URL Phishing

Spotting the Threat

The email threats faced by organizations today vary greatly in complexity, volume, and impact. Here we take a closer look so you can spot the threat before it harms you or your organization.

Cybercriminals use fake websites to trick victims into keying in sensitive information through a tactic known as URL phishing.

The sites they develop and the web addresses they use may look legitimate, but engaging can lead to identity theft, data theft, compromised networks or a number of other potentially devasting cyberattacks.
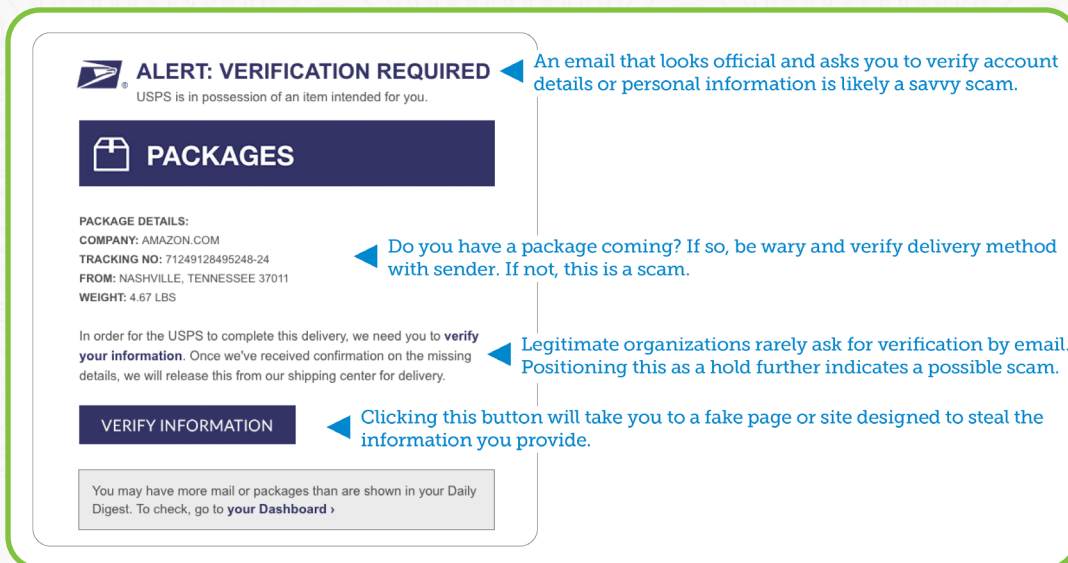
URL phishing can be avoided by:

• Being a healthy skeptic when evaluating emails you receive.

• Hovering over links in emails to reveal the true web address.

• Keying in the site name being referenced instead of clicking on any links.

• Looking closely at web pages for signs it may be fake, such as poor grammar, poor design or branding that seems off or out of date.

The sample email shown highlights some of the clues you can watch for.

Example

ALERT: VERIFICATION REQUIRED
USPS is in possession of an item intended for you.

PACKAGES

PACKAGE DETAILS:
COMPANY: AMAZON.COM
TRACKING NO: 71249128495248-24
FROM: NASHVILLE, TENNESSEE 37011
WEIGHT: 4.67 LBS

In order for the USPS to complete this delivery, we need you to **verify your information**. Once we've received confirmation on the missing details, we will release this from our shipping center for delivery.

VERIFY INFORMATION

You may have more mail or packages than are shown in your Daily Digest. To check, go to **your Dashboard ›**

An email that looks official and asks you to verify account details or personal information is likely a savvy scam.

Do you have a package coming? If so, be wary and verify delivery method with sender. If not, this is a scam.

Legitimate organizations rarely ask for verification by email. Positioning this as a hold further indicates a possible scam.

Clicking this button will take you to a fake page or site designed to steal the information you provide.