# Lesson 3

# Emails, Spam and Phishing

It’s Important that you can recognise the difference between an email that is legitimate and one that is not. Spam emails are used for the purposes of advertising, phishing, spreading malware, etc. Have a look at the email below and see if you can spot the signs of a phishing email.

From: Mark (fnxoes2@bizeresd.com)

To: student@school.com

Subject: Final Notice – Account Closure

---

Dear Customer,

I am write to you about you’re Music and Apps account. There is an outstanding balance from your latest purchace and it needs paid as soon as you kan or your account will be clozed. Visit www.paydfdoemxke.com/pay-by-card

If you do not pay then we will seize assets from your house and press criminal changes which will result in jail time.

Thankss,

Tom - Director of Apples  Tel: 077324564***

# Lesson 3 (Continued)

# Emails, Spam and Phishing

Read the points below and you will begin to recognise the difference between legitimate emails and spam.

- **Sender's Address** – does the address look legitimate? E.g. service@PayPal.com or x3kfoce@paaypal.com
- **Mailing lists** – did you sign up to this website's mailing list?
- **Vague** – "Dear Customer," surely a legitimate company will know your name.
- **Links** – if you hover over the link you will see the hyperlink. This is the destination address. Do they match?
- **Poor Spelling and Grammar** – "We is contracting you wiht regarsd to you're account."
- **Personal Information Required** – if the email is asking for personal information and details, it is generally not a good sign. If you have given a company your details, they will have them stored.
- **Too Good to be True** – "Congratulations! You have won our competition of the month, which is an overnight stay in Lapland! Click **here** to book your flights." #DELETE #INYOURDREAMS
- **Unrealistic Threats** – "There is an outstanding balance on your account. If this is not paid IMMEDIATELY we will seize assets and press criminal charges."

# Lesson 3 (Continued)

# Emails, Spam and Phishing

**Asking for Money** – some emails pose as vulnerable, high-powered and even helpful people. Somewhere along the line, money will be asked for.

**Phone Numbers** – this is a tough one. Spammers nowadays have a reachable phone number and they will convince you that they are legitimate. Search online for customer service numbers on official websites to clarify. It would be rare that a company would use a mobile number like in the example.

## Activity – Phishing Trip

Get into pairs and create an email for your friend using some of the key SPAM features described on the previous pages. If you want to really challenge your partner, only add in one of the features previously discussed and see if they can spot it.

#PhishingTrip