Ofcom's work on telecoms facilitated scams

Huw Saunders – Director of Network Infrastructure and Resilience

9 December 2020

Overview

- Our past work related to scams
- Nuisance calls and the connection to telecoms facilitated scams
- Current work
- Looking to the future

Ofcom's earlier work on scams

- Ofcom has no formal powers to deal with scams, other than under "persistent misuse" powers which are aimed at encouraging telcos to withdraw services from problematic end users and discourage identifiable bad practice.
- However we have historically conducted work in this space focussing on mitigating harms to consumers from malicious voice calls and SMS, which stretches back over more than 5 years.
- **Courier fraud**
  - Using the old PSTN "Called Party Held" (CPH) feature, the fraudster would keep the line open and play a dial tone after suggesting an identity confirming outbound call
  - We worked with UK telcos and their vendors to reduce the CPH period from two minutes to a few seconds.
- **SMS Smishing**
  - Ofcom encouraged the UK MNOs and the messaging eco-system to work together on putting together a registry of protected names to reduce the opportunity for "smishing" scams

Ofcom's continuing nuisance calls work

- Ofcom's nuisance calls work and its evolution to address scams:
  - Important work area for us for many years but Ofcom's main powers are limited to silent and abandoned calls only (ICO has lead on "robocalls")
  - Initial traffic growth around 5+ years ago fuelled by low call terminations rates and development of low cost VoIP automated calling platforms
  - Traffic was mainly marketing campaign driven for quasi legitimate purposes (list generation for financial service mis-selling etc)
  - Call volumes are estimated as being in range 5 to 10 billion per annum across UK fixed and mobile – some telcos have estimated that they may have constituted 25% of call attempts
  - Current strategy is to work with industry to block numbers at the network level as previous enforcement action was ineffective
  - Most UK mass market comms providers have implemented blocking solutions and we also liaise with call screening consumer app and device providers

Number spoofing and the growth of scams

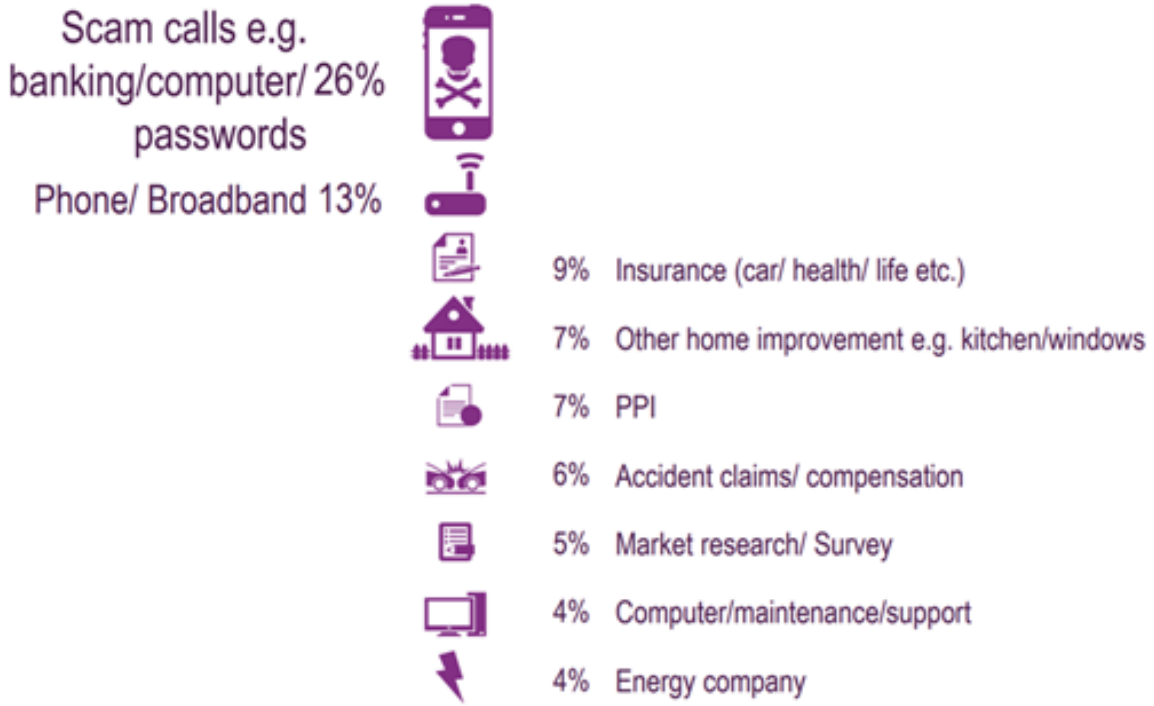
- First wave of nuisance calls in the UK tended to have missing or incomplete Caller Line Identity (CLI) to obfuscate who originated them and where they were, generally to make enforcement more difficult rather than to mislead the called party.
- Call blocking solutions are relatively easily configured to address such traffic
- Over time, calls using “spoofed” CLI have become increasingly common. In simple volumetric terms, spoofing is still mostly used for obfuscation rather than attempts to impersonate, using random but genuine numbers which are changed frequently, reducing the effectiveness of call blocking solutions
- However, more traffic is being seen where the intent is to use a spoofed CLI to facilitate fraud, often by trying to mislead the called party as to the identity of the caller
- Preventing CLI spoofing by adopting authentication techniques such as STIR offers only a longer term solution in the UK because of delays in mass market adoption of SIP
- Short term mitigations are our initial focus and we are continuing to work with industry on a collaborative basis on new approaches

Consumer feedback on scam related calls

In 2019, a quarter of calls where the product/service was identified were thought to be scams.

20

Most common products promoted by all nuisance calls, where product/ service was identified, 2019



NB: This was the participant's understanding of the product or service being promoted and may not reflect the actual reason for the call.

Scam mitigations

- **The Do Not Originate list**
  - Working with banks (via UK Finance), tax and government agencies and telecoms sector
  - Aim is to block numbers that these organisations will not originate calls from – typically those they use only for incoming calls from consumers/customers etc such as the "security" numbers found on the back of credit and debit cards
  - 12,000 numbers currently on the list that is regularly updated and shared with telcos
  - Not 100% effective, but covers a substantial amount of the mass market networks
  - HMRC, the UK tax authority reported in 2019 – ***"Since the controls were introduced in April this year, HMRC has reduced to zero the number of phone scams spoofing genuine inbound HMRC numbers. This has resulted in the tax authority already receiving 25% fewer scam reports against the previous month."***
- **Stop Scams UK**
  - Bringing banks and telcos together to stop scams at source under joint Ofcom and Financial Conduct Authority sponsorship
  - More updates in new year, but promising work so far.

Extending our work in collaboration with a wider range of stakeholders and partners

- Call blocking/filtering apps and devices
  - Hiya/TNS/First Orion/Google/Truecall
  - DNO list and broader collaboration
- Now also working collaboratively with the UK Home Office, Scottish Government and other public sector organisations such as Trading Standards on a cross sector approach addressing mitigation measures, consumer education, better enforcement and other initiatives
- Reviewing our current regulatory policy positioning with a view to determining whether we need more formal powers to help protect consumers, including being able to mandate particular actions from telcos
- Most obviously looking to encourage deployment of a STIR/SHAKN type CLI authentication solution for spoofing as soon as possible, but this is constrained by telcos technology refresh roadmaps, particularly with regard to PSTN switch-off and mass adoption of SIP based voice
- Shorter term focus on what is acceptable use of UK CLI – should international ingress traffic with UK CLI be blocked apart from roaming mobiles and some limited call centre uses?

Supporting and monitoring other regulatory and policy initiatives

- We have had an extensive long term outreach and collaboration programme with other regulators, both bilaterally and multilaterally through UCENET and other routes, to exchange information and best practice
- USA - FTC/FCC mandate from Congress has allowed regulatory imposition of measures such as the implementation of STIR/SHAKEN but this has taken much longer than anticipated and long tale of TDM small telco customers in danger of being left behind
- Australia - ACMA
  - blocking international traffic with an Australian CLI
  - Implementing their own version of our DNO list
- France – ARCEP mandating international originated traffic with a French CLI is blocked
- As STIR is introduced more widely, a key challenge is how certification approaches can be harmonised to allow cross border recognition
- Happy to work with GSMA and other agencies on this key issue

Thank you!