Business Update – Avoiding Cyber Crime

Information correct as at 09:00am on 18.12.2020

- Most companies will not contact you via email asking you to sign in to make changes to your account.
- If you receive an email which you think may be genuine do not click on the link in the email. Go onto the web and browse manually to the site which has emailed you and login that way.
- Microsoft or Internet Service Providers will not contact you via phone, ever. If you receive a phone call from anyone do not under any circumstances let them login to your PC.

Farm accounts tend to come under more scrutiny from cyber criminals at this time of year as they know that BPS payments will be arriving. If you are at all suspicious about any contact either by email or phone, then do not respond. Listed below are some top tips to minimise the risk of Cyber fraud.

Remember

- Passwords need to be unfamiliar, unconnected words with a mix of capital letters, special characters and numbers e.g. BluePieDog5!
- Adopt the two-factor authentication process, if offered by websites such as online banking, which then provides another layer of security and privacy
- **Do not** ignore software and hardware updates – they repair weaknesses and are essential to keep you safe
- Report any and all suspicious activity to your service provider e.g., BT, Sky etc or to your IT department
- Secure all devices including smartphones
- Identify your security weaknesses and fix them – keep cyber security measures under review
- Be careful when clicking links or files in emails – Look out for odd spelling, awkwardly worded messages and strange configurations of email addresses. If in doubt – **do not click!**
- Phishers tend to send messages that require an urgent answer or authority cues that pressure you to act – **Do not respond!**
- Make doubly certain that any changes to bank details are from a genuine source – always verify by phone call to a trusted staff member
- Lock your computer when you move away from it
- Back up your data via the Cloud or with a plug in back up device

Shopping online

- Make sure the retailer is legitimate – many offers contain links to fake websites. Do some research
- Use a credit card for online purchases as most credit card providers protect online purchases and are obliged to give a refund in certain circumstances
- Paying by PayPal, Apple Pay or Google Pay also means the vendor will not see your bank details and these platforms have their own dispute resolution processes
- When it is time to pay online – check to see that there is a 'closed padlock' icon in the browser address bar

For more detailed information: https://www.cyberaware.gov.uk