Fraudulent emails and Purchase Orders

An important message for existing and potential suppliers to the Henry Boot Group of Companies ("the Group").

We want to alert you to a fraud scam that is targeting existing and potential suppliers of equipment to the Group, as well as other businesses, nationally and globally. Please take the necessary precautions so that you are not a victim of this scam.

The scam operates in the following way:

1. A supplier will receive an email or phone call requesting a quotation for specific item/s of equipment. These may be in large or small quantities and of low to high values
2. Once the quotation has been provided, a purchase order is emailed to the supplier that bears resemblance to an authentic Group purchase order
3. The purchase order typically instructs delivery to an address that may or may not be affiliated with the Group
4. After shipping the item/s of equipment, the supplier never receives payment and is unable to retrieve the shipped products

Identifying fraudulent emails and purchase orders

The following will be evident in these fraudulent emails and purchase orders:

1. An incorrect domain name will be used to send emails and purchase orders. Ensure you verify the order is valid with the Group. We advise all suppliers to consult with their IT or cyber security advisors to ensure they remain vigilant and informed on how to identify a suspicious communication.
2. The delivery address may or may not be a Group address. Fraudulent addresses will typically be a domestic residence or a self-storage facility, often not anywhere near a Group address. Or, the delivery address may be a genuine Group address, which is later changed or redirected.
3. The email will often be poorly written with grammatical, spelling or language usage errors.
4. Use of a false or unknown contact from the Group may be used. If requests for quotations or purchase orders are received from a new Group contact that raises your suspicion, please contact us via the relevant contact details set out below or a known Group contact to verify the validity of the request. Do not contact the name/number used on the email/purchase order.
5. The e mail may use names of the Group's senior management team as contacts – **note that senior managers and Board members will never be the first point of contact in a purchasing query.**
6. Phone numbers (particularly mobile numbers) not associated with the Group may be used. Typically, a mobile number may be a "personal number" starting with "070". The Group will never use a mobile number as a first contact number for a purchase.
7. The order can be for a variety of products and may or may not be for products normally purchased by the Group.

8. Various quantities may be requested but many will be for large orders.
9. Orders may request to ship priority or overnight.

If you are ever unsure about a quotation request sent by email, or the subsequent purchase order, please contact us via the details below or a known Group contact.

Please do not attempt to call any phone numbers contained within the fraudulent emails that purport to be Group numbers as they may attract a service charge.

Advice for Suppliers

In addition to the above information, suppliers should note the following:

1. If you are ever unsure about a quotation request sent by email, or the subsequent purchase order, please contact us via the details below or a known Group contact
2. Please do not attempt to call any phone numbers contained within the fraudulent emails that purport to be Group numbers as they may attract a large, international service charge
3. Consult with your IT or cyber security advisors to ensure all are informed on how to identify a suspicious communication
4. Report the incident on Action Fraud, the UK's national reporting centre for fraud and cybercrime in England, Wales and Northern Ireland. You can report fraud or cybercrime using their online reporting service at any time; the service enables suppliers to both report a fraud and find help and support. You can also get help by calling 0300 123 2040 to speak to their fraud and internet crime specialists. When you report to Action Fraud you will receive a police crime reference number. Reports taken are passed to the National Fraud Intelligence Bureau. Action Fraud does not investigate cases and cannot advise you on the progress of a case.

What we are doing

The Group is, wherever possible, reporting all instances of known fraudulent activity to the Police via Action Fraud.

Keeping relevant Group staff members aware of all activities and updates to this situation.

Contact Details

Henry Boot Construction Limited - hbc@henryboot.co.uk
https://www.henrybootconstruction.co.uk/contact-us

Henry Boot Developments Limited - hbdl@henryboot.co.uk
https://www.henrybootdevelopments.co.uk/contact/

Hallam Land Management Limited – info@hallamland.co.uk
https://www.hallamland.co.uk/contact-us/

Henry Boot PLC – plc@henryboot.co.uk http://www.henryboot.co.uk/contact-us/

Banner Plant Limited - http://www.bannerplant.co.uk/contact