Australian
Cyber Conference
2021

Daryl Sheppard

possibilities

AISA

# Cyber Security and the Three Card Monte Con
## How old scams are new again and what to do about it

# Topics

- How we got here
- Why is it a problem
- Old cons new tricks
- What we can do about it

# How we got here (1)

- Pre 1960s
  - Computers protected by physical measures
  - Guards, gates and guns
  - Limit number of given users
  - Business functions important but generally not critical
  - Security awareness training provided to users

# How we got here (2)

- 1970s to mid 1980s
  - Computers start to have basic forms of connectivity
  - Non-physical security mechanisms started to develop
  - User population began to expand
  - Business functions becoming more critical
  - Security awareness training provided to users

# How we got here (3)

- Mid 1980s to present
  - Massive rise in interconnectivity
  - Massive rise in number of users
  - Business functions essential and often without manual alternatives
  - IT Security industry starts to take shape and grows in both software and hardware
  - Security awareness training provided to users

# Why is it a problem (1)

- In October 2016, the FriendFinder Network. Initially 3.5 million account details reported breached. Full figure could include up to 412 million
- In 2016, ride share service Uber. Disclosure of personal information of 57 million users and 600,000 drivers
- In 2017, Equifax. 143 million consumer records, 209,000 credit card numbers and personal information
- In 2017, Yahoo. 3 billion user account credentials breached over a period of years
- In 2018, Marriott International. Loss of 500 million customer details between 2014 and 2018
- In 2020, Likud political party in Israel. Details of every eligible voter exposed.
- And many more…

# Why is it a problem (2)

- All major businesses
- All likely formal IT support arrangements with security capabilities
- The risk of data breaches are not really a secret
- Many factors involved

# The Cons

- Basic principles
- Applied to a real-world hustle
- Implications for cyber
- Do not try this at home!

# Three Card Monte

- Three cards
- Operator manipulates the cards
- Select the right card and you win select the wrong card and you loose

# Three Card Monte

- Simple odds? Where is the scam?
- Street theatre
- Performer and several shills
- Shills demonstrate that the game is 'fair'
- Operator draws in the mark
- Shills may also be primed to pickpocket the mark

# Principle #1 The Distraction Principle

*While you are distracted by what retains your interest, hustlers can do anything to you, and you won't notice*

- A basic principle of many different hustles
- Look the other way
- From a cyber security perspective
  - Balance between usability and security
  - Users generally want to follow the rules, but are distracted
  - Distractions can be work, time or a combination

# Principle #2 The Herd Principle

*Even suspicious marks will let their guard down when everyone next to them appears to share the same risks*

- Three card monte relies on shills to encourage the mark into the operator's trap
- Theory is safety in numbers – not the case when they are all conspiring against you
- From a cyber security perspective
  - The herd can easily be created with social media ‘sock puppets’ and astro turfing
  - Can be used to enhance the reputation of any online service/organisation

# Counterfeit Pen Con

- The operator poses as a police officer and enters a shop
- Advises shop keeper that counterfeit money is being passed around locally
- Gives the shop keeper a fake counterfeit detection pen to use on any notes they receive in the shop
- The concept of the pen is (or was at the time) real, however the pen the operator gave the shop keeper is fake
- The operator then alerts accomplices that the shop can now safely receive counterfeit money

FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
L 89823401 J
WASHINGTON, D.C.
ONE DOLLAR

# Principle #3 The Social Compliance Principle

*Society trains people not to question authority. Hustlers exploit this “suspension of suspiciousness” to make you do what they want*

- Shop keeper happily accepts the fake pen provided to him by the operator poses as ‘authority’
- Wouldn’t work with a stranger but would work if that stranger fits within an already established authority structure
- From a cyber security perspective
  - Training users to obey certain people without question is a double edge sword
  - Those in authority need to establish safeguards for users

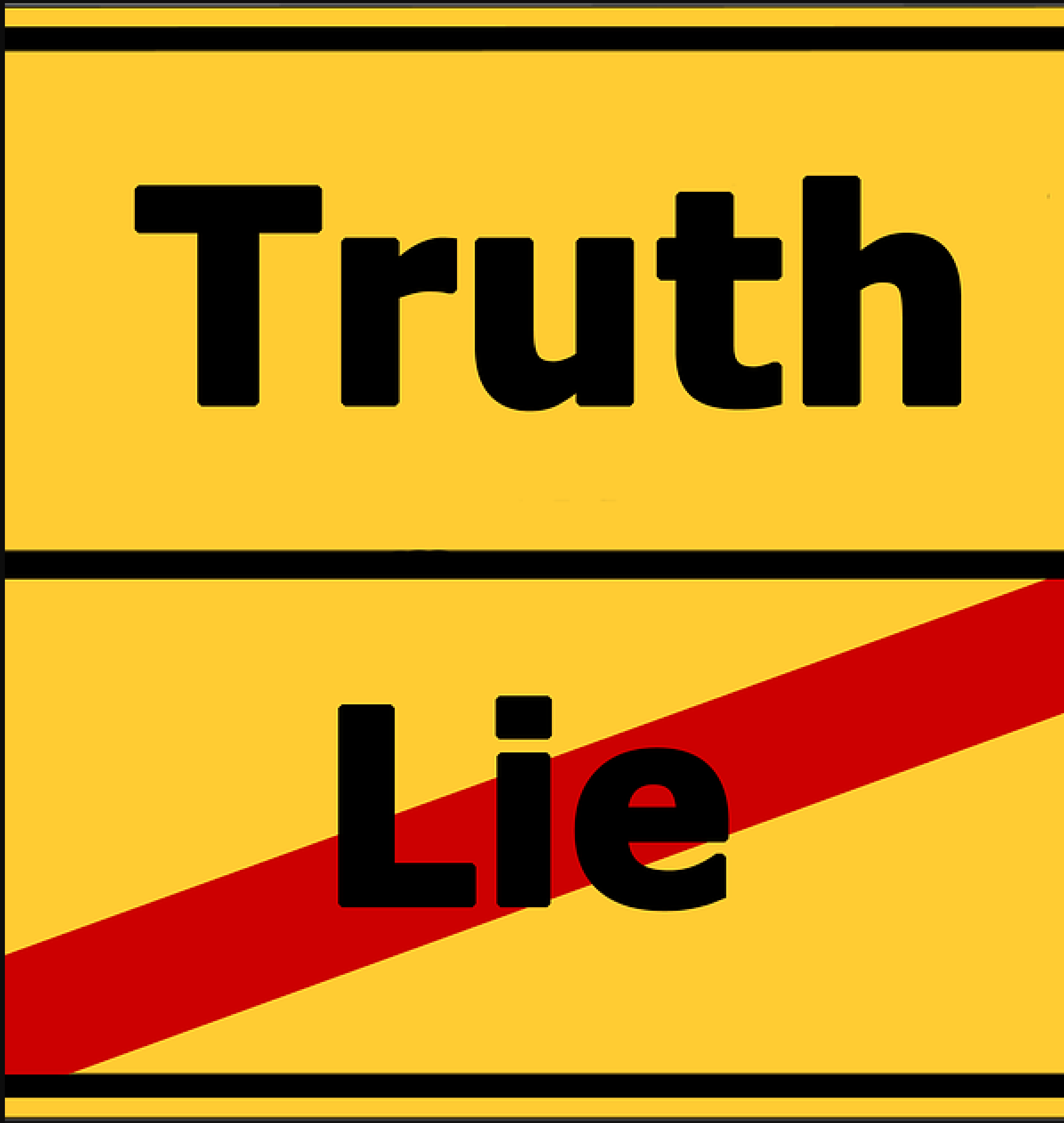
# Gadget Scam

- The operators sell a homemade electronic device meant to recharge transport cards to the value of $100
- The device is just a box with some flashing lights
- The operator convinces the mark by demonstrating it on their card
- The operator uses slight of hand to swap out the marks card with one that is already loaded with cash
- The operator charges the mark $300 for the device

# Principle #4 The Dishonesty Principle

*Anything illegal you do will be used against you by the fraudster, making it harder for you to seek help once you realise you've been had*

- The mark purchased the device which had it worked would obviously have been illegal
- Difficult to complain to police about such a device
- From a cyber security perspective
    - A core component of Nigerian scam or other money mule scams
    - Several attacks on systems will go unreported
    - Few corporate users will report the trojan entered their computer due to an offer of free porn!
    - Balance between righteousness and security needs to be struck
    - Policy guaranteeing amnesty if the user cooperates with the investigation



# Cash Machine Con

- The operators set up a rudimentary stand-alone ATM and deploy it on a busy street
- The cash machine has the front of a real ATM but contains a human operator with a laptop and a magstripe reader
- When a mark inserts the card, the operator takes it and obtains the data using the magstripe reader
- The mark enters the PIN number into ATM machine allowing the operator to obtain it
- This provides both the magstripe data which can be cloned onto another card and the necessary PIN number
- The ATM machine then returns the card to the user and displays an ‘Out of Service Message’

Statement
Receipt
NCR
Sorry, this machine is temporarily out of service
Insert Card
Audio Jack
For customer assistance, or to report problems with this ATM, please call 800.432.1000.
Insert Cash
Insert Check
Cash
No envelope. Making deposits has never been easier.

# Principle #5 The Deception Principle

*Things and people are not what they seem. Hustlers know how to manipulate you to make you believe that they are*

- Cash machine con is risky but a big reward
- People believe they can protect themselves, but against a determined and resourced adversary…..
- From a cyber security perspective
    - Do average users understand what the padlock on a website means?
    - Authenticate for everyone not just the technical

# Ring Reward Rip-Off (1)

- Ring Reward Rip-Off
- The operator purchases a cheap ring and then goes to a pub
- At the pub, the operator strikes up a conversation about the ring with the bartender and casually indicates that it is worth thousands of dollars
- The operator leaves and then an accomplice enters the pub for a drink
- The operator calls the pub and indicates that she lost the ring and asks the bartender to look for it

# Ring Reward Rip-Off (2)

- The accomplice tells the bartender that he found the ring and asks ‘what is in it for me?’
- The operator talks to the mark who tells the bartender she will pay $200 reward
- The bartender wanting to make some profit for himself tells the accomplice that a $20 reward is offered
- The accomplice haggles with the bartender to get as higher price as possible but below the $200 mark
- The bartender pays the accomplice for the ring who then pockets the money and walks out
- The operator never comes to collect the cheap ring

# Principle #6 The Need and Greed Principle

*Your needs and desires make you vulnerable. Once hustlers know what you really want, they can easily manipulate you*

- This is a complicate one
- Requiring some significant social engineering skills
- Appeals to a base instinct of an individual
- May not always work
- From a cyber security perspective
  - You need to understand what your users want and what drives them
  - Personnel vetting
  - Design systems to protect users from temptation

# Principle #7 The Time Principle

*When you are under time pressure to make an important choice, you use a different decision strategy. Hustlers steer you towards a strategy involving less reasoning*

- The mark is forced to act quickly or lose the opportunity
- Time pressure can shift decision making from reasoned to an affect-dominated strategy
- From a cyber security perspective
  - Identify situations where an attacker can impact a users decision making strategy
  - Devise a protocol that will guide the human decision making component of the system to the correct decision strategy

# What we can do about it

- Understand your users
- Understand your business
- Go beyond the risk assessment
- Don’t always look for a technical solution
- Modify your system design practices accordingly
- Innovate with your security awareness training

# Questions?