Procurement Newsletter

November 2023

- Cyber-attacks on business
- Actions to prevent Invoice Scams, Mandate and Push Fraud
- Actions to protect your business from Phishing and Ransomware
- Additional Resources

POST OFFICE

Procurement Newsletter

We are the Post Office and there is no-one like us. From our travel and financial services, passports to postage, the Post Office network is serving communities across the UK. We have a network of more than 11,500 branches across the UK and every one of our branches is at the heart of its community.

We are introducing a series of quarterly newsletters to our Supplier partners to:

- Raise awareness of our values and the subjects that matter to us.
- Provide news, information and training that will help you to do business with us.
- Help you find opportunities to work with us as we grow and change for the future.

Cyber-attacks on Business

Companies and sole traders use technology for all aspects of their operations, especially to process financial transactions. It is important that all our supply chain partners are aware of the potential risks from cyber-attacks, and the steps they can take to prevent it. There are many types of attempted fraud that you might be targeted with, but here are a few of the more common cyber-attacks directed at financial transactions:

1. Invoice Scams are where criminals send an invoice or bill to a business which might appear to be a genuine request for payment for goods or services. The invoice might say that payment is overdue and may even be accompanied by threats that non-payment will result in credit recovery action or a bad mark on your credit rating. This is a way of trying to pressurise your account staff into paying for goods and services that haven't been ordered or received. The invoice is a fake.
2. Mandate Fraud is where criminals contact businesses via email, usually claiming to be from a company that they have been dealing with. They will inform them of a change of bank account details and request a payment to be made to the new account which they control. They may be using a fake e-mail address which will seem very similar to the genuine business or customer addressees. The request is fraudulent.
   In the case of Payment Diversion Fraud (a type of Mandate Fraud) they might have access to the real business or customer emails accounts (via a phishing or hacking attachment) to identify and target genuine payments. Examples that are often reported are transfers to conveyancing solicitors but electronic transfers of funds of any kind are at risk.
3. Push Fraud is where a criminal will impersonate someone such as a member of your management to request that you make an urgent or sensitive payment. This could be a direct payment, or it might be to support invoice scam. We often see stories in the media about people who have been phoned by a stranger, someone impersonating a bank, or other trusted institution. In business though, the names that staff know are used, playing on the desire to be helpful and unwillingness to question senior colleagues.
4. Phishing is a type of cyber-attack where attackers attempt to trick individuals into divulging sensitive information such as usernames, passwords, and financial details. They can use this to access your system or give them information to persuade your staff that their other types of attack are genuine.
5. Ransomware is a type of cyber-attack where hackers will take control of your systems and claim that they will sell or destroy data unless a ransom is paid. They may also exploit your data to attack your customers and suppliers by impersonating you.

See the link to Action Fraud under Additional Resources below for an extensive list of fraud types that you could be exposed to.

Actions to prevent Invoice Scams, Mandate and Push Fraud

To protect yourself from these types of fraud, here are some points to be consider:

Email and Communication Authenticity:

- Be cautious of any emails requesting changes to payment details. Assume that they are fraudulent until they can be validated. Incoming phone calls should also be viewed with suspicion.
- If there is a way for suppliers and customers to maintain their own account information on a system, this should be the preferred option.

Robust Processes and Validation of data

- Change requests for payment or other details should be checked with the company directly by calling them on a known phone number or in person with existing account managers.
- Consider using a bank account validation solution to carry out basic checks, there are several available online.
- Educate your own staff on the dangers of impersonation and push fraud; and have robust processes internally for them to communicate with finance colleagues.

Separation of duty

- Payment processes should have two stages, with built in separation so that the decision to make a payment does not fall solely to one person. This enables the necessary sense checks and questioning of the request that could reduce your risks.

Delay

- Don't be rushed and listen to your instincts. You are protecting your business.
- Criminals may try to rush or panic you into action, but a genuine customer/ supplier will understand the need for caution.

Actions to protect your business from Phishing and Ransomware

To protect yourself from phishing, here are the top 5 points to be aware of:

Email and Website Authenticity:

- Be cautious of unsolicited emails, especially those requesting personal information or providing urgent warnings.
- Check the sender's email address for inconsistencies or slight variations from legitimate addresses.
- Hover over links in emails to preview the actual URL. Verify that the URL matches the expected destination and is spelled correctly.

Official Communication Channels:

- Legitimate organizations typically do not request sensitive information via email.
- If you receive an unexpected email claiming to be from a known organization, contact them directly using official contact information to verify the request.

Security Indicators:

- Look for security indicators in emails, such as misspelled words, poor grammar, or generic greetings, as these may be signs of a phishing attempt.
- Legitimate websites use encryption (https://) to secure data transmission. Be cautious if a website lacks this encryption, especially if it involves entering sensitive information.

Attachments and Downloads:

- Avoid opening attachments or downloading files from unknown or suspicious sources.
- Malicious software (malware) can be disguised as seemingly harmless files, so only download attachments from trusted sources.

Use Multi-Factor Authentication (MFA):

- Enable multi-factor authentication whenever possible to add an extra layer of security. Even if your password is compromised, MFA helps protect your accounts. MFA often involves receiving a code on your phone or email in addition to entering your password, making it more difficult for attackers to gain unauthorized access.
- By staying vigilant and following these guidelines, you can significantly reduce the risk of falling victim to phishing attacks. Always prioritize the security of corporate and sensitive information.

Additional Resources

NCSC (National Cyber Security Centre): https://www.ncsc.gov.uk/collection/small-business-guide/avoiding-phishing-attacks
NCSC Small Business Guide: https://www.ncsc.gov.uk/collection/small-business-guidance--response-and-recovery
Action Fraud https://www.actionfraud.police.uk/business-protection
Poster https://data.actionfraud.police.uk/cms/wp-content/uploads/2022/03/2a.-Payment-Diversion-Fraud-Business-Email-Compromise-BEC-Flyer.pdf
British Library Ransomware Attack https://www.bbc.co.uk/news/entertainment-arts-67484639
Cyber Attack impacting several businesses https://www.thisismoney.co.uk/money/mortgageshome/article-12799857
Push Fraud example https://www.bbc.co.uk/news/uk-england-kent-67198918
0

Who do I contact for help?

Please read the guidance on our website **https://corporate.postoffice.co.uk/en/governance/our-suppliers/working-with-us/**

If you require any further advice please contact procurement@postoffice.co.uk