Educational Resource
Types of Phishing

Phishing

Phishing is the fraudulent practice of sending emails that appear to be from reputable companies to trick individuals into revealing sensitive information like account details, passwords, and credit card numbers. Some common methods for identifying phishing include:

- Suspicious or Slightly Changed Sender Email Address
- Destination Email Address/Recipient is Incorrect
- Urgent or Time-sensitive Response Requested
- Embedded Links or Attachments
- Asking for Confidential Information
- Asking for Payment Information
- Spelling and Grammar Errors

Spear Phishing

This type of phishing is targeted and personalized to a specific individual, group, or organization. Cybercriminals send emails to specific and well-researched targets while acting as a trusted sender. The goal is to either infect devices with malware or convince victims to hand over personal information or money.

Whaling

Whaling is a highly targeted phishing attack that targets end users that include high profile individuals like politicians, celebrities, and corporate executives to steal sensitive information. This is designed to encourage victims into authorizing high-value wire transfers to the attacker.

PCS

ALWAYS ON. ALWAYS CONNECTED.
YOUR 24/7 TECH PARTNER.

Who is PCS?

Much more than a leading managed IT services company, PCS is built on a foundation of friendly, helpful best-in-class customer service since our start in 2000.

PCS supports highly satisfied customers within numerous industries across the USA including: Small Business, Non-Profits, Accounting, Law, Medical, Insurance, Education, Engineering, Manufacturing, and more.

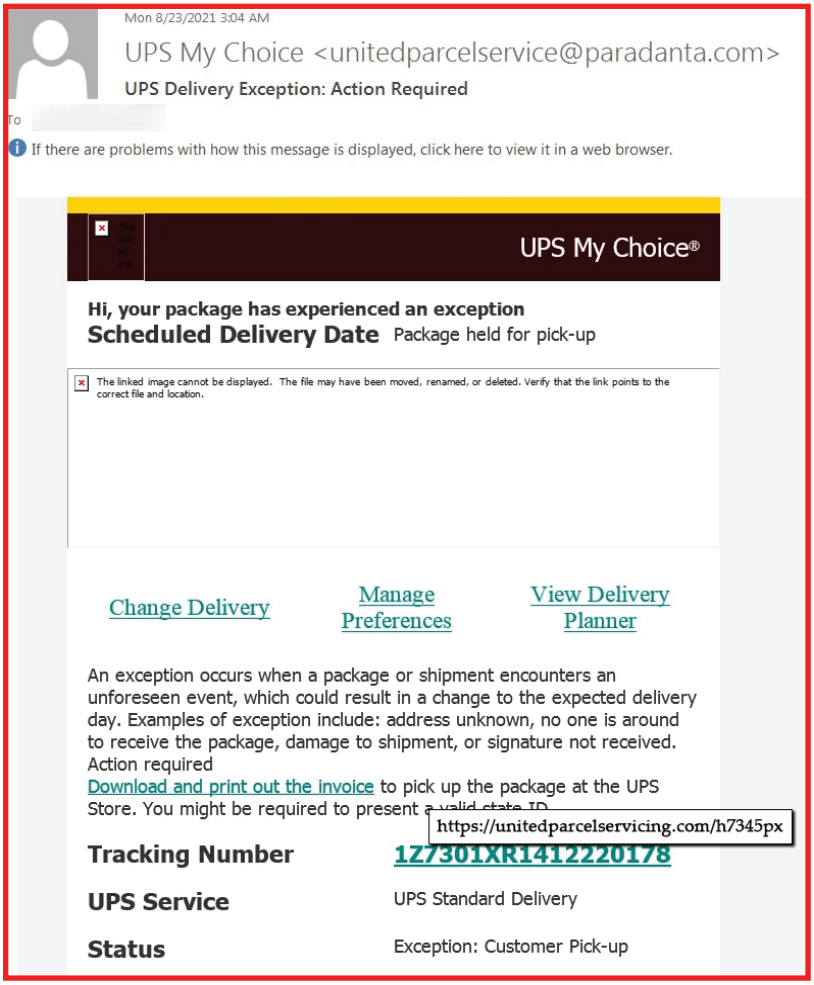
Our team of experts stand ready to help solve your technology problems. Contact PCS today to discuss your unique IT goals and needs.

www.pcsflorida.com

Test Your Skills
Phishing Identification

PCS
ALWAYS ON. ALWAYS CONNECTED.
YOUR 24/7 TECH PARTNER.

Phishing emails can be created to mimic any company, non-profit, or person. They're designed to create urgency and drive a quick reaction from you. Understanding this, if you received an email like the sample below, what would you reaction be?



Mon 8/23/2021 3:04 AM

UPS My Choice <unitedparcelservice@paradanta.com>

UPS Delivery Exception: Action Required

To

If there are problems with how this message is displayed, click here to view it in a web browser.

UPS My Choice®

Hi, your package has experienced an exception

Scheduled Delivery Date Package held for pick-up

The linked image cannot be displayed. The file may have been moved, renamed, or deleted. Verify that the link points to the correct file and location.

Change Delivery | Manage Preferences | View Delivery Planner

An exception occurs when a package or shipment encounters an unforeseen event, which could result in a change to the expected delivery day. Examples of exception include: address unknown, no one is around to receive the package, damage to shipment, or signature not received.
Action required
Download and print out the invoice to pick up the package at the UPS Store. You might be required to present a valid state ID.

https://unitedparcelservicing.com/h7345px

Tracking Number	1Z7301XR1412220178
UPS Service	UPS Standard Delivery
Status	Exception: Customer Pick-up

Some tips to help determine email validity:

1. Ask yourself if it makes sense that you should be getting an urgent shipping communication.
2. Look at the sender's email address. The domain (@paradanta.com) doesn't appear to be legitimate nor match something from UPS.
3. Without clicking anything, hover your mouse over a link to see where you are really being directed. Notice that the company name in the link is incorrect. UPS doesn't have "servicing" in its name.

This is a simplistic example of a phishing email. It's important to understand that hackers are getting increasingly better at building convincing emails. Therefore, you need to take the time to review emails with a critical eye.

Being educated in identifying phishing techniques is key to avoiding hacks. Contact PCS to learn about Phishing Training options designed to help keep you informed and safe.

www.pcsflorida.com

PCS Florida:
Lakewood Ranch, FL
info@pcsflorida.com
941.270.4446