AdaptiveMobile Security

Analysis of Current & High Risk Financial Services SMS Phishing Attacks

Simeon Coney

Chief Strategy Officer

Increasing digital life on phones

- Financial institutions amongst many leveraging the benefit of continued connectivity of mobiles
- Brings many advantages in greater convenience, enhanced security & better awareness / education of financial position
- Significant investments made in protecting their own services and infrastructure
- However most customer interaction is done over mobile infrastructure that is not under the control of these institutions
- We are “trained” / conditioned to respond to alerts & notifications on our phone and this lowers our critical assessment

Mobile Devices & Networks are large & tempting attack surface

Stealing credentials
for account take-over
- Social Engineering: Spam, Spoofing, Impersonation, Phishing
- Redirection

Stealing information
to improve attack effectiveness
- Location tracking
- Hijacking

Recruiting unwitting devices / people
to target more victims
- Mobile Malware

Socially Engineered Mobile Messaging Banking Attacks

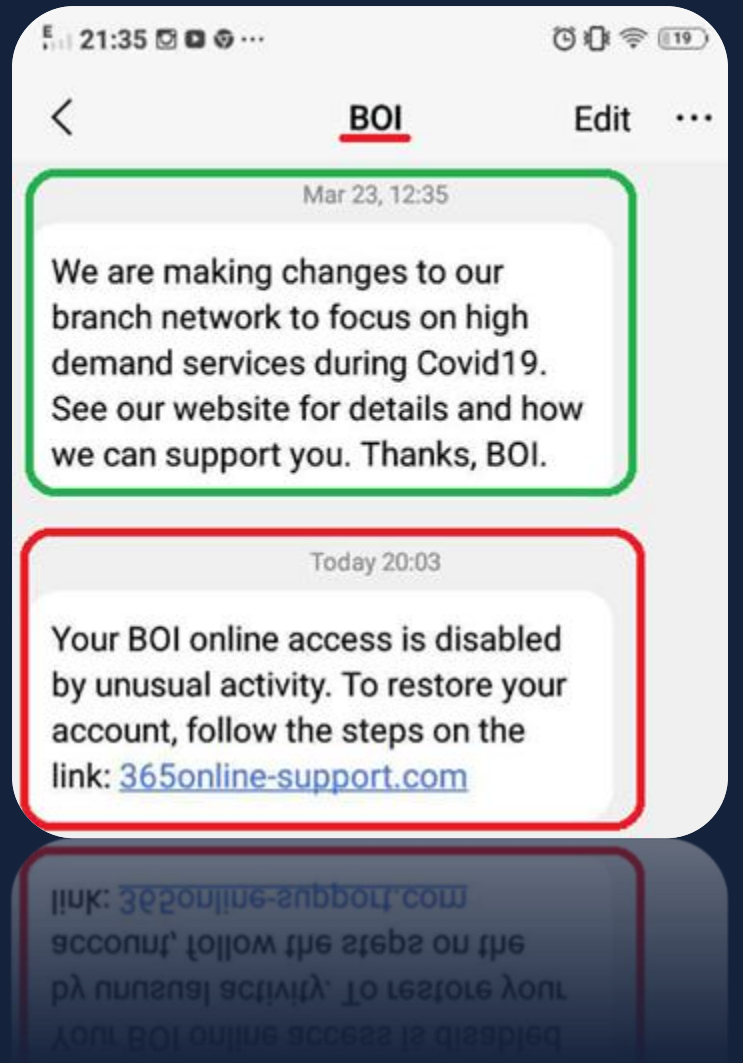
- A mobile number shows which country (or city) the potential victim is in (Email addresses don’t)
- Attackers can interrogate networks to confirm this exactly
- They use this information to launch targeted campaigns imitating banks’ real identities
- And time attacks during public holidays / times when banks’ helplines are closed
- And exploit users partial awareness of security risks
  e.g. Calling to alert of a “potential fraud”

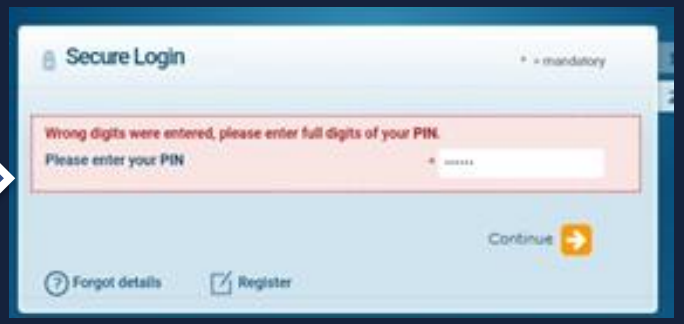
Technique: Sender Spoofing into your Inbox

- Phones group messages from the same sender together
- Attackers exploit this, to put their fake messages into the same group as legitimate messages
- Victims know first message was legitimate, so more likely to trust the new (fake) message

Legitimate

Fake



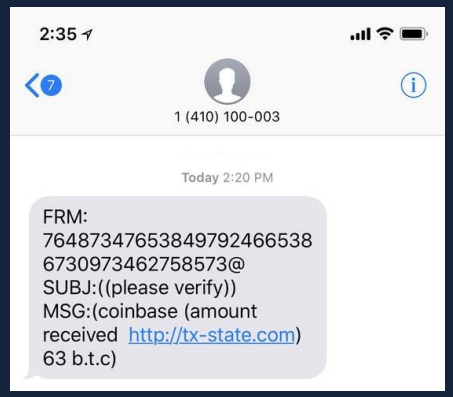


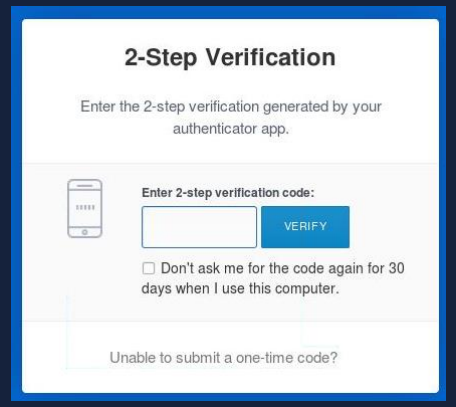
Attacker requests partial PIN

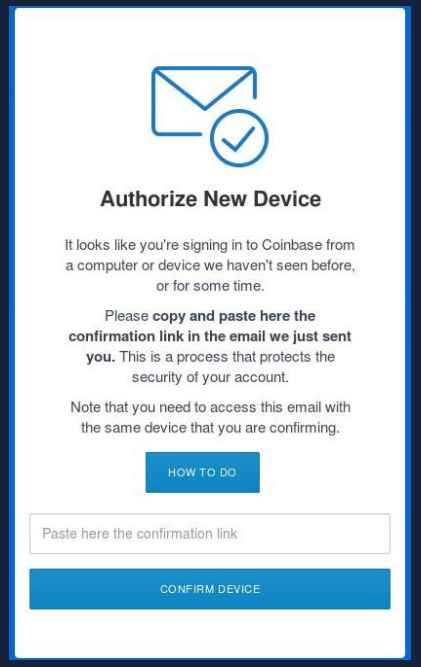
Attacker pretends PIN wrong & then requests full PIN

Cryptocurrencies are not immune

- Increasing popularity of cryptocurrencies has led to increase in cryptocurrency-based cybercrimes targeting mobile subscribers
- SMS phishing campaigns designed to gain access to users' accounts
  - SMS received by subscribers contained a malicious URL to the phishing page (volumes shown in the figure)
  - 2FA information required for account access requested and passed to a remote session initialised automatically by the malicious actors to siphon Bitcoin or Litecoin from the account





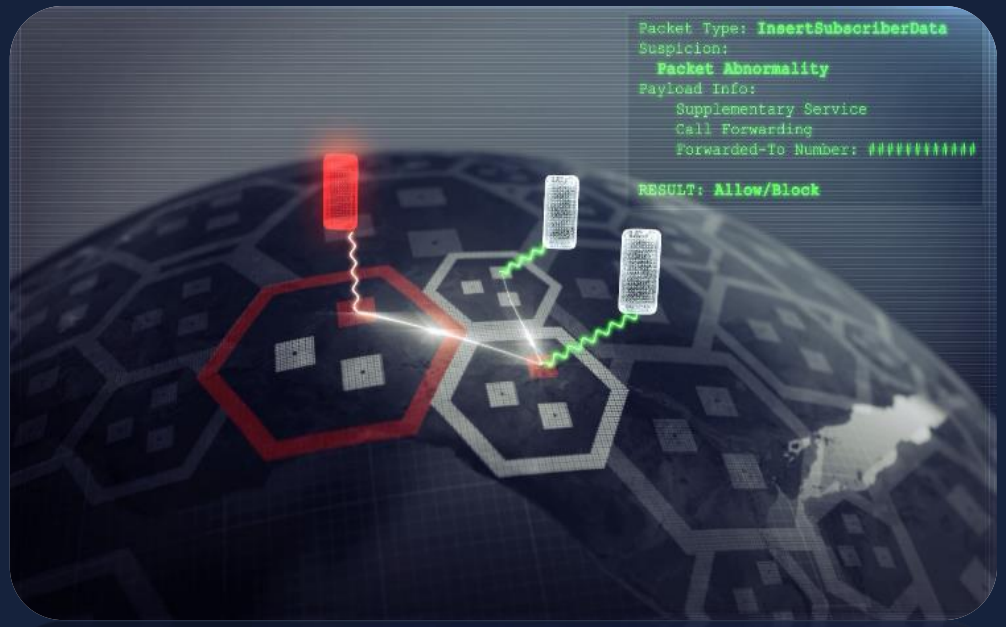


Full blog details available at:
https://www.adaptivemobile.com/blog/cryptocurrency-scam-cybercrime

Mobile Networks Implement Signalling Firewalls to Assure 2FA

Attackers can exploit Mobile Operator who have no SS7 Signalling defences:

- Automatic interception of 2FA / mTAN SMS
- Temporary Call Forwarding set for 2FA Flash Calls / Call-Back Validation



Why are mobile networks vulnerable?

Mobile networks interconnected via protocols defined decades ago

- Lack of End-to-End Authentication, as all considered to be trusted
- Once access is gained at one level,
  connectivity to any node addressed by GT is possible
- Mobile “applications” do not validate originating point of incoming requests
- New standards are based upon the same principles as these legacy protocols

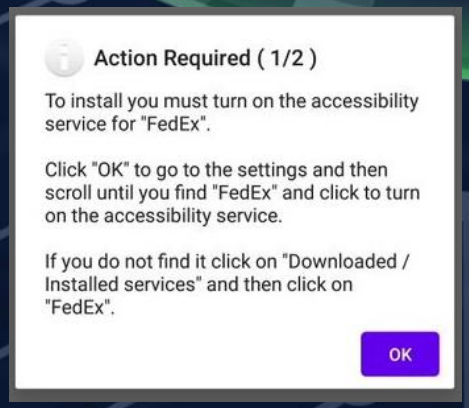
Mobile Malware recruited into the battle

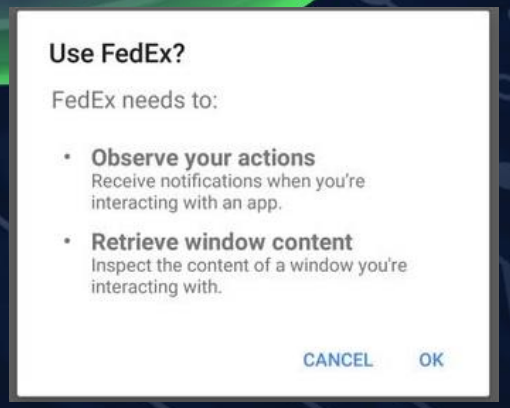
Malware used to:

- Steal passwords
- Steal credit card numbers
- Steal banking credentials
- Distribute messages to more victims

Current wave of Flubot gaining details from victims

Some victims receiving Social Engineering scam calls several days later





Improving Security

Mobile Networks can protect themselves

Messaging Firewalls prevent:

- Spam
- Scams
- Phishing
- Malware spread

Signalling Firewalls prevent:

- Location interrogation
- Call / Message interception
- Call / Message redirection

Users can take steps to protect:

- Don’t respond, reply or click on anything that looks suspicious
- If in doubt, hang up, and call back on a number you trust (from an alternative device if possible)
- Challenge anyone who calls, to first prove whom they are

Thank You!

AdaptiveMobile
Security