Oxfordshire businesses warned to protect against COVID19 scams

Businesses in Oxfordshire must be vigilant against scams and fraud…
Malicious email attachments, false government grant phone calls and CEO impersonation scams are among a raft of scams undermining businesses as a result of the COVID-19 pandemic.
Oxfordshire County Council is supporting *Businesses Against Scams* – an initiative from National Trading Standards; with a free online training tool to protect businesses, employees and customers from costly scams.
With remote working and many businesses having to stop or diversify their trading practices, criminals are seizing the opportunity to target employees who are isolated from colleagues. Scams include criminals impersonating government officials or a senior member of the business in order to put pressure on employees to give out sensitive information or make payments.
Criminals will also try and gain access to businesses devices and networks, and everything stored on them. They can do this by:

- Sending emails with malicious attachments;
- Exploiting vulnerabilities in operating systems if they are not up-to-date;
- Trying to get you to click links or visit malicious websites.

Once they have access to a device and to data, they may try to steal that data or extract money by getting businesses to pay a ransom.
At a time when Oxfordshire businesses are already facing challenges posed by the coronavirus pandemic, the proliferation of related scams are adding further strain. This includes scams directly targeting businesses – such as tax refund frauds – which can lead to significant financial losses for businesses.
Scams targeting customers also undermine businesses, causing reputational damage and potential loss of custom. The emotional and mental impact on employees and business owners who have fallen victim to a scam can also be devastating and long-lasting.
The increased risk for businesses has led National Trading Standards to encourage more businesses to join *Businesses Against Scams.* The initiative provides free tools for businesses to help upskill and train their workforce, through free online training modules that will help staff identify and prevent potential scams. Businesses can take the training and sign up at: www.friendsagainstscams.org.uk/BAS.

Councillor Judith Heathcoat, Oxfordshire County Council's cabinet member for Community Safety, said:
"Criminals will use every opportunity to defraud, and they don't care 'one iota' about the devastation it can cause to businesses or residents.
"We want everyone in Oxfordshire to be vigilant. That's why we are supporting *Businesses Against Scams* as a free tool for organisations to help them to protect their business, their staff and their customers.
"Businesses in Oxfordshire must be vigilant against scams and fraud."

Four common scams targeting businesses include:
Government grant/tax refund scams – A business is contacted by phone, email or post by government imposters suggesting the business might qualify for a special

COVID-19 government grant or a tax refund. Variations on the scheme involve contacts through text messages, social media posts and messages.
Businesses should be cautious about unexpected urgent communications offering financial assistance. Check that the information is genuine by using official government websites.
Invoice/mandate scams – A business may be contacted out of the blue by someone claiming to be from a regular supplier. They state that their bank account details have changed and will ask you to change the payment details.
Never rush a payment. Use contact details that you have used before to check that it is genuine.
CEO impersonation scams - A sophisticated scam that plays on the authority of company directors and senior managers. An employee receives a phone call or email from someone claiming to be a senior member of staff – they ask for an urgent payment to a new account and instil a sense of panic. Scammers may even hack a staff email account or use spoofing software to appear genuine.
Be cautious about unexpected urgent requests for payment and always check the request in person if possible.
Tech support scams – With more people working remotely and IT systems under pressure, criminals may impersonate well-known companies and offer to repair devices. Criminals are trying to gain computer access or get hold of passwords and login details. Once they have access, criminals can search the hard drive for valuable information.
Always be suspicious of cold callers. Genuine companies would never call out of the blue and ask for financial information.

If a business believes they have been the victim of a scam they must contact their bank immediately and report any suspicious activity to Action Fraud www.actionfraud.police.uk or by calling 0300 123 2040.
Businesses Against Scams is a new element of the successful *Friends Against Scams* initiative, run by National Trading Standards to provide free online training to protect and prevent people from becoming victims of scams www.friendsagainstscams.org.uk/