Pharming simulation

# Introduction

You will use this worksheet to see a simulation of how an attacker can change a DNS to direct unsuspecting users to a malicious website. This simulation uses a pretend bank called CSO Bank. After the pharming attack has taken place, the user will be sent to the malicious website, COS Bank.

This activity uses **Packet Tracer**. The networks used in this simulation are based on a similar principle to the ones used in previous lessons. You will notice that there is still a home network on the left side with a single PC. You will also notice that there is:

* An ISP network with the ISP’s DNS
* A network for the “cso-bank” web server
* A network for the “cos-bank” web server

# Visit CSO Bank .

| **Steps** | **Instructions** |
| --- | --- |
| 1. **Locate** the Packet Tracer software | * Teacher enter the instructions for opening Packet Tracer on your school network here |
| 1. **Open** the A1 Pharming simulation | * Go to File > Open * Teacher enter the instructions for locating the A1 Pharming simulation here |
| 3. **Access** the browser for PC0(1) | * Make sure that you have the select tool selected:      * Click on PC0(1) in the **home network**. This is the PC that is on the far left side of the screen. * Click on **Desktop**. * Click on **Web Browser**. |
| 4. **Visit** cso-bank.com | * Type in the **URL** for the real bank, which is: [www.cso-bank.com](http://www.cambridgepunting.com) * It might take a little while to load in the first instance because the network might still be setting up. * Notice the heading on the website says “CSO Bank” and the user is required to enter their personal ID and security number. * Close the web browser window. |

# The pharming attack .

| **Steps** | **Instructions** |
| --- | --- |
| 1. Access the DNS settings | * Click on the server for the internet service provider network. * Click on **services**. * Click on **DNS**. |
| 1. Change the IP address | * You will notice that there is already an entry for CSO Bank. * Click on the CSO Bank entry to select it. * Delete the IP address in the address section above the entry. * Enter the IP address for the malicious website:   176.0.0.10   * Click **save** to update the IP address. |

# Spot the attack .

| **Steps** | **Instructions** |
| --- | --- |
| 1. Access the browser | * Click on PC0(1) in the **home network**. This is the PC that is on the far left side of the screen. * Click on **Desktop**. * Click on **Web Browser**. |
| 1. Change the IP address | * Type in the same web address that you did last time to try and access the CSO Banking site:   [www.cso-bank.com](http://www.cso-bank.com) |
| 1. Spot the difference | * Notice how the website appears to be very similar to the real CSO bank. Can you spot the difference? |

# Explorer task .

The **computer misuse act** was created in 1990. It covers **three** main offences:

* Unauthorised access to computer material
* Unauthorised access with intent to commit or facilitate the commission of further offences
* Unauthorised acts with intent to impair, or with recklessness as to impairing, the operation of a computer

There are also further offences relating to those listed above:

* Unauthorised acts causing, or creating risk of, serious damage
* Making, supplying, or obtaining articles for use in an offence

Pharming is a cyber crime. Which one of the three principles of the computer misuse act does pharming relate to? Give a reason for your answer.

|  |
| --- |

Research the computer misuse act. What is the maximum penalty (punishment) for a pharming attack?

|  |
| --- |