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?

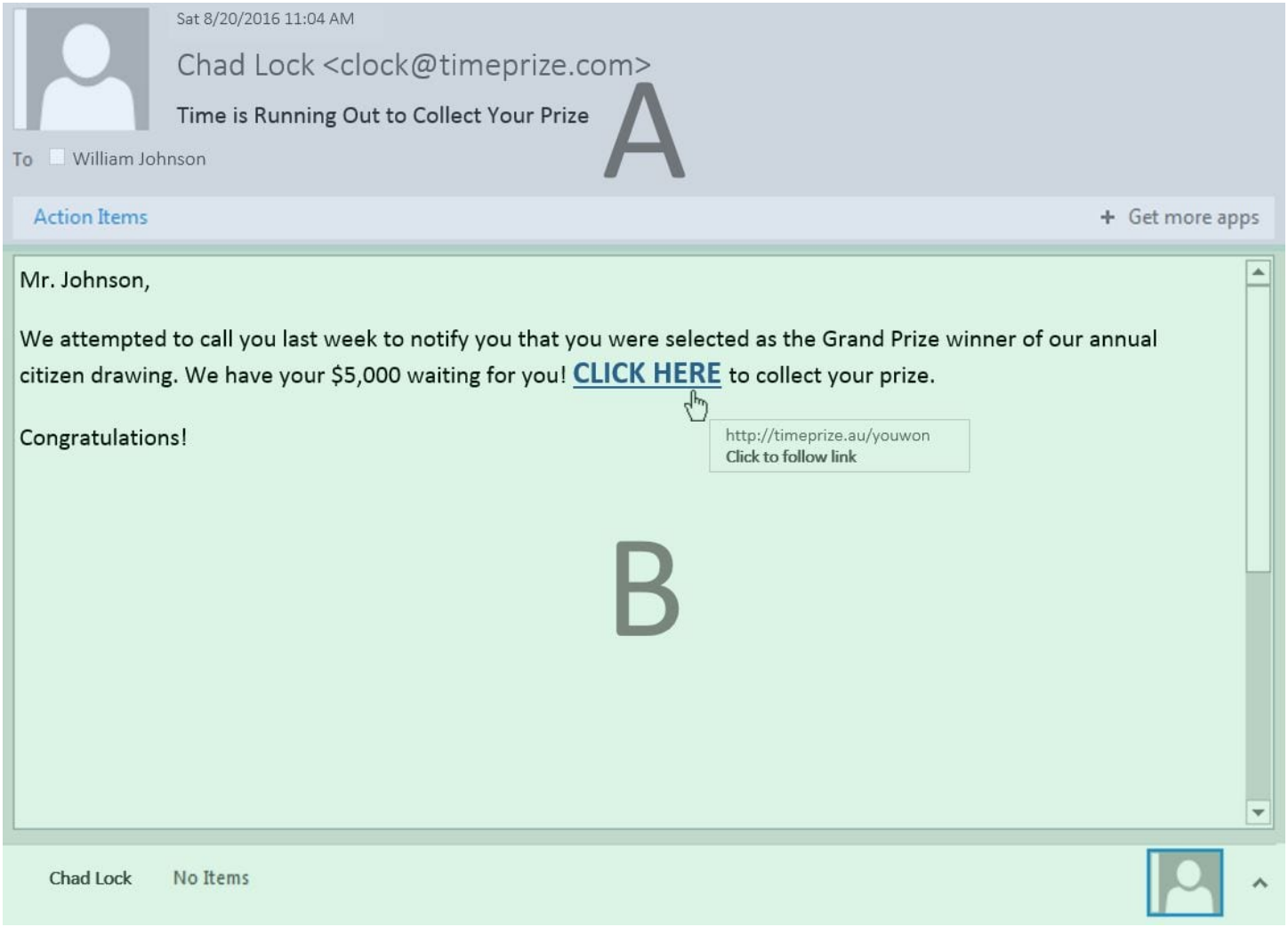
1. Question

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?

- 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?



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

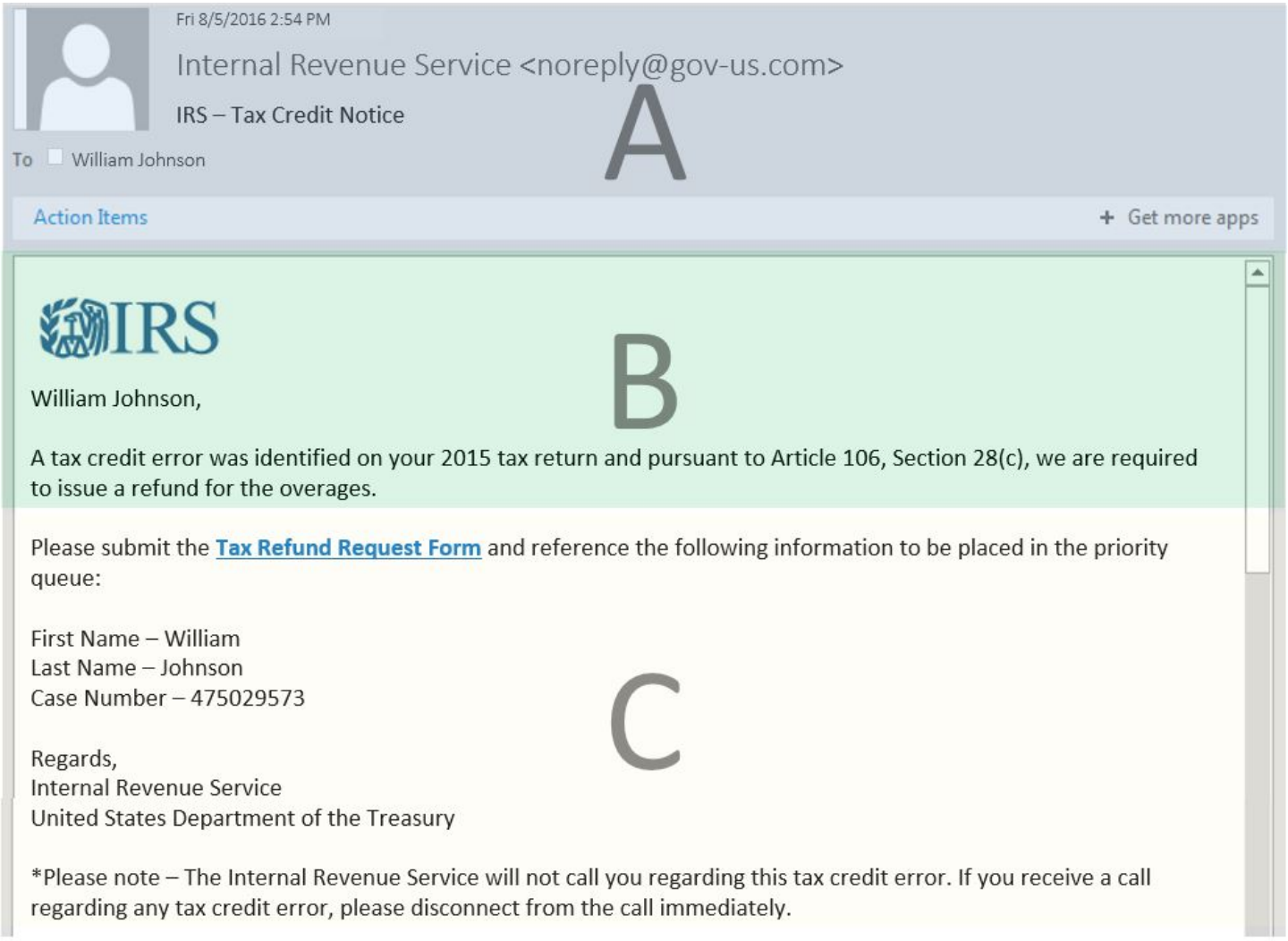
3. Question

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?



- 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.