RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

SESSION ID: HPS-W03

Designing Effective Phishing Simulation Drills

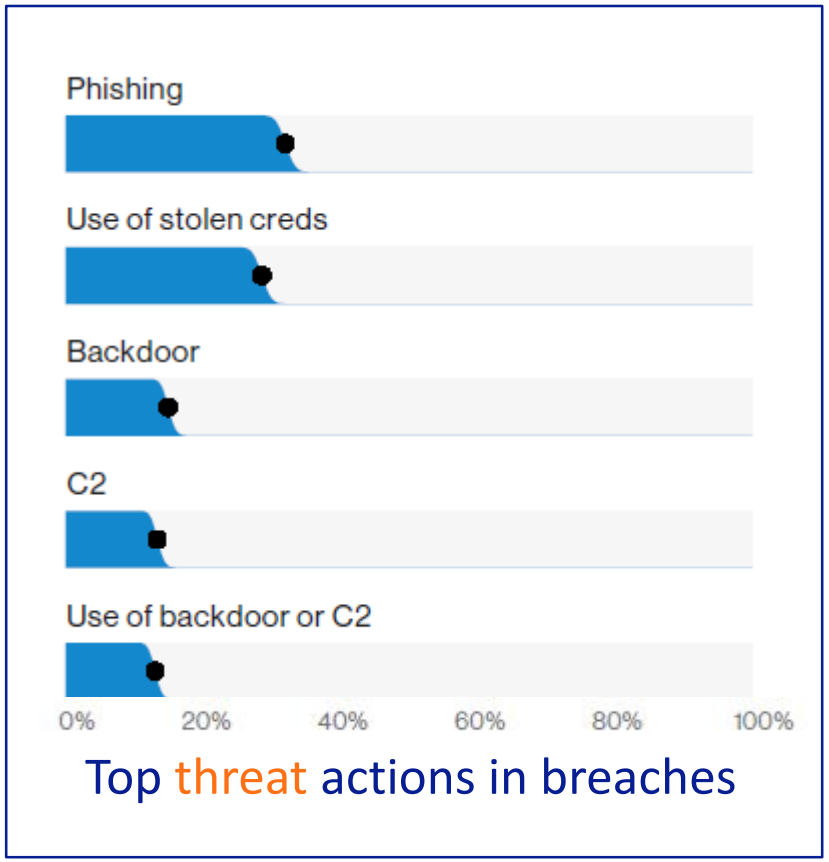
Ang Leong Boon

Head (IT Security)
National University of Singapore

RSAConference2019
Asia Pacific & Japan

Introduction

Verizon's 2019 Data Breach Report

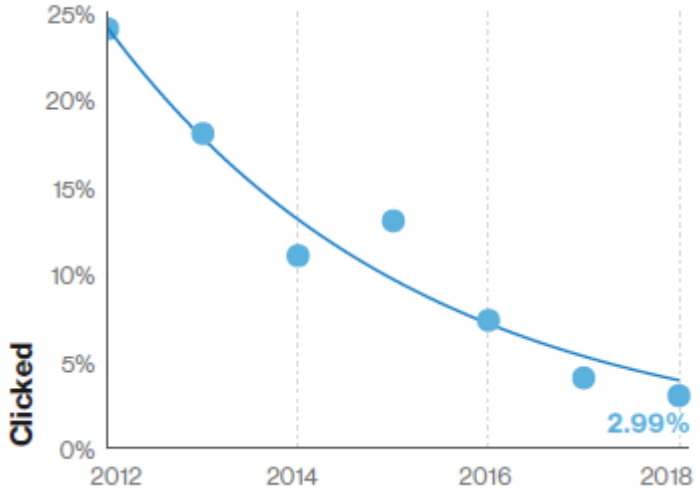


Top threat actions in breaches

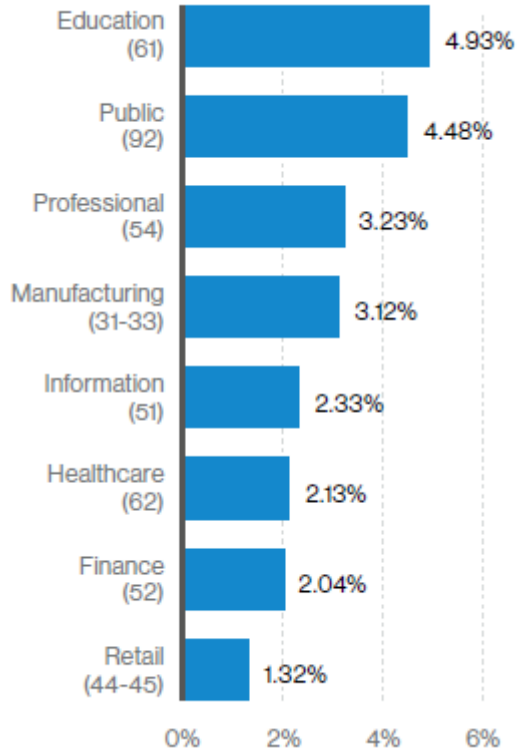
Top social actions in breaches

EMAIL is the most common delivery method

Verizon's 2019 Data Breach Report



Click rates for phishing drills



Click rates for phishing drills across industries

Phishing in Singapore

Cyber threats in Singapore go up; phishing attacks see biggest jump

By FARIS MOKHTAR

Reuters file photo

There was an increase in all forms of cyber threats last year, with phishing attacks topping the list and surging by almost 10 times, according to the latest annual report by the Cyber Security Agency of Singapore (CSA) released on Tuesday (June 19).

Published 19 JUNE, 2018 UPDATED 19 JUNE, 2018

Pretexting in Singapore

Businesses in Singapore lost nearly S$58 million to email impersonation scams last year: CSA report

Rachel Tay

June 18, 2019

According to the Cyber Security Agency of Singapore, 378 business email impersonation scams were recorded in 2018, an increase from 332 in 2017. Pixabay

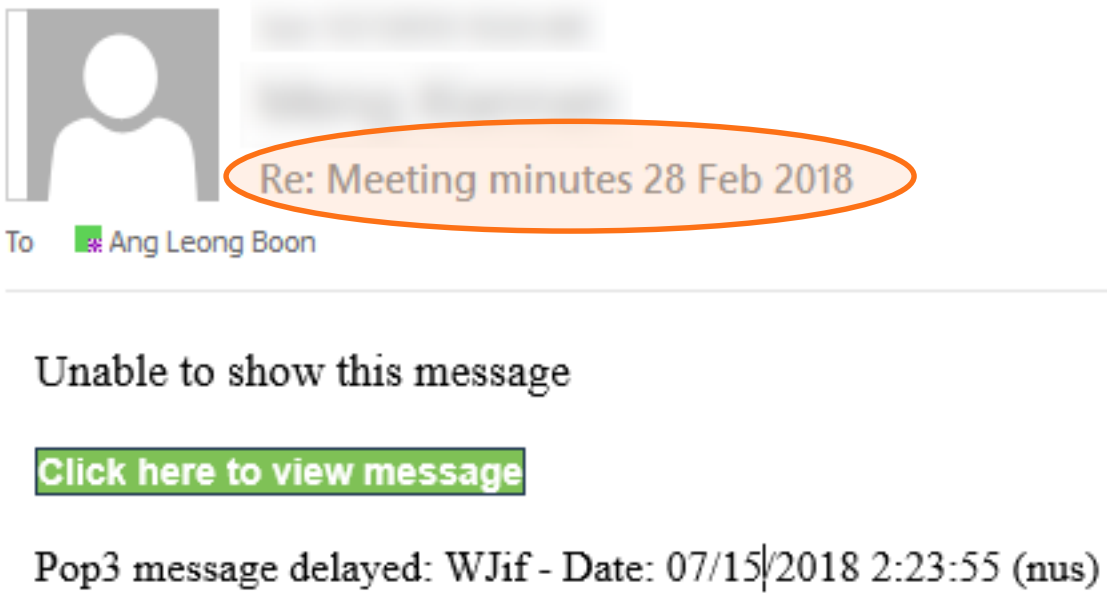
RSAConference2019
Asia Pacific & Japan

Phishing in NUS

Phishing Trends in NUS #1

Website Spoofing

Phishing Trends in NUS #2



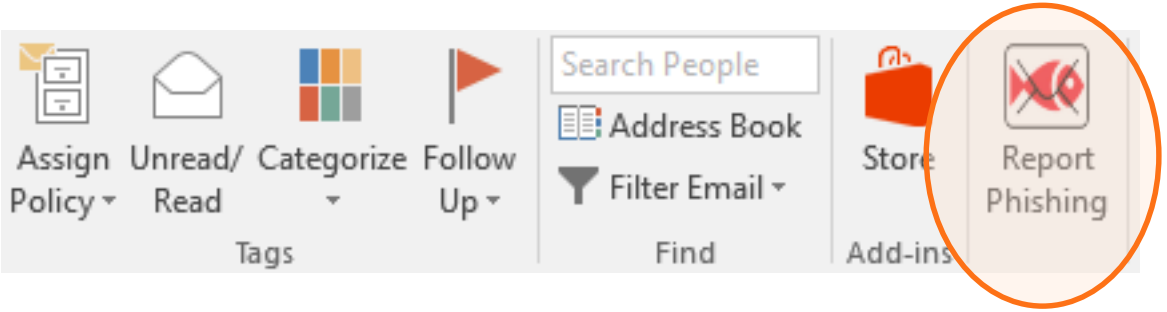
Using existing/familiar email subject

Phishing Trends in NUS #3

iTunes gift card scam
via Pretexting and
Business Email Compromise

Mitigating Phishing Threats in NUS

- Email filters
- Two-factor authentication
- Phishing drills
- “Report Phishing” button
- User education
- Customized office stationery



RSAConference2019
Asia Pacific & Japan

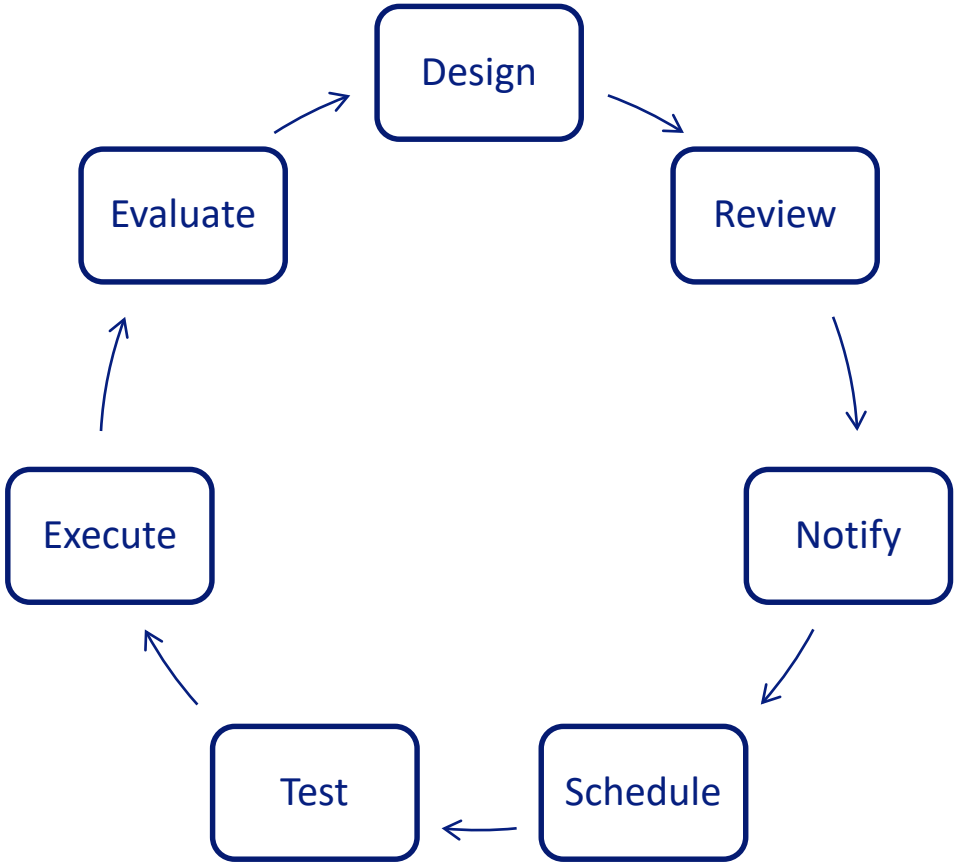
Phishing Drills in NUS

Phishing Drill: Objectives

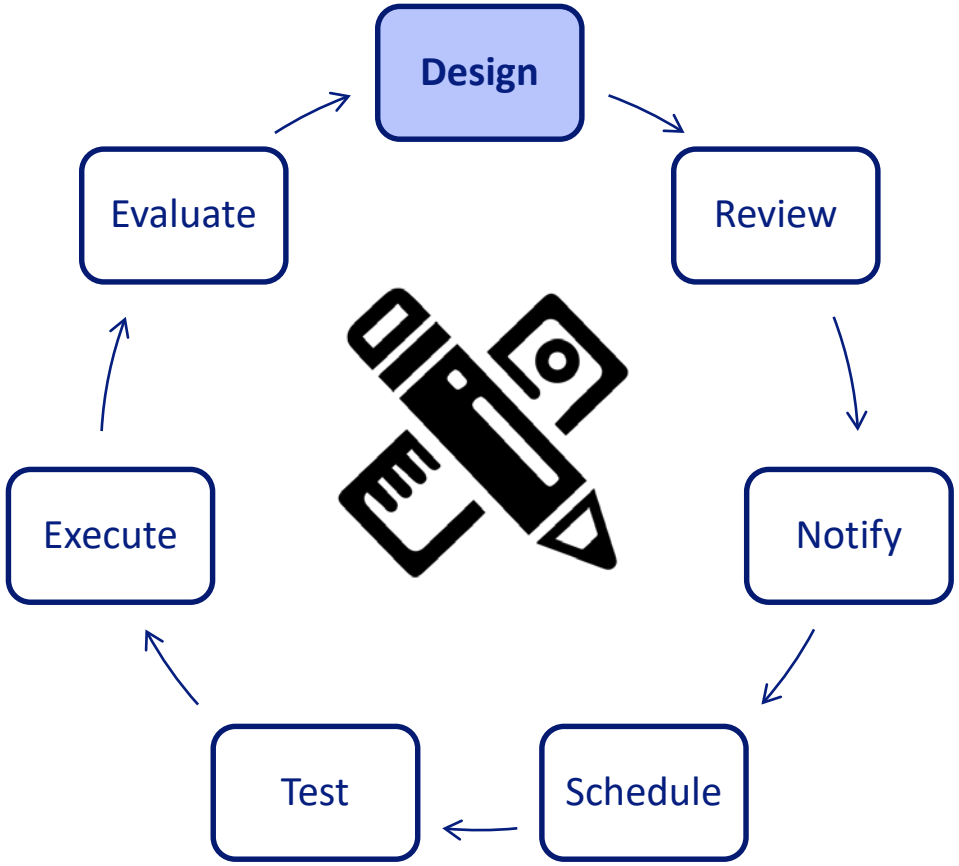
- Reduce the **probability** of successful phishing
  - ↓ users who fall prey to phishing
  - ↓ users who fall prey to phishing repeatedly

- Reduce the **impact** of successful phishing
  - ↑ users who report phishing emails

Phishing Drill: Lifecycle

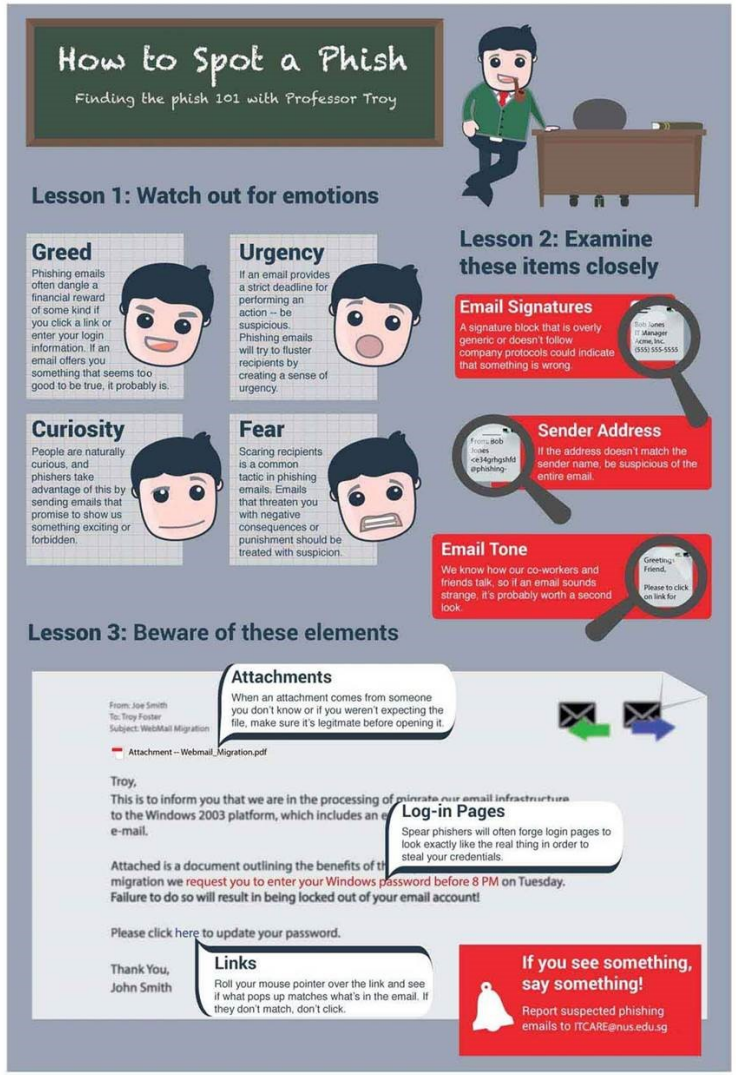


Phishing Drill: Design



- Target audience
- Techniques
- Themes
- Training material
- Frequency
- Phishing platform

Phishing Drill Design: Pre-drill



Phishing Drill Design: Technique and Theme

From: IT Security <IT_Security_Helpdesk@nus.edu.sg>

Subject: [IT Security Alert] Trojan Detected on your Computer!

Dear name,

Warning! Please read immediately.

We found a Trojan from the IP address: 192.168.85.1 trying to access your personal information on your computer.

Download Windows Trojan Removal

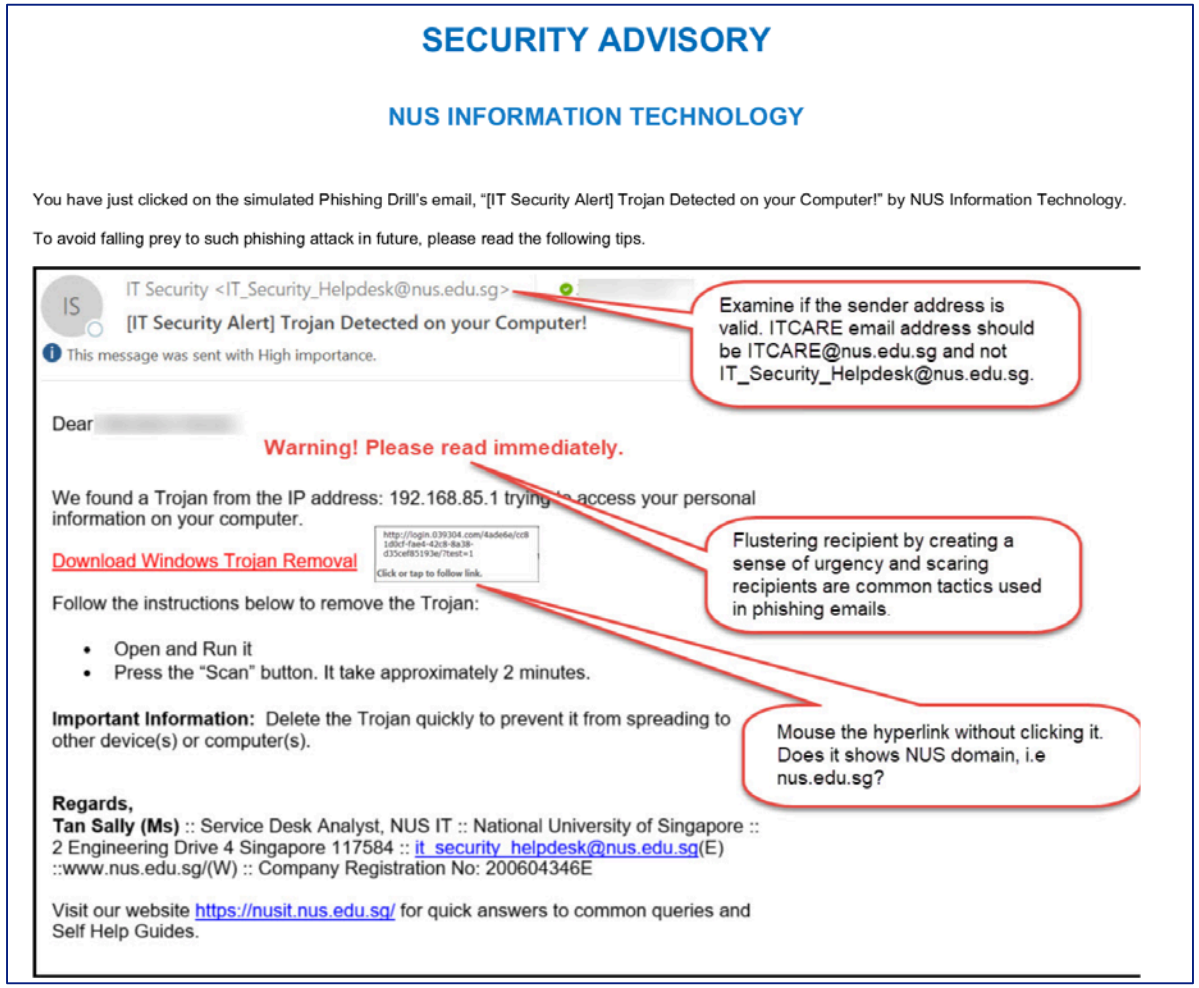
Follow the instructions below to remove the Trojan:

- Open and Run it
- Press the "Scan" button. It take approximately 2 minutes.

Important Information: Delete the Trojan quickly to prevent it from spreading to other device(s) or computer(s).

Regards,
Tan Sally (Ms) :: Service Desk Analyst, NUS IT :: National University of Singapore :: 2 Engineering Drive 4 Singapore 117584 :: it_security_helpdesk@nus.edu.sg(E) ::www.nus.edu.sg/(W) :: Company Registration No: 200604346E

Phishing Drill Design: Post-drill



SECURITY ADVISORY

NUS INFORMATION TECHNOLOGY

You have just clicked on the simulated Phishing Drill's email, "[IT Security Alert] Trojan Detected on your Computer!" by NUS Information Technology.

To avoid falling prey to such phishing attack in future, please read the following tips.

IS

IT Security <IT_Security_Helpdesk@nus.edu.sg>

[IT Security Alert] Trojan Detected on your Computer!

This message was sent with High importance.

Examine if the sender address is valid. ITCARE email address should be ITCARE@nus.edu.sg and not IT_Security_Helpdesk@nus.edu.sg.

Dear

Warning! Please read immediately.

We found a Trojan from the IP address: 192.168.85.1 trying to access your personal information on your computer.

Download Windows Trojan Removal

Flustering recipient by creating a sense of urgency and scaring recipients are common tactics used in phishing emails.

Follow the instructions below to remove the Trojan:

- Open and Run it
- Press the "Scan" button. It take approximately 2 minutes.

Important Information: Delete the Trojan quickly to prevent it from spreading to other device(s) or computer(s).

Mouse the hyperlink without clicking it. Does it shows NUS domain, i.e nus.edu.sg?

Regards,
Tan Sally (Ms) :: Service Desk Analyst, NUS IT :: National University of Singapore :: 2 Engineering Drive 4 Singapore 117584 :: it_security_helpdesk@nus.edu.sg(E) ::www.nus.edu.sg/(W) :: Company Registration No: 200604346E

Visit our website https://nusit.nus.edu.sg/ for quick answers to common queries and Self Help Guides.

Phishing Drill Design: Control Groups

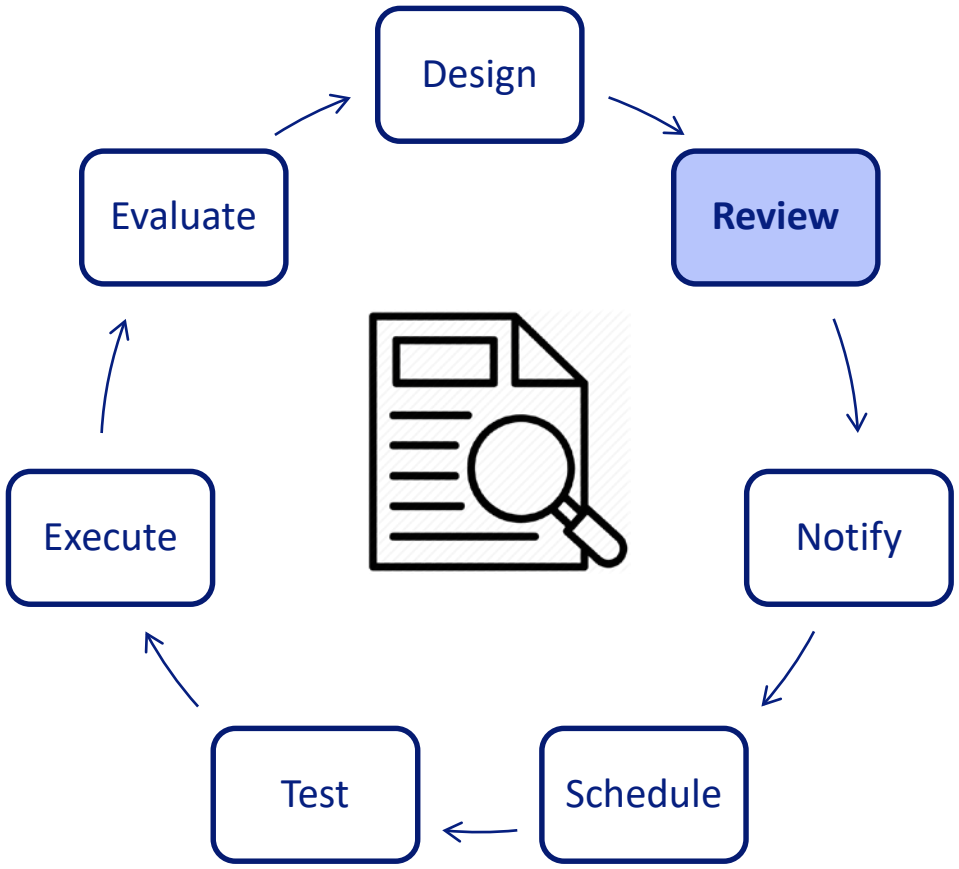
- Divide users into groups
  - Random
  - Department
  - Job function
- Determine parameters for each group (choose only one)
  - Frequency
  - Sender
  - Pre/Post education
  - Theme
- Conduct the same final evaluation drill(s) for all groups

Phishing Drill Design: Control Group Example

Parameter: Frequency of drills

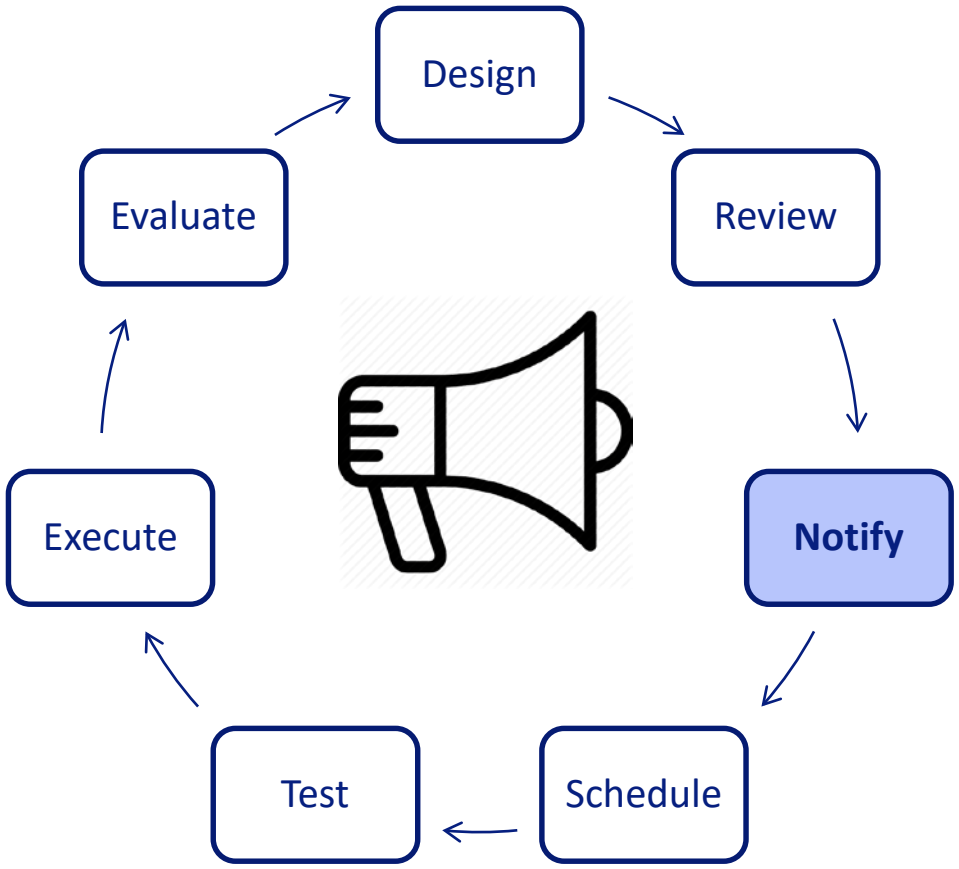
	Training			Evaluation	
	Drill 1	Drill 2	Drill 3	Drill 4	Drill 5
Group 1	✓	✓	✓	✓	✓
Group 2			✓	✓	✓
Group 3				✓	✓

Phishing Drill: Review



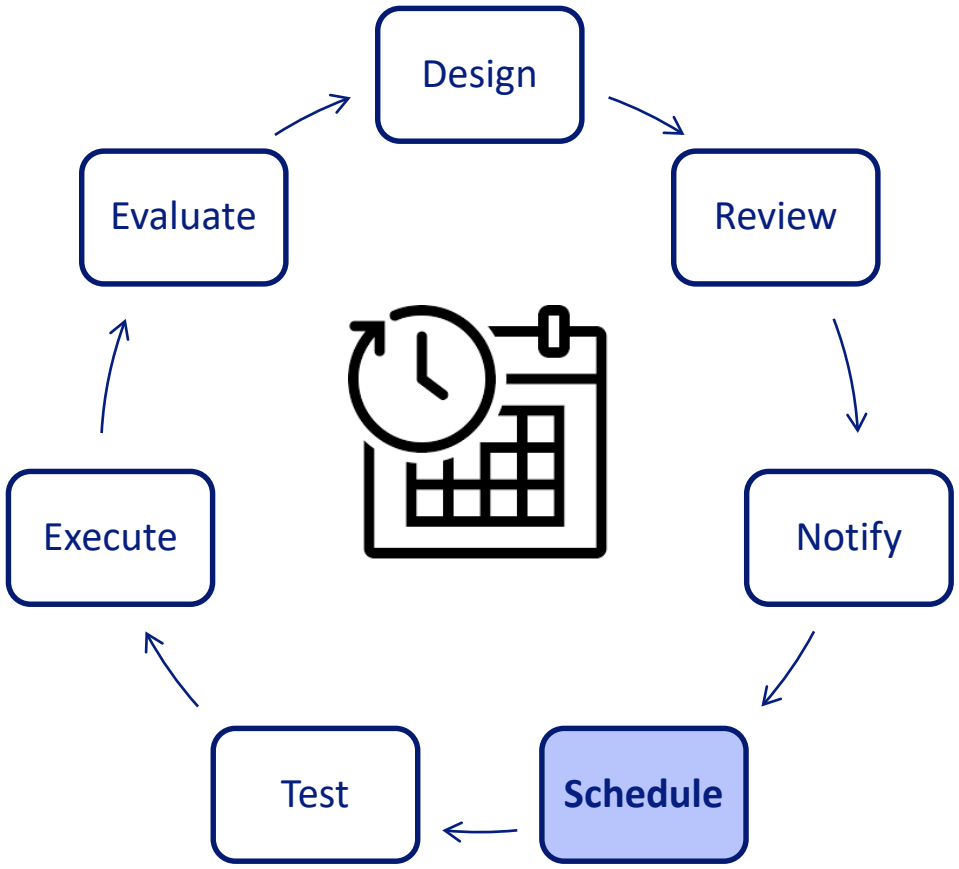
- Existing domain
- Trademarks
- Sensitive content
- Obtain necessary approval

Phishing Drill: Notify



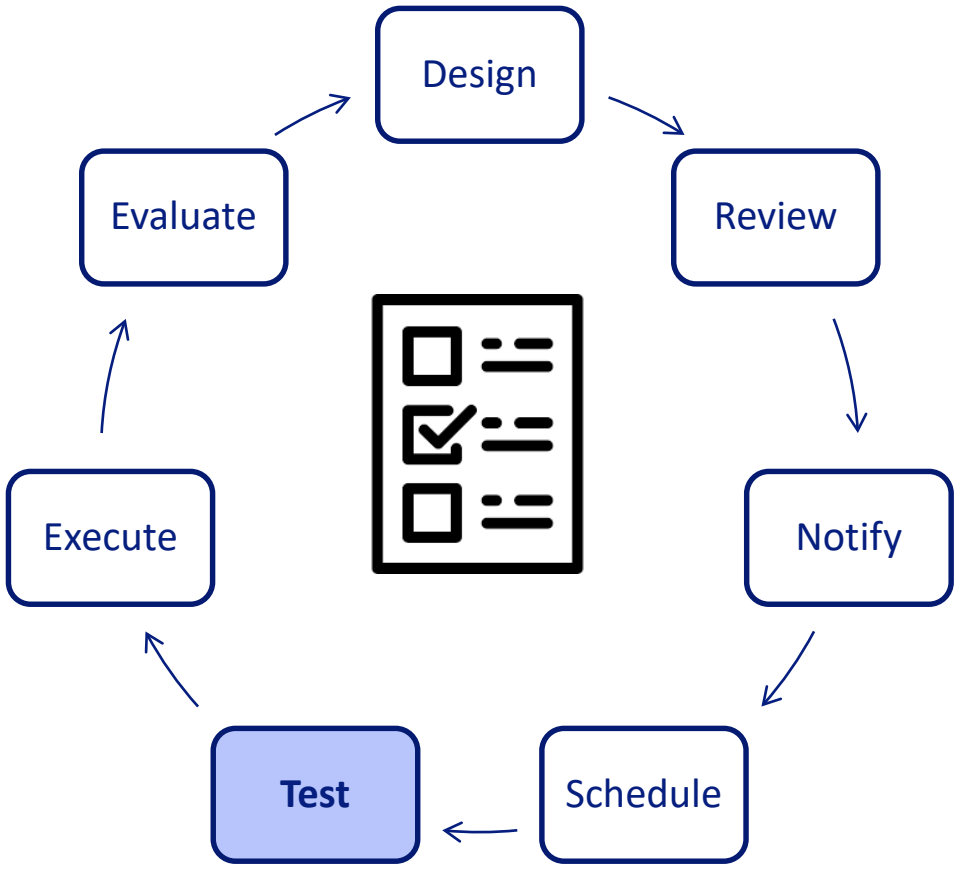
- Pre-drill
- During drill
- Post-drill

Phishing Drill: Schedule



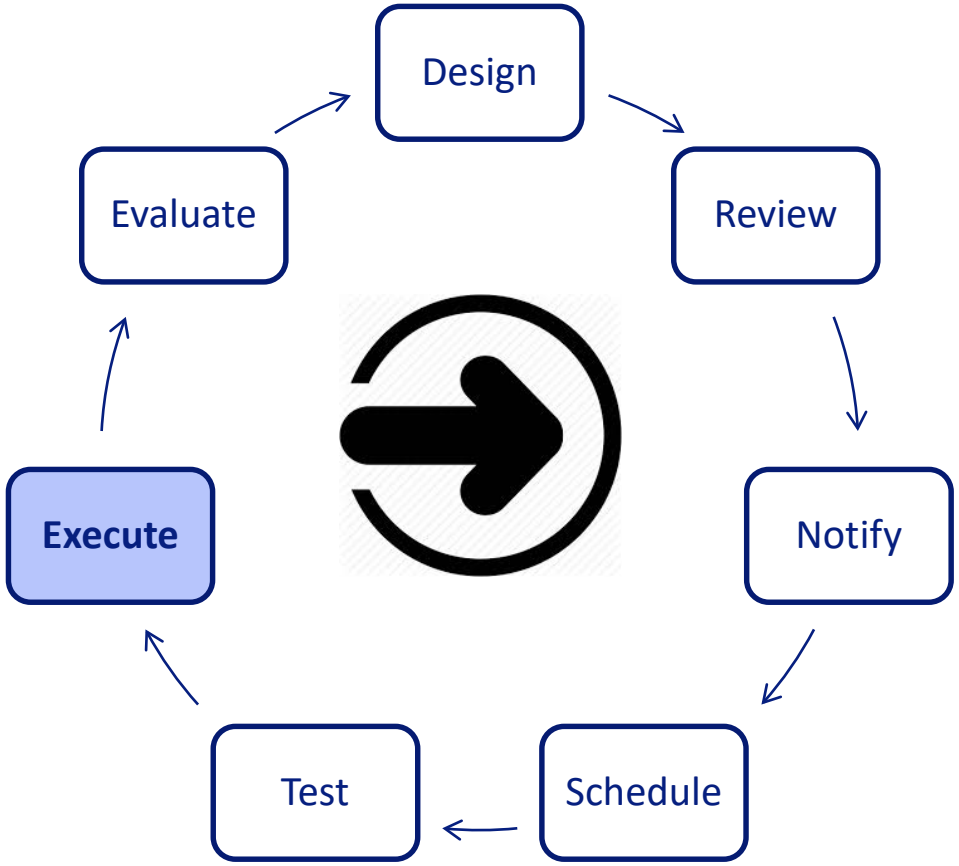
- Working hours
- Day of week
- Holidays
- Rate-limiting
- Duration

Phishing Drill: Test



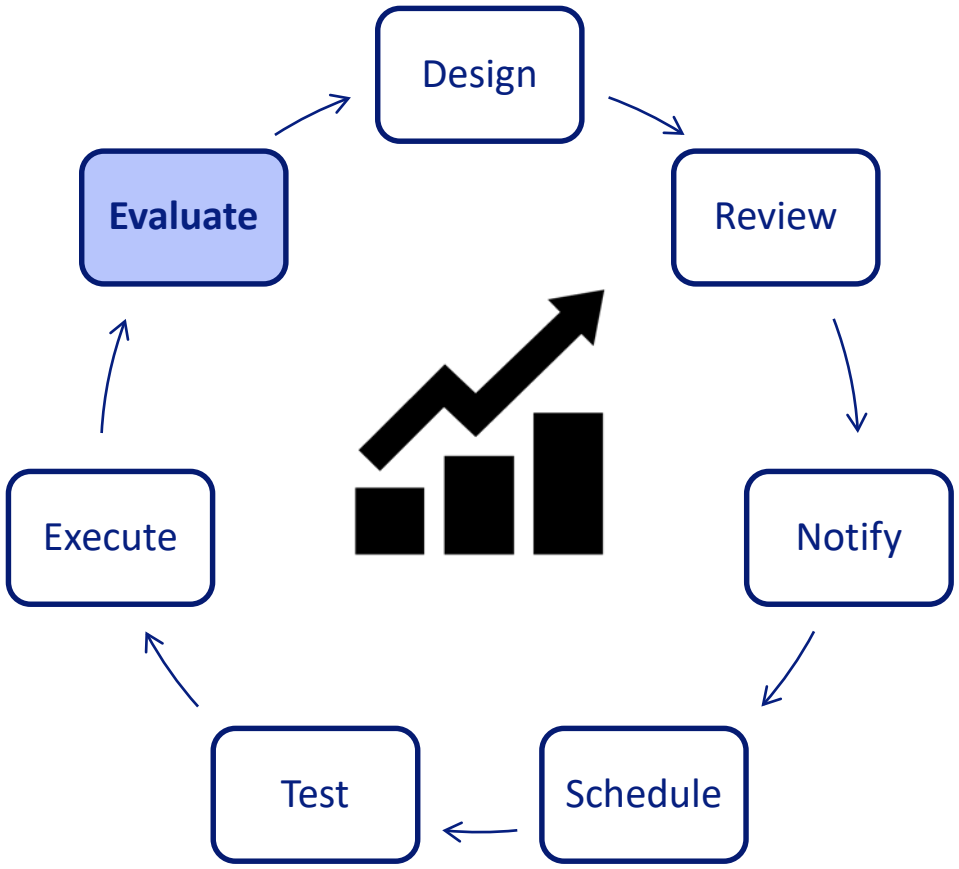
- Test sending to small group
- Verify look and feel
- Ensure links are working
- Verify recipient list

Phishing Drill: Execute



- Prepare for user queries
- Prepare scripted answers for helpdesk

Phishing Drill: Evaluate

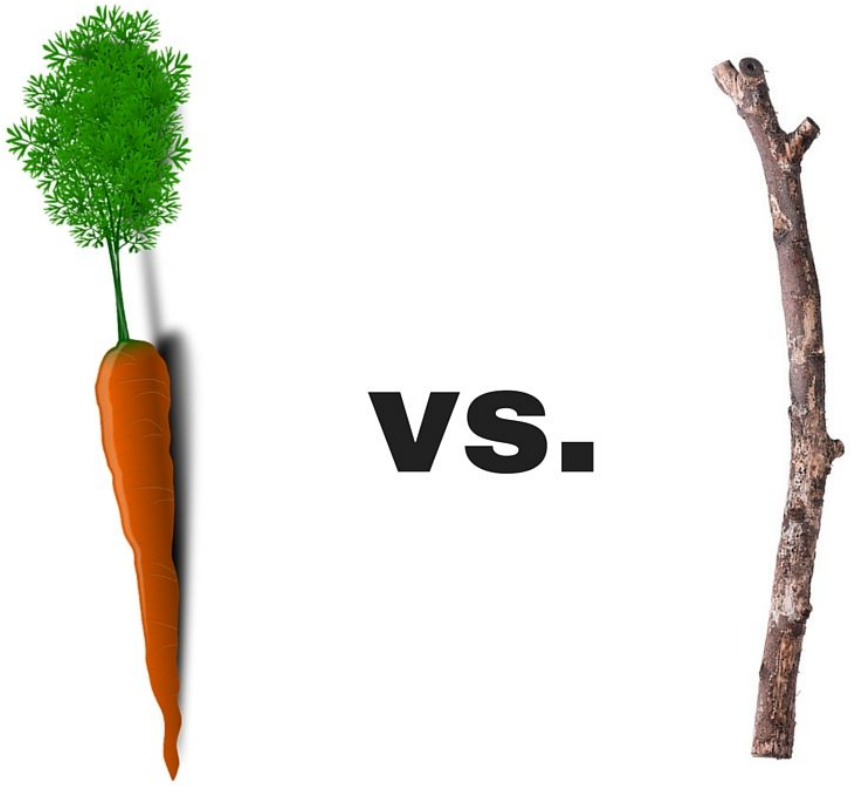


- Compare with industry
- Comparison across departments
- Comparison with previous drills
- Identify users who fall prey repeatedly

Lessons Learnt

- Anxiety and frustration from users
- Backlash from certain themes
- Branding of departments used in some themes
- Overwhelmed service desk
- Does clicking = falling prey?

Lessons Learnt



RSAConference2019
Asia Pacific & Japan

Summary

Conduct your own Phishing Drill

- Next week
  - Identify and categorize groups of personnel at risk
- Over the next 3 months
  - Evaluate various phishing education platforms
  - Obtain management buy-in for a phishing drill
  - Collect samples of phishing emails in your organization
  - Design drills specific to your organization
- After 6 months you should conduct your first phishing drill!

RSAConference2019
Asia Pacific & Japan

Q&A