

Phishing Scam Quiz

Large corporations are becoming proactive in the fight against phishing scams by sending fake phishing emails to gauge susceptibility of their organization. JPMorgan duped 20% of their staff into clicking on a fake email. Test your skills against the average scam, with our Phishing Quiz. Can you (or your staff) recognize a scam?

1. Question

People are getting smarter about cyber-crime due to the frequent media exposure of these events. The result is cyber criminals developing new ways to trick the unsuspecting public. In the email below, choose which section contains a sign of phishing? Or are there no signs of phishing in this email?

The screenshot shows an email interface. At the top, the sender is 'Wells Fargo Security <noreply@wellfargo.com>' with the subject 'Wells Fargo – Unauthorized Login Attempt'. The recipient is 'William Johnson'. Below the header is an 'Action Items' bar with a '+ Get more apps' link. The main body of the email has a light green header with the Wells Fargo logo and the text 'WELLS FARGO'. Below this, it says 'Mr. Johnson,' followed by a paragraph: 'Here at Wells Fargo we take your account security very seriously. Recently, there was an unauthorized login to your account. To unlock your account, please login through the secure link below:'. A red button with the text 'CLICK HERE' is centered below the paragraph. At the bottom of the email body, it says 'Thank you, Wells Fargo Security' followed by the Wells Fargo logo and 'WELLS FARGO'. Below that, it says 'To learn more about how Wells Fargo keeps you safe, explore the resources below:'. The email footer shows 'Wells Fargo' and 'No Items' on the left, and a user profile icon on the right.

A

B

C

- A
- B
- C
- There is no evidence that this is a phishing email.

2. Question

Nearly every day, the IT professional has to be on alert for the latest cyber scam. They must use a critical eye to identify how criminals try to trick the public. Use your critical “IT eye” and choose the section that contains the sign of a scam. Or are there no signs of phishing in this email?

Sat 8/20/2016 11:04 AM

Chad Lock <clock@timeprize.com>

Time is Running Out to Collect Your Prize

To: William Johnson

Action Items + Get more apps

Mr. Johnson,

We attempted to call you last week to notify you that you were selected as the Grand Prize winner of our annual citizen drawing. We have your \$5,000 waiting for you! [CLICK HERE](#) to collect your prize.

Congratulations!

<http://timeprize.au/youwon>
Click to follow link

Chad Lock No Items

- A
- B
- There is no sign of phishing in this email.

3. Question

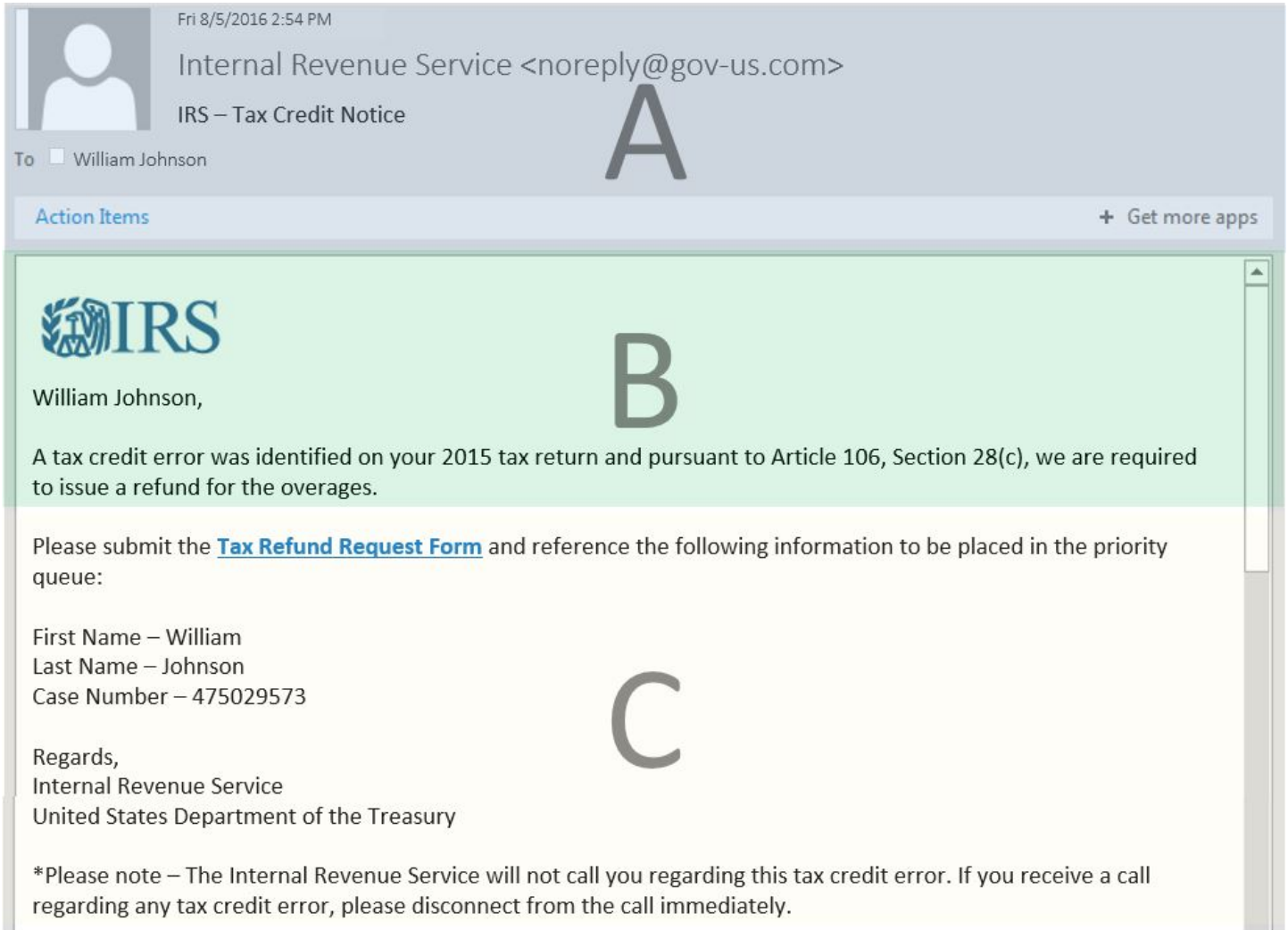
You receive a call from someone who asks for you by name stating they are calling from Microsoft Tech Support. They ask you to search your task bar for “drwizz.” You ask for more information and they respond with “I am a computer security expert from Microsoft. We have been alerted that your PC has been infected with malware and are contacting you to assist so that your network is not compromised.” Upon looking in your task bar you find “drwizz” and the representative offers to remote in to remove the “malware”. Should you allow them to assist you?



- Yes.
- No.

4. Question

No one enjoys an email from the IRS. In fact, unsolicited contact from the Internal Revenue Service could make even the coolest personality break a sweat. Take a look at this email and choose the section that contains a sign of phishing. Or are there no signs of phishing in this email?



The screenshot shows an email interface. At the top, the sender is 'Internal Revenue Service <noreply@gov-us.com>' with the subject 'IRS – Tax Credit Notice'. The recipient is 'William Johnson'. Section A is the header area. Section B is a green banner with the IRS logo and text: 'William Johnson, A tax credit error was identified on your 2015 tax return and pursuant to Article 106, Section 28(c), we are required to issue a refund for the overages.' Section C is a yellow banner with text: 'Please submit the [Tax Refund Request Form](#) and reference the following information to be placed in the priority queue: First Name – William, Last Name – Johnson, Case Number – 475029573. Regards, Internal Revenue Service, United States Department of the Treasury. *Please note – The Internal Revenue Service will not call you regarding this tax credit error. If you receive a call regarding any tax credit error, please disconnect from the call immediately.'

- A
- B
- C
- Sections A, B, and C.
- There is no sign of phishing in this email.

Answers

- 1 A. Notice the email address: wellfargo.com, not wellsfargo.com
- 2 B. This URL is taking you OUTSIDE the country to a .au website in Australia. Does that sound legitimate?
- 3 No. No one from Microsoft will be calling you and saying they have detected malware on your PC. This is not what they do. This is a malicious caller.
- 4 Sections A, B, and C. Section A has a gov-us.com return address. This should be a .gov IF you were to ever receive an email from the IRS! Section B – there is no such thing as “Article 106, Section 28(c)”, and C asks you to fill out a form for this refund. The IRS will not be sending you an email so you can get a refund.