JESUS RODRIGUEZ
ASSISTANT DISTRICT ATTORNEY

OFFICE OF
THE DISTRICT ATTORNEY
COUNTY OF SAN DIEGO

BONNIE M. DUMANIS
DISTRICT ATTORNEY

San Diego
330 West Broadway
San Diego, CA 92101
(619) 531-4040

San Diego County District Attorney

December 14, 2016
For Immediate Release

Contact: Steve Walker, (619) 531-3890
Tanya Sierra, (619) 531-3315
***En Español* Barbara Medina, (619) 531-3305**

Phishing Scams on the Rise During the Holidays; Tips to Protect Yourself

Amazon and PayPal Scams Among the Most Common

The San Diego County District Attorney's Office is warning consumers about common online scams that often increase during the holiday shopping season, including email phishing schemes that trick the public into providing financial information by posing as legitimate businesses.

Fraudsters purporting to be from Amazon and PayPal, for example, are sending email messages to unsuspecting victims warning them that there is a problem processing their order at Amazon or that the user's account has been limited at PayPal due to excessive login attempts. In both cases, the consumer is asked to resubmit personal and financial information. Both scams use the companies' official logos and can look legitimate.

"Don't fall for it," District Attorney Bonnie Dumanis said. "Always make sure you log on directly to the official website for the business identified in the email instead of linking to it from an unsolicited email. Also, don't provide personal information in response to an email."

Below is a list of tips to help you avoid becoming a victim of a holiday shopping scam:

- Use one credit card for all online purchases to avoid exposing other cards.
- Do NOT click on links from unsolicited emails; go to the website instead.
- Make sure the website is legitimate and uses an SSL indicator.
- Make sure the computer you are using has an updated anti-virus protection.
- Avoid using a public computer.
- Avoid using open Wi-Fi for financial transactions.
- Do not trust sellers who ask you to pay with a wire transfer or prepaid debit cards.

[RELATED: 3 Things You Should Know For Safe Online Shopping]

The FBI recently released a list of ways you can protect yourself online. Read the entire list, here. Below are a few tips from their list:

- Check your credit card statement routinely.
- Do not respond to unsolicited (spam) email.
- Do not click on links contained within an unsolicited email.
- Be cautious of email claiming to contain pictures in attached files, as the files may contain viruses. Only open attachments from known senders. Scan the attachments for viruses if possible.
- Avoid filling out forms contained in email messages that ask for personal information.
- Always compare the link in the email to the link you are actually directed to and determine if they actually match and lead you to a legitimate site.
- Log on directly to the official website for the business identified in the email instead of linking to it from an unsolicited email. If the email appears to be from your bank, credit card issuer, or other company you deal with frequently, your statements or official correspondence from the business will provide the proper contact information.
- If you are requested to act quickly or there is an emergency, it may be a scam. Fraudsters create a sense of urgency to get you to act quickly.
- Verify any requests for personal information from any business or financial institution by contacting them using the main contact information on their official website.

For more tips and information, visit the Computer And Technology Crime High-Tech Response Team (CATCH) Website.

###

Follow the District Attorney's Office on