Closing the Phishing Hole – Fraud, Risk and Nonbanks

Ross Anderson

Cambridge University

Security Economics

- Many security failures are due to incentive failures rather than just technology
- Viruses now don’t attack the infected machine but use it to attack others
- Why is Microsoft software so insecure, despite market dominance?
- Electronic banking: UK banks were less liable for fraud, so we ended up suffering more of it

New View of Infosec

- Systems are often insecure because the people who could fix them have no incentive to
- Customers suffer when e-business can dump fraud risks that only they can practically control; everyone suffers when infected PCs spam you
- In IT markets, firms ship too little security when building market share, then add lots (of the wrong kind) to lock customers in
- Now 100+ researchers in security economics!
- What about the economics of financial crime?

Phishing

- Bank customer is lured to bogus website
- Money transferred from / via her account
- Losses last year: £35m UK, > $100m USA
- One gang (‘Rockphish’) does over half of it!
- Technical measures aren’t going to fix this soon
  - Banks train customers to click on links
  - IE toolbar was broken before it shipped
  - ‘Blame-and-train’ isn’t how you fix security usability
  - Least bad option may be 2-channel authorization for serious transactions

Studying the Phishermen

- Stolen money gets shipped through 2 or 3 hacked accounts, then turned into eGold
- People thought: because eGold doesn’t respond to warrants. But they do now
- It’s actually about transaction revocability!
- The typical bank recovers 60–95% of phished funds (the one that does only 60% gets hit for most of the losses)
- What’s the right regulatory response?

Back in the good old days…

- If someone did a wire fraud, or a check fraud, the money would be clawed back
- When I bought a car, I paid Lloyds £40 for a bank draft (cashier’s check) – to insure the dealer against the check bouncing later
- In business, you had acceptance of bills, factoring without recourse, LCs, …
- The risk of giving a customer an irrevocable instrument was recognized and priced

Money Laundering Controls

- Current focus is on the entry phase (the pizza parlours) rather than the layering phase in the middle or the exit phase
- We're beginning to realize this is inefficient (you want to catch the Don not the smurfs)
- Anything that allows bank credit to be turned into portable wealth will eventually be abused by the phishermen too!
- Tracing money and tracking people are not perfect substitutes…

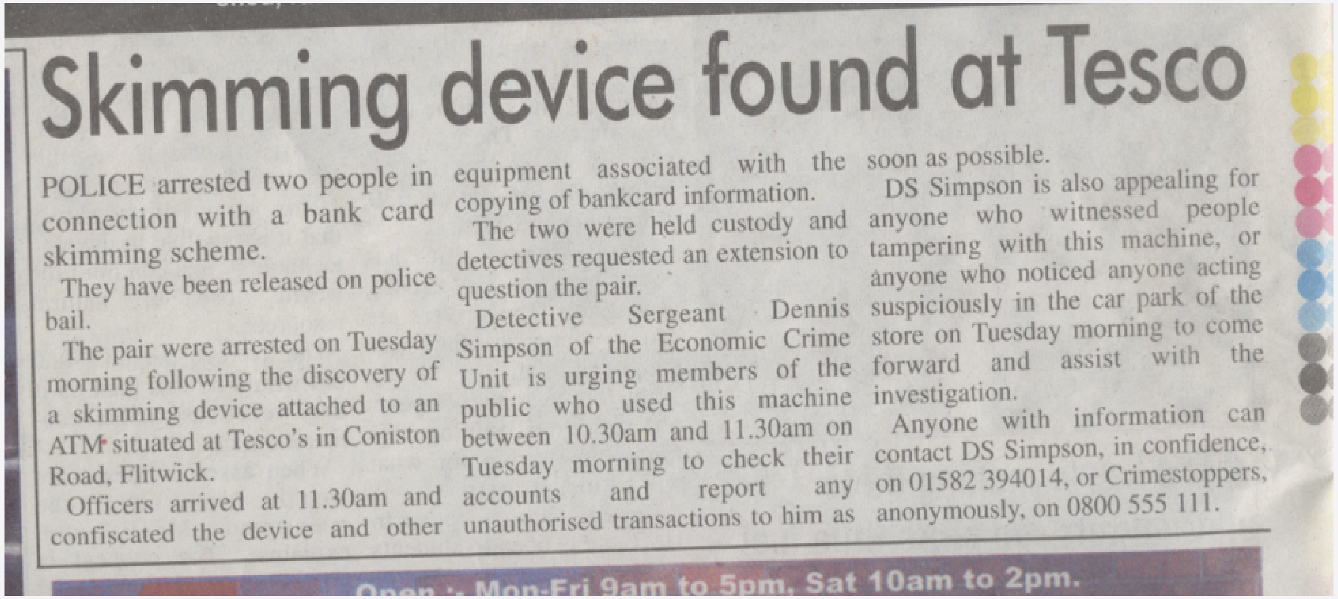
The Identity Circus

- Since 9/11, FATF etc have created huge costs for banks with address due diligence
- References were always better than collecting easily-forged copies of gas bills
- Effects too on women, poor, third world…
- Doesn’t help recover phished assets!
- Emphasis on ‘identity’ came at expense of transaction traceability and revocability
- This affected even hawala, hundi systems!

The Role of Customer Rights

- US banks: regulation E
- UK banks: ‘our systems are secure, and sue us if you disagree’. This dogma led to moral hazard, thus to higher fraud
- eGold: acts done with your password are your liability, and all transactions are irrevocable
- PayPal: we’ll adjudicate; sue us if you disagree, and pay our costs if you lose (as in England)
- EU PSD: banks can set dispute resolution procedures using their terms and conditions

In the absence of Reg E, breach reporting laws…



Skimming device found at Tesco

POLICE arrested two people in connection with a bank card skimming scheme.

They have been released on police bail.

The pair were arrested on Tuesday morning following the discovery of a skimming device attached to an ATM situated at Tesco's in Coniston Road, Flitwick.

Officers arrived at 11.30am and confiscated the device and other equipment associated with the copying of bankcard information.

The two were held custody and detectives requested an extension to question the pair.

Detective Sergeant Dennis Simpson of the Economic Crime Unit is urging members of the public who used this machine between 10.30am and 11.30am on Tuesday morning to check their accounts and report any unauthorised transactions to him as soon as possible.

DS Simpson is also appealing for anyone who witnessed people tampering with this machine, or anyone who noticed anyone acting suspiciously in the car park of the store on Tuesday morning to come forward and assist with the investigation.

Anyone with information can contact DS Simpson, in confidence, on 01582 394014, or Crimestoppers, anonymously, on 0800 555 111.

Observing PayPal

- PayPal has ended up doing many of the things this analysis suggests
  - payments are revocable for 180 days
  - you can’t take cash out in dodgy jurisdictions
  - they don’t collect millions of gas bills as CDD
  - Risk management more based on reputation systems than due diligence
  - and scale makes phishing detection easier
- But then, they’re a big phishing target

The problem – and solution

- There are places to get ‘free’ cashiers’ checks, and they’re attracting the villains
- eGold, Western Union, Finnish banks …
- Principled approach – any financial institution that sells an irrevocable instrument (including cash) for stolen funds should be liable
- Time limit – at least 90 days (PayPal is 180!)
- Nonbanks mustn’t be able to create a hole through which stolen / laundered funds vanish

The way forward

- Phishing, keyloggers, etc are here to stay
- As well as having a few big bent insiders, we’ll have many compromised accounts at any time
- We must move from ‘payment system integrity’ to ‘payment system resilience’
- We must keep counterparty risks (payment, fraud, legal, data-security) transparent, so the market can price them
- Thus: payments should be revocable by default
- This will benefit banks, and customers

More …

- Workshop on the Economics of Information Security: June 6–8, Carnegie-Mellon University, Pittsburgh
- Economics and Security Resource Page – www.cl.cam.ac.uk/~rja14/econsec.html (or follow link from www.ross-anderson.com/) which has survey papers, research papers, links to past conference proceedings