Red Teaming

Simulating Social Engineering Threats

Chong Rong Hwa & Terence Teo
GovTech Red Team
August 2018

Presentation Outline

1. Who Are We?

2. Adversary Simulation

3. Cybersecurity in Healthcare

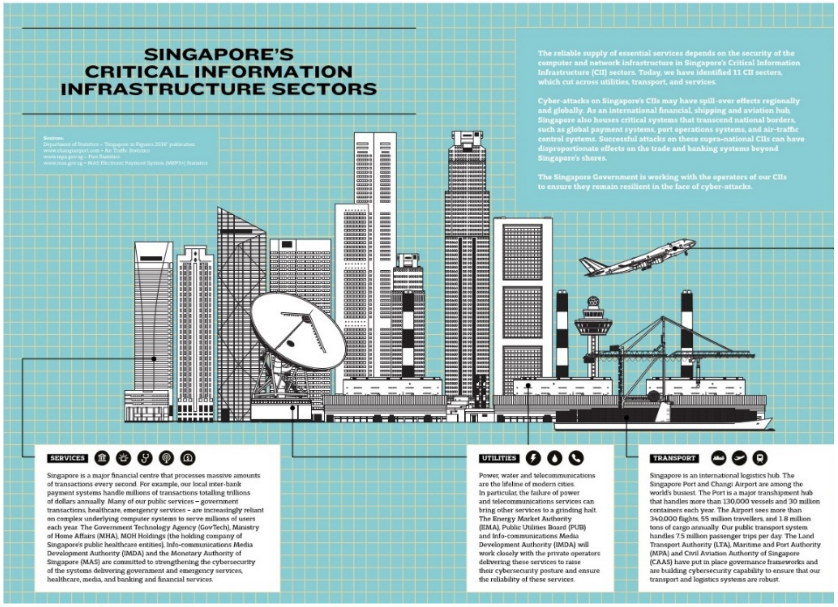
1. Social Engineering – A Relevant Threat

2. Key Takeaways

#WHOAREWE

GovTech Red Team

Critical Information Infrastructure – Government Sector Lead



SINGAPORE'S CRITICAL INFORMATION INFRASTRUCTURE SECTORS

The reliable supply of essential services depends on the security of the computer and network infrastructure in Singapore's Critical Information Infrastructure (CII) sectors. Today, we have identified 11 CII sectors, which cut across utilities, transport, and services.

Cyber-attacks on Singapore's CIIs may have spill-over effects regionally and globally. As an international financial, shipping and aviation hub, Singapore also houses critical systems that transcend national borders, such as global payment systems, port operations systems, and air-traffic control systems. Successful attacks on these supra-national CIIs can have disproportionate effects on the trade and banking systems beyond Singapore's shores.

The Singapore Government is working with the operators of our CIIs to ensure they remain resilient in the face of cyber-attacks.

Sources:
Department of Statistics – 'Singapore in Figures 2016' publication
www.changiairport.com – Air Traffic Statistics
www.mpa.gov.sg – Port Statistics
www.mas.gov.sg – MAS Electronic Payment System (MEPS+) Statistics

SERVICES

Singapore is a major financial centre that processes massive amounts of transactions every second. For example, our local inter-bank payment systems handle millions of transactions totalling trillions of dollars annually. Many of our public services – government transactions, healthcare, emergency services – are increasingly reliant on complex underlying computer systems to serve millions of users each year. The Government Technology Agency (GovTech), Ministry of Home Affairs (MHA), MOH Holdings (the holding company of Singapore's public healthcare entities), Info-communications Media Development Authority (IMDA) and the Monetary Authority of Singapore (MAS) are committed to strengthening the cybersecurity of the systems delivering government and emergency services, healthcare, media, and banking and financial services.

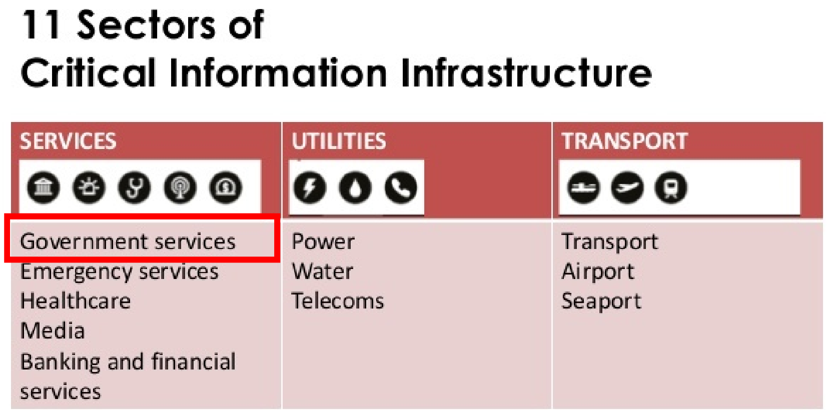
UTILITIES

Power, water and telecommunications are the lifeline of modern cities. In particular, the failure of power and telecommunications services can bring other services to a grinding halt. The Energy Market Authority (EMA), Public Utilities Board (PUB) and Info-communications Media Development Authority (IMDA) will work closely with the private operators delivering these services to raise their cybersecurity posture and ensure the reliability of these services.

TRANSPORT

Singapore is an international logistics hub. The Singapore Port and Changi Airport are among the world's busiest. The Port is a major transhipment hub that handles more than 130,000 vessels and 30 million containers each year. The Airport sees more than 340,000 flights, 55 million travellers, and 1.8 million tons of cargo annually. Our public transport system handles 7.5 million passenger trips per day. The Land Transport Authority (LTA), Maritime and Port Authority (MPA) and Civil Aviation Authority of Singapore (CAAS) have put in place governance frameworks and are building cybersecurity capability to ensure that our transport and logistics systems are robust.

Image source: Cyber Security Agency of Singapore



11 Sectors of Critical Information Infrastructure

SERVICES	UTILITIES	TRANSPORT
Government services Emergency services Healthcare Media Banking and financial services	Power Water Telecoms	Transport Airport Seaport

Image source: Benjamin Ang, Centre of Excellence for National Security

Hard Cybersecurity Problems

Social Engineering Attacks

- Phishing emails to deliver malware
- Social engineer through social media and messaging applications

Supply-chain Attack

- Trusted hardware and trusted software vendors
- Internet facing that interacts with business partner’s portals that do not have end-to-end integrity protection.

Shadow IT & Weak Hosting Sites

- Unmanaged IT Systems
- Projects hosted on insecure vendor’s hosting site

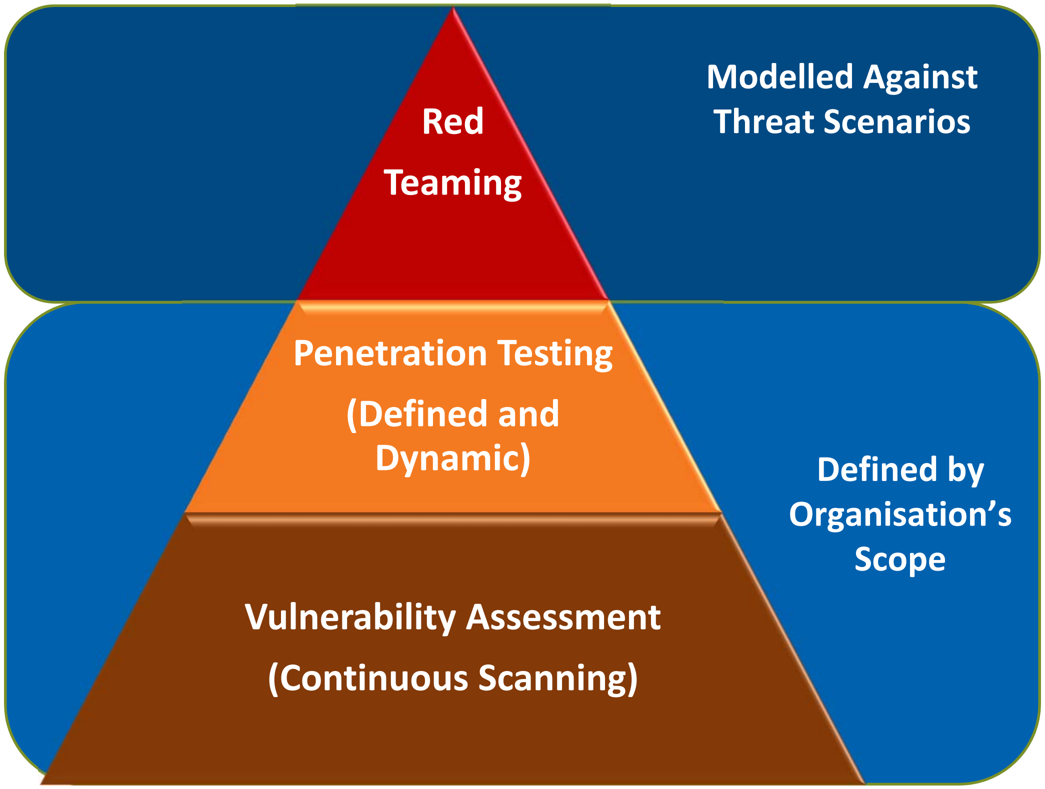
GOVTECH SINGAPORE

Adversary Simulation

Holistic Security Testing Approach

- Important to test IT environment (People, Process & Technology)

- Incorporate 3 tiers into System Development Life Cycle (SDLC):
  - Secure configuration review & Vulnerability Assessment
  - Penetration Testing
  - Adversary Simulation


Red Teaming
Modelled Against Threat Scenarios
Penetration Testing (Defined and Dynamic)
Defined by Organisation's Scope
Vulnerability Assessment (Continuous Scanning)

VAPT vs Red-teaming (Adversary Simulation)

Why Adversary Simulation?

Vulnerability Assessment Penetration Testing (VAPT) is an **asset-centric security test**, where the testers would focus on testing the security of the IT system, e.g. Web Application & S/W, that contains the data.

IT System – Safe
Data – Gold Bar

VAPT Analogy

Testers would validate the security of the safe to ensure that it could not be opened without secret and key.

Adversary Simulation (AS) is an **adversarial-goal centric security test**, where the testers would test the IT environment, including PPT, with the goal of identifying the weakness that might lead to access of data.

E.g. Lack of IT administration process, insecure administrative laptop and etc.

IT Environment – Bank
(People, Process & Tech)

AS Analogy

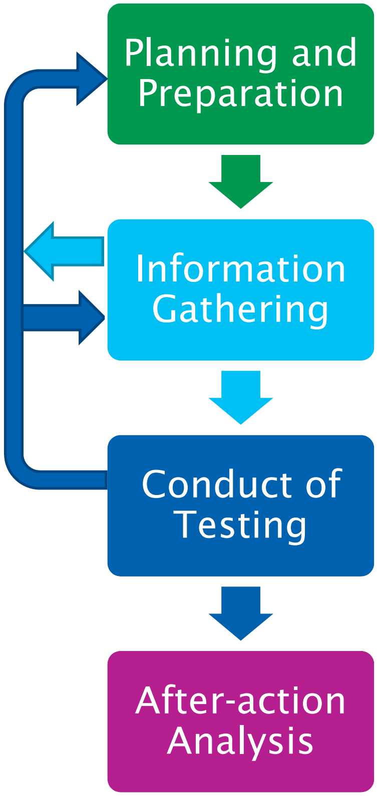
Testers would simulate an attacker to steal the gold bars (in the safe) that is located inside the bank.

The attacker would probably need to bypass the security operations and do things like:

- Social engineer the authorized personnel
- Break through the windows
- Compromise the security IT systems

Adversary Simulation

Methodology & Simulated Attackers



Planning and Preparation

- Preparation of attacker's server
- Coding and testing of tools
- Research in technology

Information Gathering

- Attack surface exploration
- Network discovery
- Social engineering

Conduct of Testing

- People
- Process
- Technology

After-action Analysis

- Root cause analysis
- Propose mitigation
- Advise security consultant

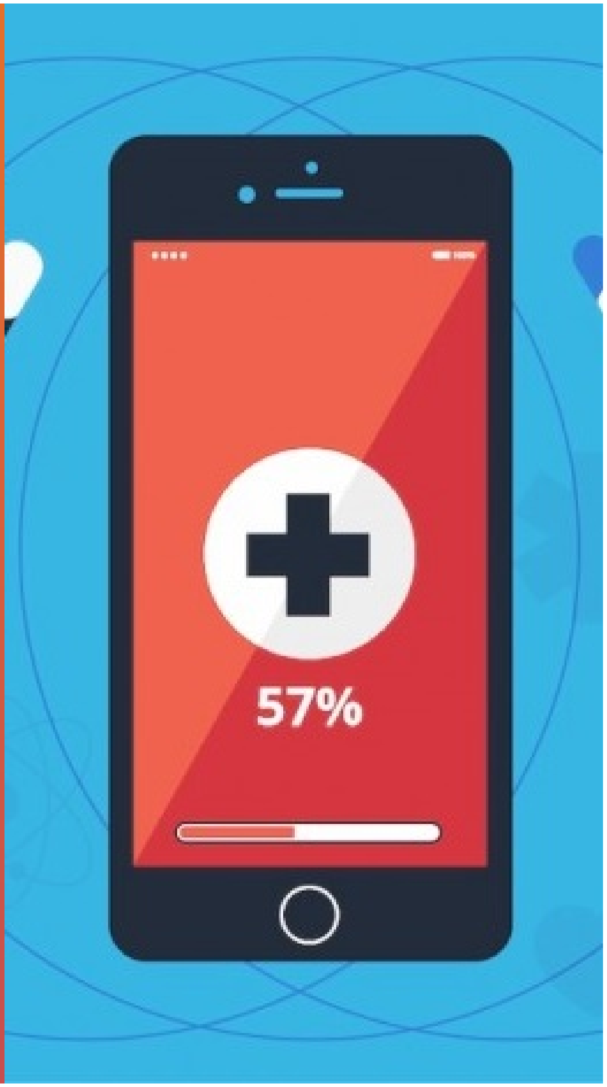
Sophisticated threat actor

An attacker with skills and abilities above run-of-the-mill hackers, however, not as resourceful as state-sponsored threat actors who are equipped with unknown hacking tools, tactics and procedures.

Malicious insider

An attacker who is a person within the organization, such as an employee, former employee, contractor or business associate, who abuses their access to data and systems, to conduct malicious acts.

Cybersecurity in Healthcare

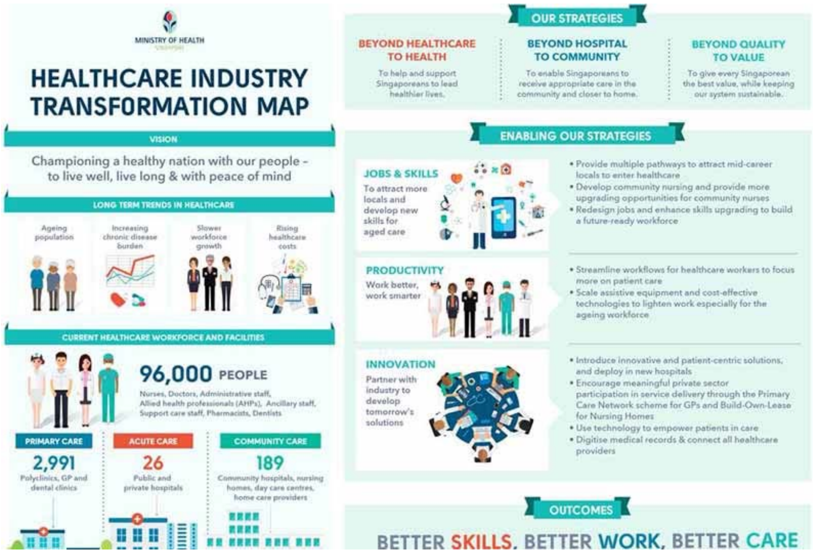


Digital Transformation of Healthcare

Private health sector urged to digitise records

Image source: Straits Times

Singapore Govt may start using drones to deliver medicine and for security



MINISTRY OF HEALTH

HEALTHCARE INDUSTRY TRANSFORMATION MAP

VISION

Championing a healthy nation with our people - to live well, live long & with peace of mind

LONG TERM TRENDS IN HEALTHCARE

Ageing population

Increasing chronic disease burden

Slower workforce growth

Rising healthcare costs

CURRENT HEALTHCARE WORKFORCE AND FACILITIES

96,000 PEOPLE

Nurses, Doctors, Administrative staff, Allied health professionals (AHPs), Ancillary staff, Support care staff, Pharmacists, Dentists

PRIMARY CARE	ACUTE CARE	COMMUNITY CARE
2,991	26	189
Polyclinics, GP and dental clinics	Public and private hospitals	Community hospitals, nursing homes, day care centres, home care providers

OUR STRATEGIES

BEYOND HEALTHCARE TO HEALTH	BEYOND HOSPITAL TO COMMUNITY	BEYOND QUALITY TO VALUE
To help and support Singaporeans to lead healthier lives.	To enable Singaporeans to receive appropriate care in the community and closer to home.	To give every Singaporean the best value, while keeping our system sustainable.

ENABLING OUR STRATEGIES

JOBS & SKILLS
To attract more locals and develop new skills for aged care

- Provide multiple pathways to attract mid-career locals to enter healthcare
- Develop community nursing and provide more upgrading opportunities for community nurses
- Redesign jobs and enhance skills upgrading to build a future-ready workforce

PRODUCTIVITY
Work better, work smarter

- Streamline workflows for healthcare workers to focus more on patient care
- Scale assistive equipment and cost-effective technologies to lighten work especially for the ageing workforce

INNOVATION
Partner with industry to develop tomorrow's solutions

- Introduce innovative and patient-centric solutions, and deploy in new hospitals
- Encourage meaningful private sector participation in service delivery through the Primary Care Network scheme for GPs and Build-Own-Lease for Nursing Homes
- Use technology to empower patients in care
- Digitise medical records & connect all healthcare providers

OUTCOMES

BETTER SKILLS, BETTER WORK, BETTER CARE

Image source: Opengovasia

GOVTECH SINGAPORE

Cyberattacks in Healthcare

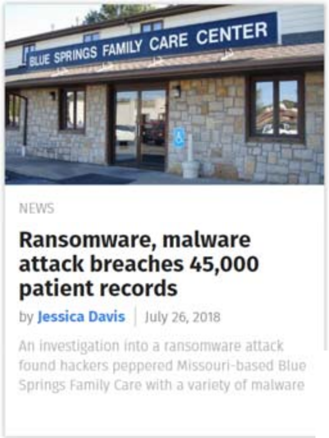
Cyberattacks in healthcare put human lives at risk
Patients could be harmed, even fatally
Health or business services could be interrupted
Protected health data could be lost
Lost trust in connected devices

Image source: GovTech Singapore

- Ranks among the top five industries most targeted by cyberattacks
- Puts not only patient data but also human lives at risk
- Become part of the organizational culture in both healthcare providers and medtech companies
- Governments can help by enacting industry-wide standards for cybersecurity in healthcare

Healthcare Data Breaches

Healthcare Data Breaches

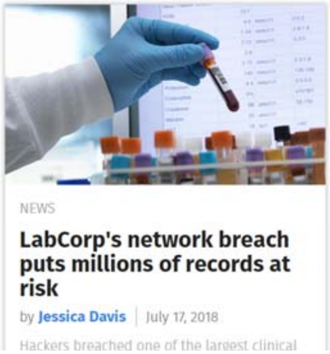


NEWS

Ransomware, malware attack breaches 45,000 patient records

by Jessica Davis | July 26, 2018

An investigation into a ransomware attack found hackers peppered Missouri-based Blue Springs Family Care with a variety of malware

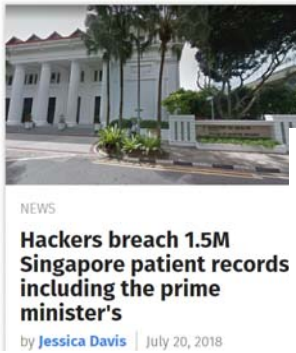


NEWS

LabCorp's network breach puts millions of records at risk

by Jessica Davis | July 17, 2018

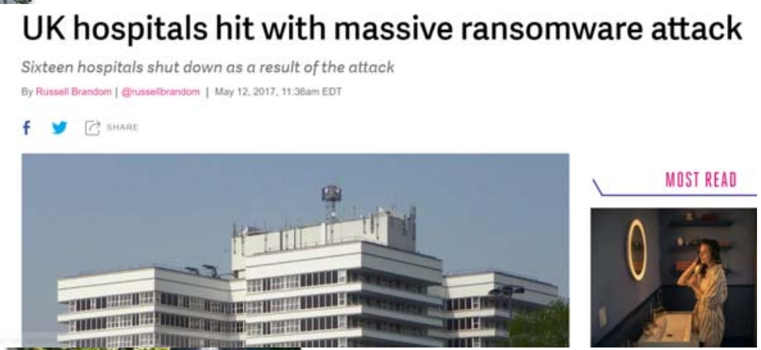
Hackers breached one of the largest clinical



NEWS

Hackers breach 1.5M Singapore patient records including the prime minister's

by Jessica Davis | July 20, 2018



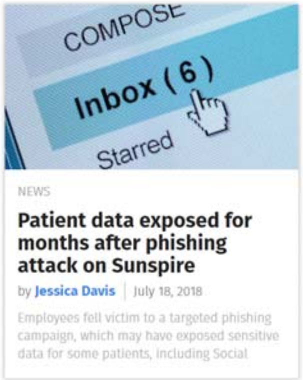
UK hospitals hit with massive ransomware attack

Sixteen hospitals shut down as a result of the attack

By Russell Brandom | @russellbrandom | May 12, 2017, 11:36am EDT

SHARE

Image sources: Healthcare IT News

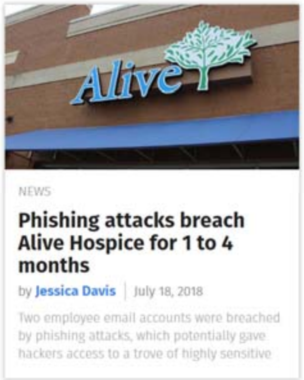


NEWS

Patient data exposed for months after phishing attack on Sunspire

by Jessica Davis | July 18, 2018

Employees fell victim to a targeted phishing campaign, which may have exposed sensitive data for some patients, including Social

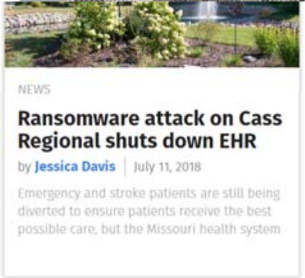


NEWS

Phishing attacks breach Alive Hospice for 1 to 4 months

by Jessica Davis | July 18, 2018

Two employee email accounts were breached by phishing attacks, which potentially gave hackers access to a trove of highly sensitive



NEWS

Ransomware attack on Cass Regional shuts down EHR

by Jessica Davis | July 11, 2018

Emergency and stroke patients are still being diverted to ensure patients receive the best possible care, but the Missouri health system

Image source: The Verge

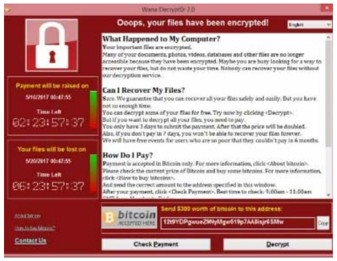
Timeline of Key HealthCare Cybersecurity Incidents

January 2015

Anthem Blue Cross (7.8million)

"These emails and calls are not from anthem and no notifications have been sent from anthem since the initial notification on Feb. 4, 2015".

Anthem Inc. Data Breach



Ooops, your files have been encrypted!

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

WannaCry Ransomware

May 2017

July 2018

SingHealth Data Breach (1.5million)

Social Engineering – A Relevant Threat

Exploiting the weakest link – Us Humans

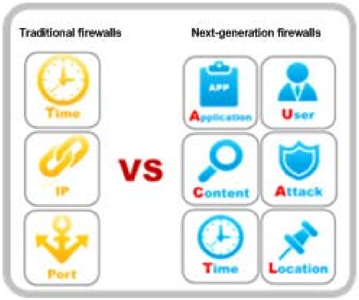
What is social engineering?

The use of **psychological manipulation** of people into **performing actions** or **divulging confidential information**.

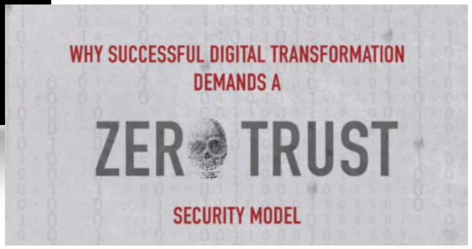
Image sources: Network Access (https://www.networkaccess.com/cyber-criminals-use-social-engineering-hack-businesses/)

Why social engineer?

- Why social engineer?



Because There Is No Patch To Human Stupidity



WHY SUCCESSFUL DIGITAL TRANSFORMATION DEMANDS A

ZER☠ TRUST

SECURITY MODEL

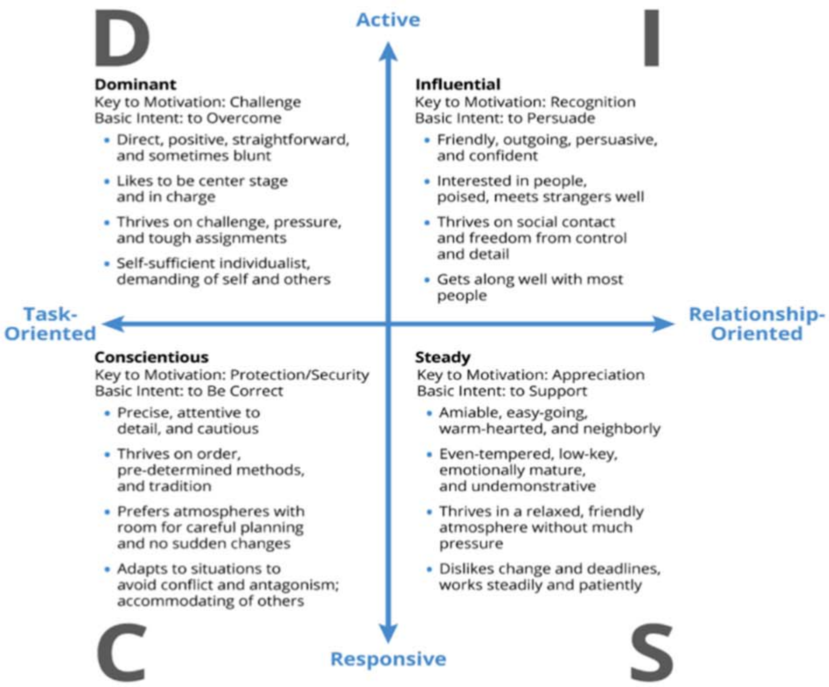
Identification & Authentication System
An autonomous system managing user access to a vehicle, his identification and authentication based on Blockchain technology and cryptographic module for certificates.
+ BLOCKCHAIN
infopulse
remme

Exploiting TRUST

Trust – Closely linked with benevolence, which leads to trust, resulting in information leakage and compromise of system

Exploiting DISC

DISC – Observable human behaviors (4 key traits)



Dominant
Key to Motivation: Challenge
Basic Intent: to Overcome

- Direct, positive, straightforward, and sometimes blunt
- Likes to be center stage and in charge
- Thrives on challenge, pressure, and tough assignments
- Self-sufficient individualist, demanding of self and others

Influential
Key to Motivation: Recognition
Basic Intent: to Persuade

- Friendly, outgoing, persuasive, and confident
- Interested in people, poised, meets strangers well
- Thrives on social contact and freedom from control and detail
- Gets along well with most people

Conscientious
Key to Motivation: Protection/Security
Basic Intent: to Be Correct

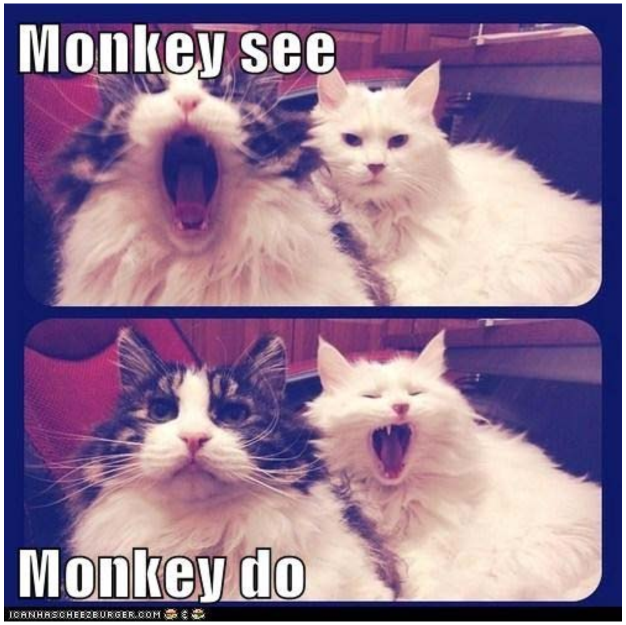
- Precise, attentive to detail, and cautious
- Thrives on order, pre-determined methods, and tradition
- Prefers atmospheres with room for careful planning and no sudden changes
- Adapts to situations to avoid conflict and antagonism; accommodating of others

Steady
Key to Motivation: Appreciation
Basic Intent: to Support

- Amiable, easy-going, warm-hearted, and neighborly
- Even-tempered, low-key, emotionally mature, and undemonstrative
- Thrives in a relaxed, friendly atmosphere without much pressure
- Dislikes change and deadlines, works steadily and patiently

Exploiting HERD MENTALITY

Herd mentality – Influence



[redacted]

The Big Four

Social Engineer's Playbook

1. Who am I?

2. What do I have to offer?

3. How long do I need?

4. Am I a threat?

Exploiting Trust

- Sympathy

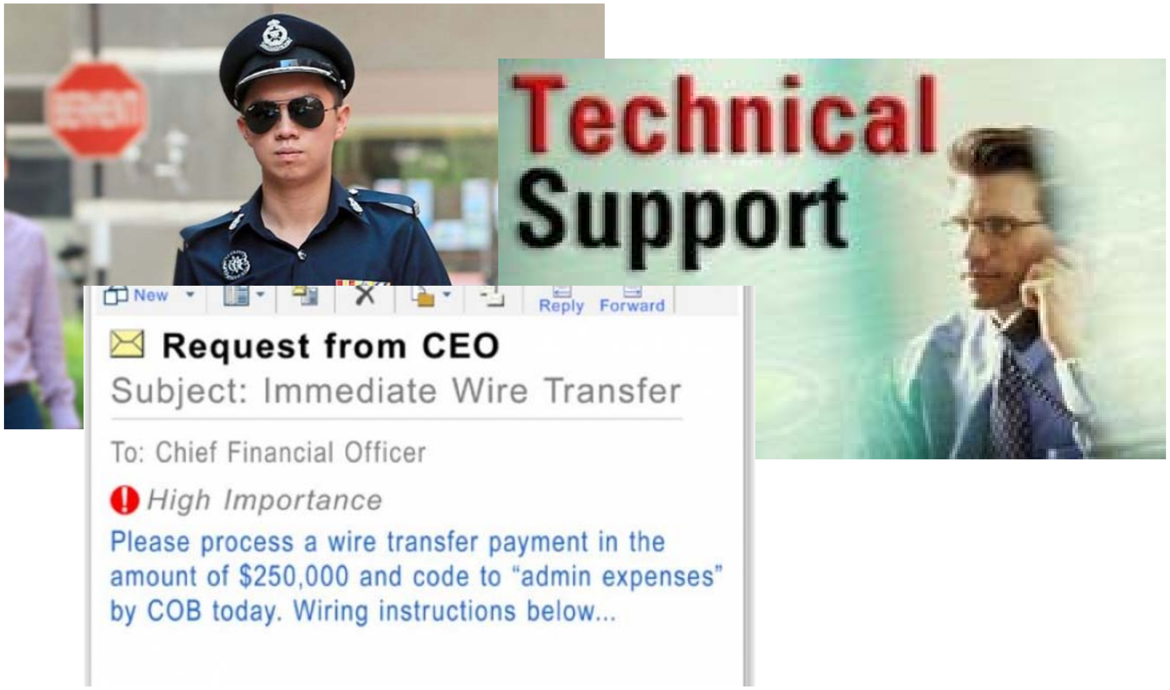
Sympathy

SG Cares

Exploiting Trust

- Authority

Assumed Authority



Request from CEO

Subject: Immediate Wire Transfer

To: Chief Financial Officer

❗ *High Importance*

Please process a wire transfer payment in the amount of $250,000 and code to "admin expenses" by COB today. Wiring instructions below...

Exploiting Trust

- Scarcity

Scarcity - to create a feeling of urgency in a decision-making context

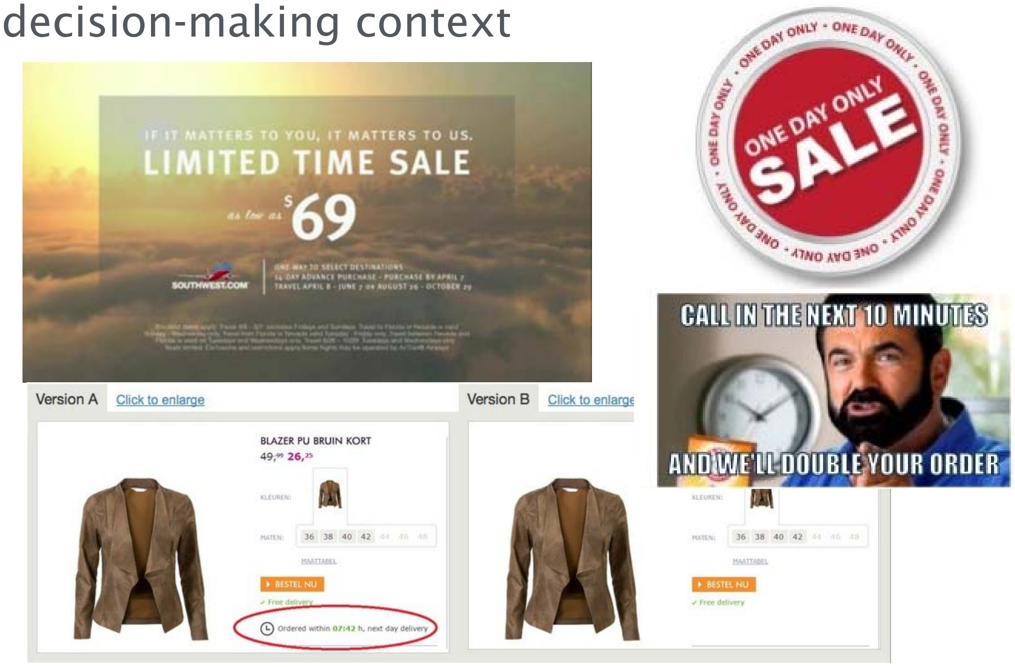

IF IT MATTERS TO YOU, IT MATTERS TO US.
LIMITED TIME SALE
as low as $69
SOUTHWEST.COM
ONE-WAY TO SELECT DESTINATIONS
14-DAY ADVANCE PURCHASE - PURCHASE BY APRIL 7
TRAVEL APRIL 8 - JUNE 7 OR AUGUST 26 - OCTOBER 29
ONE DAY ONLY • ONE DAY ONLY • ONE DAY ONLY
ONE DAY ONLY SALE
CALL IN THE NEXT 10 MINUTES
AND WE'LL DOUBLE YOUR ORDER
Version A
Click to enlarge
Version B
Click to enlarge
BLAZER PU BRUIN KORT
49,99 26,25
KLEUREN:
MATEN:
36 38 40 42 44 46 48
MAATTABEL
BESTEL NU
✓ Free delivery
Ordered within 07:42 h, next day delivery

Image source: 9 essential ways to use Scarcity to increase sales – Kaleigh Moore (https://sumo.com/stories/scarcity-marketing)

HOL

Common Social Engineering Delivery Techniques

Phishing

Emails appearing to be from reputable sources with the goal of influencing or gaining personal information

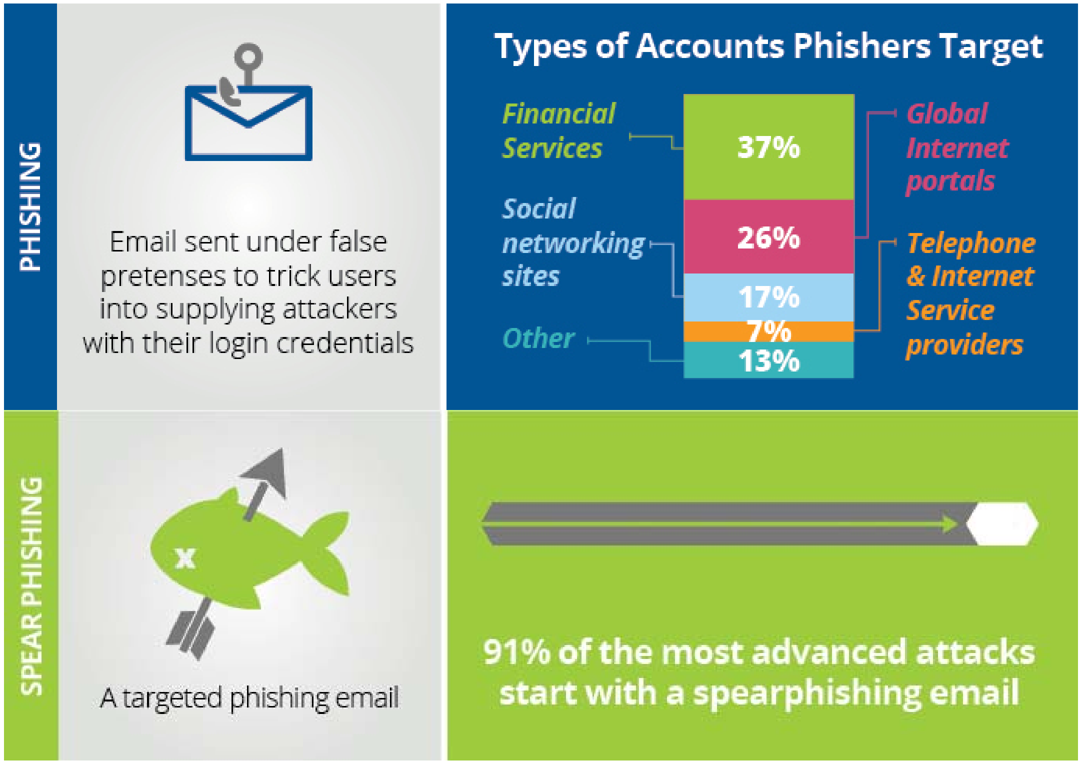
Vishing/Smishing

Eliciting information or attempting to influence action via the telephone, may include such tools as "call/SMS spoofing."

In-person Impersonation

Pretexting as another person with the goal of obtaining information or access to a person, company, or computer system.

Types of Social engineering attacks: Email



Email sent under false pretenses to trick users into supplying attackers with their login credentials

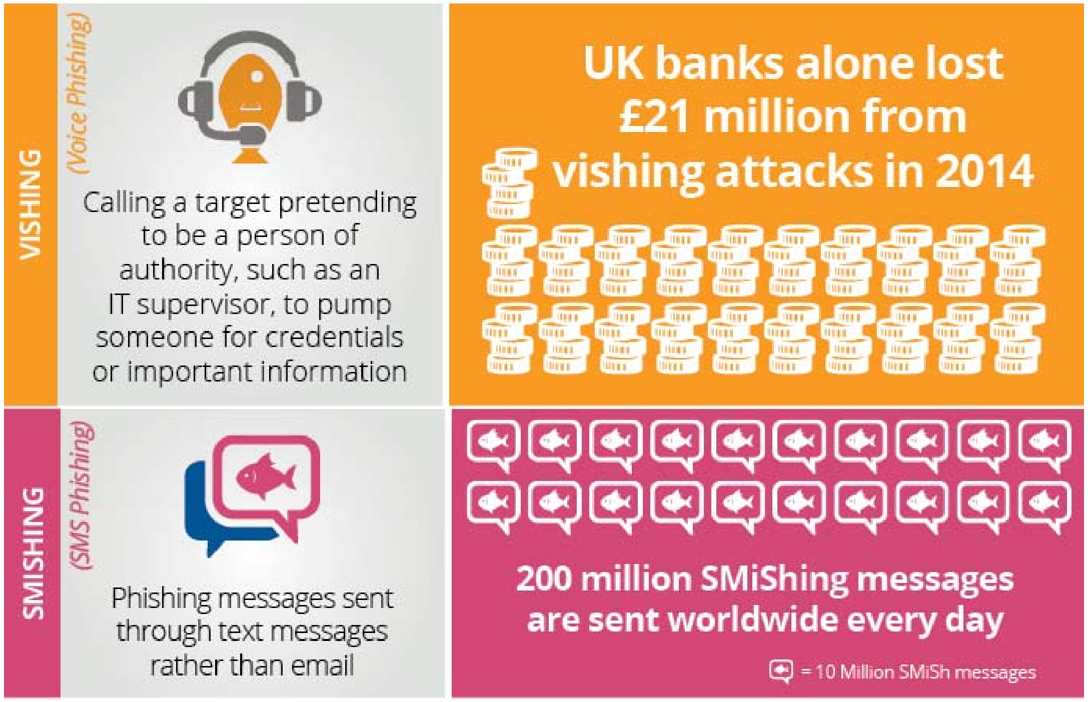
A targeted phishing email

91% of the most advanced attacks start with a spearphishing email

Image source: OneSpan

GOVTECH SINGAPORE

Types of Social engineering attacks: Voice & Text Message



VISHING (Voice Phishing)

Calling a target pretending to be a person of authority, such as an IT supervisor, to pump someone for credentials or important information

UK banks alone lost £21 million from vishing attacks in 2014

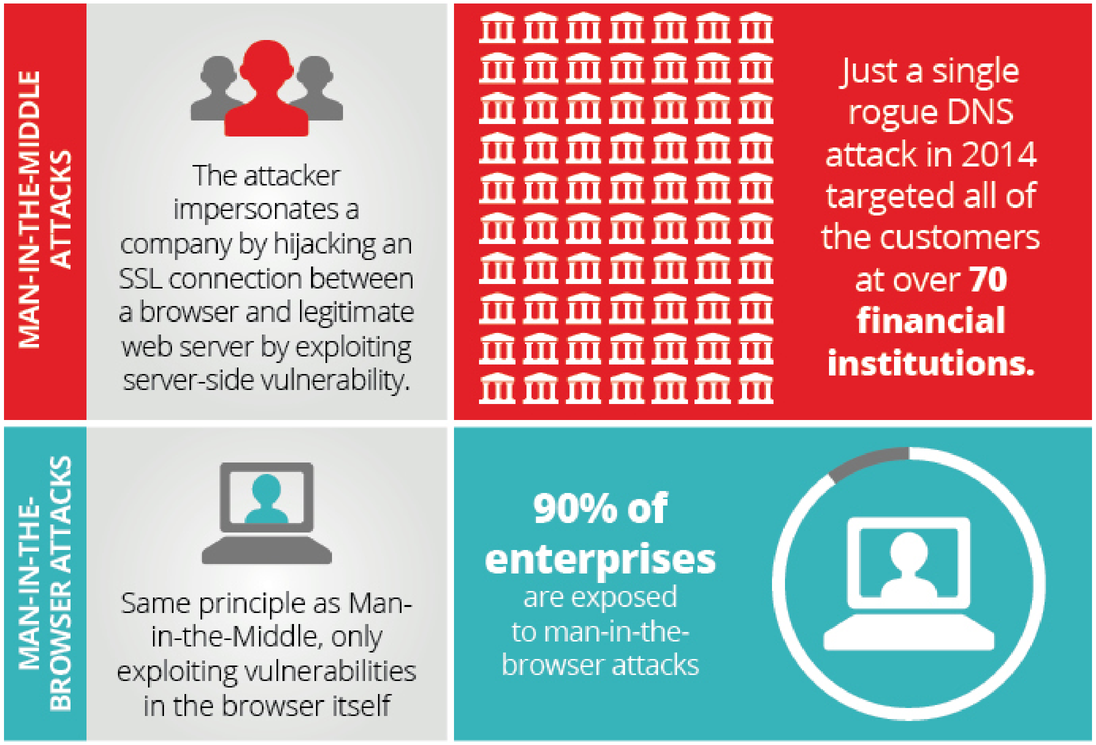
SMISHING (SMS Phishing)

Phishing messages sent through text messages rather than email

200 million SMiShing messages are sent worldwide every day

Image sources: OneSpan

Types of Social engineering attacks: Man-in-the-middle



The attacker impersonates a company by hijacking an SSL connection between a browser and legitimate web server by exploiting server-side vulnerability.

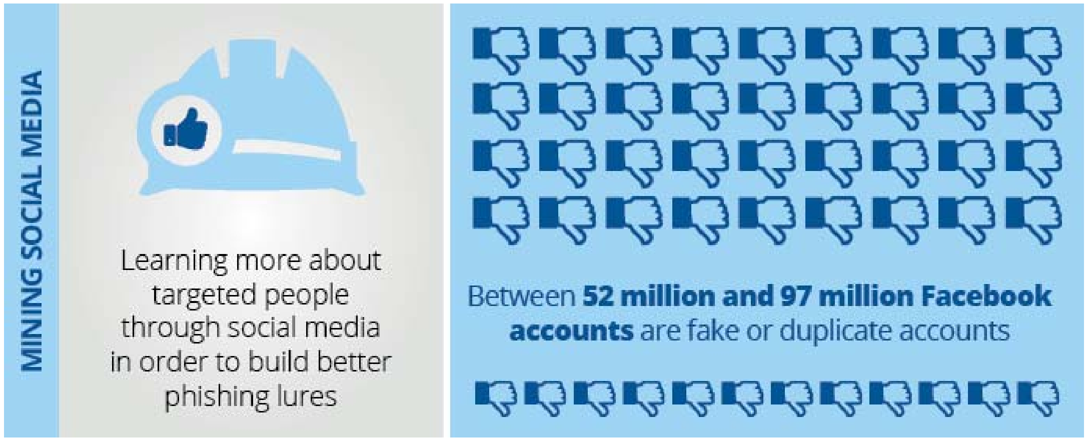
Just a single rogue DNS attack in 2014 targeted all of the customers at over **70 financial institutions.**

Same principle as Man-in-the-Middle, only exploiting vulnerabilities in the browser itself

90% of enterprises are exposed to man-in-the-browser attacks

Image sources: OneSpan

Types of Social engineering attacks: Social Media



MINING SOCIAL MEDIA

Learning more about targeted people through social media in order to build better phishing lures

Between **52 million and 97 million Facebook accounts** are fake or duplicate accounts

Image sources: OneSpan

Types of Social engineering attacks: In-person Impersonation

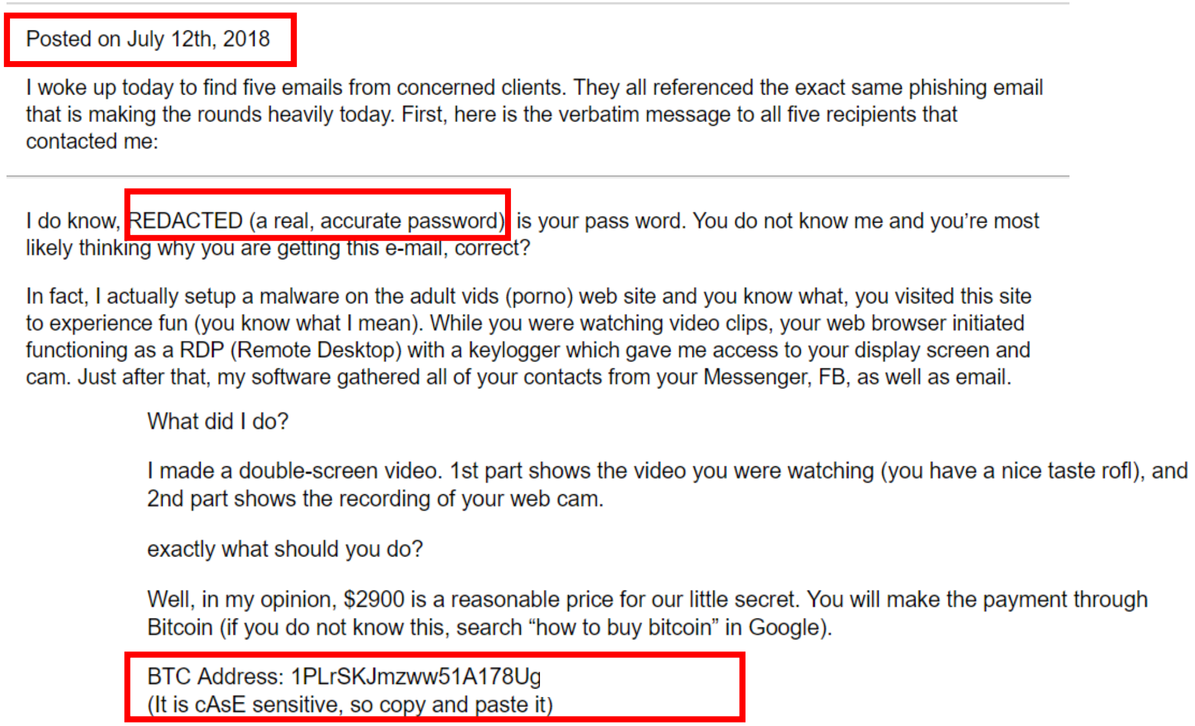
- Types of Social engineering attacks:
- In-person Impersonation

Image sources: VISTA InfoSec

New Email Phishing Campaign – Breach Data

New Phishing Campaign Using Breach Data

Image source: IntelTechniques



Posted on July 12th, 2018

I woke up today to find five emails from concerned clients. They all referenced the exact same phishing email that is making the rounds heavily today. First, here is the verbatim message to all five recipients that contacted me:

I do know, REDACTED (a real, accurate password) is your pass word. You do not know me and you're most likely thinking why you are getting this e-mail, correct?

In fact, I actually setup a malware on the adult vids (porno) web site and you know what, you visited this site to experience fun (you know what I mean). While you were watching video clips, your web browser initiated functioning as a RDP (Remote Desktop) with a keylogger which gave me access to your display screen and cam. Just after that, my software gathered all of your contacts from your Messenger, FB, as well as email.

What did I do?

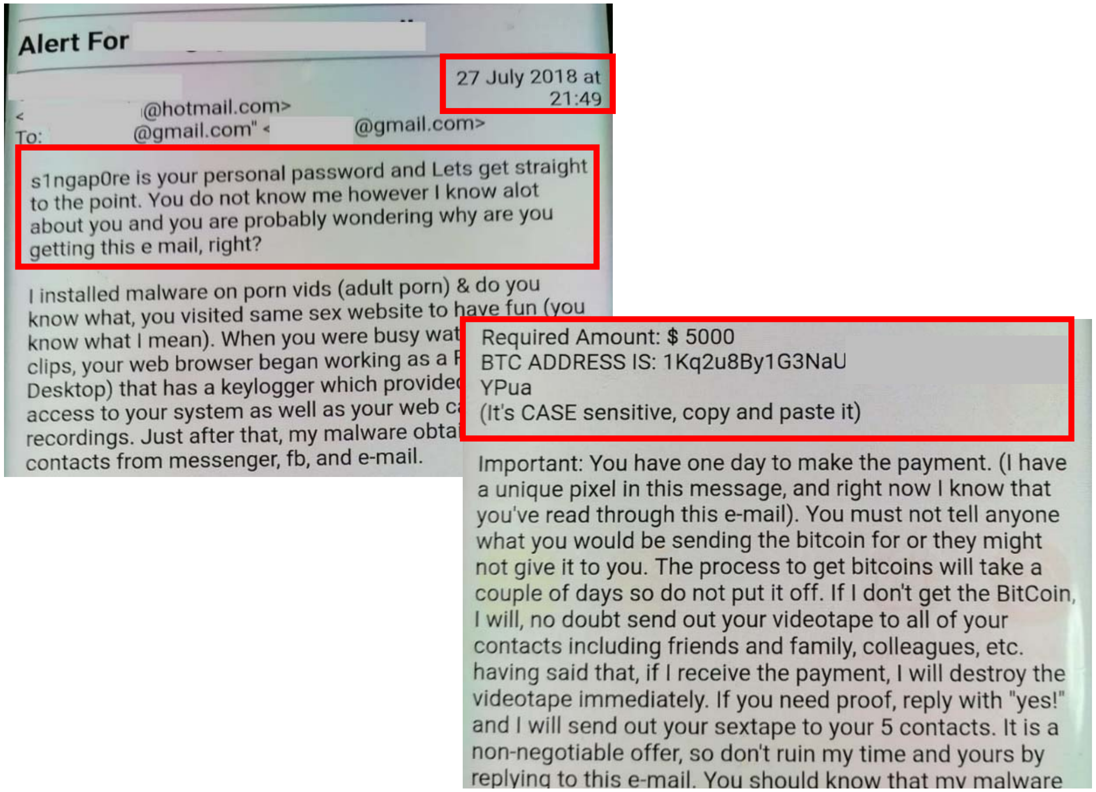
I made a double-screen video. 1st part shows the video you were watching (you have a nice taste rofl), and 2nd part shows the recording of your web cam.

exactly what should you do?

Well, in my opinion, $2900 is a reasonable price for our little secret. You will make the payment through Bitcoin (if you do not know this, search "how to buy bitcoin" in Google).

BTC Address: 1PLrSKJmzww51A178Ug
(It is cAsE sensitive, so copy and paste it)

New Email Phishing Campaign arising from SingHealth Data Breach



Alert For [redacted]

[redacted]

27 July 2018 at 21:49

< [redacted] @hotmail.com>

To: [redacted] @gmail.com" < [redacted] @gmail.com>

s1ngap0re is your personal password and Lets get straight to the point. You do not know me however I know alot about you and you are probably wondering why are you getting this e mail, right?

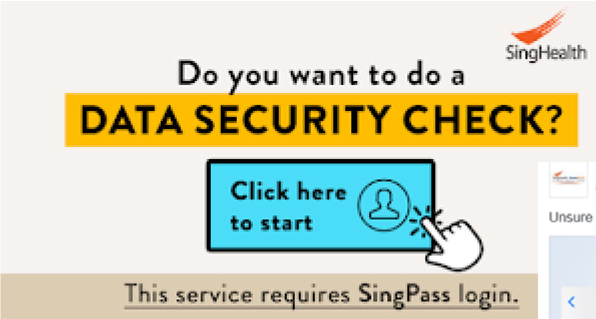
I installed malware on porn vids (adult porn) & do you know what, you visited same sex website to have fun (you know what I mean). When you were busy wat clips, your web browser began working as a F Desktop) that has a keylogger which provided access to your system as well as your web ca recordings. Just after that, my malware obtai contacts from messenger, fb, and e-mail.

Required Amount: $ 5000
BTC ADDRESS IS: 1Kq2u8By1G3NaU [redacted]
YPua
(It's CASE sensitive, copy and paste it)

Important: You have one day to make the payment. (I have a unique pixel in this message, and right now I know that you've read through this e-mail). You must not tell anyone what you would be sending the bitcoin for or they might not give it to you. The process to get bitcoins will take a couple of days so do not put it off. If I don't get the BitCoin, I will, no doubt send out your videotape to all of your contacts including friends and family, colleagues, etc. having said that, if I receive the payment, I will destroy the videotape immediately. If you need proof, reply with "yes!" and I will send out your sextape to your 5 contacts. It is a non-negotiable offer, so don't ruin my time and yours by replying to this e-mail. You should know that my malware

GOVTECH SINGAPORE

Other phishing attacks arising from SingHealth Data Breach



SingHealth

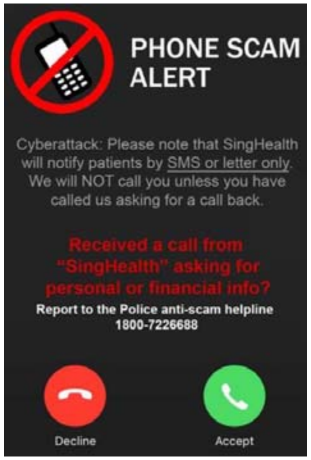
Do you want to do a

DATA SECURITY CHECK?

Click here to start

This service requires SingPass login.

Images source: The Straits Times

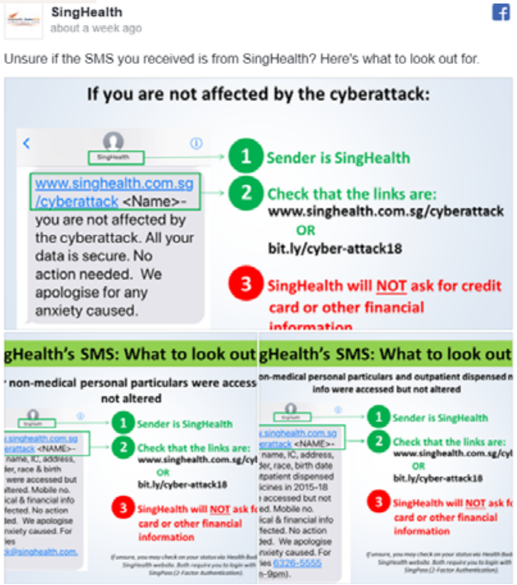


PHONE SCAM ALERT

Cyberattack: Please note that SingHealth will notify patients by SMS or letter only. We will NOT call you unless you have called us asking for a call back.

Received a call from "SingHealth" asking for personal or financial info?

Report to the Police anti-scam helpline 1800-7226688



SingHealth
about a week ago

Unsure if the SMS you received is from SingHealth? Here's what to look out for.

If you are not affected by the cyberattack:

www.singhealth.com.sg/cyberattack <Name>- you are not affected by the cyberattack. All your data is secure. No action needed. We apologise for any anxiety caused.

1 Sender is SingHealth

2 Check that the links are: www.singhealth.com.sg/cyberattack OR bit.ly/cyber-attack18

3 SingHealth will NOT ask for credit card or other financial information

gHealth's SMS: What to look out

non-medical personal particulars were access not altered

.singhealth.com.sg erattack <NAME>- name, IC, address, der, race & birth were accessed but ltered. Mobile no. ical & financial info fected. No action ded. We apologise nxiety caused. For ies k@singhealth.com.

1 Sender is SingHealth

2 Check that the links are: www.singhealth.com.sg/cyl OR bit.ly/cyber-attack18

3 SingHealth will NOT ask fo card or other financial information

(If unsure, you may check on your status via Health Bud SingHealth website. Both require you to login with SingPass (2-Factor Authentication).

gHealth's SMS: What to look out

on-medical personal particulars and outpatient dispensed m info were accessed but not altered

.singhealth.com.sg erattack <NAME>- name, IC, address, der, race, birth date tpatient dispensed icines in 2015-18 accessed but not ed. Mobile no. ical & financial info fected. No action ded. We apologise nxiety caused. For ies 6326-5555 n-9pm).

1 Sender is SingHealth

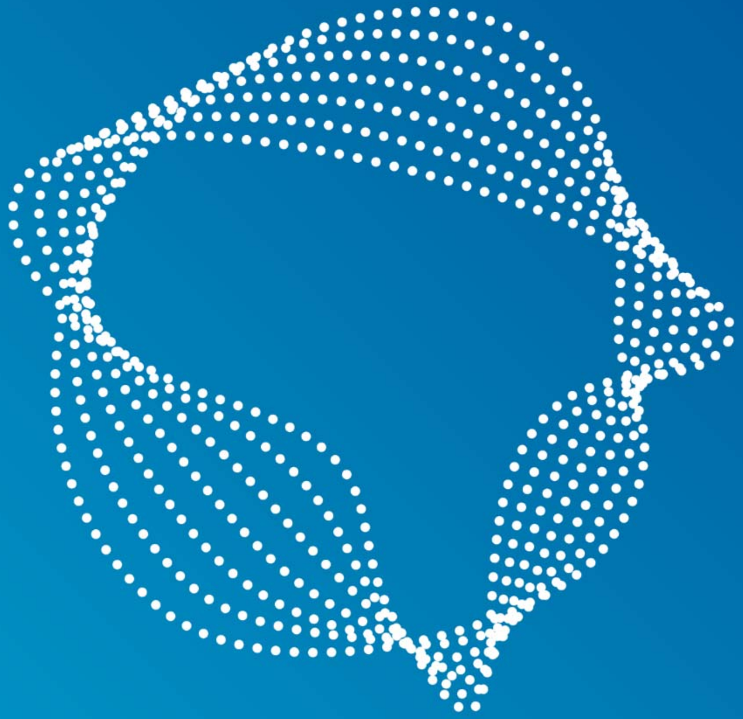
2 Check that the links are: www.singhealth.com.sg/cyl OR bit.ly/cyber-attack18

3 SingHealth will NOT ask fo card or other financial information

(If unsure, you may check on your status via Health Bud SingHealth website. Both require you to login with SingPass (2-Factor Authentication).

GOVTECH SINGAPORE

Key Takeaways



Key Takeaways

- Phishing techniques consider human behaviours to increase success rate
- Processes help to mitigate phishing attacks
- Cyber security awareness assessment identifies weaknesses in these processes and not People
- Determine level of security awareness maturity – SANS 5 stages Security Awareness Maturity Model (https://www.sans.org/sites/default/files/2018-05/2018%20SANS%20Security%20Awareness%20Report.pdf)

Stay vigilant & don’t be an easy phishing target!

Questions?

Thank you

GOVTECH