BLOG

Protecting your farming business from scams during covid-19

During Covid-19, criminals have been using every opportunity to target farming businesses with scams and malware. They will often impersonate people, other organisations and even the police, usually spending hours researching a business before contacting them, with the hope it will make it easier for them to be successful.

Contact can be made by phone, email, text, social media or even in person and the scammer will usually try to trick the business into downloading malware, parting with money or confidential information, or purchasing goods that do not exist.

Farmers have been warned to remain vigilant to suspicious websites falsely advertising vehicles and machinery.

Ian Smith, Business Development Manager – Commercial Finance at Paragon, said: "Given the restrictions that have been in place due to the ongoing coronavirus, many farmers have had to make 'big ticket' purchases online or via phone, when they would usually travel to view the item prior to purchasing. It's important that farmers remain wary and only purchase items from trusted sources."

Invoice scams, when a farmer attempts to make a payment to a legitimate payee, but the scammer intervenes is also a common tactic. It will often involve the interception of emails, where the scammer poses as the supplier, seeking payment. These scammers often know when regular payments are due, so the contact appears even more genuine.

It's advised that farmers avoid using public Wi-Fi to make payments, as personal data can be stolen, and they should ensure secure payment methods are always used.
Websites that have a 'https' web address and a padlock in the browser means that it is difficult for scammers to intercept.

The following tips can help to protect your business…

- Reject unsolicited offers, particularly those that offer 'quick fixes'
- Ensure any employees are educated on staying safe and dealing with potential scams
- Be wary of social media adverts or sponsored adverts online
- Always verify the sender of communications and do not click on links from senders that you don't know

- Avoid clicking on links and opening or downloading attachments from unknown senders
- Never give out personal details or confidential business information
- Ensure you have the latest security software on your laptop or computer
- Carry out your research on any companies you are planning on dealing with
- Carry out thorough checks of your bank statements so any suspicious activity can be flagged

What to do if you think your business has been scammed?

Law enforcement, the government and industry bodies are working together to help tackle coronavirus-related scams and prevent businesses falling victim to them.

If you or an employee suspects that your business has been scammed or fallen victim to cyber-crime, you can call Action Fraud on 0300 123 2040. The National Cyber Security Centre also has a wealth of further advice on how to keep your business safe.