

## **CYBER AND FRAUD PROTECT WEEKLY SECURITY ARTICLE**

*Thursday 17<sup>th</sup> December 2020*

**This advice has been collated by EMSOU and is intended for wider distribution within the East Midlands to raise awareness among businesses and the public.**

**If you require any further information, assistance or guidance please contact the [EMSOU Protect Team](#)**

### **UK Finance warns public to be aware of parcel delivery scams in the run up to Christmas**

UK Finance is warning consumers to be vigilant against criminals looking to defraud them by posing as parcel delivery companies, as more people across the country are expected to shop online this Christmas than ever before.



Cybercriminals are sending out phishing emails, claiming that they have been unable to deliver parcels, packages or large letters. These emails ask the recipient to pay a fee or provide additional details in order to rearrange the delivery.

Nor are these bogus messages restricted to email - cybercriminals are also making phone calls, sending text messages and posting fake delivery notices through letterboxes. Customers have been tricked into clicking on links which will take them to a fake website. Any information entered at this point, is used by the criminal to commit fraud.

#### **Advice:**

- Never follow a link. Go directly to the official website by typing the address directly into the web browser or using a reliable search engine.
- Never contact the company using a phone number contained within the message. Find the genuine customer support number online.
- Remain vigilant and check delivery notifications carefully to ensure they are genuine. Signs that the message may be fake include:
  - Generic greetings, such as Dear Sir/Madam.
  - Poor spelling and grammar.
  - Obscure addressing. The 'from' field for an email may be incorrectly spelt or appear as a strange variation of the company's name. Text messages may also show a generic mobile number rather than a company name, which you would expect to see.
- Always question claims that you are due goods or services that you haven't ordered or are unaware of, especially if you have to pay any fees upfront.

#### **Reporting**

Please report all Fraud and Cybercrime to Action Fraud by calling 0300 123 2040 or [online](#).

Forward suspicious emails to [report@phishing.gov.uk](mailto:report@phishing.gov.uk).

Report SMS scams by forwarding the original message to 7726 (spells SPAM on the keypad).