

PHISHING CHECKLIST

HOW TO RECOGNIZE PHISHING MESSAGES

- 1 Unexpected email and generic greeting
- 2 Suspicious attachment (.zip, .exe, .doc, .jar, .pdf)
- 3 Misleading information and requests for verification of personal information
- 4 Mismatched hyperlinks
- 5 Urgent, threatening language, or rewards
- 6 Grammatical errors



Reply Reply All Forward IM

tech@t-mobile.com
Urgent: Account Cancellation **5**

Patch.zip
41 KB **2**

Dear Employee **1**
We received a notification that your computer requires a critical update.

4 [Sign in here](#) or download the zip to update your computer. If you believe this is a mistake please contact us as soon as possible.

3 If this is not resolved with 48 hours of your receiving this email, your account will be locked.

Sincerely,

tmobile tech suport **6**

T | tech support
techsupport@tmobileusa.onmicrosoft.com
800-245-1000
Tmobile

HOW TO REPORT PHISHING MESSAGES IN OUTLOOK

- 1 In Outlook's desktop app, click on the Outlook ribbon, and select Phishing
- 2 In Outlook's mobile app, tap > In the Report Message menu, tap Report as phishing and tap REPORT
- 3 If the **Report Message** button is unavailable, click Forward > Forward as Attachment. Address the email to Phish@t-mobile.com and provide details.

HOW TO REPORT A PHISHING TEXT MESSAGE

REPORTING ON AN ANDROID PHONE

- 1 In the Messages app , open the conversation.
- 2 Tap **Block** > **Report spam** > OK.

REPORTING ON AN iPhone OR iOS DEVICE

- 1 In iMessage, tap **Report Junk**
- 2 Tap