



FLAGLER BEACH POLICE DEPARTMENT

204 SOUTH FLAGLER AVENUE • FLAGLER BEACH, FL 32136

(386) 517-2023 • FAX (386) 517-2022

WWW.FBPD.ORG

CHIEF MATTHEW P. DOUGHNEY

PUBLIC AWARENESS ANNOUNCEMENT

December 15, 2016

"Active Holiday Scams"

The Flagler Beach Police Department is providing this awareness announcement in an effort to warn citizens in our community that there are active computer "scams" occurring nationwide during this holiday season. To date there have been no victims in Flagler Beach and we hope this information thwarts anyone from becoming a victim.

The first scam involves an e-mail you receive from what appears to be Amazon.com claiming there is a problem processing orders. The email message says, "You will not be able to access your account or place orders with us until we confirm your information." A "click here" link connects you to an authentic-looking Amazon webpage and asks you to confirm your name, address and credit card information (including expiration and CVV security code). After entering your personal information and hitting the "Save & Continue tab", consumers are redirected to the actual Amazon website. The information you've submitted on this webpage provides the fraudsters with everything they need to make unauthorized charges on your account. The initial e-mail message may appear as depicted below;

Example:

Subject: Your Amazon.com order cannot be shipped

Hello, There was a problem processing your order. You will not be able to access your account or place orders with us until we confirm your information. click here to confirm your account. We ask that you not open new accounts as any order you place may be delayed.

For more details, read our Amazon Prime Terms & Conditions.

Sincerely,

Amazon.com.au

© Amazon.com.au, Inc. or its affiliates. All rights reserved. Amazon, Amazon.com, the Amazon.com logo, Prime and Amazon Prime are trademarks of Amazon.com, Inc

The second scam involves an e-mail you'll receive from either "Chase Support" or "USAA". The e-mails will advise that they've "*noticed some possible problems with your account*" and that they have to suspend your account temporarily "*while they take a closer look.*" The e-mail will then direct you to click on a link, an example of which follows;

Please follow the next steps on getting your account reactivated (be sure to reference your corresponding Chase or USAA account profile information).

[Click here](#) to resolve now.

By clicking on the link you'll be forwarded to a website and asked to provide personal information, which will ultimately provide the fraudsters with information that will be used to their advantage.

If you receive suspicious e-mails of this nature please be cautious, do not click on any link or provide any personal information online in response to these e-mails. If you do receive these types of e-mails, please contact your local Law Enforcement agency for assistance.

If you have any questions regarding these active scams, please feel free to contact Chief Doughney at (386) 517-2023.

Additional information on these scams can be found at the following websites;

AARP website; <http://blog.aarp.org/2016/12/02/new-amazon-phishing-scam-confirm-your-information-to-process-order/>

Chase website: <https://www.chase.com/digital/resources/privacy-security/security/how-you-can-protect>

USAA website; https://www.usaa.com/inet/wc/security_how_avoid_identify_scams