PACKAGE DELIVERY SCAMS: STAY ALERT FOR IMPOSTOR MESSAGES

Package delivery scams are a rapidly growing form of business impostor scams, where criminals impersonate legitimate delivery companies to steal personal information or money. These scams typically begin with an unexpected text, email or phone call claiming there's a problem with a delivery, such as an incorrect address or unpaid fee. These phishing (impersonated) messages often include links or phone numbers that prompt recipients to disclose sensitive personal or financial information, or to pay fees or taxes under false pretenses. To appear credible, the messages contain well-known business names and logos. These links also may install malware – any software designed to cause damage or gain unauthorized access – to steal sensitive data.

Legitimate delivery companies will not ask you for credit card details or passwords in an unsolicited text, email or phone call.

Criminals create a sense of urgency by warning that the package will be returned, or additional fees will apply if immediate action isn't taken. These scams are especially effective because online shopping is so common that the messages seem plausible.

HOW TO PROTECT YOURSELF

- Don't click on links in unsolicited messages
- Be cautious of scam indicators:
  - » Unexpected and urgent requests for payment to release a package
  - » Requests for personal or financial details (including card numbers)
  - » Links to suspicious or misspelled website or email addresses that mimic known delivery services
  - » Generic greetings or vague messages that don't include your name or the sender's identity
- Always verify tracking numbers directly with the legitimate courier service or retailer on its official website before taking any action

Report scams to the legitimate delivery service and to the Federal Trade Commission (FTC).

PACKAGE DELIVERY SCAMS: STAY ALERT FOR IMPOSTOR MESSAGES

EXAMPLES OF PACKAGE DELIVERY SCAM MESSAGES

Phishing Email: *Incomplete Information*

Hello,

We were unable to deliver your package due to incomplete information. Please click on the link to update the information: **trakpkg.bgq/178625**

If a response is not received within two business days, the package will be returned to the sender.

Thank you,

Customer Care Team

Phishing Email: *Unpaid Customs Fees*

Dear Customer,

Your package could not be delivered due to:

- *Unpaid customs fee*

Please use the button below to fix this problem. Respond ASAP to avoid penalties.

Thank you,

Delivery Team

PAY NOW

Phishing Email: *Tracking Delivery Status*

A package is on its way to you. Use the link below to track delivery status.

Pkgdeliver/axpgt.196643/

Enter the required information to track your package.

Sincerely.

Courier Service

Phishing Email: *Schedule Delivery*

An attempt to deliver a package to your address failed. Please use the link below or call us at the number provided to schedule delivery. You must respond within 24 hours to avoid extra fees.

http://service.deliver/sched.com

Your immediate attention is needed to ensure delivery.

The Customer Service Team

PACKAGE DELIVERY SCAMS: STAY ALERT FOR IMPOSTOR MESSAGES

CONCLUSION: CUSTOMER BEWARE

Just because package deliveries have become so commonplace doesn't mean we should be any less vigilant when looking for scam indicators. Be wary of companies that ask for credit card details, passwords or account information in an unsolicited email or text. It is most likely a scam.

The scams mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, use of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.