29th April 2020

ONLINE TOOL TACKLES BUSINESS SCAMS

Businesses are being warned that they are in the sights of criminals trying to cash in on the coronavirus pandemic.

Like scams against individuals, scams targeting businesses are on the rise as fraudsters try to take advantage of the current difficulties.

Malicious email attachments, false government grant phone calls and emails impersonating senior staff are among a raft of scams targeting businesses.

The increasing risk has led National Trading Standards to launch ‘Businesses Against Scams’ – a free online training tool to protect businesses, employees and customers from costly scams.

With remote working common and many businesses having to stop entirely or diversify, 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 to 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 your 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 your device and your data, they may try to steal your data or extract money from you by getting you to pay a ransom.

‘Businesses Against Scams’ 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 https://www.friendsagainstscams.org.uk/BAS.

Rebecca Elliott, Trading Standards Officer at Pembrokeshire County Council urged County businesses to get involved.

“We are seeing a rise in scams targeting businesses during this period of uncertainty.

“With staff working from home, moved to other duties and so on there is greater opportunity for scammers to try to take advantage.

“The ‘Businesses Against Scams’ initiative empowers businesses and their employees to take a stand against scams by equipping them with the advice and knowledge on how to identify and prevent a scam.”

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 https://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/

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.