48730, 32548 - Cyber Security & Essentials

Lab 2: Pharming Attack

Tutor: Ngoc LE

Outline:

1 Concepts, Pharming or Phishing

2 Designed Network

3 The overview tasks of Lab 2

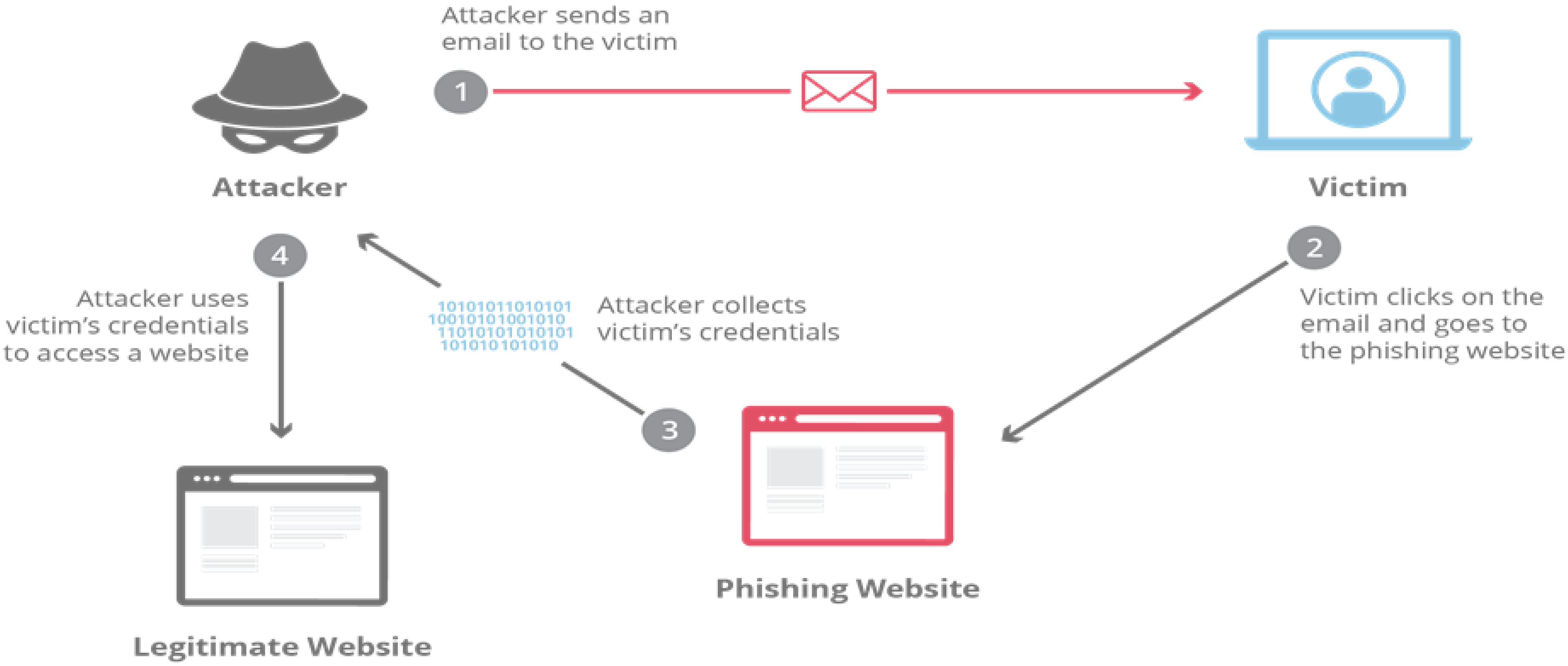
1. Phishing attack [1]

What is it?

- Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers
- Victims open an email, instant message, or text message...
- Then tricked into clicking a malicious link, which can lead to the installation of malware.
- **One by one**

[1] https://www.imperva.com/learn/application-security/phishing-attack-scam/

1. Phishing attack [2]



1 Attacker sends an email to the victim

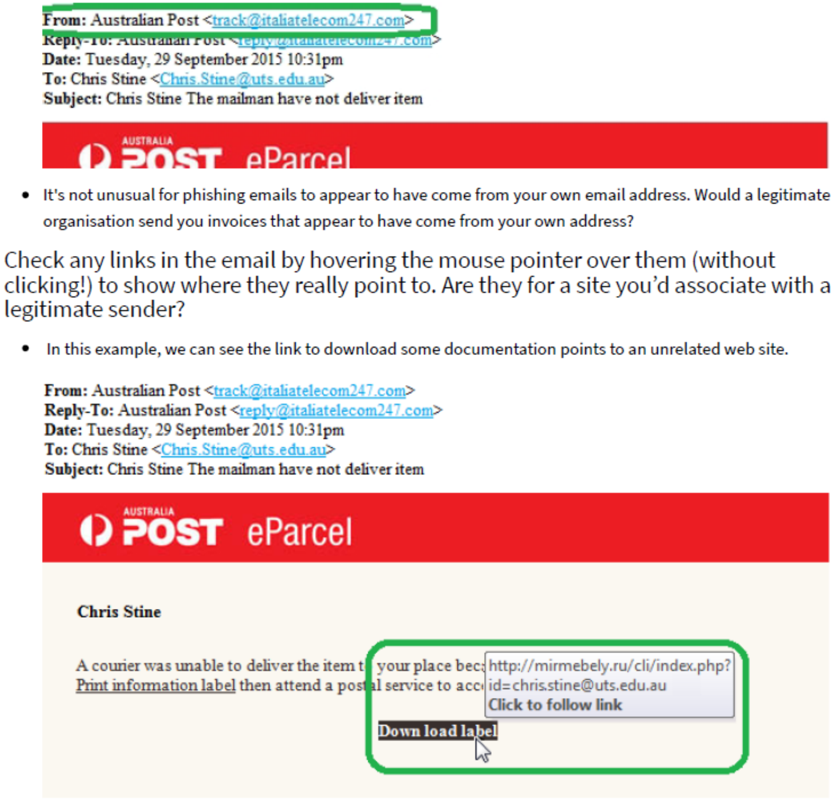
2 Victim clicks on the email and goes to the phishing website

3 Attacker collects victim’s credentials

4 Attacker uses victim’s credentials to access a website

[2] https://www.cloudflare.com/learning/security/threats/phishing-attack/

1. Phishing attack [3]



From: Australian Post <track@italiatelecom247.com>
Reply-To: Australian Post <reply@italiatelecom247.com>
Date: Tuesday, 29 September 2015 10:31pm
To: Chris Stine <Chris.Stine@uts.edu.au>
Subject: Chris Stine The mailman have not deliver item

- It's not unusual for phishing emails to appear to have come from your own email address. Would a legitimate organisation send you invoices that appear to have come from your own address?

Check any links in the email by hovering the mouse pointer over them (without clicking!) to show where they really point to. Are they for a site you'd associate with a legitimate sender?

- In this example, we can see the link to download some documentation points to an unrelated web site.

From: Australian Post <track@italiatelecom247.com>
Reply-To: Australian Post <reply@italiatelecom247.com>
Date: Tuesday, 29 September 2015 10:31pm
To: Chris Stine <Chris.Stine@uts.edu.au>
Subject: Chris Stine The mailman have not deliver item

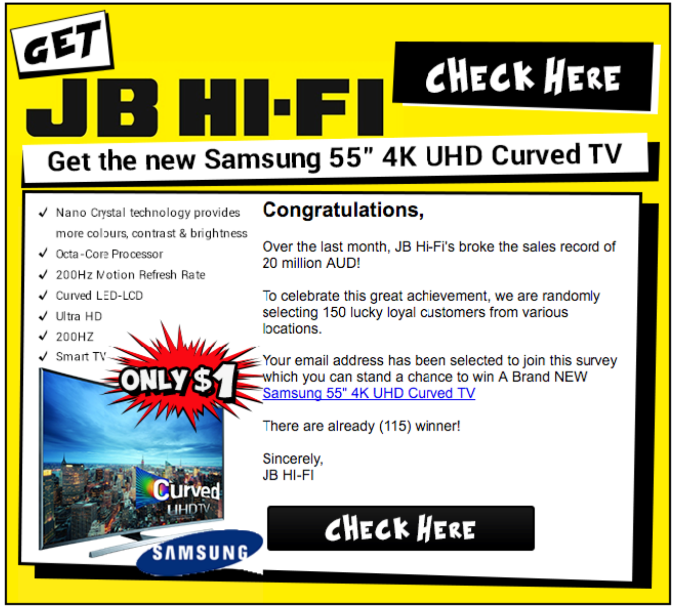
Chris Stine

A courier was unable to deliver the item t your place bec
Print information label then attend a postal service to acc

http://mirmebely.ru/cli/index.php?id=chris.stine@uts.edu.au
Click to follow link

Is the email offering something that is too good to be true?

- If you receive an email claiming that you won the lottery but you've never actually bought a ticket, then you should be suspicious.
- Think before you click, could you really buy the latest TV for $1?



GET
JB HI-FI
CHECK HERE
Get the new Samsung 55" 4K UHD Curved TV
✓ Nano Crystal technology provides more colours, contrast & brightness
✓ Octa-Core Processor
✓ 200Hz Motion Refresh Rate
✓ Curved LED-LCD
✓ Ultra HD
✓ 200HZ
✓ Smart TV
ONLY $1
Curved UHD TV
SAMSUNG
CHECK HERE

Congratulations,

Over the last month, JB Hi-Fi's broke the sales record of 20 million AUD!

To celebrate this great achievement, we are randomly selecting 150 lucky loyal customers from various locations.

Your email address has been selected to join this survey which you can stand a chance to win A Brand NEW Samsung 55" 4K UHD Curved TV

There are already (115) winner!

Sincerely,
JB HI-FI

[3] https://uts.service-now.com/serviceconnect/?id=kb_article&sys_id=cc46ab316f57de00d031a5c5eb3ee4bc

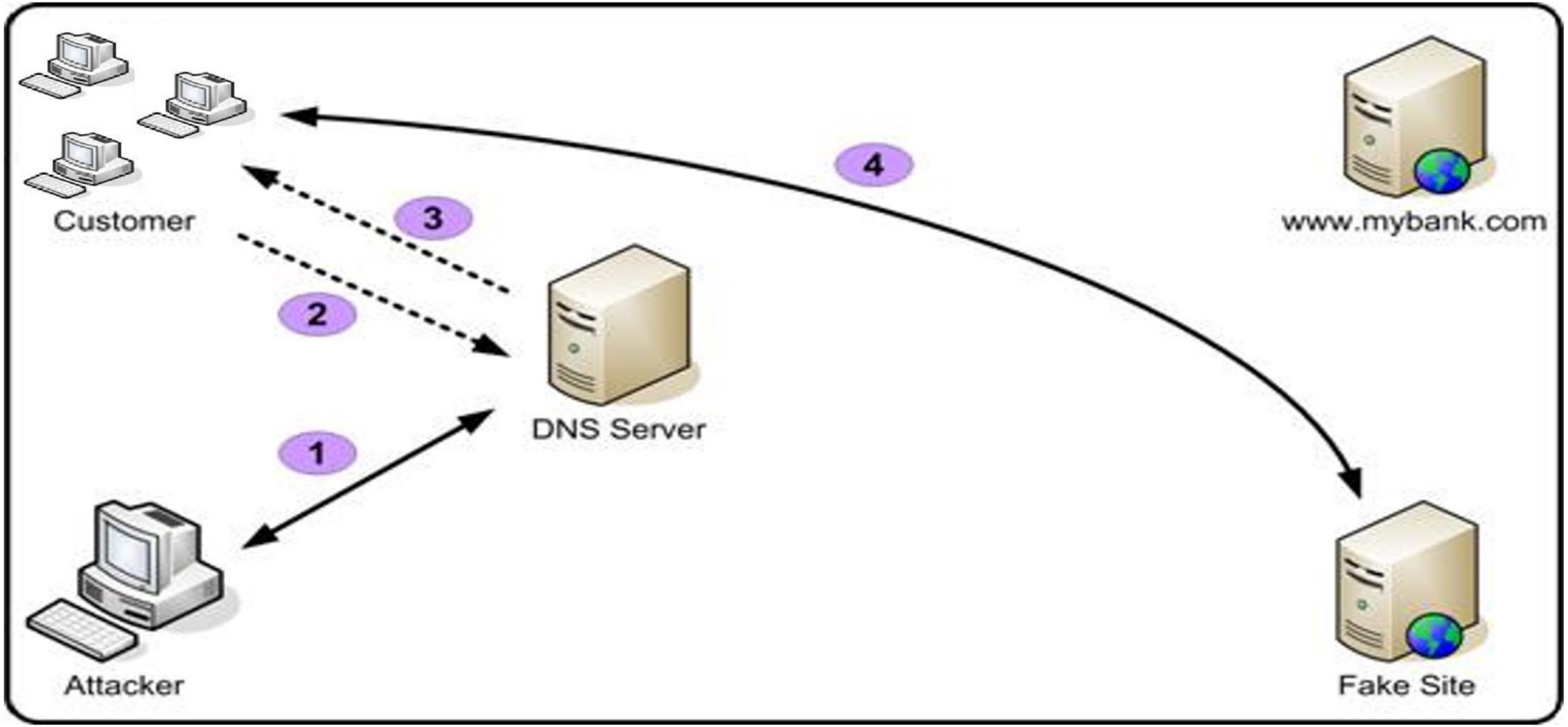
1. Pharming attack [4]

What is it?

- Is the **exploitation of a vulnerability in Domain Name Service (DNS)** server software that allows a hacker to redirect that website's traffic to another web site.
- DNS servers are the machines responsible for **resolving Internet names** into their real addresses, and are used anytime a user types the name of a website into his or her web browser and attempts to view a web page.
- **One by many (Farm of Phishing)**

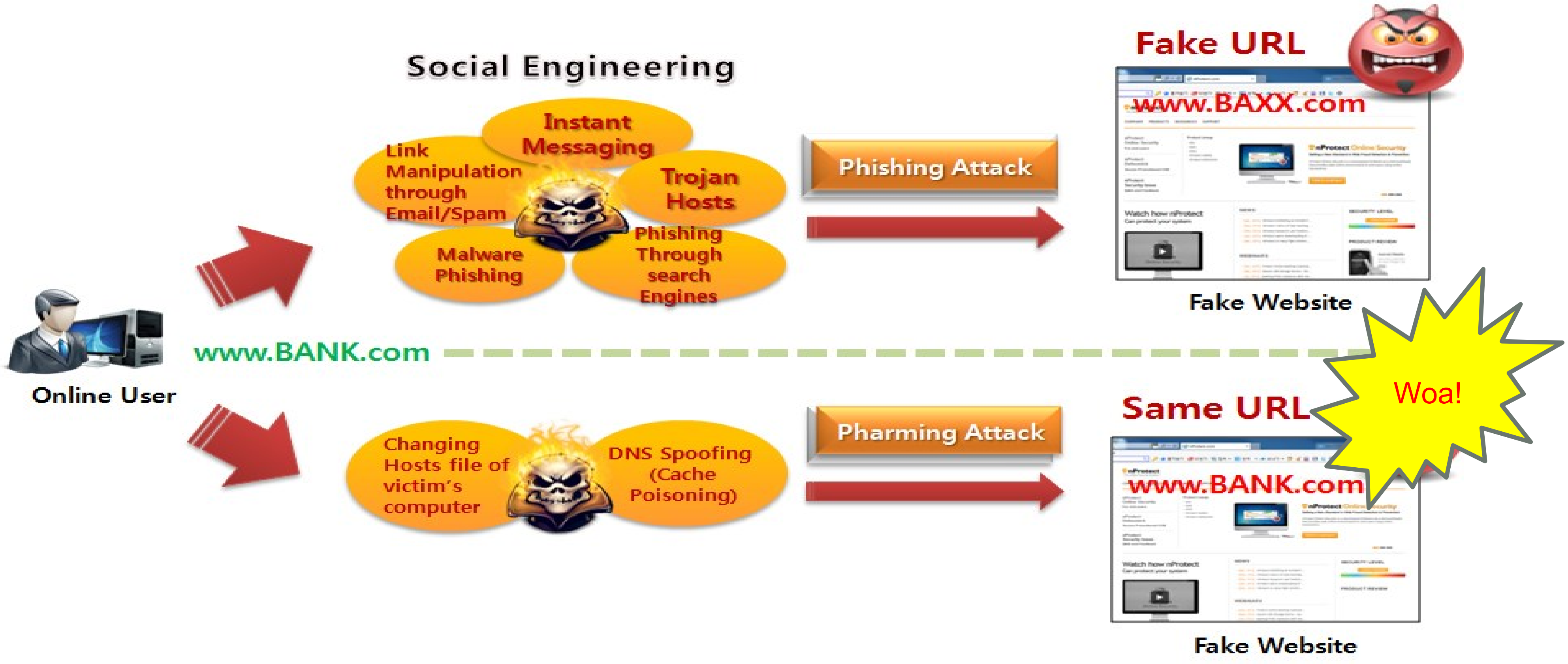
[4] http://nos.nprotect.com/newsletter/062014.html

1. Pharming [5]



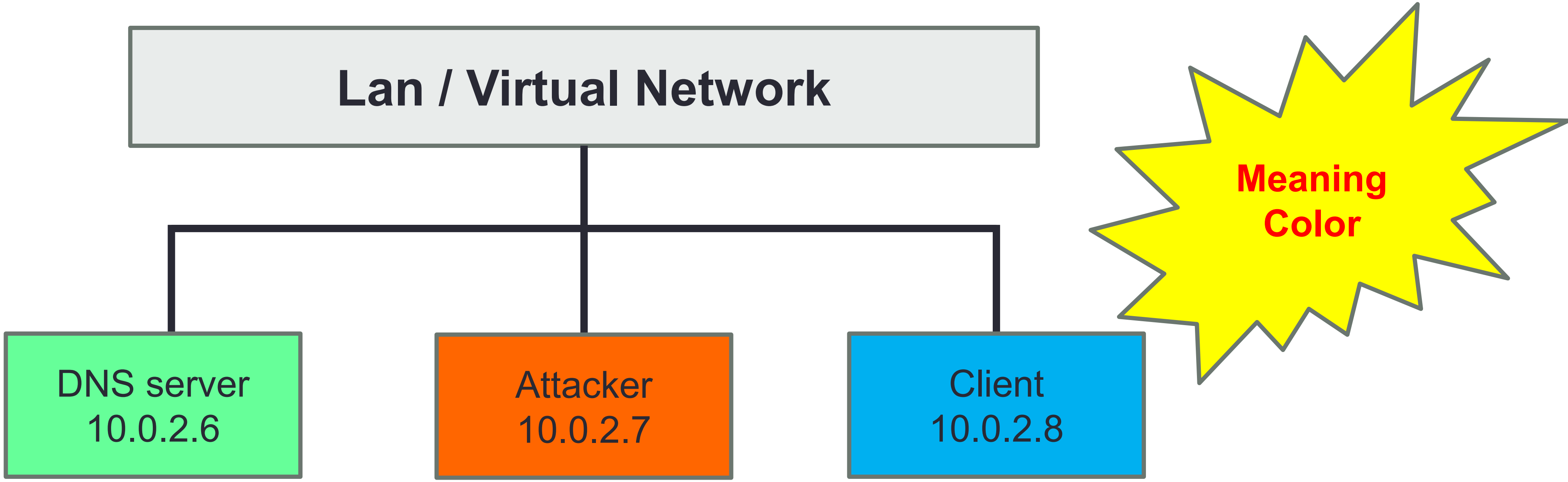
[5] http://www.technicalinfo.net/papers/Pharming2.html

1. Difference: Phishing - Pharming [4]



[4] http://nos.nprotect.com/newsletter/062014.html

2. Our network design



Lan / Virtual Network

DNS server
10.0.2.6

Attacker
10.0.2.7

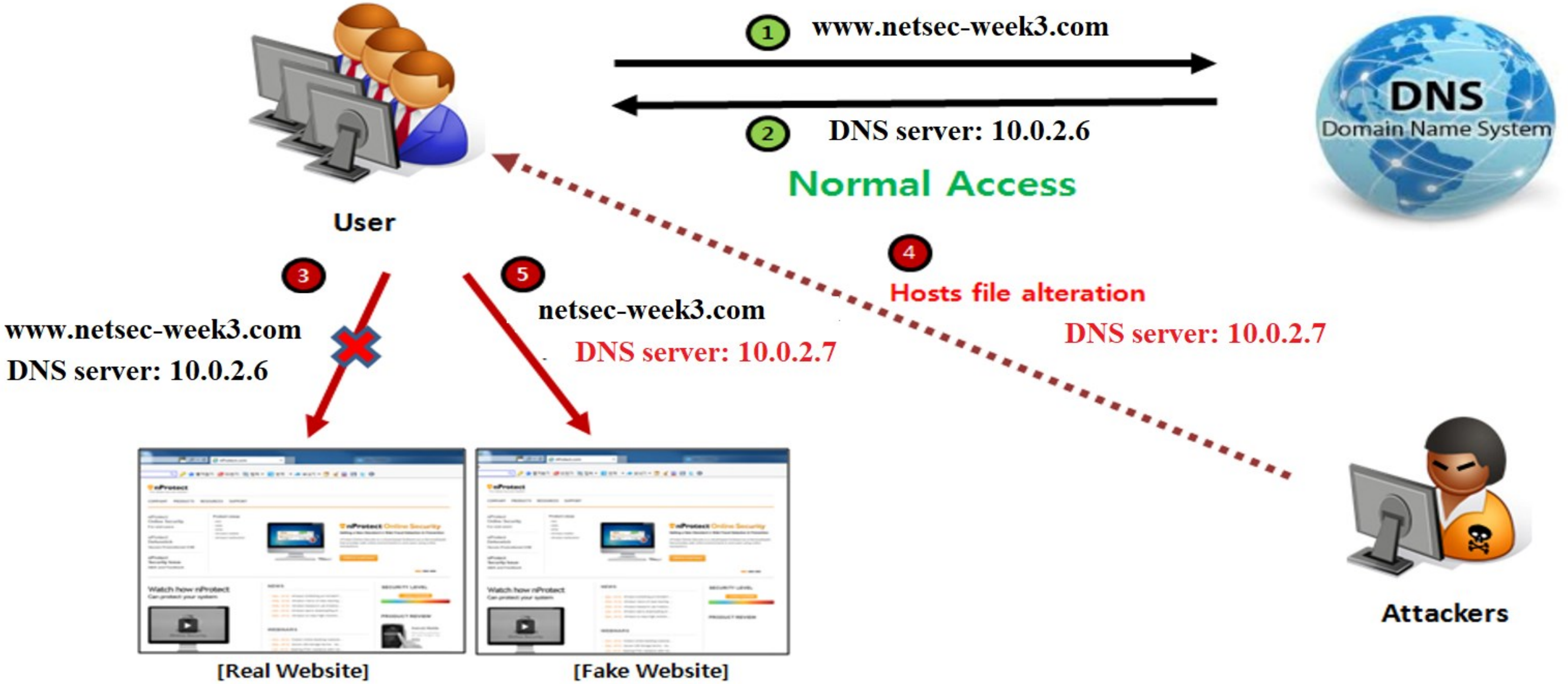
Client
10.0.2.8

Meaning
Color

3. Outline of the Lab 2

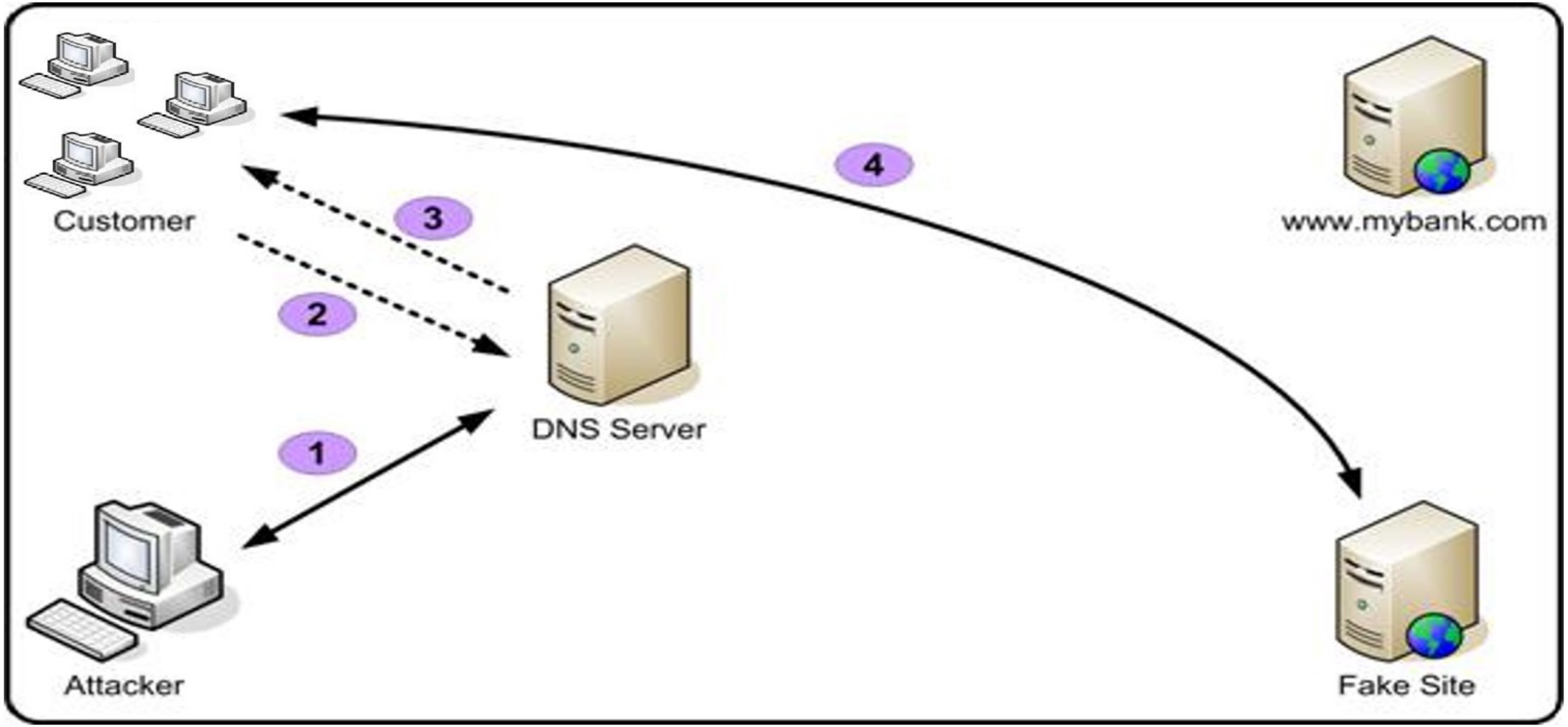
1. Checking network
2. Task 1: Pharming by modifying HOSTS file
3. Task 2: Pharming by spoofing DNS response
4. Task 3: DNS Server Cache Poisoning
5. Tidy up and sign up your machine correctly

Task 1: Pharming [4]



[4] http://nos.nprotect.com/newsletter/062014.html

Task 2 and 3: spoofing and cache poisoning [5]



[5] http://www.technicalinfo.net/papers/Pharming2.html

THANK YOU!

Question & Answer