Your Package has Arrived ID#00093321

FROM: Parcel Delivery Service <support@aucrack.com>
SENT: November 28, 2014
TO: Doe, John <john.doe@email.com>
CC: jon.info@cmail.com
SUBJECT: Your Package has Arrived ID#00093321
ATTACHMENT: OrderConfirmation.pdf (186KB)

Dear Customer,

Your parcel has arrived on November 27. We were not able to deliver it to you after repeated attempts. To receive your parcel, click on the link below, verify your address, print the label, or complete the attached document. Take the complete form to the office.

Order ID#00093321
==========
Tracking ID: 1X2FDG2345K3456
Tracking Label: http://www.fedex.com/1X2FDG2345K3456
Ship Date: 2014/11/03
==========
Fed Ex 1995 - 2014

http://www.dogboyfrx.com/dump.php?ky=3udxabe84f75cbd8430aef6=

CHECK THE E-MAIL ADDRESS.

In this example, it appears that the e-mail comes from a legitimate business, but the "FROM" address is someone's email account. Additionally, the "CC" field contains another address from someone you may or may not know or work with on a daily basis. It is good practice to be aware of the sender's e-mail address and who may be copied on the e-mail, as well.

BE SUSPICIOUS OF ATTACHMENTS.

Only click on those you are expecting. Cyber criminals hide malicious programs in phishing e-mails to hack your computer.

BE SUSPICIOUS OF HOW E-MAILS ARE ADDRESSED.

"Dear Customer" or e-mails that use other generic greetings can be a indicator of an attack. If a trusted organization has a need to contact you, they will know your name and information.

BE SUSPICIOUS OF GRAMMAR OR SPELLING MISTAKES.

Most businesses proof read their messages carefully before sending them.

Always read e-mails carefully.

BE SUSPICIOUS OF ANY E-MAIL THAT REQUIRES AN IMMEDIATE RESPONSE.

This is a technique used by criminals to rush people into making a mistake. **Stop and think** before you act on the request in the e-mail.

BE CAREFUL WITH LINKS.

In this example, it appears that the link is a valid one. However, when the mouse pointer is hovering over the link, it shows the true destination of where you would go, if you clicked it. If the destination is different to what is shown in the email, this is an indicator of an attack.

YOU SHOULD ALSO KNOW.....

- If a similar e-mail comes from your friend then it does not mean that they sent it. Your friend's computer or e-mail account may have been compromised. If you get a suspicious e-mail from a trusted friend or colleague, contact them on the phone.
- In the case of spear phishing, the cyber criminal may already know some information about you. Remember that companies will not contact you via e-mail to confirm your personal information. Always contact the company on the phone, if you receive a suspicious e-mail. **DO NOT** use the phone number listed in the e-mail. Instead use a trusted telephone directory service or official website to obtain the number.