70	09	54	82	63	21	47	36	18
x 1,000,000	53	77	66	29	40	12	31	05	87	94

1970s: SWIFT

- Key management?
  - Send keys between senior bank managers in person or by post
- Transaction control
  - Clerk A enters transactions
  - Accountant B checks and can change them
  - Manager C releases them
- Owned by 11,000 banks worldwide
- SWIFT now ‘sends’ $125tr a year but **it’s the banks’ own systems that balance funds**
- Hard part is the laundry step



- MACs for integrity, logs for non-repudiation

SWIFT attacks

May 2015

Hackers open four fake accounts at RCBC bank.

Late 2015

Initial breach of Bangladeshi Bank via phishing email; malware begins "spying" on bank processes.

Feb 4, 2016

- 35 fraudulent SWIFT requests ($951M total) to federal reserve bank in New York.
- One instruction misspelled "Foundation".
- Typo + volume of requests caused the Fed and a routing bank (Deutsche Bank) to halt 30 of the 35 transactions.

Feb 8, 2016

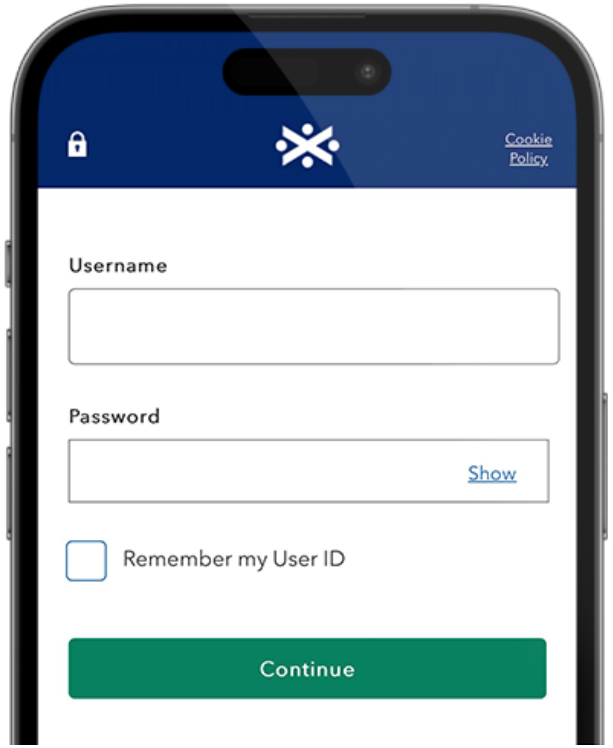
$81m withdrawn from RCBC and moved to casinos in Phillippines.

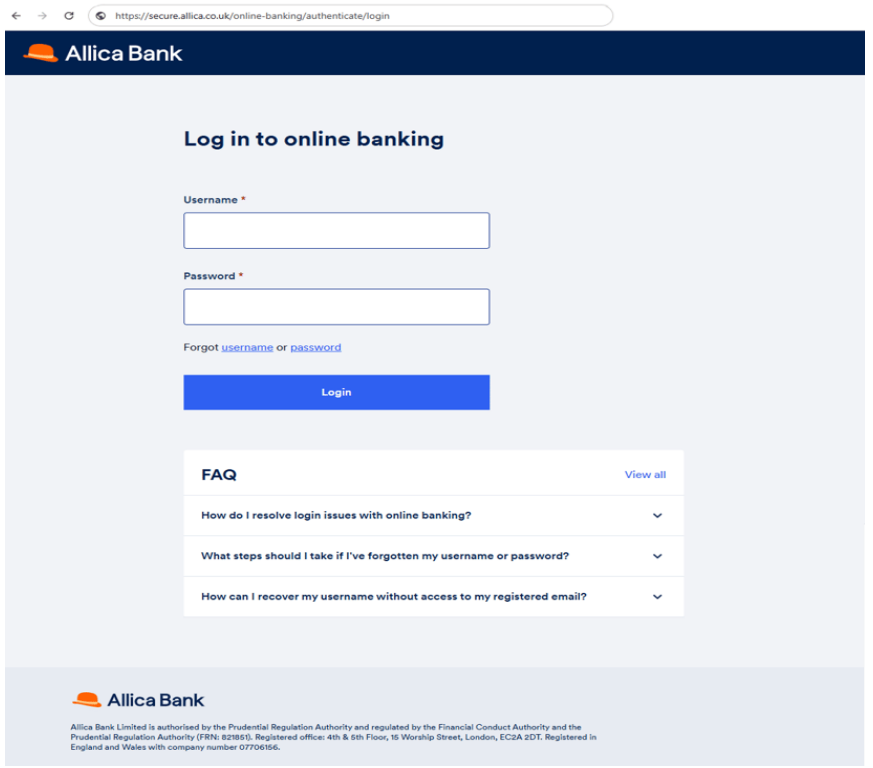
The Lazarus heist: How North Korea almost pulled off a billion-dollar hack

21 June 2021

How banks move money around

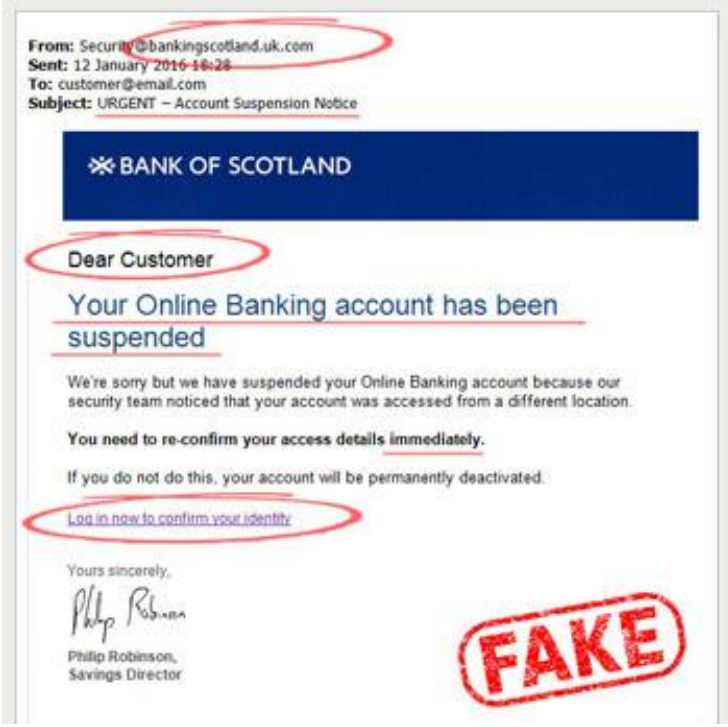
When the request comes from the internet





Online electronic banking

- Early pilots in 1980s; phone banking in 1990s; online banking from mid 1990s
- Phishing from 2005 killed static passwords
- "Remember, your bank (or any other official source) will never ask call and ask you to confirm your bank account details."
  - NCSC: https://www.ncsc.gov.uk/collection/phishing-scams/spot-scams
  - But how consistent is this followed?
  - Idea of security "norms"


From: Security@bankingscotland.uk.com
Sent: 12 January 2016 16:28
To: customer@email.com
Subject: URGENT – Account Suspension Notice

BANK OF SCOTLAND

Dear Customer

Your Online Banking account has been suspended

We're sorry but we have suspended your Online Banking account because our security team noticed that your account was accessed from a different location.

You need to re-confirm your access details immediately.

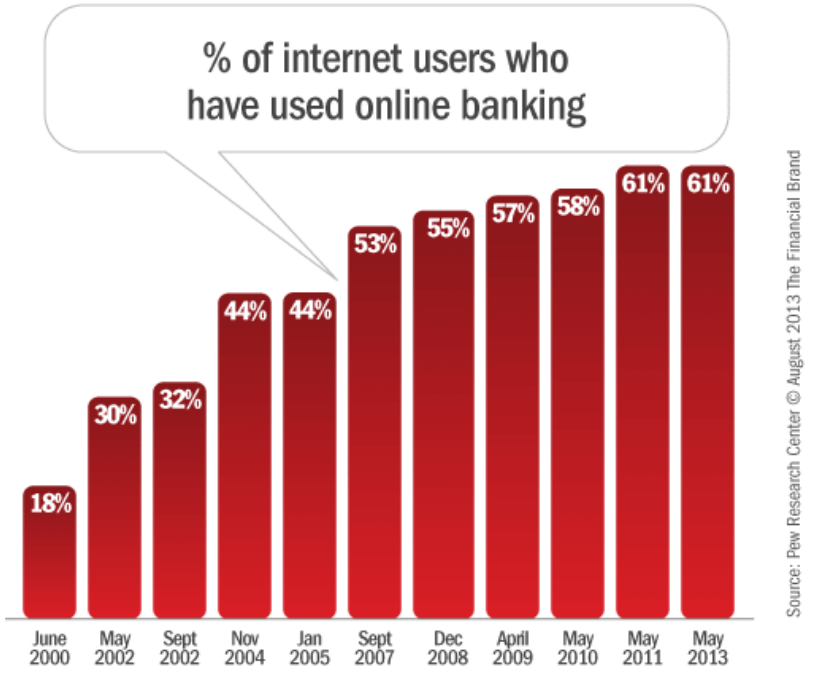
If you do not do this, your account will be permanently deactivated.

Log in now to confirm your identity

Yours sincerely,

Philip Robinson,
Savings Director

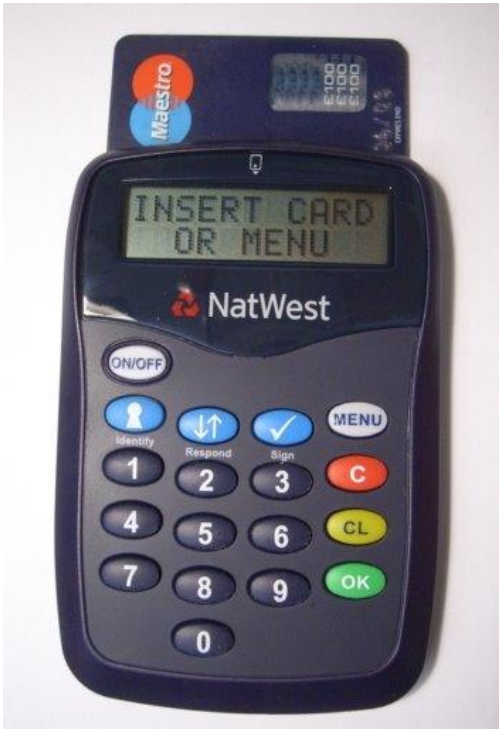
FAKE



The quest for MFA in banking

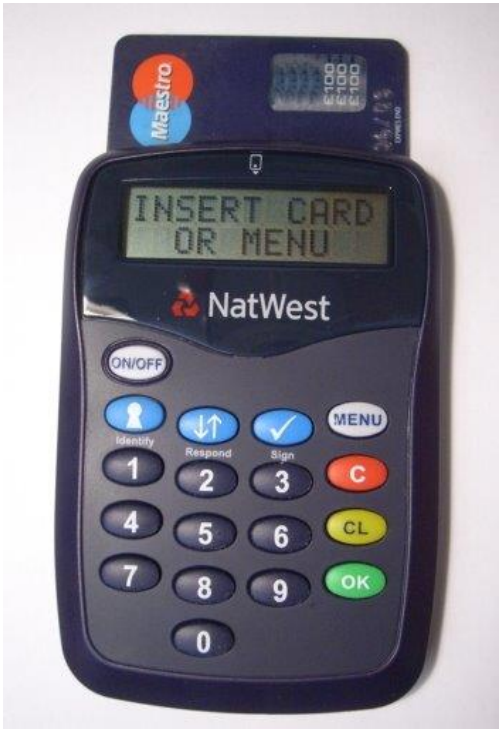
1. The "Little" Calculator (CAP Readers)
   - Secure enough, failed at usability
2. SMS-based OTP
   - Very usable, failed at security
3. App-based push requests --> number matches
   - Fine as of today
     - Problems with physical theft
     - Biometric auth even better
     - Reset issues

Chip Authentication Program (CAP)



- EMV version: each customer has a chipcard
- Easy mode:
  - User --> CAP: PIN
  - CAP --> User: $\{N, PIN\}_{KC}$
    - N incremented and tracked by bank… Why?
    - How could you ensure CAP code is fresh?
- **What went wrong?**

Chip Authentication Program (CAP)



- EMV version: each customer has a chipcard
- Easy mode:
  - User --> CAP: PIN
  - CAP --> User: $\{N, PIN\}_{KC}$
    - N incremented and tracked by bank… Why?
    - How could you ensure CAP code is fresh?
- Man in the browser attacks motivate **serious mode** (e.g. for new payees):
  - User --> CAP: PIN, £ amount, last 8 digits of payee A/C
  - CAP --> User: $\{N, PIN, +\ transaction\ details\}_{KC}$
- **What went wrong?**

What goes wrong with CAP calculators…

guardian.co.uk

Police think French pair tortured for pin details

Matthew Taylor
The Guardian, Saturday July 5 2008

Laurent Bonomo and Gabriel Ferez, two French exchange students who were killed in London. Photographs: Met police/Getty

The two French students who were bound up and brutally murdered at a bedsit in south London may have been tortured for their bank and credit card pin numbers, police said yesterday.

Laurent Bonomo and Gabriel Ferez, both 23, were found at Bonomo's flat in New Cross, south London, on Sunday night. They had been stabbed more than 200 times, bound, gagged, and tortured over several hours.

Underestimating the capabilities of threat actors

Usability issues

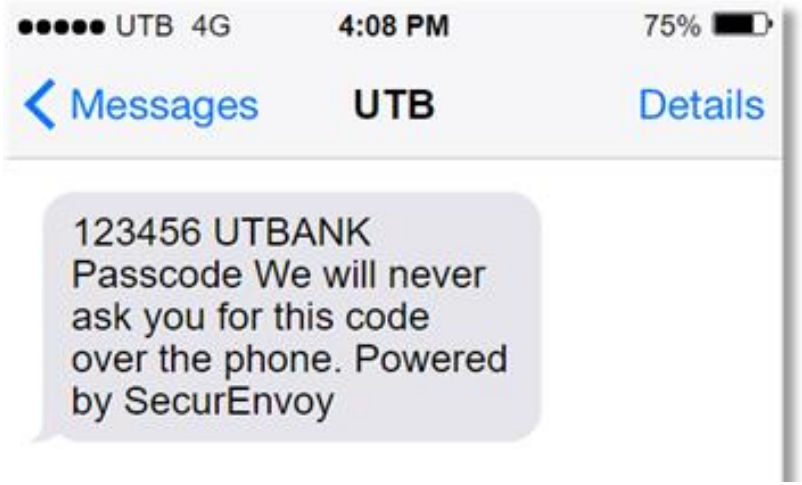
Move to SMS One Time Pass

Why

- "Everyone has a phone"
- Don't need to distribute CAP device
- People carry their phones everywhere

Attacks

- Socially engineer recipient
- Socially engineer phone provider
  - "I've lost my phone, please give me a new SIM"
  - Telecomm providers argue they don't provide auth
- Hack phone network?
  - SS7 hacking has been seen against German and UK banks (starting 2018)



Cryptocurrency investor's $224 million suit against AT&T over stolen coins moves forward

PUBLISHED TUE, JUL 23 2019•9:49 AM EDT UPDATED TUE, JUL 23 2019•3:48 PM EDT

Kate Rooney
@KROONEY

WATCH LIVE

KEY POINTS

- A federal judge in California allows a case against AT&T alleging that it involves the theft of millions of dollars worth of cryptocurrency through a man's phone to move forward.
- The case brought attention to a hacking method known as "SIM swapping," where criminals steal phone numbers to log into cryptocurrency accounts, then transfer the money to themselves.

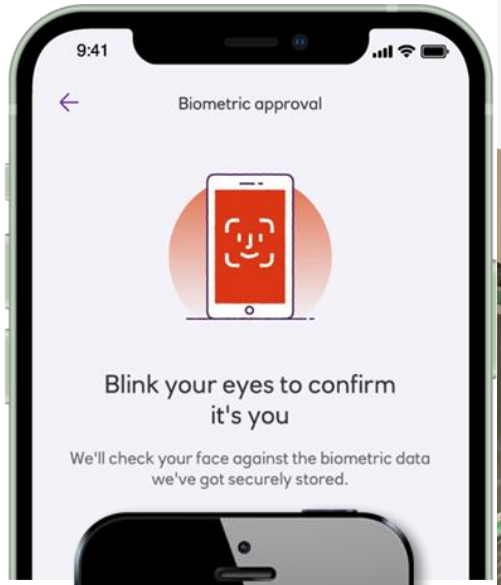
App-based authentication

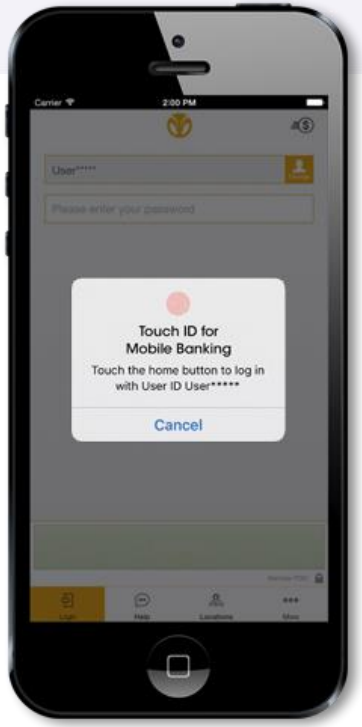
Why

- Send code to phone, but only to an app that requires auth
  - Phone as "something you have"
- Biometric auth
  - "something you are"
  - Stored in secure enclave

Attacks

- Get physical access to phone
  - Mostly thwarted by biometric auth
- Install app on a new phone
  - Some use SMS-OTP, others e-KYC, and others device binding/chaining
  - Deep fakes?





'Train phone snatcher stole £21,000 from my bank apps'

Michael Race & Sean Dilley
Business reporter & Transport correspondent, BBC News

13 December 2024

Niall McNamee was scrolling through his phone on the London Underground when a thief on the platform snatched it from his hand just as the doors closed.

Two days later the 30-year-old discovered his bank accounts had been drained by about £21,000 - including a £7,000 loan taken out in his name.

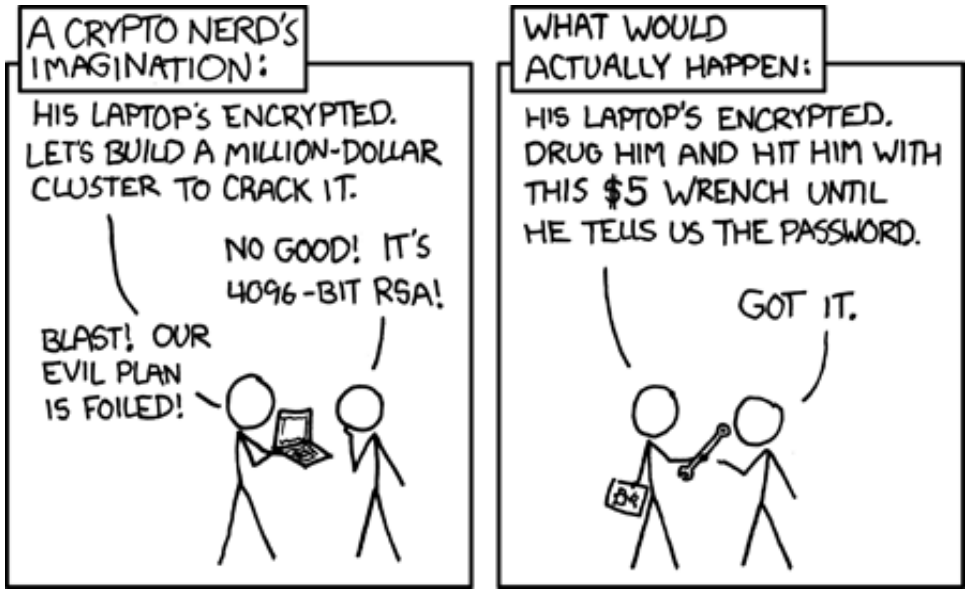
When geography impacts digital threats

Bogotá police take down gang drugging victims in Teusaquillo and Chapinero

By Steve Hide *September 27, 2025*

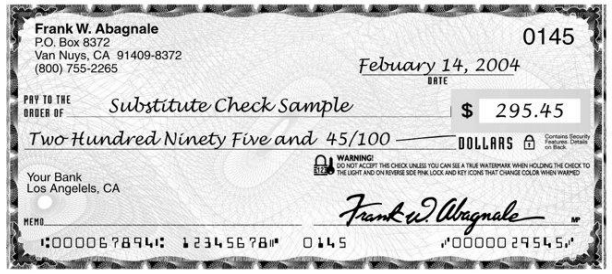
City security chief warns of continued risks to revellers after capture of 'La 57'

Members of the La 57 gang after their capture in Bogotá this week. Photo: Bogotá mayor's office.



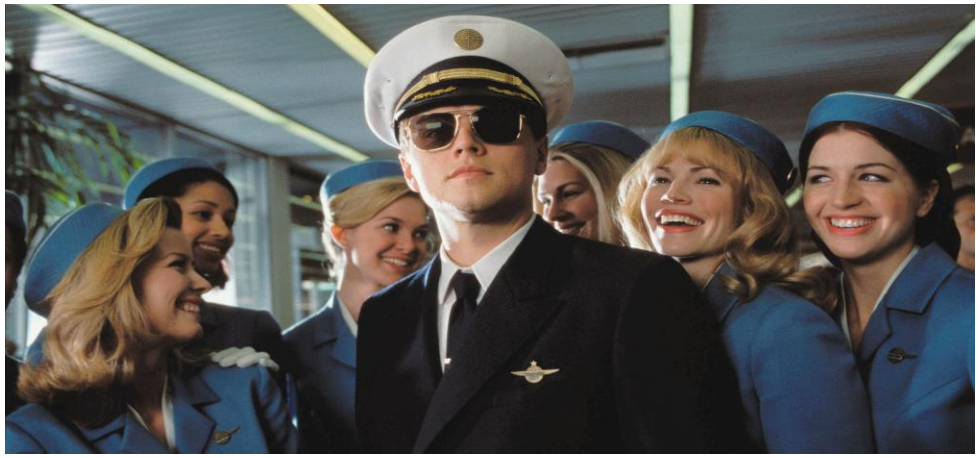
How banks move money around

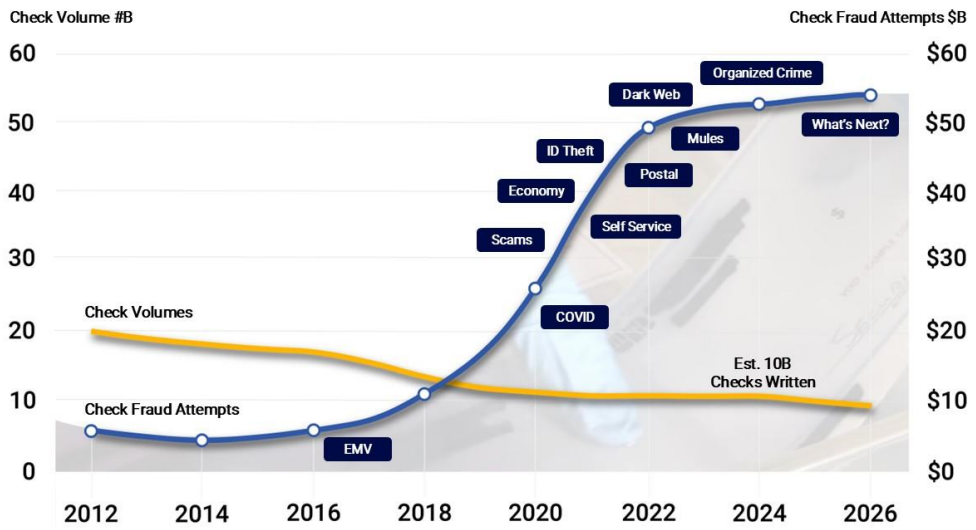
When the bank is not directly involved in the transaction, but the card is



Cheques

- “Dear RBS, Please pay Alice £100 from my account no. 1234, signed Bob”
  1. Alice takes cheque to her bank
  2. Alice's bank sends to the Bob's bank
  3. Bob's bank verifies the cheque + balance
  4. Approve transferring £100 to Alice's bank
- Slow (3–10 days) with two forms of uncertainty:
  - Is this the real account owner
    - Authentication failures
  - Are they good for the money?





1980s: ATM networks

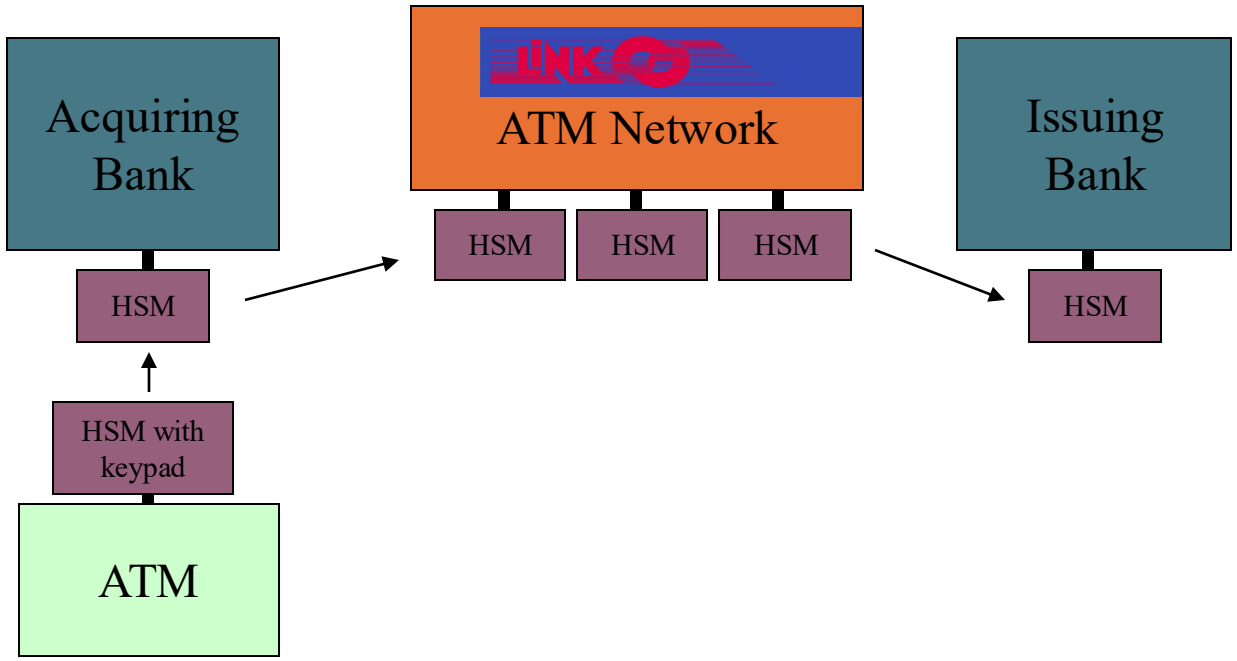
Security policy:

"Only the customer should know their PIN"

- Magnetic strip stores account holder name, number, expiry date
  - **NOT PIN**

How it worked

- Issuing bank verifies PIN
  - Hardware security modules keep PINs from individual bank staff
- A network switch translates PINs and also keeps settlement accounts



See Ross' video for gory PIN attacks: https://youtu.be/qVXa3_MlSzY?si=sVsXExbsGrLag7bN&t=1150

How are PINs generated ?

Start with your primary account number (PAN)

5641 8203 3428 2218

Encrypt with your bank's PIN Key

22BD 4677 F1FF 34AC

Chop off the End

2213

decimalise

(B->1)

(D->3)

CVVs similar, but use different keys and card version no. too

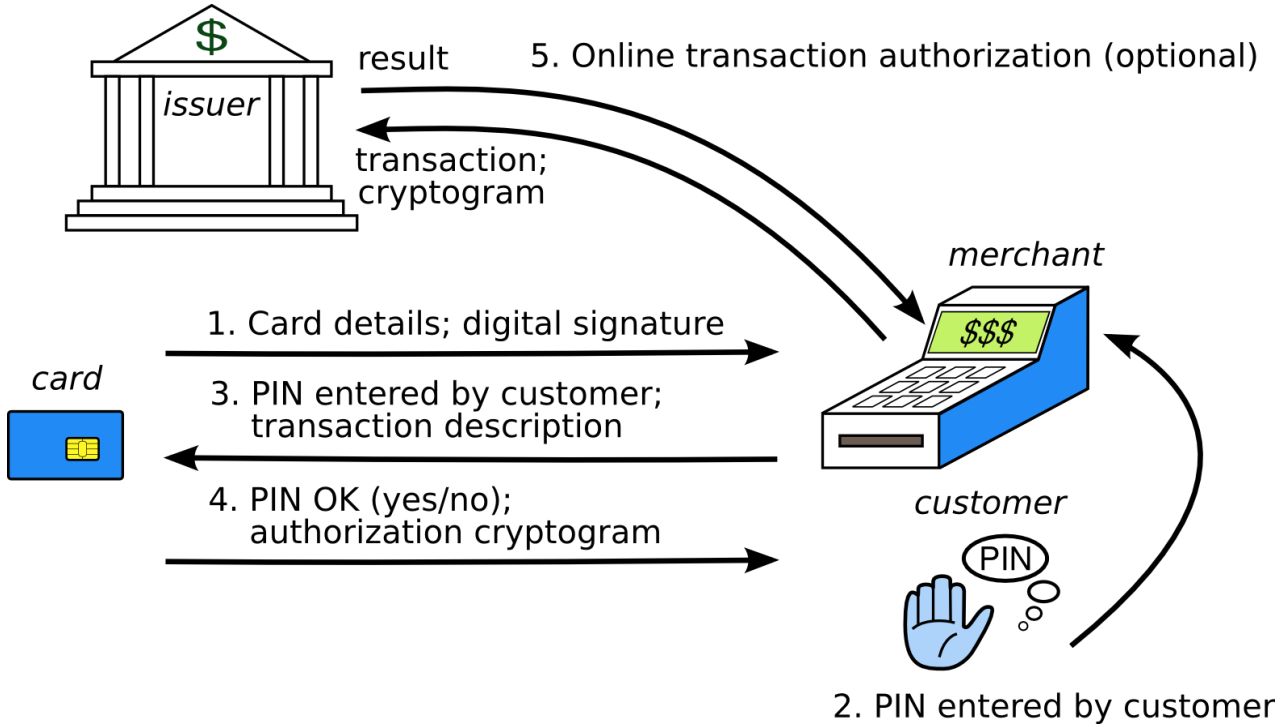
Store offset to allow customer to change PIN

What went wrong

- Magnetic strip cards were easy to copy
  - Fraud industrialised using ATM skimmers
  - PIN shoulder surfed
- Various implementation bugs, insider attacks, network diversion, malware, social engineering PINs for stolen cards (see Ross' book for more)
- Fix:
  - intrusion detection systems, e.g. FICO
  - **move to smartcards with EMV from 2004**

Europay/MasterCard/VISA (EMV)

- EMV from 2004, for debit & credit cards
  - Need backwards compatibility & offline option (where all the pain comes)



- No Pin attack (2010)
  - "In this paper we describe and demonstrate a protocol flaw which allows criminals to use a genuine card to make a payment without knowing the card's PIN, and to remain undetected even when the merchant has an online connection to the banking network"

The Preplay Attack (2014)

- British sailor goes into bar in Barcelona and pays €33 for two drinks
- Wakes up with a sore head and finds that €33,000 taken in ten payments of €3,300
- Lloyds says ‘Your card and PIN were used…’
- 10 transactions an hour apart, from the same terminal, but through three banks

EMV lacks a trustworthy user interface!

Contactless

- Tickets 1990s; cards 2005; phones 2011-14
- Various flavours
  1. PED device sends (N, d, X)
     - Nonce, transaction details (Amount, Date)
  2. Card answers with a MAC as the CVV
     - Calculated with (N, d, X)
- Vulnerable to replay attacks
- EMV allows a few tap-and-pay transactions with a limit, then demands PIN
- Various bugs and blunders; most notably the limit may fail with foreign currency

'I feel held to ransom by contactless payments'

Roger Wicks says he believes contactless payments are not safe

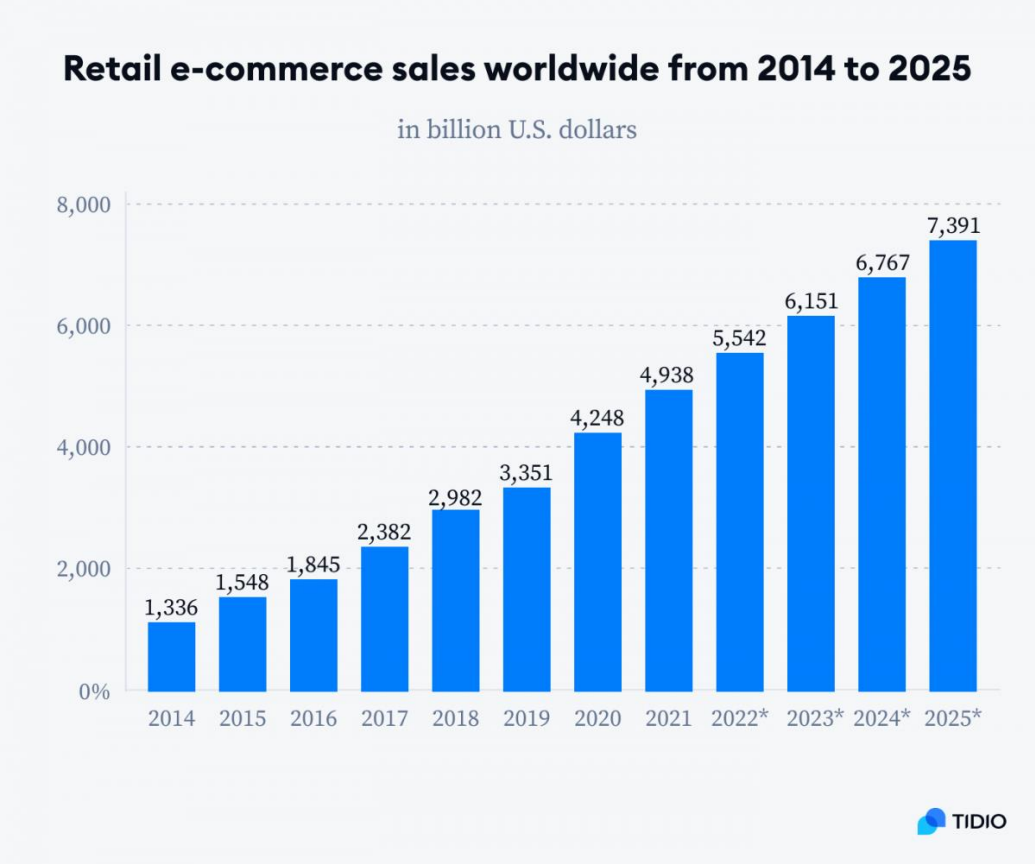
Sarah-May Buccieri

BBC News , Lincoln

6 June 2025

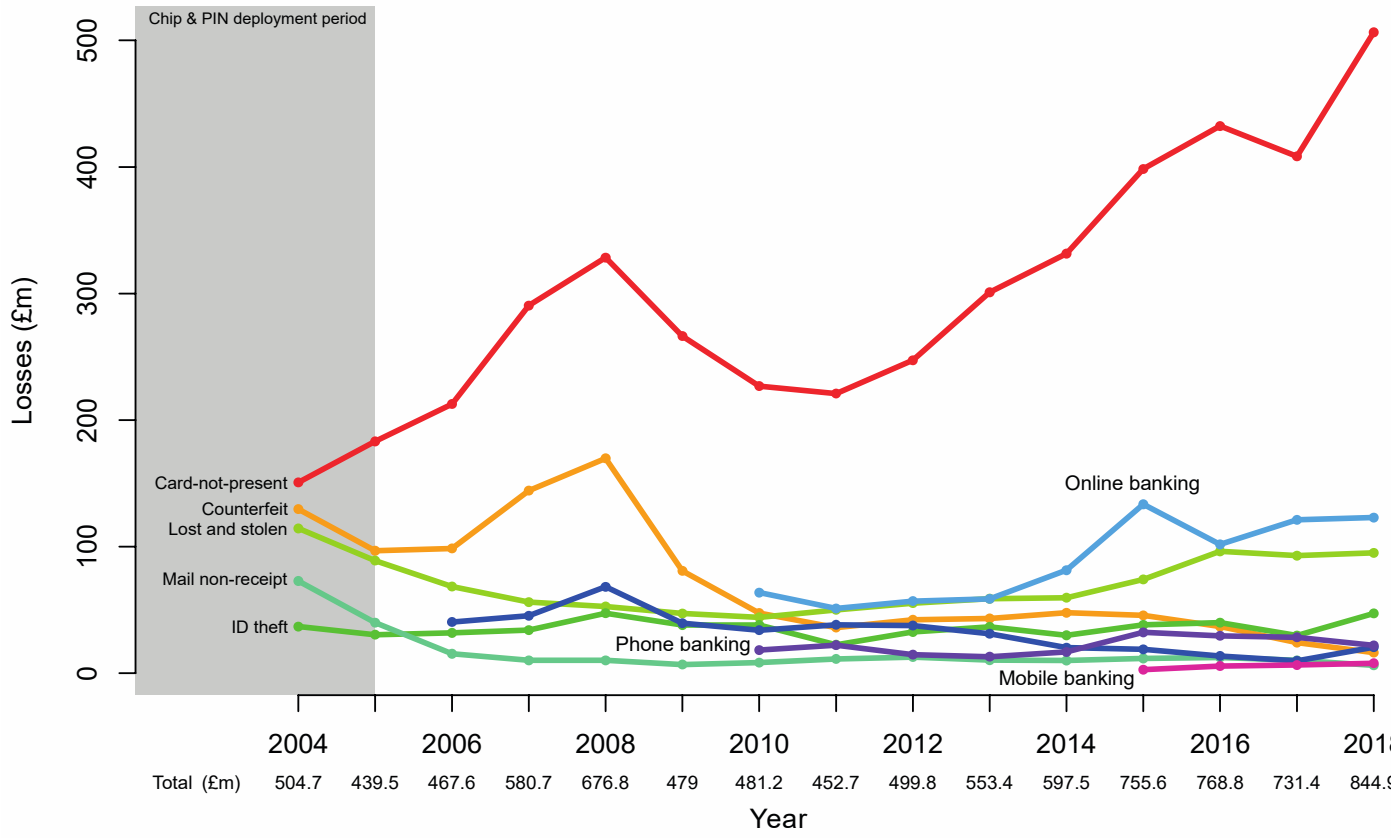
Ecommerce payments

When the bank is not directly involved in the transaction, and the card isn't there either



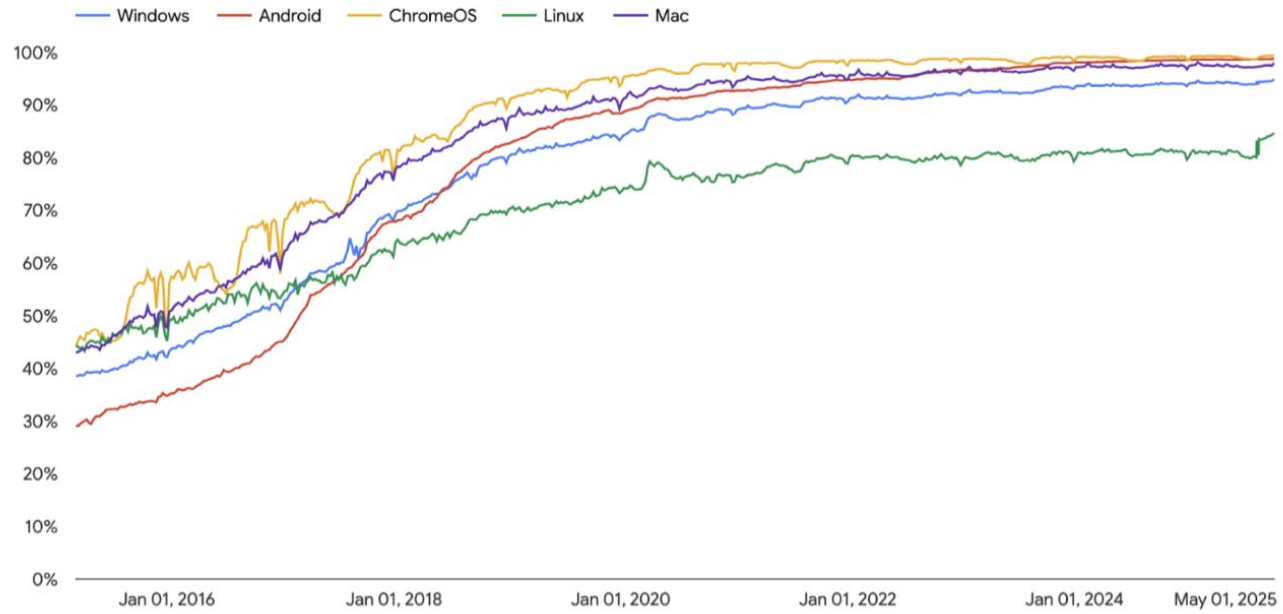
Fraud in the UK since EMV

- EMV worked… but it caused the fraud to find new channels
- Card-not-present fraud shot up at once
- Counterfeit took off once the crooks realised:
  - It's easier to steal card and pin details once pins are used everywhere
  - You could still use mag-strip fallback for several years (especially overseas)
  - Tamper-resistance didn't work properly



TLS and online card payments

- Ecommerce requires static info
  - card details + CVV
- Netscape hacked together SSL; Verisign was set up to sell certificates to anyone with a website
- SSL became TLS and was ‘verified’, but remained open to middleperson attacks in too many ways
  - Ongoing work to fix (and break) it



Carding forums

- Underground forums sprang up to trade card data, malware, cashout services etc
- Cyber-crooks started to specialize and get good at their jobs
  - Especially data breaches at retail firms

"Fixes"

- Tell retailers not to store CVV
- Merchant websites got fraud engines that turned down several percent of baskets
- PCI DSS
  - See next week's lecture

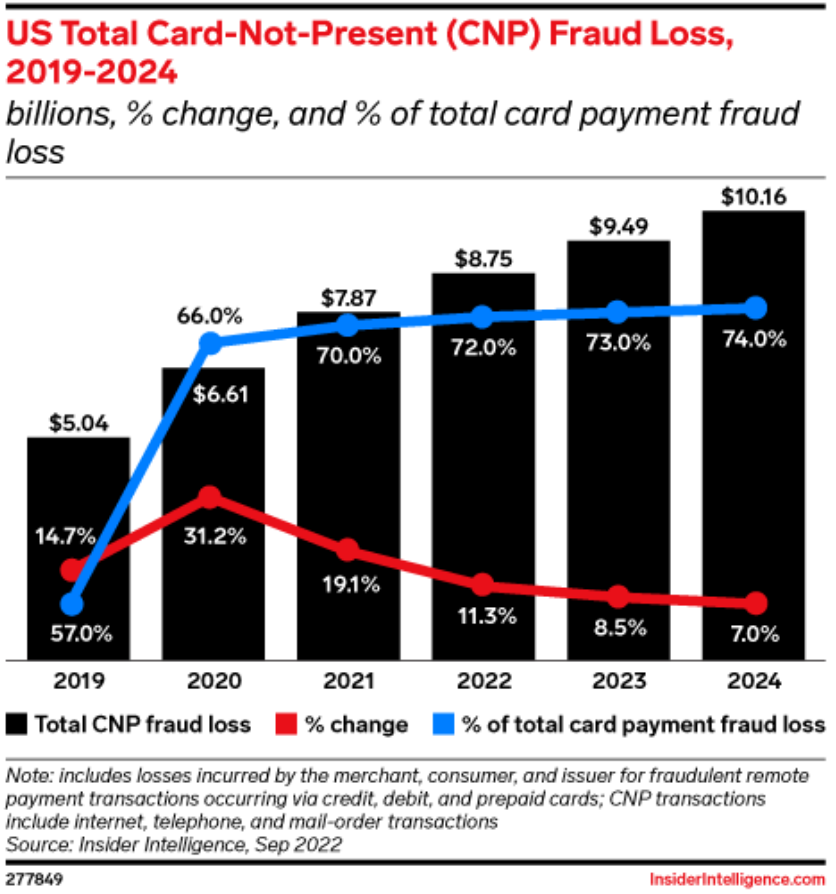
How to guess a CVV, bit by bit

- Of Alexa top 500 websites, 26 only ask for primary account number + exp date
- 37 use PAN + postcode (numeric digits only for some, add door number for others)
- 291 ask for PAN + expdate + CVV

Or just install a keylogger the old fashioned way

Optimal amount of fraud is non-zero

- US prioritised low friction
  - In Europe, they use 3D secure to verify payment
- Losses higher than any crime in FBI IC3 report
  - Investment fraud at ~$8bn
  - "society has decided by regulation (specifically, Regulation E) that that loss should flow to their financial institution"
- Absorbed by banks + credit card fees as cost of doing business

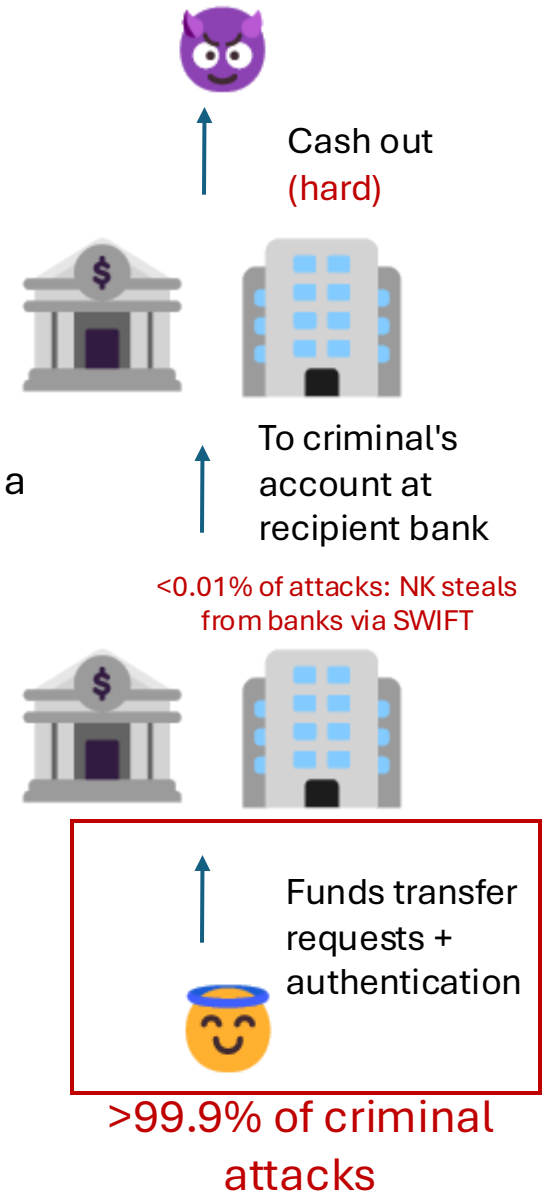


https://www.bitsaboutmoney.com/archive/optimal-amount-of-fraud/

How can a "hacker" steal from a bank?

1. **Money Creation**
   Violate Clark-Wilson integrity model and credit criminal's account without debiting another account
   - Hard thanks to MAC
   - No known examples, which would exploit implementation details
     - Lucky given this violates trust in the entire banking system
2. **Break authentication and impersonate the victim**
   Work within Clark-Wilson model and credit criminal's account by debiting victim's account via the criminal authenticating as the victim (or some delegated authority)
   - All kinds of attacks have been demonstrated here
     - Forging signature of a physical cheque
     - Getting access to victim's banking website account/app
     - Impersonating card, stealing/bypassing PIN, manipulating terminal
     - Compromise SWIFT to manipulate interbank transfers
   - Occasionally used by criminals at scale
3. **Socially engineer the victim**
   Work within Clark-Wilson model and socially engineer victim to credit criminal's account by debiting their own account, authenticating as themselves
   - Vast majority of cybercrime losses across investment fraud, business email compromise etc

Today's lecture



Modern defenses for customers

Vanguard

Name a trusted contact on your account

A trusted contact is a person Vanguard can reach out to if we ever have concerns about your physical or mental well-being or suspect you may be a victim of, or vulnerable to, **financial exploitation**. A trusted contact should be someone with integrity that you can rely on to provide unbiased information about your health, whereabouts, and well-being. **A trusted contact will not have access to your accounts unless you also designate them as an authorized agent. There is no cost associated with adding a trusted contact to your account, and it only takes two minutes.**

https://investor.vanguard.com/investor-resources-education/retirement/protect-your-finances-as-you-age

Starling Bank

What is a Connected card?

If someone's spending on your behalf at the moment, the Starling Connected card could make life a little easier for everyone.

From friends and family to a neighbour or childminder, it's an additional debit card you can give to anyone you trust, so they can buy whatever you need; no cash, contact, IOUs or fiddly bank details. The money comes out of a designated Space you'll set in the app (rather than your main account) and it's capped at £200, so you're always in control.

https://www.starlingbank.com/features/connected-shopping-card/